Akademia Bialska im. Jana Pawła II

CYBERZAGROŻENIA W SEKTORACH BEZPIECZEŃSTWA PAŃSTWA



Redakcja naukowa
Tomasz Grudniewski
Marta Chodyka
Zbigniew Ciekanowski

Biała Podlaska 2026

Akademia Bialska im. Jana Pawła II

CYBERZAGROŻENIA W SEKTORACH BEZPIECZEŃSTWA PAŃSTWA

Redakcja naukowa
Tomasz Grudniewski
Marta Chodyka
Zbigniew Ciekanowski

Biała Podlaska 2026

Wydawca

Akademia Bialska im. Jana Pawła II

Recenzja

prof. dr hab. inż. dr h.c. Jarosław Wołejszo

płk prof. dr hab. inż. Leszek Elak

Redaktor techniczny

mgr inż. Ewelina Melaniuk

© Copyright by Akademia Bialska im. Jana Pawła II

Książka jest udostępniana na licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne – Bez utworów zależnych 4.0 Międzynarodowa

ISBN 978-83-68103-37-3

https://doi.org/10.29316/9788368103373

Nakład: 50 egzemplarzy

Wydawnictwo AB JPII

ul. Sidorska 95/97

21-500 Biała Podlaska

wydawnictwo.akademiabialska.pl

Projekt okładki, skład i druk:

druk-24h.com.pl

DRUKARNIA CYFROWA

Hurtowa 21, 15-399 Białystok

tel. 535 500 898

e-mail: studio@druk-24h.com.pl

Spis treści

Wprowadzenie. 7

Ireneusz Fura
Strukturalne uwarunkowania zagrożeń bezpieczeństwa globalnego w perspektywie do 2034 roku 11

Iwona Lasek-Surowiec, Małgorzata Zdunek, Marek Giec
Zagrożenia asymetryczne we współczesnym środowisku bezpieczeństwa 35

Leszek Elak, Marek Ciekanowski
Charakterystyka i uwarunkowania współczesnych zagrożeń bezpieczeństwa – aspekty militarne, cybernetyczne i środowiskowe . 53

Jakub Bieniek, Sławomir Żurawski, Marcin Oskierko
System zarządzania kryzysowego NATO w architekturze współczesnego bezpieczeństwa międzynarodowego 71

Marcin Oskierko, Sławomir Żurawski, Marek Giec
Rola zarządzania kryzysowego Unii Europejskiej w kształtowaniu bezpieczeństwa europejskiego 89

Dariusz Brążkiewicz, Rafał Mazurek
Budowa strategicznego bezpieczeństwa cyberobrony sił zbrojnych RP 105

Marta Chodyka
Cyberodporność systemów granicznych 125

Marcin Oskierko, Aleksandra Żaneta Nasiadka
Rola Wojsk Obrony Terytorialnej w ochronie granicy państwowej w warunkach kryzysu migracyjnego – ujęcie systemowe i praktyczne 149

Marcin Chodyka
Migracje zarobkowe i bezpieczeństwo gospodarcze państwa 169

Karolina Włodarczyk
Zatrudnianie cudzoziemców spoza Unii Europejskiej – szanse i zagrożenia dla bezpieczeństwa gospodarczego państwa 189

Radosław Dawidziuk
Percepcja ryzyka geopolitycznego a gotowość do mobilności akademickiej wśród studentów uczelni wyższej 211

Karol Zygo
Hybrydyzacja zagrożeń na granicy polsko-białoruskiej a zdrowie publiczne. Analiza ryzyk epidemiologicznych i systemowych w warunkach wymuszonej migracji 235

Oskar Stefański
Cyberzagrożenia a proces transformacji energetycznej. W jaki sposób nowe zagrożenia mogą spowalniać proces transformacji energetycznej państwa na przykładzie Polski? 255

Tomasz Grudniewski
Bezpieczeństwo energetyczne państwa w erze decentralizacji dostaw 273

Małgorzata Orłowska, Michał Mogilnicki
Wybrane cyberzagrożenia w logistyce XXI w. Wykorzystanie sztucznej inteligencji w ochronie łańcuchów dostaw 289

Zbigniew Piskor
Ewolucja cyberzagrożeń transportu lotniczego 309

Sławomir Żurawski, Marek Ciekanowski, Rafał Parczewski
Zarządzanie bezpieczeństwem transportu publicznego w aglomeracjach miejskich w Polsce 325

Ewelina Melaniuk
Taksonomia incydentów ransomware 2024-2025 341

Elżbieta Cygnar, Agata Bubenko, Sławomir Żurawski
Cyberbezpieczeństwo dzieci i młodzieży w dobie współczesnych zagrożeń 355

Dorota Charkiewicz, Marcin Czosnek
Prawo pacjenta do ochrony tajemnicy medycznej w świetle ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta 369

Ireneusz Fura
Wybrane zagrożenia bezpieczeństwa globalnego 385

Zbigniew Ciekanowski, Wiesława Załoga, Martyna Zaroślak
Rola wojsk obrony cyberprzestrzeni w systemie bezpieczeństwa państwa wobec zagrożeń hybrydowych 415

Marta Chodyka
Model zarządzania incydentem cyberbezpieczeństwa w administracji odpowiedzialnej za ochronę granic 431

Tomasz Grudniewski
Bezpieczeństwo energetyczne państwa a detekcja anomalii z wykorzystaniem LSTM Autoencoder i danych ENTSO-E 445

WPROWADZENIE

Współczesne bezpieczeństwo państwa coraz rzadziej daje się opisać w kategoriach odseparowanych domen: „wojskowej", „wewnętrznej", „gospodarczej" czy „społecznej". Logika ryzyka przesuwa się w stronę środowiska sieciowego i systemów krytycznych, a zagrożenia nabierają charakteru wielowarstwowego: łączą presję polityczną z oddziaływaniami informacyjnymi, sabotażem cyfrowym, wymuszeniami ekonomicznymi i działaniami na granicach państw. W rezultacie cyberprzestrzeń nie jest już jedynie kanałem wsparcia dla tradycyjnych operacji, lecz przestrzenią współkształtującą dynamikę konfliktów, podatność infrastruktury oraz ciągłość funkcjonowania instytucji publicznych. To właśnie w tym kontekście powstała niniejsza monografia, poświęcona cyberzagrożeniom w sektorach bezpieczeństwa państwa.

Za punkt wyjścia przyjmujemy założenie, że odporność państwa wymaga ujęcia systemowego: rozpoznania zależności między instytucjami i sektorami, identyfikacji węzłów krytycznych (infrastruktura, dane, łańcuchy dostaw, zasoby ludzkie), a także integracji mechanizmów prewencji, reagowania i odbudowy. Cyberzagrożenia nie uderzają bowiem wyłącznie w serwery i sieci, ale przede wszystkim w procesy – decyzyjne, logistyczne, operacyjne, finansowe i społeczne – które umożliwiają realizację zadań państwa. Skutkiem może być nie tylko utrata poufności lub dostępności danych, lecz także paraliż usług, destabilizacja zaufania, eskalacja napięć oraz wymierne koszty gospodarcze i zdrowotne. Struktura tomu prowadzi czytelnika od poziomu strategicznego i geopolitycznego, przez architekturę bezpieczeństwa międzynarodowego i narodowego, aż po analizy sektorowe oraz problematykę wrażliwych grup i danych szczególnie chronionych. Pierwszy

blok koncentruje się na diagnozie środowiska bezpieczeństwa i jego ewolucji. Ireneusz Fura w rozdziale otwierającym przedstawia strukturalne uwarunkowania zagrożeń bezpieczeństwa globalnego w perspektywie do 2034 roku, wskazując długofalowe czynniki kształtujące ryzyko: napięcia geopolityczne, zależności gospodarcze, zmiany technologiczne i rosnącą rolę instrumentów niemilitarnych. Uzupełnieniem tej perspektywy jest analiza Iwony Lasek-Surowiec, Małgorzaty Zdunek i Marka Gieca dotycząca zagrożeń asymetrycznych, które w praktyce stanowią jeden z najczęściej wykorzystywanych modeli oddziaływania na państwa – zwłaszcza wtedy, gdy agresor dąży do uzyskania efektu politycznego przy ograniczonych kosztach i z zachowaniem wiarygodnej zaprzeczalności. Drugi blok podejmuje problem odporności instytucjonalnej i zarządzania kryzysowego w wymiarze sojuszniczym i unijnym. Jakub Bieniek, Sławomir Żurawski i Marcin Oskierko analizują system zarządzania kryzysowego NATO w architekturze współczesnego bezpieczeństwa międzynarodowego, pokazując, w jaki sposób mechanizmy planowania, koordynacji i wymiany informacji wpływają na zdolność do reagowania na zdarzenia o charakterze wielodomenowym, w tym cybernetycznym. Z kolei Marcin Oskierko, Sławomir Żurawski i Marek Giec przedstawiają rolę zarządzania kryzysowego Unii Europejskiej w kształtowaniu bezpieczeństwa europejskiego – perspektywę szczególnie istotną w kontekście współdziałania państw członkowskich, ochrony infrastruktury oraz wzmacniania odporności wspólnych polityk i rynków. Trzeci blok skupia się na wymiarze obronnym i granicznym, gdzie cyberzagrożenia splatają się z presją hybrydową i wyzwaniami operacyjnymi. Dariusz Brążkiewicz i Rafał Mazurek podejmują temat budowy strategicznego bezpieczeństwa cyberobrony Sił Zbrojnych RP, akcentując znaczenie zdolności defensywnych, rozwoju kompetencji, procedur oraz integracji cyberobrony z innymi komponentami systemu obronnego. W podobnej logice – łączącej ujęcie systemowe i praktyczne – Marcin Oskierko i Aleksandra Żaneta Nasiadka analizują rolę wojsk obrony terytorialnej w ochronie granicy państwowej w warunkach kryzysu migracyjnego. Ten wątek poszerzają rozdziały odnoszące się do bezpieczeństwa gospodarczego i migracji: Marcin Chodyka omawia migracje zarobkowe w kontekście bezpieczeństwa gospodarki państwa, a Karolina Włodarczyk przedstawia szanse i zagrożenia wynikające z zatrudniania cudzoziemców spoza UE. Karol Zygo dopełnia ten obraz

analizą hybrydyzacji zagrożeń na granicy polsko-białoruskiej w powiązaniu ze zdrowiem publicznym, akcentując ryzyka epidemiologiczne i systemowe w warunkach wymuszonej migracji. Tak ujęta problematyka pokazuje, że granica państwowa jest dziś nie tylko linią geograficzną, lecz węzłem oddziaływań politycznych, społecznych, informacyjnych i logistycznych – podatnym także na zakłócenia cyfrowe i operacje wpływu. Czwarty blok obejmuje bezpieczeństwo sektorowe, w którym cyberryzyka stają się czynnikiem ograniczającym tempo rozwoju i stabilność usług krytycznych. Oskar Stefański analizuje cyberzagrożenia w procesie transformacji energetycznej, stawiając pytanie o to, w jaki sposób nowe ryzyka mogą spowalniać transformację państwa – na przykładzie Polski. Małgorzata Orłowska i Michał Mogilnicki podejmują temat wybranych cyberzagrożeń w logistyce XXI wieku, koncentrując się na wykorzystaniu sztucznej inteligencji w ochronie łańcuchów dostaw. Zbigniew Piskor przedstawia ewolucję cyberzagrożeń transportu lotniczego – obszaru o wysokiej wrażliwości operacyjnej i regulacyjnej, gdzie bezpieczeństwo cyfrowe jest warunkiem niezawodności, ciągłości i zaufania. Sławomir Żurawski, Marek Ciekanowski i Rafał Parczewski analizują z kolei zarządzanie bezpieczeństwem transportu publicznego w aglomeracjach miejskich w Polsce, akcentując znaczenie integracji systemów, koordynacji instytucjonalnej oraz zarządzania ryzykiem w środowisku złożonych zależności infrastrukturalnych i społecznych. Piąty blok skupia się na specyficznych typach zagrożeń oraz środowiskach operacyjnych. Ewelina Melaniuk przedstawia taksonomię incydentów ransomware 2024-2025, porządkując zjawisko, które w ostatnich latach stało się jednym z najdotkliwszych instrumentów presji na instytucje publiczne i przedsiębiorstwa, łącząc cyberatak z wymuszeniem ekonomicznym oraz ryzykiem ujawnienia danych. Teksty te podkreślają, że cyberzagrożenia są problemem przekrojowym: dotyczą zarówno systemów typowo lądowych i administracyjnych, jak i środowisk, w których bezpieczeństwo zależy od integracji sensorów, łączności, danych i procedur współdziałania. Szósty blok podejmuje kwestie szczególnie wrażliwe społecznie i prawnie: bezpieczeństwo dzieci i młodzieży oraz ochronę danych medycznych. Elżbieta Cygnar, Agata Bubenko i Sławomir Żurawski analizują cyberbezpieczeństwo dzieci i młodzieży w dobie współczesnych zagrożeń, wskazując na konieczność działań edukacyjnych, profilaktycznych i systemowych. W obszarze ochrony zdrowia Dorota Charkiewicz

i Marcin Czosnek omawiają prawo pacjenta do ochrony tajemnicy medycznej w świetle ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Wspólnym mianownikiem tych rozdziałów jest teza, że bezpieczeństwo cyfrowe ma bezpośredni wymiar humanocentryczny: dotyka ochrony najsłabszych uczestników systemu oraz danych, których naruszenie może mieć poważne konsekwencje dla życia, zdrowia i godności. Tom zamyka rozdział Ireneusza Fury poświęcony wybranym zagrożeniom bezpieczeństwa globalnego, który domyka kompozycję monografii, ponownie osadzając analizowane zjawiska w szerszym kontekście ryzyk i trendów o znaczeniu międzynarodowym. Taka klamra kompozycyjna podkreśla, że cyberzagrożenia sektorowe – choć ujawniają się lokalnie i instytucjonalnie – są często odbiciem procesów globalnych, technologicznych i geopolitycznych.

Niniejsza monografia ma charakter problemowy i aplikacyjny. Łączy analizy strategiczne i instytucjonalne z ujęciami sektorowymi, prawnymi i społecznymi, oferując zarówno diagnozę, jak i wskazania użyteczne dla praktyków. Adresujemy ją przedstawicielom administracji publicznej, służbom i formacjom odpowiedzialnym za bezpieczeństwo, Siłom Zbrojnym, ekspertom cyberbezpieczeństwa, osobom zajmującym się zarządzaniem ryzykiem i ciągłością działania, środowisku akademickiemu, a także wszystkim, którzy podejmują decyzje w obszarach krytycznych dla odporności państwa.

Miłej lektury – Redaktorzy

Ireneusz Fura[1]
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej, Warszawa

https://doi.org/10.29316/9788368103373_1

STRUKTURALNE UWARUNKOWANIA ZAGROŻEŃ BEZPIECZEŃSTWA GLOBALNEGO W PERSPEKTYWIE DO 2034 ROKU

STRUCTURAL FACTORS UNDERLYING GLOBAL SECURITY THREATS: A OUTLOOK THROUGH 2034

Streszczenie

Celem rozdziału jest analiza współczesnych i przyszłych uwarunkowań rozwoju przestępczości zorganizowanej w perspektywie globalnej oraz identyfikacja kluczowych czynników wpływających na jej ewolucję w kontekście zmian technologicznych, społeczno-gospodarczych i geopolitycznych. Szczególna uwaga została poświęcona roli nowych technologii, procesów globalizacji, migracji oraz niestabilności politycznej jako determinantów rozwoju międzynarodowych sieci przestępczych. Główny problem badawczy sformułowano: W jaki sposób zmiany technologiczne, ekonomiczne i społeczno-polityczne wpływają na rozwój oraz transformację współczesnej przestępczości zorganizowanej w skali globalnej? Problem ten obejmuje również zagadnienia związane z wykorzystaniem cyberprzestrzeni, systemów

[1] https://orcid.org/0000-0003-0649-2395, e-mail: irekfura@poczta.onet.pl

finansowych oraz słabości instytucji państwowych przez zorganizowane grupy przestępcze. W opracowaniu zastosowano przede wszystkim metody jakościowe. Wykorzystano analizę literatury przedmiotu oraz analizę dokumentów i raportów instytucji międzynarodowych, takich jak raporty Europolu, World Economic Forum czy Haskiego Centrum Studiów Strategicznych. Zastosowano także metodę analizy porównawczej oraz metodę analizy prognostycznej, umożliwiające identyfikację trendów i potencjalnych kierunków rozwoju przestępczości zorganizowanej w perspektywie najbliższej dekady.

Słowa kluczowe: bezpieczeństwo globalne, zagrożenia, siły strukturalne, rozwój społeczny, przestępczość zorganizowana

Abstract

The aim of the chapter is to analyse the current and future determinants of organised crime's development globally and to identify the key factors influencing its evolution amid technological, socio-economic, and geopolitical changes. Particular attention was paid to the roles of new technologies, globalisation, migration, and political instability in shaping the development of international criminal networks. The main research problem was formulated as follows: How do technological, economic, and socio-political changes affect the development and transformation of modern organised crime on a global scale? This problem also includes issues related to the use of cyberspace, financial systems and the weaknesses of state institutions by organised crime groups. The study mainly uses qualitative methods. An analysis of the literature on the subject and of documents and reports from international institutions, such as Europol, the World Economic Forum, and the Hague Centre for Strategic Studies, was used. The methods of comparative analysis and prognostic analysis were also used, enabling the identification of trends and potential directions of development in organised crime over the next decade.

Keywords: global security, threats, structural forces, social development, organised crime

Wstęp

Współczesne środowisko bezpieczeństwa międzynarodowego ulega dynamicznym przemianom, które są konsekwencją złożonych procesów politycznych, społecznych, gospodarczych oraz technologicznych. Globalizacja, rozwój technologii informacyjnych, zmiany klimatyczne, migracje ludności oraz transformacje demograficzne powodują powstawanie nowych zagrożeń i wyzwań dla systemów bezpieczeństwa państw oraz społeczności

międzynarodowej. W rezultacie tradycyjne postrzeganie bezpieczeństwa, koncentrujące się głównie na wymiarze militarnym, zostało rozszerzone o liczne czynniki o charakterze pozamilitarnym, które coraz częściej decydują o stabilności systemu globalnego. W literaturze przedmiotu wskazuje się, że współczesne zagrożenia dla bezpieczeństwa globalnego są w dużym stopniu determinowane przez tzw. siły strukturalne, obejmujące przede wszystkim uwarunkowania geostrategiczne, technologiczne, klimatyczne oraz demograficzne. Czynniki te oddziałują na siebie wzajemnie, tworząc skomplikowaną sieć zależności, która wpływa zarówno na rozwój gospodarczy, funkcjonowanie państw, jak i bezpieczeństwo społeczeństw. Szczególnie istotną rolę odgrywa przy tym rozwój nowych technologii, w tym sztucznej inteligencji, który z jednej strony stwarza nowe możliwości rozwoju cywilizacyjnego, z drugiej natomiast generuje nowe rodzaje zagrożeń, w tym w cyberprzestrzeni czy w obszarze informacyjnym.

Istotnym elementem współczesnego środowiska bezpieczeństwa jest również nasilająca się polaryzacja społeczna, wzrost napięć wewnątrzpaństwowych oraz rozwój zorganizowanych form przestępczości. Globalne sieci przestępcze coraz częściej wykorzystują procesy globalizacji, rozwój technologii cyfrowych oraz nierówności społeczno-ekonomiczne do rozszerzania swojej działalności. W konsekwencji zagrożenia o charakterze transnarodowym stają się jednym z kluczowych wyzwań dla państw oraz instytucji odpowiedzialnych za bezpieczeństwo międzynarodowe. Złożoność i wielowymiarowość współczesnych zagrożeń powodują konieczność prowadzenia pogłębionych analiz prognostycznych, pozwalających identyfikować potencjalne kierunki rozwoju środowiska bezpieczeństwa w perspektywie długoterminowej. Szczególnego znaczenia nabierają w tym kontekście analizy obejmujące zarówno krótkoterminowe, jak i długoterminowe trendy rozwojowe, które mogą wpływać na stabilność systemu międzynarodowego.

Celem niniejszego opracowania jest przedstawienie i analiza strukturalnych uwarunkowań zagrożeń dla bezpieczeństwa globalnego w perspektywie do roku 2034. W rozdziale podjęto próbę identyfikacji kluczowych czynników kształtujących współczesne środowisko bezpieczeństwa oraz określenia ich potencjalnego wpływu na rozwój zagrożeń o charakterze globalnym w nadchodzącej dekadzie.

Rozwój społeczny

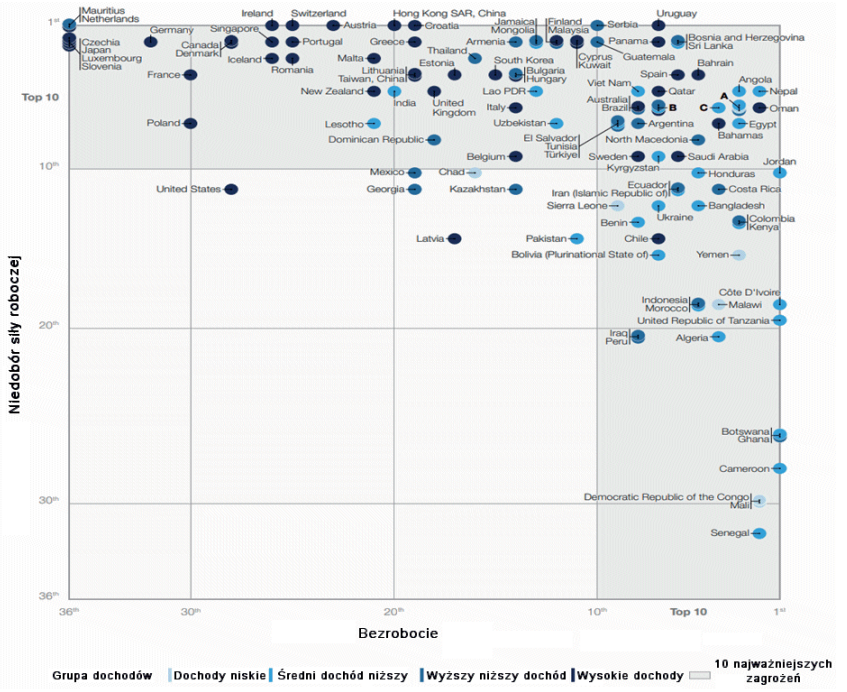
Ostatnie dekady to ogromny postęp cywilizacyjny ludzkości, zarówno w technice, gospodarce, nauce, jak i w medycynie. Jednak takie osiągnięcia ludzkości muszą się liczyć z tym, że nawet najlepiej funkcjonujące systemy mogą zostać zachwiane, czego przykładem był okres pandemii wirusa COVID-19 (2020-2022). Okres ten był odczuwalny globalnie w wielu aspektach życia, w tym gospodarkach, gdzie świetnie prosperujące gospodarki wielu państw w ciągu kilku miesięcy znacznie spowolniły, a mobilność pracowników została w tamtym czasie ograniczona do niezbędnego minimum. Efektem tamtego okresu jest zauważalna malejąca mobilność gospodarcza – lub zdolność do poprawy statusu ekonomicznego i związanych z nim wyników zarówno w gospodarkach rozwiniętych, jak i rozwijających się, wraz ze zmianami na rynkach pracy i obecną edukacją. Polityka pracy i polityka społeczna stają się przestarzałe w kontekście zmian demograficznych (World Economic Forum, 2024). Nowym elementem na globalnej liście zagrożeń w horyzoncie dwuletnim jest brak możliwości ekonomicznych i prawdopodobnie dotkliwość ta pogorszy się w dłuższej perspektywie. Powodem tego zjawiska, zdaniem respondentów GRPS, będą: bezrobocie jako główny czynnik napędzający, brak możliwości ekonomicznych wynikających ze złożonej mieszanki innych globalnych zagrożeń. Obejmuje to krótkoterminowe ryzyka gospodarcze, takie jak pogorszenie koniunktury gospodarczej i inflacja, oraz pilne ryzyka społeczne, takie jak erozja praw człowieka, przemoc wewnątrzpaństwowa i polaryzacja społeczna (World Economic Forum, 2024).

Należy liczyć się z tym, że bez właściwego zarządzania zachodzącymi transformacjami gospodarczymi w skali regionalnej, a może i globalnej, mobilność gospodarcza zatrzyma się na obecnym poziomie, a następnie może odwrócić się. Wpływ na to w następnej dekadzie będą mieć między innymi: zmiany klimatyczne, postępy w dziedzinie technologii sztucznej inteligencji, zmiany demograficzne i dynamika geopolityczna. Zjawiska te będą się nasilać i oddziaływać na siebie, a skutkiem tego w wielu krajach będzie prawdopodobnie brak korelacji między popytem a podażą pracy. Podobnych problemów należy spodziewać się także między wieloma państwami. W takiej sytuacji spójność społeczna i polityczna w najbliższych dziesięciu latach będzie wątpliwa.

Zmiany klimatyczne i gwałtowny rozwój sztucznej inteligencji będą powodować powstawanie zakłóceń na rynkach pracy gospodarek na całym świecie. Zmiany te będą przyczyną zdecydowanych zmian jakościowych i ilościowych miejsc pracy oraz ich rozkładu, a także ich utraty, co za tym doprowadzi do powstania różnych zagrożeń, głównie dla bezpieczeństwa wewnętrznego państw przyjmujących emigrantów. Te gospodarki, które nie będą mogły tworzyć kolejnych miejsc pracy, przekwalifikowywać czy asymilować emigrantów, będą narażone na spowolnienie gospodarcze i w konsekwencji na opóźnienie rozwoju. Jednak będą także takie gospodarki, w których w związku z mobilnością zawodową i społeczną ich obywateli będą borykać się z deficytem pracowników w istotnych gałęziach przemysłu, co także powoduje spowalnianie przemian gospodarczych i postępu gospodarczego.

Zauważyć trzeba, że wymienione zjawiska (zmiany klimatyczne i technologie sztucznej inteligencji) mogą paradoksalnie w określonych przypadkach pomóc w rozwiązywaniu problemu nierówności ekonomicznych poprzez stworzenie nowych możliwości uzyskania dochodu w wielu sektorach. Transformacja w kierunku zerowej emisji netto doprowadzi do ogólnego wzrostu liczby miejsc pracy w sektorze energetycznym. Według szacunków Międzynarodowej Agencji Energetycznej w sprawie zerowej emisji netto do 2050 r. powstanie około 14 mln nowych miejsc pracy w sektorze dostaw energii, a produkcja paliw kopalnych może stracić 5 mln pracowników, co wyraźnie powoduje zapotrzebowanie na około 9 mln pracowników w tym obszarze. Ponadto branże czystej energii, takie jak motoryzacja i budownictwo, wymagałyby dodatkowych około 16 milionów pracowników. Oznacza to, że do 2030 r. może powstać łącznie ponad 30 mln miejsc pracy w sektorze czystej energii, efektywności energetycznej i technologii niskoemisyjnych. Należą do nich świeżo utworzone miejsca pracy, na przykład dzięki poprawie wydajności. Obejmują one również nowe role dla obecnych pracowników w budownictwie, przy wytwarzaniu produktów redukujących emisje, takich jak pojazdy elektryczne i urządzenia hiperwydajne, oraz w innowacyjnych technologiach, takich jak wodór (Cozzi, Motherway, 2021). Mając na uwadze perspektywy rozwoju infrastruktury odnawialnej, należy oczekiwać, że globalny sektor budowlany do 2030 roku znacznie zwiększy swoją wielkość, a miejsca pracy związane z tym, tj. handel i inżynieria, będą jednymi z tych, które według prognoz odnotują największy wzrost w nadchodzących latach.

Trzeba liczyć się z tym, że wraz z rozwojem technologii odnawialnych znacząco wzrośnie rotacja miejsc pracy, ponieważ przemiany te powodują równoległe wypieranie pracowników, a procesy te nie będą równomiernie rozłożone między gospodarkami ani w ich obrębie. Trzeba być świadomym, że wiele tworzonych miejsc pracy nie będzie znajdować się w tej samej lokalizacji, branży lub przedziale umiejętności co dostępni lub zwolnieni pracownicy, co oznaczać będzie wzrost znaczenia możliwości mobilności potencjalnych pracowników. Rosnące niedopasowanie siły roboczej między krajami jest już widoczne; znalazło się w pierwszej piątce rankingów ryzyka dla 52 krajów w ciągu najbliższych dwóch lat, podczas gdy bezrobocie znajduje się w pierwszej piątce zagrożeń w 30 krajach. Jak pokazano na Rysunku 1, prawie wszystkie badane kraje uwzględniają co najmniej jedno z tych zagrożeń w swoich rankingach Top 10: kraje o niskim i niższym średnim dochodzie mają tendencję do umieszczania bezrobocia wyżej, podczas gdy respondenci o wyższych, średnich i wysokich dochodach są bardziej zaniepokojeni niedoborem siły roboczej (World Economic Forum, 2024).



Rysunek 1. Postrzeganie ryzyka w poszczególnych krajach: Zatrudnienie

Źródło**:** World Economic Forum, 2024.

W związku z powyższym jednym z najważniejszych wyzwań społecznych w najbliższej dekadzie będzie tworzenie miejsc pracy w poszczególnych gospodarkach. Proces ten w dużej mierze będzie uzależniony od dostępu do inwestycji w transformację klimatyczną i technologiczną oraz od wyboru ich rozmieszczenia. Problematyka ta jest już szeroko wspierana przez wiele rządów, a fundusze i subsydia są ukierunkowane na krajowy rozwój powiązanych branż. Należy jednak mieć na uwadze różny poziom rozwoju gospodarczego państw i ich zdolności czasowe i aspekty społeczne zmian strukturalnych swoich gospodarek do spodziewanych potrzeb globalnego rynku. Spowodować to może, że inwestycje prawdopodobnie staną się jeszcze bardziej skoncentrowane w stosunkowo stabilnych gospodarkach rozwiniętych. Globalna luka w finansowaniu energii odnawialnej jest również silnie skoncentrowana na rynkach wschodzących ze względu na wyższe ryzyko, a co za tym idzie, mniejszą skłonność do inwestowania potencjalnych inwestorów. W związku z tym, że Stany Zjednoczone, Europa i Chiny nie są narażone na taki sam stopień ryzyka niedoinwestowania i stosowania na tych rynkach różnego rodzaju zachęt finansowych, kapitał inwestycyjny jest bardziej dostępny, a luka w finansowaniu jest mniejsza, szczególnie w krajach Europy Zachodniej (D'Olier-Lees, 2023).

Natomiast rynki postrzegane jako niestabilne lub mniej stabilne, o niższych dochodach, podatne na konflikty wewnętrzne i zewnętrzne są postrzegane przez potencjalnych inwestorów, szczególnie prywatnych, jako zbyt ryzykowne dla inwestycji lub działalności gospodarczej, w tym dla transformacji klimatycznej. Sytuacja taka dodatkowo może w najbliższej dekadzie pogłębić najsłabsze gospodarki, które w większości borykają się z wieloma problemami związanymi między innymi: zadłużeniem, niestabilnością polityczną czy problemami społecznymi. Problematyka transformacji klimatycznej i nowoczesnych technologii może być przyczyną wytworzenia w najbliższych latach zagrożeń w obszarze podaży pracy i popytu na nią. Jesteśmy już świadkami sytuacji, w której to nadwyżka demograficzna niektórych rynków rozwijających się przeradza się w dylemat demograficzny, który poprzez migracje ludności generuje problemy struktur społecznych w państwach wysoko rozwiniętych. Skutkiem tego zjawiska jest zagrożenie dla bezpieczeństwa wewnętrznego tych państw. Dodatkowo państwa, które nie poczynią istotnych inwestycji związanych z transformacją klimatyczną

czy nowymi technologiami, nie będą czerpać dochodów związanych z tymi obszarami i tym samym będą zagrożone podobnymi problemami jak te wysoko rozwinięte, ale o większej skali. Zdaniem wielu ekspertów, większość rozwiniętych gospodarek tworzących miejsca pracy w sektorze transformacji klimatycznej może pogorszyć i tak trudną sytuację na rynkach pracy (Ragsdale, Hall, 2023).

Pojawienie się nowych miejsc pracy spowoduje odpłynięcie wykwalifikowanych pracowników przede wszystkim z branży budowlanej, głównie mieszkaniowej (LaRocco, Goldberg, 2023). Problem ten dotyczy w zasadzie wszystkich wysoko rozwiniętych gospodarek, np. Europy, Stanów Zjednoczonych, Australii czy Chin. Zjawisko to może zachęcić do zastępowania dotychczasowych miejsc pracy wymagających niższych kwalifikacji oraz zachęcić do migracji i zwiększonej mobilności siły roboczej. W związku z kurczącą się i starzejącą się siłą roboczą, firmy w gospodarkach rozwiniętych będą starały się wykorzystać możliwości w zakresie produktywności oferowane przez sztuczną inteligencję, wdrażając je szybko i na dużą skalę. Należy przewidywać, że już w najbliższej dekadzie to generatywna sztuczna inteligencja będzie w coraz większym stopniu zastępować pracowników o średnich kwalifikacjach (inteligencja biologiczna i maszynowa), zwłaszcza w sektorze usług. Sytuacja taka, umożliwiając sprawne wdrożenie technologii sztucznej inteligencji, może w stosunkowo krótkim czasie wyprzeć kompetencje ludzkie, prowadząc do przejścia od niedoboru pracowników do niepełnego zatrudnienia i bezrobocia w niektórych częściach tych gospodarek oraz wywołując podobny efekt w gospodarkach rozwijających się.

Eksperci World Economic Forum przewidują, że w miarę zbliżania się do 2030 r. widoczna będzie erozja krytycznych filarów Celów Zrównoważonego Rozwoju (SDGs) i może nadać ton następnej dekadzie, ponieważ międzynarodowe wsparcie dla ścieżek zrównoważonego rozwoju zawęża się. W związku z licznymi problemami wewnętrznymi wielu gospodarek i słabnącą współpracą międzynarodową istnieje ryzyko pojawienia się wzrostu zjawiska ubóstwa, a tym samym motywacje na użytek wewnętrznych spraw państw oraz ich bezpieczeństwa narodowego mogą być powodem kierowania pomocy na potrzeby doraźne społeczeństw, a nie perspektywiczne, np. środki pomocowe przeznaczone na transformację klimatyczną mogłyby zostać przekierowane na budowę infrastruktury podwójnego zastosowania.

Sytuacja w wielu przypadkach będzie mieć przyzwolenie społeczne i przyznać trzeba, że byłaby wiarygodnie uzasadniona, szczególnie w gospodarkach dotkniętych bezrobociem czy szerszymi kryzysami gospodarczymi lub zagrożonych atakiem zbrojnym i utratą suwerenności.

Ważnym aspektem w najbliższej dekadzie będzie niebezpieczeństwo zachwiania indywidualnych dróg do dobrobytu gospodarczego z uwagi na przedstawione wcześniej dwojakie przemiany gospodarcze, co utrwala podziały technologiczne, edukacyjne i społeczne. Bierność rządzących lub ich partykularne cele polityczno-gospodarcze mogą doprowadzić do zniechęcenia pracowników do przekwalifikowania się, równoległego do mobilności zawodowej i społecznej. Trzeba się liczyć z faktem braku dostępu do możliwości uzyskania dochodu przez coraz szersze grupy pracowników, zarówno fizycznych, jak i umysłowych. Jak twierdzą eksperci z World Economic Forum, zjawisko to, niestety, jest nieuchronne i może zaskoczyć pracowników.

Najnowsze badania wskazują, że przed 2027 r. trzech na pięciu pracowników będzie wymagało szkolenia. Problemem będzie mobilność pracowników związana z ich klasą społeczno-ekonomiczną i wiekiem. Pomimo możliwości wykorzystania sztucznej inteligencji w procesie szkolenia pracowników, nie wszyscy będą mieć możliwość przekwalifikowania się w obrębie danego kraju czy między krajami (World Economic Forum, 2023).

Będzie to spowodowane brakiem przez niektórych pracowników odpowiednich środków finansowych, niezbędnych do przekwalifikowania się na potrzeby innych gałęzi przemysłu. Pracownicy ci będą zmuszeni do pozostania lub znalezienia mniej ambitnych, ale bardziej stabilnych i bezpiecznych źródeł zatrudnienia. Dodatkowo, powszechnie postępująca automatyzacja funkcji na wielu już podstawowych poziomach zatrudnienia może stworzyć pewną barierę edukacyjną dla wejścia na rynek pracy, potęgując jednocześnie wyzwania związane z mobilnością społeczną. W dłuższej perspektywie miejsca pracy dla wyżej wykwalifikowanych, droższych pracowników mogą być również zagrożone zarówno ze względu na inteligencję maszyn, jak i moc maszyn, przy czym bariery wynikają z przestarzałości i naturalnej utraty przez nich umiejętności, a także z postępu technologicznego.

Właściwi decydenci/rządzący muszą mieć świadomość, że konieczne może być wdrożenie przygotowanych odpowiednich działań ochronnych w obszarze socjalnym dla tych pracowników, którzy będą mieć trudności

z ponownym wejściem na rynek pracy. Sytuacja taka może spowodować pojawienie się zjawiska ubóstwa czy bezdomności, a w krajach szczególnie ubogich także zjawiska głodu. Należy liczyć się z tym, że w wielu państwach może pojawić się problem z dostępem do artykułów pierwszej potrzeby, w tym do opieki zdrowotnej i zakwaterowania, dla pewnych grup społecznych. Sytuacja taka będzie sprzyjać rozwojowi przestępczości, w tym tej zorganizowanej. Rządzący chętnie będą mogli wykorzystać takie sytuacje do wzmocnienia sił zbrojnych czy sił porządkowych w celu utrzymania bezpieczeństwa wewnętrznego. Mogą także wystąpić zjawiska radykalizujące nastroje społeczne, jak nacjonalizm czy rasizm. Nie można również wykluczyć przymusowych przesiedleń, ekonomicznie zasadnych migracji w poszukiwaniu lepszych warunków ekonomicznych i, być może, pomocy społecznej.

Wymienione skutki mogą być wyczuwalne zarówno w gospodarkach rozwijających się, jak i w gospodarkach wysoko rozwiniętych. Prawdopodobne zakłócenia w zatrudnieniu mogą również sprawić, że wiedza, technologia, dochody i bogactwo staną się jeszcze bardziej skoncentrowane, utrwalając cykle ubóstwa.

Sytuacje wynikające z warunków ekonomicznych będą rodziły frustracje prowadzące do podziałów społecznych, a sprzeciw wobec technologii i zrównoważonego rozwoju będzie napędzany przez pracowników zagrożonych tymi dwoma transformacjami. Trzeba mieć świadomość możliwości wybuchu protestów społecznych, w tym strajków i zamieszek, które będą paraliżować usługi publiczne, transport i infrastrukturę, w tym krytyczną.

Badania przedstawione w Global Risks Report wykazały, że konkurujące ze sobą wymagania inwestycyjne oznaczają, że niewiele krajów prawdopodobnie będzie miało fiskalną przestrzeń do inwestowania w kapitał ludzki w dłuższej perspektywie – w edukację i systemy opieki zdrowotnej, które mają fundamentalne znaczenie dla realizacji możliwości gospodarczych. Będzie to najbardziej odczuwalne na najbardziej wrażliwych rynkach, które, jak już wcześniej wspomniano, mogą stanąć w obliczu potencjalnego kryzysu inwestycyjnego o destrukcyjnych skutkach długoterminowych. Ponieważ przestrzeń fiskalna jest ograniczona, a finansowanie prywatne pozostaje ograniczone, rynki te będą w coraz większym stopniu zmuszone do wyboru pomiędzy, na przykład, spłatą zadłużenia zagranicznego, zapewnieniem

silnej i natychmiastowej siatki bezpieczeństwa dla osób znajdujących się w trudnej sytuacji, inwestowaniem w przyszłe dywidendy wzrostowe oferowane przez działania w dziedzinie klimatu i rozwój technologiczny, zarządzaniem zmianą klimatu i przystosowaniem się do niej lub wspieraniem długoterminowych zdolności adaptacyjnych kapitału ludzkiego poprzez systemy opieki zdrowotnej i edukacji.

Wynikiem takiej sytuacji będą oczekiwania społeczeństw w stosunku do rządowych działań interwencjonistycznych, które będą mogły doprowadzić do rozluźnienia polityki fiskalnej, a tym samym do zapewnienia bezpieczeństwa socjalnego obywateli, w tym na przykład stabilności zatrudnienia. Możliwe okazać się może wzrost podatków nakładanych na sektor technologiczny (automatyzacji lub sztucznej inteligencji) i redystrybucja uzyskanych z tego tytułu zysków na potrzeby socjalne. Przykładem mogą być działania interwencyjne wielu rządów podczas pandemii (programy masowych szczepień) i niedawnego kryzysu energetycznego w Europie (pakiety wsparcia finansowego dla gospodarstw domowych i przedsiębiorstw) (Agyemang, Giles, 2023).

Trzeba zauważyć, że rządzący, których działania będą uważane za niewystarczające, będą tracić na popularności, a zyskiwać będą ruchy, które będą zbijać kapitał polityczny na rozczarowaniu klas niższych i średnich, które nie będą widzieć szans w przyszłości własnej i swoich rodzin. Sytuacje takie będą rodzić niepokoje społeczne, radykalizm polityczny i społeczny czy emigrację zarobkową.

Reasumując, transformacja ekologiczna i sztuczna inteligencja dają i będą dawać znaczne możliwości rozwoju społeczeństw, ale muszą one być wprowadzane z rozwagą i z uwzględnieniem poziomu rozwoju poszczególnych społeczeństw, ich potrzeb, możliwości ekonomicznych. W przypadku właściwego zarządzania i współpracy międzynarodowej, realizowana może być w najbliższej dekadzie skuteczna mobilność zawodowa i społeczna, która skutecznie będzie chroniła przed zagrożeniami i zapewniała ponadnarodowy rozwój gospodarczy i społeczny. Przykładem mogą być działania wielu korporacji bazujących na pracy w formie zdalnej połączonej z wymianą umiejętności a także z transferem technologii. Ważnym aspektem powinno być wsparcie wielostronnych i międzynarodowych mechanizmów finansowych, które mogłyby również zmniejszyć rzeczywiste i postrzegane ryzyko

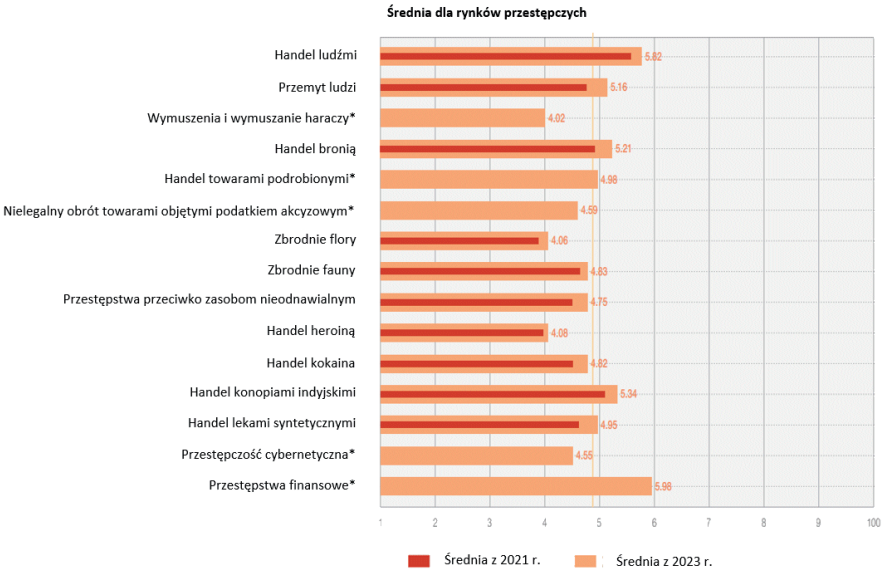
w krajach najbardziej podatnych na zagrożenia, aby odblokować przepływy finansowania.

Perspektywiczne zmiany w systemach zatrudnienia mogą być trudne do akceptacji przez społeczeństwa, ale mając na uwadze, że zmiany klimatyczne, jak i technologie sztucznej inteligencji będą wpływać na rynki pracy, rozwiązania mające na celu poprawę mobilności gospodarczej muszą być dostosowane do konkretnych zagrożeń, takich jak niedobory siły roboczej na poziomie przemysłu i kraju. W wyniku takich działań, na przykład, pracownicy zwolnieni z branż wysokoemisyjnych mogą zasilić sektor ekologiczny, ale warunkiem w wielu przypadkach będzie ich gotowość do przekwalifikowania się oraz mobilność. Wymierną pomoc społeczeństwom dotkniętym w szczególny sposób przez transformację klimatyczną i technologie sztucznej inteligencji może udzielić rozwój takich sektorów jak na przykład: zdrowie, opieka, edukacja, turystyka, hotelarstwo, rolnictwo, usługi osobiste i kultura. Niemniej, w najbliższej dekadzie płynne przejście transformacji klimatycznej i implementacja technologii sztucznej inteligencji, wymagać będzie nieuniknionej współpracy podmiotów publicznych i prywatnych.

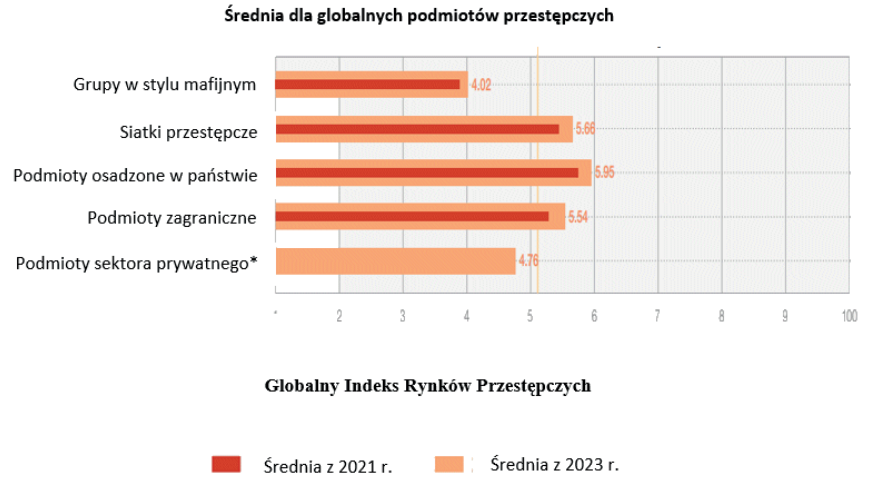
Przestępczość zorganizowana

Powszechna globalizacja życia społeczeństw nie ominęła również przestępczości zorganizowanej, która niestety rozwija się zarówno pod względem celów, jak i operacji, stając się tym samym ogromnym problemem dla wszystkich krajów. Analiza danych wskazuje, że nastąpił wzrost przestępczości na wszystkich rynkach (Rysunek 2) a przestępczość zorganizowana nadal jest główną sprawcą ofiar śmiertelnych. Dane Instytutu Ekonomii i Pokoju zawarte w opracowaniu *Global Peace Index 2023* oraz Biura Narodów Zjednoczonych ds. UNODC w materiale Global Study on Homicide pokazuje, że w wyniku działalności zorganizowanych grup przestępczych w latach 2000-2019 rocznie traciło życie około 65 000 osób.

A. Światowe rynki przestępcze



B. Podmioty przestępcze na całym świecie



Rysunek 2. Globalne rynki przestępcze

Źródło: World Economic Forum, 2024.

Średnie globalne z 2021 r. w porównaniu z 2023 r. W 2023 r. do Globalnego Indeksu Przestępczości Zorganizowanej dodano szereg nowych wskaźników, oznaczonych gwiazdką. Przestępstwa finansowe odnoszą się do przestępczości zorganizowanej, która powoduje straty finansowe dla państwa, podmiotu i/lub osób prywatnych poprzez szereg działań. Biorąc jednak pod uwagę pokrywanie się z innymi kategoriami, w przypadku gdy takie działania można przypisać innemu rynkowi przestępczemu w ramach indeksu, przestępstwa finansowe podlegają odpowiedniemu wskaźnikowi rynkowemu (na przykład oszustwa związane z zamówieniami publicznymi dotyczącymi zamówień rolnych należą do przestępstw związanych z florą).

Nielegalna działalność gospodarcza jest ryzykiem, które nie jest uwzględniane w pierwszej dziesiątce globalnych ryzyk dotkliwości w perspektywie krótkoterminowej i długoterminowej w horyzoncie dwuletnim, jak i 10-letnim. Jednak zagrożenia wynikające z nielegalnej działalności gospodarczej należy traktować niezwykle poważnie zarówno w perspektywie krótkoterminowej, jak i długoterminowej. Spowodowane są one między innymi przez pogorszenie koniunktury gospodarczej, brak możliwości gospodarczych, brak bezpieczeństwa cybernetycznego i mimowolną migrację, a także bezrobocie, przemoc wewnątrzpaństwową i konfrontację geoekonomiczną (World Economic Forum, 2024).

To syndykaty przestępcze i powiązane z nimi nielegalne rynki będą napędzać w najbliższych latach rozwój przestępczości zorganizowanej. Z kolei zjawisko ekspansji nielegalnych rynków wynikać będzie z sytuacji społeczno-gospodarczych w poszczególnych krajach czy regionach świata, ale także z ich charakterystyk środowiskowych. Dodatkowo, w celu prowadzenia tych procederów będą wykorzystywane nowe technologie związane z cyberprzestrzenią i jej bezpieczeństwem. W najbliższych 10 latach należy liczyć się z tym, że mogą upaść niektóre legalne rządy, powodując tym samym sytuacje, w których to zorganizowane grupy przestępcze będą starały się wykorzystać słabość podmiotów państwowych w celu realizacji swoich celów na styku z podmiotami państwowymi.

W nadchodzącej dekadzie tzw. „czarne rynki" prawdopodobnie będą się dalej rozprzestrzeniać, tworząc kolejne źródła dla swojej działalności, której kosztami tak naprawdę będą ponosić (będą obłożone) poszczególne społeczeństwa.

Raport Haskiego Centrum Studiów Strategicznych wprowadza nowe, proste ramy opisu głównych sił kształtujących współczesną przestępczość zorganizowaną. Ramy te obejmują różne czynniki, które mieszczą się w pięciu kategoriach analizy i wzajemne powiązania między tymi kategoriami:

- towary i usługi, które leżą u podstaw globalnej działalności przestępczej,
- osoby zaangażowane w działalność przestępczą lub utrzymujące się z niej,
- pieniądz, systemy finansowe i infiltracja gospodarcza, które leżą u podstaw nielegalnego handle,
- technologia, która w coraz większym stopniu przenika wszelkie formy przestępczości zorganizowanej,
- zakres, w jakim wszystkie te zmienne pozwalają podmiotom przestępczym na projekcję siły (politycznej) i sprawowanie faktycznej kontroli nad (nowym) terytorium (Bastrup-Birk i in., 2023).

Ponadto, umożliwiając analizę konkretnych zmian w ramach każdej z tych kategorii, ramy te mogą stanowić wytyczne w zakresie monitorowania nowych wydarzeń, a także informować o interwencjach politycznych.

Zdaniem autorów wymienionego raportu, współczesna przestępczość zorganizowana w globalnie powiązanym świecie charakteryzuje się bardziej płynnymi, zdecentralizowanymi, zaawansowanymi technologicznie i odpornymi sieciami handlowymi. Cechą charakterystyczną przestępczości zorganizowanej jest to, że sieci te wykorzystują w ramach swojej działalności szeroką gamę profesjonalnych usługodawców i systemowych podmiotów wspomagających. W globalnej gospodarce przestępczej różne podmioty wchodzą w relacje i dokonują transakcji, zgodnie ze swoimi potrzebami biznesowymi, wykorzystując wyspecjalizowane organizacje ponadnarodowe, na przykład w zakresie księgowości, logistyki czy bezpieczeństwa (cybernetycznego).

W najbliższej dekadzie międzynarodowa przestępczość zorganizowana będzie w coraz większym stopniu oparta na szarej (lub równoległej) globalnej nielegalnej gospodarce, a także na niejawnych instrumentach transferowych i inwestycyjnych. Aspekty te będą się coraz częściej krzyżować z formalnie regulowanym systemem finansowym. Trzeba liczyć się z tym, że

przestępcze struktury finansowe będą tworzone na bazie skomplikowanych struktur finansowych i korporacyjnych. Pod pozorem legalnej działalności, celem takiego działania będzie chęć ukrycia prawdziwych środków finansowych lub innych dóbr. Charakterystyczne jest i w najbliższej przyszłości będzie, że grupy przestępcze (siatki przestępcze) na całym świecie łączą podobne metody prania brudnych pieniędzy. Prawdopodobnie rozwijane będą takie metody jak zakładanie małych, lokalnych przedsiębiorstw opartych na gotówce, nabywanie nieruchomości na dużą skalę i inwestowanie w sektorach od budownictwa, wydobycia i transportu po gospodarkę odpadami i energię odnawialną. Coraz częstszym zjawiskiem będzie przenikanie grup zorganizowanej przestępczości w struktury podmiotów władzy.

Zwrócić należy uwagę, że zagrożenia społeczno-gospodarcze zwiększą narażenie na działalność organizacji przestępczych. Migracja związana z konfliktami lub klimatem będzie prawdopodobnie napędzać wyzysk ze strony podmiotów przestępczych zajmujących się na przykład pracą dzieci i cyberniewolnictwem. Dodatkowo, dezintegracja społeczna, segregacja miejska, ubóstwo i nierówności ekonomiczne, potencjalne czynniki napędzające działalność przestępczą, mogą skłonić więcej osób do działalności przestępczej. Według badań GRPS, najsilniejszym czynnikiem napędzającym nielegalną działalność gospodarczą jest bezrobocie. Jeżeli w następnej dekadzie ubóstwo i bezrobocie staną się chronicznym problemem w krajach narażonych na kryzysy związane z utrzymaniem, przestępczość może stać się głównym źródłem dochodu i jedynym sposobem dostępu do artykułów pierwszej potrzeby dla niektórych społeczności.

W związku z tym, że przestępczość zorganizowana jest zakorzeniona w społeczeństwie i gospodarce, rekrutacja do organizacji przestępczych, w coraz większym stopniu odbywa się w kontekście szybkich zmian klimatycznych, demograficznych, technologicznych i systemowych. Do rozprzestrzeniania się społecznych źródeł i „punktów zapalnych" przestępczości zorganizowanej przyczyniają się i przyczyniać się będą migracja i urbanizacja, które często znajdują się w enklawach ubóstwa i marginalizacji i/lub tam, gdzie formalne zarządzanie i administrowanie są ograniczone i tym samym nieskuteczne. Ponadto zorganizowane grupy przestępcze rutynowo wykorzystują wstrząsy, ogniska niestabilności, a także politycznie, gospodarczo i społecznie zmarginalizowane grupy wyborców oraz możliwości

strukturalne (w tym geostrategiczne zmiany w systemie międzynarodowym) do ustanawiania przyczółków na nowych rynkach, rekrutacji nowych członków lub rozszerzania swojej działalności. Ich dostęp i wpływy nie pozostały niezauważone przez podmioty państwowe, które coraz częściej zwracają się do podmiotów przestępczych jako niezaprzeczalnych dźwigni zastępczych wpływów w wielobiegunowym świecie. Prowadzić to będzie do jeszcze szerszego powstania mikroekonomicznych i politycznych obszarów nielegalnej działalności. W celu realizacji swoich interesów siatki przestępcze, wspierane i napędzane przez niepohamowany popyt na nielegalne towary i usługi, będą się również coraz bardziej sprawne w wykorzystywaniu zarówno nowych technologii, jak i wstrząsów strukturalnych w systemie międzynarodowym, począwszy od różnego rodzaju pandemii i zmiany klimatu, a skończywszy na konfliktach i niestabilności zarówno krajowych, jak i regionalnych i globalnych.

Należy liczyć się także ze wzrostem zagrożenia w wyniku szybkiej integracji zaawansowanych technologii, a tym samym z narażeniem znacznej części światowej populacji na potencjalne wykorzystanie cyfrowe i fizyczne. Spodziewać się należy, że siatki przestępczości zorganizowanej będą w coraz większym stopniu przyjmować mieszane modele biznesowe wykorzystujące nowe technologie w celu dywersyfikacji nielegalnego finansowania i fragmentacji fizycznej obecności przestępczości zorganizowanej. Zjawisko to będzie stwarzać poważne niebezpieczeństwo dla osób fizycznych i legalnych przedsiębiorstw – i może potencjalnie prowadzić do przemocy, która podważy władzę rządów i zagrozi kontroli terytorialnej państw.

Przestępczość zorganizowana będzie wykorzystywać znacznie większy stopień zaawansowanych technologii, w tym cyberprzestępczość, która będzie dla niej coraz tańszym źródłem dochodów. Takie zagrożenia będą stawać się coraz bardziej niebezpieczne nawet dla liderów biznesu krajów i regionów rozwijających się. Trzeba mieć świadomość, że nowoczesne technologie będą doskonałym narzędziem dla zorganizowanych grup przestępczych w celu rozwijania swojej działalności w zakresie geograficznym. Dzięki technologii sieci przestępcze mogą rozprzestrzeniać nielegalną działalność, wykorzystując luki regulacyjne i egzekucyjne w zakresie prawa podmiotów państwowych. W niektórych sytuacjach ekspansja geograficzna zorganizowanych grup przestępczych będzie mogła również prowadzić

do przemocy politycznej, która podważy władzę rządów. W ciągu następnej dekady zwiększająca się niestabilność rządów niektórych państw i nieskuteczność rozwiązywania problemów społeczeństw mogą spowodować, że alternatywnymi rozwiązaniami problemów społeczno-gospodarczych staną się działania zorganizowanych siatek grup przestępczych. W sytuacjach ekstremalnych niektóre państwa mogą pośrednio wspierać przestępczość zorganizowaną lub stać się na nią podatne.

Korupcja może być dla wielu państw problemem, który przez całe lata będzie niszczycielski dla porządku prawnego i rozwoju społeczno-gospodarczego. Na przykład korupcja mogłaby skutecznie doprowadzić do kontroli węzłów transportowych, organów ścigania i części sektora publicznego przez zorganizowane grupy przestępcze (Europol, 2023a). To z kolei podważyłoby praworządność, zakłóciłoby konkurencję i jeszcze bardziej osłabiłoby wzrost gospodarczy, podważając zarówno zaufanie społeczne, jak i zdolności w zakresie egzekwowania prawa.

Zorganizowana przestępczość, prawdopodobnie będzie się dalej rozwijać w kontekście zwiększonej wielobiegunowości międzynarodowej i konkurencji geostrategicznej. Sytuacja międzynarodowa wymagająca poszukiwania rozwiązań na wysokich szczeblach międzypaństwowych może spowodować zmniejszenie zainteresowania problemami społeczeństw. Ewentualny powrót do rywalizacji wielkich mocarstw i renegocjacja stref wpływów będą najbardziej dotkliwie odczuwalne w krajach i regionach, które są niestabilne i dotknięte konfliktami. W takich przypadkach podmioty przestępcze będą również dążyć do zapewnienia sobie strategicznych korzyści albo z własnej woli, albo jako pełnomocnicy patronów państwowych.

Opierając się na tych ustaleniach, eksperci Haskiego Centrum Studiów Strategicznych podkreślają, że ogólna ewolucja w kierunku tego, co sprowadza się do (co najmniej) czwartego pokolenia przestępczości. Ewolucja ta sprawiła, że pierwsze pokolenie historycznych (około XIX wieku) grup przestępczych zdolnych do tworzenia lokalnych nielegalnych rynków utorowało drogę drugiemu pokoleniu, które w dużej mierze wyrosło z epoki prohibicji i powojennych czarnych rynków. Począwszy od lat siedemdziesiątych XX wieku, w kontekście nowoczesnego transportu i handlu międzynarodowego pojawiła się przestępczość zorganizowana trzeciej generacji, obejmująca transnarodową przestępczość, a także „super'' kartele (głównie

wyspecjalizowane w handlu narkotykami), z których najbardziej znane są w Ameryce Łacińskiej. Czwarte, a właściwie „następne" pokolenie przestępczości zorganizowanej charakteryzuje się zdecentralizowanymi, rozproszonymi, komórkowymi i skutecznymi sieciami, które są coraz bardziej osadzone w tkance społecznej. To pokolenie przestępczości zorganizowanej również łączy i zmniejsza dystans między różnymi dziedzinami, funkcjami, rolami i usługami na całym świecie. W tym przypadku możliwości strukturalne, próżnia polityczna i społeczna, luki prawne i regulacyjne, globalne rozwiązania finansowe, przestępcze łańcuchy dostaw i rynki detaliczne są niezmiennie połączone w złożony, zintegrowany, spiralny i samoregulujący się (szary) system gospodarczy. W ujęciu realnym doprowadziło to prawdopodobnie do ogólnego wzrostu względnej siły (politycznej), siły ekonomicznej i odpowiednio ogólnego zagrożenia ze strony przestępczości zorganizowanej, co w najbardziej znaczący sposób przejawia się w zasypywaniu i zniekształcaniu legalnych gospodarek oraz erozji formalnych systemów zarządzania i „międzynarodowego systemu opartego na zasadach" – który już teraz znajduje się w szybkim odwrocie na szczeblu państwowym.

Zdaniem ekspertów Europol-u, aby skutecznie zapobiegać rozprzestrzenianiu się nielegalnej działalności zarówno na rynkach geograficznych, jak i gospodarczych, powinno się zająć trzema kluczowymi obszarami:

- zdolnością do prania nielegalnych zysków,
- komunikacja, która umożliwia tworzenie rozległych siatek przestępczych,
- korupcją.

Podczas gdy ryzyko związane z przeciwdziałaniem inwigilacji musi być traktowane ostrożnie, demontaż szyfrowanej komunikacji może być radykalnym narzędziem do rozbijania międzynarodowych sieci przestępczych. Na przykład likwidacja narzędzia do szyfrowanej komunikacji EncroChat, powszechnie wykorzystywanego przez zorganizowane grupy przestępcze, doprowadziła do tej pory do 6 558 aresztowań na całym świecie (197 z aresztowanych to cele o wysokiej wartości) i skonfiskowania lub zamrożenia blisko 900 milionów euro w funduszach przestępczych (Europol, 2023b). Problemy wszystkich trzech obszarów można rozwiązać na wielu poziomach zarządzania, jednak to, jak to wykazują badania, przepisy

krajowe i lokalne, ma największy potencjał w zakresie stymulowania działań w zakresie ograniczania ryzyka i gotowości w odniesieniu do nielegalnej działalności gospodarczej.

Podsumowanie

Jednym z największych zagrożeń w dwuletnim i dziesięcioletnim horyzoncie czasowym, jest polaryzacja społeczna. Polaryzacja społeczna i pogorszenie koniunktury gospodarczej są postrzegane jako najbardziej powiązane ze sobą – a zatem najbardziej wpływowe – ryzyka w globalnej sieci ryzyka, jako czynniki napędzające i możliwe konsekwencje wielu rodzajów ryzyk. Należy przypuszczać, że w ciągu najbliższych lat wiele podmiotów rządowych na świecie będzie wykorzystywać dezinformację do dalszego pogłębiania podziałów społecznych i politycznych w państwach dla nich konkurencyjnych. Z tego tytułu należy się liczyć z pojawianiem się niepokojów społecznych i zamieszek. Zjawiska te mogą przybierać różne formy, od gwałtownych protestów i przestępstw z nienawiści po konfrontację obywatelską i terroryzm.

Należy przewidywać, że w wielu państwach wraz z podważaniem prawdy wzrośnie również ryzyko krajowej propagandy i cenzury. Prawdopodobne jest, że w odpowiedzi na dezinformację rządy niektórych krajów będą w coraz większym stopniu kontrolować przekaz informacji w oparciu o to, co uznają za „prawdziwe" oraz interpretować prawo wg „własnego uznania". Swobody związane z internetem, prasą i dostępem do szerszych źródeł informacji, które już teraz w wielu krajach zanikają, mogą przerodzić się w szersze represje wobec przepływu informacji w szerszym gronie krajów. W prognozach na najbliższą dekadę pojawia się wiele innych zagrożeń. Jednym z najpoważniejszych problemów stają się koszty utrzymania. Kolejnymi problemami będą najprawdopodobniej zjawisko inflacji i pogorszenie się koniunktury gospodarczej. Przypuszczać należy, że sytuacja ekonomiczna małych i średnich przedsiębiorstw oraz mocno zadłużonych krajów stanie się szczególnie trudna, a wiele rynków będzie bardzo wrażliwych na zmieniające się zawirowania kosztów pieniądza, szczególnie tych najbardziej podatnych na zagrożenia. Z dużym prawdopodobieństwem, w wyjątkowo trudnej sytuacji znajdą się kraje wrażliwe na zmianę klimatu lub podatne na konflikty wewnętrzne. Prawdopodobnie następować będzie wyraźna różnica

w obszarze rozwoju infrastruktury, inwestycji, handlu czy cyfryzacji tych krajów, a następstwem tych zjawisk będą niepokoje społeczne czy dalsza degradacja ich środowiska naturalnego.

Niebezpiecznym staje się rozwój sztucznej inteligencji (AI), szczególnie dla krajów, dla których to korzyści komercyjne i aspekty geopolityczne będą nadrzędne nad własnym interesem publicznym. Różnice w rozwoju cyfryzacji między krajami o wysokich i niskich dochodach doprowadzą do wyraźnej dysproporcji w dystrybucji powiązanych korzyści i zagrożeń, np. produkcji gospodarczej, klimatu, finansów, edukacji i ochrony zdrowia czy tworzenia powiązanych miejsc pracy.

W perspektywie 10-letniej w miarę równomierny postęp rozwojowy i poziom życia są niemożliwe. Rozwijające się kierunki rozwoju gospodarczego świata, środowiskowe czy nowe technologie prawdopodobnie umocnią istniejące wyzwania związane z mobilnością zawodową i społeczną, blokując jednostkom dostęp do dochodów i możliwości zdobywania kwalifikacji, a tym samym możliwość poprawy statusu ekonomicznego społeczeństw wielu krajów.

Brak możliwości ekonomicznych jest jednym z 10 największych zagrożeń w okresie dwóch lat, ale wydaje się, że w dłuższej perspektywie jest mniejszym zmartwieniem dla globalnych decydentów. Wysokie wskaźniki odpływu miejsc pracy – zarówno tworzenia, jak i likwidacji miejsc pracy – mogą doprowadzić do głębokiego rozdwojenia rynków pracy między gospodarkami rozwiniętymi i rozwijającymi się oraz w ich obrębie. Chociaż nie należy lekceważyć korzyści w zakresie wydajności wynikających z tych przemian gospodarczych, wzrost eksportu oparty na produkcji lub usługach może już nie oferować tradycyjnych ścieżek do większego dobrobytu dla krajów rozwijających się. Zawężenie indywidualnych ścieżek do stabilnych źródeł utrzymania wpłynęłoby również na wskaźniki rozwoju społecznego – od ubóstwa po dostęp do edukacji i opieki zdrowotnej. Wyraźne zmiany w umowie społecznej wraz ze spadkiem mobilności międzypokoleniowej radykalnie zmieniłyby dynamikę społeczną i polityczną zarówno w gospodarkach rozwiniętych, jak i rozwijających się.

Literatura

1. Agyemang, E., Giles, C. (2023). *Big government is back. How will we pay for it?*, The Financial Times. Pobrane z: https://www.ft.com/content/b7b7a315-46ce-483d-b374-5eff371aa30c?syn-25a6b1a6=1 (dostęp: 12.01.2026).
2. Bastrup-Birk, J., Frinking, E., Arentze, L., de Jong, E., Bekkers, F. (2023). *Next Generation Organised Crime Systemic change and the evolving character of modern transnational organised crime*, The Hague Centre for Strategic Studies. Pobrane z: https://hcss.nl/wp-content/uploads/2023/05/Next-Generation-Organised-Crime-HCSS-2023-V2.pdf (dostęp: 12.01.2026).
3. Cozzi, L., Motherway, B. (2021). *The importance of focusing on jobs and fairness in clean energy transitions*, International Energy Agency. Pobrane z: https://www.iea.org/commentaries/the-importance-of-focusing-on-jobs-and-fairness-in-clean-energy-transitions (dostęp: 12.01.2026).
4. D'Olier-Lees, T. (2023). *Renewable Energy Funding in 2023: A 'Capital Transition' Unleashed*, S&P Global. Pobrane z: https://www.spglobal.com/en/research-insights/featured/special-editorial/renewable-energy-fundingin-2023-a-capital-transition-unleashed (dostęp: 12.01.2026).
5. European Labour Authority. (2023). *Report on labour shortages and surpluses 2022* https://doi.org/10.2883/50704
6. Europol. (2023a). *European Financial and Economic Crime Threat Assessment 2023: The Other Side of the Coin: An Analysis of Financial and Economic Crime*. Pobrane z: https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime (dostęp: 12.01.2026).
7. Europol. (2023b). *Dismantling encrypted-criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized*. Pobrane z: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized (dostęp: 12.01.2026).
8. LaRocco, L. A., Goldberg, N. R. (2023). *The iconic American hard hat job that has the highest level of open positions ever recorded*, CNBC. Pobrane

z: https://www.cnbc.com/2023/07/29/the-hard-hat-job-with-highest-level-of-open-positions-ever-recorded.html (dostęp: 12.01.2026).
9. Ragsdale, J., Hall, A. (2023). *The global impact of labor shortages across the construction-industry*, WTW. Pobrane z: https://www.wtw-co.com/en-ch/insights/2023/09/the-global-impact-of-labor-shortages-across-theconstruction-industry (dostęp: 12.01.2026).
10. United Nations Office on Drugs and Crime. (2023). *Global study on homicide 2023*. United Nations.
11. World Economic Forum. (2024). *The Global Risks Report 2024, 19th edition*. Pobrane z: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (dostęp: 12.01.2026).
12. World Economic Forum. (2023). *Future of Jobs Report 2023*. Pobrane z: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf (dostęp: 12.01.2026).

Iwona Lasek-Surowiec[1]
Państwowa Akademia Nauk Stosowanych w Chełmie
Małgorzata Zdunek[2]
Marek Giec[3]

https://doi.org/10.29316/9788368103373_2

ZAGROŻENIA ASYMETRYCZNE WE WSPÓŁCZESNYM ŚRODOWISKU BEZPIECZEŃSTWA

ASYMMETRIC THREATS IN THE CONTEMPORARY SECURITY ENVIRONMENT

Streszczenie

Celem rozdziału jest przedstawienie istoty oraz charakterystyki zagrożeń asymetrycznych we współczesnym środowisku bezpieczeństwa, a także wskazanie ich głównych form, podmiotów sprawczych oraz sposobów przeciwdziałania. Problem badawczy sformułowano: w jaki sposób zagrożenia asymetryczne wpływają na współczesny system bezpieczeństwa państw oraz jakie czynniki determinują ich rosnące znaczenie w środowisku międzynarodowym? Przyjęto hipotezę, że zagrożenia asymetryczne, ze względu na swoją nieprzewidywalność, elastyczność organizacyjną podmiotów je generujących oraz wykorzystywanie dysproporcji potencjałów,

[1] https://orcid.org/0000-0002-7231-7993, e-mail: isurowiec@panschelm.edu.pl
[2] https://orcid.org/0009-0001-9305-2840, e-mail: malgosia.piechowicz@gmail.com
[3] https://orcid.org/0009-0006-1061-6740, e-mail: marekgiec666@gmail.com

stanowią jedno z kluczowych wyzwań dla bezpieczeństwa państw i wymagają stosowania niestandardowych metod przeciwdziałania. W rozdziale zastosowano metody badawcze właściwe dla nauk o bezpieczeństwie, w szczególności analizę literatury przedmiotu, analizę porównawczą oraz metodę analizy systemowej, pozwalające na identyfikację typów zagrożeń asymetrycznych, ich uwarunkowań oraz konsekwencji dla bezpieczeństwa narodowego i międzynarodowego. Główny wniosek wskazuje, że współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą rolą aktorów niepaństwowych oraz niestandardowych form oddziaływania, które mogą generować skutki nieproporcjonalne do posiadanego potencjału, co wymusza redefinicję dotychczasowych modeli reagowania i rozwój kompleksowych działań asymetrycznych w wymiarze militarnym, policyjnym i politycznym.

Słowa kluczowe: zagrożenia asymetryczne, bezpieczeństwo państwa, terroryzm, przeciwnik asymetryczny, działania asymetryczne

Abstract

The aim of the chapter is to present the essence and characteristics of asymmetric threats in the modern security environment, and to outline their main forms, causative agents, and countermeasures. The research problem is formulated as follows: how do asymmetric threats affect the modern security systems of states, and what factors determine their growing importance in the international environment? It has been hypothesised that asymmetric threats, due to their unpredictability, the organisational flexibility of entities that generate them, and the use of disparities in potential, pose key challenges for state security and require non-standard countermeasures. The chapter uses research methods specific to the security sciences, in particular the analysis of the literature on the subject, comparative analysis, and systemic analysis, allowing for the identification of types of asymmetric threats, their determinants, and their consequences for national and international security. The main conclusion indicates that the modern security environment is characterised by a growing role of non-state actors and non-standard forms of influence, which may generate effects disproportionate to their potential, forcing the redefinition of existing response models and the development of comprehensive asymmetric actions across the military, police and political dimensions.

Keywords: asymmetric threats, state security, terrorism, asymmetric adversary, asymmetric actions

Wstęp

W środowisku bezpieczeństwa narodowego oraz międzynarodowego zagrożenia stanowią jeden z kluczowych czynników determinujących dynamikę procesów polityczno-strategicznych. Ich charakter oraz intensywność oddziałują bezpośrednio na przebieg wydarzeń, wymuszając jednocześnie opracowywanie i implementację nowych koncepcji strategicznych, doktryn operacyjnych oraz rozwiązań taktycznych. Zakończenie zimnej wojny i rozpad dwubiegunowego ładu międzynarodowego zapoczątkowały fundamentalną transformację architektury bezpieczeństwa globalnego. Powstała wówczas konieczność redefinicji dotychczasowych paradygmatów bezpieczeństwa oraz wypracowania adekwatnych mechanizmów reagowania na nowe spektrum zagrożeń (Koziej, 2011). Konsekwencją rozpadu Układu Warszawskiego było stopniowe włączanie państw Europy Środkowo-Wschodniej w struktury Sojuszu Północnoatlantyckiego, co istotnie przeobraziło układ sił w wymiarze regionalnym i globalnym. Nowy porządek bezpieczeństwa kształtowany był nie tylko przez procesy modernizacji potencjałów militarnych, intensyfikację współpracy sojuszniczej oraz rozwój wspólnych ćwiczeń wojskowych, lecz również przez redefinicję katalogu podmiotów oddziałujących na bezpieczeństwo międzynarodowe – w tym rosnącą rolę aktorów pozapaństwowych (Potulski, 2013). Zamach terrorystyczny przeprowadzony 11 września 2001 r. na World Trade Center na terytorium Stanów Zjednoczonych stanowił punkt zwrotny w normatywnym i instytucjonalnym postrzeganiu zagrożeń dla bezpieczeństwa państwa (Liedel, 2010). W jego następstwie dokonano pogłębionej rewizji obowiązujących rozwiązań systemowych, prowadzącej do wypracowania zróżnicowanych strategii prewencyjnych, ukierunkowanych na minimalizację ryzyka wystąpienia aktów terrorystycznych oraz ograniczenie ich potencjalnych skutków prawnych, społecznych i infrastrukturalnych (National Commission on Terrorist Attacks Upon the United States, 2004).

Na podstawie zgromadzonych doświadczeń operacyjnych oraz analiz ryzyka dokonano również redefinicji katalogu obiektów podlegających szczególnej ochronie. Wielkokubaturowe obiekty użyteczności publicznej, charakteryzujące się wysoką koncentracją ludności cywilnej i kwalifikowane jako tzw. miękkie cele, zostały włączone do systemu infrastruktury krytycznej, podlegającej wzmożonym reżimom ochronnym, organizacyjnym i prawnym.

Wskazane wydarzenia przyczyniły się jednocześnie do intensyfikacji dyskursu naukowego i strategicznego wokół kategorii zagrożeń asymetrycznych, które od tego momentu stały się jednym z kluczowych przedmiotów analiz w obszarze bezpieczeństwa narodowego i międzynarodowego (Jasiński, 2013).

W literaturze przedmiotu z zakresu studiów nad bezpieczeństwem przyjmuje się, iż zagrożenie bezpieczeństwa stanowi wielowymiarowy i dynamiczny układ zdarzeń zachodzących zarówno w środowisku wewnętrznym państwa, jak i w jego otoczeniu międzynarodowym. Zdarzenia te, cechujące się wysokim prawdopodobieństwem wystąpienia, mogą prowadzić do ograniczenia bądź utraty warunków niezakłóconego funkcjonowania, stabilności oraz rozwoju państwa (Czywilis, 2007). Źródłem tak rozumianych zagrożeń są, w szczególności, działania o charakterze przymusowym lub destrukcyjnym, realizowane przy wykorzystaniu instrumentów przemocy politycznej, ekonomicznej bądź militarnej. Mogą one przyjmować zarówno formę bezpośrednią, jak i pośrednią, oddziałując na podstawowe struktury państwowości oraz system bezpieczeństwa (Dworecki, 1994). Tak ujęta definicja zagrożenia dla bezpieczeństwa stanowi podstawę do jego dalszej systematyzacji oraz klasyfikacji według przyjętych kryteriów analitycznych, umożliwiając prowadzenie pogłębionych badań nad jego genezą, charakterem oraz konsekwencjami. W doktrynie bezpieczeństwa przyjmuje się, iż zagrożenie bezpieczeństwa stanowi złożony układ zdarzeń zachodzących w sferze wewnętrznej państwa bądź w jego relacjach międzynarodowych, którego wystąpienie – z wysokim stopniem prawdopodobieństwa – może prowadzić do naruszenia lub ograniczenia warunków niezakłóconego funkcjonowania oraz rozwoju państwowości (Dworecki, 1994).

W nawiązaniu do problematyki niniejszego opracowania, zasadne jest przywołanie definicyjnego ujęcia zagrożeń asymetrycznych, stanowiących jedno z istotnych źródeł współczesnych zagrożeń bezpieczeństwa. Pojęcie to definiowane jest jako sposób myślenia, organizowania oraz prowadzenia działań w sposób odmienny względem przeciwnika, polegający w szczególności na wykorzystywaniu wszelkiego rodzaju dysproporcji występujących w szeroko rozumianych potencjałach stron konfliktu. Asymetryczność ta odnosi się zarówno do sfery militarnej, jak i niemilitarnej, obejmując zróżnicowane instrumenty oddziaływania na bezpieczeństwo państwa (Kaczmarek, Łepkowski, Zdrodowski, 2008).

W ujęciu doktrynalnym zagrożenie asymetryczne oznacza prowadzenie działań konfrontacyjnych z naruszeniem konwencjonalnych zasad użycia siły, w szczególności poprzez eksploatowanie efektu zaskoczenia w przestrzeni operacyjnej i strategicznej oraz stosowanie środków walki w sposób nieprzewidywalny i niestandardowy (Ciekanowski, 2009). Należy ponadto odnieść się do samego pojęcia asymetryczności, które w literaturze przedmiotu utożsamiane jest przede wszystkim ze specyfiką sposobu prowadzenia działań przez strony potencjalnego konfliktu. W ujęciu strategicznym asymetryczność oznacza stan nierównowagi potencjałów, w którym jeden z podmiotów dysponuje zasobami, zdolnościami operacyjnymi oraz instrumentami oddziaływania pozostającymi w wyraźnej dysproporcji względem drugiej strony. Dysproporcja ta może dotyczyć zarówno komponentów militarnego, technologicznego i ekonomicznego, jak również organizacyjnych czy demograficznych (Thornton, 2007). Klasycznym przykładem relacji asymetrycznej jest konfrontacja wysoko rozwiniętego państwa federalnego, jakim są Stany Zjednoczone, z zdecentralizowaną organizacją terrorystyczną o charakterze sieciowym, taką jak Al-Kaida.

W konsekwencji zagrożeń asymetrycznych nie należy redukować wyłącznie do katalogu stosowanych metod, technik czy taktyk działania. Ich istota odnosi się bowiem przede wszystkim do charakteru podmiotu prowadzącego działania oraz do sposobu, w jaki wykorzystuje on istniejące dysproporcje potencjałów stron konfliktu. Asymetryczność przejawia się zatem w celowym stosowaniu zróżnicowanych środków i instrumentów oddziaływania, generowanych w toku konfrontacji, których dobór ukierunkowany jest na kompensowanie własnych ograniczeń oraz maksymalizację podatności przeciwnika (Liedel, 2010).

Pierwsza z wymienionych kategorii odnosi się do podmiotowego zakresu zagrożeń asymetrycznych. W ujęciu wojskowym zagrożeniem asymetrycznym może być każdy aktor – zarówno państwowy, jak i pozapaństwowy – który w określonych uwarunkowaniach operacyjnych posługuje się metodami uznawanymi za niekonwencjonalne. O kwalifikacji zagrożenia decyduje zatem nie status podmiotu, lecz charakter stosowanych przez niego sposobów działania. W tym kontekście zagrożenie asymetryczne dla danego państwa może stanowić zarówno inne państwo, jak i aktor niepaństwowy. Zastosowanie przez przeciwnika niestandardowych form oddziaływania

– wynikających z dysproporcji potencjałów militarnych, technologicznych bądź organizacyjnych – przesądza o asymetrycznym charakterze konfrontacji. Takie podejście interpretacyjne dominuje w doktrynie i analizach środowisk wojskowych.

Druga kategoria eksponuje przede wszystkim rolę podmiotów transnarodowych oraz subnarodowych. Wysoka dynamika organizacyjna, zdecentralizowana struktura oraz elastyczność operacyjna sprzyjają stosowaniu metod asymetrycznych. W tym ujęciu to właśnie odmienność sposobów działania, w połączeniu z dysproporcją potencjałów stron konfliktu, pozwala uwypuklić specyfikę zagrożeń generowanych przez aktorów pozapaństwowych.

Charakterystyka zagrożeń asymetrycznych

W literaturze przedmiotu zagrożenia asymetryczne ujmowane są zasadniczo w dwóch komplementarnych perspektywach analitycznych (Blank, 2003; Olech, 2020):

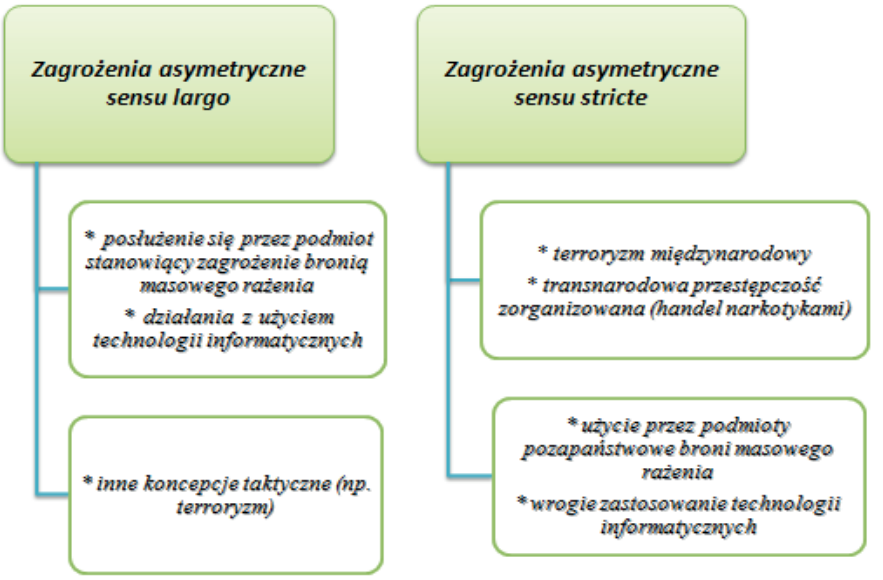
- zagrożenia asymetryczne sensu largo (ujęcie wojskowe),
- zagrożenia asymetryczne sensu stricte (ujęcie politologiczne).

Schematycznie omawiany problem przedstawiono na Rysunku 1.

Pierwsza z wymienionych kategorii odnosi się do podmiotowego zakresu zagrożeń asymetrycznych. W ujęciu wojskowym zagrożeniem asymetrycznym może być każdy aktor – zarówno państwowy, jak i pozapaństwowy – który w określonych uwarunkowaniach operacyjnych posługuje się metodami uznawanymi za niekonwencjonalne. O kwalifikacji zagrożenia decyduje zatem nie status podmiotu, lecz charakter stosowanych przez niego sposobów działania. W tym kontekście zagrożenie asymetryczne dla danego państwa może stanowić zarówno inne państwo, jak i aktor niepaństwowy. Zastosowanie przez przeciwnika niestandardowych form oddziaływania – wynikających z dysproporcji potencjałów militarnych, technologicznych bądź organizacyjnych – przesądza o asymetrycznym charakterze konfrontacji. Takie podejście interpretacyjne dominuje w doktrynie i analizach środowisk wojskowych (Sadowska, 2017).

Druga kategoria eksponuje przede wszystkim rolę podmiotów transnarodowych oraz subnarodowych. Wysoka dynamika organizacyjna, zdecentralizowana struktura oraz elastyczność operacyjna sprzyjają stosowaniu metod asymetrycznych. W tym ujęciu to właśnie odmienność sposobów działania,

w połączeniu z dysproporcją potencjałów stron konfliktu, pozwala uwypuklić specyfikę zagrożeń generowanych przez aktorów pozapaństwowych.



Rysunek 1. Rodzaje zagrożeń asymetrycznych

Źródło: Ciekanowski, 2009.

Odnosząc się do katalogu zagrożeń asymetrycznych ujmowanych w perspektywie *sensu stricte,* wskazać należy na kilka kluczowych kategorii oddziaływania, generowanych przede wszystkim przez aktorów pozapaństwowych, w szczególności:

- terroryzm międzynarodowy – stanowi formę przemocy politycznej ukierunkowanej przeciwko ludności cywilnej, terytorium, instytucjom państwowym bądź mieniu państwa innego niż kraj pochodzenia sprawców. Motywacje ideologiczne, religijne lub polityczne determinują wybór celów ataku, taktyk operacyjnych oraz środków użycia siły, istotnym uwarunkowaniem efektywności działalności terrorystycznej pozostaje dostęp do stabilnych źródeł finansowania, nasilenie aktywności struktur terrorystycznych odnotowano szczególnie po zamachach z 11 września 2001 r., co wpłynęło na globalizację tego zagrożenia (Kacperska, 2017),

- transnarodowa przestępczość zorganizowana – obejmuje struktury o nielegalnym, trwałym i zhierarchizowanym charakterze, realizujące swoje cele poprzez stosowanie przemocy, zastraszania, szantażu oraz mechanizmów korupcyjnych, ich działalność koncentruje się na generowaniu nielegalnych dochodów, m.in. z handlu narkotykami, bronią czy ludźmi, skala oddziaływania tych podmiotów na bezpieczeństwo państwa pozostaje ściśle powiązana z poziomem stabilności instytucjonalnej i kondycją systemu prawnego danego kraju (Marczyk, 2013),
- użycie broni masowego rażenia przez podmioty pozapaństwowe – dotyczy ryzyka pozyskania i zastosowania środków bojowych o charakterze nuklearnym, biologicznym bądź chemicznym przez aktorów niepaństwowych, potencjalne skutki obejmują masowe straty ludzkie oraz rozległe zniszczenia infrastrukturalne, pomimo relatywnie niskiej liczby odnotowanych incydentów, zagrożenie to pozostaje szczególnie istotne ze względu na skalę możliwych konsekwencji oraz trudności w kontroli proliferacji (Kukla, 2017),
- wrogie wykorzystanie technologii informatycznych (cyberzagrożenia) – obejmuje działania podejmowane w cyberprzestrzeni przeciwko systemom teleinformatycznym państw, infrastrukturze krytycznej oraz zasobom informacyjnym, choć początkowo aktywność podmiotów pozapaństwowych ograniczała się do relatywnie prostych form zakłóceń, takich jak defacement stron internetowych, współcześnie obserwuje się systematyczny wzrost kompetencji technologicznych tych aktorów, co przekłada się na rosnący poziom ryzyka dla bezpieczeństwa państw (Ciekanowski, 2009).

Należy zwrócić uwagę, że problematyka zagrożeń asymetrycznych została również szeroko omówiona w literaturze przedmiotu dotyczącej bezpieczeństwa morskiego (Rokiciński, 2005; Sokół, 2019). Współczesne środowisko morskie, obejmujące zarówno pas nadmorski, jak i akweny pozostające w obszarze odpowiedzialności sił morskich, generuje specyficzne spektrum zagrożeń o charakterze asymetrycznym. Do kluczowych kategorii zagrożeń asymetrycznych w środowisku morskim zalicza się w szczególności (Rokiciński, 2005):

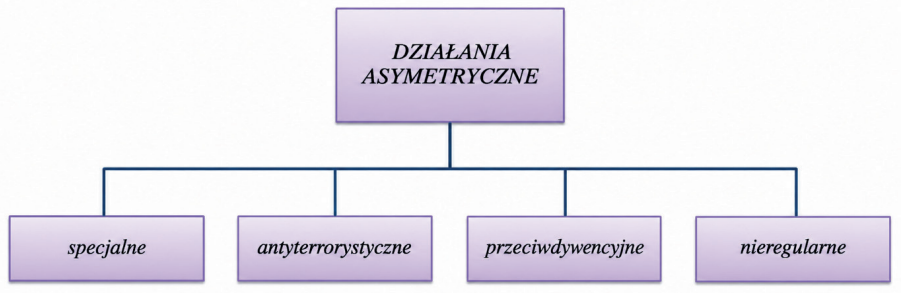
- proliferację broni masowego rażenia – analizowaną w kontekście wykorzystania morskich szlaków komunikacyjnych do transportu surowców strategicznych, komponentów technologicznych oraz systemów przenoszenia, które mogą zostać użyte w procesie wytwarzania lub dostarczania broni nuklearnej, biologicznej i chemicznej, zagrożenie to pozostaje istotnym wyzwaniem dla międzynarodowych reżimów kontroli zbrojeń oraz bezpieczeństwa żeglugi,
- terroryzm morski – obejmujący zarówno bezpośrednie akty przemocy, jak i groźbę ich użycia wobec środków transportu morskiego, jednostek pływających wykonujących zadania państwowe, infrastruktury portowej oraz obiektów zlokalizowanych w pasie nadbrzeżnym, działania te ukierunkowane są na destabilizację bezpieczeństwa ekonomicznego i transportowego państw nadmorskich,
- nielegalną migrację drogą morską – stanowiącą złożone wyzwanie dla systemów ochrony granic, obejmujące zorganizowane przerzuty ludności realizowane z wykorzystaniem morskich kanałów przerzutowych, często powiązane z działalnością grup przestępczych,
- transnarodową przestępczość zorganizowaną – przejawiającą się, w szczególności, w morskim przemycie i dystrybucji środków odurzających, handlu bronią, a także transporcie oraz nielegalnym składowaniu substancji i materiałów niebezpiecznych dla środowiska morskiego,
- piractwo morskie – polegające na dokonywaniu zbrojnych napadów na statki handlowe oraz inne jednostki pływające, motywowanych najczęściej chęcią uzyskania korzyści finansowych, przejęcia ładunku bądź wymuszenia okupu.

Pomiędzy wskazanymi wcześniej kategoriami zagrożeń asymetrycznych dostrzegalne są istotne różnice, determinujące specyfikę poszczególnych ich typów. Zróżnicowanie to odnosi się zarówno do charakteru samych zagrożeń, jak i do podmiotów stanowiących źródło ich generowania oraz intensywności oddziaływania. Odmienność ta przejawia się w zakresie stosowanych metod działania, skali operacyjnej, poziomu zorganizowania struktur sprawczych, a także w dynamice i częstotliwości występowania poszczególnych form zagrożeń w środowisku bezpieczeństwa. Zagrożenia wynikające z asymetrycznego charakteru współczesnego środowiska bezpieczeństwa

neutralizowane są przede wszystkim w ramach działań asymetrycznych, stanowiących adekwatną formę reakcji na niestandardowe metody oddziaływania przeciwnika (Sadowska, 2017).

Działania asymetryczne ujmowane są jako kompleksowy zespół przedsięwzięć o charakterze politycznym, militarnym oraz policyjnym, ukierunkowanych na przeciwdziałanie aktorowi asymetrycznemu w warunkach nasilających się procesów globalizacyjnych. Istotą jest prowadzenie operacji w sposób elastyczny i niestandardowy, z wykorzystaniem dostępnych przewag jakościowych, przy jednoczesnej minimalizacji ryzyka utraty własnego potencjału (Robertson, 1997). Czynności składające się na działania asymetryczne realizowane są najczęściej na poziomie taktycznym i operacyjnym, w warunkach umożliwiających osiągnięcie założonych celów przy ograniczonych nakładach sił i środków.

Szczegółowa typologia działań asymetrycznych została przedstawiona poniżej – Rysunek 2 (Rokiciński, 2005).



Rysunek 2. Rodzaje działań asymetrycznych
Źródło: Elak, 2014.

Działania specjalne stanowią wyspecjalizowaną kategorię operacji militarnych realizowanych przez komponenty sił specjalnych, obejmującą w szczególności rozpoznanie specjalne, akcje bezpośrednie, pomoc militarną oraz działania towarzyszące. Na potrzeby konkretnych przedsięwzięć operacyjnych wydzielane są odpowiednio przygotowane siły i środki, przeznaczone do realizacji zadań w ramach operacji połączonych. Zasadniczym celem działań specjalnych pozostaje pozyskiwanie, analiza i przekazywanie informacji o przeciwniku, jego infrastrukturze oraz terenie prowadzenia operacji, a także systematyczne obniżanie jego potencjału bojowego (Jagodziński,

2020). Istotnym wymiarem tych operacji jest również neutralizacja obiektów o kluczowym znaczeniu militarnym na terytorium przeciwnika oraz udzielanie wsparcia pozostałym komponentom sił zbrojnych, siłom sojuszniczym, a w określonych warunkach także podmiotom cywilnym zaangażowanym w działania stabilizacyjne. Operacje specjalne prowadzone są zasadniczo w przestrzeni operacyjnej przeciwnika, w szczególności na obszarach, gdzie jego zdolności rozpoznawcze i bojowe pozostają ograniczone bądź nieskuteczne (Stringer, 2022).

Działania antyterrorystyczne obejmują z kolei zespół przedsięwzięć ukierunkowanych na neutralizację struktur terrorystycznych oraz eliminację generowanego przez nie zagrożenia. W ich toku realizowane są operacje przeszukania wyznaczonych rejonów, zatrzymywania osób podejrzanych o działalność terrorystyczną, obezwładniania sprawców, a w sytuacjach uzasadnionych - użycia środków przymusu bezpośredniego, w tym siły zbrojnej. Działania te ukierunkowane są na przywrócenie stabilności bezpieczeństwa, ochronę ludności cywilnej oraz zabezpieczenie funkcjonowania struktur państwowych i wojskowych (Gardocka, 2021). Istotną kategorię stanowią również działania przeciwdywersyjne, skoncentrowane na przeciwdziałaniu aktywności grup dywersyjno-rozpoznawczych, sabotażowych oraz terrorystycznych. W przypadku braku możliwości ich bezpośredniej neutralizacji podejmowane są przedsięwzięcia zmierzające do ograniczenia ich swobody operacyjnej, w tym izolowanie rejonów ich aktywności, blokowanie manewru, organizowanie zasadzek czy prowadzenie działań pościgowych. Działania te mogą przyjmować zarówno charakter zaczepny – ukierunkowany na wykrycie, zniszczenie bądź obezwładnienie przeciwnika, jak i obronno-ochronny, skoncentrowany na zabezpieczeniu obiektów i infrastruktury o znaczeniu strategicznym. Realizowane są one zarówno na terytorium własnym, jak i na obszarach okupowanych czy w przestrzeni państw trzecich, w ramach operacji koalicyjnych (Jakubczak, 2020).

Działania nieregularne stanowią natomiast szczególną formę walki prowadzonej w warunkach kontroli terenu przez przeciwnika, z wykorzystaniem niestandardowych metod operacyjnych zapewniających siłom je realizującym zdolność przetrwania oraz skutecznego oddziaływania na jego potencjał militarny. Mogą mieć one charakter działań wymuszonych, podejmowanych w reakcji na nagłe zagrożenia dla pododdziałów, bądź działań

planowych, realizowanych zarówno w wariancie defensywnym – polegającym na pozostawaniu w ugrupowaniu przeciwnika po wykonaniu zadania – jak i ofensywnym, zakładającym przenikanie na jego tyły po przekroczeniu linii styczności (Michalak, 2016). Ich zasadniczym celem pozostaje prowadzenie rozpoznania, osłabianie potencjału bojowego i logistycznego przeciwnika, dezorganizacja jego systemów dowodzenia oraz zabezpieczenie działań, a także ograniczanie możliwości użycia jego sił i środków w określonym miejscu i czasie. Decyzje o podjęciu działań nieregularnych podejmowane są – co do zasady – na wyższych szczeblach dowodzenia, jednak w sytuacjach nadzwyczajnych, takich jak utrata łączności z przełożonym, mogą zostać podjęte autonomicznie przez dowódców pododdziałów (Elak, 2014; Gryga, 2020a, 2020b).

Przeciwnik asymetryczny jako uczestnik działań

W nawiązaniu do wcześniej przedstawionych ustaleń analitycznych zasadne staje się pogłębione rozpatrzenie pojęcia przeciwnika asymetrycznego w kontekście sfer jego aktywności operacyjnej. Przeciwnik asymetryczny to najczęściej aktor niepaństwowy, pozbawiony klasycznych atrybutów podmiotowości państwowej, takich jak terytorium, ludność czy sformalizowane struktury instytucjonalne. Brak podmiotowości prawnomiędzynarodowej powoduje, iż nie funkcjonuje on w ramach reżimów prawa międzynarodowego, co w istotny sposób komplikuje zarówno proces jego identyfikacji, jak i stosowanie wobec niego standardowych mechanizmów reagowania obronnego (Koziej, 2006; Wejkszner, 2009). Przeciwnik asymetryczny wykorzystuje wszelkie dostępne środki walki, niejednokrotnie sięgając także po metody i narzędzia zakazane przez prawo międzynarodowe konfliktów zbrojnych. Z tego względu często pozostaje poza reżimem konwencji międzynarodowych, w tym norm prawa humanitarnego (Pfanner, 2005).

Struktury tego typu przybierają zróżnicowane formy organizacyjne - od ugrupowań rebelianckich i partyzanckich, poprzez formacje paramilitarne, aż po najemne komponenty zbrojne. Ich działalność cechuje się wysokim stopniem konspiracji oraz zdolnością do funkcjonowania w bezpośrednim przenikaniu ze środowiskiem ludności cywilnej, co znacząco utrudnia ich identyfikację oraz neutralizację operacyjną. Dodatkowo operują one

najczęściej w niewielkich, rozproszonych grupach, co zwiększa ich mobilność oraz utrudnia przeciwdziałanie ze strony sił konwencjonalnych (Geiß, 2006).

Motywacja do prowadzenia walki ma nierzadko charakter ideologiczny lub religijny, przyjmując postać radykalizmu bądź fanatyzmu, co wzmacnia determinację bojową oraz gotowość do ponoszenia strat własnych (Elak, 2012). Dla zobrazowania specyfiki zagrożeń asymetrycznych wskazać należy, iż pomimo częstych założeń o ograniczonych zdolnościach operacyjnych struktur terrorystycznych do prowadzenia działań na szeroką skalę, pojedyncze, wysoko spektakularne akty przemocy mogą generować nieproporcjonalnie rozległe skutki destrukcyjne. Skala oddziaływania takich incydentów wynika nie tyle z potencjału militarnego sprawców, ile z wyboru celów o wysokiej wrażliwości infrastrukturalnej oraz symbolicznej (Kuć, 2020). Szczególną podatność w tym zakresie wykazuje środowisko morskie. Dostępność szlaków żeglugowych, relatywna otwartość infrastruktury portowej oraz możliwości wykorzystania środków transportu morskiego do przerzutu materiałów wybuchowych stwarzają dogodne warunki do przeprowadzenia ataków terrorystycznych. Potencjalne cele obejmują zarówno infrastrukturę portową, jak i jednostki pływające znajdujące się w akwenach portowych (Sokół, 2019).

Analiza scenariuszy zagrożeń wskazuje, iż operacje wymierzone w obiekty portowe oraz statki zacumowane w portach mogą przyjmować formę ataków bombowych, realizowanych z użyciem jednostek nawodnych bądź ładunków ukrytych w transporcie morskim. Tego rodzaju *modus operandi* stanowi dla ugrupowań terrorystycznych atrakcyjne narzędzie oddziaływania, umożliwiające nie tylko zadanie strat materialnych, lecz także czasowe zakłócenie funkcjonowania infrastruktury krytycznej oraz – w skrajnych przypadkach – przejęcie kontroli nad wybranymi obiektami (Zboina, 2014).

Podsumowanie

Różnorodność współczesnych zagrożeń bezpieczeństwa stanowi bezpośrednią konsekwencję przeobrażeń systemowych, jakie dokonały się w środowisku międzynarodowym w ostatnich dekadach. Fundamentalne znaczenie miało w tym zakresie zakończenie zimnej wojny i rozpad

dwubiegunowego ładu globalnego, który przez dziesięciolecia determinował strukturę rywalizacji polityczno-wojskowej. Transformacje ekonomiczne, społeczne i ustrojowe wymusiły na podmiotach stosunków międzynarodowych redefinicję percepcji zagrożeń oraz rewizję dotychczasowych modeli reagowania.

Współcześnie prognozowanie charakteru zagrożeń, ich lokalizacji, potencjału sprawczego czy zastosowanych środków oddziaływania pozostaje zadaniem wysoce utrudnionym. Szczególnego znaczenia nabrało w tym kontekście wykształcenie kategorii przeciwnika asymetrycznego, który – ze względu na brak klasycznych atrybutów państwowości, elastyczność strukturalną oraz niekonwencjonalne metody działania – wymusił zmianę paradygmatu bezpieczeństwa zarówno w wymiarze narodowym, jak i sojuszniczym. Asymetria, rozumiana jako przeciwieństwo symetrii, a więc brak współmierności potencjałów, struktur i sposobów prowadzenia działań, generuje szczególnie złożone wyzwania operacyjne. Podmioty trudne do jednoznacznej identyfikacji, nieosadzone w określonych ramach terytorialnych czy instytucjonalnych, mogą dysponować zdolnościami oddziaływania nieproporcjonalnymi do swojego formalnego potencjału. Zjawisko to znajduje odzwierciedlenie zwłaszcza w działalności współczesnych organizacji terrorystycznych, w tym ugrupowań o podłożu fundamentalistycznym, które wykorzystują niestandardowe metody walki oraz efekt zaskoczenia strategicznego.

W rezultacie dotychczasowe, monolityczne modele zagrożeń, charakterystyczne dla epoki rywalizacji blokowej, utraciły dominujące znaczenie. Ich miejsce zajęły zagrożenia rozproszone, wielowymiarowe i trudne do przewidywania w zakresie formy oraz skutków. Symbolicznym momentem tej transformacji były zamachy z 11 września 2001 r., które unaoczniły skalę oddziaływania niepaństwowego aktora terrorystycznego na globalny system bezpieczeństwa. W odpowiedzi uruchomiono mechanizm obrony zbiorowej przewidziany w art. 5 Traktatu Waszyngtońskiego, co potwierdziło kluczową rolę NATO w przeciwdziałaniu zagrożeniom asymetrycznym oraz w kształtowaniu współczesnej architektury bezpieczeństwa międzynarodowego.

Literatura

1. Blank, S. J. (red.). (2003). *Asymmetric warfare: Threat and response in the twenty-first century*. Strategic Studies Institute, U.S. Army War College.
2. Ciekanowski, Z. (2009). Działania asymetryczne jako źródło zagrożeń bezpieczeństwa. *Bezpieczeństwo i Technika Pożarnicza*, *3,* 47-72.
3. Czywilis, D. (2007). Pojęcie bezpieczeństwa międzynarodowego w ujęciu teorii konstruktywizmu. *Rocznik Bezpieczeństwa Międzynarodowego*, *2,* 67-286, https://doi.org/10.34862/rbm.2007.20
4. Dworecki, S. (1994). *Zagrożenia bezpieczeństwa państwa*. Warszawa: Akademia Obrony Narodowej.
5. Elak, L. (2012). Wyzwania wobec sił zbrojnych na początku XXI wieku. W: R. Bani, K. Zdulskiego (red.), *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku* (s. 93). Łódź: Wydawnictwo Naukowe Ibidem.
6. Elak, L. (2014). *Podstawy działań taktycznych*. Warszawa: Akademia Obrony Narodowej.
7. Gardocka, N. (2021). Prawne metody walki z terroryzmem. W: J. Jędrzejewska, J. Kozłowska (red.), *Wybrane zagadnienia z zakresu prawa, bezpieczeństwa i terroryzmu*. Lublin: Wydawnictwo Naukowe Tygiel.
8. Geiß, R. (2006). Asymmetric conflict structures. *International Review of the Red Cross*, *88*(864), 757-777. https://doi.org/10.1017/S1816383107000781
9. Gryga, M. (2020a). *Działania nieregularne i niekonwencjonalne a Polska [Raport – Cz. 1].* Pobrane z: https://defence24.pl/polityka-obronna/dzialania-nieregularne-i-niekonwencjonalne-a-polska-raport-cz-1 (dostęp: 28.01.2026).
10. Gryga, M. (2020b). *Działania nieregularne i niekonwencjonalne w warunkach Polski [Raport – Cz. 2].* Pobrane z: https://defence24.pl/sily-zbrojne/dzialania-nieregularne-i-niekonwencjonalne-w-warunkach-polski-raport-cz-2 (dostęp: 28.01.2026).
11. Jagodziński, B. (2020). Działania i rozwój jednostek specjalnych. *Przegląd Bezpieczeństwa Wewnętrznego, 22*, 167-184.

12. Jakubczak, R. (2020). *Powszechna obrona terytorialna w bezpieczeństwie narodowym RP*. Warszawa.
13. Jasiński, A. (2013). *Architektura w czasach terroryzmu. Miasto-przestrzeń publiczna-budynek*. Warszawa: Wolters Kluwer Polska.
14. Kacperska, E. (2017). Terroryzm międzynarodowy jako problem globalny współczesnej gospodarki. *Zeszyty Naukowe Szkoły Głównej Gospodarstwa Wiejskiego. Ekonomika i Organizacja Gospodarki Żywnościowej*, *120,* 17-31. https://doi.org/10.22630/EIOGZ.2017.120.36
15. Kaczmarek, J., Łepkowski, W., Zdrodowski, B. (red.). (2008). *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa: Akademia Obrony Narodowej.
16. Koziej, S. (2006). *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*. Toruń: Wydawnictwo Adam Marszałek.
17. Koziej, S. (2011). Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja. *Bezpieczeństwo Narodowe, 18,* 19-39.
18. Kuć, M. (2020). The Specific Nature of Asymmetric Conflicts. *Teka Komisji Prawniczej PAN Oddział W Lublinie*, *13*(2), 375-381. https://doi.org/10.32084/tekapr.2020.13.2-28
19. Kukla, K. (2017). Przeciwdziałanie użyciu broni masowego rażenia przez terrorystów na przykładzie Stanów Zjednoczonych. *Wiedza Obronna*, *44*(1/2), 50-72.
20. Liedel, K. (2010). *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*. Warszawa: Difin.
21. Marczyk, A. (2013). Główne rodzaje przestępczości zorganizowanej. *Security, Economy & Law, 2,* 93-107.
22. Michalak, A. (2016). Działania nieregularne – współczesne wyzwania. *Kwartalnik Bellona*, *686*(3), 84-98.
23. National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report. Executive Summary*. Pobrane z: https://govinfo.library.unt.edu/911/report/911Report_Exec.html (dostęp: 28.01.2026).
24. Olech, A. K. (2020). *Zagrożenia asymetryczne i ich wpływ na współczesne konflikty na przykładzie Ukrainy*. Warszawa: Instytut Nowej Europy.

25. Pfanner, T. (2005). Asymmetrical warfare from the perspective of humanitarian law and humanitarian action. *International Review of the Red Cross*, *87*(857), 149-174. https://doi.org/10.1017/S1816383100181238
26. Potulski, J. (2013). Czym jest geopolityka? Spory wokół statusu badawczego geopolityki. W: P. Eberhardt (red.), *Studia nad geopolityką XX wieku*. Warszawa: Instytut Geografii i Przestrzennego Zagospodarowania im. Stanisława Leszczyckiego PAN.
27. Robertson, W. G. (1997). *Asymmetric Threats and the Future of U.S. National Security*. Arlington: CACI International Inc. Symposium Report.
28. Rokiciński, K. (2005). Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich. *Zeszyty Naukowe Akademii Marynarki Wojennej*, *1*(160), 151-171.
29. Sadowska, E. (2017). Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie. *Rocznik Bezpieczeństwa Międzynarodowego*, *11*(2), 18-27, https://doi.org/10.34862/rbm.2017.2.3
30. Sokół, M. (2019). Zagrożenia asymetryczne w regionie bałtyckim – wybrane aspekty. *Krakowskie Studia Małopolskie, 24,* 168-180, https://doi.org/10.15804/ksm201909
31. Stringer, K. D. (2022). Special Operations Forces (SOF): The Integrators for Total Defense and Resistance. *Journal on Baltic Security*, *8*(1), 65-75. https://doi.org/10.57767/jobs_2022_0001
32. Thornton, R. (2007). *Asymmetric Warfare: Threat and Response in the Twenty-First Century*. Cambridge: Polity Press.
33. Wejkszner, A. (2009). Wojny XXI wieku. Istota współczesnych konfliktów asymetrycznych. W: S. Wojciechowski, R. Fiedler (red.), *Zagrożenia asymetryczne współczesnego świata*. Poznań: Wydawnictwo Naukowe Wydziału Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza.
34. Zboina, J. (2014). *Bezpieczeństwo na lądzie, morzu i w powietrzu w XXI wieku*. Józefów: CNBOP-PIB.

Leszek Elak[1]
Akademia Sztuki Wojennej w Warszawie
Marek Ciekanowski[2]
Społeczna Akademia Nauk filia w Warszawie

https://doi.org/10.29316/9788368103373_3

CHARAKTERYSTYKA I UWARUNKOWANIA WSPÓŁCZESNYCH ZAGROŻEŃ BEZPIECZEŃSTWA – ASPEKTY MILITARNE, CYBERNETYCZNE I ŚRODOWISKOWE

CHARACTERISTICS AND CONTEXT OF CONTEMPORARY SECURITY THREATS – MILITARY, CYBER, AND ENVIRONMENTAL ASPECTS

Streszczenie

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą liczbą zagrożeń o zróżnicowanym charakterze, obejmujących zarówno działania militarne i asymetryczne, jak i zagrożenia technologiczne oraz środowiskowe. Do najistotniejszych należą konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe, które mogą destabilizować funkcjonowanie państw, wpływać na bezpieczeństwo społeczeństwa oraz zakłócać działanie infrastruktury krytycznej. Celem rozdziału jest przedstawienie istoty tych zagrożeń, ich genezy, sposobów oddziaływania oraz

[1] https://orcid.org/0000-0002-5255-9768, e-mail: l.elak@akademia.mil.pl
[2] https://orcid.org/0009-0009-1271-0652, e-mail: marek@ciekanowski.pl

znaczenia dla bezpieczeństwa państwa. Problem badawczy sformułowano: w jaki sposób konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe oddziałują na bezpieczeństwo państwa i społeczeństwa? Przyjęto hipotezę, że współczesne zagrożenia bezpieczeństwa mają charakter złożony i wielowymiarowy, a ich skuteczne ograniczanie wymaga zintegrowanych działań państwa w sferze militarnej, organizacyjnej, technologicznej i prawnej. W opracowaniu wykorzystano metodę analizy literatury przedmiotu, analizę dokumentów i opracowań dotyczących bezpieczeństwa oraz metodę porównawczą, co pozwoliło na ukazanie omawianych zjawisk w szerszym kontekście funkcjonowania systemów bezpieczeństwa. Przeprowadzona analiza wskazuje, że współczesne zagrożenia często występują równocześnie i wzajemnie się uzupełniają, dlatego skuteczne przeciwdziałanie im wymaga kompleksowego podejścia do bezpieczeństwa, obejmującego współpracę instytucji państwowych, rozwój technologii, działania prewencyjne oraz podnoszenie świadomości społecznej.

Słowa kluczowe: bezpieczeństwo państwa, cyberataki, konflikty hybrydowe, terroryzm, katastrofy środowiskowe

Abstract

The modern security environment is characterised by a growing number of diverse threats, including both military and asymmetric operations, as well as technological and environmental threats. The most important are hybrid conflicts, cyberattacks, terrorism, and environmental disasters, which can destabilise state functioning, affect societal security, and disrupt the operation of critical infrastructure. The aim of the chapter is to present the essence of these threats, their genesis, their impact, and their significance for national security. The research problem was formulated as follows: how do hybrid conflicts, cyberattacks, terrorism, and environmental disasters affect the security of the state and society? The hypothesis was adopted that contemporary security threats are complex and multidimensional, and their effective reduction requires integrated state actions in the military, organisational, technological and legal spheres. The study uses the methods of analysing the literature on the subject, analysing documents and studies on security, and the comparative method, which allows for presenting the discussed phenomena in the broader context of the functioning of security systems. The analysis indicates that contemporary threats often occur simultaneously and complement each other, so effective countermeasures require a comprehensive security approach that includes cooperation among state institutions, technology development, preventive measures, and increased social awareness.

Keywords: state security, cyberattacks, hybrid conflicts, terrorism, environmental disasters

Wstęp

Współczesne środowisko bezpieczeństwa charakteryzuje się wysoką dynamiką zmian oraz rosnącą złożonością zagrożeń, które coraz częściej mają charakter wielowymiarowy i trudny do jednoznacznej identyfikacji. Postęp technologiczny, globalizacja, rozwój cyberprzestrzeni, a także nasilające się procesy społeczno-polityczne i środowiskowe sprawiają, że państwa muszą mierzyć się z nowymi formami oddziaływania, wykraczającymi poza tradycyjnie rozumiane konflikty zbrojne. Współczesne zagrożenia obejmują zarówno działania o charakterze militarnym i asymetrycznym, jak i zagrożenia wynikające z działalności człowieka, zmian klimatycznych czy rozwoju infrastruktury przemysłowej i teleinformatycznej. Szczególne znaczenie w tym kontekście zyskują konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe. Zjawiska te, mimo odmiennego charakteru, łączy zdolność do destabilizowania funkcjonowania państw, zakłócania działania infrastruktury krytycznej, wywoływania strat gospodarczych oraz oddziaływania na społeczeństwo poprzez wytwarzanie poczucia zagrożenia i niepewności. W wielu przypadkach zagrożenia te występują równocześnie i wzajemnie się przenikają, co dodatkowo utrudnia skuteczne przeciwdziałanie.

Celem niniejszego rozdziału jest przedstawienie istoty oraz charakterystyki wybranych współczesnych zagrożeń dla bezpieczeństwa, ze szczególnym uwzględnieniem konfliktów hybrydowych, cyberataków, terroryzmu oraz katastrof środowiskowych. W opracowaniu omówiono genezę tych zjawisk, ich podstawowe definicje, mechanizmy oddziaływania oraz przykłady występowania, a także wskazano ich znaczenie dla bezpieczeństwa państwa i społeczeństwa.

Analiza została oparta na metodzie analizy literatury przedmiotu, materiałów źródłowych oraz dostępnych opracowań dotyczących bezpieczeństwa i zarządzania kryzysowego. Pozwoliło to na ukazanie omawianych zagrożeń w szerszym kontekście funkcjonowania współczesnych państw oraz systemów bezpieczeństwa. Podjęta problematyka ma istotne znaczenie zarówno w wymiarze teoretycznym, jak i praktycznym, gdyż właściwe rozpoznanie charakteru współczesnych zagrożeń stanowi podstawę skutecznego planowania działań zapobiegawczych, reagowania kryzysowego oraz budowania odporności państwa i społeczeństwa na sytuacje nadzwyczajne.

Istota i charakter konfliktów hybrydowych we współczesnym środowisku bezpieczeństwa

Pojęcie wojny hybrydowej zostało rozpowszechnione pierwszy raz przez Franka Hoffmana jako „jakikolwiek adwersarz używający kombinacji broni konwencjonalnej, nieregularnej taktyki, terroryzmu i przestępczości w tym samym czasie i na tym samym polu bitwy celem osiągnięcia celów politycznych" (Hajduk, Stępniewski, 2015). Pomimo tego, początki tej idei sięgają lat 60. XX wieku. Za pierwszego autora opisującego konflikty, które współcześnie określamy mianem wojen hybrydowych, uznaje się Jewgienija Messnera – twórcę koncepcji wojny buntowniczej. W swoich analizach Messner podkreślał, że nowoczesna wojna może przyjmować charakter ograniczony koalicyjnie lub mieć wymiar światowy. Ilustrował to na przykładzie wojny koreańskiej, podczas której Chiny jawnie wspierały Koreę Północną, natomiast Związek Radziecki angażował się nieoficjalnie. Zdaniem Messnera powodowało to zmianę przeciwnika, tradycyjnie rozumianego jako siły zbrojne wrogiego państwa. Od teraz uważał on, że głównym przeciwnikiem w wojnie będzie cały naród, a cały naród może być atakowany nie tylko środkami kinetycznymi, które to są dosyć kosztowne dla państw. W konfliktach określanych jako wojny buntownicze obserwuje się zacieranie granicy pomiędzy działaniami zbrojnymi uznawanymi przez prawo międzynarodowe za legalne a metodami walki zakwalifikowanymi jako bezprawne. Wynika to z braku wyraźnego rozgraniczenia między siłami zbrojnymi a ludnością cywilną. W tego rodzaju konfliktach kluczową rolę odgrywają formacje nieregularne, powoływane przez niezadowolone grupy społeczne, takie jak uzbrojeni członkowie organizacji zawodowych, którzy w warunkach miejskich mogą stanowić istotny czynnik siły. Zatarcie granic pomiędzy armią regularną a nieregularną prowadzi jednocześnie do erozji zasad etyki wojennej. Messner zwracał uwagę, że zmieniający się charakter wojny wymusza na sztabach skupienie się na rozwijaniu strategii, działań operacyjnych oraz taktyki opartej na terrorze, podstępie i zdradzie (Hajduk, Stępniewski, 2015).

Dalszy rozwój technologiczny, rewolucja cyfrowa i wprowadzenie nowych środków przekazu (mass media pokroju telewizji czy radia, ale także socialmediów) doprowadziły do sytuacji, w której działania hybrydowe bardzo mocno skupiają się na informacjach kierowanych do społeczeństwa

(Kamionka, 2023, s. 62). Już Messner w swoim dziele pisał o potrzebie działania informacyjnego na nieprzyjacielu, którą określał mianem *dywersji informacyjnej* (obok klasycznych dywersji i sabotażu). Do tego szczególnie ważne staje się dokładne zidentyfikowanie sposobów funkcjonowania systemów wczesnego ostrzegania przeciwnika oraz jego procedur zarządzania kryzysowego. Poza analizą kondycji systemu finansowego państwa i jego zdolności obronnych, kluczowe znaczenie ma również zgromadzenie pogłębionych danych dotyczących obiektów i sieci o znaczeniu strategicznym. Do najistotniejszych należą tu rozwiązania z zakresu teleinformatyki, infrastruktura transportowa, systemy produkcji i dystrybucji energii, w tym sieci gazowe, naftowe i elektroenergetyczne, dostępność zasobów surowcowych i paliwowych, a także mechanizmy zapewniające ciągłość dostaw żywności i wody oraz sprawne funkcjonowanie opieki zdrowotnej (Sykulski, 2015, s. 106-107).

Z perspektywy podmiotów planujących działania polityczno-militarne zgodnie z założeniami koncepcji J. Messnera kluczowe znaczenie ma stopniowe doprowadzenie do narastania frustracji wśród szerokich warstw społeczeństwa oraz pogłębianie sporów w obrębie elit władzy. Następnie dąży się do osłabienia sytuacji gospodarczej, inicjowania niepokojów społecznych, a w konsekwencji do eskalacji w postaci jawnych działań zbrojnych. Są one prowadzone między innymi przez odpowiednio przygotowane jednostki sił specjalnych oraz funkcjonariuszy służb specjalnych, którzy działają po stronie przeciwnika. Skuteczność wojny buntowniczej w znacznym stopniu zależy od efektywnego prowadzenia operacji informacyjnych, obejmujących zarówno oddziaływanie na społeczeństwo państwa będącego celem ataku, jak i wpływanie na opinię międzynarodową. Istotnym elementem tych działań jest podważanie wiarygodności i reputacji atakowanego państwa, co w optymalnym wariancie prowadzi do jego politycznej izolacji. Realizacja koncepcji Messnera zakłada przede wszystkim unikanie oficjalnego udziału państwa w otwartym konflikcie zbrojnym. Grupy dywersyjne zaangażowane w działania nie posiadają oznaczeń identyfikujących ich przynależność, a ich uczestnicy – w świetle prawa międzynarodowego – nie są uznawani za żołnierzy regularnych sił zbrojnych. Pozwala to państwu inicjującemu na formalne zaprzeczenie swojemu zaangażowaniu w przypadku silnego oporu ze strony przeciwnika. W rezultacie dochodzi do swoistego

„odpaństwowienia" zarówno formacji zbrojnych, jak i samego konfliktu, który z zewnętrznej perspektywy może być postrzegany jako wojna domowa lub przejaw wewnętrznego chaosu.

W konfliktach określanych jako wojny buntownicze nie funkcjonuje tradycyjna linia frontu, a działania mogą zostać zapoczątkowane wewnątrz państwa, często z dala od jego granic. Istotnym elementem jest wykorzystywanie skupisk mniejszości narodowych i etnicznych, które mogą stanowić podatny grunt do wywoływania napięć społecznych i zamieszek, a jednocześnie pełnić rolę zaplecza logistycznego dla prowadzonych operacji. Ważnym aspektem przygotowań do tego typu konfliktów jest również inspirowanie oraz finansowe wspieranie ugrupowań radykalnych i ekstremistycznych, zarówno politycznych, jak i religijnych, działających na terytorium państw uznawanych za wrogie, a następnie rozwijanie ich aktywności w oparciu o strategię oporu niekierowanego (Sykulski, 2015). Z tego względu kluczowe znaczenie ma sprawne wykorzystanie zdolności wywiadowczych oraz skuteczne prowadzenie walki informacyjnej, która umożliwia przeniesienie konfrontacji z klasycznego pola walki do znacznie szerszej przestrzeni oddziaływania. Obejmuje ona przede wszystkim sferę świadomości społecznej, określaną jako noosfera, a także cyberprzestrzeń. Decydującą rolę odgrywają tu długofalowe działania psychologiczne i informacyjne, nastawione na stopniowe kształtowanie postaw, emocji i przekonań społeczeństwa.

Rozwojowi wojen buntowniczych sprzyja ponadto powstawanie niewielkich i słabych państw oraz wzrost znaczenia podmiotów nieuznawanych i dysfunkcyjnych, określanych mianem państw upadłych. Jewgienij Messner już na początku lat siedemdziesiątych XX wieku wskazywał na rosnącą rolę terroru jako narzędzia walki, w tym możliwość zastosowania skrajnych środków oddziaływania, takich jak punktowe użycie taktycznych ładunków jądrowych czy tzw. brudnych bomb, których głównym celem byłoby wywołanie silnego efektu psychologicznego. W tego rodzaju działaniach szczególnie istotne pozostają morale społeczeństwa oraz zdolność aparatu państwowego do opanowania narastającego strachu w taki sposób, aby nie przerodził się on w powszechną panikę. Już w okresie międzywojennym w działalności Kremla można dostrzec świadome stosowanie elementów strategii, które dziś określamy mianem wojny hybrydowej. ZSRR, formalnie pozostając w stanie pokoju z Polską po traktacie ryskim z 1921 roku, nie rezygnował z dążenia

do osłabienia sąsiedniego państwa przez działania poniżej oficjalnego progu otwartego konfliktu zbrojnego. Na północno-wschodnich rubieżach II RP, szczególnie na terenach Kresów zamieszkałych przez mniejszości narodowe, częste były prowokacje i akcje dywersyjne, które miały destabilizować sytuację społeczno-polityczną i podważać autorytet władz polskich.

Strategia ta zaczęła się ujawniać już w pierwszej połowie lat 20. XX wieku, choć najbardziej intensywnie realizowana była w 1924 r. Sowiecka agencja wywiadu wojskowego, Razwiedupr, kierowana przez zaawansowanych oficerów takich jak Jan Berzin, prowadziła zorganizowane działania dywersyjne na obszarach województw wileńskiego, nowogródzkiego i poleskiego. Celem było nie tylko sianie niepokoju, ale także przygotowanie warunków do ewentualnego powstania, które mogłoby posłużyć do ewentualnej aneksji tych terenów do ZSRR (Rodak, 2016). W praktyce działania te przybierały formę regularnych ataków na instytucje państwowe i strategiczne punkty II RP. Jednym z najbardziej znanych incydentów był atak na Stołpce w nocy z 3 na 4 sierpnia 1924 r., kiedy to około sześćdziesięcioosobowy oddział, prawdopodobnie dowodzony przez oficera sowieckiego wywiadu Stanisława Waupszasowa, przeprowadził skoordynowany atak na starostwo, posterunki policji i koszary, zabijając policjantów i cywilów oraz doprowadzając do chaosu w mieście tuż przy polsko-sowieckiej granicy (Rodak, 2016).

Podstawą sukcesów tych operacji była nie tylko agresja militarna w formie partyzanckiej, ale też wielostronna działalność propagandowa i agitacyjna wśród miejscowej ludności, szczególnie Białorusinów i Ukraińców, którzy często byli niezadowoleni z sytuacji społeczno-gospodarczej po I wojnie światowej i traktach powojennych. Sowieccy agitatorzy, często wracający repatrianci lub weterani Armii Czerwonej, potrafili wykorzystać lokalne niezadowolenie i historyczne antagonizmy, by zwiększać podatność ludności na idee komunistyczne i antypaństwowe.

Aktywność dywersyjna była na tyle nasilona, że w 1924 r. odnotowano co najmniej 207 incydentów zbrojnych tego typu na Kresach, co świadczy o skoordynowanym i długotrwałym charakterze tej ofensywy. Oddziały Razwiedupru korzystały zarówno z własnych ludzi, jak i lokalnych rekrutów, w tym działaczy Komunistycznej Partii Zachodniej Białorusi czy elementów przestępczych.

Dopiero zdecydowane środki podjęte przez polski rząd w postaci utworzenia Korpusu Ochrony Pogranicza oraz represji wobec działaczy proradzieckich doprowadziły do spadku liczby incydentów w regionie w 1925 r. Sowiecka operacja hybrydowa została częściowo wygaszona również z powodu zmian wewnętrznych w Moskwie i rosnącej krytyki wewnątrz sowieckich struktur wywiadowczych, co doprowadziło do oficjalnego zaniechania akcji (Rodak, 2016).

W 2014 roku Rosja prowadziła wobec Ukrainy działania o charakterze wojny hybrydowej, łącząc środki militarne, informacyjne i polityczne w sposób mający na celu osiągnięcie strategicznych celów bez formalnego wypowiedzenia wojny (Elak i in., 2024). Konflikt rozpoczął się od wydarzeń wokół Krymu, gdzie w lutym rosyjskie siły specjalne, pozbawione oficjalnych oznaczeń, zajęły budynki rządowe i przejęły kontrolę nad półwyspem (Oskierko i in., 2025). Te nieoznakowane jednostki, określane później mianem „zielonych ludzików", stanowiły przykład zastosowania sił zbrojnych w sposób zamaskowany, co utrudniało przypisanie im jednoznacznej odpowiedzialności państwowej. Zajęcie Krymu zakończyło się formalną aneksją półwyspu przez Rosję w marcu 2014 roku, mimo że nie doszło do oficjalnej wojny między państwami (Instytut Nowej Europy, b.d.).

Równocześnie Rosja prowadziła operacje informacyjne i propagandowe, które miały podważać legitymację władz w Kijowie po wydarzeniach Euromajdanu oraz tworzyć narracje uzasadniające ingerencję w sprawy Ukrainy, w tym ochronę ludności rosyjskojęzycznej. Prowadzono dezinformację zarówno wewnątrz Ukrainy, jak i wobec opinii międzynarodowej, co miało na celu stworzenie wewnętrznych podziałów społecznych i osłabienie odporności państwa ukraińskiego (Kłaczyński, 2019). Agresja Rosji na Ukrainę pokazała słabą jedność Europy wobec zagrożeń zewnętrznych, wynikającą z rozbieżnych interesów państw UE. Wydarzenia takie jak Euromajdan i wojna hybrydowa nie doprowadziły do wspólnego stanowiska w sprawach wschodnich (Trofymowych, 2016, s. 184).

Unia Europejska powinna wypracować spójną strategię wobec zagrożeń hybrydowych, wzmacniać zdolności analityczne i operacyjne oraz zwiększać samodzielność w zakresie bezpieczeństwa. Ważne jest też rozwijanie współpracy z NATO i innymi partnerami oraz zwalczanie szantażu migracyjnego (Żurawski, Oskierko, 2025, s. 65).

Zagrożenia środowiskowe i ich wpływ na bezpieczeństwo państwa

Na początku warto rozróżnić katastrofę środowiskową i ekologiczną. Katastrofa ekologiczna oznacza nieodwracalne zniszczenie uniemożliwiające przetrwanie gatunków, natomiast środowiskowa obejmuje każde katastrofalne zdarzenie w środowisku. W referacie autor skupi się na katastrofach środowiskowych ze względu na ich precyzyjne znaczenie. Katastrofa ekologiczna to trwałe zaburzenie struktur i funkcji ekosystemu bez możliwości kompensacji. Katastrofa ekologiczna skutkuje nieodwracalnymi zmianami jakościowymi i ilościowymi w łańcuchach troficznych. Rozróżnia się katastrofy ekologiczne antropogeniczne – powodowane przez człowieka, i nieantropogeniczne, zwane też katastrofami naturalnymi, wywoływane przez czynniki niezależne od człowieka. Do powodowanych przez czynniki ludzkie możemy zaliczyć:

- długotrwałe emisje szkodliwych substancji,
- zanieczyszczanie mórz i oceanów np. w wyniku wycieku ropy z tankowca,
- awarie przemysłowe powodujące wycieki substancji radioaktywnych i toksycznych.

Zaś do katastrof naturalnych (nieantropogenicznych) należą:

- huragany, tornada fale zimna bądź upałów, powodzie, susze,
- tsunami, wybuchy wulkanów, trzęsienia ziemi,
- pożary lasów, osuwiska i lawiny.

Czynniki antropogeniczne, oddziałując łącznie z procesami naturalnymi, często prowadzą do katastrof ekologicznych, których konsekwencje obejmują rozległe obszary lub mają zasięg globalny. Przykładowo, intensywna, monokulturowa gospodarka rolna w połączeniu z niekorzystnymi warunkami klimatycznymi sprzyja pustynnieniu znacznych terenów Ziemi, natomiast emisja dwutlenku węgla oraz innych gazów cieplarnianych, współdziałając z parą wodną obecną w atmosferze, potęguje efekt cieplarniany, co może skutkować istotnym wzrostem poziomu oceanów na skutek topnienia lodowców. Trzęsienia ziemi to jedne z najbardziej niebezpiecznych klęsk żywiołowych. Powstają wskutek nagłego uwolnienia energii w skorupie ziemskiej, najczęściej przez procesy tektoniczne. Silne wstrząsy (powyżej 6

stopni w skali Richtera) mogą powodować rozległe zniszczenia budynków, infrastruktury oraz poważne straty ludzkie.

Na terenach górskich wstrząsy sejsmiczne mogą wywoływać osuwiska i lawiny, natomiast trzęsienia podmorskie prowadzą do powstawania potężnych fal tsunami. Dane średnioroczne wskazują, że na świecie występuje około 100 trzęsień ziemi o magnitudzie powyżej 6 stopni w skali Richtera, co oznacza, że zjawisko to pojawia się średnio co kilka dni. Statystyki z lat 1984-1994 ukazują skalę jego tragicznych konsekwencji – około 90 tysięcy ofiar śmiertelnych, blisko pół miliona rannych oraz kilka milionów osób pozbawionych dachu nad głową. Należy również zaznaczyć, że trzęsienia ziemi mogą mieć charakter wzbudzony, np. w wyniku eksplozji jądrowych przeprowadzanych na obszarach aktywnych sejsmicznie.

Pożar definiuje się jako niekontrolowane i samorzutne rozprzestrzenianie się ognia, które stanowi bezpośrednie zagrożenie dla życia i zdrowia ludzi oraz powoduje poważne straty materialne. Współcześnie zjawisko to należy do jednych z istotniejszych zagrożeń o charakterze naturalnym i cywilizacyjnym. Pożary o podłożu naturalnym mogą być wywoływane przez różnorodne czynniki, takie jak wyładowania atmosferyczne, procesy samozapłonu (np. torfu czy siana), skupienie promieni słonecznych przez szkło lub soczewki, a także uszkodzenia infrastruktury energetycznej. Szczególnie dotkliwe konsekwencje środowiskowe niosą ze sobą pożary lasów i obszarów puszczańskich. Zjawiska te prowadzą do znacznej emisji gazów cieplarnianych, nasilają procesy erozji gleb, a także powodują lokalne zmiany warunków klimatycznych i hydrologicznych. Pożary niszczą nie tylko rozległe obszary drzewostanu, generując istotne straty ekonomiczne, lecz również leśne zasoby użytkowe oraz uprawy. W ich wyniku obniżeniu ulegają kluczowe funkcje lasu, takie jak zdolność retencjonowania wody czy jego korzystny wpływ na stan środowiska przyrodniczego. Ponadto dochodzi do degradacji cennej fauny oraz zakłócenia planowej gospodarki leśnej. Pożary obejmujące duże obszary stanowią również bezpośrednie zagrożenie dla pobliskich miejscowości i osiedli ludzkich.

Następnym zjawiskiem są burze i huragany. Gdy prędkość wiatru jest odpowiednio wysoka, skutki takich czynników mogą spowodować katastrofalne w skutkach zniszczenia budynków i urządzeń, a także śmierci ludzi i zwierząt. Huragany i trąby powietrzne sieją na swej drodze spustoszenia na

lądzie. Sztorm wywołuje wysokie i silne fale na morzu, które stanowią zagrożenie dla jednostek pływających i platform wiertniczych, a wdzierając się na brzeg, powodują przybrzeżne powodzie i wiele zniszczeń urządzeń brzegowych. Częstym zjawiskiem towarzyszącym są wybuchy przemysłowe. W ich wyniku dochodzi do zniszczenia obiektów i instalacji technicznych, powstawania pożarów oraz uszkodzeń systemów produkcyjnych. Najczęściej obserwuje się eksplozje kotłów wysokoprężnych, a także wybuchy gazów, par benzyny i innych substancji wykorzystywanych w przemyśle naftowym. Do najbardziej tragicznych w skutkach należą jednak eksplozje pyłu węglowego i gazów w kopalniach, jak również wybuchy butli gazowych oraz gazu w sieciach komunalnych. Poważne awarie przemysłowe zaliczane są do zdarzeń o charakterze nadzwyczajnym, powodujących znaczące straty w sferze zdrowotnej, środowiskowej oraz materialnej. W ich następstwie dochodzi do uwolnienia znacznych ilości substancji niebezpiecznych, które mogą oddziaływać szkodliwie na rozległe obszary. Mianem obszaru skażonego określa się teren wraz z znajdującą się na nim infrastrukturą, który został objęty działaniem substancji chemicznych, promieniotwórczych lub biologicznych. Natomiast rejon porażenia to obszar, na którym występują bezpośrednie skutki skażenia, takie jak negatywne oddziaływanie na ludzi, zwierzęta i rośliny, a także uszkodzenia sprzętu oraz różnego rodzaju obiektów spowodowane działaniem toksycznych czynników. Najważniejsza rzeczą wartą zapamiętania jest to, że rozprzestrzenianie się toksycznych środków przemysłowych stwarza zagrożenie dla życia organizmów żywych oraz wprowadza gwałtowne zmiany w naturalnym ekosystemie natury.

Katastrofy środowiskowe nasiliły się głównie przez działalność człowieka ze względu na rozwój przemysłu. Z tego względu w dzisiejszych czasach coraz bardziej rośnie znaczenie i wartość środowiska naturalnego, a samo rozumienie bezpieczeństwa ekologicznego ulega znacznej zmianie. Klęski żywiołowe, katastrofy wywołane działalnością człowieka, mogą i stanowią poważne zagrożenia dla państwa. W tej części autor postara się przedstawić działania człowieka, które mają na celu niwelowanie katastrof środowiskowych. Najważniejszym dokumentem dotyczącym bezpieczeństwa ekologicznego w Polsce jest Konstytucja RP. W rozdziale 5 podkreśla ona, że państwo zapewnia ochronę środowiska, opierając się na zasadzie zrównoważonego rozwoju. Konstytucja nakłada także obowiązek budowania

świadomości ekologicznej oraz zachęca do poszukiwania nowych dróg rozwoju z poszanowaniem środowiska. Warto tutaj wspomnieć o idei ekorozwoju, która została przedstawiona po raz pierwszy w 1975 roku przez Program Środowiskowy ONZ. Według Encyklopedii PWN, ekorozwój to długotrwały, samopodtrzymujący się rozwój gospodarczy, prowadzony z uwzględnieniem ochrony środowiska i troski o sprawiedliwość międzypokoleniową.

Podstawowe założenia światowej polityki ekorozwoju określono w 1993 roku w Deklaracji w sprawie Środowiska i Rozwoju oraz w Agendzie 21 podczas konferencji ONZ w Rio de Janeiro. Zasady ochrony środowiska, które obowiązują w polskim prawie, mają duże znaczenie: pomagają interpretować przepisy szczegółowe, wskazują kierunki przyszłych regulacji i precyzują zasady tworzenia aktów wykonawczych. Jedną z najważniejszych jest zasada zrównoważonego rozwoju, sformułowana w Deklaracji z Rio, a następnie włączona do prawa polskiego, między innymi przez art. 5 Konstytucji RP. Ustawa Prawo ochrony środowiska definiuje ją jako rozwój społeczno-gospodarczy polegający na łączeniu działań politycznych, ekonomicznych i społecznych przy jednoczesnym utrzymaniu równowagi przyrody oraz trwałości potrzeb obecnych i przyszłych pokoleń.

Zasada przezorności nakazuje podejmowanie działań zapobiegawczych, gdy brak jasnych dowodów na brak szkodliwości dla środowiska. Zasada prewencji wymaga analizy możliwych skutków przed rozpoczęciem działań, co stanowi podstawę przeciwdziałania degradacji środowiska, szczególnie poprzez procedurę oceny oddziaływania na środowisko. Obie zasady są obecne w prawie Unii Europejskiej oraz polskim systemie prawnym.

Cyberprzestrzeń jako domena zagrożeń bezpieczeństwa

Cyberatak to najnowsze zjawisko spośród tych omówionych w pracy. Wynika to z faktu, że cybernetyczne środowisko istnieje znacznie krócej niż tradycyjne zagrożenia, takie jak terroryzm, zagrożenia środowiskowe czy wojny hybrydowe, które towarzyszą ludzkości od starożytności pod różnymi nazwami i w różnych formach (Ciekanowski i in., 2023). Cyberprzestrzeń, czyli środowisko, gdzie zachodzą te ataki, powstała dopiero w latach 60. XX wieku. Pierwsze systemy cyberprzestrzeni zostały stworzone na potrzeby wojska, by umożliwić przesyłanie informacji na duże odległości między komputerami. Bodźcem do rozwoju tej technologii były ograniczenia

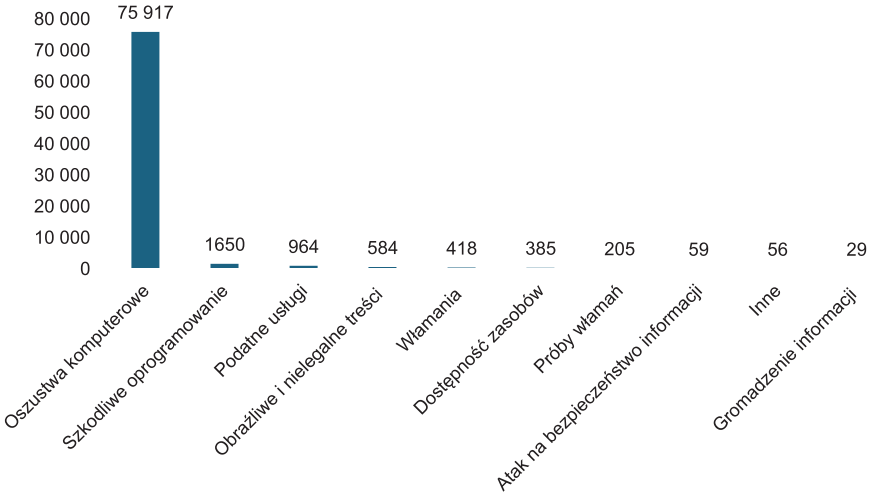
istniejących systemów komunikacji, które pozwalały na swobodną wymianę danych tylko w zamkniętych sieciach lokalnych.

Zjawisko cyberataku po dziś dzień rozwinęło się na tyle, że zostało zdefiniowane jako jedno z głównych zagrożeń i narzędzi w prowadzeniu operacji wojskowych czy pozyskiwania informacji wywiadowczych nie tylko na potrzeby państw, ale i podmiotów prywatnych. Według definicji zjawisko to oznacza każdy rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste (Słownik PWN, b.d.). Wartą uwagi jest również definicja podawana przez firmę Microsoft, przodującą w produkcji oprogramowania komputerowego. Definicja mówi natomiast o cyberataku jako celowe działanie osoby lub grupy osób mające na celu naruszenie, uszkodzenie lub zakłócenie działania systemów komputerowych, sieci lub urządzeń cyfrowych, często w złych zamiarach, takich jak kradzież danych, szpiegostwo, oszustwa finansowe lub sabotaż systemu (Microsoft, b.d.).

Wymienione w definicjach obiekty narażone na cyberataki i ich cele są skrupulatnie realizowane przez przeciwników nie tylko biznesowych czy przestępczych, ale w szczególności państwowych. Do zrealizowania takich celów ataków jak zawartych w definicji podmioty agresorów cyberprzestrzeni wykorzystują metody takie jak:

- Ataki malware,
- Phishing i sphere phishing,
- DoS, DDoS,
- MitM,
- Ransomware.

Poniżej na Rysunku 1 przedstawiono incydenty obsłużone przez CERT Polska w 2023 r. w podziale na kategorie.



Rysunek 1. Incydenty obsłużone przez CERT Polska w 2023 r. w podziale na kategorie

Źródło: CERT, 2023.

Powyższe metody ataków są najpopularniejszymi i najchętniej wykorzystywanymi ze względu na ich metodę przebiegu. Przykładowo, ataki malware polegają na uzyskaniu nieuprawnionego dostępu do określonego urządzenia czy sieci za pomocą szkodliwego oprogramowania lub nieświadomego dawania dostępu nieupoważnionej osobie (Trend Micro, b.d.).

W ujęciu Państwa polskiego cyberataki zyskują na znaczeniu w kwestii bezpieczeństwa tak samo jak w środowisku prywatnym i biznesowym. Cyberataki zyskują na znaczeniu w kwestii bezpieczeństwa tak samo jak w środowisku prywatnym i biznesowym, co zyskuje dodatkowe znaczenie na przestrzeni ostatnich lat, odkąd Rosja zintensyfikowała działania pod progiem wojny na nasz kraj. Jak pokazują statystyki, w Polsce dochodzi do 1500 cyberataków tygodniowo, co jest wzrostem w porównaniu z rokiem 2024 o 23% (Pasławski, 2025).

W związku z takimi wzrostami zagrożenia cyberatakami na podmioty naszego państwa, które trwają od ponad dekady, władze systematycznie rozwijają zdolności kontrdziałania przeciwko temu zjawisku.

Począwszy od napisania Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku. Doktryna ta zawiera elementy zdefiniowania poszczególnych zjawisk zachodzących w sferze cyberbezpieczeństwa oraz

cele, jak i środki przeciwdziałania tym zagrożeniom. W toku ewolucji świadomości państwa do zapobiegania tym aktom agresji siły zbrojne również dostrzegły potencjał domeny cyber do oddziaływania na przeciwnika oraz zdobywania przewagi informacyjnej. Doprowadziło to w roku 2022 do sformowania Wojsk Obrony Cyberprzestrzeni jak i ich odpowiednika w strukturze Wojsk Obrony Terytorialnej. Przez zdobycie takich elementów państwo uzyskało zdolności do kontrowania przyszłych zagrożeń, jakie stoją przed państwem. Jednakże w odróżnieniu od wojsk konwencjonalnych wojska cybernetyczne nie są ograniczone swoim terenem i mogą oddziaływać w czasie rzeczywistym w dowolnym miejscu na świecie, co, jak pokazują przykłady z historii, jest ich największym atutem w świecie zinformatyzowanych instytucji i nowoczesnych armii.

Takie formacje, zarówno nasze, jak i przeciwnika, mogą również rozmywać swoją odpowiedzialność za pomocą aktorów pozapaństwowych, jak robi to Federacja Rosyjska za pomocą tak zwanych farm trolli, czy Chiny przez PLA 61389, które w ramach swoich działań nie posiadają bezpośrednich jawnych powiązań ze strukturami swojego państwa, a niejednokrotnie swoje operacje wykonują z terenów nie należących do państwa, pod które podlegają. Ich operacje również nie stanowią jawnej operacji wojskowej, a jedynie wykupienie usługi u grup hakerskich lub stworzenie fikcyjnej grupy hakerskiej, tak jak ma to miejsce w przypadku chińskim (Volt Typhoon, APT31 i APT41) (Makeittogether, b.d.).

Taki sposób zarządzania siłą w cyberprzestrzeni prowadzi do sytuacji, w których sprawca cyberataku nie może zostać zidentyfikowany na bieżąco, a jedynie po długotrwałym dochodzeniu. Uniemożliwia to szybką i adekwatną reakcję podczas trwania ataku. Ten problem przestaje mieć znaczenie jedynie w sytuacjach otwartej agresji zbrojnej, kiedy działania w cyberprzestrzeni stanowią wsparcie tradycyjnych operacji militarnych.

Podsumowanie

Przeprowadzona analiza wskazuje, że współczesne środowisko bezpieczeństwa charakteryzuje się dużą dynamiką zmian oraz rosnącą złożonością zagrożeń, które coraz częściej mają charakter wielowymiarowy i wzajemnie powiązany. Konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe stanowią istotne wyzwania dla funkcjonowania państw,

ponieważ oddziałują nie tylko na sferę militarną, lecz także na gospodarkę, infrastrukturę krytyczną, środowisko naturalne oraz bezpieczeństwo społeczne. Szczególnie istotnym zjawiskiem jest zacieranie się granic pomiędzy stanem pokoju i konfliktem, co utrudnia jednoznaczne rozpoznanie zagrożeń oraz podjęcie adekwatnych działań zapobiegawczych i reagowania.

Współczesne zagrożenia cechują się również wysokim stopniem nieprzewidywalności oraz możliwością występowania efektów kaskadowych, w których jedno zdarzenie może prowadzić do kolejnych kryzysów w innych obszarach funkcjonowania państwa. Rozwój technologii informatycznych i telekomunikacyjnych, globalizacja oraz postępujące zmiany środowiskowe powodują, że państwa są coraz bardziej podatne na różnego rodzaju oddziaływania, zarówno ze strony innych państw, jak i podmiotów niepaństwowych.

Wnioskiem wynikającym z przeprowadzonych rozważań jest konieczność stosowania kompleksowego i zintegrowanego podejścia do bezpieczeństwa, obejmującego działania prewencyjne, rozwój systemów wczesnego ostrzegania, wzmacnianie odporności infrastruktury krytycznej, a także podnoszenie poziomu świadomości społecznej. Kluczowe znaczenie ma również współpraca międzynarodowa oraz stałe doskonalenie systemów zarządzania kryzysowego, które umożliwiają skuteczne reagowanie na pojawiające się zagrożenia.

Współczesne państwa, aby skutecznie przeciwdziałać nowym formom zagrożeń, powinny rozwijać zarówno zdolności technologiczne i organizacyjne, jak i mechanizmy prawne oraz instytucjonalne, pozwalające na szybkie i adekwatne reagowanie na sytuacje kryzysowe. Tylko takie podejście umożliwia ograniczanie skutków zagrożeń oraz zapewnienie stabilnego i bezpiecznego funkcjonowania państwa i społeczeństwa.

Literatura

1. CERT. (2023). *Raport roczny z działalności CERT Polska*. Pobrane z: https://cert.pl/posts/2024/04/raport-roczny-2023 (dostęp: 17.01.2026).
2. Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. (2023). Cyberspace as a source of new threats to the security of the European Union. *European Research Studies Journal, 26*(3), 782-797.

3. Elak, L., Oskierko, M., Żurawski, S. (2024). Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 10*(1), 81-95.
4. Hajduk, J., Stępniewski, T. (2015). Wojna hybrydowa Rosji z Ukrainą: Uwarunkowania i instrumenty. *Studia Europejskie, 4,* 135-152.
5. Instytut Nowej Europy. (b.d). Wszystko *jest wojną. Rosyjskie działania hybrydowe wobec państw Trójmorza*. Pobrane z: https://ine.org.pl/wszystko-jest-wojna-rosyjskie-dzialania-hybrydowe-wobec-panstw-trojmorza (dostęp: 17.01.2026).
6. Kamionka, M. (2023). Rosyjska wojna hybrydowa w mediach społecznościowych na przykładzie portalu Facebook. *Wiedza Obronna*, *82*(1), 63-76.
7. Kłaczyński, R. (2019). Rosyjsko-ukraiński konflikt 2014-2017 jako przykład wojny hybrydowej. Geneza, Polityka, Gospodarka. *Rocznik Bezpieczeństwa Międzynarodowego, 11*(2), 78-90.
8. Microsoft. (b.d.). *Co to jest cyberatak?* Pobrane z: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-cyberattack (dostęp: 17.01.2026).
9. Makeittogether. (b.d.). *Raport Sophos: Chińskie grupy hakerskie eskalują, ataki na urządzenia brzegowe*. Pobrane z: https://makeittogether.pl/raport-sophos-chinskie-grupy-hakerskie-eskaluja-ataki-na-urzadzenia-brzegowe (dostęp: 17.01.2026).
10. Oskierko, M., Nasiadka, A., Ochyra-Żurawska, K. (2025). Wojska Obrony Terytorialnej w ochronie granicy państwowej w warunkach wojny hybrydowej. *Prawo i Bezpieczeństwo, 2*(5), 98-110.
11. Pasławski, K., CRN. (b.d.). *Ponad 1800 cyberataków tygodniowo na polskie firmy.* Pobrane z: https://crn.pl/aktualnosci/ponad-1800-atakow-tygodniowo-na-polskie-firmy/ (dostęp: 17.01.2026).
12. Rodak, W. (2016). *Leśna, Łowcza i Stołpce. Wojna hybrydowa na kresach II RP. Zielone ludziki 1.0*. Pobrane z: https://naszahistoria.pl/lesna-lowcza-i-stolpce-wojna-hybrydowa-na-kresach-ii-rp-sowieckie-zielone-ludziki-10/ar/c1-9813528#google_vignette (dostęp: 17.01.2026).
13. Sykulski, L. (2015). Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera. *Przegląd Geopolityczny, 11,* 103-112.

14. Słownik PWN. (b.d.). *Cyberatak*. Wydawnictwo Naukowe PWN. Pobrane z: https://sjp.pwn.pl/sjp/cyberatak,5606168.html#google_vignette (dostęp: 17.01.2026).
15. Trendmicro. (b.d.). *15 najczęstrzych rodzajów cyberataków*. Pobrane z: https://www.trendmicro.com/pl_pl/what-is/cyber-attack/types-of-cyber-attacks.html (dostęp: 17.01.2026).
16. Trofymowych, V. (2016). Wojna hybrydowa jako instrument kluczowy rosyjskiej geostrategii rewanżu. *Ante Portas – Studia nad Bezpieczeństwem*, *1*(6), 175-186.
17. Żurawski, S., Oskierko, M. (2025). Unia Europejska wobec kryzysu migracyjnego jako narzędzia wojny hybrydowej. *De Securitate Et Defensione. O Bezpieczeństwie i Obronności*, *11*(1), 51-67.

Jakub Bieniek[1]
Akademia Sztuki Wojennej w Warszawie
Sławomir Żurawski[2]
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Marcin Oskierko[3]
Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103373_4

SYSTEM ZARZĄDZANIA KRYZYSOWEGO NATO W ARCHITEKTURZE WSPÓŁCZESNEGO BEZPIECZEŃSTWA MIĘDZYNARODOWEGO

NATO'S CRISIS MANAGEMENT SYSTEM WITHIN THE FRAMEWORK OF CONTEMPORARY INTERNATIONAL SECURITY

Streszczenie

Celem rozdziału jest analiza systemu zarządzania kryzysowego Organizacji Traktatu Północnoatlantyckiego oraz ocena jego znaczenia dla współczesnej architektury bezpieczeństwa międzynarodowego. Problem badawczy sformułowano: w jakim stopniu system zarządzania kryzysowego NATO stanowi skuteczny instrument

[1] https://orcid.org/0000-0003-2206-1667, e-mail: j.bieniek@akademia.mil.pl
[2] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl
[3] https://orcid.org/0000-0003-3450-6037, e-mail: moskierko@panschelm.edu.pl

reagowania na współczesne zagrożenia bezpieczeństwa oraz jakie mechanizmy decydują o jego efektywności? Przyjęto hipotezę, że system zarządzania kryzysowego NATO jest jednym z kluczowych narzędzi reagowania na współczesne zagrożenia, ponieważ umożliwia integrację działań politycznych, wojskowych i cywilnych oraz zapewnia zdolność adaptacji Sojuszu do zmieniającego się środowiska bezpieczeństwa. W procesie badawczym zastosowano metody właściwe dla nauk o bezpieczeństwie, w szczególności analizę literatury przedmiotu, analizę instytucjonalno-prawną dokumentów NATO, metodę systemową oraz elementy studium przypadku odnoszące się do wybranych operacji reagowania kryzysowego. Przeprowadzona analiza wskazuje, że rozwój zdolności reagowania kryzysowego NATO stanowi odpowiedź na rosnącą złożoność zagrożeń, takich jak konflikty regionalne, zagrożenia hybrydowe, kryzysy humanitarne czy agresja państwowa, a zarządzanie kryzysowe pozostaje jednym z podstawowych mechanizmów kształtowania bezpieczeństwa międzynarodowego i stabilności w obszarze euroatlantyckim.

Słowa kluczowe: zarządzanie kryzysowe NATO, bezpieczeństwo międzynarodowe, operacje reagowania kryzysowego, współpraca cywilno-wojskowa, bezpieczeństwo euroatlantyckie, organizacje międzynarodowe

Abstract

The aim of the chapter is to analyse the crisis management system of the North Atlantic Treaty Organisation and assess its importance for the contemporary international security architecture. The research problem was formulated: to what extent is the NATO crisis management system an effective instrument for responding to contemporary security threats, and what mechanisms determine its effectiveness? It is hypothesised that NATO's crisis management system is a key tool for responding to today's threats, as it enables the integration of political, military, and civilian activities and ensures the Alliance's ability to adapt to a changing security environment. The research process used methods specific to security sciences, in particular, the analysis of the literature on the subject, the institutional and legal analysis of NATO documents, the systemic method and the elements of the case study relating to selected crisis response operations. The analysis indicates that NATO's development of crisis response capabilities is a response to the growing complexity of threats such as regional conflicts, hybrid threats, humanitarian crises, and state aggression, and that crisis management remains one of the basic mechanisms for shaping international security and stability in the Euro-Atlantic area. Keywords: NATO crisis management, international security, crisis response operations, civil-military cooperation, Euro-Atlantic security, international organisations.

Keywords: NATO crisis management, international security, crisis response operations, civil-military cooperation, Euro-Atlantic security, international organisations

Wstęp

Współczesne środowisko bezpieczeństwa międzynarodowego charakteryzuje się rosnącą złożonością oraz dynamiką zagrożeń o charakterze asymetrycznym, hybrydowym i transgranicznym. Konflikty zbrojne, terroryzm, kryzysy humanitarne, katastrofy naturalne oraz zagrożenia cybernetyczne powodują, że zarządzanie kryzysowe staje się jednym z kluczowych elementów funkcjonowania systemu bezpieczeństwa międzynarodowego. Szczególną rolę w tym zakresie odgrywa Organizacja Traktatu Północnoatlantyckiego (NATO), która – obok realizacji funkcji obrony zbiorowej – rozwija zdolności reagowania kryzysowego w wymiarze politycznym, wojskowym i cywilnym.

Celem rozdziału jest analiza systemu zarządzania kryzysowego NATO w ujęciu instytucjonalnym i funkcjonalnym oraz ocena jego znaczenia dla współczesnej architektury bezpieczeństwa międzynarodowego. W rozdziale przyjęto hipotezę badawczą, zgodnie z którą system zarządzania kryzysowego NATO stanowi kluczowy instrument reagowania na współczesne zagrożenia bezpieczeństwa, umożliwiający integrację działań politycznych, wojskowych i cywilnych państw członkowskich Sojuszu.

W procesie badawczym zastosowano metody właściwe dla nauk o bezpieczeństwie i stosunkach międzynarodowych, w szczególności analizę instytucjonalno-prawną dokumentów NATO, analizę literatury przedmiotu, metodę systemową oraz elementy studium przypadku odnoszące się do wybranych operacji reagowania kryzysowego.

NATO jako organizacja bezpieczeństwa zbiorowego – wprowadzenie teoretyczne

Organizacja Traktatu Północnoatlantyckiego (NATO) stanowi jeden z najważniejszych elementów współczesnego systemu bezpieczeństwa międzynarodowego. Powstała w 1949 roku jako sojusz obronny państw euroatlantyckich, którego podstawowym celem jest zapewnienie bezpieczeństwa zbiorowego jego członków poprzez współpracę polityczną i wojskową. Fundamentem funkcjonowania Sojuszu pozostaje Traktat Północnoatlantycki, w szczególności zasada kolektywnej obrony wyrażona w art. 5 oraz mechanizm konsultacji politycznych określony w art. 4 (Traktat Północnoatlantycki, 2000). Początkowym celem NATO była ochrona państw sygnatariuszy

Traktatu Waszyngtońskiego oraz zapewnienie ich bezpieczeństwa militarnego w warunkach rywalizacji blokowej okresu zimnej wojny, zwłaszcza w kontekście zagrożenia ze strony Związku Radzieckiego i państw pozostających w jego strefie wpływów. Jednocześnie Traktat Północnoatlantycki wskazywał na konieczność rozwijania zdolności obronnych państw członkowskich. Zgodnie z art. 3 Traktatu, strony zobowiązały się do utrzymywania i rozwijania indywidualnej oraz zbiorowej zdolności do odparcia zbrojnej napaści poprzez stałą i skuteczną samopomoc oraz pomoc wzajemną (Czaplińska, 2021).

Po zakończeniu zimnej wojny rola NATO uległa znaczącej ewolucji. Sojusz przekształcił się z organizacji skoncentrowanej przede wszystkim na obronie terytorialnej w podmiot zdolny do reagowania na zróżnicowane zagrożenia bezpieczeństwa międzynarodowego, w tym konflikty regionalne, terroryzm, zagrożenia hybrydowe oraz kryzysy humanitarne. Rozszerzenie Sojuszu o nowe państwa członkowskie oraz rozwój współpracy partnerskiej spowodowały również wzrost znaczenia działań stabilizacyjnych, konsultacyjnych i wspierających rozwój zdolności obronnych państw członkowskich oraz partnerów NATO (NATO, 2022a). Taki układ zasadniczych zadań NATO odpowiada sojuszniczym ocenom zmieniającego się środowiska strategicznego oraz umożliwia elastyczne reagowanie na pojawiające się zagrożenia. Pozwala on państwom członkowskim na podejmowanie decyzji dotyczących zaangażowania Sojuszu w sposób dostosowany do charakteru konkretnego kryzysu, bez automatyzmu działania, a jednocześnie w oparciu o mechanizm konsultacji i wspólnego uzgadniania stanowiska (Kupiecki, 2000).

Współczesna doktryna NATO wskazuje trzy podstawowe zadania Sojuszu:

- odstraszanie i obronę,
- zapobieganie kryzysom i zarządzanie nimi,
- bezpieczeństwo kooperatywne (NATO, 2022a).

Realizacja tych zadań opiera się na połączeniu instrumentów politycznych i wojskowych oraz współpracy z partnerami międzynarodowymi, co pozwala NATO funkcjonować jako kluczowy mechanizm stabilizacyjny w środowisku bezpieczeństwa charakteryzującym się rosnącą niepewnością i dynamiką zagrożeń (NATO, 2022a). W tym kontekście szczególne znaczenie ma rozwinięty przez Sojusz system zarządzania kryzysowego, stanowiący jeden z podstawowych obszarów jego działalności operacyjnej.

Istota zarządzania kryzysowego w NATO

Zarządzanie kryzysowe NATO stanowi istotny element architektury bezpieczeństwa euroatlantyckiego, umożliwiający reagowanie na sytuacje zagrożenia zarówno w wymiarze militarnym, jak i stabilizacyjnym oraz humanitarnym. Ewolucja funkcji Sojuszu po zakończeniu zimnej wojny doprowadziła do rozszerzenia zakresu jego aktywności o operacje reagowania kryzysowego prowadzone poza terytorium państw członkowskich, a także do rozwoju mechanizmów współpracy cywilno-wojskowej i planowania strategicznego.

Współczesne rozumienie zarządzania kryzysowego w NATO obejmuje działania podejmowane przed wystąpieniem kryzysu, w jego trakcie oraz po jego zakończeniu. Oznacza to integrację instrumentów politycznych, wojskowych i cywilnych w celu zapobiegania konfliktom, reagowania na zagrożenia oraz stabilizacji sytuacji pokryzysowej. Szczególnego znaczenia nabrało to w kontekście doświadczeń operacji stabilizacyjnych NATO oraz współczesnych zagrożeń dla bezpieczeństwa europejskiego, w tym agresji Federacji Rosyjskiej na Ukrainę.

W tym ujęciu zarządzanie kryzysowe NATO należy traktować jako proces ciągły i wielowymiarowy, obejmujący zarówno działania prewencyjne, planowanie operacyjne, prowadzenie operacji reagowania kryzysowego, jak i działania stabilizacyjne oraz odbudowę zdolności bezpieczeństwa państw dotkniętych konfliktem lub kryzysem.

Zarządzanie kryzysowe w NATO obejmuje działania podejmowane w sytuacjach zagrożenia dla bezpieczeństwa państw członkowskich oraz dla stabilności międzynarodowej, zarówno na obszarze traktatowym, jak i poza nim. Mechanizmy te wynikają z charakteru Sojuszu jako organizacji polityczno-wojskowej odpowiedzialnej za utrzymanie bezpieczeństwa w obszarze euroatlantyckim oraz za reagowanie na kryzysy o charakterze międzynarodowym. Zarządzanie kryzysowe obejmuje działania realizowane przed wystąpieniem kryzysu, w jego trakcie oraz po jego zakończeniu, w tym operacje stabilizacyjne, pomoc humanitarną oraz współpracę z instytucjami krajowymi i międzynarodowymi (Kwiecińska, Żurawski, 2023).

Zgodnie ze słownikiem terminów i definicji NATO AAP-6, zarządzanie kryzysowe oznacza skoordynowane działania podejmowane w celu rozładowania napięcia kryzysowego, zapobieżenia jego eskalacji do konfliktu

zbrojnego oraz powstrzymania wrogich działań. Definicja ta wskazuje na kompleksowy charakter reagowania kryzysowego, obejmujący działania prewencyjne, stabilizacyjne i operacyjne, realizowane przy wykorzystaniu instrumentów politycznych i wojskowych (NATO, 2014). Problematykę tę rozwija doktryna AJP-01 Allied Joint Doctrine, która określa strategiczny kontekst operacji Sojuszu. Dokument ten podkreśla, że NATO posiada zdolność działania w całym kontinuum bezpieczeństwa, od zapobiegania kryzysom, poprzez ich zarządzanie, aż po operacje prowadzone w warunkach konfliktu zbrojnego. Zdolności te mogą być wykorzystywane zarówno na obszarze euroatlantyckim, jak i poza nim, w zależności od charakteru zagrożenia oraz decyzji politycznych państw członkowskich podejmowanych na zasadzie konsensusu (NATO, 2022a).

Zarządzanie kryzysowe NATO obejmuje zarówno działania wynikające z art. 5 Traktatu Waszyngtońskiego (obrona kolektywna), jak i operacje reagowania kryzysowego prowadzone poza mechanizmem kolektywnej obrony (non-Article 5 crisis response operations). Doktryna NATO wskazuje, że Sojusz dysponuje zdolnością prowadzenia szerokiego spektrum działań reagowania kryzysowego – od operacji bojowych, poprzez operacje stabilizacyjne i pokojowe, aż po działania związane z pomocą humanitarną i reagowaniem na katastrofy naturalne lub technologiczne.

Kluczowym elementem zarządzania kryzysowego NATO jest koordynacja instrumentów politycznych, wojskowych i cywilnych, realizowana zgodnie z koncepcją Comprehensive Approach. Podejście to zakłada współpracę z partnerami międzynarodowymi, w szczególności z ONZ, Unią Europejską oraz organizacjami regionalnymi, w celu zapewnienia spójności działań politycznych, wojskowych i humanitarnych.

Istotnym elementem systemu zarządzania kryzysowego NATO jest również mechanizm konsultacji sojuszniczych wynikający z art. 4 Traktatu Waszyngtońskiego, umożliwiający wczesną identyfikację zagrożeń oraz uzgodnienie wspólnych działań politycznych i wojskowych (NATO, 2022b).

Istotną cechą zarządzania kryzysowego NATO jest jego ciągłość czasowa, obejmująca:

- zapobieganie kryzysom,
- reagowanie na kryzys,
- działania stabilizacyjne i odbudowę po konflikcie.

Podejście to wynika z przyjętej przez NATO koncepcji reagowania w całym kontinuum bezpieczeństwa, od zapobiegania konfliktom po operacje wojskowe (NATO, 2022b).

Operacje zarządzania kryzysowego NATO obejmują w szczególności:

- operacje reagowania kryzysowego nieobjęte art. 5, prowadzone na podstawie mandatu organizacji międzynarodowych lub na zaproszenie państwa dotkniętego kryzysem,
- operacje pomocy w przypadku katastrof naturalnych, humanitarnych lub spowodowanych przez człowieka, w tym pandemii oraz incydentów CBRN.

Tak rozumiane zarządzanie kryzysowe stanowi zintegrowany proces obejmujący działania polityczne, cywilne i wojskowe realizowane od fazy zapobiegania kryzysom, poprzez reagowanie, aż po stabilizację pokonfliktową, będący jednym z podstawowych mechanizmów realizacji zadań NATO w zmieniającym się środowisku bezpieczeństwa.

Struktura instytucjonalna zarządzania kryzysowego NATO

Struktura instytucjonalna zarządzania kryzysowego NATO opiera się na powiązaniu poziomów politycznych, wojskowych i administracyjnych, co pozwala Sojuszowi na przygotowanie decyzji, ich autoryzację oraz wdrożenie w formie działań operacyjnych. System ten odzwierciedla międzyrządowy charakter NATO: decyzje o zaangażowaniu podejmowane są przez państwa członkowskie wspólnie, w drodze konsensusu, a następnie przekładane na rozwiązania planistyczne i wykonawcze w strukturze wojskowej.

Centralnym organem politycznego kierowania NATO oraz kluczowym elementem systemu zarządzania kryzysowego jest Rada Północnoatlantycka (North Atlantic Council, NAC). Jest to jedyny organ NATO ustanowiony bezpośrednio przez Traktat Północnoatlantycki (art. 9) (Traktat Północnoatlantycki, 2000), co nadaje mu szczególną legitymizację instytucjonalną oraz pozycję najwyższej władzy decyzyjnej w strukturze organizacyjnej Sojuszu. NAC pełni funkcję forum konsultacji politycznych państw członkowskich w sprawach bezpieczeństwa międzynarodowego i kierunków działania NATO. W sytuacjach kryzysowych Rada nadzoruje proces podejmowania decyzji dotyczących użycia instrumentów politycznych i wojskowych, inicjuje konsultacje sojusznicze na podstawie art. 4 Traktatu

Północnoatlantyckiego oraz autoryzuje operacje reagowania kryzysowego. Podejmowanie decyzji w formule jednomyślności i konsensusu zapewnia polityczną legitymizację działań Sojuszu, choć jednocześnie determinuje dynamikę procesu decyzyjnego, wymagając uzgodnienia stanowisk wszystkich członków (NATO, 2024).

Z politycznym poziomem decyzji sprzężony jest wojskowy poziom doradczy. Komitet Wojskowy NATO (Military Committee, MC) stanowi najwyższy organ wojskowy Sojuszu (Żurawski vel Grajewski, 2012; NATO, 2026e) i pełni funkcję łącznika między NAC a strukturą dowodzenia. W systemie zarządzania kryzysowego MC odpowiada za formułowanie wojskowych ocen sytuacji bezpieczeństwa, opracowywanie rekomendacji wariantów działania oraz nadzorowanie planowania operacyjnego realizowanego przez dowództwa strategiczne NATO. Rola Komitetu Wojskowego odzwierciedla mechanizm cywilnej kontroli nad użyciem sił zbrojnych: decyzje o uruchomieniu operacji pozostają w gestii NAC, natomiast MC zapewnia wojskowy „transfer" decyzji politycznych do poziomu planowania i prowadzenia operacji, a także nadzór nad realizacją przyjętych rozstrzygnięć (NATO, 2024, 2026d). Uzupełnieniem poziomu decyzyjnego NAC i MC jest rozbudowany system komitetów NATO, który stanowi podstawową infrastrukturę konsultacyjną i przygotowawczą Sojuszu. Komitety tworzą instytucjonalne ramy wymiany informacji, uzgadniania stanowisk oraz opracowywania rekomendacji i projektów decyzji w obszarach politycznych, strategicznych, operacyjnych i technicznych. W pracach komitetów uczestniczą przedstawiciele wszystkich państw członkowskich, a zasada konsensusu ma zastosowanie na wszystkich poziomach struktury, co wzmacnia spójność procesu decyzyjnego oraz utrzymuje jego międzyrządowy charakter. Na szczycie systemu komitetowego, obok NAC i MC, funkcjonuje także Grupa Planowania Jądrowego (Nuclear Planning Group, NPG), której zakres kompetencji dotyczy polityki nuklearnej i procedur konsultacyjnych w tej dziedzinie. Sieć komitetów podporządkowanych organom nadrzędnym pełni w tym układzie rolę „mechanizmu produkcji decyzji": przygotowuje analizy i warianty rozwiązań, które następnie mogą zostać zatwierdzone na poziomie politycznym (NATO, 2024).

Sprawność tego systemu zależy od zaplecza analityczno-administracyjnego. Sztab Międzynarodowy NATO (International Staff, IS) stanowi

cywilną strukturę doradczą i administracyjną wspierającą proces decyzyjny Sojuszu, w szczególności działalność Rady Północnoatlantyckiej. Do jego podstawowych zadań należy przygotowywanie materiałów analitycznych, dokumentów strategicznych i rekomendacji, a także koordynacja wdrażania decyzji podejmowanych na różnych szczeblach struktury komitetowej. IS zapewnia ciągłość konsultacji i prac decyzyjnych w Kwaterze Głównej NATO w Brukseli oraz współpracuje z Międzynarodowym Sztabem Wojskowym (International Military Staff, IMS), który stanowi zaplecze wykonawcze Komitetu Wojskowego. Taka konfiguracja wzmacnia integrację wymiaru cywilnego i wojskowego w zarządzaniu kryzysowym, minimalizując ryzyko rozbieżności między decyzją polityczną, planowaniem wojskowym a koordynacją wdrożenia (NATO, 2026a).

Poziom wykonawczy zarządzania kryzysowego stanowi zintegrowaną strukturę dowodzenia NATO (NATO Command Structure, NCS). Na jej czele stoją dwa dowództwa strategiczne: Allied Command Operations (ACO) oraz Allied Command Transformation (ACT) (Żurawski vel Grajewski, 2012; NATO, 2026c). ACO, z siedzibą w Supreme Headquarters Allied Powers Europe (SHAPE) w Mons, odpowiada za planowanie i prowadzenie wszystkich operacji wojskowych NATO. Dowództwem kieruje Naczelny Dowódca Sojuszniczy w Europie (Supreme Allied Commander Europe, SACEUR), który realizuje zadania na poziomie strategicznym pod nadzorem Komitetu Wojskowego oraz w ramach politycznej kontroli NAC. Struktura ACO obejmuje trzy poziomy dowodzenia – strategiczny, operacyjny i taktyczny – umożliwiając dowodzenie siłami połączonymi i wielonarodowymi. Na poziomie operacyjnym funkcjonują dowództwa połączone (Joint Force Commands) w Brunssum, Neapolu i Norfolk, natomiast na poziomie taktycznym działają dowództwa komponentów: lądowego (LANDCOM w Izmirze), morskiego (MARCOM w Northwood) oraz powietrznego (AIRCOM w Ramstein). Układ ten wspiera elastyczne reagowanie na zagrożenia i prowadzenie operacji wielodomenowych (NATO, 2026c).

Drugim strategicznym dowództwem jest ACT z siedzibą w Norfolk, kierowane przez Naczelnego Dowódcę ds. Transformacji (Supreme Allied Commander Transformation, SACT). ACT odpowiada za rozwój zdolności wojskowych NATO, transformację struktur dowodzenia, rozwój doktryn, szkolenie oraz interoperacyjność sił zbrojnych państw członkowskich.

W praktyce ACO koncentruje się na prowadzeniu bieżących operacji, natomiast ACT zapewnia zdolność adaptacji Sojuszu do zmian środowiska bezpieczeństwa, wzmacniając przygotowanie NATO do przyszłych kryzysów (NATO, 2026c).

W konsekwencji instytucjonalny model zarządzania kryzysowego NATO można przedstawić jako sekwencyjny proces obejmujący: konsultacje i decyzję polityczną podejmowaną przez Radę Północnoatlantycką (NAC), wojskową ocenę sytuacji i rekomendacje przygotowywane przez Komitet Wojskowy oraz Międzynarodowy Sztab Wojskowy (MC/IMS), przygotowanie i koordynację implementacji decyzji w ramach systemu komitetów i Sztabu Międzynarodowego (IS), a następnie planowanie i prowadzenie operacji przez Allied Command Operations (ACO). Proces ten jest uzupełniany przez działalność Allied Command Transformation (ACT), odpowiedzialnego za rozwój zdolności, interoperacyjność i adaptację Sojuszu do zmieniającego się środowiska bezpieczeństwa. Tak ukształtowana architektura instytucjonalna stanowi fundament spójności strategicznej NATO oraz umożliwia efektywne łączenie instrumentów politycznych i wojskowych w reagowaniu na sytuacje kryzysowe.

NATO Crisis Management Process jako model reagowania kryzysowego Sojuszu

W najnowszym ujęciu koncepcyjnym NATO Crisis Management Process przedstawiany jest jako czterofazowy cykl reagowania kryzysowego, obejmujący:

- ocenę sytuacji i ostrzeganie (Assessment and Warning),
- konsultacje i decyzję polityczną (Consultation and Decision),
- planowanie i koordynację działań (Planning and Coordination),
- realizację oraz analizę doświadczeń (Implementation and Follow-up) (Antonova, Antonov, 2025).

Model ten stanowi syntetyczne ujęcie procedur reagowania kryzysowego NATO i odpowiada bardziej szczegółowemu, sześciostopniowemu procesowi zarządzania kryzysowego stosowanemu w planowaniu operacyjnym Sojuszu.

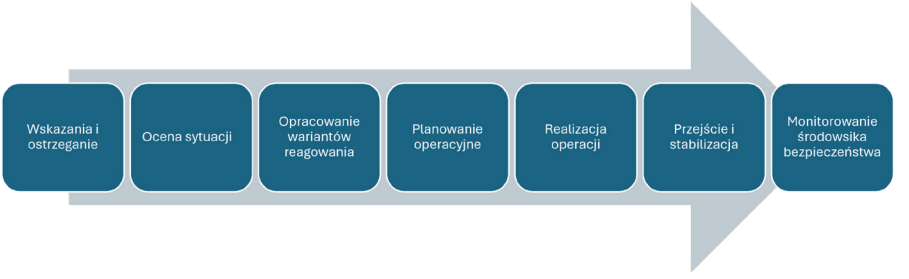
Instytucjonalna struktura NATO, obejmująca Radę Północnoatlantycką, Komitet Wojskowy, Sztab Międzynarodowy oraz zintegrowaną

strukturę dowodzenia wojskowego, znajduje swoje operacyjne odzwierciedlenie w sformalizowanym mechanizmie reagowania kryzysowego Sojuszu, określanym jako NATO Crisis Management Process (NCMP). Proces ten integruje polityczne podejmowanie decyzji z planowaniem operacyjnym i prowadzeniem działań wojskowych oraz cywilnych, zapewniając spójność reagowania NATO w sytuacjach kryzysowych.

NCMP obejmuje sześć kolejnych etapów zarządzania kryzysowego:

1. Wskazania i ostrzeganie (Indications and Warning),
2. Ocena sytuacji (Assessment),
3. Opracowanie wariantów reagowania (Response Options Development),
4. Planowanie operacyjne (Planning),
5. Realizacja operacji (Execution),
6. Przejście i stabilizacja (Transition) (North Atlantic Treaty Organisation).

Proces rozpoczyna się od etapu wskazań i ostrzegania, obejmującego monitorowanie środowiska bezpieczeństwa oraz identyfikację potencjalnych zagrożeń. Następnie realizowane jest ocena sytuacji oraz opracowanie wariantów reagowania, które tworzą podstawę polityczno-wojskowego procesu decyzyjnego NATO. Kolejnym etapem jest planowanie operacyjne prowadzone przez Allied Command Operations pod kierownictwem Naczelnego Dowódcy Sojuszniczego w Europie (SACEUR). Po zatwierdzeniu planów operacyjnych przez Radę Północnoatlantycką rozpoczyna się faza realizacji operacji. Ostatni etap obejmuje działania stabilizacyjne oraz stopniowe przekazywanie odpowiedzialności władzom lokalnym lub organizacjom międzynarodowym. Schemat procesu NATO Crisis Management Process przedstawiono na Rysunku 1.



Rysunek 1. NATO Crisis Management Process (NCMP) jako cykl reagowania kryzysowego Sojuszu

Źródło: opracowanie własne na podstawie NATO, 2022a, 2026d.

Schemat ukazuje zarządzanie kryzysowe NATO jako proces cykliczny, w którym monitorowanie środowiska bezpieczeństwa prowadzi do identyfikacji zagrożeń, a następnie do podejmowania decyzji politycznych, planowania operacyjnego i realizacji działań przez strukturę dowodzenia NATO. Etapy oceny sytuacji oraz opracowania wariantów reagowania stanowią kluczowy element integrujący wymiar polityczny i wojskowy procesu decyzyjnego Sojuszu.

Planowanie operacyjne, realizowane przez Allied Command Operations, umożliwia przekształcenie decyzji politycznych w konkretne działania wojskowe lub stabilizacyjne. Z kolei etap przejścia i stabilizacji ma na celu przywrócenie trwałego bezpieczeństwa oraz przekazanie odpowiedzialności władzom lokalnym lub partnerom międzynarodowym. W praktyce poszczególne etapy NCMP nie mają charakteru ściśle sekwencyjnego i mogą się częściowo pokrywać, co wynika ze złożoności współczesnych kryzysów bezpieczeństwa. Mechanizm ten zapewnia jednak spójność procesu decyzyjnego NATO oraz umożliwia skuteczne powiązanie decyzji politycznych z planowaniem i prowadzeniem operacji wojskowych. W konsekwencji NATO Crisis Management Process stanowi operacyjne rozwinięcie instytucjonalnego modelu zarządzania kryzysowego Sojuszu, umożliwiając reagowanie na kryzysy w całym kontinuum bezpieczeństwa – od zapobiegania konfliktom po działania stabilizacyjne po ich zakończeniu.

Zapobieganie kryzysom i zarządzanie kryzysowe NATO: ewolucja podejścia oraz doświadczenia operacyjne po zimnej wojnie

Zapobieganie kryzysom oraz zarządzanie kryzysowe stanowią jeden z kluczowych obszarów aktywności NATO, obok obrony zbiorowej i bezpieczeństwa kooperatywnego. Po zakończeniu zimnej wojny zakres działań Sojuszu rozszerzył się o operacje reagowania kryzysowego prowadzone poza obszarem traktatowym, co doprowadziło do wykształcenia kompleksowego modelu reagowania obejmującego działania dyplomatyczne, wojskowe i stabilizacyjne. Charakter reakcji NATO pozostaje uzależniony od skali i dynamiki kryzysu oraz jego konsekwencji dla bezpieczeństwa międzynarodowego.

Fundamentem reagowania NATO na bezpośrednie zagrożenia dla bezpieczeństwa państw członkowskich pozostaje art. 5 Traktatu Północnoatlantyckiego, ustanawiający zasadę obrony zbiorowej. Jednorazowe uruchomienie tej klauzuli po zamachach z 11 września 2001 r. potwierdziło jej adaptacyjny charakter oraz zdolność Sojuszu do reagowania na zagrożenia asymetryczne. Równolegle do logiki obrony zbiorowej zasadniczego znaczenia nabrały operacje reagowania kryzysowego prowadzone poza scenariuszami art. 5. Obejmują one szerokie spektrum działań – od zapobiegania konfliktom i utrzymania pokoju, przez stabilizację i budowanie pokoju, po działania humanitarne i egzekwowanie mandatu międzynarodowego. Wymiar cywilny zarządzania kryzysowego NATO wzmacnia instytucjonalizację mechanizmów koordynacyjnych, w tym Euro-Atlantic Disaster Response Coordination Centre (EADRCC), który pełni funkcję podstawowego narzędzia synchronizowania pomocy państw członkowskich i partnerskich w sytuacjach katastrof naturalnych, kryzysów humanitarnych i zdarzeń masowych (Jacuch, 2019).

Przełomowym doświadczeniem dla operacyjnego wymiaru zarządzania kryzysowego NATO były konflikty na Bałkanach w latach dziewięćdziesiątych. W tym kontekście szczególne znaczenie miała operacja Allied Force (1999), będąca reakcją NATO na eskalację konfliktu w Kosowie oraz narastający kryzys humanitarny. Po wyczerpaniu możliwości rozwiązania konfliktu na drodze dyplomatycznej NATO rozpoczęło 24 marca 1999 r. kampanię powietrzną przeciwko Federalnej Republice Jugosławii. Operacja trwała 78 dni i doprowadziła do wycofania sił jugosłowiańskich z Kosowa oraz ustanowienia międzynarodowej obecności stabilizacyjnej, w tym sił KFOR (Marszałek, 2020). Odmienny charakter miały operacje stabilizacyjne NATO w Macedonii Północnej (2001-2003), realizowane na wniosek władz państwa w warunkach napięć wewnętrznych. Sekwencja operacji Essential Harvest, Amber Fox i Allied Harmony ilustruje model reagowania, w którym instrument wojskowy służy implementacji porozumienia politycznego oraz wsparciu reform sektora bezpieczeństwa (Przybylska-Maszner, 2010).

Najbardziej złożoną operacją stabilizacyjną NATO była misja ISAF w Afganistanie (2001-2014), prowadzona na podstawie mandatu Rady Bezpieczeństwa ONZ. Z perspektywy zarządzania kryzysowego kluczowa była ewolucja jej celów – od stabilizacji bezpieczeństwa po budowę zdolności

afgańskich sił bezpieczeństwa i stopniowy transfer odpowiedzialności (Miler, 2013). Do doświadczeń NATO w zakresie reagowania kryzysowego należą również operacje antypirackie w rejonie Rogu Afryki (2008-2016) (Miler, 2013) oraz działania humanitarne, w tym operacja pomocowa po trzęsieniu ziemi w Pakistanie w latach 2005-2006 (NATO, 2026c).

Współczesny wymiar zarządzania kryzysowego NATO szczególnie wyraźnie ujawnia się w systemowym wsparciu Ukrainy po rozpoczęciu pełnoskalowej agresji Federacji Rosyjskiej. Decyzje podjęte na szczycie NATO w Waszyngtonie w 2024 r. doprowadziły do utworzenia mechanizmów koordynacji pomocy wojskowej i szkoleniowej (NSATU) oraz długoterminowych zobowiązań wsparcia.

Analiza instytucjonalnych podstaw oraz doświadczeń operacyjnych NATO wskazuje, że zarządzanie kryzysowe stało się jednym z centralnych instrumentów realizacji bezpieczeństwa zbiorowego w warunkach postzimnowojennego środowiska strategicznego. Ewolucja Sojuszu – od organizacji skoncentrowanej na odstraszaniu i obronie terytorialnej do podmiotu zdolnego do prowadzenia wielowymiarowych operacji reagowania kryzysowego – odzwierciedla zmiany charakteru zagrożeń oraz rosnącą współzależność bezpieczeństwa międzynarodowego.

Doświadczenia operacyjne NATO potwierdzają znaczenie integracji instrumentów politycznych, wojskowych i cywilnych w reagowaniu na współczesne kryzysy bezpieczeństwa. Współczesne zagrożenia, w tym konflikty hybrydowe, agresja państwowa, terroryzm, zagrożenia cybernetyczne czy katastrofy humanitarne, wymagają dalszej adaptacji modelu zarządzania kryzysowego Sojuszu. Przykład wsparcia Ukrainy pokazuje, że rośnie znaczenie instrumentów instytucjonalnych, koordynacyjnych i szkoleniowych, które uzupełniają tradycyjne operacje wojskowe. Zarządzanie kryzysowe NATO pozostaje zatem kluczowym mechanizmem umożliwiającym Sojuszowi utrzymanie zdolności adaptacyjnych w warunkach zmieniającego się środowiska bezpieczeństwa oraz realizację jego podstawowej funkcji – zapewnienia bezpieczeństwa państw członkowskich i partnerów.

Podsumowanie

Analiza instytucjonalnych i operacyjnych aspektów zarządzania kryzysowego NATO wskazuje, że Sojusz wykształcił wielopoziomowy system

reagowania na zagrożenia bezpieczeństwa międzynarodowego, oparty na współdziałaniu struktur politycznych i wojskowych oraz procedurach planowania operacyjnego. Kluczową rolę w tym systemie odgrywa powiązanie decyzji politycznych podejmowanych przez Radę Północnoatlantycką z procesem wojskowego doradztwa i planowania realizowanego przez Komitet Wojskowy oraz strukturę dowodzenia NATO.

Doświadczenia operacyjne Sojuszu po zakończeniu zimnej wojny potwierdzają rosnące znaczenie operacji reagowania kryzysowego jako jednego z podstawowych narzędzi oddziaływania NATO na środowisko bezpieczeństwa międzynarodowego. Operacje prowadzone na Bałkanach, w Afganistanie, na obszarach morskich zagrożonych piractwem oraz w ramach działań humanitarnych pokazują zdolność NATO do prowadzenia zróżnicowanych działań stabilizacyjnych i wsparcia bezpieczeństwa w środowisku wielonarodowym.

Szczególnie istotnym współczesnym przykładem jest systemowe wsparcie Ukrainy, które wskazuje na rosnące znaczenie instrumentów koordynacyjnych, szkoleniowych i instytucjonalnych w reagowaniu na konflikty o wysokiej intensywności. Doświadczenia te potwierdzają, że zarządzanie kryzysowe NATO pozostaje jednym z kluczowych obszarów funkcjonowania Sojuszu, wzmacniając jego rolę w utrzymaniu stabilności i bezpieczeństwa euroatlantyckiego.

Literatura

1. Antonova, M. L., Antonov, S. I. (2025). NATO's role in a non-military crisis. *Journal Scientific and Applied Research, 29,* 139-147.
2. Czaplińska, K. (2021). Traktat Północnoatlantycki: Powstanie NATO i początki organizacji. W: J. M. Fiszer (red.), *Przeszło 70 lat Sojuszu Północnoatlantyckiego: Geneza, stan obecny i perspektywy* (s. 17-26). Oficyna Wydawnicza Uczelni Łazarskiego.
3. Traktat Północnoatlantycki. (2000). *Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r.* (Dz. U. z 2000 r. Nr 87, poz. 970).
4. Jacuch, A. (2019). Disaster response mechanisms in EU and NATO. *Przegląd Europejski, 53*(3), 67-81.
5. Kupiecki, R. (2000). *NATO u progu XXI wieku*. Wydawnictwo ASKON.

6. Kwiecińska, M., Żurawski, S. (2023). Rola i znaczenie zarządzania kryzysowego NATO dla bezpieczeństwa Polski na przykładzie współpracy NATO-RCB. *International Journal of New Economics and Social Sciences, 7*(2), 171-182.
7. Marszałek, M. (2020). Pokojowe zaangażowanie NATO w Kosowie: Geneza – stan obecny – przyszłość. *Kwartalnik Bellona, 701*(2), 89-104.
8. Miler, A. (2013). Współczesne operacje pokojowe NATO. W: R. Czulda, R. Łoś, J. Regina-Zacharski (red.), *NATO wobec wyzwań współczesnego świata* (s. 185-198). Instytut Badań nad Stosunkami Międzynarodowymi.
9. NATO. (2014). *AAP-6 Słownik terminów i definicji NATO*. Agencja Standaryzacyjna NATO.
10. NATO. (2022a). *NATO 2022 Strategic Concept*, Madrid.
11. NATO. (2022b). *Allied Joint Doctrine AJP-01, Edition F, Version 1*. NATO Standardization Office, Brussels.
12. NATO. (2024). *North Atlantic Council (NAC)*. Pobrane z: https://www.nato.int/en/about-us/organization/nato-structure/north-atlantic-council-nac?selectedLocale= (dostęp: 17.01.2026).
13. NATO. (2026a). *International Staff*. Pobrane z: https://www.nato.int/en/about-us/organization/nato-structure/international-staff?selectedLocale= (dostęp: 17.01.2026).
14. NATO. (2026b). *Allied Command Transformation*. Pobrane z: https://www.nato.int/en/about-us/organization/nato-structure/allied-command-transformation?selectedLocale= (dostęp: 17.01.2026).
15. NATO. (2026c). *Allied Command Operations (ACO)*. Pobrane z: https://www.nato.int/en/about-us/organization/nato-structure/allied-command-operations-aco?selectedLocale= (dostęp: 17.01.2026).
16. NATO. (2026d). *Crisis management*. Pobrane z: https://www.nato.int/en/what-we-do/introduction-to-nato/crisis-management?selectedLocale= (dostęp: 17.01.2026).
17. NATO. (2026e). *Military Committee*, Pobrane z: https://www.nato.int/en/about-us/organization/nato-structure/nato-military-committee/military-committee (dostęp: 17.01.2026).

18. NATO. (2026f). *Committees*. Pobrane z: https://www.nato.int/en/about us/organization/nato structure/committees?selectedLocale= (dostęp: 17.01.2026).
19. Przybylska-Maszner, B. (2010). EUPAT – policyjny zespół doradczy w Byłej Jugosłowiańskiej Republice Macedonii. W: B. Przybylska-Maszner (red.), *Misje cywilne Unii Europejskiej* (s. 241-258). Wydawnictwo Naukowe WNPiD UAM.
20. Żurawski vel Grajewski, P. (2012). *Bezpieczeństwo międzynarodowe. Wymiar militarny*. Wydawnictwo Naukowe PWN.

Marcin Oskierko[1]
Państwowa Akademia Nauk Stosowanych w Chełmie
Sławomir Żurawski[2]
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Marek Giec[3]

https://doi.org/10.29316/9788368103373_5

ROLA ZARZĄDZANIA KRYZYSOWEGO UNII EUROPEJSKIEJ W KSZTAŁTOWANIU BEZPIECZEŃSTWA EUROPEJSKIEGO

THE ROLE OF THE EUROPEAN UNION'S CRISIS MANAGEMENT IN SHAPING EUROPEAN SECURITY

Streszczenie

Celem rozdziału jest analiza instytucji oraz mechanizmów reagowania kryzysowego UE, a także ocena ich znaczenia dla wzmacniania zdolności państw członkowskich do przeciwdziałania sytuacjom kryzysowym. Rozdział podejmuje problem roli zarządzania kryzysowego Unii Europejskiej w systemie bezpieczeństwa europejskiego w kontekście współczesnych zagrożeń o charakterze transgranicznym. Przedstawiono rozwój unijnego systemu reagowania kryzysowego, w tym funkcjonowanie Unijnego Mechanizmu Ochrony Ludności, Centrum Koordynacji

[1] https://orcid.org/0000-0003-3450-6037, e-mail: moskierko@panschelm.edu.pl
[2] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl
[3] https://orcid.org/0009-0006-1061-6740

Reagowania Kryzysowego oraz Zintegrowanego Mechanizmu Reagowania Kryzysowego. Analiza została uzupełniona o przykłady wykorzystania tych instrumentów w sytuacjach kryzysowych ostatnich lat, takich jak pandemia COVID-19, katastrofy naturalne oraz wojna w Ukrainie. Problem badawczy sformułowano: jaką rolę pełni system zarządzania kryzysowego UE w kształtowaniu bezpieczeństwa w Europie? W badaniach zastosowano analizę instytucjonalno-prawną, analizę dokumentów strategicznych Unii Europejskiej, analizę literatury przedmiotu oraz metodę studium przypadku. Wyniki wskazują, że system zarządzania kryzysowego UE stanowi istotny element bezpieczeństwa europejskiego, zwiększając zdolność państw członkowskich do skoordynowanego reagowania na zagrożenia o charakterze ponadnarodowym oraz wzmacniając odporność europejskiej architektury bezpieczeństwa.

Słowa kluczowe: zarządzanie kryzysowe UE, bezpieczeństwo europejskie, Unijny Mechanizm Ochrony Ludności, odporność państw, zagrożenia transgraniczne

Abstract

The article examines the role of the European Union's crisis management system within the broader framework of European security, in the context of contemporary transnational threats. The aim of the study is to analyse the institutions and mechanisms of EU crisis response and to assess their significance for strengthening Member States' ability to respond to crisis situations. The paper discusses the development of the EU crisis response system, including the functioning of the Union Civil Protection Mechanism, the Emergency Response Coordination Centre, and the Integrated Political Crisis Response arrangements. The analysis is complemented by selected case studies of recent crises, including the COVID-19 pandemic, natural disasters, and the war in Ukraine. The research is based on institutional and legal analysis, examination of EU strategic documents, literature review, and the case study method. The findings indicate that the EU crisis management system constitutes an important component of European security, enhancing coordinated response capabilities and strengthening the resilience of the European security architecture.

Keywords: EU crisis management, European security, EU Civil Protection Mechanism, state resilience, cross-border threats

Wstęp

Współczesne środowisko bezpieczeństwa europejskiego charakteryzuje się rosnącą złożonością zagrożeń o charakterze transgranicznym, wielowymiarowym i dynamicznym. Globalizacja procesów społeczno-gospodarczych, rozwój technologiczny, zmiany klimatyczne, migracje, pandemie

oraz konflikty zbrojne powodują, że bezpieczeństwo państw europejskich coraz częściej zależy od zdolności do współpracy międzynarodowej oraz koordynacji działań na poziomie regionalnym. W tym kontekście szczególnego znaczenia nabiera zarządzanie kryzysowe jako element systemu bezpieczeństwa, obejmujący zapobieganie sytuacjom kryzysowym, przygotowanie do nich oraz reagowanie na ich skutki. Unia Europejska, mimo że nie jest klasyczną organizacją bezpieczeństwa zbiorowego, wykształciła w ostatnich dekadach rozbudowany system reagowania kryzysowego, oparty na współpracy państw członkowskich, instytucji unijnych oraz wyspecjalizowanych agencji. Rozwój tego systemu był konsekwencją zarówno ewolucji europejskiej architektury bezpieczeństwa po zakończeniu zimnej wojny, jak i doświadczeń wynikających z kolejnych kryzysów o charakterze ponadnarodowym. Szczególnie istotne znaczenie miały wydarzenia ostatnich lat, takie jak pandemia COVID-19, kryzys migracyjny, katastrofy naturalne oraz wojna w Ukrainie, które ujawniły potrzebę wzmacniania zdolności reagowania kryzysowego na poziomie Unii Europejskiej oraz integracji instrumentów cywilnych, politycznych i technologicznych.

W tym kontekście zasadne staje się podjęcie analizy roli zarządzania kryzysowego Unii Europejskiej w systemie bezpieczeństwa europejskiego. Problem badawczy rozdziału koncentruje się na określeniu znaczenia unijnych mechanizmów reagowania kryzysowego dla zdolności państw członkowskich do przeciwdziałania zagrożeniom o charakterze transgranicznym oraz na ocenie ich wpływu na funkcjonowanie europejskiej architektury bezpieczeństwa. Celem rozdziału jest analiza instytucjonalnych i operacyjnych instrumentów zarządzania kryzysowego UE, identyfikacja ich roli w reagowaniu na współczesne zagrożenia oraz ocena ich znaczenia dla wzmacniania odporności państw członkowskich. Przyjęto hipotezę badawczą, zgodnie z którą system zarządzania kryzysowego Unii Europejskiej stanowi istotny komponent bezpieczeństwa europejskiego, zwiększający zdolność państw członkowskich do reagowania na sytuacje kryzysowe poprzez koordynację działań, mobilizację wspólnych zasobów oraz rozwijanie ponadnarodowych zdolności reagowania. W rozdziale zastosowano analizę instytucjonalno-prawną, analizę dokumentów strategicznych i regulacyjnych Unii Europejskiej, analizę literatury przedmiotu oraz metodę studium przypadku odnoszącą się do wybranych kryzysów współczesnych. Zastosowano również

podejście systemowe, umożliwiające ukazanie zarządzania kryzysowego jako elementu szerszego systemu bezpieczeństwa europejskiego.

Bezpieczeństwo europejskie i rola Unii Europejskiej w reagowaniu kryzysowym

Bezpieczeństwo europejskie stanowi współcześnie złożony system współzależności politycznych, gospodarczych, militarnych i społecznych, w którym kluczową rolę odgrywają organizacje międzynarodowe oraz państwa narodowe. Po zakończeniu zimnej wojny bezpieczeństwo Europy przestało być definiowane wyłącznie w kategoriach militarnych, obejmując również zagrożenia pozamilitarne i nietradycyjne jego komponenty, związane z utrzymaniem pokoju, przeciwdziałaniem terroryzmowi, handlowi narkotykami oraz przestępczości zorganizowanej, ograniczaniem proliferacji broni masowego rażenia, ochroną środowiska naturalnego, a także zapobieganiem konfliktom etnicznym i ich eskalacji (Bryła, 2013). Bezpieczeństwo europejskie można analizować również z perspektywy teorii regionalnych kompleksów bezpieczeństwa (Regional Security Complex Theory), zgodnie z którą współzależność bezpieczeństwa koncentruje się przede wszystkim na poziomie regionalnym. Wynika to z faktu, że większość zagrożeń oddziałuje silniej na państwa geograficznie bliskie, co powoduje powstawanie regionalnych struktur bezpieczeństwa opartych na wzajemnych relacjach współpracy, rywalizacji oraz percepcji zagrożeń. W tym ujęciu Europa stanowi przykład regionu o wysokim stopniu współzależności bezpieczeństwa, w którym działania instytucji międzynarodowych, w tym Unii Europejskiej, wpływają na stabilność i zdolność reagowania państw członkowskich (Buzan, Wæver, 2003). W konsekwencji zarządzanie kryzysowe stało się jednym z podstawowych instrumentów zapewniania stabilności i odporności systemu bezpieczeństwa europejskiego.

Dążenia Unii Europejskiej do wzmacniania bezpieczeństwa w wymiarze zewnętrznym wynikają z kilku kluczowych uwarunkowań. Po pierwsze, związane są z aspiracją UE do umacniania własnej tożsamości oraz zwiększania znaczenia jako podmiotu stosunków międzynarodowych. Po drugie, wynikają z potrzeby rozszerzania procesu integracji europejskiej o obszary bezpieczeństwa i obronności. Po trzecie, stanowią odpowiedź na konieczność zapewnienia bezpieczeństwa poprzez przeciwdziałanie istniejącym

zagrożeniom oraz ograniczanie ryzyka ich wystąpienia w przyszłości (Jagusiak, Moch, 2023). NATO pozostaje strukturą bezpieczeństwa zbiorowego o rozwiniętych zdolnościach operacyjnych i gotowości do działania w wymiarze militarnym. Unia Europejska natomiast, choć nie jest klasyczną organizacją bezpieczeństwa zbiorowego, odgrywa coraz większą rolę w kompleksowym reagowaniu na współczesne zagrożenia. W obliczu dynamicznych zmian środowiska bezpieczeństwa, w tym zagrożeń wynikających z działań Federacji Rosyjskiej, szczególnego znaczenia nabiera komplementarność potencjałów Unii Europejskiej i NATO. Współpraca obu organizacji może obejmować nie tylko uzupełnianie militarnych zdolności NATO pozawojskowymi instrumentami UE, lecz także rozwijanie wspólnych zdolności w obszarach takich jak cyberbezpieczeństwo, przeciwdziałanie dezinformacji, ochrona infrastruktury krytycznej oraz budowanie odporności państw i społeczeństw na zagrożenia hybrydowe. Współdziałanie to wzmacnia europejski system bezpieczeństwa, łącząc potencjał militarny NATO z cywilnymi, gospodarczymi i instytucjonalnymi zasobami Unii Europejskiej (Madej, 2022).

Istotnym elementem tej ewolucji było przyjęcie koncepcji kompleksowego podejścia do bezpieczeństwa (comprehensive approach), zakładającego integrację polityk sektorowych, zdolności reagowania kryzysowego oraz instrumentów finansowych i prawnych. Podejście to znajduje odzwierciedlenie w dokumentach strategicznych UE, takich jak Globalna Strategia UE z 2016 r. (European External Action Service, 2016) oraz Strategiczny Kompas z 2022 r. (Council of the European Union, 2022), które podkreślają znaczenie odporności (resilience) państw członkowskich i społeczeństw europejskich Odporność ta rozumiana jest jako zdolność do zapobiegania kryzysom, przygotowania na ich wystąpienie, skutecznego reagowania oraz odbudowy po ich zakończeniu.

W tym kontekście zarządzanie kryzysowe stało się jednym z filarów bezpieczeństwa europejskiego, umożliwiając koordynację działań państw członkowskich w sytuacjach zagrożeń o charakterze ponadnarodowym. Mechanizmy unijne nie zastępują krajowych systemów reagowania, lecz je uzupełniają, wzmacniając interoperacyjność struktur odpowiedzialnych za bezpieczeństwo oraz umożliwiając szybkie mobilizowanie zasobów w sytuacjach kryzysowych. Szczególne znaczenie ma tu zasada solidarności,

wyrażona w art. 222 Traktatu o funkcjonowaniu Unii Europejskiej, zobowiązujący państwa członkowskie do wspólnego działania w przypadku katastrof naturalnych, zamachów terrorystycznych lub innych poważnych zagrożeń (European Union, 2012).

Rosnąca rola UE w zarządzaniu kryzysowym wynika również z transformacji środowiska bezpieczeństwa w Europie. Kryzysy ostatnich lat – w tym pandemia COVID-19, kryzys migracyjny, katastrofy klimatyczne oraz wojna w Ukrainie – pokazały, że bezpieczeństwo państw europejskich ma charakter współzależny i wymaga skoordynowanych działań na poziomie ponadnarodowym (Council of the European Union, 2022). Doświadczenia te przyczyniły się do wzmocnienia instrumentów reagowania kryzysowego oraz zwiększenia znaczenia współpracy między instytucjami unijnymi a państwami członkowskimi. W rezultacie zarządzanie kryzysowe Unii Europejskiej należy postrzegać jako istotny komponent systemu bezpieczeństwa europejskiego, którego funkcją jest zwiększanie zdolności reagowania na zagrożenia transgraniczne, wzmacnianie odporności państw członkowskich oraz budowanie wspólnych zdolności reagowania na sytuacje kryzysowe (Decyzja nr 1313/2013/UE, 2013). System ten stanowi jeden z elementów szerszej architektury bezpieczeństwa europejskiego, obejmującej zarówno struktury cywilne, jak i wojskowe, a jego znaczenie rośnie wraz ze wzrostem liczby złożonych zagrożeń o charakterze wielowymiarowym.

Instytucje odpowiedzialne za zarządzanie kryzysowe w UE

Kluczową rolę w systemie zarządzania kryzysowego Unii Europejskiej odgrywa Komisja Europejska, w szczególności Dyrekcja Generalna ds. Ochrony Ludności i Pomocy Humanitarnej (DG ECHO), odpowiedzialna za opracowywanie i realizację polityki reagowania kryzysowego oraz pomocy humanitarnej. DG ECHO koordynuje działania podejmowane w ramach Unijnego Mechanizmu Ochrony Ludności, mobilizując zasoby państw członkowskich oraz współpracując z organizacjami międzynarodowymi i partnerami lokalnymi. Zakres jej działalności obejmuje zapobieganie katastrofom, ograniczanie ich skutków oraz udzielanie wsparcia państwom i społecznościom dotkniętym sytuacjami kryzysowymi, zarówno w przypadku katastrof naturalnych, jak i zdarzeń spowodowanych działalnością człowieka (Mucha, 2023).

Na szczeblu politycznym koordynację reakcji Unii Europejskiej w sytuacjach poważnych kryzysów wspierają Rada Unii Europejskiej, jej prezydencja oraz Komitet Stałych Przedstawicieli (COREPER), wykorzystując Zintegrowany Mechanizm Reagowania Kryzysowego (IPCR). Mechanizm ten umożliwia szybkie gromadzenie informacji, prowadzenie konsultacji międzyinstytucjonalnych oraz przygotowywanie decyzji politycznych dotyczących reagowania kryzysowego.

W zarządzaniu kryzysowym Unii Europejskiej uczestniczą również inne instytucje i podmioty, w tym Parlament Europejski, agencje unijne oraz wyspecjalizowane systemy wsparcia. Parlament Europejski pełni funkcję ustawodawczą i kontrolną, uczestnicząc w procesie tworzenia regulacji prawnych oraz zatwierdzaniu środków finansowych przeznaczonych na reagowanie kryzysowe. Istotną rolę w obszarze bezpieczeństwa zdrowotnego odgrywa Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC), które odpowiada za monitorowanie chorób zakaźnych, identyfikację nowych zagrożeń zdrowotnych oraz wspieranie państw członkowskich w zapobieganiu i kontroli epidemii. Do jego kluczowych zadań należy prowadzenie sieci nadzoru epidemiologicznego, obsługa systemów wczesnego ostrzegania i reagowania, opracowywanie opinii naukowych oraz informowanie o ryzyku zdrowotnym (ECDC, 2025). System zarządzania kryzysowego UE wspierany jest również przez narzędzia technologiczne i sieci współpracy. Program kosmiczny Copernicus, w szczególności usługa Emergency Management Service, dostarcza danych satelitarnych umożliwiających monitorowanie sytuacji kryzysowych, mapowanie skutków katastrof oraz planowanie działań ratowniczych. Ważną rolę odgrywa także Europejska Sieć Wiedzy Ochrony Ludności (UCPKN), która wspiera szkolenia, ćwiczenia oraz wymianę doświadczeń i dobrych praktyk między państwami członkowskimi.

Udział instytucji unijnych, agencji wyspecjalizowanych oraz systemów wsparcia technologicznego pokazuje wielopoziomowy charakter zarządzania kryzysowego w Unii Europejskiej, łączący działania operacyjne, eksperckie i legislacyjne w celu zwiększania odporności państw członkowskich na zagrożenia o charakterze transgranicznym.

Mechanizmy zarządzania kryzysowego w Unii Europejskiej

Podstawowym instrumentem operacyjnego reagowania kryzysowego w Unii Europejskiej jest Unijny Mechanizm Ochrony Ludności (UCPM), ustanowiony decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE. Mechanizm ten umożliwia koordynację pomocy państw członkowskich w przypadku klęsk żywiołowych, katastrof technologicznych oraz innych sytuacji kryzysowych zarówno na terytorium Unii Europejskiej, jak i poza jej granicami (Decyzja nr 1313/2013/UE, 2013).

Unijny Mechanizm Ochrony Ludności funkcjonuje jako wielopoziomowy system współpracy państw uczestniczących, oparty na strukturze obejmującej Centrum Koordynacji Reagowania Kryzysowego (ERCC), europejską pulę ochrony ludności (European Civil Protection Pool – ECPP), Wspólny System Łączności i Informowania w Sytuacjach Kryzysowych (CECIS) oraz krajowe punkty kontaktowe. ERCC zapewnia całodobową zdolność operacyjną, koordynując działania pomocowe i analizując informacje o sytuacjach kryzysowych (European Commission, 2026). Europejska pula ochrony ludności stanowi dobrowolny zasób zdolności reagowania zgłaszanych przez państwa członkowskie, obejmujący wyspecjalizowane zespoły ratownicze, moduły interwencyjne, sprzęt oraz ekspertów. System CECIS umożliwia natomiast szybką komunikację między ERCC a państwami uczestniczącymi oraz wymianę informacji dotyczących potrzeb i dostępnych zasobów (Paluch, 2024).

Istotne wzmocnienie funkcjonowania mechanizmu nastąpiło w wyniku przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/836 z dnia 20 maja 2021 r., zmieniającego decyzję nr 1313/2013/UE. Nowelizacja ta była odpowiedzią na doświadczenia związane z pandemią COVID-19 oraz rosnącą liczbą zagrożeń o charakterze transgranicznym. Szczególne znaczenie miało rozszerzenie inicjatywy rescEU, obejmujące tworzenie europejskiej rezerwy strategicznych zasobów reagowania kryzysowego, takich jak zapasy medyczne, środki transportu, sprzęt do zwalczania pożarów lasów czy zdolności reagowania na zagrożenia chemiczne, biologiczne, radiologiczne i jądrowe. Rozporządzenie umożliwiło Komisji Europejskiej bezpośrednie finansowanie, nabywanie lub wynajmowanie takich zdolności,

co wzmocniło operacyjną autonomię Unii Europejskiej w sytuacjach nadzwyczajnych (European Union, 2021).

Jednocześnie zwiększono wsparcie finansowe dla działań zapobiegawczych, przygotowawczych i reagowania kryzysowego oraz rozwinięto Europejską Sieć Wiedzy Ochrony Ludności jako narzędzie wymiany doświadczeń i doskonalenia kompetencji w zakresie ochrony ludności. W rezultacie zmiany wprowadzone rozporządzeniem (UE) 2021/836 przyczyniły się do zwiększenia odporności systemu zarządzania kryzysowego Unii Europejskiej oraz wzmocnienia solidarności między państwami członkowskimi w obliczu współczesnych zagrożeń.

W przypadku poważnych i złożonych sytuacji kryzysowych Unia Europejska wykorzystuje Zintegrowany Mechanizm Reagowania Kryzysowego (Integrated Political Crisis Response – IPCR), który umożliwia koordynację reakcji politycznej na poziomie instytucji unijnych i państw członkowskich. Mechanizm ten wspiera działania Rady Unii Europejskiej, jej prezydencji oraz Komitetu Stałych Przedstawicieli (COREPER), zapewniając narzędzia umożliwiające gromadzenie i analizę informacji, koordynację współpracy międzyinstytucjonalnej oraz przygotowanie propozycji działań politycznych. IPCR może funkcjonować w różnych trybach, od monitorowania sytuacji i wymiany informacji po pełną aktywację, obejmującą przygotowywanie propozycji decyzji dla Rady UE lub Rady Europejskiej (Council of the European Union). Mechanizmy zarządzania kryzysowego Unii Europejskiej tworzą zintegrowany system reagowania, łączący zdolności operacyjne państw członkowskich z instrumentami koordynacyjnymi instytucji unijnych oraz umożliwiający skuteczną reakcję na zagrożenia o charakterze transgranicznym.

Funkcjonowanie systemu zarządzania kryzysowego UE w wybranych sytuacjach kryzysowych

Funkcjonowanie systemu zarządzania kryzysowego Unii Europejskiej można najlepiej ocenić poprzez analizę wybranych sytuacji kryzysowych, w których wykorzystano unijne mechanizmy reagowania. Doświadczenia ostatnich lat pokazują, że instrumenty UE są wykorzystywane zarówno w przypadku zagrożeń zdrowotnych, katastrof naturalnych, jak i konfliktów zbrojnych oraz kryzysów humanitarnych. Analiza studiów przypadków

pozwala ocenić skuteczność współpracy państw członkowskich oraz rolę instytucji unijnych w koordynowaniu działań pomocowych.

Pandemia COVID-19 stała się transgranicznym kryzysem o charakterze globalnym, oddziałującym nie tylko na systemy ochrony zdrowia, lecz także na gospodarkę i życie społeczne państw członkowskich Unii Europejskiej (Marcinkowski, 2023). Kryzys ten ujawnił ograniczony zakres kompetencji UE w obszarze zdrowia publicznego, który pozostaje w dużej mierze domeną państw członkowskich (Żyłka, 2024), a także niedostateczny poziom koordynacji działań w początkowej fazie pandemii. Jednocześnie doświadczenia pandemii pokazały niewystarczający charakter dotychczasowych instrumentów reagowania na poważne transgraniczne zagrożenia zdrowotne oraz potrzebę wzmocnienia roli Unii Europejskiej w obszarze bezpieczeństwa zdrowotnego. W konsekwencji pandemia stała się impulsem do zmian instytucjonalnych i prawnych prowadzących do rozwoju koncepcji Europejskiej Unii Zdrowotnej oraz nowych mechanizmów reagowania kryzysowego (Maciejczyk-Krysiak, 2024).

W odpowiedzi na pandemię COVID-19 Unia Europejska stopniowo rozwijała instrumenty koordynacji działań państw członkowskich, obejmujące zarówno obszar zdrowia publicznego, jak i wsparcie gospodarcze oraz logistyczne. Jednym z kluczowych elementów była organizacja wspólnych zakupów szczepionek i środków ochrony medycznej, co umożliwiło zapewnienie ich dostępności na rynku europejskim oraz ograniczenie konkurencji między państwami członkowskimi. Równolegle rozwijano systemy monitorowania zagrożeń epidemiologicznych oraz współpracę instytucji unijnych z krajowymi systemami ochrony zdrowia. W dłuższej perspektywie pandemia COVID-19 przyczyniła się do zwiększenia znaczenia współpracy europejskiej w obszarze zarządzania kryzysowego oraz do rozwoju instrumentów solidarnościowych, które mogą być wykorzystywane w przypadku innych zagrożeń o charakterze transgranicznym.

Doświadczenia pandemii przyczyniły się do wzmocnienia europejskiego systemu zarządzania zagrożeniami zdrowotnymi, czego wyrazem było m.in. utworzenie Urzędu ds. Gotowości i Reagowania na Stany Zagrożenia Zdrowia (HERA), rozwój rezerw medycznych rescEU oraz zwiększenie roli instytucji takich jak Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) i Europejska Agencja Leków (EMA). Pandemia COVID-19

stała się zatem istotnym impulsem do dalszego rozwoju unijnego systemu zarządzania kryzysowego i wzmacniania odporności Unii Europejskiej na zagrożenia o charakterze transgranicznym (Żyłka, 2024).

Rozwój europejskich zdolności reagowania kryzysowego należy również rozpatrywać w szerszym kontekście ewolucji polityki bezpieczeństwa Unii Europejskiej po wejściu w życie Traktatu z Lizbony. Reforma instytucjonalna umożliwiła bowiem tworzenie nowych organów i mechanizmów współpracy w obszarze bezpieczeństwa i obrony, przy jednoczesnym zachowaniu decyzyjnej roli państw członkowskich. W konsekwencji polityka bezpieczeństwa UE przyjęła charakter hybrydowy, łączący elementy międzyrządowe i ponadnarodowe, co ma istotne znaczenie dla zdolności reagowania na współczesne zagrożenia transgraniczne (Piechowicz, 2023).

Agresja Federacji Rosyjskiej na Ukrainę w 2022 r. doprowadziła do uruchomienia największej operacji Unijnego Mechanizmu Ochrony Ludności od momentu jego powstania. Ukraina zwróciła się o pomoc za pośrednictwem mechanizmu jeszcze przed rozpoczęciem działań zbrojnych, a po wybuchu wojny liczba wniosków o wsparcie systematycznie rosła, obejmując m.in. obszary zdrowia, schronienia, energii, transportu i logistyki, sprzętu ratowniczego oraz reagowania na zagrożenia CBRN (Paluch, 2024). Unia Europejska, działając poprzez Centrum Koordynacji Reagowania Kryzysowego (ERCC) oraz mechanizm rescEU, skoordynowała dostarczanie pomocy humanitarnej i technicznej, obejmującej m.in. sprzęt medyczny, generatory prądu, środki ochrony osobistej oraz wyposażenie ratownicze. Wsparcie realizowane było za pośrednictwem logistycznych hubów zlokalizowanych w Polsce, Rumunii i na Słowacji, a także poprzez ewakuacje medyczne pacjentów z Ukrainy do szpitali w państwach europejskich. Działania te potwierdziły zdolność Unii Europejskiej do mobilizacji zasobów państw członkowskich oraz koordynacji pomocy w warunkach długotrwałego konfliktu zbrojnego o charakterze humanitarnym (Paluch, 2024).

Szczególną rolę w realizacji operacji pomocowych odegrały państwa graniczne Unii Europejskiej, zwłaszcza Polska, która stała się jednym z głównych centrów logistycznych wsparcia Ukrainy. Na terytorium Polski funkcjonowały huby logistyczne Unii Europejskiej oraz centrum ewakuacji medycznej Medevac Hub w Rzeszowie, wspierające transport pacjentów do placówek medycznych w państwach członkowskich. Doświadczenia te

potwierdzają znaczenie współpracy między poziomami krajowym i unijnym w systemie zarządzania kryzysowego UE.

W literaturze wskazuje się, że do najpoważniejszych kryzysów globalnych ostatnich lat – obok kryzysu zdrowotnego związanego z pandemią COVID-19 oraz kryzysu bezpieczeństwa wywołanego agresją Federacji Rosyjskiej na Ukrainę – należy również kryzys klimatyczny, którego konsekwencje w XXI w. ulegają nasileniu i generują złożone, wielosektorowe skutki (Mik, 2024).

Katastrofy naturalne, w tym pożary lasów, stają się coraz częstszym wyzwaniem dla państw europejskich w związku z nasilającymi się skutkami zmian klimatu. W ostatnich latach Unia Europejska systematycznie rozwijała zdolności reagowania w tym obszarze, rozbudowując europejską pulę ochrony ludności oraz rezerwę rescEU. Mechanizmy te umożliwiają szybkie rozmieszczenie wyspecjalizowanych zespołów ratowniczych, sprzętu gaśniczego oraz wsparcia logistycznego w przypadku katastrof naturalnych o dużej skali.

Przykładem wykorzystania unijnych mechanizmów reagowania kryzysowego w obliczu katastrof naturalnych były pożary lasów w Grecji w 2024 r. W odpowiedzi na sytuację kryzysową uruchomiono Unijny Mechanizm Ochrony Ludności (UCPM), a Centrum Koordynacji Reagowania Kryzysowego (ERCC) skoordynowało działania państw członkowskich, obejmujące m.in. wysłanie samolotów gaśniczych oraz wsparcie techniczne. Równolegle wykorzystano system satelitarny Copernicus Emergency Management Service do monitorowania sytuacji i planowania działań ratowniczych. Przypadek ten potwierdził znaczenie wspólnych europejskich zdolności reagowania w sytuacjach katastrof naturalnych o dużej skali oraz rosnącą rolę mechanizmów solidarnościowych w systemie zarządzania kryzysowego UE (European Commission, 2026).

Analiza doświadczeń ostatnich lat, obejmujących pandemię COVID-19, katastrofy naturalne oraz wojnę w Ukrainie, wskazuje, że system zarządzania kryzysowego Unii Europejskiej ulega stopniowemu wzmocnieniu. Rozwój instrumentów operacyjnych, politycznych i finansowych umożliwia coraz bardziej skoordynowane reagowanie na zagrożenia transgraniczne oraz zwiększa odporność państw członkowskich na sytuacje kryzysowe o charakterze wielowymiarowym.

Podsumowanie

System zarządzania kryzysowego Unii Europejskiej stanowi obecnie jeden z istotnych elementów europejskiej architektury bezpieczeństwa, odpowiadający na rosnącą złożoność zagrożeń o charakterze transgranicznym. Analiza instytucji i mechanizmów reagowania kryzysowego UE, w szczególności Unijnego Mechanizmu Ochrony Ludności, Centrum Koordynacji Reagowania Kryzysowego oraz Zintegrowanego Mechanizmu Reagowania Kryzysowego, wskazuje na stopniowe wzmacnianie zdolności Unii Europejskiej do koordynowania działań państw członkowskich w sytuacjach nadzwyczajnych.

Studia przypadków obejmujące pandemię COVID-19, wojnę w Ukrainie oraz katastrofy naturalne potwierdzają, że doświadczenia kolejnych kryzysów przyczyniają się do rozwoju instrumentów reagowania kryzysowego oraz zwiększania poziomu współpracy między państwami członkowskimi i instytucjami unijnymi. Szczególnie widoczne jest to w rozbudowie zdolności operacyjnych rescEU, rozwoju europejskiego systemu reagowania na zagrożenia zdrowotne oraz wzmocnieniu mechanizmów solidarnościowych.

Jednocześnie analiza funkcjonowania unijnego systemu reagowania kryzysowego wskazuje, że jego skuteczność zależy od współpracy państw członkowskich oraz komplementarności poziomów krajowego i unijnego. Unia Europejska nie zastępuje krajowych systemów zarządzania kryzysowego, lecz pełni funkcję koordynacyjną, wspierając mobilizację zasobów, wymianę informacji oraz wspólne działania w sytuacjach kryzysowych.

W rezultacie można stwierdzić, że zarządzanie kryzysowe UE staje się coraz ważniejszym instrumentem wzmacniania odporności europejskiego systemu bezpieczeństwa. Rosnąca liczba zagrożeń o charakterze globalnym – zdrowotnych, klimatycznych, technologicznych i militarnych – wskazuje, że rozwój wspólnych zdolności reagowania kryzysowego pozostanie jednym z kluczowych kierunków integracji europejskiej w obszarze bezpieczeństwa.

Literatura

1. Bryła, J. (2013). System zarządzania kryzysami Unii Europejskiej – znaczenie dla bezpieczeństwa międzynarodowego. *Przegląd Politologiczny, 2*, 101-116.

2. Buzan, B., Wæver, O. (2003). *Regions and powers: The structure of international security.* Cambridge University Press.
3. Council of the European Union. (2022). *A strategic Compass for security and defence*. Pobrane z: https://www.consilium.europa.eu/en/policies/strategic-compass/ (dostęp: 17.01.2026).
4. Council of the European Union. (2024). *The integrated political crisis response (IPCR).* Pobrane z: https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/ (dostęp: 17.01.2026).
5. ECDC. (2025). Consolidated annual activity report 2024. *European Centre for Disease Prevention and Control*. Pobrane z: https://www.ecdc.europa.eu/en/publications-data/consolidated-annual-activity-report-2024 (dostęp: 17.01.2026).
6. European Commission. (2026). *Emergency Response Coordination Centre (ERCC).* Pobrane z: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en (dostęp: 17.01.2026).
7. European External Action Service. (2016). *Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy*. Pobrane z: https://www.coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy (dostęp: 17.01.2026).
8. European Union. (2012). *Traktat o funkcjonowaniu Unii Europejskiej* (Dz. Urz. UE C 326 z 26.10.2012).
9. European Union. (2013). *Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności* (Dz. Urz. UE L 347 z 20.12.2013).
10. European Union. (2021). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/836 z dnia 20 maja 2021 r. zmieniające decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności* (Dz. Urz. UE L 185 z 26.05.2021).
11. OCHA. (2024). *Greece – wildfires, update (media, Greek Civil Protection, EFFIS) (ECHO Daily Flash of 13 August 2024).* ReliefWeb. Pobrane z: https://reliefweb.int/report/greece/greece-wildfires-update-media-greek-civil-protection-effis-echo-daily-flash-13-august-2024 (dostęp: 17.01.2026).

12. Jagusiak, B., Moch, N. (2023). Unia Europejska jako wspólnota bezpieczeństwa i obronności. *Studia Wschodnioeuropejskie, 19*(2), 336-359. https://doi.org/10.31971/24500267.20.22
13. Maciejczyk-Krysiak, N. (2024). Europejski mechanizm reagowania na zagrożenia zdrowotne w ramach Europejskiej Unii Zdrowotnej. *Prawo i Więź, 6*(53), 645-664. https://doi.org/10.36128/PRIW.VI53.1160
14. Madej, M. (2022). Kilka uwag o miejscu Unii Europejskiej w polskiej polityce bezpieczeństwa po rosyjskiej inwazji na Ukrainę. W: R. Kuźniar (red.), *Bezpieczeństwo Polski w świetle wojny na wschodzie* (s. 103-114). Wydawnictwo Naukowe Scholar.
15. Marcinkowski, T. (2023). Dylematy kryzysowe Unii Europejskiej: pandemia i zielony ład. *Rocznik Integracji Europejskiej, 17*, 207-220. https://doi.org/10.14746/rie.2023.17.13
16. Mik, C. (2024). Wpływ kryzysów globalnych na zmianę podejścia Unii Europejskiej do sytuacji kryzysowych. Aspekty prawne, *Prawo i Więź, 6* (53), 363-397. https://doi.org/10.36128/PRIW.VI53.1229
17. Mucha, M. (2023). Międzynarodowe mechanizmy pomocy krajom dotkniętym katastrofą oraz działania ratownicze zespołów poszukiwawczo-ratowniczych na przykładzie misji polskiej ciężkiej grupy poszukiwawczo-ratowniczej po trzęsieniu ziemi w Turcji. *Rocznik Bezpieczeństwa Międzynarodowego 17*(1)*,* 116-144. https://doi.org/10.34862/rbm.2023.1.6
18. Paluch, A. (2024). Unijny mechanizm ochrony ludności wobec współczesnych sytuacji kryzysowych – uwagi de lege lata i de lege ferenda, *Prawo i Więź, 6*(53), 1105-1136. https://doi.org/10.36128/PRIW.VI53.839
19. Piechowicz, M. (2023). Wspólna Polityka Bezpieczeństwa i Obrony UE w perspektywie teoretycznej, praktycznej i agencyjno-instytucjonalnej, *Przegląd Politologiczny, 1*, 37-51. https://doi.org/10.14746/pp.2022.28.1.3
20. Żyłka, B. (2024). Kryzys epidemiologiczny COVID-19 i jego wpływ na transformację unijnego systemu zarządzania transgranicznymi zagrożeniami zdrowotnymi. Działania Unii Europejskiej w kontekście pandemii. *Prawo i Więź, 6*(53)*.* 597-615. https://doi.org/10.36128/PRIW.VI53.1143

Dariusz Brążkiewicz[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska
Rafał Mazurek[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103373_6

BUDOWA STRATEGICZNEGO BEZPIECZEŃSTWA CYBEROBRONY SIŁ ZBROJNYCH RP

BUILDING STRATEGIC CYBER DEFENCE CAPABILITIES FOR THE POLISH ARMED FORCES

Streszczenie

Pojawiające się coraz częściej cyberataki na infrastrukturę krytyczną pokazują zagrożenia stwarzane zarówno dla podmiotów cywilnych, jak i wojskowych. Wymaga to intensyfikacji działań na rzecz ochrony przed zagrożeniami cyberbezpieczeństwa. Tworzony w wojsku komponent cyberobrony ma na celu zwiększenie zdolności Sił Zbrojnych RP oraz wzmocnienie koordynacji i współpracy wojskowych struktur przeznaczonych do jej realizacji. Utworzone Wojska Obrony Cyberprzestrzeni mają za zadanie prowadzenie działań w cyberprzestrzeni w pełnym spektrum – od obrony, przez rozpoznanie, po działania ofensywne. Ponadto mają zapewnić bezpieczeństwo systemów teleinformatycznych całych Sił Zbrojnych RP oraz

[1] https://orcid.org/0000-0002-5372-1210, e-mail: d.brazkiewicz@dyd.akademiabialska.pl
[2] e-mail: mazurek.rafal2000@gmail.com

obronę cyberprzestrzeni jako jedno z podstawowych zadań kolektywnej obrony NATO. Przedmiotem badań niniejszego rozdziału jest znaczenie tworzenia cyberbezpieczeństwa w środowisku wojskowym i organizacja jego zwalczania w obecnym środowisku cyberprzestrzeni. Celem rozdziału jest przedstawienie zagrożenia w cyberprzestrzeni oraz utworzenie struktur w Siłach Zbrojnych RP zdolnych do przeciwdziałania tym zagrożeniom. W związku z przedmiotem i celem badań, powstał główny problem badawczy, który został wyrażony w postaci następującego pytania: Jakie znaczenie ma budowa kompleksowej cyberobrony przez Siły Zbrojne RP i jaki jest jej kierunek rozwoju, zgodny z przyjmowanymi założeniami prawnymi? Poszukiwanie naukowych rozstrzygnięć, w odniesieniu do określonego głównego problemu badawczego, wymagało przyjęcia i rozwiązania szczegółowych problemów badawczych: 1) Jakie jest zagrożenie w cyberprzestrzeni dla Sił Zbrojnych RP? 2) Jaki jest kierunek rozwoju bezpieczeństwa cyberobrony w NATO i Siłach Zbrojnych RP? 3) Jak realizowane jest tworzenie i rozwój Wojsk Obrony Cyberprzestrzeni? Przeprowadzone badania wstępne, określony cel badań i problemy badawcze zdeterminowały przyjętą na potrzeby badań hipotezę główną: Istniejące od niedawna zagrożenie w cyberprzestrzeni wymaga podejmowania systemowych rozwiązań w celu ochrony cyberprzestrzeni, szczególnie w Siłach Zbrojnych RP. Weryfikacji dostępnych materiałów dokonano poprzez analizę i krytykę dostępnej literatury przedmiotu oraz faktów z informacji prasowych.

Słowa kluczowe: cyberprzestrzeń, cyberobrona, Wojska Obrony Cyberprzestrzeni Sił Zbrojnych RP

Abstract

More and more frequent cyberattacks on critical infrastructure demonstrate the threats posed to both civilian and military entities. This requires intensified actions to protect against cybersecurity threats. The cyber defence component being created in the army is aimed at increasing the capabilities of the Polish Armed Forces and strengthening the coordination and cooperation of military structures intended for its implementation. The established Cyberspace Defence Forces are tasked with conducting operations in cyberspace in the full spectrum – from defence, through reconnaissance, to offensive activities. In addition, they are to ensure the security of the IT systems of the entire Polish Armed Forces and the defence of cyberspace as one of the basic tasks of NATO's collective defence. The subject of this chapter's research is the importance of creating cybersecurity in the military environment and organizing their fight in the current cyberspace environment. The aim of the chapter is to present the threats in cyberspace and the structures within the Polish Armed Forces capable of countering them. In connection with the subject of the research and the purpose of the research, the main research problem arose, which

was expressed in the form of the following question: What is the importance of building comprehensive cyber defence by the Polish Armed Forces and what is its direction of development, consistent with the adopted legal assumptions?
The search for scientific solutions in relation to a specific main research problem required the adoption and solution of detailed research problems: 1) What is the threat in cyberspace to the Polish Armed Forces? 2) What is the direction of development of cyber defence security in NATO and the Polish Armed Forces? 3) How is the creation and development of the Cyberspace Defence Forces implemented? The preliminary research, the specific research goal, and the research problems determined the main hypothesis for the research: The existing threat in cyberspace requires systemic solutions to protect it, especially within the Polish Armed Forces. The available materials were verified by analysing and critiquing the literature on the subject and by reviewing press releases.

Keywords: cyberspace, cyber defence, Cyberspace Defence Forces of the Polish Armed Forces

Wstęp

Na obecną chwilę realizacja systemowej obrony w cyberprzestrzeni jest jednym z priorytetów obejmujących obszar funkcjonowania cywilnych struktur rządowych i samorządowych, bezpieczeństwa społeczeństwa oraz wojskowych struktur organizacyjnych. Te ostatnie struktury, odpowiedzialne głównie za bezpieczeństwo zewnętrzne państwa, muszą być przygotowane na przeciwdziałanie wszelkim działaniom w cyberprzestrzeni zakłócającym prawidłową realizację działań obronnych i ochronnych. To szczególne znaczenie wynika również z faktu wykorzystywania przez Siły Zbrojne RP wielu komunikatorów, którymi realizowane jest przekazywanie informacji niejawnych, tak ważnych w działaniach wojskowych. Bezpieczeństwo państwa w coraz większym stopniu zależy od zdolności skutecznej obrony w cyberprzestrzeni. Dynamiczny rozwój technologii informatycznych stwarza równocześnie szeroki wachlarz szans i ryzyka. Aktualne konflikty zbrojne toczą się w pięciu obszarach: lądowym, powietrznym, morskim, kosmicznym oraz cyberprzestrzeni. Siły Zbrojne Rzeczypospolitej Polskiej, działając w ramach struktur NATO oraz Unii Europejskiej, konsekwentnie podnoszą własne zdolności, co posiada realne przełożenie na prowadzenie działań oraz odporność wschodniej flanki NATO w cyberprzestrzeni.

Budowa ww. zdolności są fundamentem współczesnego bezpieczeństwa działań sił zbrojnych w okresie pokoju czy wojny. Szczególne przygotowania w postaci ćwiczeń pozwalają na wieloaspektowe analizy skuteczności działań Sił Zbrojnych RP oraz kierunkowanie kolejnych działań w obronie cyberprzestrzeni. Tworzenie nowych struktur cyberobrony i szkolenie specjalistyczne personelu są nieodzownymi elementami bezpieczeństwa cyberprzestrzeni.

Narastające zagrożenie w cyberprzestrzeni dla przepływu informacji i działań Sił Zbrojnych RP

Rozważając zagadnienia związane z cyberprzestrzenią, należy przytoczyć, z czym są związane dane pojęcia, by uniknąć posługiwania się terminami używanymi potocznie, często przeinaczonymi w swym znaczeniu w stosunku do ich pierwotnego rozumienia.

Cyberprzestrzeń jest domeną o zasięgu globalnym, charakteryzującą się dynamicznymi zmianami. Stanowi wirtualny, nieograniczony przestrzenią ani czasem port komunikacyjny tworzony przez dwie składowe: hardware i software. Pierwszą z nich są wszystkie fizyczne systemy służące do odbierania, przechowywania oraz wysyłania danych. Drugą z nich jest całe oprogramowanie odpowiedzialne za przesyłanie oraz przetwarzanie informacji (Gwoździewicz i in., 2024b).

Cyberzagrożeniem są natomiast działania mające na celu spowodowanie szkody w warstwie fizycznej lub programowej poprzez nieautoryzowany dostęp do warstwy sieciowej systemu, uszkodzenie sieci lub systemu informatycznego, co najczęściej prowadzi do kradzieży danych lub informacji. Zagrożenia mogą pochodzić zarówno z zewnątrz organizacji, jak i wewnątrz, przyjmując różne formy. Stanowią poważne zagrożenie dla bezpieczeństwa państwa oraz społeczeństwa. Trudnością w walce z nimi jest ciągłe monitorowanie oraz udoskonalanie zabezpieczeń (Gwoździewicz i in., 2024b).

Z kolei cyberbezpieczeństwo można przedstawiać na dwa sposoby: jako stan oraz proces. Obejmuje trzy poziomy: fizyczny, informatyczny oraz organizacyjno-prawny. Obejmuje ochronę infrastruktury krytycznej, systemów, sieci, aplikacji, chmury, danych i utrzymanie ciągłości działania. W 2018 r. cyberbezpieczeństwo zdefiniowano jako odporność systemów na działania naruszające poufność, integralność, dostępność i autentyczność

danych. Natomiast w prawie Unii Europejskiej, począwszy od 2019 roku, oznacza działania ochronne przed cyberzagrożeniami, w tym cyberatakami. Do zwiększenia poziomu bezpieczeństwa w cyberprzestrzeni stosuje się wiele narzędzi, w tym monitorowanie zabezpieczeń, uwierzytelnienie wieloskładnikowe przy logowaniu do systemu, zarządzanie dostępem do systemów oraz wykrywanie incydentów z wykorzystaniem sztucznej inteligencji (Gwoździewicz i in., 2024b).

Mimo wielu zalet, cyberprzestrzeń uważana jest również za piąty obszar działań wojennych, występujący na równi z obszarem lądowym, morskim, powietrznym oraz kosmicznym, który obejmuje takie składowe jak sieci informacyjno-telekomunikacyjne, infrastruktura i obsługiwane przez nią dane, systemy komputerowe oraz urządzenia odpowiedzialne za sterowanie procesami. Współdziałanie systemów sieciowych z systemami fizycznymi oraz ich w wielu przypadkach nierozerwalność, zmuszają do podchodzenia do kwestii ich obrony kompleksowo. Historia ostatnich lat pokazała między innymi, jak za pomocą jednego urządzenia podpiętego do komputera zamkniętej sieci uszkodzono wirówki wykorzystywane do wzbogacania uranu (Zetter, 2018).

Jednym z zagrożeń w cyberprzestrzeni jest dezinformacja. Samo pojęcie dezinformacji jest stosunkowo nowe, lecz jej formy są używane od lat przez różne państwa, w celu osiągania celów politycznych, ekonomicznych bądź militarnych. Termin ten powstał w latach dwudziestych XX wieku w Związku Radzieckim, gdzie w 1923 r. powstało: Specjalne biuro dezinformacyjne do prowadzenia aktywnych operacji wywiadowczych (Wachowicz, 2019). Dezinformacja jest rodzajem oszustwa stosowanym do wprowadzania w błąd oraz manipulowania opinią publiczną. Jej forma przybiera spreparowaną formę, która jest celowo rozpowszechniana, by dezorientować odbiorców. Celem tych działań jest stworzenie zamieszania, w którym wynik końcowy jest korzystny z punktu widzenia finansowego lub politycznego grupy je stosującej. Może występować zarówno w czasie pokoju, jak i wojny, na której stanowi kolejną płaszczyznę walk. Spreparowana informacja może być celowo wymierzona w konkretną grupę społeczną lub nie posiadać grupy docelowej. Bardzo często dezinformacja stosowana jest w artykułach z dość chwytliwymi oraz przyciągającymi uwagę nagłówkami (Szymańska, 2023). Również poradnik bezpieczeństwa z 2025 roku poświęca uwagę

problemowi dezinformacji oraz przedstawia kilka kluczowych form walki z nią. Między innymi zaleca weryfikację informacji w kilku miejscach od siebie niezależnych, powstrzymanie się od rozpowszechniania nieprawdziwych informacji pod wpływem emocji, nierozpowszechnianie informacji – poprzez robienie zdjęć oraz nagrywanie filmów i późniejsze ich publikowanie – o ruchach wojsk, miejscach rozlokowania sprzętu oraz ważnych obiektach. Zaleca się weryfikację informacji w źródłach publicznych, do których zalicza się Polskie Radio, Telewizję Polską oraz rządowe strony internetowe (MSWiA, MON, RCB, 2025).

Kwestia wojskowego odstraszania również w cyberprzestrzeni jest kluczowym, strategicznym celem sił zbrojnych. By odstraszanie było skuteczne, musi spełniać trzy warunki: faktyczna zdolność działania, zdecydowana gotowość użycia posiadanych środków oraz jasna deklaracja podejmowanych działań względem potencjalnego agresora. W cyberprzestrzeni skuteczność odstraszania jest o tyle ograniczona, o ile występują trudności w sprecyzowaniu lub ustaleniu sprawcy ataku, co niewątpliwie utrudnia szybką i jednoznaczną odpowiedź. Dlatego szczególnie ważne jest budowanie silnych zdolności, w obliczu których potencjalny przeciwnik zniechęci się do przeprowadzenia ataku z niewymiernym kosztem dla własnych strat. Wojskowa cyberobrona musi posiadać również zdolności ofensywne, by kontratakować. Kompleksowość cyberobrony opiera się zatem na kompleksowym podejściu do strategii odstraszania, determinacji oraz zdolności reakcji (Ganuza, 2020).

Konflikty hybrydowe nie są aktualnie odosobnionym przypadkiem. Nasuwa się stwierdzenie, że w trzecim dziesięcioleciu XXI wieku wszystkie konflikty, w tym zbrojne, są konfliktami hybrydowymi. Działania hybrydowe w kontekście walki między państwami mogą sięgać swoimi sposobami do działań symetrycznych, przeplatając je z działaniami poniżej progu wojny. Destabilizacja polityczna danego regionu przygotowuje grunt pod przyszłą interwencję zbrojną państwa agresywnego, co tłumaczy się niesieniem pomocy uciemiężonej grupie społecznej, przy czym część opinii publicznej pod wpływem dezinformacji jest przekonana o słuszności. Odnosząc się do współczesnych konfliktów zbrojnych, hybrydowość rozumiana jest jako współistnienie starych i nowych wojen (Banasik, Parafianowicz, 2015). Jedną z częściej przytaczanych w literaturze przedmiotu definicji

wojny hybrydowej jest ta skonstruowana przez Franka Hoffmana, a cechuje ją: „zbieżność [...] fizyczna i psychologiczna, kinetyczna i niekinetyczna bojowników i cywilów [...], sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone" (Tyson, 2007).

Informacja jest obecnie kluczowym zasobem w relacjach międzynarodowych, przyjmowanym jako zasób strategiczny. Z uwagi na tak dużą jej wartość powstały zjawiska nazywane wojnami informacyjnymi. Są to działania, które tworzą problematyczne definicje i przypisują je istniejącym już pojęciom w zachodniej nauce. Taka modyfikacja i przeinaczenie ich znaczenia mają prowadzić w dalszej perspektywie do modyfikacji lub niszczenia systemów komunikacyjnych, osiągając tym cele polityczne, ekonomiczne bądź militarne. Stosowanie technik propagandowych, prowadząc wojnę informacyjną, nie zawsze jest działaniem wielkim, przełomowym – często wystarczy użycie odpowiedniego słowa bądź zdania, by kształtować poglądy docelowej grupy społecznej. Podając za przykład Federację Rosyjską i jej system oddziaływania informacyjnego, który ma charakter masowy, sprowadza się do publikowania sfabrykowanych treści pod odpowiednią tezą oraz powielania ich na wielu kontach, często również spreparowanych, co daje odbiorcy przekonanie, że skoro ta informacja występuje w tylu źródłach, to z pewnością jest prawdziwa. Idealnym przykładem kampanii dezinformacyjnej stosowanej przez Federację Rosyjską na początku 2022 roku (ta przyjęta retoryka utrzymuje się do chwili obecnej), było określenie napaści zbrojnej na Ukrainę jako „walki z pronazistowskim rządem ukraińskim" oraz rozpoczęcie „Specjalnej Operacji Wojskowej". Warto przypomnieć działania z 2014 r., kiedy to doszło do aneksji Półwyspu Krymskiego przez „zielonych ludzików" przedstawianych przez Federację Rosyjską jako oddolną inicjatywę, a po pewnym czasie dzień napadu na Krym ustanowiono jako święto rosyjskich sił specjalnych (Kiera, 2023).

W nocy z 9 na 10 września 2025 r. Federacja Rosyjska ponad dwudziestoma statkami bezzałogowymi naruszyła polską przestrzeń powietrzną. Wydarzeniom tym towarzyszyła zintensyfikowana aktywność dezinformacyjna w sieci ze strony Białorusi oraz Federacji Rosyjskiej. Celem państw, które w tym samym czasie prowadziły ćwiczenia „Zapad-2025", było zrzucenie odpowiedzialności za atak na Ukrainę oraz podważenie skuteczności

polskich służb i wojska. Rozpoczęto rozprzestrzenianie licznych fałszywych narracji, w tym obwiniano Ukrainę o prowokację, jednocześnie sugerując, że ma chęć (Ukraina) wciągnąć Polskę oraz NATO do pełnoskalowej wojny z Federacją Rosyjską. Przykładami fałszywych informacji z tego czasu są doniesienia o zestrzeleniu bezzałogowych statków powietrznych nad miejscowościami, gdzie ich fizycznie nie było, oraz o tym, że konstrukcje, które znalazły się na terenie Polski, nie są w stanie przelecieć 500 kilometrów (PAP, 2025). Sugerowanie, że państwo polskie nie jest w stanie ostrzec obywateli o zagrożeniu, a Wojsko Polskie nie jest przygotowane do obrony kraju. Ponadto sugerowano, że Rosja nie odpowiada za atak, ponieważ nie ma w tym żadnego interesu, kreując się jednocześnie na stronę pokrzywdzoną, a drony nad Polską jako medialną manipulację oraz fałszywy alarm wojenny.

Rozwój cyberbezpieczeństwa w NATO i Siłach Zbrojnych RP

W dniach 8-9 lipca 2016 r. odbył się Szczyt NATO w stolicy Polski – Warszawie. Tematyką zorganizowanego szczytu były kwestie związane z Afganistanem, Wschodem oraz Południem. Podjęto oraz podkreślono udział Unii Europejskiej w przywracaniu bezpieczeństwa w Europie Wschodniej, odniesiono się do kwestii stabilności Libii oraz położono nacisk na rolę walki z Państwem Islamskim. Owocem spotkania było podpisanie między Unią Europejską a Stanami Zjednoczonymi deklaracji o zacieśnieniu praktycznej współpracy w określonych dziedzinach, wśród których znalazły się:

- walka z zagrożeniami hybrydowymi,
- współpraca na morzu w kwestii migracji,
- koordynacja działań z zakresu bezpieczeństwa cybernetycznego,
- rozwój zdolności obronnych,
- zwiększenie jakości wspólnych ćwiczeń (Rada Unii Europejskiej, 2024).

W trakcie obrad przedstawiciele państw zaangażowanych w szczyt wspólnie uznali, że cyberprzestrzeń jest domeną sojuszniczych działań operacyjnych. Ma to związek z artykułem piątym Traktatu Waszyngtońskiego, którego treść zobowiązuje do kolektywnej obrony w przypadku zaistnienia zagrożenia (Soloch, Pietrzak, 2016).

W ramach Unii Europejskiej funkcjonuje wspólna polityka cyberobrony, mająca na celu, poprzez współpracę i wymianę informacji pomiędzy państwami, zwiększenie odporności na cyberataki poprzez lepsze ich wykrywanie oraz zapobieganie im w przyszłości. Pierwszym dokumentem rysującym podwaliny pod obecne systemy sojusznicze, było przyjęcie w 2014 r. ram polityki w zakresie cyberobrony, które cztery lata później zaktualizowano. Natomiast 22 maja 2023 r. Rada Europejska przyjęła konkluzje w sprawie polityki Unii Europejskiej w zakresie cyberobrony. Wypełniając konkluzje podjęte w 2023 r., w październiku 2024 r. został zatwierdzony unijny wykaz cyberdziałań – pierwszy taki kompleksowy dokument dotyczący cyberbezpieczeństwa (Rada Unii Europejskiej, b.d.).

Europejska polityka w zakresie cyberobrony składa się z czterech filarów:

- sojuszniczych działań na rzecz silniejszej cyberobrony,
- zabezpieczenia ekosystemu obronnego Unii Europejskiej,
- inwestowania w zdolności z zakresu cyberobrony,
- partnerstwa w przezwyciężaniu wyzwań.

Natomiast w Polsce program CYBER.MIL.PL został zapoczątkowany w lutym 2019 r., jako odpowiedź na zwiększone potrzeby z zakresu cyberbezpieczeństwa. Celem programu jest zwiększenie poziomu bezpieczeństwa struktur państwowych oraz obywateli w cyberprzestrzeni. W lutym tego roku została zaprezentowana koncepcja sformowania nowego rodzaju wojsk – Wojsk Obrony Cyberprzestrzeni. Powołano Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, na które składają się już wcześniej istniejące Narodowe Centrum Kryptologii i Inspektorat Informatyki. Działanie to pozwoliło zebrać w jednym miejscu specjalistów z dziedziny cyberbezpieczeństwa. Scalenie dwóch dotąd oddzielnych podmiotów pozwoliło na zwiększenie przepływu informacji oraz podniesienie poziomu umiejętności personelu (Wojska Obrony Cyberprzestrzeni, b.d.).

Celem programu CYBER.MIL.PL jest zwiększenie bezpieczeństwa państwa oraz obywateli w obszarze cyberprzestrzeni. Obejmuje sobą cztery składowe: ujednolicenie i budowę struktur cyberbezpieczeństwa, edukację poprzez szkolenia oraz treningi, współpracę oraz tworzenie silnej pozycji na arenie międzynarodowej, zwiększanie poziomu bezpieczeństwa w kluczowych dla funkcjonowania państwa sieciach oraz systemach.

Program CYBER.MIL.PL tworzą:

- Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni,
- Służba Kontrwywiadu Wojskowego – pełniąca rolę Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe – koordynuje obsługę incydentów komputerowych mających miejsce w resorcie obrony narodowej. Podejmuje współpracę z podmiotami krajowymi w celu realizacji zadań przeciwdziałającym zagrożeniom w cyberprzestrzeni (Służba Kontrwywiadu Wojskowego, b.d.),
- Wojska Obrony Terytorialnej – w ramach wojsk Obrony Terytorialnej rozwijany jest Zespół Działań Cyberprzestrzennych (ZDC WOT) odpowiedzialny za wykorzystywanie wyzwań z zakresu cyberbezpieczeństwa. Głównym celem ZDC WOT jest zabezpieczenie lokalnej społeczności,
- Wojskowy Instytut Łączności im. prof. Janusza Groszkowskiego - Państwowy Instytut Badawczy – powstały w 1951 roku, obecnie nadzorowany przez Ministra Obrony Narodowej- instytut jest odpowiedzialny za badania naukowe oraz prace rozwojowe obejmujące systemy: dowodzenia, łączności, informatyki, walki radioelektronicznej oraz ochrony informacji na rzecz obrony i bezpieczeństwa państwa,
- Akademia Marynarki Wojennej – Wydział Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej w Gdyni na kierunku Systemy informacyjne w bezpieczeństwie prowadzi specjalność Cyberbezpieczeństwo obejmującą swym zakresem zagadnienia: działalność cyberprzestrzeni, rozpoznawanie zagrożeń w sieci, rozwijanie procedur reagowania na zagrożenia, biały wywiad, informatyka śledcza oraz audyt systemów teleinformatycznych,
- Wojskowa Akademia Techniczna – Wydział Cybernetyki Wojskowej Akademii Technicznej w Warszawie – odpowiedzialny jest za kursy specjalistyczne z zakresu cyberbezpieczeństwa i kryptologii na poziomie krajowym i międzynarodowym. Wyposażenie pracowni w narzędzia dedykowane do modelowania, budowy algorytmów i narzędzi analizy cyberprzestrzeni pomaga ćwiczyć oraz rozwijać zagadnienia związane z analizą wojny informacyjnej,

- Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (ECSC) – odpowiedzialne jest za zwiększanie kompetencji pracowników oraz żołnierzy Sił Zbrojnych Rzeczypospolitej Polskiej z zakresu działań w cyberprzestrzeni. Do najważniejszych zadań ECSC należą: kształcenie kadr, organizacja i prowadzenie ćwiczeń, współpraca z partnerami krajowymi oraz zagranicznymi, skupianie potencjału eksperckiego z resortu obrony narodowej.

Ćwiczenie „Cyber Coalition 22", rozpoczęte 28 listopada 2022 r., było jednym z największych na świecie z zakresu cyberobrony. Zaangażowanych w ćwiczenia było około 1000 ćwiczących z 26 państw Paktu Północnoatlantyckiego. Celem ćwiczenia było wzmocnienie zdolności NATO do odstraszania, obrony oraz przeciwdziałania zagrożeniom w cyberprzestrzeni ze szczególnym uwzględnieniem systemów wojskowych (sieci, systemów teleinformatycznych, infrastruktury krytycznej, łańcucha dostaw). Scenariusze ćwiczenia zakładały szeroki zakres działań, między innymi obronę przed skondensowanym cyberatakiem fikcyjnego państwa na państwo sojusznicze. Rolą Polski w tych ćwiczeniach było stanowienie Dowództwa Regionalnego dla państw wschodniej flanki Paktu Północnoatlantyckiego, które koordynowało działanie 10 krajów przeprowadzających strategiczną operację.

Do wydarzeń, które bezpośrednio odnoszą się do bezpieczeństwa z zakresu cyberbezpieczeństwa, należy zaliczyć zorganizowany przez Ministerstwo Obrony Narodowej Międzynarodowy Kongres Bezpieczeństwa INESCON, który miał miejsce w Poznaniu w dniach 2-3 kwietnia 2025 r. W wydarzeniu brało udział szerokie grono ekspertów z dziedziny IT specjalizujących się w cyberbezpieczeństwie. Celem kongresu było zwiększenie świadomości w kwestii aktualnych potrzeb bezpieczeństwa oraz wyzwań, jakie stawiają procesy zabezpieczania sieci i reagowania na incydenty w niej. Dodatkowo, mimo samych ćwiczeń przeprowadzanych w dwóch strefach – CyberHackLab i CyberBastion – uczestnicy mogli zapoznać się z licznymi nowatorskimi technologiami, w tym związanymi z AI. Na tegorocznym wydarzeniu poruszono szereg kwestii, w tym kilka związanych z bezpieczeństwem narodowym, a ich zakresy brzmiały następująco:

- zintegrowane zarządzanie kryzysowe w zakresie cyberbezpieczeństwa,
- Tarcza Wschód – fortyfikacja wschodniej flanki NATO w cieniu wojny w Ukrainie.

Aktualnie obowiązującymi we wrześniu 2025 r., aktami prawnymi z zakresu cyberbezpieczeństwa w Unii Europejskiej są między innymi następujące dokumenty:

- Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2) – państwa członkowskie UE dokonały przeglądu dyrektywy pod koniec 2020 r. i miały czas do 18 października 2024 r. na pełne wdrożenie dyrektywy,
- Unijny akt o cyberbezpieczeństwie – rozporządzenie Unii Europejskiej 2019/881 miało na celu osiągnięcie wysokiego poziomu cyberbezpieczeństwa i odporności w sieci państw sojuszniczych poprzez przekształcenie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i nadanie jej stałego mandatu,
- Akt dotyczący cyberodporności – jego celem jest ochrona konsumentów i przedsiębiorstw nabywających wyposażenie informatyczne oraz software z komponentem cyfrowym. Wprowadza określone obowiązki oraz wymogi, które muszą spełniać producenci oraz detaliczni sprzedawcy. Akt zaczął być wiążący od 10 grudnia 2024 roku, a obowiązki z niego wynikające (wprowadzone ustawą) będą miały zastosowanie od 11 grudnia 2027 r.

Aktualnie obowiązującymi, we wrześniu 2025 r., aktami prawnymi z zakresu cyberbezpieczeństwa w NATO są między innymi następujące dokumenty:

- NATO Cyber Defence Pledge (2016) – Cyber Defence Pledge stał się obowiązującym aktem od 8 lipca 2016 roku. Podkreśla znaczenie cyberbezpieczeństwa jako kluczowego elementu wspólnej obrony. W ramach dokumentu państwa sojusznicze zobowiązały się do wzmacniania obrony i ochrony cyberprzestrzeni. Dokument określa cyberprzestrzeń jako strategiczny wymiar bezpieczeństwa NATO (Cyber Defence),
- Dokument C-M (2002)49 – przepisy z dnia 17 czerwca 2002 r. z późniejszymi zmianami o tytule Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego zawiera szereg dyrektyw wykonawczych, w tym: Dyrektywę Bezpieczeństwa Obiegu Informacji, Dyrektywę Projektów Niejawnych i Bezpieczeństwa Przemysłowego, Dyrektywę zarządzania INFOSEC w systemach teleinformatycznych,

- AJP-3.20 (Allied Joint Publication 3.20) – jest dokumentem uzupełniającym szerszą doktrynę AJP-3, która dotyczy prowadzenia operacji sojuszniczych. Dokument ten obejmuje planowanie, prowadzenie i ocenę operacji w cyberprzestrzeni w kontekście operacji sojuszniczych państw NATO. Doktryna jest przeznaczona głównie dla środowiska wojskowego – dowódców, sztabów i sił NATO z poziomu operacyjnego – lecz korzystają z niej jako wytycznych partnerzy oraz państwa spoza NATO.

Powstanie i rozwój Wojsk Obrony Cyberprzestrzeni

W Polsce funkcjonuje Krajowy System Cyberbezpieczeństwa, którego celem jest zapewnienie bezpieczeństwa między innymi w świadczeniu kluczowych usług cyfrowych oraz systemów do ich świadczenia (Krajowy). Aktualnie obowiązującymi we wrześniu 2025 roku, aktami prawnymi krajowymi – polskimi – dotyczącymi cyberbezpieczeństwa są między innymi następujące dokumenty:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560),
- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. z 2018 r. poz. 1806),
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. z 2018 r. poz. 2180),
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. z 2018 r. poz. 2080),
- Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999),
- Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1999),

- Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2479),
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. z 2018 r. poz. 1831),
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. z 2018 r. poz. 1830).

Powołanie Wojsk Obrony Cyberprzestrzeni określa Ustawa z dnia 11 marca 2022 roku o obronie Ojczyny, w art. 15 ust. 4, pkt 2. Wojska te są właściwe do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych RP (Ustawa o obronie Ojczyzny, 2025). Dodatkowo posiada zdolności ofensywne.

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) zostało utworzone na bazie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz bezpośrednio podporządkowanych jednostek. Do kluczowych zadań jednostki należy zapewnienie bezpieczeństwa w sektorze teleinformatycznym resortu obrony narodowej. Jednocześnie zajmuje się prowadzeniem badań mających na celu projektowanie nowych rozwiązań, ich wdrażanie oraz użytkowanie. Poza wyżej wymienionymi zadaniami DKWOC zajmuje się również działalnością naukowo-edukacyjną, badawczo-rozwojową oraz opiniodawczą. W resorcie obrony narodowej DKWOC pełni rolę instancji odpowiedzialnej za kryptologię, cyberbezpieczeństwo oraz tworzenie i eksploatowanie systemów IT.

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni ma swoją siedzibę główną w Legionowie, w dawnych koszarach 1. Warszawskiej Dywizji Zmechanizowanej.

Pod DKWOC podlegają następujące jednostki:

- CWSD SZ – Centrum Wsparcia Systemów Dowodzenia Sił Zbrojnych – ma swoją siedzibę w Białobrzegach, stanowi organ wykonawczy DKWOC i odpowiada za działania z zakresu wsparcia dowodzenia poprzez wprowadzanie systemów teleinformatycznych, kierowania środami walki oraz rozpoznania w całych Siłach Zbrojnych RP – obejmuje również wspieranie polskich kontyngentów wojskowych oraz polskich jednostek zaangażowanych w misje pokojowe,
- CZC SZ – Centrum Zasobów Cyberprzestrzeni Sił Zbrojnych im. Mariana Rejewskiego w Warszawie, odpowiada za zapewnienie wymaganych zasobów oraz usług potrzebnych do utrzymania systemów teleinformatycznych oraz jego rozwoju, realizuje inwestycje oraz remonty z zakresu infrastruktury informatyki i telekomunikacji,
- RCI Bydgoszcz – Regionalne Centrum Informatyki Bydgoszcz w Bydgoszczy, odpowiada przede wszystkim za utrzymanie między innymi następujących elementów: systemy teleinformatyczne, systemy transmisyjne, sieci transmisji danych, łączność radiową, łączność radioliniową oraz satelitarną, a Centrum odpowiada za region czterech województw: kujawsko-pomorskiego, wielkopolskiego, zachodniopomorskiego oraz pomorskiego,
- RCI Gdynia – Regionalne Centrum Informatyki Gdynia w Gdyni, odpowiedzialne jest za te same systemy co RCI Gdynia, dodatkowo zajmuje się obserwacją techniczną oraz zabezpieczeniem działań jednostek wojskowych na morzu i lądzie, odpowiada przede wszystkim za funkcjonowanie systemów łączności Centrum Operacji Morskich - Dowództwa Komponentu Morskiego,
- RCI Kraków – Regionalne Centrum Informatyki Kraków w Krakowie, pełni bliźniacze podstawowe zadania do pozostałych RCI, a obszarem odpowiedzialności jest sześć województw: małopolskie, śląskie, łódzkie, mazowieckie, świętokrzyskie, lubelskie oraz podkarpackie,
- RCI Olsztyn – Regionalne Centrum Informatyki Olsztyn w Olsztynie, a zakres zadań jest tożsamy z pozostałymi RCI. Obejmuje następujące województwa: warmińsko-mazurskie, podlaskie, mazowieckie, lubelskie, współpracuje z 16 i 18 Dywizją Zmechanizowaną oraz 1 Dywizją Piechoty Legionów,

- RCI Warszawa – Regionalne Centrum Informatyki Warszawa w Warszawie, pełni zadania bliźniacze do pozostałych RCI, odpowiada za resort obrony narodowej,
- RCI Wrocław – Regionalne Centrum Informatyki Wrocław we Wrocławiu, odpowiada za realizację zadań tożsamych pozostałym RCI na obszarze następujących województw: dolnośląskie, lubuskie, łódzkie, opolskie, śląskie, wielkopolskie,
- WBZC – Wojskowe Biuro Zarządzania Częstotliwościami im. płk. Mieczysława Ornatowskiego w Warszawie jest odpowiedzialna za organizację oraz dostęp do widma elektromagnetycznego oraz zarządza częstotliwościami. Dodatkowo zapewnia bezpieczne warunki do niezakłóconego korzystania z wojskowych systemów radioelektronicznych,
- JDC „A" – Jednostka Działań w Cyberprzestrzeni „A" w Białobrzegach, przeznaczenie: prowadzenie operacji w cyberprzestrzeni,
- JDC „B" – Jednostka Działań w Cyberprzestrzeni „B" w Gdyni, przeznaczenie: prowadzenie operacji w cyberprzestrzeni,
- JDC „C" – Jednostka Działań w Cyberprzestrzeni „C" we Wrocławiu, przeznaczenie: prowadzenie operacji w cyberprzestrzeni,
- JWD – Jednostka Wsparcia Działań Dowódcy KWOC w Legionowie – przeznaczenie: zabezpieczenie systemu dowodzenia i łączności.

Cyber LEGION jest programem mającym umożliwić specjalistom z dziedziny IT połączenie służby wojskowej z pracą na rynku cywilnym. 9 maja 2025 r. pierwsza dwudziestka ekspertów złożyła w ramach programu przysięgę wojskową, stając się żołnierzami rezerwy Wojsk Obrony Cyberprzestrzeni. W ramach Cyber LEGIONU znajdują się między innymi takie projekty jak:

- Cyber-GYM – ćwiczenia w gronie najlepszych specjalistów z dziedziny IT,
- Nie tylko A(rmia) – przeznaczony dla specjalistów mających inną kategorię zdrowia niż A,
- Hack the Army – atakowanie-testowanie rządowych systemów bezpieczeństwa w kontrolowanych warunkach,
- E-Sport – rozwój sztucznej inteligencji na potrzeby obronne oraz techniki dronowe (Pawłowska, 2025).

W 2024 r. odnotowano 600 tysięcy zgłoszeń incydentów zagrażających cyberbezpieczeństwu Polski (mniej więcej 300 dziennie). Raport ABW opublikowany w maju 2025 r., określa jako jednego z agresorów rosyjską grupę APT28. Świadczy to o prowadzeniu szeroko zakrojonej kampanii hybrydowej ze strony Federacji Rosyjskiej przeciw Polsce. Mimo tylu codziennych zagrożeń polscy specjaliści z dziedziny cyberbezpieczeństwa odnoszą sukcesy i są światową czołówką. Świadczyć o tym może zajęcie drugiego miejsca przez zespół fińsko-polski w ćwiczeniach Locked Shields 2024. Generał Molenda (Dowódca KWOC) podkreśla znaczenie sztucznej inteligencji w kwestii cyberobrony (Davidson, b.d.).

Podsumowanie

Do skutecznej cyberobrony wymagane jest połączenie zdolności technologicznych, organizacyjnych oraz prawnych podmiotów, które jest zwieńczone jasną strategią odstraszania potencjalnych agresorów w cyberprzestrzeni. Takie działania realizowane w Siłach Zbrojnych RP gwarantują wysoki stopień odporności i możliwości przeciwdziałania w obszarze cyberprzestrzeni. Polski system cyberobrony skonsolidowany jest głównie przez program CYBER.MIL.PL, w składzie którego jedną z najważniejszych funkcji pełnią Wojska Obrony Cyberprzestrzeni. Natomiast powstanie Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni jest zasadniczym krokiem w komasacji tego bezpieczeństwa w Siłach Zbrojnych RP w obszarach związanych z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT.

NATO oraz Unia Europejska nadają cyberbezpieczeństwu rangę strategiczną, o czym świadczy szereg przepisów z tej dziedziny obligujących państwa członkowskie do spełniania ich wytycznych. Przyszłość kolektywnej obrony państw wyżej wskazanych struktur opiera się przede wszystkim na współpracy państw członkowskich realizowanej poprzez wymianę doświadczeń, kształtowanie specjalistów zdolnych do reagowania na aktualne zagrożenia oraz tworzenie coraz nowszych metod podnoszących bezpieczeństwo cybernetyczne.

Literatura

1. Banasik, M., Parafianowicz, R. (2015). Teoria i praktyka działań hybrydowych. *Zeszyty Naukowe AON, 2*(99), 5-25.
2. Ganuza, N. (2020). *Cyber defense handbook: Guidelines for the design, planning, implementation and development of a military cyber defense.* Inter-American Defense Board.
3. Kiera, J. (2023). Wojna informacyjna jako instrument polityki zagranicznej Federacji Rosyjskiej – wprowadzenie. *Studia Politicae Universitatis Silesiensis, 36/37*, 51-69. https://doi.org/10.31261/spus.16882
4. MSWiA, MON, RCB. (2025). *Poradnik bezpieczeństwa*.
5. Soloch, P., Pietrzak, P. (2016). Szczyt NATO w Warszawie: Uwarunkowania, rezultaty, wnioski dla Polski. *Bezpieczeństwo Narodowe, I-IV*, 13-33.
6. Szymańska, N. (2023). Dezinformacja jako narzędzie manipulacji medialnej. *Roczniki Studenckie Akademii Wojsk Lądowych, 7*, 39-49.
7. Tyson, D. (2007). *Security convergence: Managing enterprise security risk.* Butterworth-Heinemann.
8. Wachowicz, M. J. (2019). Ujęcie teoretyczne pojęcia dezinformacji. *Wiedza Obronna*, *1-2*, 226-253. https://doi.org/10.34752/x40y-nc78

Akty prawne

1. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825).
2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560).
3. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. z 2018 r. poz. 1806).
4. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. z 2018 r. poz. 2180).
5. Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu

informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. z 2018 r. poz. 2080).
6. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999).
7. Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1952).
8. Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. z 2018 r. poz. 1831).

Netografia

1. Davidson, R. (b.d.). *Między strategią a promocją: Polska cyberobrona w świetle zarządzania ryzykiem.* Davidson Consulting. Pobrane z: https://www.davidson.pl/post/miedzy-strategia-a-promocja-polska-cyberobrona-w-swietle-zarzadzania-ryzykiem (dostęp: 12.02.2026).
2. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni. (b.d.). *Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni.* Pobrane z: https://www.cyber.mil.pl/ncbc-dkwoc (dostęp: 12.02.2026).
3. Gwoździewicz, S., Sadowski, S., Szyłkowska, M. (2024a). *Cyberbezpieczeństwo. Encyklopedia Bezpieczeństwa Narodowego.* Pobrane z: https://encyklopedia.revite.pl/articles/view/123 (dostęp: 12.02.2026).
4. Gwoździewicz, S., Sadowski, S., Szyłkowska, M. (2024b). *Cyberprzestrzeń. Encyklopedia Bezpieczeństwa Narodowego.* Pobrane z: https://encyklopedia.revite.pl/articles/view/124 (dostęp: 12.02.2026).
5. Gwoździewicz, S., Sadowski, S., Szyłkowska, M. (2024c). *Cyberzagrożenie. Encyklopedia Bezpieczeństwa Narodowego.* Pobrane z: https://encyklopedia.revite.pl/articles/view/127 (dostęp: 12.02.2026).
6. Ministerstwo Cyfryzacji. (b.d.). *Krajowy system cyberbezpieczeństwa.* Pobrane z: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa--rozwiewamy-watpliwosci-przedsiebiorcow (dostęp: 12.02.2026).

7. NATO. (2016, 8 lipca). *Cyber Defence Pledge.* Pobrane z: https://www.nato.int/cps/en/natohq/official_texts_133177.htm (dostęp: 12.02.2026).
8. Pawłowska, A. (2025). Zostań cyberlegionistą! Wojsko rusza z nowym programem. *Polska Zbrojna.* Pobrane z: https://polska-zbrojna.pl/home/articleshow/43793?t=Zostan-cyberlegionista-Wojsko-rusza-z-nowym-programem (dostęp: 12.02.2026).
9. PAP. (2025). *Drony nad Polską wywołały falę dezinformacji: Eksperci zweryfikowali fakty i obalili teorie spiskowe.* Pobrane z: https://www.pap.pl/aktualnosci/drony-nad-polska-wywolaly-fale-dezinformacji-eksperci-zweryfikowali-fakty-i-teorie (dostęp: 12.02.2026).
10. Rada Unii Europejskiej. (2024). *Szczyt NATO w Warszawie, 8-9.7.2016*. Pobrane z: https://www.consilium.europa.eu/pl/meetings/international-summit/2016/07/08-09 (dostęp: 12.02.2026).
11. Rada Unii Europejskiej. (b.d.). *Cyberobrona.* Pobrane z: https://www.consilium.europa.eu/pl/policies/cyber-defence (dostęp: 12.02.2026).
12. MON. (b.d.). *Służba Kontrwywiadu Wojskowego.* Pobrane z: https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzba-kontrwywiadu-wojskowego (dostęp: 12.02.2026).
13. Wojska Obrony Cyberprzestrzeni. (b.d.). *Wojska Obrony Cyberprzestrzeni.* Pobrane z: https://www.cyber.mil.pl/wojska-obrony-cyberprzestrzeni (dostęp: 12.02.2026).
14. Wojsko Polskie. (b.d.). *O nas.* Pobrane z: https://www.wojsko-polskie.pl/woc/kadra (dostęp: 12.02.2026).
15. Zetter, K. (2018). Stuxnet: *Początek ataku na infrastrukturę krytyczną świata. Wszystko Co Najważniejsze*. Pobrane z: https://wszystkoconajwazniejsze.pl/kim-zetter-stuxnet (dostęp: 12.02.2026).

Marta Chodyka[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_7

CYBERODPORNOŚĆ SYSTEMÓW GRANICZNYCH

CYBER RESILIENCE OF BORDER SYSTEMS

Streszczenie

Celem rozdziału jest opracowanie i uzasadnienie referencyjnego modelu cyberodporności systemów granicznych (BORDER-CyRes), który integruje działania w obszarze prewencji, detekcji, reagowania i odtwarzania w wymiarze technicznym, organizacyjnym i proceduralnym. Problem badawczy sformułowano: w jaki sposób projektować i operacjonalizować cyberodporność systemów teleinformatycznych wspierających ochronę granic, aby zapewnić jednocześnie ciągłość odprawy, bezpieczeństwo informacji oraz skuteczną koordynację działań międzyinstytucjonalnych w warunkach rosnących zagrożeń cybernetycznych? Przyjęto hipotezę, że zastosowanie zintegrowanego modelu cyberodporności opartego na podejściu warstwowym, łączącego rozwiązania techniczne, organizacyjne i proceduralne oraz uwzględniającego wymagania regulacyjne i realne profile zagrożeń, umożliwia zwiększenie zdolności systemów granicznych do utrzymania funkcji krytycznych i szybkiego odtworzenia działania po incydencie. W badaniach zastosowano metody badawcze, w tym analizę normatywną aktów prawnych i standardów, analizę danych wtórnych i raportów dotyczących zagrożeń cybernetycznych oraz walidację

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl

scenariuszową modelu w odniesieniu do wybranych typów incydentów, takich jak ataki DDoS, ransomware oraz incydenty łańcucha dostaw. Uzyskane wyniki wskazują, że zaproponowany model cyberodporności umożliwia systematyczne projektowanie architektury bezpieczeństwa, usprawnienie procesów reagowania na incydenty oraz lepsze dopasowanie mechanizmów ochrony do specyfiki środowiska granicznego, co może wspierać zarówno praktykę operacyjną instytucji granicznych, jak i dalsze badania nad bezpieczeństwem infrastruktury krytycznej.

Słowa kluczowe: cyberodporność, ochrona granic, EES, interoperacyjność, SOC, CSIRT, NIS2, Zero Trust, reagowanie na incydenty

Abstract

The aim of the chapter is to develop and justify a reference model of cyber resilience for border systems (BORDER-CyRes), which integrates activities in the areas of prevention, detection, response, and recovery across the technical, organisational, and procedural dimensions. The research problem was formulated as follows: how to design and operationalise the cyber resilience of ICT systems supporting border protection to ensure the continuity of check-in, information security, and effective coordination of interinstitutional activities in the face of growing cyber threats? It was hypothesised that the use of an integrated cyber resilience model based on a layered approach, combining technical, organisational, and procedural solutions, and accounting for regulatory requirements and real-world threat profiles, enables border systems to maintain critical functions and quickly recover from incidents. The research used methods including normative analysis of legal acts and standards, analysis of secondary data and reports on cyber threats, and scenario validation of the model for selected incident types, such as DDoS attacks, ransomware, and supply chain incidents. The results indicate that the proposed cyber resilience model enables the systematic design of security architecture, the improvement of incident response processes, and the better adaptation of protection mechanisms to the specifics of the border environment, thereby supporting both the operational practice of border institutions and further research on the security of critical infrastructure.

Keywords: cyber resilience, border management, EES, interoperability, SOC, CSIRT, NIS2, Zero Trust, incident response

Wstęp

Cyfrowa transformacja zarządzania granicami zewnętrznymi UE materializuje się m.in. poprzez wdrażanie Systemu Wjazdu/Wyjazdu (EES) jako elementu „Smart Borders", zastępującego tradycyjne stemplowanie paszportów elektronicznymi zapisami oraz wykorzystującego dane biometryczne

w procesie kontroli. Równolegle rośnie rola systemów zarządzanych przez eu-LISA oraz komponentów interoperacyjności, które – łącząc wcześniej rozdzielone bazy – wzmacniają zdolność wykrywania oszustw tożsamości i zagrożeń bezpieczeństwa, ale jednocześnie zwiększają złożoność architektury oraz „promień rażenia" incydentów cybernetycznych. W praktyce oznacza to, że cyberincydent nie jest już problemem pojedynczej aplikacji „na granicy", lecz może obejmować: urządzenia i sensory w terenie (w tym OT), łączność i lokalne zasoby punktu odpraw, systemy krajowe i międzyresortowe, zależności usługowe i prawne wobec komponentów UE, partnerów (dostawcy urządzeń biometrycznych, integratorzy, operatorzy telekomunikacyjni, podmioty portowe i lotniskowe).

Problem badawczy niniejszego opracowania koncentruje się na tym, w jaki sposób projektować i operacjonalizować cyberodporność systemów teleinformatycznych wspierających ochronę oraz zarządzanie granicami, tak aby przy wysokiej presji czasowej i rygorystycznych wymogach dostępności usług (w szczególności w procesach odprawy) zapewnić jednocześnie bezpieczeństwo informacji, w tym ochronę danych biometrycznych, ciągłość świadczenia usług, interoperacyjność rozwiązań oraz skoordynowane reagowanie pomiędzy instytucjami, przy zachowaniu obowiązków raportowania i wymogów zarządzania kryzysowego. W tym kontekście rozdział odpowiada na trzy komplementarne pytania badawcze: po pierwsze, jakie mechanizmy techniczne i organizacyjne są krytyczne dla cyberodporności „systemu systemów" granicy w ujęciu cyklu prewencja–detekcja–reakcja–odtwarzanie, po drugie, w jaki sposób integrować workflow reagowania na incydenty w środowisku międzyinstytucjonalnym z wymaganiami raportowania oraz koordynacji na poziomie krajowym i unijnym, w tym z logiką ścieżki „24-72-30 dni", po trzecie, jakie mierniki oraz kryteria priorytetyzacji umożliwiają przełożenie danych o krajobrazie zagrożeń (m.in. kampanii DDoS, naruszeń danych, incydentów ransomware) na decyzje architektoniczne i operacyjne właściwe dla środowiska granicznego.

Celem badawczym jest opracowanie referencyjnego modelu cyberodporności systemów granicznych (BORDER-CyRes) oraz jego walidacja w oparciu o dane sektorowe i ponadsektorowe, a także scenariusze incydentów, prowadzące do sformułowania rekomendacji wdrożeniowych adresowanych do instytucji granicznych oraz ekosystemu podmiotów

współpracujących. Podjęcie tematu uzasadniają dane wskazujące na wysoką presję zagrożeń w administracji publicznej w UE: raporty ENISA konsekwentnie klasyfikują sektor publiczny jako jeden z najczęściej atakowanych, przy dominacji incydentów wpływających na dostępność (w szczególności kampanii DDoS) oraz istotnym udziale naruszeń danych. Ponieważ funkcje graniczne należą do obszarów o wysokiej krytyczności dla państwa, podatność ta ma wymiar nie tylko informacyjny, lecz także operacyjny, społeczny i polityczny – zakłócenia odpraw mogą prowadzić do powstawania kolejek i przerw w świadczeniu usług, generować konsekwencje reputacyjne, a także eskalować koszty i ryzyka wtórne, co wzmacnia potrzebę podejścia systemowego do cyberodporności w ujęciu międzyinstytucjonalnym.

Przegląd literatury

W literaturze inżynierii systemów pojęcie „systemu systemów" odnosi się do konfiguracji, w której spójne zdolności operacyjne powstają wskutek współdziałania wielu względnie autonomicznych systemów składowych, zarządzanych i rozwijanych niezależnie, a jednak powiązanych wspólną misją i zależnościami informacyjnymi oraz usługowymi. W tym ujęciu infrastruktura ICT granicy ma strukturę z natury rozproszoną i wielowarstwową: obejmuje warstwę brzegową (sensory oraz urządzenia rejestrujące i weryfikacyjne), warstwę lokalnej infrastruktury punktu granicznego (sieci, stanowiska odpraw, serwisy wspólne), warstwę centralnych systemów krajowych, a w warunkach europejskich również integrację z wielkoskalowymi systemami informacyjnymi oraz komponentami interoperacyjności (Wojciechowska-Filipek, Ciekanowski, 2019; Parlament Europejski i Rada UE, 2019). Taka topologia powoduje, że ryzyko cybernetyczne nie jest własnością pojedynczej aplikacji „na granicy", lecz ma charakter end-to-end: awaria lub kompromitacja jednego elementu może propagować się przez zależności transakcyjne, tożsamościowe i sieciowe, oddziałując na ciągłość odprawy i skuteczność realizacji zadań państwa (ENISA, 2024).

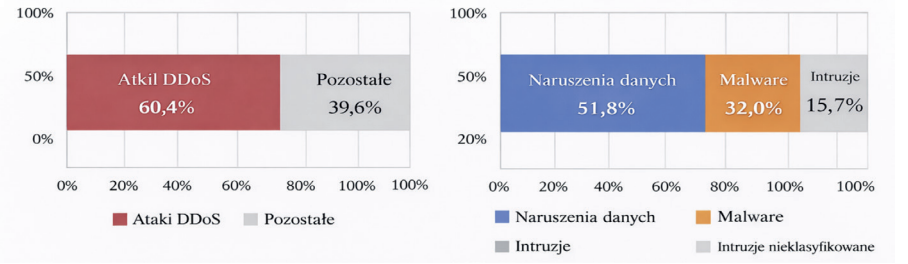
Istotnym tłem systemowym jest europejskie zintegrowane zarządzanie granicami, rozwijane m.in. w ramach mandatu Frontex, który wzmacnia wymiar współdziałania operacyjnego i informacyjnego pomiędzy podmiotami krajowymi oraz poziomem unijnym (Ciekanowski i in., 2022; Parlament Europejski i Rada UE, 2019). Równolegle eu-LISA pełni rolę agencji

odpowiedzialnej za operacyjne zarządzanie wybranymi wielkoskalowymi systemami IT w obszarze wolności, bezpieczeństwa i sprawiedliwości, co sprzyja odchodzeniu od modelu „silosowego" na rzecz ekosystemu integrującego systemy tożsamościowe i migracyjne w skali UE (Parlament Europejski i Rada UE, 2018c, Parlament Europejski i Rada UE, 2019b). W rezultacie interoperacyjność staje się nie tylko zagadnieniem integracji technicznej, lecz także trwałą własnością architektoniczną, która musi łączyć wymagania dostępności i wydajności operacyjnej z reżimami ochrony danych, kontroli dostępu oraz audytowalności działań (Parlament Europejski i Rada UE, 2019; ENISA, 2024). W tym sensie cyberodporność w środowisku granicznym powinna być projektowana jako zdolność ekosystemu do utrzymania kluczowych funkcji pomimo incydentów oraz do kontrolowanego odtwarzania i adaptacji, przy jednoczesnym zachowaniu spójności międzyinstytucjonalnej (ENISA, 2024). Dodatkową cechą infrastruktury granicznej jest współobecność komponentów klasy IT oraz OT (np. bramki i systemy kontroli dostępu, urządzenia peryferyjne, nadzoru wideo, a niekiedy także elementy łączności kryzysowej), co wymusza równoległe uwzględnienie odmiennych reżimów utrzymaniowych i modeli ryzyka (Ciekanowski, 2020; NIST, 2024). Z perspektywy praktyk bezpieczeństwa oznacza to konieczność łączenia mechanizmów typowych dla IT (np. zarządzanie tożsamością i dostępem, centralizacja i korelacja logów, detekcja i reakcja na stacjach roboczych) z wymaganiami charakterystycznymi dla OT, takimi jak twarde utwardzanie konfiguracji, dopuszczanie oprogramowania oparte o listy dozwolone, restrykcyjna kontrola łączności oraz podejście do aktualizacji uwzględniające krytyczność ciągłości działania (NIST, 2024, ENISA, 2024). W literaturze i zaleceniach podkreśla się przy tym, że w środowiskach, gdzie OT pełni funkcje krytyczne, priorytetem bywa bezpieczeństwo operacyjne i przewidywalność pracy systemu, co wymaga starannego projektowania segmentacji, izolacji domen oraz procedur reagowania tak, aby nie doprowadzić do niekontrolowanej degradacji procesów kluczowych (NIST, 2024).

Wdrażanie unijnego Systemu Wjazdu/Wyjazdu (EES) ma wymierny charakter operacyjny, ponieważ wiąże się z przejściem od tradycyjnych praktyk rejestracji do elektronicznego zapisu zdarzeń granicznych oraz wykorzystania danych biometrycznych w procesie kontroli (Parlament Europejski i Rada UE, 2017). W polskich realiach Straż Graniczna komunikuje

etapowe uruchamianie rozwiązań oraz stopniowe gromadzenie danych biometrycznych (wizerunek twarzy i odciski palców) w okresie przejściowym, co dodatkowo wzmacnia presję na dostępność usług w czasie odprawy (Straż Graniczna, 2025). Konsekwencje dla cyberodporności są wprost dwutorowe: po pierwsze, rośnie znaczenie zdolności do utrzymania ciągłości odprawy przy zakłóceniach i ograniczeniach przepustowości, a po drugie, wzmacnia się waga ochrony danych wrażliwych, w tym danych biometrycznych, których przetwarzanie w czasie rzeczywistym zwiększa wymagania dotyczące integralności, poufności oraz rozliczalności operacji (Parlament Europejski i Rada UE, 2017; ENISA, 2024; Straż Graniczna, 2025).

Dane sektorowe dla administracji publicznej UE – istotne także dla funkcji granicznych realizowanych przez podmioty publiczne – wskazują na dominację incydentów uderzających w dostępność usług. Analiza ENISA dla sektora administracji publicznej identyfikuje 586 publicznie raportowanych incydentów w okresie styczeń-grudzień 2024 i pokazuje, że ataki DDoS stanowią ponad 60% zdarzeń, co silnie akcentuje potrzebę odporności na zakłócenia dostępności usług (ENISA, 2026). W tej samej analizie, w grupie incydentów związanych z „intrusion-related" skutkami udanych włamań, największy udział mają naruszenia danych (51,8%), a następnie malware (~32%) oraz intruzje nieklasyfikowane (15,7%), co wzmacnia wniosek, że cyberodporność granicy nie może być redukowana do ochrony perymetrycznej, lecz wymaga dojrzałego zarządzania tożsamością, ciągłego monitoringu zdarzeń, detekcji nadużyć oraz zdolności odzyskiwania po naruszeniu – zwłaszcza przy przetwarzaniu danych wrażliwych (ENISA, 2026; NIST, 2024). Szersze ujęcie krajobrazu zagrożeń – obejmujące okres od około połowy 2023 do połowy 2024 – potwierdza utrzymywanie się priorytetów takich jak zagrożenia dla dostępności i ransomware oraz wskazuje na rolę czynników geopolitycznych i wzrost aktywności aktorów ukierunkowanych na efekt widoczności i zakłóceń (ENISA, 2024). Jest to spójne z tezą, że infrastruktury publiczne stanowią atrakcyjny cel zarówno dla hacktywizmu nastawionego na zakłócanie usług, jak i dla cyberprzestępczości (w tym ransomware) oraz podmiotów o charakterze państwowym, realizujących cele szpiegowskie (cyberespionage) (ENISA, 2024; Verizon, 2025). Incydenty przedstawione zostały na Rysunku 1.



a) b)

Rysunek 1. Incydenty cybernetyczne w sektorze administracji publicznej UE, styczeń – grudzień 2024, N = 586 z podziałem na a) incydenty na dostępność usług, b) incydenty „intrusion-related"

Źródło: opracowanie własne na podstawie ENISA, 2026.

Perspektywa ponadsektorowa dodatkowo wzmacnia znaczenie czynników organizacyjnych i łańcucha dostaw. W podsumowaniu raportu Verizon DBIR 2025 wskazano stabilny udział „czynnika ludzkiego" na poziomie około 60%, wzrost udziału naruszeń angażujących strony trzecie z 15% do 30% oraz wzrost udziału naruszeń o motywacji szpiegowskiej do 17% (Verizon, 2025). W kontekście systemów granicznych ma to szczególne znaczenie, ponieważ ekosystem techniczny granicy jest silnie zależny od dostawców urządzeń (w tym urządzeń biometrycznych), integratorów oraz operatorów usług infrastrukturalnych (łączność, serwis, oprogramowanie), a zatem ryzyko cybernetyczne ma w dużej mierze charakter współdzielony i łańcuchowy (Chodyka i in., 2025; Verizon, 2025; ENISA, 2024). Jednocześnie metryki czasu wykrycia (dwell time) wskazują, że w incydentach ransomware „okno czasowe" na przerwanie łańcucha zdarzeń może być operacyjnie krótkie, a wykrycie wewnętrzne potrafi być istotnie opóźnione, co podnosi wymagania wobec automatyzacji detekcji, segmentacji środowiska oraz gotowości do odtwarzania (Mandiant, 2025). W konsekwencji, wyniki analiz sektorowych i ponadsektorowych prowadzą do spójnego wniosku projektowego: cyberodporność systemów granicznych powinna w równym stopniu obejmować inżynierię dostępności (w tym odporność na przeciążenia i degradację), zarządzanie tożsamością i dostępem, obserwowalność zdarzeń oraz zdolności odtworzeniowe, jak i mechanizmy organizacyjne związane z zarządzaniem dostawcami, koordynacją międzyinstytucjonalną oraz gotowością proceduralną do działania pod presją czasu (ENISA, 2026; Verizon, 2025; Mandiant, 2025).

Metodologia

Badanie zrealizowano w paradygmacie design science research (DSR), ukierunkowanym na zaprojektowanie i ocenę artefaktu rozwiązującego problem praktyczno-inżynierski. Artefaktem jest referencyjny model cyberodporności systemów granicznych BORDER-CyRes, ujmowany jako spójny zestaw: konstruktów (role i zdolności), relacji (zależności warstw „systemu systemów"), mechanizmów technicznych i organizacyjnych oraz procedur operacyjnych (m.in. workflow reagowania i odtwarzania). Przyjęto iteracyjną logikę DSR (wymagania, projekt, walidacja) oraz triangulację przesłanek, aby model równoważył wymagania zgodności i interoperacyjności z realnym profilem zagrożeń i ograniczeniami wdrożeniowymi środowiska granicznego.

Przeprowadzono analizę normatywno-regulacyjną, wyprowadzając wymagania dla cyberodporności z obowiązków zarządzania ryzykiem i raportowania incydentów w logice 24-72-30 (Parlament Europejski i Rada UE, 2022) oraz z implementacyjnych wskazówek dot. środków zarządzania ryzykiem (ENISA, 2026). NIS2 przewiduje: early warning ≤24 h, incident notification ≤72 h, raport pośredni na żądanie CSIRT/organu oraz raport końcowy nie później niż 1 miesiąc po notyfikacji (plus szczególny reżim dla incydentów trwających). Równolegle uwzględniono ramy instytucjonalne i architektoniczne zarządzania granicami oraz interoperacyjności (w tym Frontex i eu-LISA) (Parlament Europejski i Rada UE, 2018a; Parlament Europejski i Rada UE, 2019), a także wymagania wynikające z EES w zakresie przetwarzania danych identyfikacyjnych i biometrycznych (Parlament Europejski i Rada UE, 2017) oraz krajowe uwarunkowania etapowego wdrożenia EES (Straż Graniczna, 2025). Rezultatem tego strumienia był zestaw wymagań zgodności obejmujący m.in. raportowanie, interoperacyjność, ochrona danych biometrycznych oraz ciągłość odprawy jako usługi krytycznej. Następnie wykonano syntetyczny przegląd ram praktyk, traktując cyberodporność jako cykl prewencji–detekcji–reakcji–odtwarzania. Do porządkowania rezultatów i mapowania zdolności użyto NIST CSF 2.0 (z uwzględnieniem specyfiki IT/OT), a do projektowania pokrycia detekcyjnego i reakcyjnego – taksonomii MITRE ATT&CK oraz zasad architektonicznych Zero Trust (NIST, 2024; MITRE, 2025; Rose i in., 2020). Priorytety modelu

skalibrowano następnie na podstawie danych wtórnych i metryk operacyjnych, zestawiając wnioski z raportów ENISA (w tym sektorowych dla administracji publicznej oraz horyzontalnych TL) (ENISA, 2024; ENISA, 2026) z danymi ponadsektorowymi (Verizon, 2025) oraz metrykami czasu wykrycia i dynamiki ransomware (Mandiant, 2025). W kolejnym kroku artefakt zwalidowano scenariuszowo (DDoS, ransomware, łańcuch dostaw), stosując BORDER-CyRes jako „szablon decyzyjny" i oceniając go kryteriami: RTO/RPO, MTTD/MTTR, zgodność z raportowaniem 24-72-30, minimalizacja ryzyka naruszeń danych (zwłaszcza biometrycznych) oraz wykonalność w rozproszonym środowisku IT/OT (Parlament Europejski i Rada UE, 2017; Parlament Europejski i Rada UE, 2022; NIST, 2024). Ograniczenia wynikają z charakteru danych wtórnych i zależności od praktyk raportowania (ENISA, 2024; ENISA, 2026). Zasady etyczne i ochrony danych zapewniono przez wykorzystanie informacji publicznych i zagregowanych oraz projektowanie scenariuszy bez przetwarzania rzeczywistych danych osobowych, w tym biometrycznych (Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

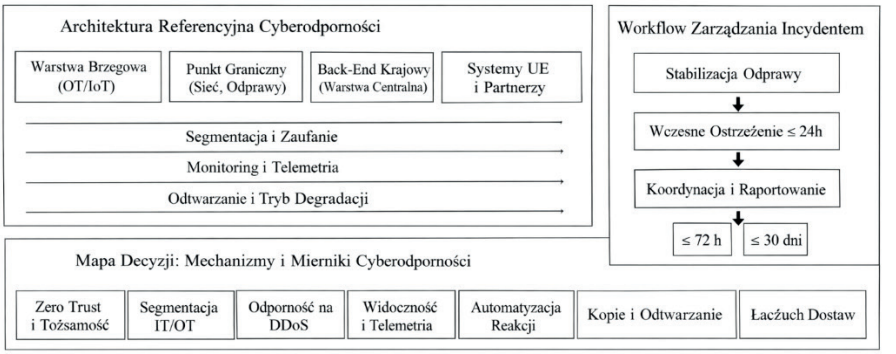
Wyniki

Wyniki prac projektowych w paradygmacie design science research materializują się w trzech komplementarnych artefaktach:

- architekturze referencyjnej cyberodporności,
- operacyjnym workflow zarządzania incydentem z mapowaniem na obowiązki raportowe oraz koordynację krajową i unijną,
- wdrożeniowej „mapie decyzji" w postaci zestawu mechanizmów wraz z miernikami i odniesieniami do ram referencyjnych.

Z perspektywy walidacji użyteczności, artefakty te zostały osadzone w realiach środowiska granicznego „systemu systemów" oraz zilustrowane na przykładzie drogowego przejścia granicznego Terespol–Brześć jako reprezentatywnego punktu odprawy ruchu osobowego, w którym priorytetem operacyjnym jest utrzymanie ciągłości odprawy przy jednoczesnej ochronie danych wrażliwych, w tym danych identyfikacyjnych i biometrycznych przetwarzanych w ramach EES (Elak i in., 2024; Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

W celu syntetycznego przedstawienia zależności pomiędzy trzema artefaktami modelu BORDER-CyRes – architekturą referencyjną, workflow reagowania na incydent oraz mapą decyzji wdrożeniowych – opracowano zintegrowany schemat koncepcyjny. Rysunek 2 przedstawia relacje pomiędzy warstwami techniczną, operacyjną oraz decyzyjno-wdrożeniową w ujęciu całościowym, ilustrując sposób przejścia od struktury systemu granicznego do mechanizmów reakcji oraz do zestawu mechanizmów i mierników implementacyjnych.



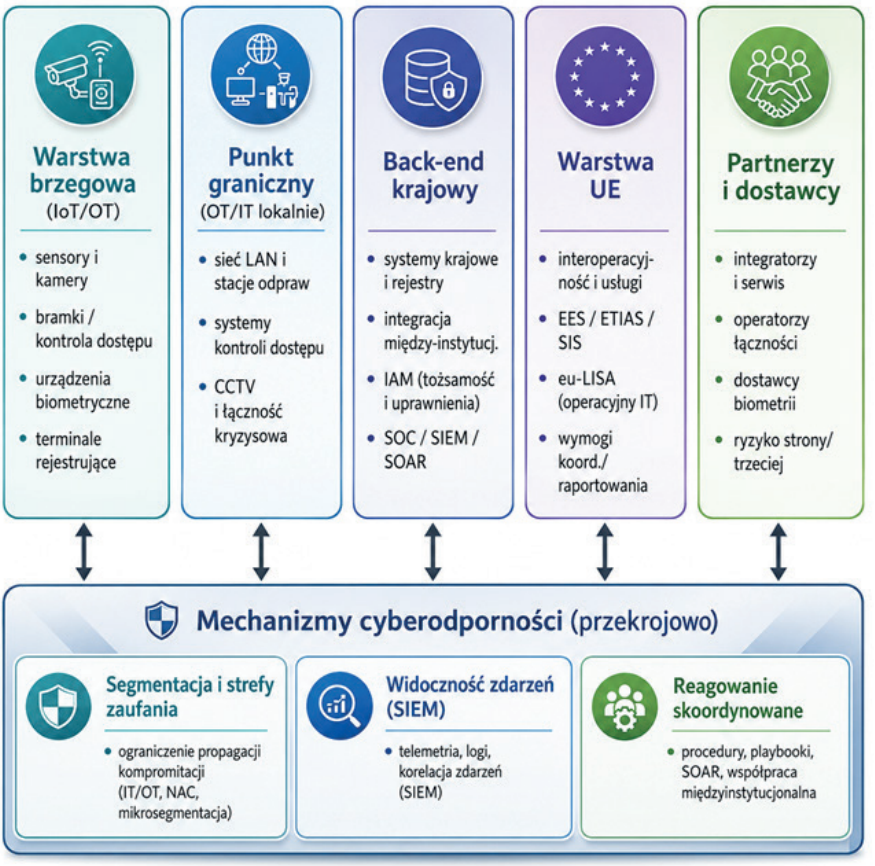
Rysunek 2. Relacje pomiędzy warstwą techniczną, operacyjną oraz decyzyjno-wdrożeniową

Źródło: opracowanie własne.

W części górnej przedstawiono architekturę referencyjną jako układ warstw: warstwę brzegową (OT/IoT), punkt graniczny (infrastruktura lokalna), warstwę centralną (back-end krajowy) oraz integrację z systemami UE i partnerami. W części środkowej zobrazowano workflow reagowania w logice „podwójnego rytmu", łączącej stabilizację operacyjną odprawy z równoległym uruchomieniem ścieżki raportowej 24-72-30. Część dolna przedstawia mapę decyzji – zestaw mechanizmów technicznych i organizacyjnych, które przekładają wnioski analityczne na działania wdrożeniowe. Takie trójwarstwowe ujęcie pozwala interpretować cyberodporność nie jako zbiór izolowanych zabezpieczeń, lecz jako powiązany system zależności pomiędzy architekturą, operacjami oraz governance. W instancji dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że decyzje architektoniczne (np. segmentacja IT/OT) są bezpośrednio sprzężone z procedurami reagowania (np. izolacja segmentu w czasie ≤24 h) oraz z obowiązkami raportowymi

i koordynacyjnymi. W dalszej części rozdziału przedstawiono kolejno: architekturę referencyjną jako wynik pierwszy, workflow zarządzania incydentem jako wynik drugi oraz mapę decyzji i mechanizmy wdrożeniowe jako wynik trzeci.

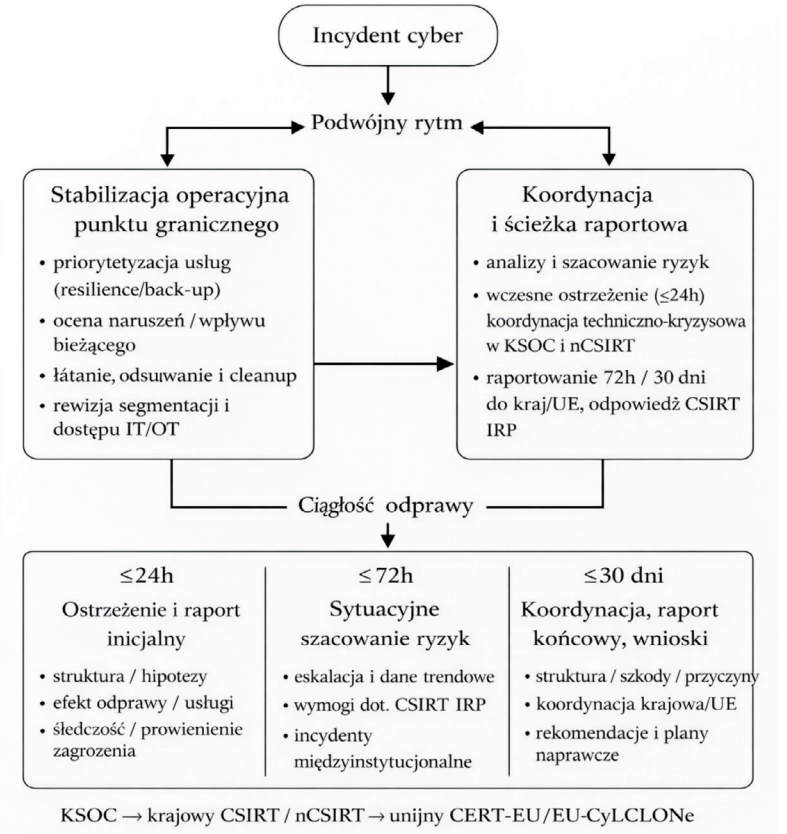
Pierwszym wynikiem jest architektura referencyjna, która traktuje granicę jako rozproszony ekosystem „end-to-end": od urządzeń i komponentów brzegowych (w tym OT/IoT), przez lokalną infrastrukturę punktu granicznego (sieć, stanowiska odpraw, usługi wspólne), po warstwę back-endu krajowego (tożsamość, monitoring, odtwarzanie), interoperacyjność i wielkoskalowe systemy UE oraz zależności partnerów i dostawców. Logika tej architektury została przedstawiona na Rysunku 3.



Rysunek 3. Ekosystem teleinformatyczny ochrony granic

Źródło: opracowanie własne.

Jej kluczowym założeniem jest projektowanie cyberodporności nie jako zbioru izolowanych kontroli, lecz jako własności systemu zdolnego do utrzymania funkcji krytycznych mimo incydentu oraz do kontrolowanego odtworzenia po zakłóceniu (NIST, 2024; NIST, 2021). W instancji dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że krytyczne punkty kontrolne cyberodporności nie są skoncentrowane wyłącznie „w centrali", lecz rozkładają się wzdłuż całego łańcucha odprawy: od warstwy brzegowej (urządzenia weryfikacyjne i rejestracyjne, urządzenia wspierające kontrolę), przez segmentację i kontrolę dostępu w sieci lokalnej, po centralne zdolności IAM oraz SOC/SIEM/SOAR i mechanizmy odtwarzania. Szczególny nacisk położono na ograniczanie propagacji kompromitacji poprzez segmentację i strefy zaufania, zwiększanie obserwowalności poprzez telemetrię, logi i korelację, a także na zdolność do odtworzenia i pracy w trybie degradacji, co jest spójne z priorytetyzacją dostępności i ciągłości działania w środowiskach krytycznych (NIST, 2024, ENISA, 2024). Wymiar „end-to-end" obejmuje również zależności zewnętrzne: model zakłada, że ryzyko w punkcie granicznym jest współdzielone z dostawcami technologii, serwisu i łączności, a zatem musi być zarządzane w sposób systemowy (Verizon, 2025, ENISA, 2024). Uzasadnieniem tej części architektury są dane DBIR wskazujące na wzrost udziału naruszeń angażujących strony trzecie (z 15% do 30%), co przekłada się na konieczność formalizacji wymagań bezpieczeństwa wobec dostawców i kontroli kanałów serwisowych w środowiskach granicznych (Verizon, 2025). Drugim wynikiem jest workflow reagowania na incydent, który integruje logikę operacyjną odprawy z obowiązkami raportowania i koordynacji. Mechanizm ten został przedstawiony na Rysunku 4 i opiera się na założeniu „podwójnego rytmu" działań.

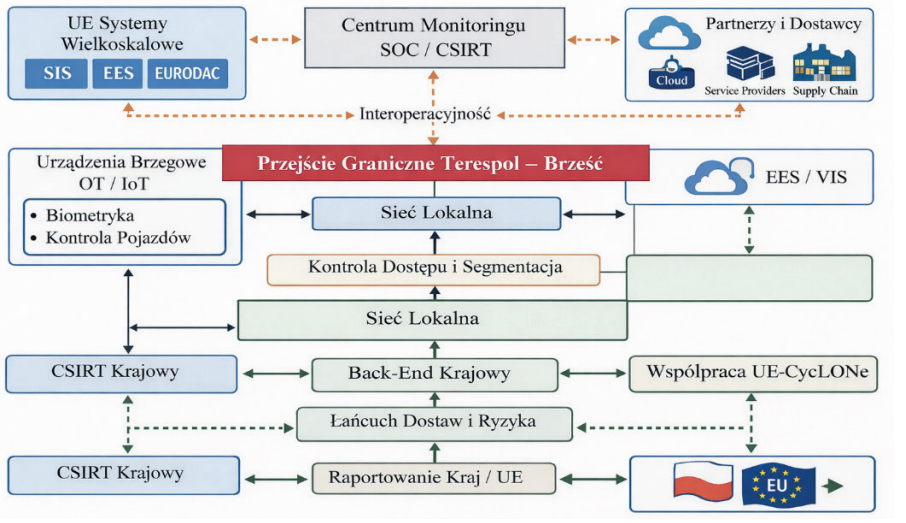


Rysunek 4. Mechanizm zarządzania incydentami cyber

Źródło: opracowanie własne.

Pierwszy rytm to natychmiastowa stabilizacja usług w punkcie granicznym, rozumiana jako utrzymanie ciągłości odprawy poprzez priorytetyzację usług, ograniczanie skutków, izolację segmentów oraz działania typu cleanup i przywracanie stanu operacyjnego. Drugi rytm to równoległe budowanie obrazu sytuacji oraz uruchomienie ścieżki eskalacyjno-raportowej w logice 24-72-30 dni, wymaganej przez NIS2 (Parlament Europejski i Rada UE, 2022). W konsekwencji etap „wczesne ostrzeżenie ≤24h" nie jest w modelu traktowany jako czynność następcza wobec działań technicznych, lecz jako proces uruchamiany równolegle, ponieważ w środowisku granicznym szybka eskalacja ma bezpośredni wpływ na zdolność do utrzymania odprawy oraz na ograniczenie ryzyka wtórnego. Dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że decyzje o przejściu w tryb degradacji,

uruchomieniu łączy zapasowych, wdrożeniu reguł mitigacji DDoS czy izolacji segmentu nie są wyłącznie decyzjami lokalnymi. Wymagają one wczesnej koordynacji z właściwymi strukturami krajowymi (w tym SOC/CSIRT) oraz – w razie potrzeby – kanałami współpracy na poziomie UE, aby zapewnić spójność reakcji w ekosystemie interoperacyjnym (Parlament Europejski i Rada UE, 2022; ENISA, 2024; ENISA, 2026). Takie ujęcie jest szczególnie istotne w warunkach nadreprezentacji incydentów wpływających na dostępność (zwłaszcza DDoS) w sektorze administracji publicznej w UE, gdzie opóźnienie eskalacji może bezpośrednio przełożyć się na długotrwałe zakłócenie usług granicznych i utratę kontroli nad dynamiką incydentu (ENISA, 2024; ENISA, 2026). Logika workflow jest zgodna z podejściem do obsługi incydentów jako procesu obejmującego równolegle identyfikację, ograniczanie, usuwanie skutków i odtwarzanie, uzupełnionego o wymagania raportowe oraz zarządzanie informacją o incydencie (Nelson i in., 2025; Parlament Europejski i Rada UE, 2022). Trzecim wynikiem jest zestawienie danych i przesłanek, które uzasadniają priorytety mechanizmów cyberodporności, a następnie ich syntetyzacja w formie wdrożeniowej mapy decyzji. Mapa ekosystemu teleinformatycznego ochrony granic Terespol–Brześć przedstawiona została na Rysunku 5.



Rysunek 5. Ekosystem teleinformatyczny ochrony granic Terespol–Brześć

Źródło: opracowanie własne.

Dane sektorowe ENISA dla administracji publicznej UE wskazują dominację incydentów wpływających na dostępność (DDoS > 60% zdarzeń w analizowanym zbiorze), co wspiera priorytet inżynierii dostępności i odporności sieci, w tym zdolności do kontrolowanej degradacji usług (ENISA, 2026). Jednocześnie w grupie incydentów intrusion-related największy udział stanowią naruszenia danych (51,8%), co wzmacnia potrzebę wzmocnienia zarządzania tożsamością i dostępem oraz monitoringu i korelacji zdarzeń (ENISA, 2026; NIST, 2024). Wreszcie metryki czasu wykrycia i charakterystyka incydentów ransomware (dwell time) wskazują, że brak wykrycia wewnętrznego może oznaczać długotrwałą obecność intruza, co zwiększa ryzyko współwystąpienia zakłóceń operacyjnych i naruszeń danych, a tym samym uzasadnia nacisk na automatyzację reakcji, segmentację oraz gotowość odtworzeniową (Mandiant, 2025). W ujęciu instancji dla drogowego przejścia granicznego Terespol–Brześć priorytety te mają konsekwencje bezpośrednie: wysoka wrażliwość odprawy na niedostępność usług powoduje, że mechanizmy dostępności i degradacji muszą być projektowane „w pierwszej kolejności", a dopiero następnie uzupełniane o pełne spektrum kontroli poufności i integralności, jednocześnie przetwarzanie danych identyfikacyjnych i biometrycznych (EES) wymusza wzmocnienie rozliczalności dostępu i obserwowalności, ponieważ potencjalny wpływ naruszenia jest istotny zarówno prawnie, jak i operacyjnie (Parlament Europejski i Rada UE, 2017; ENISA, 2024; Straż Graniczna, 2025). Syntetycznym wyrazem trzeciego wyniku jest Tabela 1, przygotowana w wariancie dopasowanym do instancji Terespol.

Tabela 1. Mapa decyzji BORDER-CyRes – priorytetowe zdolności, minimalny zakres wdrożenia i mierniki (instancja: drogowe przejście graniczne Terespol–Brześć)

Priorytet	Zdolność (co)	Minimalny zakres wdrożenia (co konkretnie wdrożyć – MVP)	Jak mierzyć (2–3 wskaźniki)	Właściciel / warstwa	Odniesienia (skrót)
P1	Dostępność + „degraded border ops”	Ochrona anty-DDoS (np. rate-limiting/ scrubbing), redundancja łączy, procedura pracy w degradacji (minimalny zestaw funkcji odprawy, priorytety kolejek), test przełączenia	Dostępność usług (%), czas przełączenia (min), przepustowość w degradacji (% normy)	Centrala + przejście + operator łączności	ENISA PA TL, NIS2 (ciągłość)
P1	Tożsamość i dostępy uprzywilejowane	MFA dla operatorów i adminów, PAM dla kont uprzywilejowanych, zasada najmniejszych uprawnień, eliminacja kont współdzielonych	% kont uprzywilejowanych z MFA, liczba kont „shared”, czas odebrania uprawnień (h)	Back-end krajowy + stanowiska odpraw	NIST ZT, NIS2
P1	Segmentacja IT/OT + kontrola dostępu do sieci (NAC)	Podział na strefy (stanowiska odpraw, urządzenia brzegowe/biomet., strefa serwisowa), reguły komunikacji „tylko konieczne”, NAC dla urządzeń, szybka procedura izolacji segmentu	Liczba dozwolonych połączeń między strefami, czas izolacji segmentu (min), % urządzeń objętych NAC	Punkt graniczny (LAN) + centrala	NIST ZT, CIS v8
P1	Widoczność (logi + EDR) i korelacja zdarzeń	Centralizacja logów z przejścia, EDR na stacjach odpraw, spójne identyfikatory transakcji odprawy, korelacja w SIEM	Pokrycie logowania (% systemów krytycznych), MTTD (czas wykrycia), odsetek alarmów wysokiej trafności	SOC/SIEM (kraj) + przejście	NIST CSF 2.0
P1	Odtwarzanie po ransomware (kopie niezmienialne + obrazy stacji)	Kopie immutable (offline/odseparowane), testy odtworzeń, „golden images” stanowisk odpraw, runbook „clean restore”	RTO/RPO dla usług odprawy, % udanych testów odtworzeń, czas odtworzenia stanowiska (min/h)	Back-end krajowy + przejście	NIST 800-160, M-Trends

Priorytet	Zdolność (co)	Minimalny zakres wdrożenia (co konkretnie wdrożyć – MVP)	Jak mierzyć (2–3 wskaźniki)	Właściciel / warstwa	Odniesienia (skrót)
P2	Automatyzacja reakcji (playbooki)	Gotowe playbooki: blokada konta, izolacja hosta, odcięcie segmentu, reguły firewall, szybkie „zamrożenie zmian" na przejściu, półautomatyczna obsługa IOC	Czas od alarmu do akcji, % incydentów obsłużonych playbookiem, MTTR (czas przywrócenia)	SOC/CSIRT + lokalne procedury	NIST IR (800-61)
P2	Łańcuch dostaw i serwis (third-party)	Wymagania bezpieczeństwa w umowach, kontrola kanałów serwisowych, rejestr dostawców krytycznych, kontrola aktualizacji (okna serwisowe), SBOM tam, gdzie możliwe	% dostawców ocenionych, czas usunięcia podatności (dni), liczba incydentów third-party	Centrala + dostawcy	DBIR, ENISA
P2	Raportowanie i koordynacja (24h/72h/1 miesiąc)	Szablony zgłoszeń, jedno „case management", RACI (kto decyduje o degradacji/komunikuje/raportuje), ćwiczenia (DDoS, ransomware, supply chain)	Czas do „wczesnego ostrzeżenia" (h), kompletność zgłoszenia (% pól), liczba ćwiczeń/rok	Kierownictwo + CSIRT + przejście	NIS2, EU-CyCLON

Źródło: opracowanie własne.

Tabela ma charakter mapy decyzji wdrożeniowych. Zestawia priorytetowe zdolności cyberodporności w instancji dla drogowego przejścia granicznego Terespol–Brześć, definiując minimalny zakres wdrożeniowy (MVP) oraz mierniki umożliwiające weryfikację skuteczności. Priorytety P1 obejmują mechanizmy bezpośrednio warunkujące ciągłość odprawy i ograniczenie „blast radius", natomiast P2 uzupełniają zdolności automatyzacji, zarządzania dostawcami oraz zgodności raportowej i koordynacyjnej. Zastosowanie praktyczne modelu BORDER-CyRes w instytucji granicznej, w tym na przykładzie drogowego przejścia granicznego Terespol–Brześć, wymaga równoległego potraktowania trzech płaszczyzn: architektury technicznej, operacji bezpieczeństwa oraz governance i zgodności. W płaszczyźnie architektonicznej punktem startowym jest formalna identyfikacja usług krytycznych odprawy jako wątków misji (np. transakcja weryfikacji i transakcja rejestracji danych w logice EES) oraz ich zależności, a następnie przypisanie parametrów ciągłości RTO/RPO. Takie podejście jest spójne z definicją cyberodporności jako redukcji ryzyka misji zależnej od zasobów cybernetycznych i pozwala projektować mechanizmy degradacji w sposób kontrolowany, zamiast ad hoc (NIST, 2021; NIST, 2024). W płaszczyźnie operacyjnej kluczowe jest ustanowienie zdolności detekcji i reakcji (SOC/CSIRT) z automatyzacją playbooków oraz zapewnienie wysokiej jakości telemetryki z punktu granicznego. Presja czasowa obserwowana w incydentach ransomware oraz ryzyko długotrwałej obecności intruza uzasadniają inwestycje w skrócenie MTTD i MTTR oraz w możliwość szybkiej izolacji segmentu bez wywołania niekontrolowanej degradacji odprawy (Mandiant, 2025; Nelson i in., 2025). W płaszczyźnie zarządczej niezbędne jest zbudowanie schematu decyzyjnego i odpowiedzialności (RACI) dla działań krytycznych, w szczególności: kto podejmuje decyzję o przejściu w tryb „degraded border ops", kto raportuje incydent w logice 24-72-30, a kto odpowiada za komunikację do interesariuszy, co jest wymagane zarówno przez NIS2, jak i przez specyfikę środowiska międzyinstytucjonalnego (Parlament Europejski i Rada UE, 2022).

Wymiar międzyinstytucjonalny i transgraniczny stanowi w modelu odrębną oś ryzyka. Cyberodporność przejścia granicznego jest wrażliwa na „pęknięcia zaufania" między podmiotami o różnych mandatach, dojrzałości i kanałach komunikacji, co wzmacnia potrzebę standaryzacji wymiany

informacji oraz wspólnych ćwiczeń operacyjnych obejmujących zarówno DDoS, ransomware, jak i incydenty łańcucha dostaw (ENISA, 2024, ENISA, 2026). W ujęciu unijnym mechanizmy koordynacyjne (w tym EU-CyCLONe) wspierają zarządzanie dużymi incydentami i budowę wspólnej świadomości sytuacyjnej, natomiast w ujęciu praktycznym przekłada się to na konieczność posiadania „pakietu interoperacyjności cyber": uzgodnionych formatów IOC, bezpiecznych kanałów wymiany, zdefiniowanych punktów kontaktu oraz procedur szybkiego potwierdzania wpływu incydentu na ciągłość odprawy. Z perspektywy Terespola oznacza to, że gotowość do współdziałania musi obejmować zarówno warstwę techniczną (telemetria i wymiana IOC), jak i proceduralną (eskalacja i raportowanie), ponieważ incydent może oddziaływać wzdłuż zależności kraj-UE (Parlament Europejski i Rada UE, 2018b; Parlament Europejski i Rada UE, 2019a; Parlament Europejski i Rada UE, 2022).

Osadzenie w realiach Polski wymaga uwzględnienia krajowego systemu cyberbezpieczeństwa i relacji z CSIRT-ami poziomu krajowego, a także praktyk współpracy w incydentach krytycznych (Sejm Rzeczypospolitej Polskiej, 2018). W praktyce konsekwencją dla projektowania cyberodporności przejścia granicznego jest utrzymywanie stałych kanałów eskalacji i wymiany informacji o zagrożeniach, włączanie scenariuszy DDoS, ransomware i supply chain do cyklu ćwiczeń (w tym testów przełączenia na „degraded mode"), a także konsekwentne wzmacnianie ochrony tożsamości i kont uprzywilejowanych, co jest spójne zarówno z logiką Zero Trust (Rose i in., 2020), jak i z obserwacjami dotyczącymi czynnika ludzkiego i third-party w naruszeniach (Verizon, 2025). Dodatkowo, etapowe wdrażanie EES i związane z nim obciążenia operacyjne oraz przetwarzanie danych biometrycznych wzmacniają wymagania dotyczące dostępności, integralności i rozliczalności w okresie przejściowym, co powinno być uwzględnione w parametryzacji RTO/RPO i w projektowaniu trybów degradacji odprawy (Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

Wnioski

Rozdział odpowiada na problem projektowania i operacjonalizacji cyberodporności systemów granicznych w warunkach „systemu systemów", proponując i uzasadniając referencyjny model BORDER-CyRes.

Zasadniczym wkładem jest integracja trzech perspektyw: architektonicznej (warstwowy ekosystem end-to-end), operacyjnej (workflow reagowania w logice „podwójnego rytmu") oraz wdrożeniowej (mapa decyzji: mechanizmy–mierniki–ramy). Taka konstrukcja umożliwia przejście od opisu środowiska granicznego jako układu zależności kraj–UE–partnerzy do spójnego zestawu decyzji projektowych i operacyjnych, które mogą być mierzone i testowane w praktyce. W ujęciu aplikacyjnym kluczowym wnioskiem jest to, że cyberodporność przejścia granicznego – zilustrowana na przykładzie drogowego przejścia granicznego Terespol–Brześć wymaga traktowania ciągłości odprawy jako funkcji krytycznej, której utrzymanie musi być zapewniane równolegle z ochroną danych wrażliwych, w tym danych biometrycznych przetwarzanych w logice EES (European Commission, 2025; Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025). Oznacza to konieczność projektowania mechanizmów nie tylko w kategoriach prewencji, ale także jako zdolności do kontrolowanej degradacji i odtworzenia przy zachowaniu sterowności procesu odprawy. Priorytetyzację mechanizmów w modelu uzasadniają dane wskazujące na dominację incydentów wpływających na dostępność (w szczególności DDoS) w sektorze administracji publicznej UE oraz istotny udział naruszeń danych i incydentów ransomware, co potwierdza potrzebę równoczesnego wzmacniania odporności dostępnościowej, obserwowalności i gotowości odtworzeniowej (ENISA, 2024; ENISA, 2026; Mandiant, 2025). Drugim wnioskiem jest to, że skuteczna cyberodporność przejścia granicznego wymaga spójnego sprzężenia decyzji architektonicznych z procedurami operacyjnymi i obowiązkami raportowymi. Model pokazuje, że działania takie jak segmentacja IT/OT, wzmocnienie tożsamości i uprzywilejowanych dostępów czy automatyzacja reakcji nie mają wyłącznie charakteru „technicznego", determinują one wykonalność utrzymania odprawy w incydencie oraz zdolność do spełnienia wymogów raportowania i koordynacji, w tym sekwencji 24-72-30 dni (NIST, 2024; Parlament Europejski i Rada UE, 2022). W konsekwencji, etap „wczesnego ostrzeżenia ≤24h" powinien być interpretowany jako element równoległy wobec stabilizacji operacyjnej, ponieważ uruchomienie koordynacji i ścieżki raportowej wpływa na dostęp do zasobów reakcyjnych oraz na tempo działań systemowych (np. mitigacja, izolacja segmentu, przełączenia), a tym samym na ciągłość odprawy (Nelson i in., 2025; Parlament Europejski i Rada UE, 2022).

Kolejnym wnioskiem jest znaczenie ryzyka ekosystemowego, w szczególności zależności od podmiotów trzecich. W środowisku granicznym istotna część ryzyka ma charakter współdzielony z dostawcami technologii, integratorami i operatorami usług, co wzmacnia potrzebę ujęcia łańcucha dostaw jako pełnoprawnego obszaru cyberodporności, a nie komponentu pobocznego (Verizon, 2025; ENISA, 2024). Wymaga to formalizacji wymagań, kontroli kanałów serwisowych oraz testowania scenariuszy supply chain w cyklu ćwiczeń, zwłaszcza w punktach granicznych o wysokiej krytyczności operacyjnej.

Ograniczenia zaprezentowanego ujęcia wynikają, po pierwsze, z wykorzystania danych wtórnych, które odzwierciedlają obraz zagrożeń zależny od praktyk raportowania i dostępności informacji, co może wpływać na obserwowany rozkład klas incydentów (ENISA, 2024; ENISA, 2026). Po drugie, walidacja scenariuszowa – mimo że wzmacnia wykonalność wniosków – nie zastępuje weryfikacji wdrożeniowej w konkretnej architekturze organizacyjnej i technicznej (NIST, 2024). Dodatkowo, instancja dla przejścia Terespol–Brześć ma charakter referencyjny. Szczegółowe parametry (np. wartości RTO/RPO, progi przełączeń, docelowe mierniki MTTD/MTTR) wymagają doprecyzowania w oparciu o lokalne uwarunkowania przepustowości, topologii łączności, modelu odpowiedzialności oraz reżimu utrzymaniowego (NIST, 2021, NIST, 2024). Z perspektywy dalszych badań zasadne jest rozszerzenie walidacji o studia przypadków w różnych typach przejść (drogowych osobowych vs towarowych, lotniczych, kolejowych) oraz o pomiar dojrzałości wdrożeń w kategoriach NIST CSF 2.0 i Zero Trust, z jednoczesnym uwzględnieniem wymogów interoperacyjności i danych biometrycznych EES (NIST, 2024; Rose i in., 2020; Parlament Europejski i Rada UE, 2017). W kontekście NIS2 kierunkiem rozwojowym jest doprecyzowanie metryk i minimalnych artefaktów dowodowych (case management, logi, audyt integralności) tak, aby skracać czas uzyskania wiarygodnego obrazu sytuacji i wspierać koordynację kraj-UE w incydentach o dużej skali (Parlament Europejski i Rada UE, 2022; Nelson i in., 2025).

Literatura

1. Chodyka, M., Żurawski, S., Parczewska, W. (2025). Wpływ cyberzagrożeń na bezpieczeństwo granicy Rzeczypospolitej Polskiej. W: D. Brążkiewicz, M. Chodyka, T. Grudniewski, S. Żurawski (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część druga* (s. 295-307). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103236_188
2. Ciekanowski, Z. (2020). Straż graniczna w sytuacjach kryzysowych. W: Z. Ciekanowski (red.), *Państwo wobec zagrożeń* (s. 256-268). Wydawnictwo Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej. https://hdl.handle.net/20.500.13044/691
3. Ciekanowski, Z., Nowicka, J., Żurawski, S. (2022). Frontex w systemie zarządzania bezpieczeństwem granic Unii Europejskiej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 8*(2), 176-186. https://doi.org/10.34739/dsd.2022.02.12
4. Elak, L., Oskierko, M., Żurawski, S. (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
5. ENISA. (2024). *ENISA Threat Landscape 2024*. Pobrane z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 12.02.2026).
6. ENISA. (2025*). ENISA Sectorial Threat Landscape: Public Administration*. Pobrane z: https://www.enisa.europa.eu/publications/sectorial-threat-landscape-public-administration (dostęp: 12.02.2026).
7. European Commission. (2025). *Entry/Exit System (EES)*. Pobrane z: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en (dostęp: 12.02.2026).
8. Mandiant. (2025). *M-Trends 2025 report.* Pobrane z : https://services.google.com/fh/files/misc/m-trends-2025-en.pdf#page=1&zoom=auto,-263,792 (dostęp: 12.02.2026).
9. MITRE. (2025). *MITRE ATT&CK knowledge base.*
10. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

11. Nelson, A., Rekhi, S., Souppaya, M., Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
12. Parlament Europejski i Rada UE. (2017). *Rozporządzenie (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające System Wjazdu/Wyjazdu (EES)* (Dz. Urz. UE L 327 z 9.12.2017).
13. Parlament Europejski i Rada UE. (2018a). *Rozporządzenie (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)* (Dz. Urz. UE L 236 z 19.09.2018).
14. Parlament Europejski i Rada UE. (2018b). *Rozporządzenie (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (eu-LISA)* (Dz. Urz. UE L 295 z 21.11.2018).
15. Parlament Europejski i Rada UE. (2018c). *Rozporządzenie (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych* (Dz. Urz. UE L 312 z 7.12.2018).
16. Parlament Europejski i Rada UE. (2019a). *Rozporządzenie (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w dziedzinie granic i wiz* (Dz. Urz. UE L 135 z 22.05.2019).
17. Parlament Europejski i Rada UE. (2019b). *Rozporządzenie (UE) 2019/1896 z dnia 13 listopada 2019 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej* (Dz. Urz. UE L 295 z 14.11.2019).
18. Parlament Europejski i Rada UE. (2022). *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii* (Dz. Urz. UE L 333 z 27.12.2022).
19. Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). *Zero trust architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

20. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
21. Sejm Rzeczypospolitej Polskiej. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1550).
22. Straż Graniczna. (2025). *Entry/Exit System (EES) – informacje i wdrożenie w Polsce*.
23. Verizon. (2025). *2025 Data Breach Investigations Report*. Pobrane z: https://www.verizon.com/business/resources/reports/dbir/ (dostęp: 12.02.2026).
24. Wojciechowska-Filipek, S., Ciekanowski, Z. (2019). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*. CeDeWu.

Marcin Oskierko[1]
Państwowa Akademia Nauk Stosowanych w Chełmie
Aleksandra Żaneta Nasiadka[2]

https://doi.org/10.29316/9788368103373_8

ROLA WOJSK OBRONY TERYTORIALNEJ W OCHRONIE GRANICY PAŃSTWOWEJ W WARUNKACH KRYZYSU MIGRACYJNEGO – UJĘCIE SYSTEMOWE I PRAKTYCZNE

THE ROLE OF THE TERRITORIAL DEFENCE FORCES IN PROTECTING THE NATIONAL BORDER DURING A MIGRATION CRISIS – A SYSTEMIC AND PRACTICAL PERSPECTIVE

Streszczenie

Rozdział analizuje rolę Wojsk Obrony Terytorialnej (WOT) w systemie bezpieczeństwa narodowego Rzeczypospolitej Polskiej, ze szczególnym uwzględnieniem ich zadań w ochronie wschodniej granicy państwowej w warunkach zagrożeń hybrydowych i kryzysów migracyjnych. Celem rozdziału jest ukazanie miejsca i znaczenia WOT jako komponentu wspierającego zarówno podsystem obronny, jak i system

[1] https://orcid.org/0000-0003-3450-6037, e-mail: moskierko@panschelm.edu.pl
[2] https://orcid.org/0009-0008-3370-8503, e-mail: a.nasiadka97@gmail.com

bezpieczeństwa wewnętrznego, a także ocena ich praktycznego wkładu w zwiększanie odporności państwa na działania destabilizacyjne o charakterze pozamilitarnym i asymetrycznym. Główny problem badawczy sformułowano: w jakim stopniu obecny model funkcjonowania Wojsk Obrony Terytorialnej oparty na terytorialnym rozmieszczeniu, lokalnym zakorzenieniu oraz ścisłej współpracy z innymi służbami wpływa na skuteczność ochrony wschodniej granicy RP w warunkach presji migracyjnej i działań hybrydowych? W ramach analizy postawiono hipotezę badawczą, zgodnie z którą stała obecność WOT w Stałych Rejonach Odpowiedzialności, połączona z interoperacyjnością ze Strażą Graniczną i innymi służbami, istotnie zwiększa zdolność państwa do szybkiego reagowania na zagrożenia oraz ogranicza skutki prób destabilizacji bezpieczeństwa granicy. Badania przeprowadzono z wykorzystaniem metod jakościowych i ilościowych, obejmujących analizę aktów normatywnych regulujących funkcjonowanie Wojsk Obrony Terytorialnej, analizę danych statystycznych Komendy Głównej Straży Granicznej dotyczących nielegalnych przekroczeń granicy w latach 2021-2024, a także krytyczną analizę literatury przedmiotu z zakresu bezpieczeństwa narodowego, obrony terytorialnej i zagrożeń hybrydowych. Zastosowano również metodę analityczno-syntetyczną, pozwalającą na ujęcie WOT jako elementu zintegrowanego systemu reagowania kryzysowego. Przeprowadzona analiza prowadzi do wniosku, że Wojska Obrony Terytorialnej stanowią istotny czynnik wzmacniający odporność państwa na zagrożenia hybrydowe, zwłaszcza w obszarze ochrony granicy państwowej. Zaangażowanie w działania wspierające Straż Graniczną, elastyczność operacyjna oraz zdolność do szybkiego rozwinięcia sił w terenie przyczyniają się do zwiększenia skuteczności ochrony granicy i stabilności bezpieczeństwa wewnętrznego. Rozdział potwierdza zasadność dalszego rozwoju WOT jako trwałego filaru systemu bezpieczeństwa narodowego Polski.

Słowa kluczowe: Wojska Obrony Terytorialnej, bezpieczeństwo narodowe, granica wschodnia, zagrożenia hybrydowe, kryzys migracyjny

Abstract

The chapter analyses the role of the Territorial Defence Forces in the national security system of the Republic of Poland, with particular emphasis on their tasks in protecting the eastern state border amid hybrid threats and migration crises. The aim of the chapter is to show the place and importance of the Territorial Defence Forces as a component supporting both the defence subsystem and the internal security system, and to assess their practical contribution to increasing the state's resilience against destabilising, non-military, asymmetric activities. The main research problem was formulated: to what extent does the current model of the Territorial Defence Forces, based on territorial deployment, local roots, and close cooperation

with other services, affect the effectiveness of the protection of the eastern border of the Republic of Poland in the conditions of migratory pressure and hybrid activities? As part of the analysis, a research hypothesis was put forward, according to which the permanent presence of the Territorial Defence Forces in the Permanent Areas of Responsibility, combined with interoperability with the Border Guard and other services, significantly increases the state's ability to respond quickly to threats and reduces the effects of attempts to destabilise border security. The research was carried out using qualitative and quantitative methods, including the analysis of normative acts regulating the functioning of the Territorial Defence Forces, the analysis of statistical data of the Border Guard Headquarters on illegal border crossings in the years 2021-2024, as well as a critical analysis of the literature on the subject in the field of national security, territorial defence and hybrid threats. An analytical-synthetic method was also used, allowing for the recognition of WOT as an element of an integrated crisis response system. The analysis concludes that the Territorial Defence Forces are an important factor in strengthening the country's resilience to hybrid threats, especially in state border protection. Their commitment to supporting the Border Guard, operational flexibility, and ability to rapidly deploy ground forces enhance the effectiveness of border protection and the stability of internal security. The chapter confirms the legitimacy of further development of the Territorial Defence Forces as a permanent pillar of Poland's national security system.

Keywords: Territorial Defence Forces, national security, eastern border, hybrid threats, migration crisis

Wstęp

System bezpieczeństwa narodowego Rzeczypospolitej Polskiej opiera się na zintegrowanym działaniu podsystemu obronnego, którego trzon stanowią Siły Zbrojne RP. Ich zadaniem jest nie tylko obrona państwa przed agresją zewnętrzną, lecz także wspieranie administracji publicznej i społeczeństwa w sytuacjach kryzysowych oraz udział w międzynarodowych operacjach utrzymania pokoju. Współczesne środowisko bezpieczeństwa cechuje rosnąca złożoność i nieprzewidywalność zagrożeń, w tym o charakterze asymetrycznym i hybrydowym, co wymaga elastyczności i dostosowania zdolności obronnych do nowych wyzwań. Szczególne miejsce w tym systemie zajmują Wojska Obrony Terytorialnej (WOT) – piąty, odrębny rodzaj Sił Zbrojnych RP. Ich etapowe tworzenie, rozpoczęte w województwach wschodnich, było odpowiedzią na ocenę kierunków zagrożeń i potrzebę

wzmocnienia ochrony wschodniej granicy Polski, stanowiącej jednocześnie zewnętrzną granicę Unii Europejskiej i strefy Schengen. Rozmieszczenie brygad i kompanii lekkiej piechoty w powiatach oraz przypisanie im Stałych Rejonów Odpowiedzialności sprawiają, że WOT są stale obecne w terenie i gotowe do natychmiastowego działania, co znacząco zwiększa odporność państwa na sytuacje kryzysowe. Dynamiczny rozwój WOT zbiegł się z wystąpieniem nowych wyzwań bezpieczeństwa, takich jak kryzys migracyjny na granicy polsko-białoruskiej w 2021 r. i pełnoskalowa agresja Rosji na Ukrainę w 2022 r., która potwierdziła potrzebę wzmocnienia zdolności państwa do reagowania na zagrożenia hybrydowe i ochrony granicy. Udział żołnierzy WOT w operacjach „Silne Wsparcie" i „Bezpieczne Podlasie" pokazał, że formacja ta jest kluczowym elementem zarówno systemu obrony narodowej, jak i praktycznego wsparcia bezpieczeństwa wewnętrznego.

Celem rozdziału jest ukazanie roli i znaczenia Wojsk Obrony Terytorialnej w ochronie granicy państwowej oraz ocena ich skuteczności w reagowaniu na zagrożenia hybrydowe i kryzysy migracyjne. W rozdziale postawiono pytania o to, w jaki sposób działania WOT wpływają na podniesienie odporności państwa i jakie wnioski płyną z dotychczasowych działań. Przyjęto hipotezę, że stała obecność WOT w terenie znacząco zwiększa efektywność ochrony granicy i skraca czas reakcji na zagrożenia.

Badania przeprowadzono z zastosowaniem podejścia analityczno-syntetycznego, wykorzystując analizę danych statystycznych Komendy Głównej Straży Granicznej z lat 2021-2023, analizę aktów prawnych regulujących funkcjonowanie WOT, literaturę przedmiotu dotyczącą współczesnych zagrożeń bezpieczeństwa i koncepcji obrony terytorialnej. Takie podejście pozwala na kompleksową ocenę miejsca i znaczenia WOT w systemie bezpieczeństwa narodowego.

WOT jako element systemu bezpieczeństwa narodowego

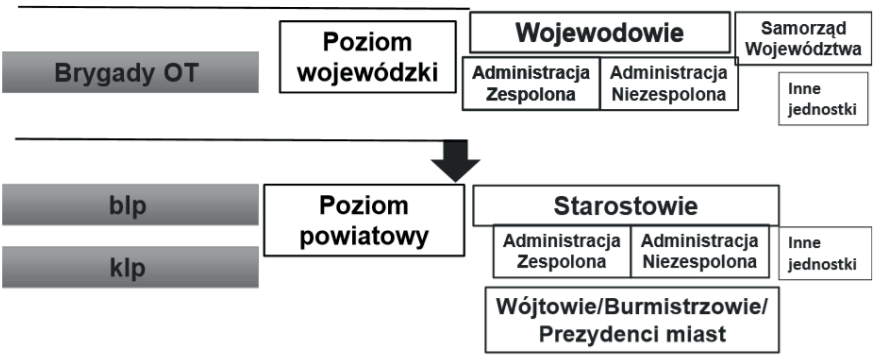
Siły Zbrojne RP są kluczowym elementem systemu bezpieczeństwa narodowego, funkcjonującym w ramach podsystemu obronnego i realizującym założenia polityki bezpieczeństwa oraz obrony państwa. Wraz ze zmianami w środowisku bezpieczeństwa rośnie również zakres powierzanych im zadań. Konieczność reagowania na zróżnicowane, w tym asymetryczne, zagrożenia wymusza elastyczność w planowaniu obronnym i regularną

aktualizację kluczowych założeń strategicznych. Dotyczy to zwłaszcza misji i zadań, które muszą być dostosowane do faktycznych możliwości i zdolności Sił Zbrojnych. W ostatnich latach obserwuje się odejście od tradycyjnego postrzegania bezpieczeństwa wyłącznie w kategoriach obrony przed agresją zbrojną – obecnie nacisk kładzie się przede wszystkim na zdolność wojska do przeciwdziałania różnorodnym, głównie niemilitarnym, zagrożeniom (Elak, 2020). Każde silne państwo powinno dysponować nowoczesnymi siłami zbrojnymi, które spełniają trzy kluczowe kryteria: wysoką sprawność, mobilność oraz interoperacyjność. Potencjał armii w istotny sposób wpływa na trwałość i stabilność państwa, stanowiąc jednocześnie gwarancję jego bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego (Oskierko, 2021). L. Elak podkreśla, że istotą nowoczesnych sił zbrojnych jest zdolność do zapewnienia obywatelom poczucia bezpieczeństwa poprzez szybkie reagowanie na zagrożenia, skuteczną obronę przed potencjalnym agresorem oraz umiejętność dostosowywania się do dynamicznie zmieniających się warunków środowiska bezpieczeństwa. Zgodnie z jego stanowiskiem, wojsko musi utrzymywać gotowość do realizacji trzech zasadniczych, konstytucyjnie określonych zadań: obrony państwa i przeciwdziałania agresji zbrojnej, wspierania organów państwowych w zakresie bezpieczeństwa wewnętrznego i niesienia pomocy społeczeństwu oraz uczestnictwa w działaniach międzynarodowych mających na celu stabilizację sytuacji i utrzymanie pokoju (Elak, 2020).

Wojska Obrony Terytorialnej, jako piąty odrębny rodzaj Sił Zbrojnych RP, rozpoczęły działalność 1 stycznia 2017 r. Ich powołanie zostało usankcjonowane ustawą z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Ustawa z dnia 16 listopada 2016 r., 2016), która stała się podstawą prawną ich funkcjonowania. Pierwsze brygady OT powstały na mocy decyzji nr PF-32/Org./SSG/ZOiU-P1 Ministra Obrony Narodowej z 24 maja 2016 r., wydanej w celu realizacji przedsięwzięć umożliwiających ich sformowanie. Decyzja ta była następstwem wcześniejszego rozstrzygnięcia – decyzji Z-7/MON z 12 maja 2016 r. w sprawie sformowania brygad obrony terytorialnej (Kwiatkowski, 2023). Proces tworzenia WOT był odpowiedzią na najbliższe i najbardziej realne zagrożenia dla bezpieczeństwa państwa, wynikające z geopolitycznego położenia Polski, w szczególności z sytuacji

bezpieczeństwa na wschodniej flance NATO i granicach Unii Europejskiej (Nastarowicz, 2017). Z tego powodu etapowy projekt formowania brygad oraz osiągania gotowości bojowej został zaplanowany w układzie terytorialnym – od wschodu na zachód kraju. Takie rozmieszczenie było ściśle powiązane z analizą kierunków możliwych zagrożeń i pozwalało na stopniowe „nawarstwianie" potencjału obronnego oraz osiąganie pełnej gotowości do działań w regionach najbardziej narażonych na destabilizację (Huzarski, 2017). Zdecydowano, że w pierwszym etapie priorytetem będzie sformowanie brygad na wschodnich terenach kraju, aby zapewnić skuteczną ochronę wschodnich granic Rzeczypospolitej, stanowiących jednocześnie zewnętrzną granicę UE i strefę Schengen. Takie rozmieszczenie miało na celu zarówno odstraszanie potencjalnego przeciwnika, jak i wzmocnienie zdolności reagowania w sytuacjach kryzysowych, w tym związanych z możliwymi falami migracyjnymi spowodowanymi konfliktami zbrojnymi na Bliskim Wschodzie lub w rejonie Europy Wschodniej (Nastarowicz, 2017).

W strukturze Sił Zbrojnych RP (Rysunek 1) Wojska Obrony Terytorialnej są ściśle powiązane z podziałem administracyjnym kraju. Na poziomie centralnym funkcjonuje Dowództwo WOT, które sprawuje kierownictwo nad całością formacji. W każdym województwie powstały brygady OT, a ich pododdziały – bataliony i kompanie lekkiej piechoty – rozmieszczono w poszczególnych powiatach. Podstawowym pododdziałem prowadzącym działania jest kompania lekkiej piechoty, która dzięki lokalnemu zakorzenieniu i znajomości terenu może szybko reagować na sytuacje kryzysowe w Stałych Rejonach Odpowiedzialności (SRO). Docelowo kompanie lekkiej piechoty mają funkcjonować we wszystkich powiatach kraju, zapewniając gotowość do realizacji zadań obronnych, wsparcia innych służb oraz działań na rzecz lokalnych społeczności (Wróbel, 2017).



Rysunek 1. Struktury Wojsk Obrony Terytorialnej i administracji publicznej w terenie

Źródło: Wróbel, 2017, s. 143.

W pierwszym etapie działalność rozpoczęły trzy brygady, których stałe rejony odpowiedzialności obejmowały wschodnie województwa kraju (Rysunek 2). 1. Brygada OT objęła swoim zasięgiem województwo podlaskie, 2. Brygada OT – województwo lubelskie, a 3. Brygada OT – województwo podkarpackie (Compa, 2020). Drugi etap, zaplanowany na lata 2017-2019, przewidywał utworzenie kolejnych trzech brygad, rozmieszczonych w województwach warmińsko-mazurskim oraz mazowieckim (gdzie powstały dwie brygady). W tym okresie rozpoczęto również proces formowania Centrum Szkolenia Wojsk Obrony Terytorialnej, Oddziału Zabezpieczenia oraz Batalionu Dowodzenia (Compa, 2020). W trzecim etapie, przypadającym na lata 2018-2020, zainicjowano formowanie siedmiu nowych brygad stacjonujących w województwach: małopolskim, śląskim, świętokrzyskim, łódzkim, wielkopolskim, kujawsko-pomorskim i pomorskim. Ostatni etap, realizowany w latach 2019-2021, miał na celu zakończenie prac planistyczno-koncepcyjnych dotyczących powołania czterech kolejnych brygad, tym razem w województwach: opolskim, dolnośląskim, lubuskim oraz zachodniopomorskim. Docelowo ustalono, że liczebność Wojsk Obrony Terytorialnej wyniesie około 53 tysięcy żołnierzy, co miało zapewnić ich pełną zdolność do realizacji zadań w całym kraju (Kukuła, 2024).



Rysunek 2. Mapa etapów tworzenia struktur WOT w Polsce
Źródło: Stachowski, 2017, s. 56.

Tak zbudowany potencjał i rozmieszczenie terytorialne sprawiają, że WOT stanowią integralną część systemu bezpieczeństwa narodowego. Istnienie i funkcjonowanie są w pełni zgodne z założeniami *Strategii Bezpieczeństwa Narodowego RP*, która wskazuje, że wobec różnorodności wyzwań i nieprzewidywalności zagrożeń system bezpieczeństwa musi być zdolny do wszechstronnej reakcji – zarówno na sytuacje lokalne, jak i te o zasięgu ogólnokrajowym. Strategia podkreśla również konieczność jego elastycznej adaptacji, tak aby umożliwić bieżące monitorowanie i prognozowanie zagrożeń, szybkie reagowanie na ich wystąpienie oraz rozwijanie zdolności do skutecznego usuwania skutków sytuacji kryzysowych. W tym kontekście WOT odgrywają kluczową rolę, stanowiąc formację stale obecną w terenie, zdolną do szybkiego reagowania i wspierania zarówno wojska operacyjnego jak i społeczności lokalnych w sytuacjach kryzysowych (MON, 2014).

Kryzys migracyjny jako element wojny hybrydowej

Nielegalna migracja stanowi poważne wyzwanie dla bezpieczeństwa wewnętrznego państwa. Ze względu na swój dynamiczny i trudny do przewidzenia charakter bywa postrzegana jako groźny element przepływów

migracyjnych. Kontrola ruchu granicznego osób przekraczających granicę jest jednym z kluczowych atrybutów suwerenności państwowej, dlatego nielegalne migracje traktowane są jako zagrożenie dla tej suwerenności i mogą osłabiać zdolność państwa do sprawowania skutecznej kontroli nad własnym terytorium i przestrzenią (Kukuła, 2022).

Pierwsze próby wykorzystania migracji jako narzędzia nacisku ze strony reżimu A. Łukaszenki miały miejsce już w 2002 r., gdy w końcowej fazie negocjacji akcesyjnych Polski do UE grożono masowym wpuszczeniem migrantów do Europy. Podobne groźby pojawiły się w latach 2010-2011, kiedy po zaostrzeniu sankcji unijnych strona białoruska zapowiedziała ograniczenie ochrony granicy z Polską, Litwą i Łotwą, koncentrując się na odcinku białorusko-ukraińskim. Towarzyszyła temu intensywna kampania medialna, a zdaniem dziennikarza T. Giczana, opracowana w tym czasie „Operacja Śluza" miała na celu wymuszenie na UE wsparcia finansowego na wzmocnienie granicy Białorusi (Oskierko, 2022).

Obecny kryzys migracyjny na zewnętrznych granicach Unii Europejskiej: polsko-białoruskich, litewsko-białoruskich oraz łotewsko-białoruskich wywołany był kryzysem politycznym związanym z wyborami prezydenckimi na Białorusi. W efekcie kolejnych sfałszowanych wyborów prezydenckich, które odbyły się 9 sierpnia 2020 r., A. Łukaszenka otrzymał 80,2% głosów. Na drugim miejscu, z poparciem 9,9%, uplasowała się jego główna kontrkandydatka – S. Cichanouska, która zaraz po ogłoszeniu wyborów w obawie przed prześladowaniami wyjechała na Litwę (Elak i in., 2024). Latem 2021 r. na granicy zewnętrznej UE z Białorusią pojawiło się nowe zjawisko określane mianem instrumentalizacji migracji. Ma on charakter złożony i wielopoziomowy. Instrumentalizacja migrantów polega na celowym wywoływaniu nieuregulowanych przepływów migracyjnych przez państwo trzecie, które zachęca obywateli innych krajów do przemieszczania się na jego terytorium lub w kierunku granic zewnętrznych UE, a następnie ułatwia ich dalszą migrację. Działania te mają na celu destabilizację państwa członkowskiego lub całej Unii i mogą zagrażać jej kluczowym funkcjom, w tym integralności terytorialnej, porządkowi publicznemu i bezpieczeństwu narodowemu (Nitszke, 2024). Tę metodę wykorzystał reżim Aleksandra Łukaszenki, aby sprawdzić zdolność Polski, Litwy i Łotwy do ochrony granic oraz przetestować skuteczność Unii Europejskiej w reagowaniu na

tego rodzaju kryzysy. Za sprowadzanie migrantów na Białoruś odpowiadała państwowa spółka Centr-kurort, kierowana bezpośrednio przez syna prezydenta Białorusi, Wiktara Łukaszenkę, współpracująca z biurami podróży w Iraku, Libii, Syrii i Turcji. Koszt tygodniowych wycieczek na Białoruś wynosił od 600 do 1000 dolarów.

Migranci przylatywali do Mińska z Bagdadu, Erbilu, Sulajmaniji, Bejrutu, Damaszku i Stambułu, gdzie podczas kontroli granicznej otrzymywali białoruskie wizy. Następnie przewożono ich autokarami do hoteli, a po kilku dniach białoruskie służby organizowały ich transport w rejon granicy (Konieczny, 2022). Jak zauważa białoruski dziennikarz Tadeusz Giczan, dla wielu Irakijczyków była to „najtańsza, najszybsza i najbezpieczniejsza droga do Unii Europejskiej" (PAP, 2024) w celu ubiegania się o azyl, podczas gdy wcześniej jedyną możliwością była wieloetapowa, ryzykowna podróż przez Turcję i Bałkany do Węgier, a następnie do Austrii i Niemiec. Droga ta była bardzo kosztowna, niebezpieczna i skomplikowana. Dzięki opracowanej przez reżim Łukaszenki turystycznej ofercie mogą bezpiecznie, komfortowo, szybko oraz bardzo tanio dostać się do Unii Europejskiej. Ponadto mają zapewnioną wszechstronną pomoc ze strony władz białoruskich (Oskierko, 2022).

Na podstawie analizy danych statystycznych udostępnionych przez Straż Graniczną dotyczących nielegalnych przekroczeń granicy na odcinku polsko-białoruskim można stwierdzić, że w latach 2018-2019 były to incydenty sporadyczne, obejmujące jedynie pojedyncze przypadki. Sytuacja uległa radykalnej zmianie w 2021 r., kiedy w wyniku działań reżimu A. Łukaszenki, polegających na organizowaniu i koordynowaniu przerzutu migrantów, odnotowano ponad 39 tys. prób nielegalnego przekroczenia granicy. W odpowiedzi na kryzys migracyjny w 2022 r. na granicy polsko-białoruskiej wybudowano zaporę graniczną, co znacząco ograniczyło skalę tego zjawiska – w 2022 r. zarejestrowano 576 prób nielegalnego przekroczenia granicy, a w 2023 r. 541 prób. Dane za pierwsze półrocze 2024 r. wskazują jednak na ponowny wzrost presji migracyjnej – Straż Graniczna ujawniła już 1571 przypadków prób nielegalnego przekroczenia granicy (Oskierko, Żurawski, 2024).

Zadania i formy zaangażowania WOT w ochronę granicy

Wojska Obrony Terytorialnej (WOT), jako piąty rodzaj Sił Zbrojnych RP, funkcjonują w ścisłym powiązaniu z podziałem administracyjnym kraju. Na poziomie centralnym działa Dowództwo WOT, w województwach – brygady, natomiast w powiatach rozmieszczone są bataliony i kompanie lekkiej piechoty. Kompania stanowi podstawowy pododdział prowadzący działania w Stałych Rejonach Odpowiedzialności (SRO), co zapewnia lokalne zakorzenienie, szybkie reagowanie na zagrożenia i bliską współpracę z lokalnymi społecznościami oraz samorządami (Wróbel, 2017).

Istotą funkcjonowania WOT jest ich „przypisanie" do określonych obszarów kraju, co pozwala na realizację dwóch zasadniczych aspektów funkcjonalnych: wsparcia wojsk operacyjnych („obrona") oraz wsparcia lokalnych społeczności („ochrona"). Zadania te rozpatrywane są w czasie pokoju, kryzysu i wojny, a ich szczegółowy zakres zależy od rodzaju i skali występujących zagrożeń (Michalak, 2017).

W czasie pokoju WOT tworzą bezpieczne środowisko operacyjne, prowadzą działania prewencyjne i wspierają społeczności lokalne, głównie w obliczu klęsk żywiołowych. Utrzymują gotowość do działań ratowniczych i porządkowych, prowadzą monitoring zagrożeń oraz szkolenia obronne. W sytuacjach kryzysu niemilitarnego formacja reaguje w celu ograniczenia skutków zdarzeń, przywrócenia normalnego funkcjonowania regionu i wsparcia układu pozamilitarnego. W czasie wojny WOT realizują działania bojowe w ramach współpracy z wojskami operacyjnymi, broniąc przydzielonych rejonów odpowiedzialności, osłaniając obiekty infrastruktury krytycznej oraz wspierając siły sojusznicze w zakresie logistycznym i zabezpieczenia ich wejścia do działań bojowych (Niedziela, 2022).

Zakres zadań WOT jest szeroki i obejmuje między innymi:

- świadczenie pomocy ludności cywilnej (ewakuacja, ochrona mienia, organizacja rejonów zakwaterowania przejściowego, dystrybucja środków pomocowych),
- wsparcie administracji rządowej i samorządowej w monitorowaniu zagrożeń i wzmocnieniu systemu bezpieczeństwa,
- udział w akcjach poszukiwawczo-ratowniczych oraz usuwaniu skutków katastrof i klęsk żywiołowych,

- wsparcie służb odpowiedzialnych za bezpieczeństwo wewnętrzne (Straż Graniczna, Policja) w sytuacjach, gdy ich potencjał jest niewystarczający,
- ochronę infrastruktury krytycznej, izolację miejsc i obszarów zagrożonych, zabezpieczenie obiektów i zbieranie informacji o potencjalnych zagrożeniach,
- działania przeciwpowodziowe i przeciwpożarowe, rozpoznanie i neutralizacja skutków awarii przemysłowych oraz skażeń chemicznych, biologicznych i radiacyjnych (Ustawa o zarządzaniu kryzysowym, 2007; Horyń, 2019).

Zgodnie z ustawą o powszechnym obowiązku obrony RP (Ustawa o obronie Ojczyzny, 2022), Strategią Bezpieczeństwa Narodowego RP (BBN, 2020) i Koncepcją Obroną RP (MON, 2017), WOT powinny posiadać zdolności w zakresie odstraszania i demonstrowania gotowości do obrony, osłony rozwinięcia wojsk, udziału w strategicznej operacji obronnej, prowadzenia działań rozpoznawczych i wsparcia ogniowego, przeciwdziałania zagrożeniom hybrydowym i asymetrycznym (Jakubczak, 2016; Pieczywok, 2023), realizacji zadań w systemie zarządzania kryzysowego oraz współdziałania z pozamilitarnymi elementami systemu obronnego państwa. Szczególne znaczenie ma interoperacyjność z wojskami operacyjnymi, sprzężenie systemów wymiany informacji o zagrożeniach, a także wspólne szkolenia i ćwiczenia, które zapewniają spójność działań w sytuacjach kryzysowych i wojennych (Stachowski, 2017).

WOT, poprzez swoje rozmieszczenie i charakter terytorialny, przyczyniają się do budowy powszechnej gotowości obronnej, wzmacniają potencjał odstraszania Sił Zbrojnych RP, zwiększają odporność państwa na kryzysy i przygotowują społeczeństwo do realizacji konstytucyjnego obowiązku obrony Ojczyzny.

Udział Wojsk Obrony Terytorialnej w ochronie granicy w warunkach wojny hybrydowej

Współczesne działania hybrydowe prowadzone poza formalnymi ramami prawa wojennego stanowią skoordynowane połączenie aktywności nieregularnych formacji zbrojnych, wspieranych przez zaawansowane technologie rozpoznania pola walki, działania agenturalne agresora, a także

szeroko zakrojonego oddziaływania informacyjnego i presji ekonomicznej. Celem tego rodzaju operacji jest osiągnięcie efektów zbliżonych do klasycznej wojny, ale bez jej formalnego wypowiedzenia i bez konieczności użycia wojsk operacyjnych w pełnym wymiarze. Istotą działań hybrydowych jest przejęcie kontroli nad terytorium państwa ofiary i ustanowienie tam władz podporządkowanych agresorowi – zarówno w formie aneksji, jak i poprzez stworzenie marionetkowych struktur politycznych bez formalnego włączenia obszaru do państwa agresora. Operacje hybrydowe mają z reguły trójetapowy przebieg: obejmują fazę przygotowania, fazę realizacji z udziałem elementów militarnych oraz etap stabilizacji, którego celem jest militarne i administracyjne utrwalenie wpływów na zajętym lub podporządkowanym terytorium (Jakubczak, 2016).

Konflikt rosyjsko-ukraiński wyraźnie wskazał na fundamentalne zadania, jakie powinny realizować formacje obrony terytorialnej, aby skutecznie wzmacniać bezpieczeństwo państwa. Ich zakres można dostosowywać do różnych sytuacji oraz poziomów gotowości bojowej. Na co dzień Wojska Obrony Terytorialnej powinny utrzymywać ścisłą więź z lokalnymi społecznościami i demonstrować gotowość do obrony zajmowanego przez nie terytorium. W czasie pokoju kluczowe jest systematyczne monitorowanie zagrożeń, w tym terrorystycznych, oraz identyfikowanie działań zmierzających do podważania autorytetu legalnych władz czy destabilizacji administracji państwowej. Bezpośrednio przed konfliktem WOT powinny niezwłocznie reagować na pojawienie się obcych podmiotów, zwłaszcza jeśli ich działalność ukierunkowana jest na osłabienie więzi społeczności lokalnej z państwem. W momencie wybuchu konfliktu lub nasilenia działań przeciwnika – niezależnie od możliwości precyzyjnego określenia chwili rozpoczęcia działań wojennych – formacje te muszą zdecydowanie bronić terytorium i ludności cywilnej, wykorzystując społeczne poparcie i zaangażowanie. Jeśli konflikt hybrydowy przerodzi się w otwarte starcie zbrojne, zadaniem WOT jest stworzenie warunków umożliwiających skuteczne wprowadzenie wojsk operacyjnych i bliską współpracę z nimi podczas prowadzenia regularnych operacji. W sytuacji zajęcia terytorium przez nieprzyjaciela, wojska te powinny prowadzić działania nieregularne, których celem jest systematyczne niszczenie siły żywej i środków bojowych wroga, dezorganizowanie jego działań i uniemożliwianie skutecznej okupacji. W przypadku uzyskania

wsparcia na poziomie krajowym lub sojuszniczym WOT mają za zadanie stworzyć warunki sprzyjające przejęciu kontroli nad terenem oraz odbudowie infrastruktury krytycznej, w tym administracji publicznej. Po zakończeniu działań wojennych priorytetem staje się odbudowa zdolności operacyjnych formacji oraz powrót do realizacji zadań typowych dla okresu pokoju (Szczurek i in., 2022).

A. Zapałowski wskazywał, że najbardziej nieprzewidywalnym kierunkiem w zakresie potencjalnych zagrożeń dla bezpieczeństwa państwa jest granica polsko-ukraińska – rosyjska agresja na Ukrainę potwierdza konieczność utrzymywania podwyższonej gotowości i zdolności reagowania również na tym odcinku (Zapałowski, 2019).

W drugiej połowie 2021 r. Republika Białorusi podjęła agresywne działania o charakterze hybrydowym, których celem było wywołanie w Polsce kryzysu migracyjnego i szeroko pojętej destabilizacji. Mając na uwadze genezę i przeznaczenie Wojsk Obrony Terytorialnej, naturalnym następstwem było ich zaangażowanie w działania na rzecz ochrony granicy. Na mocy decyzji Ministra Obrony Narodowej, od 3 września 2021 r. żołnierze WOT rozpoczęli służbę w pasie przygranicznym z Białorusią, na terenach objętych stanem wyjątkowym. Wydarzenia na granicy polsko-białoruskiej z drugiej połowy 2021 r. stały się impulsem do rozpoczęcia operacji „Silne Wsparcie", której głównym celem było wzmocnienie odporności społeczności lokalnych oraz wsparcie ich w obliczu nowego rodzaju zagrożenia o charakterze hybrydowym. Chociaż pełne dane dotyczące zaangażowania wszystkich brygad Obrony Terytorialnej nie zostały oficjalnie opublikowane, raport 2. Lubelska Brygada OT pozwala na odtworzenie znaczącego zakresu podjętych działań. Od września 2021 r. w pasie przygranicznym województw lubelskiego i podlaskiego rozpoczęto działania z udziałem żołnierzy 1. Podlaskiej i 2. Lubelskiej Brygady OT. Wraz ze wzrostem liczby prób nielegalnego przekroczenia granicy do wsparcia Straży Granicznej kierowano także żołnierzy z innych brygad WOT. W szczytowym okresie operacji w ochronę granicy zaangażowanych było blisko 2 000 terytorialsów. Działania obejmowały nie tylko patrole piesze i mobilne, lecz także – z uwagi na specyfikę terenu Lubelszczyzny – patrole konne i wodne na rzece Bug (2 Lubelska Brygada Obrony Terytorialnej, b.d.).

Do rozpoznania wykorzystano Bezzałogowe Statki Powietrzne Fly-Eye, które łącznie wykonały ponad 2 300 godzin lotów, z czego ponad 1 500 godzin zrealizowano na rzecz 2. Lubelskiej Brygady OT. Żołnierze posługiwali się również nowoczesnym sprzętem optoelektronicznym, w tym noktowizorami i termowizją, a na wybranych odcinkach granicy obsługiwali maszty oświetleniowe, co zwiększało skuteczność działań nocnych. Według danych MON w terenie przygranicznym stale obecnych jest około 1 000 żołnierzy WOT utrzymujących gotowość do natychmiastowej reakcji na pojawiające się zagrożenia. Od 2023 r. w pasie przygranicznym prowadzone są również planowe szkolenia rotacyjne i zintegrowane, których celem jest doskonalenie wyszkolenia żołnierzy, rozwijanie umiejętności działania w specyficznych warunkach terenowych oraz wzmocnienie współpracy z lokalną społecznością (Defence24, 2023).

Żołnierze WOT uczestniczą także w operacji „Bezpieczne Podlasie", będącej demonstracją gotowości Sił Zbrojnych RP oraz zdolności do szybkiego reagowania na próby destabilizacji sytuacji na granicy państwowej. W ramach tego przedsięwzięcia wspierają działania 12. Brygady Zmechanizowanej oraz 17. Wielkopolskiej Brygady Zmechanizowanej, a ich zadaniem jest m.in. zabezpieczanie patroli z udziałem kołowych transporterów opancerzonych Rosomak oraz utrzymywanie kontaktu z mieszkańcami rejonów przygranicznych, przekazując im informacje o bieżącej sytuacji (Defence24, 2023).

Operacja „Bezpieczne Podlasie", rozpoczęta 1 sierpnia 2024 r., stanowi przykład adaptacji wojskowego reagowania na złożone zagrożenia hybrydowe, w tym napięcia migracyjne na wschodniej granicy państwa[1]. Generał dywizji Arkadiusz Szkutnik, dowódca operacji, podkreślał w wywiadzie znaczenie zmiany taktyki działań: zamiast biernego monitorowania obszaru kluczowe stały się mobilność i szybkość reakcji, które decydują o skuteczności powstrzymywania prób nielegalnego przekroczenia granicy. Nowa strategia operacyjna zakłada elastyczne i proporcjonalne użycie siły. Szkutnik wskazywał, że w sytuacjach agresywnych zachowań nie stosuje się podejścia wyłącznie prewencyjnego – siły zbrojne reagują adekwatnie, w tym z użyciem broni gładkolufowej i strzałów ostrzegawczych. Podkreślił jednocześnie, że nie odnotowano przypadków oddania strzałów w kierunku ludzi – byłaby to ostateczność. Znaczącą rolę w odstraszaniu agresywnych

działań odegrało użycie środków nieletalnych. Sama obecność formacji uzbrojonych w broń gładkolufową skutecznie ograniczała eskalację napięć, minimalizując konieczność użycia siły (Polska Zbrojna, 2024).

Kwestie operacyjne obejmowały również środki ochrony operacyjnej, takie jak czasowe zasłanianie tablic rejestracyjnych pojazdów wojskowych. Generał Szkutnik wskazał, że działanie to jest zgodne z przepisami obowiązującymi w strefie buforowej i ma na celu ochronę bezpieczeństwa operacji, przy jednoczesnym utrzymaniu możliwości nakładania mandatów przez Żandarmerię Wojskową w przypadku naruszeń prawa (Polska Zbrojna, 2024). Operacja wiązała się również z dostosowaniem podstaw prawnych. Wprowadzone zmiany legislacyjne poszerzyły uprawnienia żołnierzy i funkcjonariuszy Straży Granicznej w zakresie stosowania środków przymusu bezpośredniego, a także zapewniły im realną ochronę prawną podczas działań w sytuacjach kryzysowych (Ustawa z dnia 26 lipca 2024 r. o zmianie niektórych ustaw..., 2024).

Podsumowanie

Wojska Obrony Terytorialnej w ciągu kilku lat od swojego powołania stały się istotnym elementem systemu bezpieczeństwa narodowego Polski. Ich rozmieszczenie w Stałych Rejonach Odpowiedzialności, silne zakorzenienie w lokalnych społecznościach oraz zdolność do szybkiego reagowania na pojawiające się zagrożenia sprawiają, że formacja ta wypełnia lukę pomiędzy wojskami operacyjnymi a układem pozamilitarnym. Doświadczenia z lat 2021-2024 jednoznacznie wskazują, że WOT odgrywają kluczową rolę w ochronie granicy państwowej w warunkach kryzysu migracyjnego i zagrożeń hybrydowych.

Udział żołnierzy Wojsk Obrony Terytorialnej w operacjach „Silne Wsparcie" i „Bezpieczne Podlasie" potwierdził, że formacja ta jest zdolna do realizacji zadań o szerokim spektrum – od zadań stricte wojskowych po działania prewencyjne, humanitarne i informacyjne. W 2021 r. w odpowiedzi na kryzys migracyjny na granicy polsko-białoruskiej żołnierze WOT zabezpieczyli kilkaset kilometrów granicy, prowadząc patrole piesze, konne i wodne oraz wykorzystując bezzałogowe statki powietrzne do rozpoznania sytuacyjnego. Tylko w ramach operacji „Silne Wsparcie" odnotowano kilka tysięcy patroli i interwencji w rejonach przygranicznych, co znacząco

zwiększyło wykrywalność prób nielegalnego przekroczenia granicy i poprawiło poczucie bezpieczeństwa lokalnych społeczności.

Stała obecność WOT w pasie przygranicznym pozwoliła na szybką reakcję na dynamicznie zmieniającą się sytuację, a ścisła współpraca ze Strażą Graniczną, Policją i innymi służbami doprowadziła do stworzenia zintegrowanego systemu reagowania. Analiza przeprowadzonych działań wskazuje na wysoką efektywność operacyjną WOT – są w stanie w ciągu kilku godzin od pojawienia się zagrożenia wystawić siły gotowe do działania w Stałych Rejonach Odpowiedzialności.

Wojska Obrony Terytorialnej w istotny sposób wzmacniły narodowy system reagowania kryzysowego, łącząc komponent militarny z działaniami administracji publicznej i wsparciem dla ludności. Doświadczenia z lat 2021-2024 wykazują, że WOT muszą stale rozwijać zdolności do przeciwdziałania zagrożeniom hybrydowym, zwłaszcza w obszarze zwalczania dezinformacji, neutralizacji prowokacji oraz przeciwdziałania presji migracyjnej inspirowanej z zewnątrz. Jednocześnie konieczne jest dalsze pogłębianie interoperacyjności z wojskami operacyjnymi, Strażą Graniczną i służbami specjalnymi w celu budowy efektywnego systemu wczesnego ostrzegania i szybkiego reagowania. Ważnym elementem misji WOT jest również ich oddziaływanie społeczne – formacja pełni funkcję edukacyjną i wychowawczą, wzmacniając świadomość obronną i więź państwa ze społeczeństwem. W warunkach wojny hybrydowej, gdzie jednym z celów przeciwnika jest dezintegracja społeczna i osłabienie morale, działania te mają istotne znaczenie dla budowy odporności narodowej.

Podsumowując, Wojska Obrony Terytorialnej w pełni realizują cele, dla których zostały powołane, i stanowią istotny filar systemu obronnego Polski. Analiza ich działań wskazuje na konieczność dalszego rozwoju zdolności rozpoznawczych, inwestowania w technologie monitoringu i systemy bezzałogowe. Kluczowe jest również utrzymanie wysokiej motywacji ochotników, systematyczne szkolenie oraz budowanie współpracy z administracją publiczną i służbami bezpieczeństwa, co pozwoli skutecznie odpowiadać na przyszłe wyzwania.

Literatura

1. 2 Lubelska Brygada Obrony Terytorialnej. (2025). *Podsumowanie roku 2022*. Pobrane z: https://www.wojsko-polskie.pl/2bot/articles/aktualnosci-w/podsumowanie-roku-2022/ (dostęp: 12.02.2026).
2. BBN. (2020). *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*. Biuro Bezpieczeństwa Narodowego.
3. Compa, T. (2020). Wojska Obrony Terytorialnej i Narodowe Siły Rezerwowe w systemie obrony Rzeczypospolitej Polskiej. *Facta Simonidis, 13*(1), 79-98.
4. Defence24. (2023). *2 lata służby terytorialsów na straży polskiej granicy.* Pobrane z: https://defence24.pl/sily-zbrojne/2-lata-sluzby-terytorialsow-na-strazy-polskiej-granicy#goog_rewarded (dostęp: 12.02.2026).
5. Elak, L. (2020). *Potencjał wojsk lądowych wobec współczesnych wyzwań bezpieczeństwa Rzeczypospolitej Polskiej.* Akademia Sztuki Wojennej.
6. Elak, L., Oskierko, M., Żurawski, S. (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
7. Horyń, W. (2019). Wojska obrony terytorialnej w czasie niemilitarnych zdarzeń nadzwyczajnych. *Kwartalnik Bellona, 696*(1), 42-52.
8. Huzarski, M. (2017). Podstawy normatywne i koncepcyjno-funkcjonalne tworzenia WOT. *Przegląd Nauk o Obronności, 3*, 67-82. https://doi.org/10.5604/01.3001.0012.9794
9. Jakubczak, R. (2016). Wojska Obrony Terytorialnej w sztuce wojennej. *Ante Portas – Studia nad Bezpieczeństwem, 2*(7), 23-44.
10. Konieczny, M. (2022). Operacja „Śluza" – kryzys uchodźczy związany z przerzutem nielegalnych migrantów przez polsko-białoruską granicę. *Roczniki Administracji i Prawa, 22*(2), 89-102. https://doi.org/10.5604/01.3001.0016.0948
11. Kukuła, A. (2022). Ochrona granicy państwowej przez siły zbrojne RP w warunkach nielegalnej migracji. *Zeszyty Naukowe Pro Publico Bono, 1*(1), 345-356. https://doi.org/10.5604/01.3001.0016.1990

12. Kukuła, A. (2024). Wojska Obrony Terytorialnej w systemie zarządzania kryzysowego. *Zeszyty Naukowe Pro Publico Bono, 1*(1), 227-239. https://doi.org/10.5604/01.3001.0054.8782
13. Kwiatkowski, W. (2023). Wizerunek Wojsk Obrony Terytorialnej w przekazie medialnym w latach 2016-2018. *Zeszyty Naukowe Pro Publico Bono, 1*(1), 13-30. https://doi.org/10.5604/01.3001.0054.1713
14. Michalak, A. (2017). Cele, zadania, struktura i funkcje wojsk obrony terytorialnej w XXI wieku. Bezpieczeństwo. *Teoria i Praktyka, 3*, 27-36.
15. MON. (2014). *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*. Ministerstwo Obrony Narodowej.
16. MON. (2017). *Koncepcja obronna Rzeczypospolitej Polskiej*. Ministerstwo Obrony Narodowej.
17. Nastarowicz, T. (2017). Proces tworzenia brygady Obrony Terytorialnej RP: Studium przypadku. *Bezpieczeństwo. Teoria i Praktyka, 3*, 99-114.
18. Niedziela, M. (2022). Wojska Obrony Terytorialnej w obliczu współczesnych zagrożeń dla bezpieczeństwa – studium przypadków. *Zeszyty Naukowe Pro Publico Bono, 1,* 195-208. https://doi.org/10.5604/01.3001.0016.1969
19. Nitszke, A. (2024). Instrumentalizacja migracji: Proceduralizacja versus humanizacja polityki azylowej Unii Europejskiej. *Politeja, 1*(88/1), 239-251. https://doi.org/10.12797/Politeja.20.2024.88.1.14
20. Oskierko, M., Żurawski, S. (2024). Kryzys migracyjny na granicy białorusko-polskiej jako przykład zagrożenia konfliktem o charakterze kulturowym. W: W. Śmiałek (red.), *Wielowymiarowość konfliktów kulturowych we współczesnym świecie* (s. 177-195). Grupa Wydawnicza FNCE.
21. Oskierko, M. (2021). Współdziałanie Straży Granicznej i Wojsk Obrony Terytorialnej w okresie stanu pandemii. W: L. Elak, N. Iwanowski, P. Rosłoń, K. Zygo (red.), *Wyzwania Sił Zbrojnych Rzeczypospolitej Polskiej w nowych uwarunkowaniach* (s. 211-230). Akademia Sztuki Wojennej.
22. Oskierko, M. (2022). Kryzys migracyjny na polsko-białoruskiej granicy państwowej. W: D. Dachowicz, L. Elak, Z. Ciekanowski (red.), *Zagrożenia wschodniej flanki NATO w aspekcie bezpieczeństwa wewnętrznego obszarów przygranicznych* (s. 201-220). Wydawnictwo im. prof.

Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie.

23. Pieczywok, A. (2023). *Rola i znaczenie Wojsk Obrony Terytorialnej jako instytucji integrującej i wspierającej społeczeństwo w czasie pandemii*. Uniwersytet Kazimierza Wielkiego w Bydgoszczy.
24. PAP. (2024). *Operacja Śluza: Białoruski dziennikarz ujawnia PAP kulisy tajnej akcji*. Polska Agencja Prasowa. Pobrane z: https://www.pap.pl/aktual-nosci/news%2C935470%2Coperacja-sluza-bialoruski-dziennikarz-ujawnia-pap-kulisy-tajnej-akcji.html (dostęp: 12.02.2026).
25. Polska Zbrojna. (2024, 8 listopada). *„Bezpieczne Podlasie" na półmetku*. Pobrane z: https://www.polska-zbrojna.pl/home/articleshow/42749?t=--Bezpieczne-Podlasie-na-polmetku (dostęp: 12.02.2026).
26. Stachowski, M. (2017). Koncepcja Wojsk Obrony Terytorialnej jako piątego rodzaju Sił Zbrojnych Rzeczypospolitej Polskiej: Materiał dyskusyjny. *Bezpieczeństwo. Teoria i Praktyka, 3,* 50-62.
27. Szczurek, T., Bryczek-Wróbel, P., Adamkiewicz, J. (2022). Funkcjonowanie Wojsk Obrony Terytorialnej Polski w świetle kryzysu na Ukrainie. *Zeszyty Naukowe SGSP, 83,* 123-140. https://doi.org/10.5604/01.3001.0016.0228
28. Ustawa z 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. z 2016 r. poz. 2138).
29. Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122).
30. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2022 r. poz. 655).
31. Ustawa z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczypospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa (Dz. U. z 2024 r. poz. 1248).
32. Wróbel, I. (2017). Perspektywy współdziałania wojsk obrony terytorialnej z administracją publiczną w zwalczaniu klęsk żywiołowych. *Bezpieczeństwo. Teoria i Praktyka, 3,* 131-150.
33. Zapałowski, A. (2019). Współczesne wojska Obrony Terytorialnej w obronie narodowej. *Przegląd Geopolityczny, 28,* 141-158.

Marcin Chodyka[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_9

MIGRACJE ZAROBKOWE I BEZPIECZEŃSTWO GOSPODARCZE PAŃSTWA

ECONOMIC MIGRATION AND NATIONAL ECONOMIC SECURITY

Streszczenie

Migracje zarobkowe stały się trwałym elementem funkcjonowania gospodarek, szczególnie w warunkach starzenia się populacji, regionalnych niedoborów pracy oraz rosnącej wrażliwości państw na szoki (geopolityczne, epidemiologiczne i podażowe). Jednocześnie w debacie publicznej i części opracowań eksperckich pojęcie „bezpieczeństwa gospodarczego" bywa ujmowane szeroko i niejednoznacznie, co utrudnia systematyczną ocenę bilansu korzyści oraz ryzyk wynikających z napływu pracowników-migrantów. Celem rozdziału jest prezentacja aparatu pojęciowego dotyczącego bezpieczeństwa gospodarczego państwa i migracji zarobkowych, identyfikacja determinant migracji w ujęciu strukturalnym oraz wskazanie mechanizmów (kanałów) oddziaływania migracji na kluczowe wymiary bezpieczeństwa gospodarczego – rynek pracy, finanse publiczne, produktywność/innowacyjność, ciągłość świadczenia usług i odporność instytucjonalną. W części empirycznej zastosowano

[1] https://orcid.org/0009-0004-6585-5541, e-mail: marcinchodyka@gmail.com

analizę danych wtórnych na przykładzie Polski (2000-2024) dla wskaźników: saldo migracji netto oraz stopa bezrobocia (modelowane estymaty ILO), a także na poziomie UE dla struktury pierwszych zezwoleń pobytowych w 2023 r. Wyniki wskazują, że relacja między migracją netto a bezrobociem ma charakter słaby i silnie zależy od trendów długookresowych. Wahania migracji mogą natomiast istotnie oddziaływać na segmentację rynku pracy i ryzyka nieprawidłowości (np. praca nierejestrowana), które są komponentami bezpieczeństwa gospodarczego w wymiarze instytucjonalnym i fiskalnym. Rozdział kończy się propozycją „tablicy wskaźników" (dashboardu) do monitorowania wpływu migracji na bezpieczeństwo gospodarcze oraz wskazaniem zastosowań dla administracji publicznej i analityki polityk publicznych.

Słowa kluczowe: migracje zarobkowe, bezpieczeństwo gospodarcze, rynek pracy, odporność, finanse publiczne, nieprawidłowości zatrudnienia, polityka migracyjna

Abstract

Labour migration has become a persistent feature of contemporary economies, particularly amid population ageing, regional labour shortages, and states' growing exposure to shocks (geopolitical, epidemiological, and supply-side). At the same time, in public debate and in parts of expert discourse, the notion of "economic security" is often employed in a broad, conceptually ambiguous manner, hindering a systematic assessment of the balance of benefits and risks associated with inflows of migrant workers. The aim of this chapter is to present a conceptual framework for the economic security of the state and labour migration, to identify the structural determinants of migration, and to indicate the mechanisms (transmission channels) through which migration affects key dimensions of economic security – namely the labour market, public finances, productivity/innovation, continuity of service provision, and institutional resilience. The empirical section applies secondary data analysis using Poland (2000-2024) as a case study, focusing on the following indicators: net migration balance and the unemployment rate (modelled ILO estimates). In addition, EU-level evidence on the structure of first-residence permits in 2023 is examined. The results suggest that the relationship between net migration and unemployment is weak and strongly contingent upon long-term trends; however, fluctuations in migration may significantly affect labour market segmentation and the risk of irregularities (e.g., undeclared work), which constitute components of economic security in both institutional and fiscal terms. The chapter concludes by proposing an "indicator dashboard" to monitor the impact of migration on economic security and by outlining practical applications for public administration and public policy analytics.

Keywords: labour migration, economic security, labour market, resilience, public finances, employment irregularities, migration policy

Wstęp

W debacie publicznej migracje zarobkowe często prezentowane są w kategoriach „korzyści" lub „kosztów", a wskaźniki takie jak stopa bezrobocia bywają traktowane jako szybki test wpływu imigracji na sytuację gospodarki. Jednak literatura naukowa i doświadczenia polityk publicznych sugerują, że proste relacje agregatowe mogą maskować kluczowe mechanizmy transmisji: dopasowanie kompetencji, reakcje inwestycji i technologii, segmentację sektorową, a także jakość instytucji egzekwujących standardy pracy i prawa pobytu (Ottaviano, Peri, 2012; Longhi, Nijkamp, Poot, 2010; Dias-Abey, 2021). Z perspektywy nauk o bezpieczeństwie szczególnie istotne jest to, że bezpieczeństwo gospodarcze nie jest „stanem" jednowymiarowym, lecz wiązką zdolności państwa do utrzymywania ciągłości funkcjonowania gospodarki i usług oraz do reagowania na zakłócenia. W podejściu instytucjonalno-strategicznym obejmuje ono m.in. ochronę kluczowych aktywów gospodarczych i infrastruktury krytycznej, bezpieczeństwo łańcuchów dostaw oraz zarządzanie ryzykami geopolitycznymi i technologicznymi (OECD, 2025).

Na poziomie Unii Europejskiej „bezpieczeństwo gospodarcze" zostało silnie powiązane z logiką identyfikacji zależności i zarządzania ryzykiem (de-risking) w warunkach współzależności gospodarczej. W strategii bezpieczeństwa gospodarczego UE akcentuje się, że odpowiedzi polityczne mają minimalizować ryzyka bez pełnego „odsprzęgania" od przepływów międzynarodowych, a katalog ryzyk obejmuje m.in. aspekty technologiczne. (European Commission, 2023). W tym kontekście migracje zarobkowe są zjawiskiem „strukturalnym" – powiązanym z demografią, różnicami rozwojowymi, konfliktami i globalizacją rynków pracy. Jednocześnie są zjawiskiem „instytucjonalnym", bo ich efekty zależą od ram prawnych, sprawności administracyjnej i standardów egzekwowania prawa pracy. Świetnym przykładem złożoności są migracje z Ukrainy do Polski w ostatniej dekadzie, w tym masowy napływ po 2022 r., który w literaturze analizowany jest zarówno jako shock migracyjny, jak i wyzwanie integracyjne dla rynku pracy i usług publicznych (Duszczyk, Kaczmarczyk, 2022; Postek, Walerych, 2026).

Cel rozdziału obejmuje dwa komplementarne zadania. Po pierwsze, rozdział porządkuje aparat pojęciowy i przedstawia model analityczny łączący migracje z pięcioma wymiarami bezpieczeństwa gospodarczego państwa: rynkiem pracy i podażą pracy, bezpieczeństwem fiskalnym, produktywnością i innowacyjnością, ciągłością usług oraz odpornością sektorową, integralnością instytucjonalną i spójnością społeczną jako warunkami stabilności gospodarczej. Po drugie, rozdział prezentuje ilustracyjną analizę empiryczną dla Polski (2000-2024) oraz dla Unii Europejskiej (struktura pierwszych zezwoleń pobytowych w 2023 r.), a następnie przekłada wyniki na propozycję dashboardu służącego monitorowaniu korzyści i ryzyk związanych z migracjami.

Przegląd literatury

Punktem wyjścia jest rozróżnienie między „bezpieczeństwem gospodarczym" jako kategorią polityki państwa i bezpieczeństwa narodowego a „niepewnością ekonomiczną" (economic insecurity) na poziomie jednostek i gospodarstw domowych. Pomiar niepewności ekonomicznej (np. ryzyka utraty dochodu) jest odrębnym nurtem badań, a brak konsensusu definicyjnego i pomiarowego w tym obszarze bywa wskazywany jako problem metodologiczny (Osberg, 2015). W niniejszym rozdziale perspektywa jest makro- i mezo-poziomowa: interesuje nas zdolność państwa do utrzymania funkcjonowania gospodarki (w tym instytucji i usług), co koresponduje z definicją operacyjną podkreślającą „niezakłócone funkcjonowanie gospodarki" oraz równowagę relacji gospodarczych z otoczeniem międzynarodowym.

W polskim piśmiennictwie bezpieczeństwo ekonomiczne jest ujmowane jako wymiar bezpieczeństwa narodowego, akcentując sprawność systemu gospodarczego i odporność na naciski zewnętrzne oraz zdolność do wykorzystania wewnętrznych czynników rozwoju (Księżopolski, 2011). W pracach zbiorowych podejmuje się wielowymiarową analizę uwarunkowań bezpieczeństwa ekonomicznego państwa (m.in. globalizacja, korupcja, bariery innowacji), co wspiera tezę o potrzebie budowania narzędzi monitoringu obejmujących zarówno parametry ekonomiczne, jak i jakość instytucji (Jackiewicz, Trzaskowska-Dmoch, 2018). W literaturze ekonomicznej wpływ migracji na rynek pracy analizowany jest w ramach podejść równowagi ogólnej (substytucyjność/komplementarność pracy migrantów

i rezydentów, reakcje kapitału), a wnioski często wskazują na niewielkie efekty średnie, przy jednoczesnym znaczeniu efektów rozkładowych (np. różnic między grupami dochodowymi, branżami, regionami). Kluczowa teza to potrzeba badania mechanizmów dostosowawczych gospodarki zamiast prostych korelacji (Ottaviano, Peri, 2012; Longhi, Nijkamp, Poot, 2005; Longhi, Nijkamp, Poot, 2010). Metaanalizy literatury empirycznej dostarczają syntetycznych wniosków: wpływ imigracji na płace i zatrudnienie bywa statystycznie niewielki, ale zależny od metod, horyzontu czasowego i definicji grup odniesienia. Wskazuje się, że „koszty" mogą koncentrować się w segmentach niskopłatnych, podczas gdy efekty dla grup średnio i wysokopłatnych są często małe, czasem dodatnie – co ma konsekwencje dla politycznej akceptowalności migracji oraz dla ryzyk spójności społecznej (Longhi, Nijkamp, Poot, 2010; Vargas-Silva, Sumption, 2023). Na poziomie makro istnieją również badania pokazujące, że imigracja może podnosić długookresowo PKB per capita, w znacznej mierze poprzez produktywność (a nie wyłącznie przez wzrost liczby pracujących). Przykładem jest analiza MFW wskazująca, że migracja może zwiększać dochód per capita w gospodarkach zaawansowanych, przy istotnych różnicach w zależności od struktury kwalifikacji i integracji na rynku pracy (IMF, 2016). Z perspektywy bezpieczeństwa gospodarczego jest to ważne, ponieważ identyfikuje „kanał produktywności" jako element odporności wzrostowej gospodarki. W literaturze podkreśla się również rolę instytucji prawa pracy i egzekwowania standardów jako moderatora wpływu migracji na rynek pracy. W ujęciu „legal institutionalist" skutki migracji dla płac i zatrudnienia są współtworzone przez reżimy kontraktowe, układy zbiorowe, mechanizmy ochrony pracowników i praktyki inspekcyjne (Dias-Abey, 2021). To przesuwa ciężar analizy bezpieczeństwa gospodarczego ku jakości instytucji: nawet przy niewielkich efektach makro, słabe egzekwowanie może generować ryzyka fiskalne i konkurencyjne poprzez wzrost szarej strefy. Ten wątek prowadzi do obszaru nieprawidłowości zatrudnienia, istotnego dla bezpieczeństwa gospodarczego w wymiarze instytucjonalnym i fiskalnym. OECD wskazuje, że nielegalne zatrudnienie cudzoziemców jest zjawiskiem wieloaspektowym, wynikającym zarówno z naruszeń przepisów migracyjnych, jak i prawa pracy, jego ograniczanie jest istotne z punktu widzenia polityki ekonomicznej, ochrony pracowników i legitymizacji społecznej polityki migracyjnej (OECD, 2018).

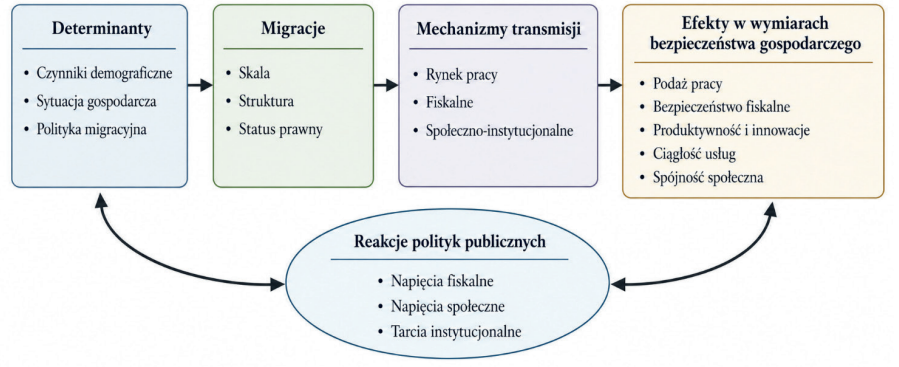
Komplementarnie, Eurofound definiuje pracę nierejestrowaną jako legalną co do natury aktywność zarobkową, która nie jest deklarowana władzom publicznym, co bezpośrednio łączy ten obszar z ryzykami fiskalnymi (Eurofound, 2026).

Z perspektywy „twardych" ryzyk bezpieczeństwa (w rozumieniu bezpieczeństwa państwa) istotne jest także eksploatacja pracy i przymus. Globalne estymaty wskazują, że w 2021 r. ok. 50 mln osób żyło w warunkach współczesnego niewolnictwa, w tym ok. 28 mln w pracy przymusowej. Chociaż są to wielkości globalne, stanowią one ważne tło dla analizy migracji zarobkowych, ponieważ migranci – zwłaszcza o słabszym statusie prawnym lub zależni od pracodawcy/pośredników – są traktowani jako grupa o podwyższonym ryzyku nadużyć w wielu sektorach (ILO, 2022). W UE znaczenie ryzyk eksploatacji znajduje odzwierciedlenie w narzędziach przygotowywanych dla inspekcji pracy. Wspólny przewodnik instytucji unijnych dla inspektorów pracy akcentuje rolę inspekcji jako kluczowego instrumentu wykrywania i przeciwdziałania wyzyskowi pracowników nienarodowych (w tym obywateli państw trzecich), co łączy kompetencje państwa regulatora z bezpieczeństwem gospodarczym (European Labour Authority, iFRA, 2025).

W ostatnich latach administracje publiczne w coraz większym stopniu cyfryzują procesy powiązane z migracją i rynkiem pracy (m.in. obsługę wniosków pobytowych, rejestry, integrację danych oraz komunikację międzyinstytucjonalną). Równolegle rośnie ekspozycja sektora publicznego na ryzyka cybernetyczne, które – w perspektywie bezpieczeństwa gospodarczego – mogą przekładać się na zakłócenia ciągłości usług publicznych oraz spadek zdolności państwa do efektywnego egzekwowania regulacji. OECD ujmuje cyberbezpieczeństwo jako jeden z komponentów bezpieczeństwa gospodarczego, wskazując, że ochrona kluczowych zasobów i infrastruktury krytycznej obejmuje również wymiar cyfrowy (OECD, 2025). Na poziomie Unii Europejskiej ramy te wzmacnia dyrektywa NIS2, ustanawiająca wspólne wymagania w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz raportowania incydentów w podmiotach kluczowych i ważnych, co ma znaczenie dla stabilności funkcjonowania usług publicznych i gospodarczych (Unia Europejska, 2022). Z kolei ENISA wskazuje, że administracja publiczna należy do sektorów szczególnie narażonych na ataki, co w praktyce

zwiększa ryzyko zakłóceń procesów administracyjnych o znaczeniu gospodarczym – w tym tych związanych z legalizacją pobytu i zatrudnienia, kontrolą zgodności oraz przepływem informacji między instytucjami (ENISA, 2025).

Powyższe ustalenia integrują model wielopoziomowy, którego uproszczoną postać przedstawiono na Rysunku 1.



Rysunek 1. Model zależności migracji a bezpieczeństwo gospodarcze
Źródło: opracowanie własne.

Model ujmuje zależności w następującym układzie: determinanty kształtują migracje (w ujęciu skali, struktury i statusu prawnego), a te uruchamiają mechanizmy transmisji (z uwzględnieniem tarć instytucjonalnych i rynkowych), co prowadzi do efektów w wymiarach bezpieczeństwa gospodarczego. Jednocześnie model uwzględnia sprzężenia zwrotne, w ramach których reakcje polityk publicznych na napięcia fiskalne, społeczne i instytucjonalne wpływają na warunki determinujące kolejne fale migracji oraz sposób ich oddziaływania.

Metodologia i dane

Opracowanie przyjmuje podejście mieszane, adekwatne do wielowymiarowości bezpieczeństwa gospodarczego. W części teoretycznej zastosowano przegląd mapujący literatury, obejmujący zagadnienia ekonomii migracji, bezpieczeństwa ekonomicznego, instytucji rynku pracy oraz zjawisk pracy nierejestrowanej i eksploatacji. W części empirycznej wykorzystano analizę danych zastanych oraz proste modelowanie zależności

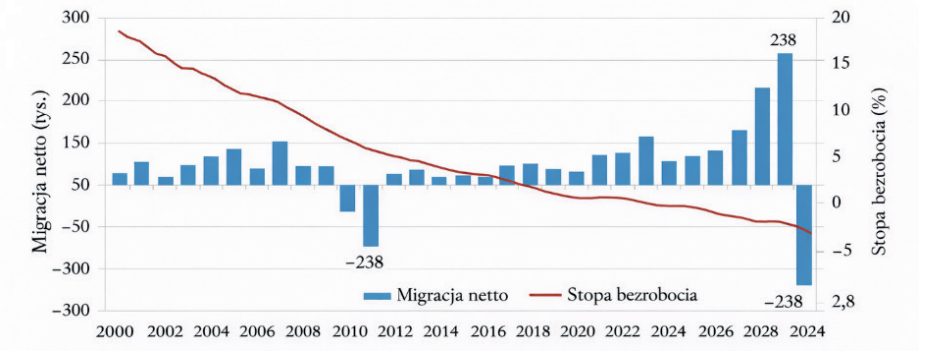
statystycznych wyłącznie w celu ilustracji zależności, a nie ich identyfikacji przyczynowo-skutkowej. Takie ujęcie ogranicza ryzyko nadinterpretacji korelacji i umożliwia osadzenie wyników w ustaleniach literatury, zwłaszcza dotyczących roli instytucji oraz uwarunkowań sektorowych. W części empirycznej dla Polski (2000-2024) wykorzystano dane o saldzie migracji netto oraz stopie bezrobocia. Saldo migracji netto jest w WDI definiowane jako liczba imigrantów minus liczba emigrantów (obywatele i nieobywatele), a źródłem bazowym są szacunki UN Population Division (World Population Prospects). Dane o bezrobociu wykorzystują estymaty modelowane ILO (ILOEST), które łączą obserwacje krajowe z imputacjami dla brakujących wartości w oparciu o modele ekonometryczne utrzymywane przez ILO, czego opis dostarcza dokumentacja metodologiczna ILO.

Dane zostały pobrane z otwartych plików WDI udostępnionych w ramach Data360 (format CSV). W analizie wykorzystano pełne szeregi roczne dla Polski w latach 2000-2024, a obliczenia wykonano na danych zgodnych z wartościami prezentowanymi na stronach wskaźników dla Polski. Na poziomie UE wykorzystano statystyki „pierwszych zezwoleń pobytowych" dla obywateli państw trzecich w 2023 r., w podziale na powód (zatrudnienie, rodzina, edukacja, inne – w tym ochrona międzynarodowa). Jest to wskaźnik użyteczny dla bezpieczeństwa gospodarczego, ponieważ przybliża strukturę kanałów migracyjnych, które różnią się tempem wejścia na rynek pracy i profilem ryzyk instytucjonalnych. Eurostat podkreśla jednocześnie ograniczenie: statystyka pierwszych zezwoleń nie obejmuje osób objętych tymczasową ochroną w związku z agresją Rosji na Ukrainę, co ma znaczenie interpretacyjne w przypadku państw granicznych UE (Eurostat, 2024; Eurostat, 2025).

Techniki analityczne obejmowały: opis trendów i punktów zwrotnych, obliczenie współczynników korelacji Pearsona między migracją netto i bezrobociem, regresję pomocniczą OLS z kontrolą trendu czasowego (rok) w celu sprawdzenia, czy relacja nie jest artefaktem współzmienności z czasem. Wyniki traktowane są jako ilustracyjne, ponieważ relacje migracji i rynku pracy są współokreślane przez liczne czynniki (koniunktura, zmiany polityk, struktura sektorowa, inwestycje, opóźnienia), co silnie ogranicza wnioskowanie przyczynowe na prostych szeregach rocznych (National Academies, 2017; Ottaviano, Peri, 2012).

Polska: migracja netto i bezrobocie w latach 2000-2024

Dane dla Polski pokazują silny trend spadkowy bezrobocia między początkiem lat 2000. a połową lat 2020. (w 2024 r. ok. 2,8% w estymatach modelowanych ILO w WDI). W tym samym czasie saldo migracji netto cechuje się znaczną zmiennością, w tym epizodem skrajnie dodatniego salda w 2022 r. oraz ujemnego w 2024 r. (dla 2024 r. World Bank Data wskazuje wartość – 238 062).



Rysunek 2. Polska migracja netto bezrobocie w latach 2000-2024

Źródło: opracowanie własne na podstawie modelowania estymaty ILO World Bank, 2026b.

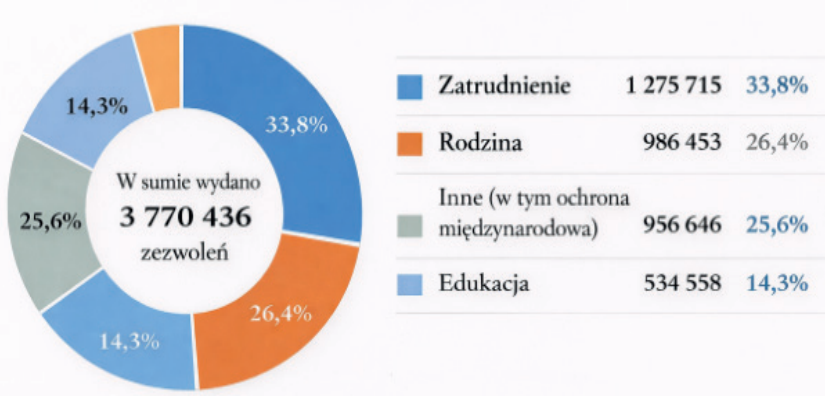
Na podstawie danych 2000-2024 obliczono współczynnik korelacji Pearsona między migracją netto (osoby) a stopą bezrobocia (%): ok. -0,21 (słaba zależność ujemna, obliczenia własne). Przy ograniczeniu próby do lat 2000-2021 korelacja wynosi ok. -0,29. Wynik jest zgodny z tezą literatury, że nie istnieje prosty, stabilny związek liniowy między imigracją a bezrobociem na poziomie całej gospodarki, a średnie efekty agregatowe bywają małe. Wyniki są jednak wrażliwe na epizody skrajne. Po wyłączeniu 2022 r. (roku nietypowego z uwagi na szok migracyjny po agresji Rosji na Ukrainę) korelacja dla lat 2000-2024 zbliża się do zera (ok. 0,05). Taka wrażliwość wspiera interpretację, że korelacje na danych rocznych mogą odzwierciedlać pojedyncze zdarzenia oraz trend długookresowy, a nie mechanizm przyczynowy „migracja – bezrobocie". Z perspektywy bezpieczeństwa gospodarczej odporności państwa to argument za stosowaniem narzędzi monitoringu wielowskaźnikowego i scenariuszowego, a nie jednego miernika. Regresja pomocnicza OLS, w której stopę bezrobocia wyjaśniano migracją netto oraz

zmienną czasową (rok), pokazuje, że po uwzględnieniu trendu czasowego współczynnik przy migracji netto jest statystycznie nieistotny (obliczenia własne), podczas gdy trend czasowy wyjaśnia znaczną część spadku bezrobocia. Taki rezultat jest spójny z podejściem instytucjonalnym: gospodarka dostosowuje się do podaży pracy poprzez reallokacje, inwestycje i zmiany technologiczne, a skutki migracji są współkształtowane przez instytucje rynku pracy i kanały legalizacji zatrudnienia (Ottaviano, Peri 2012; Dias-Abey 2021).

Analiza przedstawionych danych w kontekście bezpieczeństwa gospodarczego wskazuje, że brak wyraźnej i trwałej reakcji agregatowych wskaźników rynku pracy, w tym stopy bezrobocia, na zmiany salda migracji netto nie oznacza braku konsekwencji dla stabilności gospodarki. Oddziaływanie migracji może ujawniać się przede wszystkim poprzez mechanizmy instytucjonalne, które sprzyjają segmentacji rynku pracy oraz powstawaniu nieprawidłowości w zatrudnieniu. W badaniach dotyczących Polski zwraca się uwagę na znaczenie skali zatrudnienia cudzoziemców oraz jego koncentracji w określonych sektorach, takich jak prace sezonowe, rolnictwo czy usługi. Taka struktura zatrudnienia zwiększa ryzyko występowania pracy nierejestrowanej oraz nadużyć wobec pracowników, zwłaszcza w warunkach niewystarczającej kontroli i egzekwowania obowiązujących standardów (Duszczyk, Matuszczyk, OECD, 2018).

Unia Europejska: struktura pierwszych zezwoleń pobytowych w 2023 r.

W 2023 r. w UE wydano ponad 3,7 mln pierwszych zezwoleń pobytowych dla obywateli państw trzecich, co Eurostat określa jako najwyższy poziom w historii tej serii. zatrudnienie było głównym powodem (33,8%, ok. 1,3 mln), następnie: rodzina (26,4%, 986 453), „inne” (25,6%, 956 646, w tym ochrona międzynarodowa) oraz edukacja (14,3%, 534 558). Dane przedstawiono na Rysunku 3.



Rysunek 3. Struktura pierwszych zezwoleń pobytowych w 2023 r, Unia Europejska
Źródło: opracowanie własne na podstawie Eurostat, 2024.

Z punktu widzenia bezpieczeństwa gospodarczego rozróżnienie kanałów ma znaczenie, ponieważ „praca" jako dominujący powód oznacza, że znaczna część napływu jest bezpośrednio powiązana z rynkiem pracy – a więc z kanałem podaży pracy, kosztami pracy, bazą składkową i podatkową, ale także z ryzykami nieprawidłowości zatrudnienia (OECD, 2018). Dodatkowo Eurostat zaznacza, że osoby objęte tymczasową ochroną (np. w związku z wojną w Ukrainie) nie są ujęte w statystyce pierwszych zezwoleń, co jest kluczowe dla porównań państw pierwszego kontaktu (Eurostat, 2024). W nowszych zestawieniach Eurostat (dane zaktualizowane w 2025 r.) wskazuje się, że w 2024 r. łączna liczba pierwszych zezwoleń spadła względem 2023 r., a wśród państw o najwyższych wolumenach Polska pozostaje jednym z kluczowych krajów wydających zezwolenia – co z perspektywy bezpieczeństwa gospodarczego zwiększa wagę zdolności administracyjnych (selekcja, integracja, egzekucja) oraz odporności organizacyjnej systemu.

Dyskusja

Empiryczna ilustracja dla Polski potwierdza wniosek obecny w literaturze, że związek między migracją a bezrobociem mierzony na poziomie całej gospodarki jest zwykle słaby i zmienny, a jego interpretacja wymaga uwzględnienia trendów długookresowych oraz czynników towarzyszących, takich jak cykl koniunkturalny i struktura sektorowa zatrudnienia (Ottaviano, Peri, 2012; Vargas-Silva, Sumption, 2023). Taki wynik nie oznacza jednak,

że migracje pozostają bez znaczenia dla bezpieczeństwa gospodarczego. Oznacza on raczej, że bilans korzyści i ryzyk należy oceniać przez pryzmat konkretnych mechanizmów, które działają równolegle i nie zawsze są widoczne w jednym agregatowym wskaźniku rynku pracy. Znaczenie mają w szczególności procesy dopasowania na rynku pracy, poziom formalizacji zatrudnienia, skutki fiskalne w cyklu życia oraz wpływ migracji na ciągłość świadczenia usług w sektorach, w których występują trwałe braki kadrowe (National Academies of Sciences, Engineering, and Medicine, 2017; Blau, Hunt, 2019; International Monetary Fund, 2016). W praktyce bezpieczeństwo gospodarcze państwa można ująć jako rezultat współdziałania trzech elementów. Pierwszym elementem jest ekspozycja na ryzyko, która obejmuje skalę napływu, tempo zmian oraz strukturę migracji według kanału pobytu i aktywności na rynku pracy. Drugim elementem jest podatność, którą tworzą między innymi segmentacja rynku pracy, nierówności, zależność pracowników od pośredników oraz koncentracja zatrudnienia w sektorach niskopłatnych i wysokiego ryzyka naruszeń. Trzecim elementem jest odporność instytucjonalna, rozumiana jako zdolność państwa do egzekwowania prawa, prowadzenia działań kontrolnych, wspierania integracji, zarządzania informacją oraz skutecznego reagowania na nadużycia. Takie ujęcie jest spójne z podejściem ukierunkowanym na ograniczanie ryzyka w politykach publicznych oraz z definicjami akcentującymi ochronę krytycznych funkcji gospodarki i państwa (Komisja Europejska, 2023; OECD, 2025).

W literaturze oraz w dokumentach OECD problem nieprawidłowości w zatrudnieniu cudzoziemców jest wskazywany jako obszar o realnych konsekwencjach ekonomicznych. Zjawisko to może obniżać dochody publiczne poprzez ubytek podatków i składek, zaburzać warunki uczciwej konkurencji między przedsiębiorstwami oraz osłabiać spójność społeczną, ponieważ wzmacnia przekonanie o nierównym stosowaniu reguł (OECD, 2018). Definicje operacyjne pracy nierejestrowanej stosowane przez Eurofound dodatkowo podkreślają bezpośredni związek z bezpieczeństwem fiskalnym, ponieważ praca legalna co do charakteru staje się problemem publicznym wtedy, gdy nie jest deklarowana wobec instytucji państwa (Eurofound, 2026). Do tej grupy ryzyk dochodzi problem eksploatacji pracy. Globalne estymaty współczesnego niewolnictwa, w tym pracy przymusowej, wskazują, że nie tylko skala migracji ma znaczenie, lecz także konfiguracja zależności

prawno-ekonomicznych, która może obejmować podporządkowanie pobytu jednemu pracodawcy, zadłużenie wobec pośredników, bariery językowe lub brak dostępu do informacji o prawach. Taka konfiguracja generuje koszty dla państwa w wymiarze prawnym, społecznym i ekonomicznym, a do kosztów ekonomicznych należą między innymi obciążenia związane z kontrolą, postępowaniami, wsparciem ofiar oraz koszty reputacyjne ładu regulacyjnego (International Labour Organization, Walk Free, International Organization for Migration, 2022; European Labour Authority, European Union Agency for Fundamental Rights, 2025).

Uwzględnienie wymiaru cyfrowego jest uzasadnione tym, że funkcjonowanie współczesnej gospodarki i administracji zależy od systemów informacyjnych i usług cyfrowych, a zakłócenia w tym obszarze mogą przenosić się na ciągłość świadczenia usług publicznych oraz zdolność egzekwowania regulacji. OECD wprost zalicza cyberbezpieczeństwo do komponentów bezpieczeństwa gospodarczego, ponieważ ochrona zasobów i funkcji krytycznych obejmuje także sferę cyfrową (OECD, 2025). W praktyce procesy związane z legalizacją pobytu i pracy, obsługą wniosków oraz wymianą danych między instytucjami są coraz częściej prowadzone elektronicznie, co zwiększa efektywność zarządzania, ale równocześnie poszerza powierzchnię ryzyka. Ryzyko to ma wymiar praktyczny. ENISA wskazuje na wysoką ekspozycję administracji publicznej na ataki, w tym na zakłócenia dostępności usług, naruszenia danych i manipulacje socjotechniczne, a to może wpływać na ciągłość procesów administracyjnych istotnych dla rynku pracy i legalności zatrudnienia (ENISA, 2025). Z kolei dyrektywa NIS2 wzmacnia wspólne ramy zarządzania ryzykiem cybernetycznym i raportowania incydentów, co ma znaczenie dla ochrony roli państwa jako usługodawcy i regulatora w obszarach gospodarczo wrażliwych (Unia Europejska, 2022).

W celu przełożenia modelu pojęciowego na narzędzie analityczne można zastosować tablicę wskaźników opartą na pięciu wymiarach bezpieczeństwa gospodarczego oraz na dwóch ryzykach przekrojowych, którymi są eksploatacja pracy i odporność cyfrowa (Tabela 1). Taka konstrukcja ułatwia analizę trendów, identyfikację punktów zapalnych oraz ocenę skutków działań regulacyjnych zgodnie z logiką zarządzania ryzykiem i wzmacniania odporności (Komisja Europejska, 2023; OECD, 2025). Tablica wskaźników nie przesądza o kierunku efektów, ponieważ zakłada, że bilans korzyści

i kosztów zależy od skali migracji, struktury kwalifikacji, kanału pobytu oraz jakości instytucji. Jest to zgodne z ustaleniami literatury dla Polski i Unii Europejskiej, które akcentują rolę instytucji i specyfikę fal migracyjnych, w tym migracji z Ukrainy (Duszczyk, Kaczmarczyk, 2022; Postek, Walerych, 2026).

Tabela 1. Propozycja minimalnego zestawu wskaźników monitoringu

Wymiar bezpieczeństwa gospodarczego	Główny mechanizm oddziaływania migracji	Przykładowe wskaźniki minimalne	Interpretacja ryzyka i korzyści	Przykładowe źródła danych
Rynek pracy i podaż pracy	Uzupełnianie niedoborów oraz dopasowanie kompetencji	Stopa bezrobocia ILOEST, stopa wakatów, relacja liczby wakatów do liczby bezrobotnych, udział cudzoziemców w zatrudnieniu	Małe efekty średnie w skali kraju mogą współwystępować z silnymi efektami sektorowymi i regionalnymi	WDI ILOEST, Eurostat vacancy rate, dane administracyjne
Bezpieczeństwo fiskalne	Zmiana bazy podatkowej i składkowej oraz efekt cyklu życia	Udział pracujących cudzoziemców objętych ubezpieczeniami, wpływy ze składek, struktura wieku i aktywności zawodowej migrantów, saldo fiskalne kohort	Kluczowe znaczenie mają legalność zatrudnienia, poziom wynagrodzeń i profil demograficzny migracji	Dane krajowe ZUS i podatkowe, National Academies of Sciences, Engineering, and Medicine (2017)
Produktywność i innowacyjność	Komplementarność kwalifikacji oraz dyfuzja wiedzy	Produktywność pracy, łączna produktywność czynników produkcji TFP, udział migrantów w zawodach wysokich kwalifikacji, wskaźniki niedopasowania kwalifikacji	Efekty dodatnie są bardziej prawdopodobne przy szybkiej integracji i redukcji barier na rynku pracy	IMF (2016), OECD, Eurostat, badania firmowe

Wymiar bezpieczeństwa gospodarczego	Główny mechanizm oddziaływania migracji	Przykładowe wskaźniki minimalne	Interpretacja ryzyka i korzyści	Przykładowe źródła danych
Ciągłość usług i odporność sektorowa	Obsada sektorów krytycznych oraz redukcja wąskich gardeł kadrowych	Udział migrantów w sektorach krytycznych, rotacja kadr, czas obsadzenia wakatu, wskaźniki braków kadrowych	Migracja może stabilizować usługi, ale w sektorach niskopłatnych rośnie ryzyko nadużyć oraz wysokiej rotacji	Eurostat LFS, dane branżowe, ELA i FRA (2025)
Integralność instytucjonalna i spójność społeczna	Formalizacja zatrudnienia oraz egzekwowanie standardów	Szacunki pracy nierejestrowanej, wyniki kontroli inspekcji pracy, liczba stwierdzonych naruszeń, skuteczność postępowań wobec pośredników	Wzrost nieprawidłowości obniża dochody publiczne i zaufanie do reguł, a to pogarsza warunki stabilności gospodarczej	OECD (2018), Eurofound (b.d.), dane inspekcji pracy
Ryzyko eksploatacji przekrojowe	Zależność od pośredników oraz słaby status prawny i informacyjny	Liczba postępowań dotyczących pracy przymusowej, zgłoszenia do instytucji kontrolnych, wskaźniki handlu ludźmi w celu pracy	Wysoki koszt społeczny i prawny wpływa na legitymizację polityk oraz koszty państwa	ILO (2022), ELA i FRA (2025), dane krajowe
Odporność cyfrowa przekrojowe	Ciągłość usług i ochrona danych w administracji	Liczba incydentów cyber dotyczących administracji, dostępność usług elektronicznych, średni czas odtworzenia usług, poziom wdrożenia wymogów NIS2	Incydenty cyber mogą ograniczać zdolność legalizacji pobytu i pracy oraz osłabiać egzekucję prawa	ENISA (2025), krajowe zespoły reagowania, Unia Europejska (2022)

Źródło: opracowanie własne.

Wnioski

Uporządkowanie aparatu pojęciowego prowadzi do wniosku, że bezpieczeństwo gospodarcze państwa w analizie migracji zarobkowych wymaga ujęcia szerokiego. Obejmuje ono jednocześnie stabilność makroekonomiczną, ciągłość świadczenia usług, odporność instytucji publicznych oraz zdolność do identyfikacji i zarządzania ryzykiem. W takim ujęciu stopa bezrobocia pozostaje wskaźnikiem ważnym, ale niewystarczającym do oceny konsekwencji migracji. Perspektywa ta jest zgodna z podejściem OECD, które akcentuje ochronę krytycznych funkcji gospodarki, oraz z unijną strategią ograniczania ryzyk, która koncentruje się na mapowaniu zależności i projektowaniu odpowiedzi politycznych w warunkach silnej współzależności gospodarczej (OECD, 2025; Komisja Europejska, 2023).

Część empiryczna dla Polski w latach 2000-2024 wskazuje, że zależność między saldem migracji netto a stopą bezrobocia jest słaba, a przebieg obu szeregów jest w dużej mierze kształtowany przez trendy długookresowe. Jednocześnie wyniki okazują się wrażliwe na epizody skrajne, w szczególności na rok 2022, co potwierdza, że proste korelacje na danych rocznych nie powinny stanowić podstawy wnioskowania o wpływ migracji na bezpieczeństwo gospodarcze. Większą wartość analityczną ma systematyczne monitorowanie kanałów instytucjonalnych i sektorowych, zwłaszcza tych, które dotyczą formalizacji zatrudnienia, segmentacji rynku pracy oraz ryzyk pracy nierejestrowanej. Te kanały wpływają bezpośrednio na bezpieczeństwo fiskalne, warunki uczciwej konkurencji oraz zaufanie do reguł, a tym samym na stabilność funkcjonowania gospodarki (OECD, 2018; Eurofound, 2026). Analiza danych dla Unii Europejskiej pokazuje, że w 2023 r. dominującym powodem wydawania pierwszych zezwoleń pobytowych była praca, co oznacza, że znaczna część napływu jest bezpośrednio powiązana z rynkiem pracy i mechanizmami podaży pracy. Taki profil struktury zezwoleń zwiększa znaczenie zdolności państwa do prowadzenia selekcji i dopasowania podaży pracy do potrzeb gospodarki, do wspierania integracji w obszarach kwalifikacji, języka i warunków bytowych, a także do egzekwowania standardów zatrudnienia oraz ograniczania nadużyć i nieprawidłowości. Znaczenie administracyjnej sprawności jest dodatkowo wzmacniane przez fakt, że statystyka pierwszych zezwoleń nie obejmuje osób objętych tymczasową

ochroną, co komplikuje porównania państw i wymaga ostrożnej interpretacji danych w krajach szczególnie obciążonych migracyjnie (Eurostat, 2024; OECD, 2018).

Włączenie wymiaru cyfrowego należy traktować jako integralny element analizy, a nie jako uzupełnienie. Cyberodporność administracji publicznej wpływa na ciągłość usług, bezpieczeństwo danych i sprawność procesów, od których zależy legalizacja pobytu i pracy, wymiana informacji między instytucjami oraz skuteczność kontroli i egzekwowania prawa. Oznacza to, że zdolność państwa do realizacji polityki migracyjnej i ochrony rynku pracy jest w praktyce warunkowana poziomem bezpieczeństwa systemów informatycznych. W tym kontekście znaczenie mają zarówno ramy prawne wynikające z dyrektywy NIS2, jak i analizy wskazujące na wysoką ekspozycję administracji publicznej na incydenty cybernetyczne oraz ryzyko zakłóceń usług publicznych (Unia Europejska, 2022; ENISA, 2025; OECD, 2025).

W konsekwencji opracowanie uzasadnia podejście oparte na tablicy wskaźników, w której migracje są monitorowane równolegle w kilku wymiarach bezpieczeństwa gospodarczego. Taka operacjonalizacja obejmuje jednoczesne śledzenie wskaźników rynku pracy, bezpieczeństwa fiskalnego, produktywności i innowacyjności, ciągłości usług oraz ładu instytucjonalnego, a także uwzględnia ryzyka przekrojowe związane z eksploatacją pracy i odpornością cyfrową. Dopiero zestawienie tych obszarów w jednym narzędziu monitorującym pozwala rzetelnie oceniać bilans korzyści i ryzyk w sposób użyteczny dla administracji publicznej oraz analityki polityk publicznych, ponieważ odzwierciedla wielokanałowy i instytucjonalnie uwarunkowany charakter oddziaływania migracji na gospodarkę (Komisja Europejska, 2023; OECD, 2025).

Literatura

1. Blau, F. D., Hunt, J. (2019). The economic and fiscal consequences of immigration: Highlights from the National Academies report. *Business Economics, 54*(3), 173-176. https://doi.org/10.1057/s11369-019-00132-9
2. Dias-Abey, M. (2021). Determining the impact of migration on labour markets: The mediating role of legal institutions. *Industrial Law Journal, 50*(4), 532-557. https://doi.org/10.1093/indlaw/dwab030

3. Duszczyk, M., Kaczmarczyk, P. (2022). The war in Ukraine and migration to Poland: Outlook and challenges. *Intereconomics, 57*(3), 164-170. https://doi.org/10.1007/s10272-022-1053-6
4. Duszczyk, M., Matuszczyk, K. (2018). The employment of foreigners in Poland and the labour market situation. *Central and Eastern European Migration Review, 7*(2), 53-68. https://doi.org/10.17467/ceemr.2018.07
5. European Commission. (2023). *Joint communication to the European Parliament, the European Council and the Council on the "European Economic Security Strategy" (JOIN/2023/20 final*, *CELEX: 52023JC0020).* Pobrane z: https://ec.europa.eu (dostęp: 15.06.2026).
6. European Labour Authority, European Union Agency for Fundamental Rights. (2025, October 10). *Detecting and addressing labour exploitation: A guide for labour inspectors*. Pobrane z: https://www.publicnow.com/view/E2F0124DF4EB7C87C518AC85180D5E9B7F35E676 (dostęp: 15.06.2026).
7. European Parliament and the Council of the European Union. (2022, December 14). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333*, 80-152. Pobrane z: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (dostęp: 15.06.2026).
8. European Union Agency for Cybersecurity. (2025). *ENISA sectorial threat landscape – Public administration (Public Administration Threat Landscape 2024) (Version 1.2, revision notice January 9, 2026)*. Pobrane z: https://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape-public-administration (dostęp: 15.06.2026).
9. Eurofound. (Undeclared work. Retrieved February 11, 2026.
10. Eurostat. (2024). *More than 3.7 million first residence permits in 2023*. Eurostat News.
11. Eurostat. (2025). *Population structure and ageing. Statistics Explained (Data extracted in February 2025)*. Retrieved February 11, 2026.
12. Eurostat. (2025). *Residence permits – statistics on first permits issued during the year. Statistics Explained (Data extracted in September 12, 2025).* Retrieved February 11, 2026.

13. International Labour Organization, Department of Statistics. (2026). *ILO modelled estimates: Methodological overview (TEM).*
14. International Labour Organization. (2023). *ILO modelled estimates: Methodological overview (ILOSTAT methods page).*
15. International Labour Organization, Walk Free, International Organization for Migration. (2022). *Global estimates of modern slavery: Forced labour and forced marriage*.
16. International Monetary Fund. (2016). *Impact of migration on income levels in advanced economies (Spillover Notes No. 2016/008).*
17. Jackiewicz, A., Trzaskowska-Dmoch, A. (red.). (2018). *Bezpieczeństwo ekonomiczne państwa: Uwarunkowania, procesy, skutki.* CeDeWu.
18. Księżopolski, K. M. (2011). *Bezpieczeństwo ekonomiczne*. Dom Wydawniczy Elipsa.
19. Longhi, S., Nijkamp, P., Poot, J. (2005). A meta-analytic assessment of the effect of immigration on wages. *Journal of Economic Surveys, 19*(3), 451-477. https://doi.org/10.1111/j.0950-0804.2005.00255.x
20. Longhi, S., Nijkamp, P., Poot, J. (2010). Joint impacts of immigration on wages and employment: Review and meta-analysis. *Journal of Geographical Systems, 12*(4), 355-387. https://doi.org/10.1007/s10109-010-0111-y
21. National Academies of Sciences, Engineering, and Medicine. (2017). *The economic and fiscal consequences of immigration*. National Academies Press.
22. OECD. (2018). *Addressing the illegal employment of foreign workers. In International Migration Outlook 2018 (Chapter 4).* OECD Publishing.
23. OECD. (2025). *Economic security in a changing world*. OECD Publishing.
24. Osberg, L. (2015). *How should one measure economic insecurity? (OECD Statistics Working Papers No. 2015/01)*. OECD Publishing.
25. Ottaviano, G. I. P., Peri, G. (2012). Rethinking the effect of immigration on wages. *Journal of the European Economic Association, 10*(1), 152-197. https://doi.org/10.1111/j.1542-4774.2011.01052.x
26. Postek, Ł., Walerych, M. (2026). The impact of Ukrainian immigration on labour market dynamics in Poland: A Bayesian VAR analysis. *Economic Modelling, 155*, 107441. https://doi.org/10.1016/j.econmod.2025.107441

27. Vargas-Silva, C., Sumption, M. (2023). *The labour market effects of immigration (Briefing, 6th revision).* Oxford Migration Observatory.
28. World Bank. (2026a). *Net migration (SM.POP.NETM) – Poland (World Development Indicators).*
29. World Bank. (2026b). *Unemployment, total (% of total labor force) (modeled ILO estimate) (SL.UEM.TOTL.ZS) – Poland (World Development Indicators, ILOEST/ILOSTAT as original source per WDI metadata).*

Karolina Włodarczyk[1]

https://doi.org/10.29316/9788368103373_10

ZATRUDNIANIE CUDZOZIEMCÓW SPOZA UNII EUROPEJSKIEJ – SZANSE I ZAGROŻENIA DLA BEZPIECZEŃSTWA GOSPODARCZEGO PAŃSTWA

EMPLOYING NON-EU FOREIGN NATIONALS – OPPORTUNITIES AND RISKS FOR NATIONAL ECONOMIC SECURITY

Streszczenie

Celem rozdziału jest analiza wpływu zatrudniania cudzoziemców spoza Unii Europejskiej na bezpieczeństwo społeczno-gospodarcze Polski, ze szczególnym uwzględnieniem ostatnich pięciu lat. Problem badawczy sformułowano: W jakim stopniu zatrudnianie cudzoziemców spoza Unii Europejskiej wpływa na bezpieczeństwo społeczno-gospodarcze Polski? W ramach problemu głównego postawiono następujące pytanie szczegółowe: Jakie szanse (korzyści) oraz zagrożenia (koszty i ryzyka) dla gospodarki narodowej wiążą się z rosnącym udziałem imigrantów zarobkowych z krajów trzecich na polskim rynku pracy? Hipoteza badawcza zakłada, iż zatrudnianie cudzoziemców spoza Unii Europejskiej w Polsce w ujęciu makroekonomicznym wzmacnia bezpieczeństwo społeczno-gospodarcze państwa poprzez łagodzenie niedoborów siły roboczej, wspieranie wzrostu gospodarczego

[1] https://orcid.org/0009-0005-2201-2357, e-mail: karolina@wlodarczyk.biz.pl

oraz stabilizację systemu finansów publicznych, jednak przy braku spójnej polityki migracyjnej i skutecznych mechanizmów integracyjnych może generować zagrożenia społeczne i instytucjonalne, ograniczające długofalowe korzyści tego procesu. Wykorzystano metodę analizy literatury przedmiotu oraz danych empirycznych (statystyki GUS, ZUS, raporty badawcze) z lat 2019-2023. Przeprowadzono przegląd literatury w dziedzinie nauk o bezpieczeństwie i ekonomii, a także analizę danych statystycznych dotyczących zatrudnienia cudzoziemców w Polsce. Wyniki mogą służyć decydentom politycznym oraz instytucjom rynku pracy do opracowania zrównoważonych strategii migracyjnych, które maksymalizują pozytywne efekty ekonomiczne migracji zarobkowej, jednocześnie minimalizując potencjalne zagrożenia dla stabilności społeczno-ekonomicznej. Wnioski płynące z badań podkreślają potrzebę efektywnego zarządzania migracjami zarobkowymi poprzez usprawnienie procedur legalizacji pracy, działania na rzecz integracji cudzoziemców oraz wzmocnienie nadzoru nad rynkiem pracy, tak aby zatrudnianie cudzoziemców przekładało się na trwałe wzmocnienie bezpieczeństwa społeczno-gospodarczego kraju.

Słowa kluczowe: cudzoziemcy, rynek pracy, migracje zarobkowe, bezpieczeństwo ekonomiczne, polityka migracyjna, Polska

Abstract

The aim of the chapter is to analyse the impact of employing foreigners from outside the European Union on Poland's socio-economic security, with particular emphasis on the last five years. The research problem is formulated: what opportunities (benefits) and threats (costs and risks) for the national economy are associated with the growing share of economic immigrants from third countries on the Polish labour market? The research problem was formulated: To what extent does employing foreigners from outside the European Union affect the socio-economic security of the Polish? The research hypothesis assumes that employing foreigners from outside the European Union in Poland in macroeconomic terms strengthens the socio-economic security of the country by mitigating labour shortages, supporting economic growth and stabilising the public finance system, but in the absence of a coherent migration policy and effective integration mechanisms, it may generate social and institutional threats, limiting the long-term benefits of this process. The analysis of the literature on the subject and of empirical data (statistics from the Central Statistical Office, the Social Insurance Institution, and research reports) from 2019 to 2023 was used. A review of the literature in the fields of security sciences and economics was conducted, along with an analysis of statistical data on the employment of foreigners in Poland. The results can be used by policymakers and labour market institutions to develop sustainable migration strategies that maximise the positive economic effects of labour migration while minimising potential risks

to socio-economic stability. The research concludes that effective management of labour migration requires improving procedures for legalising work, promoting the integration of foreigners, and strengthening labour market supervision, so that the employment of foreigners contributes to a permanent strengthening of the country's socio-economic security.

Keywords: foreign workers, labour market, labour migration, economic security, migration policy, Poland

Wstęp

Współczesne procesy migracyjne stanowią jedno z kluczowych wyzwań społecznych, ekonomicznych i politycznych państw XXI wieku. W warunkach postępującej globalizacji, nierównomiernego rozwoju gospodarczego oraz narastających kryzysów o charakterze demograficznym, migracja zarobkowa staje się nie tylko zjawiskiem społecznym, lecz także istotnym elementem bezpieczeństwa państwa. Szczególne znaczenie w tym kontekście ma zatrudnianie cudzoziemców pochodzących z państw spoza Unii Europejskiej, które coraz wyraźniej wpływa na funkcjonowanie rynków pracy, systemów zabezpieczenia społecznego oraz stabilność społeczno-ekonomiczną krajów przyjmujących. Polska, która przez dziesięciolecia była przede wszystkim krajem emigracji, w ostatnich latach doświadczyła dynamicznej transformacji w kierunku państwa imigracyjnego. Rosnące zapotrzebowanie na pracowników, pogłębiające się niedobory siły roboczej wynikające z niekorzystnych trendów demograficznych oraz zmiany regulacyjne sprzyjające legalizacji pracy cudzoziemców doprowadziły do bezprecedensowego wzrostu liczby imigrantów zarobkowych. Proces ten uległ dodatkowej intensyfikacji w wyniku kryzysów zewnętrznych, w szczególności wojny w Ukrainie, która znacząco zmieniła skalę i strukturę migracji do Polski (European Labour Authority, 2023).

Zatrudnianie cudzoziemców spoza UE generuje jednocześnie szereg szans i zagrożeń. Z jednej strony przyczynia się do podtrzymania wzrostu gospodarczego, łagodzenia niedoborów kadrowych oraz stabilizacji systemów finansów publicznych. Z drugiej – rodzi wyzwania związane z integracją społeczną, presją na infrastrukturę publiczną, funkcjonowaniem rynku pracy oraz skutecznością polityki migracyjnej państwa. W tym sensie

migracja zarobkowa przestaje być wyłącznie kwestią ekonomiczną, a staje się istotnym komponentem bezpieczeństwa społeczno-gospodarczego i wewnętrznego państwa.

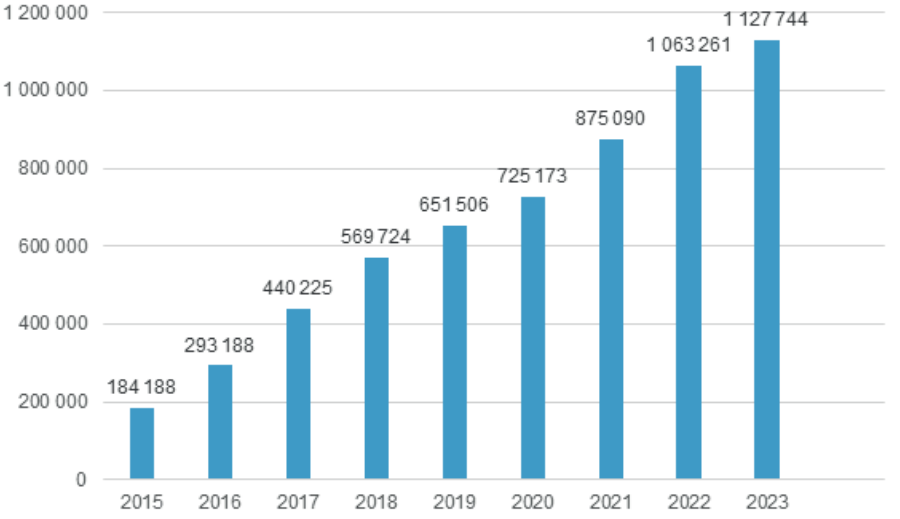
Teoretyczne ujęcie migracji zarobkowej i bezpieczeństwa ekonomicznego państwa

Polska, przez wiele dekad będąca krajem emigracji netto, w ostatnich latach doświadcza istotnej zmiany w kierunku stawania się krajem imigracji. Napływ cudzoziemców, zwłaszcza pochodzących z państw spoza Unii Europejskiej, znacząco nasilił się w drugiej połowie lat 2010. Szczególnie widoczny jest wzrost migracji zarobkowych z krajów sąsiednich spoza UE (takich jak Ukraina czy Białoruś), które przybrały na sile po 2014 r., a następnie eksplodowały po roku 2017 wraz z liberalizacją przepisów i rosnącym zapotrzebowaniem na pracowników w Polsce (Dębkowska, Kłosiewicz-Górecka, Szymańska, Wejt-Knyżewska, Zybertowicz, 2024, s. 6).

Kulminacją trendu był bezprecedensowy napływ uchodźców wojennych z Ukrainy po wybuchu pełnoskalowej wojny w lutym 2022 r., co z jednej strony zwiększyło populację cudzoziemców w Polsce, z drugiej zaś spowodowało częściowy odpływ ukraińskich pracowników (głównie mężczyzn) wracających do kraju w celu jego obrony. W rezultacie tych procesów Polska osiągnęła rekordową liczbę ponad miliona cudzoziemców aktywnych na rynku pracy – według GUS na koniec grudnia 2023 r. ponad 1,0 mln osób niebędących obywatelami RP wykonywało pracę w Polsce, co stanowiło 6,6% ogółu pracujących (dla porównania, udział ten wynosił 5,2% na początku 2022 r.) (GUS, 2024). Z kolei dane ZUS wskazują, że we wrześniu 2024 r. liczba obcokrajowców zgłoszonych do ubezpieczeń społecznych sięgnęła 1,177 mln – podczas gdy dekadę wcześniej (2014) było to zaledwie ok. 0,18 mln. Rysunek 1 ilustruje dynamiczny, ponad sześciokrotny wzrost liczby ubezpieczonych cudzoziemców w Polsce w latach 2015-2023 (Gi Group, 2024), odzwierciedlający skalę przemian rynku pracy.

Rosnąca obecność cudzoziemców – w przeważającej mierze obywateli państw trzecich (spoza UE) – rodzi pytania o jej wpływ na bezpieczeństwo społeczno-gospodarcze państwa. Bezpieczeństwo ekonomiczne państwa można ogólnie zdefiniować jako stan sprawnego, niezakłóconego funkcjonowania gospodarki narodowej, z zachowaniem kluczowych wskaźników

rozwojowych oraz równowagi ekonomicznej. W kontekście rynku pracy oznacza to m.in. zdolność kraju do utrzymania stabilności zatrudnienia, wzrostu gospodarczego oraz ładu społecznego pomimo wewnętrznych i zewnętrznych czynników wpływających na gospodarkę. Napływ pracowników z zagranicy może wzmacniać owo bezpieczeństwo (np. poprzez uzupełnienie niedoboru siły roboczej i zwiększenie bazy podatkowej), ale może też generować nowe zagrożenia (np. napięcia społeczne, presję na system socjalny czy ryzyka związane z integracją imigrantów) (Elak i in., 2024).



Rysunek 1. Liczba cudzoziemców zgłoszonych do ubezpieczeń społecznych w Polsce (stan na koniec danego roku)

Źródło: opracowanie własne na podstawie danych ZUS, 2024.

Zagadnienie wpływu imigracji zarobkowej na gospodarkę państwa goszczącego jest od lat przedmiotem zainteresowania badaczy z zakresu ekonomii i nauk o bezpieczeństwie. W literaturze przedmiotu podkreśla się, że długookresowy efekt imigracji polega na zwiększeniu liczby pracujących i potencjału wzrostu gospodarczego kraju przyjmującego (Wysieńska, Karpiński, 2011, s. 4). Napływ pracowników z zagranicy powiększa zasoby pracy, co przy odpowiednim wykorzystaniu może przekładać się na wyższe PKB oraz większe wpływy podatkowe i składkowe. Jak zauważa się w opracowaniach OECD i instytucji finansowych, imigranci często uzupełniają luki

na rynku pracy wynikające z deficytu rodzimej siły roboczej – dotyczące zarówno prac nisko wykwalifikowanych, których obywatele kraju przyjmującego nie chcą podejmować, jak i niektórych zawodów wyspecjalizowanych cierpiących na niedobory kandydatów (Dębkowska i in., 2024, s. 41). Z tego względu migranci zarobkowi postrzegani są nierzadko jako *„ratunek"* dla rynków pracy borykających się ze starzeniem się społeczeństwa i emigracją ludności rodzimej (Bankier.pl., 2025).

Prognozy demograficzne dla Polski wskazują, że do 2035 r. liczba osób w wieku produkcyjnym spadnie o ok. 2,1 mln (czyli 12-13% obecnej populacji pracujących) na skutek niskiej dzietności i przechodzenia wyżu demograficznego na emerytury. Imigracja może częściowo złagodzić ten ubytek – według szacunków Polskiego Instytutu Ekonomicznego utrzymanie obecnej relacji liczby pracujących do emerytów wymagałoby napływu ok. 2,3 mln dodatkowych migrantów do 2033 r. Choć tak duża skala imigracji jest mało realna, dane te unaoczniają, że bez udziału cudzoziemców polski rynek pracy czekają poważne niedobory kadrowe w wielu sektorach (prognozowana luka to m.in. 800 tys. wakatów w przemyśle i ok. 400 tys. w handlu do 2035 r. (Wielkopolski Związek Pracodawców, 2025).

Z drugiej strony, literatura przedmiotu zwraca uwagę na krótkookresowe i sektorowe skutki uboczne imigracji. Teoria ekonomii klasycznej sugeruje, że napływ pracowników może zwiększać podaż pracy i wywierać presję na płace w sektorach nisko wykwalifikowanych, zwłaszcza jeśli imigranci konkurują o te same stanowiska co miejscowi pracownicy. W praktyce jednak wiele badań empirycznych nie potwierdza istotnego negatywnego wpływu imigracji na wynagrodzenia lub zatrudnienie ludności rodzimej – migranci często zajmują nisze rynkowe, których nie wypełnia lokalna siła robocza, lub też ich przyjazd zbiega się ze wzrostem popytu na pracę. Przykładowo, Narodowy Bank Polski wskazuje, że imigranci z Ukrainy w Polsce cechują się bardzo wysoką aktywnością zawodową (ok. 78% z nich podejmuje pracę, co jest wyższym odsetkiem niż wśród obywateli polskich), a zarazem znacząca część z nich wykonuje prace poniżej swoich kwalifikacji i za niższe wynagrodzenia niż średnia krajowa. Mediana miesięcznych zarobków netto pracujących obywateli Ukrainy wynosi ok. 4500 zł, podczas gdy mediana dla ogółu pracowników w Polsce jest wyższa. Świadczy to o koncentracji imigrantów w sektorach o niższych płacach (np. usługach prostych,

budownictwie, przemyśle przetwórczym) oraz o istnieniu *„premii za lokalność"* – polscy pracodawcy często są skłonni płacić nieco mniej pracownikom zagranicznym niż krajowym na analogicznych stanowiskach. Niemniej, w ujęciu makroekonomicznym wpływ ten jest kompensowany przez ogólny wzrost produkcji i konsumpcji. Co więcej, dzięki imigracji bariera podażowa pracy ulega złagodzeniu, co zapobiega nadmiernym wzrostom płac mogącym wywołać spiralę kosztów i spadek konkurencyjności gospodarki. Jak zauważa raport Fundacji FOR, migracja zarobkowa przyczyniła się do utrzymania wysokiego tempa wzrostu polskiej gospodarki po 2014 r., nie powodując jednocześnie istotnego wzrostu bezrobocia ani spadku wynagrodzeń realnych miejscowych pracowników (Zywert, 2023, s. 67).

Literatura z obszaru nauk o bezpieczeństwie podkreśla natomiast społeczne i polityczne implikacje migracji, które mogą stanowić wyzwanie dla bezpieczeństwa wewnętrznego państwa. Wzrost liczby imigrantów wymusza podjęcie działań w zakresie ich integracji społecznej, zapobiegania gettoizacji oraz konfliktom na tle kulturowym. Homogeniczna etnicznie i kulturowo przez wiele lat Polska stoi przed wyzwaniem akomodacji rosnącej grupy obcokrajowców w społeczeństwie. Badania opinii publicznej pokazują, że Polacy generalnie dostrzegają pozytywy ekonomiczne obecności cudzoziemców, lecz wyrażają też pewne obawy. Według raportu Polskiego Instytutu Ekonomicznego większość Polaków (ok. 60%) uważa, że imigranci stanowią konkurencję głównie dla rodzimych pracowników nisko wykwalifikowanych, podczas gdy w odniesieniu do prac wysoko wykwalifikowanych tylko co czwarty badany postrzega cudzoziemców jako zagrożenie. Jednocześnie prawie połowa ankietowanych dostrzega dużą korzyść z wypełniania przez cudzoziemców luk na rynku pracy i uważa, że przekłada się to na zwiększone wpływy do budżetu państwa (np. w postaci podatków i składek). Obawy społeczne dotyczą natomiast głównie potencjalnego wzrostu wydatków publicznych związanych z zapewnieniem świadczeń dla imigrantów (tak twierdzi ponad połowa badanych) oraz ryzyka niepokojów społecznych – aż 55% respondentów w badaniu PIE wyraziło obawę, że napływ cudzoziemców może prowadzić do napięć czy konfliktów w społeczeństwie. Tego typu obawy nie są wyjątkowe dla Polski – badania porównawcze wskazują, że społeczeństwa wielu państw mają skłonność do przeszacowywania liczby imigrantów i przeceniania zagrożeń z nimi związanych. Istotną rolę odgrywa

tu brak rzetelnej informacji oraz bezpośrednich kontaktów – co potwierdza fakt, że Polacy mający osobiste doświadczenia we współpracy lub sąsiedztwie z cudzoziemcami rzadziej postrzegają ich jako konkurencję i częściej deklarują pozytywne nastawienie (Dębkowska i in., 2024, s. 43).

Z perspektywy bezpieczeństwa państwa zarządzanie migracjami staje się kluczowym wyzwaniem. Eksperci wskazują, że konieczne jest wypracowanie spójnej polityki migracyjnej, obejmującej zarówno przyjmowanie imigrantów zarobkowych, jak i ich integrację oraz monitorowanie skutków społeczno-ekonomicznych. W Polsce brak dotąd kompleksowej strategii – próba przyjęcia rządowej *„Polityki migracyjnej Polski"* w latach 2021-2022 zakończyła się wycofaniem projektu dokumentu, a prace nad odrębną ustawą o zatrudnianiu cudzoziemców nie zostały sfinalizowane. W rezultacie działania administracji publicznej mają często charakter doraźny i rozproszony między różne resorty (ministerstwa rodziny i pracy, spraw wewnętrznych, spraw zagranicznych itd.), co utrudnia skuteczne reagowanie na pojawiające się problemy. Literatura sugeruje potrzebę powołania centralnego organu koordynującego politykę migracyjną ponad podziałami resortowymi oraz uproszczenia procedur administracyjnych związanych z legalizacją pobytu i pracy cudzoziemców (Wielkopolski Związek Pracodawców, 2025). Jednocześnie ważne jest zapewnienie odpowiednich instrumentów kontroli i egzekwowania prawa, aby przeciwdziałać nieuczciwym praktykom (np. zatrudnianiu „na czarno", obchodzeniu przepisów przez fikcyjne samozatrudnienie itp.) oraz aby chronić samych migrantów przed wyzyskiem. Wszystkie te działania mają na celu zwiększenie bezpieczeństwa społeczno-gospodarczego poprzez zrównoważenie pozytywnych i negatywnych aspektów migracji.

Podsumowując, przegląd literatury pokazuje dualizm zjawiska zatrudniania cudzoziemców: jest to z jednej strony szansa na złagodzenie kryzysu demograficznego, wsparcie rynku pracy i wzrost gospodarczy, z drugiej – potencjalne źródło napięć społecznych i nowych wyzwań dla polityki państwa. W dalszej części rozdziału przejdziemy do analizy konkretnych danych dotyczących polskiego rynku pracy w ostatnich latach, aby empirycznie zweryfikować i zilustrować te ogólne spostrzeżenia.

Skala, struktura i ekonomiczne znaczenie zatrudnienia cudzoziemców spoza UE w Polsce

Struktura i dynamika zatrudnienia cudzoziemców. Polska w latach 2018-2023 doświadczyła gwałtownego wzrostu liczby cudzoziemców podejmujących pracę. Jak już wspomniano, pod koniec 2023 r. pracę w Polsce wykonywało ponad 1 milion cudzoziemców, z czego przytłaczającą większość (ponad 96%) stanowili obywatele państw spoza UE. Udział obywateli innych krajów Unii Europejskiej okazał się stosunkowo niewielki (tylko ok. 3,5% ogółu pracujących cudzoziemców w 2023 r., w porównaniu do 16% w roku 2015 – oznacza to, że boom migracyjny w Polsce opierał się głównie na imigrantach z krajów trzecich. Najliczniejszą grupą są Ukraińcy, których na koniec 2023 r. było około 759,4 tys., co stanowiło ~67% wszystkich pracujących cudzoziemców. Drugą co do wielkości grupą są Białorusini – ok. 129,4 tys. osób (12%). Znacznie mniejsze, choć zauważalne populacje pracowników stanowią obywatele takich państw jak Gruzja (~26,2 tys., 2%), Indie (~20,5 tys., 2%), Mołdawia (~14,8 tys., 1%), Rosja (~12,4 tys., 1%), a także państw azjatyckich odległych kulturowo od Polski – np. Wietnam (~9,8 tys.), Filipiny (~9,7 tys.) czy Turcja (~9,8 tys.). Pozostali cudzoziemcy pochodzą z ponad 150 różnych państw świata, a łączny odsetek wszystkich tych mniejszych grup narodowościowych wynosi około 17% (tj. ok. 192 tys. osób). Powyższe dane wyraźnie wskazują, że polski rynek pracy stał się w ostatnich latach atrakcyjny przede wszystkim dla migracji ze Wschodu (Europa Wschodnia, Azja Środkowa) oraz z wybranych krajów azjatyckich o nadwyżkach siły roboczej.

Warto podkreślić, że tak znaczny wzrost zatrudnienia cudzoziemców nastąpił pomimo okresowych zakłóceń, takich jak pandemia COVID-19 czy wybuch wojny na Ukrainie. O ile w początkowej fazie pandemii (2020) dynamika migracji nieco osłabła, o tyle już w 2021 r. nastąpiło odbicie – liczba pracujących cudzoziemców wzrosła wtedy o ok. 20% r/r. Jeszcze silniejsze przyspieszenie przyniósł rok 2022: według GUS w trakcie samego 2022 roku populacja pracujących obcokrajowców zwiększyła się o 27,3%, co było związane z napływem uchodźców wojennych z Ukrainy i ich stopniową absorpcją na rynku pracy. Na koniec 2022 r. w Polsce pracowało już 1,004 mln cudzoziemców (6,5% ogółu pracujących), w porównaniu do ~790 tys. na początku tegoż roku. Rok 2023 przyniósł dalszy, choć już wolniejszy wzrost

– między styczniem a grudniem 2023 liczba cudzoziemców w gospodarce narodowej zwiększyła się o kolejne 4,2% (GUS, 2024). Pewne spowolnienie dynamiki w 2023 r. wynikało ze zmian regulacyjnych: wprowadzono specustawę ułatwiającą zatrudnianie uchodźców z Ukrainy bez potrzeby uzyskiwania tradycyjnych zezwoleń na pracę, co paradoksalnie spowodowało spadek liczby rejestrowanych nowych zezwoleń i oświadczeń o powierzeniu pracy w oficjalnych statystykach (w 2023 r. wydano łącznie 1,92 mln dokumentów legalizujących pracę cudzoziemców, tj. mniej niż 2,15 mln w rekordowym 2021 r.). Nie oznacza to jednak realnego zmniejszenia skali zatrudnienia – przeciwnie, cudzoziemcy nadal przybywali do Polski, lecz większa część z nich korzystała z uproszczonych procedur lub tymczasowej ochrony zamiast standardowych pozwoleń.

Ważnym aspektem wpływu imigrantów na rynek pracy jest charakter wykonywanej przez nich pracy. Dane ZUS za 2023 r. wskazują, że ok. 58,8% ubezpieczonych cudzoziemców było zatrudnionych na podstawie umowy o pracę, natomiast 36,3% pracowało w oparciu o umowy cywilnoprawne (zlecenia, umowy agencyjne), a 4,6% prowadziło własną działalność gospodarczą jako osoby samozatrudnione. Oznacza to, że większość pracujących obcokrajowców jest włączona w rynek pracy na zasadach podobnych do pracowników polskich (etat), ale znaczna część działa w bardziej elastycznych formach zatrudnienia. Warto zauważyć, że wśród imigrantów z dłuższym stażem w Polsce rośnie odsetek przedsiębiorców – np. udział samozatrudnionych wśród Ukraińców przybyłych przed 2022 r. wzrósł z ~3% w 2019 r. do 8% w 2025 r., co wskazuje na ich stopniową integrację i rozwijanie własnych inicjatyw biznesowych.

Odnośnie do branż, w których cudzoziemcy znajdują zatrudnienie – dane urzędowe i analizy wskazują na nieco inne rozkłady niż potoczne wyobrażenia społeczne. Według ZUS najwięcej obcokrajowców pracuje w sektorach: usług administracyjnych i wspierających (m.in. firmach outsourcingowych, agencjach pracy tymczasowej), przetwórstwie przemysłowym, a także transporcie i gospodarce magazynowej. To w tych branżach koncentrowała się większość dokumentów legalizujących zatrudnienie cudzoziemców w ostatnich latach. Dla porównania, ankietowani Polacy sądzili, że cudzoziemcy najczęściej pracują w budownictwie, handlu oraz gastronomii. Rzeczywiście, w budownictwie imigranci także stanowią istotną

część siły roboczej (zwłaszcza Ukraińcy i Białorusini jako wykwalifikowani robotnicy budowlani); podobnie w sektorze logistycznym (wielu kierowców zawodowych pochodzi z Ukrainy). Jednak pewne zaskoczenie może budzić duży udział cudzoziemców w usługach administrowania – wynika on z faktu, że liczne agencje zatrudnienia rejestrują pracowników tymczasowych (np. do prac prostych w fabrykach) właśnie w tej kategorii sektoralnej. W efekcie, faktycznie wielu imigrantów wykonuje prace fizyczne lub proste prace usługowe, lecz formalnie są oni rejestrowani przez agencje w sektorze „działalność wspierająca".

Na uwagę zasługuje także coraz większa rola cudzoziemców jako pracodawców i przedsiębiorców w Polsce. W 2023 r. cudzoziemcy założyli co dziesiątą nowo zarejestrowaną firmę w kraju. Zdecydowany prym wiodą tu obywatele Ukrainy – ok. 72% wszystkich nowych działalności gospodarczych zakładanych przez obcokrajowców przypadało na Ukraińców. Oznacza to, że rosnąca społeczność ukraińska w Polsce nie tylko podejmuje pracę najemną, ale też coraz częściej rozwija własne biznesy. Co piąta firma założona przez cudzoziemca należała zaś do obywatela Białorusi, co odzwierciedla falę migracji białoruskiej (m.in. startupów i specjalistów IT) po kryzysie politycznym w 2020 r. i nałożonych na Białoruś sankcjach. Cudzoziemcy najczęściej zakładają firmy w branżach takich jak informacja i komunikacja (ICT), a także w handlu i usługach. Szczególnie obecność przedsiębiorców ukraińskich w sektorze IT jest widoczna – Ukraina od lat dysponuje sporą kadrą informatyków i programistów, z których część przeniosła działalność do Polski, zakładając tu np. spółki czy jednoosobowe działalności.

Imigranci zarobkowi, zwłaszcza ze Wschodu, wypełniają w Polsce głównie wakaty na stanowiskach o niższych wymaganiach płacowych, co z jednej strony czyni polską gospodarkę bardziej konkurencyjną kosztowo, z drugiej zaś oznacza, że zarobki cudzoziemców są przeciętnie niższe niż zarobki Polaków. Wspomniana wcześniej mediana płac ukraińskich imigrantów (~4500 zł netto) jest o kilkanaście procent niższa od mediany krajowej. Przyczyną tego stanu rzeczy jest nie tylko koncentracja w gorzej płatnych sektorach, ale też często niższa pozycja przetargowa cudzoziemców na rynku pracy – wielu z nich podejmuje pracę poniżej kwalifikacji lub na mniej stabilnych warunkach (umowy czasowe, zlecenia). Niemniej jednak, imigranci w Polsce zarabiają wyraźnie więcej niż w swoich krajach

pochodzenia, co stanowi dla nich główną motywację ekonomiczną migracji. Według badań NBP, płaca z pracy w Polsce stanowi ok. 90% dochodów przeciętnego imigranta zarobkowego z Ukrainy (przybyłego przed wojną) i ok. 76% dochodów uchodźcy wojennego. Świadczy to o niewielkim korzystaniu przez nich ze świadczeń socjalnych – ich utrzymanie opiera się przede wszystkim na własnej aktywności zawodowej. Co więcej, znacząca część zarobionych środków jest transferowana do krajów pochodzenia w postaci remittancji wspierających rodziny pozostałe za granicą. Szacunki wskazują, że około 40% imigrantów z Ukrainy przekazuje regularnie środki finansowe krewnym na Ukrainie, a jeszcze większy odsetek (49%) udziela im pomocy rzeczowej (NBP, 2025). Z jednej strony, transfery te oznaczają odpływ części dochodu z polskiej gospodarki, z drugiej jednak przyczyniają się do poprawy sytuacji humanitarnej na Ukrainie i mogą budować kapitał relacji gospodarczych z Polską na przyszłość.

Cudzoziemcy pracujący w Polsce dokładają swoją cegiełkę do finansów publicznych – zarówno poprzez podatki pośrednie (VAT od konsumpcji w Polsce), jak i bezpośrednie (PIT od dochodów) oraz składki na ubezpieczenia społeczne. Według Konfederacji Lewiatan, cudzoziemcy stanowią już ponad 6% wszystkich zatrudnionych w Polsce i odpowiadają za około 5% wpływów do Funduszu Ubezpieczeń Społecznych (ZUS). Jest to istotny wkład, biorąc pod uwagę, że jeszcze dekadę temu składki od imigrantów stanowiły margines wpływów ZUS. Napływ młodych, pracujących cudzoziemców poprawia bieżącą sytuację systemu emerytalnego – odprowadzają oni składki, nie pobierając (jak dotąd) świadczeń, co netto polepsza bilans FUS. Pewnym wyzwaniem może być przyszłość – jeśli znaczna część imigrantów osiedli się na stałe i zestarzeje w Polsce, za kilkanaście czy kilkadziesiąt lat obciążą system emerytalny. Jednak wiele wskazuje, że obecna fala imigracji ma częściowo charakter cyrkulacyjny lub czasowy – znaczna część Ukraińców deklaruje zamiar powrotu do kraju, gdy sytuacja się ustabilizuje. Ponadto, niektórzy cudzoziemcy (zwłaszcza z UE) transferują swoje uprawnienia emerytalne między krajami. Należy jednak odnotować, że polski system zabezpieczenia społecznego w pewnych obszarach już ponosi dodatkowe koszty związane z imigrantami – np. opieka zdrowotna (NFZ) musi obsłużyć zwiększoną populację, a w związku z napływem uchodźców wzrosły wydatki na pomoc społeczną i edukację (dla dzieci uchodźców).

Raport NBP szacuje, że w krajach najbardziej zaangażowanych w pomoc ukraińskim uchodźcom w 2022 r. wydatki publiczne z tego tytułu wzrosły od 1% do nawet 9% w stosunku do sytuacji bez wojny. W przypadku Polski można szacować ten wzrost na kilka punktów procentowych (m.in. świadczenie 300+ na start dla uchodźców, programy mieszkaniowe, edukacja). Warto jednak zauważyć, że pracujący imigranci odciążają system – osoby, które szybko podjęły pracę, w mniejszym stopniu korzystają z pomocy socjalnej, a zamiast tego same współfinansują budżet państwa.

Wraz z rosnącą obecnością cudzoziemców w polskim społeczeństwie, pojawiła się konieczność szerszych działań integracyjnych. Wiele spośród nowych inicjatyw podejmują samorządy i organizacje pozarządowe – od kursów języka polskiego, przez doradztwo zawodowe, po projekty międzykulturowe. Dzięki temu, jak wskazują badania, poprawia się znajomość języka polskiego wśród imigrantów (zarówno wcześniejszych, jak i uchodźców wojennych), co jest kluczowe dla ich samodzielności i konkurencyjności na rynku pracy. Coraz więcej dzieci imigrantów (ponad 90% ukraińskich dzieci w Polsce) uczęszcza do polskich szkół, co sprzyja ich integracji od najmłodszych lat. Mimo tych pozytywów, wyzwaniem pozostają pewne różnice kulturowe i stereotypy. Jak wynika z sondaży PIE, Polacy deklarują najwyższy poziom zaufania do pracowników z krajów kulturowo bliskich (Europejczycy z UE, a także Ukraińcy i Białorusini), natomiast są bardziej nieufni wobec osób z odmiennych kręgów kulturowych (Azji, Afryki). Jednocześnie jednak odnotowuje się dość wysoką akceptację dla usług świadczonych przez obcokrajowców nawet o egzotycznym pochodzeniu w zawodach takich jak pracownicy branży budowlanej, kierowcy czy kelnerzy – a więc tam, gdzie liczy się głównie rzetelność pracy fizycznej. Natomiast im bardziej dana posada wymaga biegłej komunikacji z klientem lub zaufania (np. lekarz, prawnik), tym niższa jest akceptacja zatrudnienia na niej cudzoziemca nieznającego dobrze języka. To pokazuje, że integracja językowa i kulturowa jest warunkiem awansu imigrantów do pewnych zawodów i pełnej akceptacji społecznej.

Podsumowując, cudzoziemcy spoza UE stali się trwałym elementem polskiego rynku pracy, wypełniając w nim lukę zarówno ilościową (brak rąk do pracy), jak i jakościową (zapewnienie kompetencji tam, gdzie brakuje krajowych specjalistów lub chętnych do pracy). Przynoszą ze sobą znaczący

wkład w gospodarkę – pracują, zakładają firmy, płacą podatki, ale jednocześnie stawiają przed państwem i społeczeństwem nowe zadania w zakresie integracji, utrzymania spójności społecznej oraz zabezpieczenia warunków uczciwej konkurencji na rynku pracy. W następnej części rozdziału dokonana zostanie dyskusja uzyskanych wyników w świetle zidentyfikowanych szans i zagrożeń oraz odniesienie ich do szerszego kontekstu teoretycznego.

Szanse, zagrożenia i implikacje dla bezpieczeństwa społeczno-gospodarczego Polski

Wyniki analizy wyraźnie wskazują, że zatrudnianie cudzoziemców z krajów trzecich generuje istotne korzyści ekonomiczne dla Polski. Po pierwsze, imigranci uzupełniają niedobory siły roboczej w wielu branżach, umożliwiając utrzymanie ciągłości i tempa produkcji. Jak wykazało badanie ankietowe, 55,5% polskich pracodawców wprost postrzega zatrudnianie cudzoziemców jako sposób na obsadzenie wakatów, których nie udaje się zapełnić pracownikami lokalnymi. Dotyczy to zwłaszcza sektorów dotkniętych emigracją Polaków (np. budownictwo, opieka zdrowotna – pielęgniarki, opiekunki) oraz tych, gdzie praca jest trudna i nisko płatna (rolnictwo sezonowe, sprzątanie, gastronomia). Imigranci zarobkowi stali się *niezbędni* m.in. w rolnictwie i sadownictwie – bez pracowników z Ukrainy czy Azji – wiele gospodarstw nie zebrałoby plonów na czas. Po drugie, cudzoziemcy przyczyniają się do wzrostu PKB poprzez zwiększenie liczby osób pracujących i konsumpcji wewnętrznej. Ich wydatki na utrzymanie w Polsce (wynajem mieszkań, żywność, transport) napędzają popyt, co z kolei tworzy kolejne miejsca pracy. Szacunki NBP i ekonomistów wskazują, że obecność imigrantów mogła podnieść tempo wzrostu gospodarczego Polski o dodatkowe ułamki punktu procentowego rocznie w porównaniu ze scenariuszem bez imigracji. Po trzecie, imigranci wzmacniają krótkoterminowo finanse publiczne, co jest korzystne z punktu widzenia bezpieczeństwa ekonomicznego państwa. Wpływy ze składek ZUS (ok. 5% całości) i podatków płaconych przez cudzoziemców pomagają finansować system emerytalny i inne wydatki publiczne. Należy podkreślić, że większość imigrantów jest w młodym wieku produkcyjnym, a zatem przez najbliższe lata będą bardziej dawcami niż biorcami środków publicznych. Po czwarte, obecność pracowników z różnych krajów może zwiększać produktywność i innowacyjność

przedsiębiorstw. Pracodawcy dostrzegają pozytywy w postaci *„świeżych perspektyw i nowych pomysłów”* wniesionych przez cudzoziemców – wskazuje na to 26,5% firm badanych w raporcie Gi Group. Zróżnicowane kulturowo zespoły potrafią lepiej rozwiązywać problemy i obsługiwać międzynarodowych kontrahentów. Ponadto sieci kontaktów imigrantów sprzyjają internacjonalizacji polskich firm (np. eksport na rynki wschodnie dzięki pracownikom z tych krajów).

Z punktu widzenia bezpieczeństwa społecznego, kontrolowany napływ imigrantów zarobkowych może przyczynić się do stabilizacji sytuacji na rynku pracy. Gdy gospodarka rośnie, a bezrobocie jest rekordowo niskie (ok. 5% w latach 2018-2019, ponownie ~5% w 2022-2023 mimo pandemii), brak rąk do pracy staje się czynnikiem ryzyka dla rozwoju – firmy odrzucają zamówienia, inwestycje są hamowane brakiem kadr. Cudzoziemcy wypełniają tę lukę, przez co przedsiębiorstwa mogą się rozwijać, zamiast ograniczać działalność. To przekłada się na bezpieczeństwo ekonomiczne kraju, rozumiane jako zdolność gospodarki do niezakłóconego funkcjonowania i wzrostu. Dodatkowo, migranci zarobkowi działają jak *bufor* na rynku pracy – w razie spowolnienia gospodarczego część z nich może wyjechać (np. powrócić do ojczyzny), co łagodzi presję wzrostu bezrobocia wśród obywateli kraju przyjmującego. Ten mechanizm zaobserwowano w początkach pandemii: w 2020 r. wielu Ukraińców czasowo wyjechało z Polski, co pomogło uniknąć nagłego wzrostu bezrobocia krajowego, po czym wrócili w 2021 r. wraz z ożywieniem gospodarki.

Mimo wymienionych korzyści, masowe zatrudnianie cudzoziemców spoza UE pociąga za sobą także pewne zagrożenia dla gospodarki i ładu społecznego – zwłaszcza jeśli proces ten nie jest odpowiednio zarządzany. Jednym z głównych wyzwań jest ryzyko wystąpienia napięć społecznych i ksenofobii. Jeśli w społeczeństwie zakorzeni się przekonanie, że imigranci zabierają pracę miejscowym lub obniżają standardy płac i pracy, może to prowadzić do niechęci, a nawet otwartej wrogości wobec cudzoziemców. Już teraz ponad połowa Polaków obawia się wzrostu przestępczości lub niepokojów związanych z napływem pracowników zagranicznych. Narracje populistyczne mogą łatwo wykorzystać te lęki, podkopując spójność społeczną. Kolejnym zagrożeniem jest presja na system usług publicznych. Nagły wzrost liczby mieszkańców (np. o 1-1,5 mln Ukraińców w 2022 r.)

oznacza większe obciążenie szkół, przedszkoli, służby zdrowia czy transportu publicznego. Bez odpowiedniego dofinansowania i adaptacji, lokalne systemy świadczeń mogą być przeciążone, co rodzi niezadowolenie zarówno imigrantów, jak i mieszkańców (konkurencja o zasoby). Trzeba tu zaznaczyć, że Polska skorzystała ze wsparcia UE w ramach Funduszu na rzecz uchodźców, ale wciąż spora część kosztów integracji spadła na budżet samorządów i państwa. Istotnym zagrożeniem natury ekonomicznej jest możliwość rozwoju szarej strefy i wyzysku pracowników.

Długotrwałe procedury legalizacji pracy cudzoziemców w przeszłości skłaniały niektórych pracodawców do omijania prawa i zatrudniania obcokrajowców nielegalnie. W 2022 r. Państwowa Inspekcja Pracy odnotowała ok. 15 tys. przypadków nielegalnego powierzenia pracy cudzoziemcom – co prawda liczba ta nie jest ogromna, ale wykazuje wyraźną tendencję wzrostową. Nieszczelny system migracyjny i słabe egzekwowanie przepisów stanowią pokusę dla nieuczciwych podmiotów, aby np. *„wypożyczać"* cudzoziemców poprzez fikcyjne zakładanie spółek lub wykorzystywać luki prawne. Takie praktyki są groźne podwójnie: po pierwsze, rodzą nieuczciwą konkurencję wobec firm przestrzegających prawa (dumping socjalny), po drugie – narażają samych cudzoziemców na pracę bez zabezpieczeń socjalnych, ubezpieczenia czy godnych warunków. Konsekwencją może być tworzenie się segmentu rynku pracy o gorszych warunkach (dualizacja rynku) i trwałe obniżenie standardów pracy w niektórych branżach. Dlatego eksperci podkreślają, że potrzebne są rozwiązania zachęcające pracodawców do legalnego zatrudniania (np. system *„zatwierdzonych pracodawców"* z ułatwieniami proceduralnymi dla firm o dobrej reputacji) oraz wzmocnienie kontroli i surowe sankcje za naruszenia, tak aby eliminować patologiczne zjawiska.

Kolejnym wyzwaniem jest brak długofalowej strategii integracji imigrantów. Jak dotąd Polska nie wypracowała spójnego modelu integracji (w odróżnieniu np. od tradycyjnych krajów imigracyjnych, które mają rozbudowane programy językowe, społeczne, orientacyjne). To powoduje, że integracja odbywa się żywiołowo – wielu imigrantów dobrze sobie radzi (szczególnie młodsze osoby, rodziny z dziećmi w szkołach), ale część może pozostać na marginesie społeczeństwa z barierą językową i kulturową. Brak integracji niesie ze sobą długoterminowe zagrożenia: tworzenie

się izolowanych enklaw imigranckich, problem bezrobocia strukturalnego wśród niektórych grup cudzoziemców, wzrost napięć między społecznościami lokalnymi a obcokrajowcami. Z punktu widzenia bezpieczeństwa społecznego bardzo ważne jest więc inwestowanie w edukację językową, kursy adaptacyjne, doradztwo zawodowe dla cudzoziemców, a także działania skierowane do społeczności przyjmującej (promocja postaw otwartości, zwalczanie uprzedzeń). Na szczęście obserwuje się już pozytywne kroki – np. poprawa znajomości języka polskiego wśród imigrantów i rosnący odsetek deklarujących chęć pozostania w Polsce na stałe świadczą o postępującej integracji. Niemniej jednak znaczna część (zwłaszcza uchodźców wojennych) nadal nie ma pewności co do swoich planów i traktuje pobyt w Polsce jako tymczasowy, co utrudnia pełną integrację (np. nie inwestują w naukę języka ci, którzy planują wyjazd dalej na Zachód lub powrót na Ukrainę).

Wreszcie, nie można pominąć kwestii instytucjonalnych zagrożeń – czyli tego, że państwo polskie wciąż reaguje *ex post* na zjawiska migracyjne zamiast kreować je z wyprzedzeniem. Przykładem jest tu wcześniej wspomniany brak aktualnej polityki migracyjnej i dokończonych reform prawnych. Dopiero napływ kilku milionów uchodźców w 2022 r. wymusił pewne zmiany (specustawa, uproszczenie procedur dla Ukraińców). Jednak kompleksowe rozwiązania – jak choćby zapowiadany system punktowy selekcji imigrantów zarobkowych – pozostają w fazie dyskusji. O ile punktowy system (wzorowany na kanadyjskim czy australijskim) mógłby pomóc ściągać do Polski bardziej wykwalifikowanych specjalistów, o tyle istnieją obawy, że w warunkach polskich może okazać się nieskuteczny, gdyż mało jest kandydatów spełniających wyśrubowane kryteria, by przyjechać do kraju o wciąż niższych płacach niż w Europie Zachodniej. Eksperci zgodnie postulują raczej upraszczanie istniejących procedur (które obecnie bywają długotrwałe i zbiurokratyzowane) oraz poprawę koordynacji między urzędami (np. Urzędem ds. Cudzoziemców, urzędami wojewódzkimi, ZUS-em, urzędami pracy). Tylko wtedy Polska będzie w stanie sprawnie zarządzać strumieniem imigracji – tak, aby dostarczać gospodarce potrzebnych pracowników bez zbędnej zwłoki, a jednocześnie monitorować, kto i na jakich warunkach podejmuje pracę. Brak takiego systemu może być postrzegany jako zagrożenie dla bezpieczeństwa – niekontrolowana migracja rodzi ryzyka zarówno ekonomiczne (wspomniany rozwój szarej strefy), jak i potencjalnie kryminalne

czy terrorystyczne (choć dotychczas w polskich warunkach nie odnotowano takich incydentów, nieuporządkowane procesy migracyjne zawsze niosą teoretycznie ryzyko przenikania elementów przestępczych) (Oskierko, Żurawski, 2024).

Podsumowanie

Bilans szans i zagrożeń związanych z zatrudnianiem cudzoziemców spoza UE w Polsce wskazuje, że korzyści ekonomiczne przeważają, o ile kraj jest w stanie sprostać wyzwaniom integracyjnym i regulacyjnym. Polska gospodarka realnie potrzebuje imigrantów – bez nich wiele sektorów miałoby poważne problemy z kontynuacją działalności, a tempo wzrostu uległoby obniżeniu. Jak stwierdziła ekspertka Konfederacji Lewiatan, *„na polskim rynku pracy może nam zabraknąć nawet 2 mln pracowników w perspektywie dekady, a imigranci zarobkowi od lat skutecznie wypełniają luki kadrowe”.* Imigracja stała się tym samym jednym z filarów bezpieczeństwa ekonomicznego kraju – czynnikiem łagodzącym negatywne trendy demograficzne i stymulującym rozwój. Warunkiem jednak jest właściwe zarządzanie tym procesem. Bez tego, zamiast spodziewanych korzyści, mogą ujawnić się negatywne konsekwencje społeczne i ekonomiczne (Kobets, Oskierko, Strutynska, Żurawski, Brążkiewicz, 2025).

Przeprowadzone badanie pozwala sformułować następujące wnioski dotyczące wpływu zatrudniania cudzoziemców spoza Unii Europejskiej na gospodarkę i bezpieczeństwo społeczno-ekonomiczne Polski:

1. Cudzoziemcy spoza UE stali się integralną częścią polskiego rynku pracy – ich liczba przekroczyła milion, a udział w ogólnej liczbie pracujących sięga ok. 6-7%. Polska przeszła przyspieszoną transformację w kierunku kraju imigracyjnego, co oznacza zmianę dotychczasowych paradygmatów polityki rynku pracy i bezpieczeństwa wewnętrznego.
2. Zatrudnianie cudzoziemców przynosi wymierne korzyści makroekonomiczne. Imigranci zapełniają luki kadrowe wynikające ze starzenia się społeczeństwa i emigracji Polaków, przyczyniają się do wzrostu PKB oraz poprawiają sytuację funduszy ubezpieczeń społecznych (dostarczając ok. 5% składek). Są aktywni zawodowo i przedsiębiorczy, tworząc także własne miejsca pracy. W ten sposób wzmacniają

szeroko rozumiane bezpieczeństwo ekonomiczne państwa, zwiększając jego zdolność do utrzymania tempa rozwoju gospodarczego.

3. Do głównych szans związanych z imigracją zarobkową należy zahamowanie negatywnych trendów demograficznych. Napływ stosunkowo młodej populacji pracowników z zagranicy częściowo kompensuje ubytek siły roboczej. O ile imigracja nie rozwiąże w pełni kryzysu demograficznego (utrzymanie relacji pracujący–emeryci wymagałoby ponad 2 mln nowych imigrantów w dekadę), o tyle znacząco go łagodzi i kupuje czas na wdrożenie innych reform (aktywizacja biernych zawodowo, robotyzacja).
4. Imigranci przyczyniają się do wzrostu różnorodności kompetencji i umiędzynarodowienia polskiej gospodarki. Wnoszą nowe umiejętności, perspektywy kulturowe i kontakty zagraniczne, co stanowi wartość dodaną dla firm i instytucji. Silna reprezentacja obywateli Ukrainy, Białorusi, a także pojawienie się pracowników z Azji czy Ameryki Łacińskiej (np. z Indii, Filipin, a nawet z Kolumbii) sprawiają, że polski rynek pracy staje się bardziej globalny. To potencjalnie zwiększa innowacyjność i zdolność adaptacji gospodarki.
5. Zatrudnianie cudzoziemców wiąże się jednak z istotnymi zagrożeniami i kosztami, które wymagają świadomego zarządzania. Najważniejsze z nich to: (a) *ryzyko konfliktów społecznych* – pojawienie się obcych kulturowo grup może rodzić napięcia, jeśli zabraknie działań integracyjnych i edukacyjnych, (b) *obciążenie usług publicznych* – system oświaty, opieki zdrowotnej, pomocy społecznej muszą być dofinansowane i dostosowane do większej oraz zróżnicowanej grupy odbiorców, inaczej ucierpi jakość usług, (c) *rozwój szarej strefy* – bez sprawnego systemu legalizacji i kontroli pracy imigrantów istnieje pokusa nadużyć, co szkodzi uczciwej konkurencji i samym pracownikom, (d) *presja na rynku pracy* – lokalnie i w krótkim okresie nadmiar taniej siły roboczej może osłabiać pozycję negocjacyjną polskich pracowników w najsłabiej opłacanych sektorach, co wymaga monitoringu i ewentualnych interwencji (np. podnoszenia płacy minimalnej).
6. Obecne doświadczenia ujawniają braki w polskiej polityce migracyjnej. Zarówno literatura, jak i analiza sytuacji ostatnich lat wskazują na potrzebę sformułowania spójnej strategii państwa wobec imigracji

zarobkowej. Brak takiej strategii sam w sobie stanowi zagrożenie – reakcje ad hoc mogą nie wystarczyć w obliczu długofalowych trendów. Polska powinna wypracować przejrzyste zasady selekcji, przyjmowania i integracji cudzoziemców, które godzą interesy gospodarcze (popyt na pracę) z koniecznością ochrony ładu społecznego. Postulaty obejmują m.in.: uproszczenie i przyspieszenie procedur legalizacji pracy i pobytu, poprawę koordynacji między instytucjami odpowiedzialnymi za różne aspekty migracji, stworzenie mechanizmów zachęcających do legalnego zatrudniania oraz objęcie imigrantów programami integracyjnymi (nauka języka, orientacja zawodowa itp.).

7. Integracja cudzoziemców powinna stać się integralnym elementem bezpieczeństwa społeczno-gospodarczego. Sukces ekonomiczny migracji zarobkowej będzie trwały tylko wtedy, gdy imigranci zostaną włączeni w tkankę społeczną – jako pełnoprawni pracownicy i sąsiedzi, znający język i prawa, respektujący obowiązki i korzystający z praw. W przeciwnym razie mogą powstać podziały i napięcia, zagrażające spójności społecznej, a tym samym bezpieczeństwu wewnętrznemu. Dlatego państwo musi inwestować w politykę integracyjną równolegle z polityką migracyjną, mając świadomość, że te dwie sfery są ze sobą nierozerwalnie związane.

Reasumując, zatrudnianie cudzoziemców spoza UE jest zjawiskiem nieuchronnym i w dużej mierze pozytywnym dla polskiej gospodarki – stanowi odpowiedź na strukturalne wyzwania demograficzne i rozwojowe. Jednak, aby maksymalnie wykorzystać związane z tym szanse, a zminimalizować zagrożenia, konieczne jest proaktywne podejście państwa. Oznacza to przejście od biernego obserwowania trendów do aktywnego kształtowania polityki migracyjnej i rynku pracy: tworzenia zachęt do legalnej pracy, egzekwowania standardów zatrudnienia, wspierania integracji oraz rzetelnego informowania społeczeństwa o rzeczywistej roli imigrantów. Tylko wówczas zatrudnianie cudzoziemców będzie katalizatorem wzmocnienia bezpieczeństwa społeczno-gospodarczego, a nie potencjalnym źródłem destabilizacji. Polska stoi przed szansą, by – czerpiąc z doświadczeń innych państw oraz własnych obserwacji – zbudować model imigracji zarobkowej służący zarówno rozwojowi gospodarczemu kraju, jak i dobrobytowi całego społeczeństwa.

Literatura

1. Bankier.pl. (2025). *Ekonomiści: Migranci mogą być ratunkiem dla polskiego rynku pracy*. Pobrane z: https://www.bankier.pl/wiadomosc/Ekonomisci-Migranci-moga-byc-ratunkiem-dla-polskiego-rynku-pracy-8931896.html (dostęp: 12.02.2026).
2. Dębkowska, K., Kłosiewicz-Górecka, U., Szymańska, U., Wejt-Knyżewska, A., Zybertowicz, K. (2024). *Polacy o cudzoziemcach na rynku pracy – fakty, mity, opinie*. Polski Instytut Ekonomiczny.
3. Elak, L., Oskierko, M., Żurawski, S. (2024). *Security management during the migra-tion crisis on the polish-belarusian border*, Proceedings of the 66th International Scientific Con-ference of Daugavpils University. Part B "Social Sciences".
4. Gi Group. (2024). *Zatrudnianie cudzoziemców w Polsce. Wyzwania i szanse.*
5. GUS. (2023). *Ilu cudzoziemców wykonywało pracę w Polsce w maju 2023 r.* Pobrane z: https://www.prawo.pl/kadry/ilu-cudzoziemcow-wykonywalo-prace-w-polsce-w-maju-2023-r-gus (dostęp: 12.02.2026).
6. GUS, (2024). *Cudzoziemcy wykonujący pracę w Polsce w 2023 r.* Główny Urząd Skarbowy.
7. Kobets, J., Oskierko, M., Strutynska, T., Żurawski, S., Brążkiewicz, D. (2025). Wpływ sytuacji demograficznej Ukrainy związanej z wojną na bezpieczeństwo globalne. *Studia Społeczne*, *2*(58), 53-72.
8. NBP. (2025). *Publications about migration inflows and outflows*. Narodowy Bank Polski. Pobrane z: https://nbp.pl/en/publications/other/migration (dostęp: 12.02.2026).
9. NBU. (2022). *Impact of Ukrainian Migrants on Economies of Recipient Countries*. Report. National Bank of Ukraine.
10. Oskierko, M., Żurawski, S. (2024). Kryzys migracyjny na granicy białorusko-polskiej jako przykład zagrożenia o charakterze kulturowym. W: W Śmiałek (red.), *Wielowymiarowość konfliktów kulturowych we współczesnym świecie*. Grupa Wydawnicza FNCE.
11. Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. z 2022 r. poz. 583).

12. Wielkopolski Związek Pracodawców. (2025). *Przyszłość rynku pracy, migracji i integracji cudzoziemców w Polsce*. Pobrane z: https://wzp.org.pl/przyszlosc-rynku-pracy-migracji-i-integracji-cudzoziemcow-w-polsce/ (dostęp: 12.02.2026).
13. ZUS. (2024). *Cudzoziemcy w polskim systemie ubezpieczeń społecznych 2023*. Pobrane z: https://www.zus.pl/documents/10182/2322024/Cudzoziemcy+w+polskim+systemie+ubezpieczeń+społecznych_2023.pdf (dostęp: 12.02.2026).
14. Zywert, M . (2023). Imigracja zarobkowa jako determinanta zmian na rynku pracy w Polsce. W: E. Sobczak (red.), *Współczesne problemy ekonomii i zarządzania* (s. 65-80). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu. https://doi.org/10.15611/2023.95.4.05

Radosław Dawidziuk[1]
Akademia Finansów i Biznesu Vistula, Warszawa

https://doi.org/10.29316/9788368103373_11

PERCEPCJA RYZYKA GEOPOLITYCZNEGO A GOTOWOŚĆ DO MOBILNOŚCI AKADEMICKIEJ WŚRÓD STUDENTÓW UCZELNI WYŻSZEJ

PERCEPTIONS OF GEOPOLITICAL RISK AND WILLINGNESS TO ENGAGE IN ACADEMIC MOBILITY AMONG UNIVERSITY STUDENTS

Streszczenie

Celem rozdziału jest zbadanie zależności między percepcją ryzyka geopolitycznego a gotowością studentów szkół wyższych do podejmowania mobilności akademickiej. Problem badawczy dotyczy tego, w jakim stopniu i w jaki sposób postrzegane zagrożenia geopolityczne (np. konflikty zbrojne, terroryzm, niestabilność polityczna) wpływają na chęć studiowania za granicą lub uczestnictwa w wymianach akademickich. W części teoretycznej dokonano przeglądu literatury z obszaru nauk o bezpieczeństwie, obejmującego definicje ryzyka geopolitycznego oraz pojęcie mobilności akademickiej wraz z korzyściami i barierami jej towarzyszącymi. W części

[1] https://orcid.org/0009-0004-8818-5691, e-mail: r.dawidziuk@vistula.edu.pl

empirycznej przedstawiono metodologię badania własnego – ankiety diagnostycznej przeprowadzonej wśród studentów polskiej uczelni – oraz wyniki statystyczne dotyczące poziomu postrzeganego ryzyka i deklarowanej gotowości do wyjazdów zagranicznych. Wyniki wskazują m.in., że wyższa percepcja globalnych zagrożeń istotnie obniża skłonność do mobilności: studenci silnie obawiający się obecnej sytuacji geopolitycznej rzadziej planują studia za granicą. Rozdział zawiera dyskusję uzyskanych rezultatów w kontekście wcześniejszych badań (krajowych i zagranicznych) oraz rekomendacje praktyczne. Rezultaty mogą znaleźć zastosowanie w kształtowaniu programów wsparcia dla studentów – tak, aby przeciwdziałać nadmiernym obawom i zachęcać do korzystania z możliwości mobilności akademickiej pomimo niepewności globalnej.

Słowa kluczowe: ryzyko geopolityczne, percepcja ryzyka, mobilność akademicka, studenci, bezpieczeństwo

Abstract

The aim of this article is to examine the relationship between the perception of geopolitical risk and the readiness of university students to engage in academic mobility. The research problem focuses on the extent to which perceived geopolitical threats (e.g. armed conflicts, terrorism, political instability) influence students' willingness to study abroad or participate in academic exchange programs. The theoretical section reviews the literature in security studies, covering definitions of geopolitical risk and the concept of academic mobility, along with their benefits and barriers. The empirical section presents the methodology of the author's own study – a diagnostic survey conducted among students of a Polish university – as well as statistical results regarding the level of perceived risk and the declared readiness for international travel. The findings indicate, among other things, that a higher perception of global threats significantly reduces the willingness to be mobile: students who strongly fear the current geopolitical situation are less likely to plan to study abroad. The article includes a discussion of these results in the context of prior domestic and international research, and practical recommendations. The results may be applied in designing support programs for students to counteract excessive fears and encourage them to take advantage of academic mobility opportunities despite global uncertainties.

Keywords: geopolitical risk, risk perception, academic mobility, students, security studies

Wstęp

Współczesny świat charakteryzuje się narastającą niepewnością i mnożącymi się kryzysami o zasięgu globalnym. Dynamiczne zmiany w środowisku międzynarodowym – takie jak konflikty zbrojne, napięcia polityczne, ataki terrorystyczne czy niestabilność gospodarcza – sprawiają, że kwestia ryzyka geopolitycznego wysuwa się na pierwszy plan w debacie publicznej. Młode pokolenie, w tym studenci szkół wyższych, dorasta w tej rzeczywistości ciągłych doniesień o globalnych zagrożeniach. Generacja Z, uznawana za najbardziej podłączoną do informacji, jest wręcz *hiperświadoma* wydarzeń na świecie – media społecznościowe i serwisy newsowe dostarczają im w czasie rzeczywistym obrazów konfliktów, kryzysów klimatycznych czy protestów (IC3 Movement, 2025). Według koncepcji społeczeństwa ryzyka Ulricha Becka (2012), globalne zagrożenia we współczesnym świecie osiągają skalę porównywalną z wojnami i przenikają wszystkie sfery życia, a wszechobecny strach i potrzeba bezpieczeństwa zaczynają wypierać fundamentalne wartości, takie jak wolność czy równość (Beck, 2012). W takiej atmosferze niepewności życiowej naturalne jest, że młodzi ludzie odczuwają lęk przed przyszłością i ostrożniej podchodzą do decyzji życiowych – w tym decyzji o wyjeździe za granicę.

Mobilność akademicka – rozumiana jako wyjazdy studentów za granicę w celach edukacyjnych (studia częściowe, pełne studia, praktyki, wymiany itp.) – była dotychczas postrzegana bardzo pozytywnie i stanowiła ważny element internacjonalizacji edukacji wyższej. Od czasu uruchomienia programu Erasmus w 1987 roku z możliwości studiowania, szkolenia lub wolontariatu za granicą skorzystało ponad 14 milionów osób (stan na 2022 r.) (Barcakova, Launikari, 2024). Globalnie liczba studentów zagranicznych dynamicznie rosła: szacuje się, że w 2022 r. na świecie studiowało poza swoim krajem około 6,9 miliona studentów, co oznacza wzrost o 176% w porównaniu z rokiem 2002. Do głównych korzyści z mobilności edukacyjnej zalicza się rozwój cennych kompetencji (np. językowych, międzykulturowych), poszerzenie horyzontów oraz zwiększenie szans na rynku pracy dzięki zdobytym doświadczeniom międzynarodowym (Barcakova, Launikari, 2024). Nic dziwnego, że programy wymiany studentów cieszyły się rosnącym zainteresowaniem – przynajmniej do niedawna.

Ostatnie lata przyniosły jednak bezprecedensowe zakłócenia w międzynarodowej mobilności studentów. Najpierw globalna pandemia COVID-19 w 2020 r. doprowadziła do zamknięcia granic i masowego przejścia na nauczanie zdalne, co odbiło się na programach wymian. Przykładowo w Polsce liczba studentów wyjeżdżających na Erasmusa spadła z 9616 osób w 2019 r. do 3695 w 2021 r. (czyli o ponad 60%). Również napływ studentów zagranicznych do Polski zmniejszył się w tym okresie niemal czterokrotnie. Gdy wydawało się, że najgorszy okres pandemii mija i mobilność akademicka zacznie się odbudowywać, pojawiły się nowe wstrząsy geopolityczne. W lutym 2022 wybuchła wojna na Ukrainie, najbardziej brutalny konflikt zbrojny w Europie od II wojny światowej, który zdestabilizował sytuację bezpieczeństwa w regionie. W tym samym czasie narastały napięcia między światowymi mocarstwami (m.in. pogorszenie relacji USA-Chiny), a w Europie doszło do takich wydarzeń, jak Brexit czy kryzysy energetyczne. Wszystkie te czynniki tworzą klimat niepewności, w którym *mobilność* – rozumiana jako swobodne przemieszczanie się za granicę – napotyka nowe bariery.

Sygnalizowane zmiany mają swoje odzwierciedlenie w postawach studentów. Już pierwsze dane wskazują, że obecna niestabilność geopolityczna odbiła się na skłonności młodych ludzi do wyjazdów zagranicznych. Według analizy Barcakovej i Launikariego (2024) ogólnoświatowe zawirowania – wojna w Ukrainie, Brexit, a nawet zmiany klimatyczne – przerwały wzrostowy trend mobilności edukacyjnej i rodzą pytania, jak zachęcać studentów do wyjazdów w okresie niepewności (Barcakova, Launikari, 2024). Badania prowadzone w Europie wykazały, że agresja Rosji na Ukrainę czy zaostrzenie polityk imigracyjnych wywołało u studentów zwiększony niepokój przed studiowaniem za granicą, wielu obawia się, czy w ogóle będzie mile widzianych i bezpiecznych w niektórych krajach (IC3 Movement, 2025). Również w Polsce zauważalny jest wzrost lęku społecznego związanego z możliwością eskalacji konfliktów – z sondażu IBRiS z czerwca 2025 r. wynika, że aż 44% Polaków obawia się wybuchu III wojny światowej w najbliższych miesiącach, przy czym odsetek ten jest wyższy wśród kobiet (Polskie Radio, 2025). Tego rodzaju lęki przed globalnym konfliktem siłą rzeczy mogą przekładać się na ostrożność w planowaniu wyjazdów zagranicznych przez młodzież akademicką.

Motywacją do podjęcia niniejszego tematu jest potrzeba zrozumienia, czy i w jaki sposób percepcja ryzyka geopolitycznego wpływa na gotowość studentów do mobilności akademickiej. Innymi słowy, czy studenci, którzy postrzegają świat jako bardziej niebezpieczny, wykazują mniejszą chęć uczestniczenia w programach typu Erasmus lub podejmowania studiów za granicą? Problem ten sytuuje się na styku badań nad bezpieczeństwem oraz internacjonalizacją edukacji. Z jednej strony dotyczy subiektywnego poczucia bezpieczeństwa (a raczej zagrożenia) młodych ludzi, z drugiej – ich edukacyjnych wyborów i planów życiowych w globalizującym się świecie. Cel badawczy pracy można sformułować jako: *zidentyfikowanie zależności między poziomem percepcji zagrożeń geopolitycznych a deklarowaną gotowością do podjęcia mobilności zagranicznej wśród studentów*. Rozdział składa się z części teoretycznej, obejmującej przegląd literatury przedmiotu, oraz części empirycznej, prezentującej metodę i wyniki badania własnego. W zakończeniu przedstawiono dyskusję wyników na tle wcześniejszych badań oraz wnioski i rekomendacje.

Przegląd literatury

Ryzyko geopolityczne – istota i percepcja

Pojęcie ryzyka geopolitycznego (ang. *geopolitical risk*) odnosi się do zagrożeń wynikających z wydarzeń natury polityczno-militarnej i napięć na arenie międzynarodowej, które mogą zakłócać pokojowy bieg stosunków między państwami. W literaturze przedmiotu ryzyko geopolityczne definiuje się m.in. jako *„groźbę, urzeczywistnienie i eskalację negatywnych zdarzeń związanych z wojnami, terroryzmem oraz wszelkimi napięciami między państwami i aktorami politycznymi, które wpływają na pokojowy porządek stosunków międzynarodowych”* (Behn, Lang, Reghezza, 2025). Innymi słowy, są to zagrożenia wynikające z konfliktów zbrojnych (zarówno aktualnie toczących się, jak i potencjalnych), aktów terroru, narastających sporów międzypaństwowych, sankcji i wojen handlowych, rewolucji oraz innych sytuacji kryzysowych w polityce światowej. Ryzyko geopolityczne ma charakter wielowymiarowy i trudno poddaje się kwantyfikacji, gdyż wynika z szeregu powiązanych czynników politycznych, ekonomicznych i społecznych. Jego skrajna manifestacja – wojna – pociąga za sobą ofiary w ludziach

i zniszczenia materialne, ale nawet mniej ekstremalne zdarzenia (np. groźby konfliktu, pogłoski o wojnie, demonstracje siły) mogą wywoływać szerokie reperkusje ekonomiczne i psychologiczne. W ujęciu makro ryzyko geopolityczne przekłada się np. na spadki aktywności gospodarczej, odpływ kapitału z zagrożonych regionów, wzrost cen surowców (ropa, gaz) i wahania rynków finansowych. Natomiast z perspektywy jednostek i społeczeństw oznacza ono poczucie niepewności co do przyszłości oraz lęk przed tym, co może przynieść sytuacja międzynarodowa.

Percepcja ryzyka to subiektywny odbiór i ocena stopnia zagrożenia – może on znacząco odbiegać od obiektywnych miar ryzyka. Badania psychologiczne nad postrzeganiem zagrożeń (np. koncepcja *„ryzyka postrzeganego"* P. Slovica) wskazują, że ludzie często kierują się w ocenie ryzyka emocjami i wyobrażeniami, a nie chłodnymi statystykami. W przypadku ryzyka geopolitycznego dużą rolę odgrywają czynniki takie jak: doniesienia medialne (im bardziej dramatyczne relacje, tym silniejsze poczucie zagrożenia), bliskość geograficzna zagrożenia (np. wojna w sąsiednim kraju budzi większy niepokój niż konflikt na innym kontynencie), a także zaufanie do instytucji (osoby ufające własnemu państwu i sojuszom mogą czuć się bezpieczniej). W literaturze z zakresu nauk o bezpieczeństwie podkreśla się, że percepcja bezpieczeństwa i zagrożeń jest zmienna w czasie i zależy od kontekstu społeczno-politycznego (Malec, 2013; Swaine, 2020). Przykładowo, ataki terrorystyczne z 2001 r. czy seria zamachów w Europie w latach 2015-2016 znacząco zwiększyła społeczne poczucie zagrożenia terroryzmem, które z czasem jednak osłabło. Z kolei wybuch wojny na Ukrainie w 2022 r. momentalnie wywołał wzrost obaw przed konfliktem zbrojnym wśród społeczności krajów sąsiednich (w tym Polski). Zacytowany wyżej sondaż IBRiS (2025) pokazuje, że lęk przed wojną stał się zjawiskiem powszechnym: blisko połowa Polaków deklaruje taką obawę (Polskie Radio, 2025). Co istotne, kobiety częściej odczuwają strach (47% badanych Polek obawia się wojny) niż mężczyźni (40%) (Polskie Radio, 2025), co może wynikać z różnic socjalizacyjnych w reagowaniu na zagrożenia. Te różnice demograficzne w percepcji ryzyka są ważne również w kontekście studentów – warto sprawdzić, czy np. studentki silniej od studentów obawiają się wyjazdów zagranicznych z powodu zagrożeń.

Konsekwencją percepcji ryzyka geopolitycznego mogą być różnorakie reakcje behawioralne. Badania wskazują, że długotrwałe poczucie niepewności i zagrożenia zwiększa stres, lęk i może prowadzić do unikania pewnych aktywności (IC3 Movement, 2025). Młode osoby dorastające w cieniu globalnych kryzysów mogą stać się bardziej ostrożne życiowo – np. wybierać „bezpieczniejsze" ścieżki kariery, unikać branż postrzeganych jako ryzykowne, czy też rezygnować z planów międzynarodowych na rzecz opcji krajowych (IC3 Movement, 2025). Jeśli obawy nie są rozładowywane, istnieje ryzyko „pokolenia zdefiniowanego bardziej przez strach niż aspiracje" – jak obrazowo ujęto w jednym z raportów (IC3 Movement, 2025). Z punktu widzenia badań nad mobilnością interesuje nas szczególnie, czy studenci odczuwający niepokój związany z sytuacją na świecie redefiniują swoje plany edukacyjne – np. ograniczają swoje aspiracje do wyjazdów zagranicznych, wybierając pozostanie w kraju lub ewentualnie udział w formach zdalnych.

Mobilność akademicka – znaczenie, formy i bariery

Mobilność akademicka studentów stała się w ostatnich dekadach kluczowym elementem rozwoju szkolnictwa wyższego. Pojęcie to obejmuje różne formy aktywności edukacyjnej poza macierzystą uczelnią i krajem, m.in.: wyjazdy na część studiów (semestr lub rok na uczelni partnerskiej, np. w ramach programu Erasmus+), wyjazdy na pełne studia za granicą (degree mobility), praktyki lub staże zagraniczne, wyjazdy na kursy językowe, szkoły letnie, a ostatnio także mobilność wirtualną (udział w zajęciach online oferowanych przez zagraniczne uczelnie) czy mobilność hybrydową (łączącą elementy wyjazdu fizycznego i zdalnego) (Barcakova, Launikari, 2024). Tradycyjnie najwyżej ceniona była mobilność fizyczna – pobyt w obcym kraju, który umożliwia pełne zanurzenie w innej kulturze i środowisku akademickim. Jednak rozwój technologii oraz doświadczenia pandemii spowodowały wzrost znaczenia form zdalnych. Jak odnotowano, długoterminowe wyjazdy fizyczne cieszą się mniejszą popularnością niż kiedyś, a coraz więcej instytucji oferuje studentom możliwość mobilności wirtualnej lub mieszanej (Barcakova, Launikari, 2024). Ponad połowa europejskich uczelni deklaruje plany rozwijania wirtualnej mobilności studentów (Barcakova, Launikari, 2024). Nie oznacza to bynajmniej, że mobilność tradycyjna traci całkowicie na znaczeniu – nadal jest postrzegana jako niezastąpione doświadczenie

poszerzające „komfortową strefę" młodych ludzi (Barcakova, Launikari, 2024). Raczej możemy mówić o współistnieniu różnych typów mobilności, z których każdy ma swoje specyficzne walory.

Znaczenie mobilności akademickiej jest wielowymiarowe. Na poziomie indywidualnym udział w programie mobilności sprzyja rozwojowi osobistemu – studenci uczą się samodzielności, radzenia sobie w obcym środowisku, nawiązują międzynarodowe przyjaźnie i sieci kontaktów. Badania wykazują, że absolwenci z doświadczeniem zagranicznym mają często większe szanse na rynku pracy i prezentują bardziej rozwinięte kompetencje międzykulturowe (Teichler, 2015; Wałkowski, 2019). Z punktu widzenia społeczeństwa, mobilność studentów przyczynia się do wymiany wiedzy i kultury, buduje kapitał społeczny o zasięgu międzynarodowym oraz sprzyja szerzeniu postaw tolerancji i otwartości. Wreszcie, w skali makro, umiędzynarodowienie kształcenia wyższego (którego mobilność jest głównym narzędziem) wzmacnia konkurencyjność systemów edukacji i gospodarek – państwa przyciągające studentów z zagranicy zyskują talenty i potencjalnych przyszłych obywateli. Nic zatem dziwnego, że Unia Europejska i wiele krajów prowadzą aktywną politykę wspierania mobilności. Przykładem jest inicjatywa *Europejskiego Obszaru Edukacyjnego (European Education Area)*, która zakłada m.in. integrację mobilności w ścieżki kształcenia wszystkich studentów i zwiększenie udziału osób z mniejszymi szansami w programach wyjazdowych (Barcakova, Launikari, 2024).

Mimo licznych zalet, mobilność edukacyjna napotyka również bariery. Literatura wymienia zarówno przeszkody *strukturalne*, jak i *psychologiczne*. Do najczęściej wskazywanych należą bariery finansowe – koszty wyjazdu i utrzymania za granicą bywają zbyt wysokie dla części studentów (zwłaszcza jeśli stypendia są niewystarczające) – oraz bariery administracyjne i informacyjne (niedostateczna znajomość dostępnych możliwości, skomplikowane procedury aplikacyjne, problemy z uznawalnością zaliczeń po powrocie) (Barcakova, Launikari, 2024). Badania w Europie potwierdziły, że główne przeszkody to brak funduszy, brak dostatecznej informacji o programach oraz niepewność co do uznania okresu studiów za granicą (Kirdulytė i in., 2023; Barcakova, Launikari, 2024). Do tego dochodzą czynniki osobiste: niska motywacja lub priorytetowe traktowanie innych zobowiązań (np. obawa przed opóźnieniem w ukończeniu studiów – choć

faktycznie nowe analizy wskazują, że udział w wymianie zwykle nie wydłuża czasu studiowania). Co ważne, bariery te mają nierównomierny charakter – jak zauważa Di Pietro (2023), istnieją różnice demograficzne: studenci z obszarów wiejskich, o niższym statusie ekonomicznym, a także niekiedy kobiety, napotykają większe trudności i niższe *zainteresowanie* mobilnością niż ich rówieśnicy z miast, zamożniejszych rodzin czy mężczyźni (Barcakova, Launikari, 2024).

W kontekście niniejszego tematu kluczowe są bariery natury psychologicznej i bezpieczeństwa. Jeszcze dekadę temu stosunkowo rzadziej wymieniano je jako główne – dominowały kwestie finansowe i organizacyjne. Jednak wraz ze wzrostem niepewności na świecie, obawy o bezpieczeństwo podczas pobytu za granicą zaczynają odgrywać większą rolę. Studenci i ich rodzice mogą zadawać sobie pytania: *Czy kraj, do którego chcę wyjechać, jest bezpieczny? Czy nie grożą tam zamieszki, przestępczość, ataki terrorystyczne? Czy w razie pogorszenia sytuacji politycznej nie utknę daleko od domu?* Takie wątpliwości nasiliły się zwłaszcza po ostatnich doświadczeniach: wiele osób pamięta obrazy zamkniętych granic i masowych powrotów studentów z zagranicy w początkach pandemii 2020 r., a niedawno – ewakuacje studentów z Ukrainy i krajów sąsiednich w 2022 r. Można zatem przypuszczać, że ryzyko geopolityczne staje się czynnikiem hamującym mobilność. W raporcie Laurea Journal (Barcakova, Launikari, 2024) otwarcie stwierdzono, że obecna niestabilność polityczna na świecie nie sprzyja wyjazdom studentów, a uczelnie europejskie muszą zastanowić się, jak motywować młodzież do mobilności w „czasach niepewności i negatywnych trendów" (Barcakova, Launikari, 2024). Z kolei z perspektywy studentów spoza Europy – np. chińskich studentów – czynniki geopolityczne już realnie wpłynęły na ich plany edukacyjne. Mok, Shen i Gu (2024) zaobserwowali, że pogorszenie relacji Chiny-Zachód (zwłaszcza napięcia Chiny-USA) przełożyło się na utrudnienia wizowe i wybory studentów: część z nich zrezygnowała z wyjazdu do USA, kierując się do alternatywnych krajów jak Wielka Brytania czy Singapur (Mok i in., 2024). Co interesujące, w badaniu tym chińscy studenci deklarowali, iż świadomie bagatelizowali wpływ czynników geopolitycznych na swoje plany z powodu wiary w tzw. *internacjonalizm naukowy* (przekonanie, że nauka jest ponad podziałami) (Mok i in., 2024). Niemniej obiektywne przeszkody (np. brak wizy) i odczuwalne

nieprzyjazne środowisko (dyskryminacja w niektórych krajach) sprawiły, że geopolityka stała się realnym czynnikiem determinującym ich wybory (Mok i in., 2024).

Reasumując, przegląd literatury wskazuje, że kontekst geopolityczny coraz silniej zaznacza się w dyskusji o mobilności akademickiej. Tradycyjne bariery (finanse, informacja, formalności) nadal istnieją, ale na pierwszy plan wysuwają się pytania o bezpieczeństwo i stabilność świata. W sytuacji, gdy wojna toczy się w Europie, napięcia międzynarodowe rosną, a media często straszą globalnymi konfliktami, zrozumienie percepcji ryzyka wśród studentów zyskuje kluczowe znaczenie. Następna część rozdziału koncentruje się na badaniu empirycznym tej kwestii – sprawdzeniu, jak polscy studenci postrzegają obecne zagrożenia i czy wpływa to na ich gotowość do udziału w programach mobilności.

Metodologia badań

Założenia i pytania badawcze

Badanie własne zostało zaprojektowane w celu zweryfikowania zależności między postrzeganym ryzykiem geopolitycznym a gotowością do mobilności akademickiej wśród studentów. Sformułowano następujące główne pytanie badawcze: *Czy istnieje związek między poziomem percepcji ryzyka geopolitycznego a deklarowaną gotowością studentów do udziału w mobilności akademickiej (studia lub praktyki za granicą)?* Ponadto postanowiono zbadać pytania szczegółowe, m.in.:

- Jaki jest ogólny poziom percepcji ryzyka geopolitycznego w badanej grupie studentów? (Czy studenci odczuwają silny lęk przed globalnymi zagrożeniami, czy raczej umiarkowany/sporadyczny?);
- Jaki odsetek badanych deklaruje chęć wyjazdu za granicę w celach akademickich? (Jaka jest ogólna gotowość do mobilności oraz jakie formy mobilności preferują – np. program Erasmus, pełne studia II stopnia za granicą, praktyki itp.);
- Czy studenci identyfikują konkretne zagrożenia geopolityczne, które wpływają na ich obawy przed wyjazdem? (Np. wojna, terroryzm, zamieszki społeczne, restrykcje polityczne w kraju docelowym, pandemia itp.);

- Czy występują istotne różnice między podgrupami studentów w zakresie percepcji ryzyka i gotowości do mobilności? (Rozważono zmienne demograficzne: płeć, kierunek studiów – np. czy studenci bezpieczeństwa narodowego czują się inaczej niż np. filologii, doświadczenie – czy osoby, które już były za granicą, różnią się nastawieniem od tych, które nigdy nie wyjeżdżały).

Na podstawie literatury sformułowano hipotezę główną: *Studenci o wysokiej percepcji ryzyka geopolitycznego charakteryzują się niższą gotowością do podjęcia mobilności akademickiej niż studenci o niższej percepcji tego ryzyka.* Oczekiwano negatywnej korelacji między odczuwanym poziomem zagrożenia a chęcią wyjazdu – innymi słowy, im bardziej ktoś obawia się globalnej sytuacji, tym mniej skłonny będzie planować studia za granicą.

Próba badawcza

Badanie przeprowadzono wśród studentów jednej z polskich uczelni publicznych o profilu akademickim (uniwersytetu) na wschodzie Polski. Dobór próby miał charakter celowy – zaproszono do udziału studentów różnych kierunków i lat studiów, tak aby uzyskać zróżnicowaną grupę pod względem płci, specjalności i doświadczeń edukacyjnych. Ankietę udostępniono online (za pośrednictwem uczelnianej platformy e-learningowej oraz mediów społecznościowych grup studenckich) w maju 2025 r. Uzyskano N = 312 poprawnie wypełnionych kwestionariuszy. Charakterystyka demograficzna próby przedstawiała się następująco:

- Płeć: 65% badanych stanowiły kobiety, 34% mężczyźni, 1% osoby niebinarne lub niepodające płci. Nadreprezentacja kobiet jest typowa dla populacji studentów w Polsce (gdzie kobiety stanowią ok. 58% ogółu studiujących) i wynika także z większej chęci udziału kobiet w badaniach surveyowych.
- Wiek: Średnia wieku wyniosła 22,4 roku (SD = 2,1), respondenci to głównie osoby młode, w przedziale 19-26 lat. 85% stanowili studenci studiów pierwszego stopnia (licencjackich/inżynierskich), a 15% – studenci studiów magisterskich uzupełniających lub jednolitych magisterskich.
- Kierunki studiów: Respondenci reprezentowali szeroki wachlarz dziedzin: nauki społeczne i humanistyczne (43%), nauki ścisłe i techniczne

(27%), nauki ekonomiczne i zarządzanie (15%), nauki o zdrowiu i medyczne (10%) oraz inne. Dzięki temu możliwe było sprawdzenie, czy kierunek kształcenia (np. związany z bezpieczeństwem lub nie) wpływa na postrzeganie ryzyka.

- Doświadczenie zagraniczne: 28% ankietowanych deklarowało, że przed badaniem miało już doświadczenie pobytu za granicą dłuższego niż 1 miesiąc (np. wymiana studencka, staż, wakacyjna praca). Pozostałe 72% nie uczestniczyło wcześniej w długoterminowej mobilności.

Narzędzia i przebieg badania

Zastosowano metodę ankiety internetowej (CAWI – Computer-Assisted Web Interviewing) z autorskim kwestionariuszem badawczym. Kwestionariusz składał się z trzech głównych części:

1. Metryczka i dane demograficzne: pytania o płeć, wiek, kierunek i rok studiów, ewentualne wcześniejsze doświadczenia zagraniczne itp.
2. Skala percepcji ryzyka geopolitycznego: zestaw stwierdzeń mierzących poziom odczuwanego zagrożenia globalnymi wydarzeniami. Wzorowano się częściowo na istniejących skalach lęku (np. *Fear of War Scale* – FOWARS autorstwa Shoshani & Slone, 2016, w adaptacji własnej). Respondenci oceniali w skali 1-5, na ile zgadzają się z takimi stwierdzeniami jak m.in.: *„Obawiam się, że w obecnej sytuacji na świecie w każdej chwili może wybuchnąć nowy poważny konflikt zbrojny”*, *„Wiadomości o napięciach między państwami budzą mój niepokój”*, *„Czuję się bezpiecznie, planując przyszłość”* (odwrotnie kodowane) itp. Wyniki na tej skali sumowano, uzyskując indywidualny indeks percepcji ryzyka (α Cronbacha dla skali = 0,88, co wskazuje na wysoką rzetelność). Teoretyczny zakres wyników: 5 (bardzo niska percepcja ryzyka) do 25 punktów (bardzo wysoka percepcja ryzyka).
3. Pytania dotyczące mobilności akademickiej: ta część obejmowała zarówno pytania zamknięte, jak i półotwarte dotyczące planów, chęci i barier związanych z wyjazdami zagranicznymi. Kluczowe pytanie brzmiało: *„Czy rozważasz wyjazd za granicę w celu studiowania lub odbycia praktyk w ciągu najbliższych 2 lat?”* (odpowiedzi: zdecydowanie tak / raczej tak / raczej nie / zdecydowanie nie). Pytanie to posłużyło jako miara gotowości do mobilności akademickiej.

Dodatkowo pytano o preferowane formy wyjazdu (np. semestr wymiany w Europie, studia magisterskie poza Europą, krótkoterminowy wyjazd, np. szkoła letnia, mobilność wirtualna – można było zaznaczyć wiele opcji). Kolejne pytania dotyczyły barier i obaw: *„Co powstrzymuje Cię przed decyzją o wyjeździe (jeśli masz takie obawy)?"* – tu respondenci mogli wybrać spośród opcji (finanse, sprawy rodzinne, obawy o bezpieczeństwo, brak informacji, pandemia COVID, itp.) oraz dopisać własne. Istotną częścią kwestionariusza było pytanie: *„Jakie czynniki o charakterze globalnym lub politycznym budzą Twój niepokój w kontekście ewentualnego wyjazdu za granicę?"* – poproszono o zaznaczenie wszystkich pasujących odpowiedzi z listy (wojna, terroryzm, napięcia polityczne, restrykcje wizowe, dyskryminacja cudzoziemców, klęski żywiołowe, inne) oraz ocenę, jak silnie dane zjawisko go niepokoi (skala 1-5). Pozwoliło to zidentyfikować profil obaw geopolitycznych studentów.

Ankieta była anonimowa, a udział dobrowolny. Przed rozpoczęciem respondent potwierdzał zgodę na udział w badaniu. Po zebraniu danych przeprowadzono analizę statystyczną za pomocą programu IBM SPSS Statistics ver. 28. Wykorzystano statystyki opisowe (średnie, odchylenia standardowe, rozkłady procentowe), testy istotności (m.in. test χ^2 dla porównania rozkładów odpowiedzi, test t-Studenta dla różnic średnich między grupami, korelację Pearsona dla związku między zmiennymi ciągłymi) oraz analizę regresji logistycznej w celu oszacowania, jak percepcja ryzyka (jako zmienna ciągła) wpływa na prawdopodobieństwo deklaracji gotowości do wyjazdu (zmienna dychotomiczna: rozważa vs. nie rozważa wyjazdu).

Wyniki badania

Poziom percepcji ryzyka geopolitycznego wśród studentów

Pierwszym istotnym wynikiem jest zróżnicowanie poziomu postrzeganego ryzyka geopolitycznego w badanej grupie. Średni wynik na skali percepcji ryzyka wyniósł 17,3 punktu (na 25 możliwych), co odpowiada ocenie „umiarkowanie wysokie poczucie zagrożenia". Rozkład wyników był skośny w prawo – stosunkowo niewielu studentów wykazało bardzo niskie poczucie zagrożenia, natomiast około 40% osiągnęło wyniki wysokie (20 punktów i więcej).

- 24% badanych zaklasyfikowano do grupy niskiej percepcji ryzyka (wynik 5-15 pkt) – osoby te generalnie deklarowały, że nie obawiają się zanadto globalnej sytuacji, czują się raczej bezpiecznie.
- 36% mieściło się w zakresie średnim (16-19 pkt) – umiarkowane obawy, sporadyczny niepokój w reakcji na wydarzenia.
- 40% zaliczono do grupy wysokiej percepcji ryzyka (20-25 pkt) – te osoby wyraźnie odczuwają niepewność i lęk związany z aktualnymi zagrożeniami geopolitycznymi (wielu zaznaczało np. „zdecydowanie obawiam się, że wybuchnie wojna światowa").

Innymi słowy, około 4 na 10 studentów cechuje się wysokim poziomem lęku geopolitycznego, a tylko co czwarty jest wobec takich zagrożeń względnie spokojny. To dość alarmujący wynik, wskazujący na silną obecność *klimatu strachu* również w młodej populacji akademickiej. Dla porównania, w ogólnej populacji dorosłych Polaków odsetek osób obawiających się globalnego konfliktu wynosi ~44% (Polskie Radio, 2025) – nasze wyniki są zbliżone, co sugeruje, że studenci nie różnią się bardzo pod tym względem od ogółu społeczeństwa.

Zapytaliśmy również, *jakie konkretnie zagrożenia* budzą największy niepokój studentów w kontekście myśli o wyjeździe. Tabela 1 przedstawia pięć najczęściej wskazywanych kategorii zagrożeń wraz z odsetkiem studentów, którzy uznali dane zagrożenie za istotne (odpowiedzi „niepokoi mnie" lub „bardzo mnie niepokoi" na skali 1-5).

Tabela 1. Najczęściej wskazywane zagrożenia geopolityczne w kontekście wyjazdów zagranicznych (N = 312)

Rodzaj zagrożenia	Odsetek studentów uznających zagrożenie za istotne
Konflikt zbrojny / wojna	70%
Zamachy terrorystyczne	55%
Niestabilność polityczna w kraju docelowym (protesty, zamieszki)	48%
Ryzyko dyskryminacji lub wrogości wobec obcokrajowców	35%
Pandemia lub poważny kryzys zdrowotny	30%

Źródło**:** opracowanie własne.

Jak widać, wojna jest zdecydowanie największym lękiem – aż 70% studentów obawia się konfliktu zbrojnego na świecie, który mógłby ich

bezpośrednio lub pośrednio dotknąć. W kontekście wyjazdu oznacza to np. strach, że podczas pobytu za granicą wybuchnie wojna (czy to globalna, czy regionalna). Na drugim miejscu są zamachy terrorystyczne (55% obaw). Jest to interesujące, bo choć w ostatnich latach Europa nie doświadcza tak wielu ataków jak dekadę temu, pamięć o nich wciąż wpływa na wyobraźnię studentów – szczególnie ci, którzy planują wyjazd do dużych metropolii, mogą brać pod uwagę zagrożenie terrorystyczne. Trzecia w kolejności jest ogólnie pojęta niestabilność polityczna (prawie połowa badanych). Ta kategoria obejmowała sytuacje takie jak masowe protesty, zamieszki, gwałtowne zmiany rządów – czyli wszystko, co może zakłócić normalne funkcjonowanie kraju goszczącego. Stosunkowo mniejsza, choć wciąż znacząca grupa (35%) wyraziła obawę przed dyskryminacją lub wrogim traktowaniem za granicą z racji swojej narodowości czy cech (np. w kontekście narastających w niektórych miejscach nastrojów antyimigranckich). Na piątym miejscu znalazły się pandemie i globalne zagrożenia zdrowotne (30%) – co sugeruje, że doświadczenie COVID-19 zostawiło ślad w świadomości, choć obecnie mniejszy niż ryzyka natury polityczno-militarnej.

Deklarowana gotowość do mobilności akademickiej

Jednym z kluczowych parametrów badania była deklarowana chęć wyjazdu za granicę wśród studentów. Na pytanie „Czy rozważasz wyjazd za granicę w celu studiowania lub odbycia praktyk w ciągu najbliższych 2 lat?" uzyskano następujące odpowiedzi:

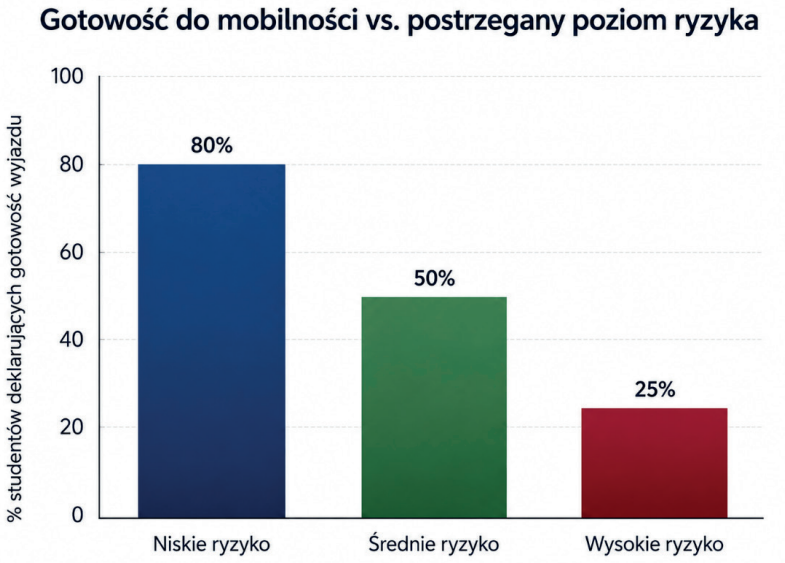
- Zdecydowanie tak: 28% respondentów,
- Raczej tak: 34%,
- Raczej nie: 22%,
- Zdecydowanie nie: 16%.

Zgrupowawszy odpowiedzi, otrzymujemy ~62% studentów ogólnie rozważających wyjazd (pozytywne nastawienie) oraz ~38% nierozważających (negatywne nastawienie). Można więc powiedzieć, że prawie dwie trzecie badanych ma otwartość na mobilność akademicką, przy czym tylko co czwarty jest do niej entuzjastycznie nastawiony („zdecydowanie tak"), a pozostali raczej się wahają lub są umiarkowanie zainteresowani. Z kolei ponad jedna trzecia nie planuje wyjazdu, z czego 16% odrzuca taką opcję kategorycznie.

Warto podkreślić, że nie pytaliśmy, *dlaczego* dana osoba nie rozważa wyjazdu – te motywy wynikają dopiero z kolejnych pytań. Ogólny odsetek 62% chętnych można uznać za dość wysoki, zważywszy że realnie odsetek studentów wyjeżdżających w skali kraju jest niższy (np. według danych FRSE, w rekordowych latach przed pandemią ok. 2% polskich studentów rocznie brało udział w Erasmusie). Nasze pytanie dotyczyło jednak samej intencji/otwartości, nie gwarantując przecież realizacji planu. Możliwe, że część z tych 62% w praktyce nie wyjedzie, ale przynajmniej bierze to pod uwagę. Zapytaliśmy też, jakie formy mobilności interesują studentów najbardziej. Wśród tych, którzy rozważają wyjazd (N = 194), najwięcej – bo 70% – wskazało klasyczny *semestr lub rok na wymianie (Erasmus+ w Europie)* jako potencjalną opcję, 25% myśli o zrobieniu *pełnego programu studiów za granicą* (np. studia magisterskie w innym kraju), a 33% rozważa *krótkoterminowe wyjazdy* (szkoły letnie, kursy, do 2 miesięcy). Ciekawym wynikiem jest, że 18% spośród chętnych dopuszcza jedynie *mobilność wirtualną* (np. uczestnictwo w kursach online zagranicznych uczelni zamiast wyjazdu). To pokazuje, że dla części studentów możliwość zdobycia międzynarodowego doświadczenia online jest atrakcyjna – zapewne jako bezpieczniejsza lub tańsza alternatywa.

Związek między ryzykiem a gotowością – analiza korelacji

Przechodząc do sedna: przeanalizowaliśmy korelację między wynikami skali percepcji ryzyka a decyzją „rozważam vs. nie rozważam wyjazdu". Otrzymano wyraźnie negatywny związek (Pearson $r = -0{,}45$, $p < 0{,}001$), co oznacza, że im wyższy poziom lęku geopolitycznego u studenta, tym mniejsze prawdopodobieństwo, że planuje on mobilność akademicką. Ta korelacja jest statystycznie istotna i umiarkowanie silna. W praktyce, jak zobrazowano na Rysunku 1, studenci o wysokiej percepcji ryzyka znacznie rzadziej deklarują chęć wyjazdu niż ci o niskiej percepcji ryzyka.



Rysunek 1. Odsetek studentów deklarujących gotowość wyjazdu za granicę w podziale na poziom postrzeganego ryzyka geopolitycznego

Źródło: opracowanie własne.

Na Rysunku 1 przedstawiono porównanie trzech grup studentów: o niskim, średnim i wysokim poziomie percepcji ryzyka (podział na tercyle wyników skali). Widzimy wyraźnie, że w grupie *niskiego ryzyka* aż około 80% studentów rozważa wyjazd (tylko 20% nie), podczas gdy w grupie *wysokiego ryzyka* odsetek rozważających spada do zaledwie 25%, a 75% deklaruje brak planów wyjazdu. Grupa średnia lokuje się pomiędzy (ok. 50% chętnych vs. 50% niechętnych). Tendencja jest więc jednoznaczna – większy strach idzie w parze z mniejszą mobilnością. Test χ^2 potwierdził istotność różnic między tymi grupami ($\chi^2 = 35{,}8$, $df = 2$, $p < 0{,}001$).

Co więcej, wykonano analizę regresji logistycznej, traktując wynik skali ryzyka jako zmienną ciągłą predykcyjną dla prawdopodobieństwa bycia w grupie „rozważam wyjazd". Wynik: iloraz szans (odds ratio) = 0,85 na każdy wzrost o 1 punkt skali ryzyka (95% CI: 0,81-0,90, $p < 0{,}001$). Oznacza to, że wzrost percepcji ryzyka o każde 1 punkt zmniejsza szanse planowania mobilności o około 15%. Wzrost o 5 punktów (np. z 15 na 20) to już spadek szans o około 50%. Ta ilościowa miara dodatkowo podkreśla siłę efektu – percepcja zagrożeń jawi się jako istotny czynnik hamujący gotowość do wyjazdu.

Inne czynniki różnicujące gotowość do mobilności

Analizowano też wspomniane zmienne demograficzne, by sprawdzić, czy np. płeć lub wcześniejsze doświadczenie modyfikują obserwowaną zależność. Kilka ciekawych wyników:

- Płeć: Kobiety w naszej próbie nieznacznie rzadziej deklarowały chęć wyjazdu niż mężczyźni (60% vs 66%), jednak różnica nie okazała się statystycznie istotna ($p = 0,28$). Natomiast kobiety miały średnio wyższy wynik percepcji ryzyka (śr. 17,8 pkt) niż mężczyźni (16,5 pkt), co jest zgodne z trendem ogólnospołecznym (Polskie Radio, 2025). Gdy kontrolujemy wpływ poziomu ryzyka, płeć nie wprowadza istotnej dodatkowej różnicy w gotowości – zatem wydaje się, że to właśnie wyższa percepcja ryzyka u kobiet tłumaczy nieco niższą ich mobilność, a nie płeć sama w sobie.
- Doświadczenie zagraniczne: Tutaj różnice były wyraźne. Osoby, które już miały wcześniej doświadczenie wyjazdu (np. brały udział w wymianie w czasie studiów licencjackich) w 80% deklarowały ponowną chęć mobilności. Natomiast w grupie bez wcześniejszego doświadczenia odsetek chętnych wyniósł 53%. Różnica ta jest istotna ($p < 0,01$). Co więcej, osoby z doświadczeniem miały istotnie niższą percepcję ryzyka (średnio 15,9 pkt) niż te bez doświadczenia (17,8 pkt), $p < 0,01$. Można to interpretować dwojako: albo odważniejsi studenci częściej decydują się wyjechać (czyli naturalna selekcja – ci o niskim lęku już wyjechali, a lękliwi zostali), albo też udział w mobilności obniża postrzegane ryzyko (uczestnicy wymian nabrali pewności siebie i teraz mniej się boją). Obie interpretacje są prawdopodobne i warte szerszego zbadania longitudinalnego. Literatura wskazuje, że doświadczenie zagraniczne często zwiększa poczucie własnej skuteczności i otwartość na ryzyko (Zmysłowski, 2018).
- Kierunek studiów: Nie odnotowano znaczących różnic między studentami różnych dziedzin pod względem gotowości do mobilności, po kontrolowaniu wpływu innych czynników. Jedynie studenci kierunków związanych z językami obcymi i filologiami częściej planowali wyjazd (co zrozumiałe – to część ich ścieżki rozwoju), a studenci kierunków inżynierskich nieco rzadziej (być może z uwagi na inne priorytety lub

mniejsze tradycje wymian w tych dziedzinach). Jednak ogólna zależność ryzyko-mobilność występowała we wszystkich grupach.

Podsumowując, hipoteza główna została potwierdzona: wysoka percepcja ryzyka geopolitycznego idzie w parze z obniżoną gotowością do mobilności akademickiej. Wynik ten utrzymuje się także przy uwzględnieniu innych zmiennych – lęk przed globalnymi zagrożeniami okazał się jednym z najsilniejszych predyktorów niechęci do wyjazdu (obok braku doświadczenia). Warto zaznaczyć, że respondenci wprost wskazywali obawy o bezpieczeństwo jako istotny powód powstrzymujący ich przed mobilnością: spośród tych, którzy nie rozważają wyjazdu, 45% zaznaczyło opcję „obawy o bezpieczeństwo za granicą" jako jedną z przyczyn (była to trzecia najczęstsza odpowiedź po „brak środków finansowych" – 64% oraz „zobowiązania rodzinne/sytuacja osobista" – 47%). Zatem czynniki ekonomiczne wciąż dominują, ale tuż za nimi plasuje się strach o bezpieczeństwo.

Dyskusja

Uzyskane wyniki rzucają światło na istotny – a dotąd słabo zbadany w Polsce – aspekt decyzji studentów o udziale w programach mobilności: poczucie bezpieczeństwa w kontekście globalnym. Wychodzi na to, że w świadomości młodych ludzi zarysował się wyraźny dylemat: *rozwój edukacyjny vs. bezpieczeństwo osobiste*. Wielu studentów, choć dostrzega korzyści płynące ze studiowania za granicą, jednocześnie obawia się globalnej niestabilności na tyle, że rezygnuje lub waha się przed wyjazdem.

Jak nasze wyniki mają się do wcześniejszych badań? W literaturze międzynarodowej coraz więcej pojawia się doniesień o wpływie czynników politycznych na mobilność studentów. Mok, Shen i Gu (2024) pokazali, że chińscy studenci topowych uczelni wprawdzie chcą kontynuować naukę za granicą, ale realia geopolityczne (wizy, napięcia) zmuszają ich do zmiany planów. Nasze badanie potwierdza ten mechanizm w innym kontekście: polscy studenci z własnej inicjatywy mogą zmieniać plany z powodu odczuwanego zagrożenia (np. ktoś planował wymianę na Wschód, ale po wybuchu wojny na Ukrainie zrezygnował). W podobnym kierunku idą ustalenia Barcakovej i Launikariego (2024), według których wojna w Ukrainie, Brexit i zmiany klimatyczne zaburzyły wzrostowy trend mobilności edukacyjnej i wymuszają pytanie o sposoby zachęcania studentów do wyjazdów

w okresie niepewności. IC3 Movement (2025) wskazuje natomiast, że wojny, spory handlowe, zmieniające się sojusze i napięcia graniczne wpływają na decyzje młodych ludzi dotyczące miejsca studiowania, wyboru kariery i wyobrażeń o przyszłości. Nasze wyniki liczbowo obrazują właśnie to zjawisko – pewna część studentów (około 1/3) uważa, że obecnie wyjazd za granicę może być zbyt ryzykowny, i woli go unikać.

Interesujące jest powiązanie między doświadczeniem a postrzeganiem ryzyka. Wychodzi na to, że osoby, które *nigdy jeszcze nie wyjechały*, mają wyższy poziom lęku (co jest zrozumiałe: boją się nieznanego). Ci zaś, którzy spróbowali – być może przekonali się, że świat nie jest aż tak straszny, jak się obawiali, dzięki czemu ich dalsza gotowość rośnie. Można tu przywołać teorię *„kapitału mobilności"* (Murphy-Lejeune, 2002), która zakłada, że kompetencje nabyte podczas pierwszych wyjazdów (językowe, międzykulturowe, psychologiczne) ułatwiają kolejne migracje i zmniejszają bariery psychiczne. Nasze wyniki są zgodne z tą teorią: brak „kapitału mobilności" wiąże się z większą barierą lękową. To implikuje, że wsparcie przy pierwszym wyjeździe (np. na krótszą mobilność) może pomóc zredukować lęki i otworzyć drogę do dalszej internacjonalizacji studenta.

Wynik silnej korelacji strachu z niechęcią do mobilności rodzi pytanie: *czy te obawy są racjonalne?* Z jednej strony, ostrożność w obliczu realnych zagrożeń jest uzasadniona. Jeśli ktoś np. planował studia w kraju, gdzie toczy się konflikt zbrojny lub panuje chaos polityczny, jego lęk i rezygnacja z takiego zamiaru są logiczne. Problematyczne jest jednak *nadmierne uogólnienie strachu* na wszystkie wyjazdy zagraniczne. Obecna sytuacja geopolityczna jest zróżnicowana – obok regionów niebezpiecznych (strefy wojny) istnieje wiele krajów relatywnie bezpiecznych. Niestety, intensywność medialnych przekazów o zagrożeniach może powodować, że studenci czują się zagrożeni *globalnie*, nawet jeśli planują wyjazd do spokojnego kraju. Zjawisko to nawiązuje do koncepcji tzw. *„lęku egzystycznego w globalnym społeczeństwie ryzyka"* (Beck, 2012), gdzie świadomość globalnych zagrożeń sprawia, że nawet jednostki dalekie od epicentrum konfliktów odczuwają ich ciężar psychiczny (Beck, 2012). Nasza próba wskazuje, że faktycznie spora część studentów ma takie poczucie „zagrożenia wiszącego w powietrzu".

Z drugiej strony, pewien poziom lęku może być efektem braku rzetelnej informacji bądź wsparcia. Można przypuszczać, że odpowiednia

edukacja i przygotowanie studentów przed wyjazdem mogą zmniejszyć ich obawy. Na przykład uniwersytety mogłyby lepiej informować o realnych zagrożeniach i środkach bezpieczeństwa w poszczególnych krajach, by oddzielić *faktyczne ryzyko* od *wyolbrzymionych obaw*. Warto też zwrócić uwagę, że mobilność akademicka odbywa się zwykle w ramach zorganizowanych programów, gdzie studenci są pod opieką instytucji (uczelni wysyłającej i przyjmującej). Program Erasmus+ posiada procedury reagowania kryzysowego – np. w razie nagłego pogorszenia sytuacji w danym kraju uczestnicy mogą liczyć na ewakuację czy pomoc finansową. Być może studenci nie są świadomi tych zabezpieczeń i dlatego wyolbrzymiają ryzyko bycia „porzuconym" za granicą w razie problemów. Zastosowanie mogłoby tu mieć włączenie elementów edukacji bezpieczeństwa do przygotowania przedwyjazdowego.

Nasze wyniki wpisują się także w szerszy obraz zmian w mobilności: coraz większą rolę zaczynają odgrywać formy alternatywne – mobilność wirtualna, hybrydowa, regionalna. Jeśli studenci boją się dalekich wyjazdów, mogą wybierać np. kraje bliższe kulturowo lub geograficznie (nasza ankieta tego bezpośrednio nie mierzyła, ale inne badania sugerują istnienie takiego trendu). Również wspomniany wzrost popularności mobilności zdalnej może świadczyć o chęci redukcji ryzyka – student może „uczestniczyć" w zajęciach zagranicznych, nie opuszczając bezpiecznego domu. To rodzi pytanie, czy w dłuższej perspektywie nastąpi spadek mobilności fizycznej wśród bardziej lękliwych pokoleń, a wzrost wykorzystania rozwiązań technologicznych. Laurea Journal donosi, że już teraz połowa uczelni europejskich planuje rozwój oferty wirtualnej mobilności (Barcakova, Launikari, 2024). Można to interpretować zarówno jako odpowiedź na potrzeby studentów, jak i na wyzwania (klimatyczne, finansowe, a także związane z bezpieczeństwem).

Należy również wspomnieć o potencjalnych konsekwencjach ograniczenia mobilności akademickiej z powodu obaw. Jeśli znaczna część młodzieży zrezygnuje z doświadczeń międzynarodowych, może to mieć ujemny wpływ na ich kompetencje i konkurencyjność. Ponadto mniej kontaktów międzykulturowych to mniejsza wzajemna tolerancja i zrozumienie – jednym z filarów pokoju jest przecież wymiana ludzi i idei. Paradoksalnie więc, uleganie strachowi przed zagrożeniami może w dłuższej skali pogłębić

podziały międzynarodowe. Dlatego ważne jest, aby instytucje edukacyjne i decydenci starali się podtrzymać mobilność, nawet w trudnych czasach. European Commission już podejmuje działania, np. nowe rekomendacje „Europe on the Move" z 2023 r. mają uczynić mobilność bardziej inkluzywną i odporną (Barcakova, Launikari, 2024). Jednak równie istotne będzie zadbanie o zdrowie psychiczne i poczucie bezpieczeństwa studentów. Raport IC3 Movement (2025) podkreśla potrzebę zapewnienia młodym ludziom wsparcia psychologicznego i doradztwa, by w świecie pełnym chaosu mogli nadal realizować swoje aspiracje (IC3 Movement, 2025). Tworzenie *„bezpiecznych przestrzeni"* do rozmowy o obawach, edukacja medialna (by umieć krytycznie oceniać doniesienia) czy pokazywanie pozytywnych stron globalnego kształcenia – to wszystko może pomóc oswoić lęki.

Wnioski

Przeprowadzone badanie pozwala sformułować następujące główne wnioski:

1. Wysoka percepcja ryzyka geopolitycznego przekłada się na niższą gotowość do mobilności akademickiej – studenci odczuwający silny lęk przed globalnymi zagrożeniami (wojnami, terroryzmem, niestabilnością) znacznie rzadziej planują wyjazdy za granicę w celach edukacyjnych niż ich koledzy, którzy takich obaw mają mniej. Wykazano istotną statystycznie negatywną korelację między poziomem lęku a chęcią uczestnictwa w programach wymiany.
2. Obawy o bezpieczeństwo za granicą stały się istotną barierą w podejmowaniu decyzji o wyjeździe. Wśród badanych studentów blisko połowa z grupy nieplanującej mobilności wskazała sytuację bezpieczeństwa jako jeden z czynników powstrzymujących. Najbardziej przeraża perspektywa konfliktu zbrojnego – 70% studentów deklaruje, że wizja wojny działa zniechęcająco na plany wyjazdowe. Znaczące są też obawy przed terroryzmem i niestabilnością polityczną.
3. Większość studentów (ok. 60%) jest wciąż zainteresowana mobilnością, ale dominują postawy niepewności i wahania („raczej tak" zamiast „zdecydowanie tak"). Tylko co czwarty student jest zdecydowany na wyjazd, podczas gdy co szósty stanowczo wyklucza taką możliwość. Świadczy to o tym, że potencjalny poziom mobilności

może być niższy niż przed kilku laty – jeśli znaczna część osób wahających się ostatecznie zrezygnuje.

4. Doświadczenie międzynarodowe obniża lęk i sprzyja mobilności. Studenci, którzy już wcześniej uczestniczyli w mobilności (np. w czasie studiów licencjackich), wykazują istotnie niższą percepcję ryzyka i znacznie częściej planują ponowne wyjazdy. To sugeruje efekt pozytywnego wzmocnienia: pierwszy wyjazd przełamuje bariery psychiczne i buduje „kapitał mobilności", ułatwiający kolejne przedsięwzięcia.
5. Nie zaobserwowano silnych różnic pod względem płci czy kierunku studiów w samej gotowości do mobilności, po uwzględnieniu wpływu innych czynników. Kobiety co prawda odczuwają nieco większy lęk geopolityczny, ale gdy on jest kontrolowany, płeć nie różnicuje już istotnie skłonności do wyjazdów. Oznacza to, że wsparcie powinno być kierowane zarówno do studentek, jak i studentów – obie grupy w podobnym stopniu wymagają zachęty, choć u kobiet warto zwrócić uwagę na łagodzenie strachu.
6. Istnieje potrzeba interwencji ze strony instytucji edukacyjnych, aby utrzymać mobilność akademicką w dobie globalnej niepewności. Uczelnie i agencje wymiany (jak NAWA czy Erasmus+) powinny wdrożyć działania informacyjne i pomocowe: rzetelnie informować o realnych ryzykach w krajach docelowych, zapewniać procedury bezpieczeństwa i awaryjnego powrotu (co już ma miejsce, ale należy to komunikować studentom), organizować wsparcie psychologiczne i mentoring dla osób obawiających się wyjazdu.
7. Rozwijanie form mobilności alternatywnej (wirtualnej, hybrydowej) może częściowo zaspokoić potrzeby tych studentów, którzy w obecnych warunkach nie zdecydują się na wyjazd fizyczny. Jednakże nie należy rezygnować z promocji tradycyjnej mobilności, gdyż nic nie zastąpi bezpośredniego kontaktu z inną kulturą. Zadaniem na przyszłość jest znalezienie równowagi: jak zapewnić młodym ludziom *globalne doświadczenie edukacyjne* przy akceptowalnym dla nich poziomie poczucia bezpieczeństwa.

Podsumowując, percepcja ryzyka geopolitycznego stanowi istotny, negatywny korelat mobilności akademickiej w badanej grupie polskich studentów. Wyniki te wpisują się w szersze obserwacje o wpływie „ducha

czasów" na postawy młodego pokolenia. W dobie, gdy – cytując Becka – „strach nieodłącznie nam towarzyszy" (Beck, 2012), wyzwaniem staje się podtrzymanie otwartości i ciekawości świata u studentów. Utrzymanie mobilności akademickiej ma znaczenie nie tylko dla jednostkowych karier, ale i dla budowania międzynarodowego zrozumienia w niestabilnych czasach. Dlatego rekomendujemy dalsze badania nad tym zagadnieniem (np. jakościowe wywiady pogłębiające motywacje i lęki studentów) oraz praktyczne działania na poziomie uczelni i polityk edukacyjnych, by mobilność pozostała realną i atrakcyjną ścieżką rozwoju dla młodego pokolenia, a nie ofiarą współczesnych zagrożeń (IC3 Movement, 2025).

Literatura

1. Barcakova, M., Launikari, L. (2024). *Geopolitical instability challenges student mobility in European higher education*. *Laurea Journal*. Pobrane z: https://journal.laurea.fi/geopolitical-instability-challenges-student-mobility-in-european-higher-education/ (dostęp: 12.02.2026).
2. Beck, U. (2012). *Społeczeństwo światowego ryzyka.* Wydawnictwo Naukowe Scholar.
3. Behn, M., Lang, J. H., Reghezza, A. (2022). Geopolitical risk and its implications for macroprudential policy. *Macroprudential Bulletin*, *28*, 1.
4. Caldara, D., Iacoviello, M. (2022). Measuring Geopolitical Risk, *American Economic Review*, *112*(4), 1194-1225.
5. IC3 Movement. (2025). *Beyond Borders: How Geopolitical Turmoil Shapes Students' Dreams*. IC3 Insights Blog. Pobrane z: : https://www.ic3movement.com/post/beyond-borders-how-geopolitical-turmoil-shapes-students-dreams (dostęp: 12.02.2026).
6. Mok, K. H., Shen, W., Gu, F. (2024). The Impact of Geopolitics on International Student Mobility: The Chinese Students' Perspective. *Higher Education Quarterly 78*(4), e12509. https://doi.org/10.1111/hequ.12509
7. Polskie Radio. (2025). *Nearly 44% of Poles fear global conflict: survey*. Serwis PolskieRadio24. Pobrane z: https://www.polskieradio.pl/395/7789/artykul/3544411,nearly-44-of-poles-fear-global-conflict-survey (dostęp: 17.06.2026).
8. Zmysłowski, F. (2018). *Mobilność a ryzyko: zmiana postaw względem zachowań ryzykownych podczas udziału w programie wymiany studenckiej Erasmus+*. Praca magisterska. Uniwersytet Jagielloński.

Karol Zygo[1]
Uniwersytet w Siedlcach

https://doi.org/10.29316/9788368103373_12

HYBRYDYZACJA ZAGROŻEŃ NA GRANICY POLSKO-BIAŁORUSKIEJ A ZDROWIE PUBLICZNE. ANALIZA RYZYK EPIDEMIOLOGICZNYCH I SYSTEMOWYCH W WARUNKACH WYMUSZONEJ MIGRACJI

THE CONVERGENCE OF THREATS ON THE POLISH-BELARUSIAN BORDER AND PUBLIC HEALTH. AN ANALYSIS OF EPIDEMIOLOGICAL AND SYSTEMIC RISKS IN THE CONTEXT OF FORCED MIGRATION

Streszczenie

Rozdział analizuje presję migracyjną na granicy polsko-białoruskiej jako element zagrożeń hybrydowych oraz jej konsekwencje dla zdrowia publicznego. Celem opracowania jest identyfikacja i jakościowa analiza ryzyk epidemiologicznych i systemowych generowanych przez wymuszoną migrację w kontekście bezpieczeństwa wewnętrznego państwa. Badanie oparto na jakościowej analizie danych statystycznych Straży Granicznej z lat 2021-2024 oraz raportów Światowej Organizacji Zdrowia dotyczących profilu epidemiologicznego państw pochodzenia migrantów.

[1] https://orcid.org/0000-0002-8274-1958, e-mail: karolzygo@interia.pl

Wyniki wskazują, że presja migracyjna generuje istotne ryzyka epidemiologiczne, w szczególności związane z chorobami zakaźnymi o znaczeniu globalnym, oraz ryzyka systemowe wpływające na funkcjonowanie struktur ochrony zdrowia i nadzoru sanitarno-epidemiologicznego. Rozdział podkreśla potrzebę uwzględniania zdrowia publicznego jako integralnego elementu analiz zagrożeń hybrydowych.

Słowa kluczowe: zagrożenia hybrydowe, presja migracyjna, zdrowie publiczne, ryzyka epidemiologiczne, ryzyka systemowe, granica polsko-białoruska

Abstract

The article analyses migratory pressure on the Polish-Belarusian border as a component of hybrid threats and its implications for public health. The aim of the study is to identify and qualitatively assess the epidemiological and systemic risks arising from forced migration in the context of internal security. The research is based on a qualitative analysis of Polish Border Guard data from 2021-2024 and World Health Organisation reports on the epidemiological profiles of migrants' countries of origin. The findings indicate that migratory pressure generates significant epidemiological risks related to globally relevant infectious diseases, as well as systemic risks affecting the functioning of public health and sanitary surveillance systems. The article highlights the need to incorporate public health considerations into analyses of hybrid threats.

Keywords: hybrid threats, migratory pressure, public health, epidemiological risks, systemic risks, Polish-Belarusian border

Wstęp

Współczesne środowisko bezpieczeństwa coraz częściej kształtowane jest przez zagrożenia o charakterze hybrydowym, łączące instrumenty polityczne, społeczne, informacyjne oraz pozamilitarne. Jednym z ich istotnych przejawów jest instrumentalizacja migracji, wykorzystywana jako narzędzie wywierania presji na państwa i organizacje międzynarodowe. Kryzys migracyjny na granicy polsko-białoruskiej, zapoczątkowany w 2021 r., stanowi przykład takiego działania, w którym presja migracyjna została użyta w sposób zaplanowany i skoordynowany, generując wielowymiarowe konsekwencje dla bezpieczeństwa państwa. Dotychczasowe analizy tego kryzysu koncentrowały się głównie na jego wymiarze politycznym, prawnym, militarnym oraz migracyjnym. Zdecydowanie rzadziej podejmowano natomiast problematykę zdrowia publicznego jako integralnego komponentu bezpieczeństwa

wewnętrznego państwa, narażonego na pośrednie oddziaływanie działań hybrydowych. Tymczasem presja migracyjna o charakterze wymuszonym i nieregularnym może generować ryzyka epidemiologiczne oraz systemowe, wpływając na funkcjonowanie nadzoru sanitarno-epidemiologicznego, zdolność reagowania kryzysowego oraz wydolność systemu ochrony zdrowia.

Celem rozdziału jest identyfikacja oraz pogłębiona, jakościowa analiza ryzyk epidemiologicznych i systemowych związanych z presją migracyjną na granicy polsko-białoruskiej, rozpatrywanych w kontekście zagrożeń hybrydowych. Autor zakłada, że zdrowie publiczne nie stanowi wyłącznie obszaru reakcji humanitarnej, lecz jest elementem odporności państwa, który może być pośrednio obciążany i destabilizowany w ramach działań hybrydowych. W ujęciu metodologicznym rozdział opiera się na jakościowej analizie ryzyka, rozumianej jako identyfikacja, charakterystyka oraz interpretacja potencjalnych zagrożeń w oparciu o dane empiryczne i źródła instytucjonalne. W badaniu wykorzystano dane statystyczne Straży Granicznej z lat 2021-2024, dotyczące skali i struktury nielegalnych przekroczeń granicy polsko-białoruskiej, a także raporty i opracowania Światowej Organizacji Zdrowia (WHO) odnoszące się do profilu epidemiologicznego chorób zakaźnych w państwach pochodzenia migrantów. Metoda badawcza polega na zestawieniu danych migracyjnych z informacjami epidemiologicznymi oraz na analizie ich implikacji dla funkcjonowania systemu zdrowia publicznego państwa przyjmującego.

Rozdział łączy perspektywę badań nad bezpieczeństwem z analizą zdrowia publicznego, traktując je jako wzajemnie powiązane i komplementarne obszary analizy. Takie podejście pozwala na całościową ocenę skutków presji migracyjnej w warunkach zagrożeń hybrydowych oraz na wskazanie potrzeby uwzględniania komponentu zdrowotnego w analizach bezpieczeństwa i w procesie kształtowania polityki państwa

Hybrydyzacja zagrożeń i instrumentalizacja migracji – ujęcie teoretyczne

Współczesne konflikty coraz częściej przybierają charakter wielomodalny i hybrydowy, co oznacza odejście od tradycyjnych podziałów na wojny konwencjonalne, nieregularne oraz terrorystyczne. Wojna hybrydowa polega na integracji różnych form prowadzenia walki w ramach jednego

teatru działań, przy jednoczesnym wykorzystywaniu zdolności konwencjonalnych, nieregularnych, terrorystycznych, cybernetycznych, a także działań o charakterze przestępczym. Istotą tego modelu jest projektowanie kombinacyjnych zagrożeń, ukierunkowanych na oddziaływanie na konkretne podatności państwa przeciwnika (Hoffman, 2009).

W takim ujęciu dochodzi do zatarcia granicy pomiędzy aktorami państwowymi i niepaństwowymi, a podmioty zaangażowane w konflikt sięgają po pełne spektrum dostępnych środków, dostosowując je do własnej kultury strategicznej oraz uwarunkowań operacyjnych. Zagrożenia hybrydowe obejmują przy tym szeroki zakres działań destabilizujących, w tym w szczególności bezpieczeństwo informacyjne państwa. Unia Europejska definiuje zagrożenia hybrydowe jako połączenie działań konwencjonalnych i niekonwencjonalnych (militarnych i niemilitarnych), stosowanych w sposób skoordynowany przez aktorów państwowych i niepaństwowych w celu osiągnięcia określonych celów politycznych (Rada Unii Europejskiej, 2026). W dokumentach UE podkreśla się wielowymiarowy charakter zagrożeń hybrydowych, opartych na wykorzystaniu środków przymusu oraz działań dywersyjnych, wymierzonych w krytyczne słabe punkty państwa (Wyrębek, 2023). Zagrożenia hybrydowe charakteryzują się synergicznym łączeniem metod oddziaływania, zdecentralizowanym planowaniem oraz wielomodalną strukturą działań, umożliwiającą osiąganie efektów zarówno w wymiarze fizycznym, jak i psychologicznym konfliktu. Model ten łączy wysoką intensywność i śmiercionośność konfliktów międzypaństwowych z długotrwałością i determinacją właściwą wojnom nieregularnym. Doświadczenia ostatnich konfliktów wskazują, że aktorzy niepaństwowi wykazują zdolność do skutecznej adaptacji zaawansowanych technologii i taktyk, co prowadzi do konwergencji zagrożeń, zamiast ich jednoznacznego rozdzielenia. W rezultacie wojna hybrydowa staje się dominującym paradygmatem współczesnego środowiska bezpieczeństwa (Hoffman, 2009).

Działania prowadzone „poniżej progu wojny" wpisują się w kategorię subwersji, która we współczesnym środowisku bezpieczeństwa stanowi rdzeń operacyjny wojny hybrydowej. W. Rosenau wyróżnił trzy podstawowe formy subwersji: działalność grup fasadowych (*front groups*), infiltrację struktur państwa oraz wzniecanie niepokojów społecznych. Mechanizmy te umożliwiają odpowiednio unikanie odpowiedzialności przez sponsorów,

dostęp do informacji i procesów decyzyjnych oraz osłabianie legitymizacji władzy publicznej i zaufania społecznego (Gil, 2021).

Choć Rosenau odnosił te działania głównie do aktorów niepaństwowych, współczesne konflikty charakteryzują się przesunięciem ciężaru subwersji w stronę państw, zwłaszcza mocarstw, które realizują ją pośrednio poprzez outsourcing destabilizacji. Tego rodzaju działania, oparte na zaprzeczalności (*plausible deniability*), pozostają poniżej progu użycia siły i pozwalają na długotrwałe oddziaływanie strategiczne bez otwartej eskalacji militarnej, stanowiąc integralny element wojny hybrydowej (Gil, 2021).

W tym kontekście zasadne jest rozróżnienie pomiędzy wschodnim a południowym wymiarem presji granicznej wobec Unii Europejskiej. Część presji wywieranej przez Federację Rosyjską ma charakter bezpośredni, a zatem źródło zagrożenia znajduje się w bezpośrednim sąsiedztwie UE. Odmienny charakter ma natomiast presja oddziałująca na granice południowe Unii Europejskiej (Hiszpanii, Włoch, Grecji oraz państw Bałkanów), która nie pochodzi bezpośrednio od państw sąsiadujących z UE, lecz z obszarów bardziej odległych. Przepływy migracyjne z Syrii oraz Afryki Subsaharyjskiej, kierowane odpowiednio przez terytorium Turcji, stanowią przykłady presji, której geneza nie leży w bezpośrednim sąsiedztwie Unii, lecz która może być instrumentalizowana – na przykład przez Turcję – jako narzędzie nacisku politycznego lub środek przetargowy w relacjach z UE (Lonardo, 2021).

Instrumentalizacja migracji jako narzędzie presji hybrydowej na granicy polsko-białoruskiej

Sytuacja panująca w początkowej fazie kryzysu na granicy polsko-białoruskiej została szczegółowo scharakteryzowana w uzasadnieniu do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z 2 września 2021 r. w sprawie wprowadzenia stanu wyjątkowego. Wskazano w nim na gwałtowny wzrost liczby oraz intensywności prób nielegalnego przekraczania granicy państwowej na odcinku granicy z Republiką Białorusi. Podkreślono jednocześnie, że nadzwyczajny charakter i bezprecedensowa skala presji migracyjnej nie miały charakteru spontanicznego, lecz stanowiły rezultat celowych i skoordynowanych działań podmiotów zewnętrznych, zmierzających do destabilizacji sytuacji na granicy Polski, a także innych państw

członkowskich Unii Europejskiej, w szczególności Litwy i Łotwy (Nowicka, Wołyńska, 2022). Równolegle formułowane narracje oskarżające Polskę o eskalację działań w strefie przygranicznej wpisywały się w spójną linię przekazu propagandowego Mińska i Moskwy, przedstawiającą Unię Europejską oraz NATO jako podmioty prowadzące działania agresywne i destabilizujące sytuację bezpieczeństwa w regionie (Wawrzusiszyn, 2022). Kryzys na granicy Białorusi z państwami Unii Europejskiej i NATO można ująć w dwóch zasadniczych fazach. W pierwszym etapie, obejmującym rok 2020, litewska straż graniczna odnotowała relatywnie niewielką skalę nielegalnych przekroczeń – zatrzymano wówczas 80 osób, które próbowały przekroczyć granicę białorusko-litewską. Sytuacja uległa jednak gwałtownej eskalacji w 2021 r., kiedy to na samej Litwie zatrzymano już ponad 4 tysiące migrantów (Konieczny, 2022).

Druga faza kryzysu charakteryzowała się przesunięciem głównego kierunku presji migracyjnej na Polskę. Działania reżimu Alaksandra Łukaszenki zostały poprzedzone zmianami w białoruskim porządku prawnym dotyczącym funkcjonowania strefy przygranicznej, w szczególności złagodzeniem przepisów Kodeksu wykroczeń administracyjnych, polegającym m.in. na zniesieniu sankcji za nielegalne przebywanie w strefie granicznej. Dodatkowo w czerwcu 2021 r., w trakcie narastającego kryzysu, białoruskie Ministerstwo Spraw Zagranicznych poinformowało o zawieszeniu wykonywania umowy o readmisji z Unią Europejską, jako reakcja na nałożone sankcje (Wysocki, 2024). Apogeum tej fazy kryzysu nastąpiło w sierpniu 2021 r., kiedy około 2100 osób podjęło próbę siłowego przekroczenia polsko-białoruskiego odcinka granicy państwowej, zabezpieczanego przez Podlaski Oddział Straży Granicznej. Równocześnie w okresie letnim 2021 r. na zewnętrznej granicy Unii Europejskiej z Białorusią zaobserwowano nową formę oddziaływania, określaną jako instrumentalizacja migracji. Zjawisko to ma wielowymiarowy charakter i jest realizowane na różnych poziomach oddziaływania, obejmując zarówno działania operacyjne w strefie przygranicznej, jak i szerszy kontekst polityczny, informacyjny oraz instytucjonalny (Nitszke, 2024). Instrumentalizacja migrantów to sytuacja, w której państwo trzecie wywołuje nieuregulowane przepływy migracyjne do Unii, aktywnie zachęcając do przemieszczania się obywateli państw trzecich na granice zewnętrzne, na swoje terytorium lub ze swojego terytorium, a następnie na

te granice zewnętrzne, lub ułatwiając to przemieszczanie się, w przypadku, gdy takie działania wskazują na to, że państwo trzecie zamierza zdestabilizować Unię lub państwo członkowskie, oraz gdy charakter takich działań może zagrozić podstawowym funkcjom państwa, w tym jego integralności terytorialnej, utrzymaniu porządku publicznego lub ochronie bezpieczeństwa narodowego (Komisja Europejska, 2021).

Jak wskazuje A. Wawrzusiszyn, działania hybrydowe ukierunkowane na zewnętrzne granice Unii Europejskiej i NATO realizowały jasno określone cele polityczne Białorusi i Federacji Rosyjskiej. W przypadku Mińska presja migracyjna miała służyć wzmocnieniu pozycji Alaksandra Łukaszenki wobec UE, wymuszeniu debaty wewnątrz Wspólnoty oraz uzyskaniu koncesji politycznych i finansowych pod pretekstem rozwiązania kryzysu humanitarnego. Działania te były prowadzone przy wielowymiarowym wsparciu Rosji, obejmującym skoordynowane stanowisko polityczne, operacje informacyjne oraz instrumenty z obszaru bezpieczeństwa. Z kolei z perspektywy Moskwy kryzys migracyjny stanowił element szerszej strategii destabilizacyjnej wobec Zachodu, umożliwiającej wywieranie presji politycznej, manipulowanie nastrojami społecznymi oraz odwracanie uwagi od działań prowadzonych w innych obszarach, w tym wobec Ukrainy (Wawrzusiszyn, 2025).

Zdrowie publiczne w paradygmacie bezpieczeństwa

Rozumienie i interpretacja pojęcia zdrowia publicznego, mimo jego intensywnego rozwoju w ostatnich dekadach, nadal pozostają niejednoznaczne. Dotyczy to w szczególności prób formułowania definicji, które mogłyby pełnić funkcję obiektywnego kryterium, pozwalającego w sposób neutralny odróżniać zjawiska i procesy mieszczące się w zakresie zdrowia publicznego od tych, które wykraczają poza jego granice pojęciowe. Istotne trudności interpretacyjne wynikają w dużej mierze z powszechnej praktyki włączania do definicji zdrowia publicznego kategorii celu, co dodatkowo komplikuje precyzyjne wyznaczenie zakresu tego pojęcia (Włodarczyk, 2007). Zdrowie publiczne stanowi wielodyscyplinarną dziedzinę badań oraz oddziaływań praktycznych, która nastawiona jest na promowanie zdrowia ludności, zapobieganie chorobom, zmniejszenie wskaźników przedwczesnej umieralności, jak również doskonalenie opieki zdrowotnej (Górnik-Durose, 2011). Zdaniem B. Uramowskiej-Żyto przy ocenie zdrowotności populacji

nie sposób odmówić znaczenia czynnikom społeczno-demograficznym, do których należą: klasa i warstwa społeczna, pozycja społeczno-ekonomiczna, pochodzenie etniczne, zawód, wykształcenie oraz stan cywilny (Uramowska-Żyto, 1980). Natomiast, jak twierdzi K. Zygo, zdrowie populacji ma przede wszystkim znaczenie z punktu widzenia jej przetrwania (Zygo, 2024). Współcześnie uważa się, że do czynników pozytywnie korelujących ze stanem zdrowia ludności należą: zatrudnienie i dobre warunki pracy, warunki mieszkaniowe i sanitarne, dochody chroniące przed ubóstwem, zaopatrzenie w zdrową żywność i czystą wodę, czyste powietrze i gleba, uczestnictwo w życiu społecznym, aktywny styl życia, łatwy dostęp do świadczeń zdrowotnych i pomocy społecznej (Szymańczak, 2010).

Zdrowie publiczne realizuje wiele istotnych funkcji społecznych. Zdaniem M. Millera oraz A. Zielińskiego funkcje te można ująć w dwóch zasadniczych kategoriach: działania ukierunkowane na całą populację oraz działania adresowane do jednostek (Miller, 2002). Na podstawie tej klasyfikacji autor rozdziału dokonał ich uszczegółowienia, przedstawiając w Tabeli 1 szczegółowe elementy wchodzące w zakres obu kategorii.

Tabela 1. Funkcje zdrowia publicznego

Działania na rzecz ogółu ludności	Działania na rzecz indywidualnych osób
• monitorowanie stanu zdrowia populacji, • walka z chorobami o znaczeniu społecznym, wypadkami i urazami, • identyfikacja i zwalczanie zagrożeń zdrowotnych w środowisku, miejscu zamieszkania, pracy, w żywności i wodzie, • nadzór epidemiologiczny, kontrola laboratoryjna chorób zakaźnych – w tym zawleczonych z zagranicy – oraz zagrożeń środowiskowych, • promocja zdrowia, organizacja aktywnego współuczestnictwa społeczeństwa w działaniach na rzecz zdrowia, determinanty zdrowia i choroby, • zarządzanie opieką zdrowotną, ekonomika zdrowia, systemy organizacji i finansowania ochrony zdrowia, • ocena jakości świadczeń zdrowotnych, zagadnienia prawne w medycynie, bioetyka, orzecznictwo lekarskie.	• profilaktyka indywidualna, organizacja służb zapobiegawczych, np. szczepienia ochronne, profilaktyka zakażeń szerzących się drogą kontaktów seksualnych, planowanie rodziny, • profilaktyka i leczenie chorób o znaczeniu społecznym: choroby zakaźne w tym AIDS, gruźlica, choroby psychiczne, uzależnienia, wybrane choroby cywilizacyjne (np. cukrzyca), • organizacja czynnego poradnictwa dla grup wysokiego ryzyka zachorowania, • podstawowa opieka zdrowotna, pomoc medyczna dla bezdomnych i innych osób pozbawionych dostępu do świadczeń zdrowotnych, • organizacja opieki zdrowotnej finansowanej przez instytucje pozarządowe.

Źródło: Zygo, 2024, s. 147.

W warunkach presji migracyjnej o charakterze hybrydowym funkcje zdrowia publicznego nabierają szczególnego znaczenia, ponieważ stanowią jeden z kluczowych elementów odporności państwa na zagrożenia epidemiologiczne, środowiskowe i systemowe. Jedną z kluczowych funkcji zdrowia publicznego jest monitorowanie potencjalnych zagrożeń oraz podejmowanie działań ochronnych, co bezpośrednio wpływa na poziom bezpieczeństwa zdrowotnego społeczeństwa i pełni istotną rolę profilaktyczną, w szczególności w zakresie zapobiegania chorobom zakaźnym. W tym kontekście szczególne znaczenie należy przypisać epidemiologii, obejmującej nadzór nad laboratoriami diagnostycznymi, a także monitorowanie zagrożeń i skażeń środowiskowych, takich jak zanieczyszczenie wody, powietrza, gleby czy żywności. Uzupełnieniem tych działań jest zapewnienie powszechnego dostępu do szczepień ochronnych oraz wczesne wykrywanie i leczenie chorób. Przykładami schorzeń o istotnym znaczeniu epidemiologicznym są m.in. HIV/AIDS, gruźlica, choroby przenoszone drogą płciową, a także choroby endemiczne występujące poza granicami kraju, takie jak gorączka Zachodniego Nilu, gorączki krwotoczne czy malaria, które w przypadku zawleczenia mogą stanowić poważne zagrożenie dla zdrowia publicznego (Zygo, 2024).

Istotnym obszarem działań zdrowia publicznego jest również identyfikacja kluczowych potrzeb zdrowotnych populacji oraz ich optymalne zaspokajanie, w tym zapewnienie dostępu do badań diagnostycznych, leków i leczenia chorób o tzw. znaczeniu społecznym. Do tej grupy zalicza się m.in. cukrzycę, otyłość i zespół metaboliczny, hipercholesterolemię, choroby układu sercowo-naczyniowego oraz zaburzenia psychiczne. W tym wymiarze ważną rolę odgrywa także funkcja promocyjna zdrowia, polegająca na kształtowaniu prozdrowotnych postaw i stylu życia, ze szczególnym uwzględnieniem działań edukacyjnych skierowanych do dzieci i młodzieży (Zygo, 2024). W obszarze profilaktyki istotnym zadaniem pozostaje ponadto monitorowanie czynników ryzyka utraty zdrowia lub życia w przestrzeni publicznej, w środowisku domowym, szkolnym oraz w placówkach ochrony zdrowia. Celem tych działań jest przede wszystkim ograniczanie liczby urazów i wypadków oraz minimalizowanie ich skutków.

Niezależnie od działań zapobiegawczych, zdrowie publiczne obejmuje również reakcję na sytuacje kryzysowe, w tym zapewnienie pomocy

ofiarom klęsk żywiołowych, katastrof oraz innych zdarzeń masowych. Ważnym elementem jest także monitorowanie dostępności świadczeń zdrowotnych dla osób znajdujących się w trudnej sytuacji życiowej, takich jak osoby doświadczające bezdomności czy bezrobocia. W tym zakresie istotne znaczenie ma również wsparcie finansowe oraz nadzór nad działalnością instytucji charytatywnych świadczących pomoc medyczną i społeczną osobom chorym z niepełnosprawnościami lub ubogim (Zygo, 2024). Kolejną istotną funkcją zdrowia publicznego jest systematyczna ocena stanu zdrowia populacji, jego porównywanie z normami międzynarodowymi oraz identyfikowanie nowych zagrożeń i wyzwań wynikających z procesów globalizacji i rozwoju cywilizacyjnego. Oprócz działań bezpośrednio skierowanych do społeczeństwa, zdrowie publiczne obejmuje także aktywności służące rozwojowi tej dziedziny jako obszaru wiedzy i praktyki, w tym podnoszenie kwalifikacji zawodowych oraz ciągłe kształcenie lekarzy i pozostałego personelu medycznego. Dynamiczny postęp cywilizacyjny wymusza bowiem konieczność stałego doskonalenia kompetencji zawodowych. Nie bez znaczenia pozostaje również tworzenie i aktualizowanie ram prawnych regulujących funkcjonowanie systemu ochrony zdrowia, w szczególności w zakresie zarządzania i finansowania placówek medycznych. Uzupełnieniem tych działań jest monitorowanie jakości, dostępności i efektywności świadczeń zdrowotnych, z uwzględnieniem współczesnych standardów bioetycznych, praw pacjenta, prawa pracy oraz międzynarodowych regulacji dotyczących ochrony zdrowia (Zygo, 2024).

Autor rozdziału wskazuje, że w warunkach wymuszonej migracji na granicy polsko-białoruskiej realizacja kluczowych funkcji zdrowia publicznego stanowi jedno z zasadniczych wyzwań dla bezpieczeństwa wewnętrznego państwa oraz jego zdolności do skutecznego.

Presja migracyjna na granicy polsko-białoruskiej a ryzyka zdrowia publicznego – analiza empiryczna

Łączna długość granicy Rzeczypospolitej Polskiej z Republiką Białorusi wynosi 418 km. Odcinek ten jest chroniony przez 19 placówek Straży Granicznej, z czego 12 placówek funkcjonuje w strukturze Podlaskiego Oddziału Straży Granicznej, zabezpieczając 247 km granicy, natomiast 7 placówek należy do Nadbużańskiego Oddziału Straży Granicznej,

odpowiedzialnego za 171 km odcinka granicznego (Oskierko, 2022). W celu wzmocnienia ochrony granicy państwowej oraz zapewnienia bezpieczeństwa wewnętrznego i porządku publicznego, na odcinek granicy z Białorusią skierowano znaczące siły i środki. W działaniach ochronnych zaangażowano łącznie około 20 tys. funkcjonariuszy i żołnierzy, w tym około 4 tys. funkcjonariuszy Straży Granicznej, około 14 tys. żołnierzy Sił Zbrojnych RP oraz około 2 tys. funkcjonariuszy Policji (Wawrzusiszyn, 2022). Ze względu na systemowy charakter kryzysu migracyjnego, związanego z długotrwałymi działaniami prowokacyjnymi i destabilizacyjnymi podejmowanymi przez reżim Alaksandra Łukaszenki, na polsko-białoruskim odcinku granicy państwowej wybudowano ogrodzenie graniczne o długości 187 km. Inwestycja ta miała charakter strategiczny i została zrealizowana na terenie województwa podlaskiego, wzdłuż lądowej granicy z Republiką Białorusi (Ustawa z dnia 29 października 2021 r. o budowie zabezpieczenia granicy państwowej, 2021). Na odcinku województwa lubelskiego granica polsko-białoruska przebiega wzdłuż rzeki Bug, która stanowi naturalną barierę terenową.

M. Oskierko oraz S. Żurawski dokonali analizy dostępnych danych statystycznych opracowanych przez Straż Graniczną. Zestawienie tabelaryczne przedstawia cudzoziemców zatrzymanych lub ujawnionych bezpośrednio na linii granicy państwowej, w strefie nadgranicznej oraz poza nią, którzy przekroczyli bądź usiłowali przekroczyć polsko-białoruską granicę państwową z naruszeniem obowiązujących przepisów prawa (Oskierko, Żurawski, 2025).

Na podstawie danych udostępnionych przez Straż Graniczną autorzy wnioskują, że w latach 2021-2024 na polsko-białoruskim odcinku granicy państwowej, w kierunku do Polski, najliczniejszą grupę zatrzymanych stanowili migranci pochodzący z Bliskiego Wschodu oraz Afryki. Wśród nich dominowali obywatele: Iraku (1754), Syrii (802), Afganistanu (711), Somalii (559), Etiopii (491), Erytrei (462), Jemenu (245), Sudanu (222) oraz Iranu (187). Pozostałe obywatelstwa były reprezentowane w liczbie nieprzekraczającej kilkudziesięciu osób (Oskierko, Żurawski, 2025).

W Tabeli 2 zaprezentowano liczbę cudzoziemców zatrzymanych lub ujawnionych przez Straż Graniczną za nielegalne przekroczenie granicy państwowej bądź usiłowanie jej przekroczenia z terytorium Republiki Białorusi do Rzeczypospolitej Polskiej.

Tabela 2. Liczba cudzoziemców zatrzymanych lub ujawnionych przez Straż Graniczną za nielegalne przekroczenie granicy państwowej bądź usiłowanie jej przekroczenia z terytorium Republiki Białorusi do Rzeczypospolitej Polskiej

Obywatelstwo	2021 r.	2022 r.	2023 r.	2024 r.	Suma
Afganistan	447	25	88	151	711
Erytrea	0	0	9	453	462
Etiopia	4	2	14	471	491
Irak	1557	167	16	14	1754
Iran	55	40	35	57	187
Jemen	19	15	23	188	245
Somalia	68	3	38	450	559
Sudan	2	22	11	187	222
Syria	272	79	86	365	802
Pozostałe obywatelstwa	439	223	221	232	1115

Źródło: Oskierko, Żurawski, 2025, s. 55.

Zdaniem autora rozdziału struktura obywatelstw cudzoziemców zatrzymanych na polsko-białoruskim odcinku granicy państwowej w latach 2021-2024 ma istotne znaczenie z perspektywy zdrowia publicznego i bezpieczeństwa epidemiologicznego. Migranci pochodzący z regionów Bliskiego Wschodu i Afryki Subsaharyjskiej charakteryzują się często odmiennym profilem epidemiologicznym, wynikającym m.in. z ograniczonego dostępu do opieki zdrowotnej, niskiego poziomu wyszczepienia populacyjnego oraz występowania chorób zakaźnych endemicznych dla tych obszarów. W warunkach wymuszonej migracji, długotrwałego przebywania w środowisku leśnym oraz braku regularnego nadzoru sanitarno-epidemiologicznego, ryzyka te ulegają spotęgowaniu.

Z punktu widzenia zdrowia publicznego szczególne znaczenie ma fakt, że ujawnienia i zatrzymania cudzoziemców następowały nie tylko bezpośrednio na linii granicy państwowej, lecz również w strefie nadgranicznej i poza nią, co utrudnia prowadzenie systematycznego monitoringu epidemiologicznego, wczesnej diagnostyki oraz wdrażanie działań profilaktycznych. W konsekwencji presja migracyjna na granicy polsko-białoruskiej generuje złożone ryzyka epidemiologiczne, środowiskowe i systemowe, obciążając lokalne struktury ochrony zdrowia oraz wymagając ścisłej koordynacji działań służb granicznych, sanitarnych i medycznych.

Choroby zakaźne w kontekście presji migracyjnej na granicy polsko-białoruskiej

W analizach procesów migracyjnych, zwłaszcza w ujęciu społecznych kosztów i korzyści, coraz większą uwagę poświęca się zagadnieniom zdrowia populacji oraz zdrowia grup szczególnie mobilnych. Mimo rosnącego zainteresowania tą problematyką, w literaturze przedmiotu oraz analizach dotyczących zdrowia publicznego w Polsce kategoria osób o wysokiej mobilności migracyjnej nadal pozostaje niedostatecznie uwzględniana, zarówno w odniesieniu do migracji wewnętrznych, jak i transgranicznych (Kawczyńska-Butrym, 2011). Człowiek może być nosicielem różnych chorób zakaźnych, co sprawia, że procesy migracyjne mogą sprzyjać reaktywacji wcześniej występujących chorób lub rozprzestrzenianiu się nowych patogenów, dotychczas niewystępujących na obszarze państwa przyjmującego. Epidemia nie musi przy tym przyjmować charakteru zjawiska masowego za sytuację epidemiczną uznaje się już wzrost zachorowalności wyraźnie przekraczający poziom uznawany za typowy dla danego obszaru. Zjawisko to ma charakter dynamiczny i pozostaje w ścisłym związku nie tylko z czynnikami środowiskowymi, lecz także z uwarunkowaniami społecznymi i demograficznymi (Szydłowski, Wilk, Wendt, 2018).

W przypadku pojawienia się choroby dotychczas niewystępującej w danym kraju, już pojedynczy potwierdzony przypadek może stanowić sygnał alarmowy dla systemu nadzoru epidemiologicznego. Opóźnione wykrycie ogniska choroby może prowadzić do poważnych konsekwencji epidemiologicznych, co podkreśla znaczenie ciągłego monitorowania stanu zdrowia populacji. Migracje ludności o dużej skali i intensywności istotnie utrudniają jednak regularną ocenę zagrożeń zdrowotnych, jednocześnie tworząc warunki sprzyjające rozwojowi epidemii (Szydłowski, Wilk, Wendt, 2018).

Eksperci Światowej Organizacji Zdrowia (WHO) wskazują, że występowanie chorób zakaźnych pozostaje w ścisłym związku z ubóstwem oraz destabilizacją społeczno-ekonomiczną. Migranci często pochodzą z obszarów dotkniętych konfliktami zbrojnymi, wojnami lub długotrwałym kryzysem gospodarczym, a proces migracji nierzadko wiąże się z wyczerpującymi i długotrwałymi podróżami, które dodatkowo zwiększają ryzyko zachorowań, w tym na choroby zakaźne oraz choroby przenoszone drogą pokarmową i wodną (Sowizdraniuk, Sowizdraniuk, 2019).

Współczesna presja migracyjna na granicy polsko-białoruskiej, mająca charakter wymuszony i hybrydowy, ujawnia jednak potrzebę szerszego spojrzenia, wykraczającego poza perspektywę jednostkową. W tym kontekście szczególnego znaczenia nabiera analiza chorób zakaźnych jako wyzwania dla zdrowia publicznego, wymagającego skoordynowanych działań systemowych, nadzoru epidemiologicznego oraz odpowiednich mechanizmów reagowania w państwie przyjmującym.

Autor rozdziału dokonał analizy profilu epidemiologicznego chorób zakaźnych występujących w państwach pochodzenia migrantów dominujących na polsko-białoruskim odcinku granicy państwowej w latach 2021-2024, w oparciu o dane Światowej Organizacji Zdrowia. Zgodnie z ustaleniami WHO regiony te charakteryzują się podwyższoną zapadalnością na wybrane choroby zakaźne, w szczególności gruźlicę, wirusowe zapalenia wątroby, malarię, odrę oraz choroby biegunkowe. W części państw, takich jak Afganistan czy Jemen, utrzymują się również choroby o znaczeniu globalnym, w tym polio i cholera. W warunkach wymuszonej migracji, ograniczonego dostępu do opieki zdrowotnej oraz braku systematycznego nadzoru sanitarno-epidemiologicznego, czynniki te mogą prowadzić do zwiększenia ryzyk zdrowotnych, zarówno po stronie samych migrantów, jak i w odniesieniu do wydolności oraz bezpieczeństwa systemu ochrony zdrowia państwa przyjmującego. Zestawienie najważniejszych chorób zakaźnych występujących w państwach pochodzenia migrantów przedstawiono w Tabeli 3.

Tabela 3. Choroby zakaźne występujące w państwach pochodzenia migrantów

Państwo pochodzenia	Choroby zakaźne o znaczeniu epidemiologicznym (wg WHO)
Irak	Gruźlica (TB), WZW B i C, odra, choroby biegunkowe, leiszmanioza
Syria	Gruźlica, WZW B i C, odra, polio (ryzyko reintrodukcji), leiszmanioza
Afganistan	Gruźlica (w tym MDR-TB), polio (endemiczne), malaria, odra, choroby pasożytnicze
Somalia	Gruźlica, malaria, HIV/AIDS, cholera, odra, schistosomatoza
Etiopia	Gruźlica, malaria, HIV/AIDS, odra, choroby pasożytnicze
Erytrea	Gruźlica, malaria, HIV/AIDS, odra
Jemen	Cholera, gruźlica, malaria, odra, WZW A i E
Sudan	Malaria, gruźlica, cholera, gorączki krwotoczne (np. Rift Valley Fever), odra
Iran	Gruźlica, WZW B i C, HIV/AIDS (grupy wysokiego ryzyka), leiszmanioza

Źródło: opracowanie własne na podstawie WHO, 2024.

Zestawienie chorób zakaźnych o znaczeniu epidemiologicznym, opracowane na podstawie danych Światowej Organizacji Zdrowia (WHO), wskazuje na wyraźne zróżnicowanie profilu zdrowotnego państw pochodzenia migrantów ujawnionych na polsko-białoruskim odcinku granicy państwowej. Jednocześnie tabela ujawnia powtarzalność określonych jednostek chorobowych, które występują w większości analizowanych krajów i mają istotne znaczenie z perspektywy zdrowia publicznego.

W niemal wszystkich państwach ujętych w zestawieniu odnotowuje się występowanie gruźlicy (TB), w tym w Afganistanie również jej postaci lekoopornej (MDR-TB). Choroba ta pozostaje jednym z najpoważniejszych globalnych zagrożeń zdrowotnych, a jej obecność w strukturze epidemiologicznej regionów pochodzenia migrantów wymaga szczególnej uwagi w zakresie wczesnej diagnostyki i nadzoru epidemiologicznego. Równie często występują wirusowe zapalenia wątroby typu B i C, zwłaszcza w krajach Bliskiego Wschodu, takich jak Irak, Syria i Iran, co wiąże się z ryzykiem przewlekłych powikłań zdrowotnych i długofalowego obciążenia systemu ochrony zdrowia. Istotnym elementem profilu epidemiologicznego analizowanych państw jest także występowanie chorób wieku dziecięcego, w szczególności odry, która pojawia się w niemal wszystkich wskazanych krajach. W przypadku Syrii oraz Afganistanu dodatkowym zagrożeniem pozostaje ryzyko reintrodukcji poliomyelitis, co wynika z przerwanych programów szczepień ochronnych w warunkach konfliktów zbrojnych i niestabilności instytucjonalnej.

W państwach Afryki Subsaharyjskiej (Somalia, Etiopia, Erytrea, Sudan) oraz w Jemenie szczególnie widoczne są choroby związane z warunkami środowiskowymi i sanitarnymi, takie jak malaria, cholera oraz schistosomatoza. Ich obecność odzwierciedla ograniczony dostęp do bezpiecznej wody pitnej, odpowiednich warunków higienicznych oraz podstawowej opieki zdrowotnej. Dodatkowo w Sudanie odnotowuje się występowanie wirusowych gorączek krwotocznych, co wskazuje na potencjalne ryzyka o charakterze wysokiego zagrożenia epidemiologicznego. Analiza tabeli potwierdza, że struktura migracji na polsko-białoruskim odcinku granicy państwowej obejmuje populacje pochodzące z regionów o wysokim obciążeniu chorobami zakaźnymi, których profil epidemiologiczny kształtowany jest przez konflikty zbrojne, kryzysy humanitarne oraz deficyty systemów

ochrony zdrowia. W warunkach wymuszonej migracji oraz ograniczonego dostępu do bieżącej opieki medycznej czynniki te mogą przekładać się na zwiększone wyzwania dla zdrowia publicznego, wymagające skoordynowanych działań w zakresie nadzoru epidemiologicznego, diagnostyki przesiewowej i profilaktyki w państwie przyjmującym.

Podsumowanie

Przeprowadzona analiza potwierdza, że presja migracyjna na granicy polsko-białoruskiej stanowi nie tylko wyzwanie o charakterze politycznym, prawnym czy bezpieczeństwa granicznego, lecz także istotne zagrożenie dla zdrowia publicznego, wpisujące się w szerszy kontekst działań hybrydowych. Wymuszona migracja, realizowana w sposób nieregularny i trudny do kontrolowania, generuje ryzyka epidemiologiczne oraz systemowe, które oddziałują na zdolność państwa do zapewnienia ciągłości nadzoru sanitarno-epidemiologicznego, skutecznej diagnostyki oraz sprawnego reagowania kryzysowego. Zdrowie publiczne ujawnia się w tym ujęciu jako obszar podatności państwa, który może być pośrednio obciążany bez użycia klasycznych środków militarnych.

Analiza struktury migracji na polsko-białoruskim odcinku granicy państwowej oraz profilu epidemiologicznego państw pochodzenia migrantów wskazuje, że ryzyka zdrowotne nie wynikają z samego faktu migracji, lecz z jej wymuszonego charakteru, ograniczonego dostępu do opieki zdrowotnej oraz przerwanych procesów profilaktycznych i diagnostycznych. W warunkach takich presji szczególnego znaczenia nabiera zdolność państwa do szybkiej identyfikacji zagrożeń, integracji danych migracyjnych i zdrowotnych oraz elastycznego dostosowywania procedur reagowania. W perspektywie praktycznej wyniki badania wskazują na potrzebę trwałego włączenia komponentu zdrowia publicznego do systemu bezpieczeństwa wewnętrznego państwa oraz do analiz zagrożeń hybrydowych. Konieczne jest rozwijanie mechanizmów wczesnego ostrzegania zdrowotnego, wzmacnianie współpracy między służbami granicznymi, sanitarnymi i systemem ochrony zdrowia, a także budowanie zdolności do prowadzenia działań profilaktycznych i diagnostycznych w warunkach presji migracyjnej. Równie istotne pozostaje traktowanie zdrowia publicznego jako elementu odporności

państwa, wymagającego planowania strategicznego, a nie wyłącznie reakcji ad hoc.

Z perspektywy badawczej rozdział potwierdza zasadność łączenia analiz bezpieczeństwa z perspektywą zdrowia publicznego oraz wskazuje na potrzebę dalszych, pogłębionych badań nad systemowymi skutkami presji migracyjnej w warunkach zagrożeń hybrydowych. Uwzględnienie wymiaru zdrowotnego pozwala na pełniejsze zrozumienie współczesnych wyzwań bezpieczeństwa oraz na formułowanie bardziej adekwatnych i kompleksowych strategii reagowania państwa.

Literatura

1. Gil, G. (2021). Subwersja w polityce (nie)bezpieczeństwa w Europie Wschodniej: wybrane problemy. Wschód Europy. *Studia humanistyczno-społeczne, 7*(2), 29-44. https://doi.org/10.17951/we.2021.7.2.29-44
2. Górnik-Durose, M. (2011). Konteksty i pogranicza – inspiracje dla spychologii zdrowia. W: M. Górnik-Durose, J. Mateusiak (red.), *Psychologia zdrowia: konteksty i pogranicza* (s. 17-39). Wydawnictwo Uniwersytetu Śląskiego.
3. Hoffman, F. G. (2009). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum, 240*. 1-8.
4. Kawczyńska-Butrym, Z. (2011). Migrant w sytuacji choroby. *Zdrowie Publiczne i Zarządzanie, 2,* 113-118. https://doi.org/10.4467/20842627OZ.11.023.0560
5. Komisja Europejska. (2021). *Wniosek. Rozporządzenie w sprawie sytuacji instrumentalizacji w obszarze migracji i azylu*. Komisja Europejska, Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych.
6. Konieczny, M. (2022). Operacja „Śluza" – kryzys uchodźczy związany z przerzutem nielegalnych migrantów przez polsko-białoruską granicę. *Roczniki Administracji i Prawa, XX, 2,* 89-102. https://doi.org/10.5604/01.3001.0016.0948
7. Lonardo, L. (2021). EU Law Against Hybrid Threats: A First Assessment. *A Journal on Law and Integration, 6*(2)*,* 1075-1096. https://doi.org/10.15166/2499-8249/514
8. Miller, M., Zieliński, A. (2002). Zdrowie publiczne – misja i nauka. *Przegląd Epidemiologiczny, 56.* 547-557.

9. Nitszke, A. (2024). Instrumentalizacja migracji. Proceduralizacja versus humanizacja polityki azylowej Unii Europejskiej. *Politeja, 1*(88/1), 239-251. https://doi.org/10.12797/Politeja.20.2024.88.1.14
10. Nowicka, J., Wołyńska, A. (2022). Eskalacja kryzysu granicznego jako efekt działania białoruskiej dezinformacji. W: D. Dachowicz, L. Elak, Z. Ciekanowski (red.), *Zagrożenia wschodniej flanki NATO w aspekcie bezpieczeństwa wewnętrznego obszarów przygranicznych* (s.137-153). Wydawnictwo im. prof. Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie.
11. Oskierko, M. (2022). Kryzys migracyjny na polsko-białoruskiej granicy państwowej. W: D. Dachowicz, L. Elak, Z. Ciekanowski (red.), *Zagrożenia wschodniej flanki NATO w aspekcie bezpieczeństwa wewnętrznego obszarów przygranicznych* (201-220). Wydawnictwo im. prof. Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie.
12. Oskierko, M., Żurawski, S. (2025). Unia Europejska wobec kryzysu migracyjnego jako narzędzia wojny hybrydowej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 11*(1), 51-67. https://doi.org/10.34739/dsd.2025.01.03
13. Sowizdraniuk, J., Sowizdraniuk, P. (2019). Analiza wpływu migracji na zachorowalność na choroby zakaźne w Polsce. *Państwo i Społeczeństwo, 1,* 91-101. https://doi.org/10.34697/2451-0858-pis-2019-1-007
14. Szydłowski, J., Wilk, D., Wendt, J. A. (2018). Wpływ migracji na rozprzestrzenianie się chorób na przykładzie Niemiec. *Zeszyty Naukowe Politechniki Śląskiej 2018, Seria: Organizacja i Zarządzanie, 126,* 197-208.
15. Szymańczak, J. (2010). Zdrowie publiczne – element systemu ochrony zdrowia. W: G. Ciura (red.), *Zdrowie Polaków* (221-250). Wydawnictwo Sejmowe.
16. Uramowska-Żyto, B. (1980). *Medycyna jako wiedza i system działań*. Ossolineum.
17. Ustawa z dnia 29 października 2021 r. o budowie zabezpieczenia granicy państwowej (Dz. U. z 2021 r. poz. 1992).

18. Wawrzusiszyn, A. (2022). Kryzys migracyjny na granicy polsko-białoruskiej i jego wpływ na bezpieczeństwo Polski. *Nowa Polityka Wschodnia, 2*(33), 45-65. https://doi.org/10.15804/npw20223303
19. Wawrzusiszyn, A. (2025). Rosyjsko-białoruskie działania hybrydowe na granicach Unii Europejskiej i NATO. *Journal of Modern Science, 1*(61)*,* 10-32. https://doi.org/10.13166/jms/203108
20. WHO. (2024). *World health statistics 2024. Monitoring health for the SDGs, Sustainable Development Goals*. World Health Organization.
21. Włodarczyk, C. W. (2007). *Zdrowie publiczne w perspektywie międzynarodowej. Wybrane problemy*. Wydawnictwo Uniwersytetu Jagiellońskiego.
22. Wyrębek, H. (2023). Zagrożenia hybrydowe bezpieczeństwa informacyjnego państwa. *Polityka i Społeczeństwo, 1*(21), 315-330. https://doi.org/10.15584/polispol.2023.1.20
23. Wysocki, K. (2024). Wpływ zarządzania refleksyjnego na eskalację kryzysu migracyjnego na granicy Białorusi z Unią Europejską. *Cybersecurity and Cybercrime, 1*(3), 1-24.
24. Zygo, K. (2024). *Wybrane aspekty bezpieczeństwa zdrowotnego Polaków – ujęcie teoretyczno-empiryczne*. Wydawnictwa Naukowego Uniwersytetu w Siedlcach.

Oskar Stefański[1]
Uniwersytet Mikołaja Kopernika w Toruniu

https://doi.org/10.29316/9788368103373_13

CYBERZAGROŻENIA A PROCES TRANSFORMACJI ENERGETYCZNEJ. W JAKI SPOSÓB NOWE ZAGROŻENIA MOGĄ SPOWALNIAĆ PROCES TRANSFORMACJI ENERGETYCZNEJ PAŃSTWA NA PRZYKŁADZIE POLSKI?

CYBER THREATS AND THE ENERGY TRANSITION. HOW MIGHT NEW THREATS SLOW DOWN A COUNTRY'S ENERGY TRANSITION, TAKING POLAND AS AN EXAMPLE?

Streszczenie

Cyberzagrożenia i transformacja energetyczna to zagadnienia ze sobą powiązane. Ponieważ systemy energetyczne są coraz częściej uzależnione od cyfryzacji, wiąże się to zarówno z korzyściami, jak i z zagrożeniami. Korzyściami mogą być szybsze dostawy i większa automatyzacja. Z kolei zagrożenia to przykładowo potencjalne cyberzagrożenia takie jak cyberataki, a także wiele innych zjawisk, którymi mogą być wyłudzenia danych i oszustwa finansowe. W Polsce od wielu lat zachodzą zarówno

[1] https://orcid.org/0009-0005-5419-0342, e-mail: oskar.stefanski@doktorant.umk.pl

proces cyfryzacji, jak i transformacji energetycznej. Celem pracy jest zbadanie tego, w jaki sposób cyberzagrożenia mogą negatywnie wpływać na transformację energetyczną państwa na przykładzie Polski. W Polsce od 2014 roku liczba zgłoszonych cyberzagrożeń w sektorze energetycznym stale rośnie w liczbach bezwzględnych, a sektor energetyczny jest wśród pięciu najczęściej obsługiwanych sektorów przez zespół CERT Polska. Najpoważniejszymi incydentami, które dotyczą polskiej transformacji energetycznej, są różne cyberataki. Najczęściej doprowadzają one do wykradzenia danych poufnych od firm energetycznych i instytucji zajmujących się energetyką. Są także inne skutki takich działań, jak utrata częściowej kontroli nad elektrowniami i stronami internetowymi firm energetycznych. Bezpośrednio powoduje to mniejszy dostęp społeczeństwa do energii elektrycznej, a także zmniejsza zaufanie Polaków do firm energetycznych. W trakcie badania przedstawione zostały w formie tabel i opisów incydenty w liczbie nominalnej, a także w formie opisowej najpoważniejsze przypadki cyberzagrożeń dotykających polskiej transformacji energetycznej i całego sektora energetycznego.

Słowa kluczowe: transformacja energetyczna, cyberzagrożenia, Polska, cyberataki, CERT Polska

Abstract

Cyber threats and the energy transition are intertwined. Since energy systems are increasingly dependent on digitalisation, this brings both numerous negative and positive consequences. Benefits include faster deliveries and greater automation. Threats include potential cyberattacks and other cyber threats, such as data theft and financial fraud. Poland has been undergoing both digitalisation and energy transition for many years. This study examines how cyber threats can negatively impact the country's energy transition, using Poland as an example. In Poland, the number of reported cyberthreats in the energy sector has been steadily increasing in absolute numbers since 2014, and the energy sector is among the five most frequently serviced sectors by CERT Polska. The most serious incidents affecting the Polish energy transition are various cyberattacks. These incidents most often result in the theft of confidential data from energy companies and institutions involved in the energy sector. Other consequences include the loss of partial control over power plants and energy company websites. This directly reduces public access to electricity and diminishes Poles' trust in energy companies. The study presented a nominal number of incidents in tables and descriptions, along with descriptive reports on the most serious cyber threats affecting the Polish energy transition and the entire energy sector.

Keywords: energy transition, cyber threats, Poland, cyberattacks, CERT Polska

Wstęp

Transformacja energetyczna to proces trwały, przez który przechodzą wszystkie państwa świata. Powszechnie transformację energetyczną określa się jako przejście z systemu energetycznego opartego na paliwach kopalnych, takich jak węgiel, ropa czy gaz ziemny, do systemu opartego na odnawialnych źródłach energii, takich jak bioenergetyka, energetyka słoneczna, wiatrowa, wodna czy wykorzystywanie wodoru (Harichandan i in., 2022). Z tego względu, że paliwa kopalne są potencjalnie skończonym źródłem energii, prędzej czy później na skutek wyczerpania zasobów, wszystkie państwa i jednostki będą zmuszone do przeprowadzenia transformacji energetycznej. Jednakże surowce te mogą być wykorzystywane w procesie przejściowym. Celem transformacji jest neutralność klimatyczna, a od tych surowców należy odchodzić stopniowo, uwzględniając potrzeby swojego społeczeństwa i systemu energetycznego. Ważna jest także perspektywa wykorzystywania nowych technologii mogących sprawiać, że konwencjonalne źródła energii staną się „czystsze". Z tego względu poszczególne typy energetyki konwencjonalnej mogą być wykorzystywane w fazie przejściowej (Pepłowska, 2025).

Kluczowe w badaniach nad transformacją energetyczną jest stwierdzenie tego, jaki obszar terytorialno-prawny ona dotyka. W literaturze przedmiotu wyznacza się dwa główne typy transformacji energetycznej. Są to transformacja energetyczna w ujęciu państwowym i transformacja energetyczna w ujęciu lokalnym (Solomon, Krishna, 2011). Transformacja w ujęciu lokalnym dotyczy, jak nazwa wskazuje, terytorium mniejszego niż państwo. Niezależnie od tego, czy to jednostka administracyjna, czy chociażby firma. Z tego względu istotne jest zaznaczenie, że badanie dotyczy transformacji energetycznej państwa, a w tym przykładzie Rzeczpospolitej Polskiej. Istotne dla tematu są też pojęcia takie jak zielona transformacja energetyczna czy czysta transformacja energetyczna ze względu na ich powszechne występowanie w literaturze. Są to procesy bliźniacze transformacji energetycznej i nie różnią się od niej (Carley, Konisky, 2020; Muhire i in., 2024).

Istotna z perspektywy badania nad transformacją energetyczną jest kwestia udziału energetyki jądrowej w transformacji energetycznej. Jest to kwestia indywidualna dla poszczególnych państw, niektóre, takie jak Niemcy, wykluczają udział energetyki jądrowej w ich miksie energetycznym

(Kędzierski, 2024). Z kolei inne, takie jak Szwecja, zakładają ważną rolę energetyki jądrowej w transformacji energetycznej (Regeringen, 2024). Ważne jest to, że w doktrynie uznaje się często istotną rolę energetyki jądrowej w transformacji energetycznej niezależnie od państwa (Blecking, 2023; Wang, Guo, Li, Jiang, 2023; Muhire i in., 2024). Przez to należy uznać, że wśród źródeł energii wykorzystywanych w ramach transformacji energetycznej, jednym z docelowych jest energetyka jądrowa. Polski proces transformacji energetycznej opiera się głównie na przejściu z energetyki opartej na węgiel i w mniejszym stopniu na inne paliwa kopalne na system energetyczny oparty na czyste źródła energii. W wciąż obowiązującym dokumencie „Polityka energetyczna Polski do 2040 roku" z 2021 roku i aktualizowanym w 2022 roku po rosyjskiej agresji na Ukrainę zakłada się, że polska energetyka opierać się będzie docelowo na miksie energetyki odnawialnej z energetyką jądrową. Głównym celem polskiej transformacji energetycznej jest neutralność klimatyczna, czyli emitowanie równej bądź mniejszej ilości gazów cieplarnianych niż ich wchłanianie. Co ważne, system energetyki Polski ma opierać się w dużym stopniu na cyfryzacji (Ministerstwo Klimatu i Środowiska, 2021).

Pojęciami kluczowymi dla transformacji energetycznej są czynniki napędzające (ang. drivers) i spowalniające (nazywane często barierami). Kluczowe dla badania będą bariery, czyli czynniki spowalniające transformację energetyczną. Bariery hamują proces transformacji energetycznej, a aby go przyspieszyć i usprawnić, należy pokonać barierę (Pereira, Silva, Ferreira, 2025). Bariery są powiązane z czynnikami napędzającymi; brak takowego czynnika może stanowić barierę (Muhire i in., 2024). Przez to istnieją między nimi wysokie zależności, często również bariery i czynniki napędzające się wykluczają. W literaturze przyjmuje się, że czynniki i bariery mają charakter polityczno-prawny, ekonomiczny, społeczny, środowiskowy i technologiczny (Muhire i in., 2024; Aparisi-Cerdá, Ribó-Pérez, García-Melón, D'Este, Poveda-Bautista, 2024). Ze względu na wyznaczenie takich kategorii łatwiej określać, co i w jaki sposób napędza bądź spowalnia transformację energetyczną. Dzięki temu łatwiej jest dokonać określenia sukcesów i problemów tego procesu w danym miejscu.

Nowe technologie niosą transformacji energetycznej wiele szans, takich jak wytwarzanie energii w sposób czystszy, tańszy i efektywniejszy,

ale także stwarzają potencjalne zagrożenia i bariery. Ze względu na aspekt technologiczny cyberbezpieczeństwo jest kluczowe dla transformacji energetycznej. Przez to zagadnienia związane z cyberbezpieczeństwem stanowią fundament do tego, aby w procesie transformacji energetycznej nie zaistniały bariery, które będą hamować ten proces. Zdaniem publicystów Światowego Forum Ekonomicznego cyberzagrożenia będą coraz istotniejszym problemem dla infrastruktury energetycznej, w tym dla całego procesu transformacji energetycznej. Cyberodporność powinna zatem stać się jednym z fundamentów (Ukyab, Simonovich, 2025). Cyberzagrożenia spowalniają proces transformacji energetycznej, stąd mogą być nazwane barierami, co powinno ułatwić badanie danego zjawiska.

Badania nad powiązaniem cyberzagrożeń z barierami i wyzwaniami w transformacji energetycznej są powszechne w dyskursie naukowym zajmującym się transformacją energetyczną. Spośród przykładowych pozycji można wymienić publikację badaczy z World Energy Council „Cyber challenges to the energy transition", którzy uznali, że cyberzagrożenia są jednymi z najmniej spodziewanych zagrożeń, a także jednymi z bardziej istotnych dla sektora energetycznego państwa. Uwzględniają w tym rolę cyberbezpieczeństwa w bezpieczeństwie energetycznym państwa i przeprowadzaniu transformacji energetycznej. Uznają także, że cyberzagrożenia są istotne w spowalnianiu transformacji energetycznej. Dodatkowo wymieniają różne incydenty związane z cyberzagrożeniami, które wpłynęły negatywnie na transformację energetyczną. Spośród nich wymieniają przykładowo cyberataki na elektrownie jądrowe i wodne w Korei Południowej z 2015 roku, cyberataki w Unii Europejskiej na infrastrukturę energetyczną z 2015 roku, a także zaburzenia w sieci połączeń energetycznych w ramach cyfryzowanego systemu energetycznego w Urugwaju i Argentynie w 2019 roku (Nottingham, Young, 2019).

W Korei Południowej atak ten doprowadził do zakłócenia dostaw energii i usług opartych na energii elektrycznej. W Unii Europejskiej hakerzy dostali się do zabezpieczeń poszczególnych elektrowni i mogli w każdym momencie wyłączyć elektrownie i przerwać dostęp energii w wybranych państwach. Z kolei w Urugwaju i Argentynie awaria sprawiła, że przestały jeździć pociągi i metro, a także zabrakło w niektórych miejscach dostępu do wody. Przedstawione cyberzagrożenia miały miejsce od 2014 roku, gdyż

od tego roku na świecie cyberzagrożenia dotykają coraz częściej procesu transformacji energetycznej. Celowo wybrane zostały różne skutki cyberzagrożeń, w tym cyberataków, aby pokazać mnogość skutków, które wystąpiły w tych państwach (Nottingham, Young, 2019).

Zdaniem Raphaela Röttingera postępująca cyfryzacja i transformacja energetyczna są ze sobą powiązane, przez co cyfryzacja niesie ze sobą wiele potencjalnych zagrożeń, w tym przede wszystkim cyberataki na infrastrukturę energetyczną. Pomimo postępującej cyfryzacji i automatyzacji systemów energetycznych w ramach transformacji, wciąż będzie wysoka zależność od czynnika ludzkiego, co sprawia, że potencjalne błędy i cyberzagrożenia ze strony hakerów będą tak samo bądź bardziej dotkliwe (Röttinger, 2024). Inni badacze są również podobnego zdania, że postępująca cyfryzacja niesie ze sobą coraz większe zagrożenia dla transformacji energetycznej i ma potencjał spowalniający, w momencie, gdy transformacja energetyczna napotka cyberzagrożenia (np. Awad, Bayoumi, 2025; Abraham, Houmd, Erdodi, 2025; Deryugina, 2023).

Z tego względu powiązanie tematyki cyberzagrożeń z transformacją energetyczną jest bardzo kluczowe, w szczególności w obliczu konfliktu cybernetycznego Polski z Rosją i Białorusią. Istotne jest zbadanie tego, jak cyberzagrożenia mogą oddziaływać na transformację energetyczną Polski na podstawie dotychczasowych doświadczeń.

Metodologia

Z uwagi na wciąż wzrastające ryzyko wystąpienia cyberzagrożeń, które mogą razić system energetyczny Polski, istotne jest zweryfikowanie tego, w jaki sposób mogą one wpływać na spowalnianie procesu transformacji energetycznej. Badanie opierać się będzie na dotychczasowych przykładach takich działań i różnych incydentach z tym związanych, które miały miejsce na terenie Polski o dotyczyły szeroko pojętego systemu energetycznego. Dlatego postawiony został cel badawczy, który dotyczy zbadania tego, w jaki sposób cyberzagrożenia mogą negatywnie wpływać na transformację energetyczną państwa na przykładzie Polski. Z tego względu postawiony zostanie problem badawczy P: W jaki sposób cyberzagrożenia mogą negatywnie wpływać na proces transformacji energetycznej państwa na przykładzie takich działań wobec Polski? Z racji dotychczasowych doświadczeń na

podstawie państw, które zostały dotknięte przez cyberzagrożenia, takich jak Stany Zjednoczone, Korea Południowa, Argentyna i Urugwaj, można postawić hipotezę badawczą odpowiadającą na postawiony problem. H: Cyberzagrożenia mogą być czynnikiem spowalniającym (barierą) transformację energetyczną państwa poprzez zakłócenie dostaw energii, kontrolowanie elektrowni przez hakerów, doprowadzenie do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Hipoteza zostanie zweryfikowana pozytywnie, częściowo pozytywnie bądź całkowicie negatywnie w ramach wniosków końcowych badania.

Kluczowe są też podstawowe założenia badawcze przyjęte w ramach badania, które dotyczą podstawowych pojęć wykorzystywanych w pracy. Jednym z nich jest transformacja energetyczna. Zgodnie z przedstawionym teoretycznym podejściem do zagadnienia transformacji energetycznej państwa w ramach wstępu, na potrzeby badania przyjęte zostanie, że jest to przejście z systemu energetycznego opartego na paliwach kopalnych na czyste źródła energii takie jak OZE, atom czy wodór. Jednakże istotny jest cały proces transformacji energetycznej, hipotetyczne zagrożenia względem chociażby elektrowni węglowych mogą spowalniać odchodzenie od ich eksploatacji. Może to mieć miejsce chociażby poprzez potrzebę reinwestycji w to źródło energii ze względu na brak alternatyw, a także przez inne powody. W Polsce przez znaczne uzależnienie od elektrowni węglowych i innych źródeł konwencjonalnych należy uwzględnić ich rolę przejściową. Zgodnie z tym polem badawczym jest cała transformacja energetyczna Polski, w tym zarówno konwencjonalne źródła energii jako źródła przejściowe, jak i niekonwencjonalne źródła energii jako źródła docelowe. Stąd istotne będzie także dalsze sprecyzowanie pola badawczego, konkretnie w zakresie stwierdzeń takich jak cyberprzestrzeń i cyberzagrożenia.

Kwestia definicyjna cyberprzestrzeni jest prosta przez to, że w Polsce jest regulowana np. w ustawie o stanie wyjątkowym. Według tejże ustawy cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami" (Ustawa z 21.06.2002 r. o stanie

wyjątkowym Dz. U. z 2017 r. poz. 1928, s. 2). Natomiast cyberzagrożenia to zagrożenia, które występują w cyberprzestrzeni. Co za tym idzie, przyjętym polem badawczym jest cyberprzestrzeń dotycząca występujących w niej cyberzagrożeń, które oddziałują na transformację energetyczną w Polsce. Stąd przedmiotem badań są cyberzagrożenia wpływające na polską transformację energetyczną i dotykające czystych źródeł energii. Strona internetowa rządu Rzeczypospolitej Polskiej wymienia przykładowe cyberzagrożenia: wirusy, robaki, spyware i wiele innych (Gov.pl, b.d.).

Podstawową metodą badawczą jest studium przypadku, jakim jest transformacja energetyczna Polski. Kluczowe w badaniu będą także cyberzagrożenia w relacji z transformacją energetyczną. Ponadto zastosowana zostanie krytyczna analiza źródeł, w tym przypadku analiza źródeł pierwotnych i wtórnych. Będą nimi źródła będą głównie dokumenty NASK (w tym szczególnie CERT Polska, dalej nazywane CERT) i dokumenty prasowe informujące o danych cyberzagrożeniach dotykających transformacji energetycznej w Polsce. Przypadki zostaną przedstawione również w formie tabeli prezentującej dane cyberzagrożenia.

Przyjętym okresem badawczym będą lata 2014-2025 ze względu na to, że od 2014 roku na świecie występuje coraz więcej cyberzagrożeń dotykających procesu transformacji energetycznej, a także wzmożoną aktywność Rosjan w cyberprzestrzeni powodującą cyberzagrożenia w Europie. Stąd jest to o tyle istotny okres, że obejmuje także czas po inwazji rosyjskiej na Ukrainę z 22 lutego 2022 roku.

Cyberzagrożenia w transformacji energetycznej Polski

Pierwszym przypadkiem cyberzagrożeń, w postaci cyberataku, który należy wymienić, jest działalność Dragonfly/Energetic Bear, która na szeroką skalę rozpoczęła się w 2014 roku i trwa do dzisiaj. Grupa Dragonfly zaatakowała wiele państw Zachodu, w tym Polskę, celując głównie w infrastrukturę energetyczną bez szczególnego różnicowania, jaki to jest typ energetyki. Grupa wysyłała zainfekowane maile na konta Gmail z załącznikiem w formacie pdf, a także zmieniała strony internetowe firm energetycznych, które następnie przekierowywały użytkowników na inne strony. Innym sposobem było użycie pakietów oprogramowania ICS. Przez to hakerzy infekowali strony internetowe firm energetycznych tzw. trojanem, a system nie

wykrywał niebezpieczeństwa związanego z potencjalnym oprogramowaniem szkodliwym dla użytkowników. Dzięki temu wykradali dane od użytkowników, a także firm i poufne informacje takie jak hasła. Hakerzy próbowali dostać się do systemu zabezpieczeń firm energetycznych, a także całej infrastruktury energetycznej. Prawdopodobnie głównym celem grupy było zdobycie informacji na temat badań geologicznych i geograficznych, planów eksploatacji złóż i planów inwestycji firm energetycznych. Dotknięty został zarówno sektor energetyki konwencjonalnej, jak i niekonwencjonalnej. Doniesienia prasowe informowały wówczas, że atak mógł być inspirowany z Rosji. Głównym skutkiem tych ataków był wyciek danych dotyczących polityki energetycznej wybranych firm. Co najistotniejsze, był to atak szpiegowski, a nie sabotażowy, jednakże sprawił, że hakerzy dostali się do ściśle tajnych danych dotyczących polskiego sektora energetycznego (Rzeczpospolita, 2014; CERT, 2015; Malko, Wojciechowski, 2015).

W 2014 roku upubliczniono także do informacji publicznej raport z ataku grupy SandWorm na sieć energetyczną w Polsce. Co istotne, główna część ataku grupy dotyczyła w większości Ukrainy, lecz także częściowo Polski, a w znacznie mniejszym stopniu innych państw NATO. Natomiast, co kluczowe, cały atak polegał na zainfekowaniu systemów energetycznych i systemów firm energetycznych w obu krajach oprogramowaniem BlackEnergy. Ataki były bardzo precyzyjne, gdyż wysyłano specjalnie tworzone zainfekowane pliki pakietu Microsoft Office i wysyłano je pracownikom przedsiębiorstw i sektora publicznego. Następnie dzięki temu skradziono dane poufne na masową skalę. Otwarcie pliku sprawiało, że był on potem pobierany i dalej instalowany na komputerze, a następnie w sposób zdalny pobierał i przesyłał poufne dane hakerom. Zdaniem CERT udało się zidentyfikować 28 unikalnych adresów IP w Polsce, które w większości dotknęły sektora energetycznego, zarówno w sferze prywatnej, jak i publicznej. Podobnie jak w przypadku działalności Dragonfly nie różnicowano sektora na ten zajmujący się energetyką konwencjonalną i niekonwencjonalną, tylko atakowano cały sektor energetyczny zasilający infrastrukturę krytyczną. Jest to także kolejny przypadek, który prawdopodobnie wiąże się z działalnością Rosji w cyberprzestrzeni (CERT, 2015). Dodatkowo należy zaznaczyć, że ta sama grupa i to samo oprogramowanie doprowadziły w grudniu 2015 roku do blackoutu na Ukrainie (CERT, 2016; Gapiński, 2016).

Kolejne większe opisywane incydenty miały miejsce po 2022 roku. W czerwcu 2022 roku Elbląskie Przedsiębiorstwo Energetyki Cieplnej (EPEC) zgłosiło, że stało się ofiarą cyberataku. Sieć informatyczna firmy została zainfekowana groźnym Ramsonware Ragnar Locker. Zainfekowanie sieci szkodliwym oprogramowaniem sprawiło, że wyciekło aż 8 GB danych osobowych klientów i pracowników firmy, w tym takich danych jak numery PESEL. Hakerzy dostali się także do danych wewnętrznych finansowych firmy. Twórcy złośliwego oprogramowania upublikowali nawet dane, które zostały przez nich skradzione. Celem hakerów była właśnie kradzież danych osobowych i finansowych firmy, a nie atak bezpośredni na systemy energetyczne. Nie zmienia to faktu, że jest to incydent poważny, przez który firma zajmująca się energetyką ciepłowniczą, kluczową w procesie transformacji energetycznej, straciła zaufanie i nie była w stanie kontrolować swoje serwery. Co warto odnotować, to incydent jedynie o charakterze lokalnym, a nie ogólnokrajowym bądź regionalnym (EPEC, 2022; Stankiewicz, 2022; Nowosad, 2022; Szczęsny, 2022).

Następnym poważnym incydentem jest proceder związany z fałszywymi sklepami z węglem, który był bezpośrednim skutkiem zaprzestania handlu surowcami energetycznymi z Rosją. Braki w dostawach węgla, na skutek rosyjskiej agresji na Ukrainę z 2022 roku sprawiły, że polskie społeczeństwo uzależnione od ogrzewania węglowego było zmuszone szukać surowca w innych miejscach niż dotychczas. CERT zwraca uwagę na to, że dotyczyło to wszelkiej maści cyberzagrożeń, nie tylko cyberataków, jak w poprzednich przypadkach. W tym czasie, gdy na polskim rynku brakowało węgla, dochodziło do licznych prób wykradania haseł przez zhackowane linki do fałszywego zakupu, a także wyłudzano dane osobowe osób kupujących. Fałszywe sklepy, często podające się za rzeczywiste (przypadek sklepu podszywającego się pod Polską Grupę Górniczą), oferowały możliwość kupna jedynie poprzez przelewy, co już budziło podejrzenia. CERT przedstawia, że w grudniu 2022 roku działało aż 12 takich fałszywych sklepów internetowych, które oszukiwały swoich nabywców (CERT, 2023). Co istotne, proceder ten powrócił w 2023 i 2024 roku wraz z rozpoczęciem sezonu grzewczego w październiku 2023 i 2024 roku (CERT, 2024; CERT, 2025). Jest to o tyle istotne, że ludzie często tracili swoje fundusze przez wywindowane ceny surowców, a także przez fałszywe oferty sprzedaży węgla. Ostatecznie

doprowadziło to do licznych nadużyć i strat finansowych gospodarstw, które mogłyby utracone fundusze wydać na wymianę pieca w swoim domu i eksploatację czystej energii bądź usprawienie działania swojego pieca.

W 2023 roku doszło do cyberataków powiązanych z grupą ATP28, które dotknęły sektory energetyczne wielu państw, w tym Polski. Grupa wykorzystywała błędy w Microsoft Outlook i przez to była w stanie dostać się do danych osobowych użytkowników. Ponadto wykradała w ten sposób hasła do zabezpieczeń. Hakerzy wykradli w ten sposób hasła pracowników sektora transportu, sektora zbrojeniowego, a także, co najważniejsze, pracowników sektora energetycznego (CERT, 2024).

Ostatni warty odnotowania incydent miał miejsce w lipcu i sierpniu 2025 roku. Rosyjscy hakerzy wówczas zaatakowali Polską elektrownię wodną i wodociąg, a także próbowali nieudanie zaatakować bioreaktor. W przypadku bioreaktora manipulowano temperaturami pomieszczeń niektórych budynków w Nowym Mieście Lubawskim. W przypadku elektrowni wodnej także manipulowano temperaturami. W lipcu Rosjanie nie byli w stanie całkowicie przejąć kontroli nad hydroelektrownią, jednakże w sierpniu udało im się dostać do systemu zabezpieczeń. Zmieniono wówczas parametry temperatur, a także ilość wody w elektrowni. Sprawiło to, że Rosjanie byli w stanie częściowo kontrolować elektrownię wodną (Klimczuk, 2025a; Klimczuk, 2025b).

Poza wymienionymi dużymi incydentami, do CERT zgłaszane były też mniejsze incydenty. Od 2018 CERT udostępnia liczbę incydentów obłużonych przez CERT w danych sektorach gospodarki państwa, a także ich procentowy udział względem innych sektorów. Incydenty to zgłoszenia do CERT różnej maści cyberzagrożeń, w tym chociażby cyberataków czy manipulacji (Tabela 1).

Tabela 1. Incydenty związane z cyberzagrożeniami w sektorze energetycznym w Polsce w latach 2018-2024 obsłużone przez CERT

Rok	Łączna ilość incydentów	Incydenty w sektorze Energetyki	Procent względem ogółu incydentów
2018	3739	20	0,53%
2019	6484	28	0,40%
2020	10420	101	0,97%
2021	29483	4084	13,85%

Rok	Łączna ilość incydentów	Incydenty w sektorze Energetyki	Procent względem ogółu incydentów
2022	39683	4320	10,89%
2023	80278	9196	11,46%
2024	103449	5216	4,50%

Źródło: opracowanie własne na podstawie raportów CERT, 2019-2025.

Ilość ogółu incydentów związanych z cyberzagrożeniami w Polsce rośnie w znacznym tempie. Istotne jest to, że ich liczba w sektorze energetycznym także do 2023 roku była w trendzie wzrostowym. Przed 2021 rokiem ich liczba stanowiła łącznie mniej niż jeden procent ogółu incydentów. Znaczny wzrost incydentów w sektorze energetycznym nastąpił w 2021 roku, gdyż w ujęciu nominalnym był on prawie czterdziestokrotny. W ujęciu procentowym wzrost z mniej niż 1% do prawie 14% względem ogółu incydentów jest także bardzo zauważalny. Do 2023 roku liczba incydentów w sektorze osiągnęła swoje maksimum nominalne wynoszące 9196 incydentów, aczkolwiek w ujęciu procentowym do ogółu wynosiła 11,46%. W 2024 roku nastąpił spadek liczby incydentów w sektorze energetycznym w ujęciu zarówno nominalnym, jak i procentowym, przy jednoczesnym wzroście ogólnej liczby incydentów związanych z cyberzagrożeniami. Pomimo takiego spadku wciąż sektor energetyczny znajdował się wówczas wśród pięciu sektorów, które są dotykane najwięcej incydentów o tym charakterze, i jest to niezmienne od 2021 roku (CERT, 2025).

Wnioski

Cyberzagrożenia dotykające sektora energetyki i transformację energetyczną w Polsce od 2021 roku są wśród pięciu (względem innych branż gospodarki) najczęściej raportowanych cyberzagrożeń, a ich liczba nominalnie stale rośnie. Spośród najważniejszych od 2014 roku przypadków cyberzagrożeń dotykających sektora energetycznego i polskiej transformacji energetycznej, zdecydowana większość to cyberataki (Tabela 2). Doniesienia prasowe uznają, że znaczna część z nich była powiązana z Rosją. Cyberataki miały głównie na celu kradzież danych osobowych i danych finansowych atakowanych jednostek, a także zaburzenie działalności firm i elektrowni, które były wówczas atakowane przez hakerów. Istotny jest także długotrwały incydent związany z fałszywymi sklepami z węglem. Doprowadził on

wiele gospodarstw domowych do utraty funduszy na rzecz fałszywych ofert sprzedaży węgla. Do 2025 roku incydenty nie dotykały bezpośrednio poszczególnych elektrowni, a jedynie firm energetycznych bądź konsumentów. Jednakże proceder z 2025, w którym, zdaniem prasy, Rosjanie kontrolowali jedną z polskich elektrowni wodnych, wydaje się najistotniejszy. Sprawia on, że w przyszłości przez braki w zabezpieczeniach i wzmożoną aktywność hakerów łatwiej będzie im przejmować kontrolę nad działalnością poszczególnych elektrowni bądź reaktorów. Istotne jest to, że taki proceder potencjalnie może doprowadzić nawet do blackoutu na mniejszą bądź większą skalę, co pokazuje przypadek Ukrainy w momencie, w którym państwo nie kontroluje swojej jednostki odpowiadającej za produkcję energetyczną.

Tabela 2. Główne incydenty w transformacji energetycznej związane z cyberzagrożeniami od 2014 roku

Incydent	Typ cyberzagrożenia	Rok/lata trwania
Ataki Dragonfly/Energetic Bear	Cyberatak	2014
Ataki Sandworm	Cyberatak	2014
Atak na EPEC	Cyberatak	2022
Fałszywe sklepy z węglem	Phishing	2022-2024
Atak ATP28	Cyberatak	2023
Atak na elektrownię wodną	Cyberatak	2025

Źródło: opracowanie własne na podstawie incydentów opisanych w badaniu.

Odpowiadając na problem badawczy P: W jaki sposób cyberzagrożenia mogą negatywnie wpływać na proces transformacji energetycznej państwa na przykładzie takich działań wobec Polski? Należy stwierdzić, że mogą to robić poprzez zmniejszanie zaufania społecznego wobec firm na podstawie dotychczasowych ataków hakerskich a także fałszywych aukcji związanych ze sprzedażą węgla. Potencjalnie mogą także doprowadzać do manipulacji na rynku, wykradać dane osobowe, a także manipulować elektrowniami i przyjmować nad nimi chociażby część kontroli, mając możliwość także wyłączenia elektrowni bądź reaktora. Dodatkowo takie zagrożenia mogą doprowadzić do tego, że potencjalne plany firm energetycznych zostaną ukradzione przez hakerów, co także może spowolnić proces transformacji energetycznej na podstawie wydarzeń z 2014 roku. Weryfikując hipotezę

badawczą H: Cyberzagrożenia mogą być czynnikiem spowalniającym (barierą) transformację energetyczną państwa poprzez zakłócenie dostaw energii, kontrolowanie elektrowni przez hakerów, co może doprowadzić do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Należy stwierdzić, że w Polsce zakłócenia dostaw energii mogą mieć rzeczywiste miejsce; kontrolowanie elektrowni przez hakerów również na podstawie incydentu z 2025 roku. Jednakże incydenty w Polsce nie doprowadziły do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Hipotezę należy zatem zweryfikować częściowo pozytywnie. Co warto także dodać: cyberzagrożenia mogą spowalniać transformację także przez zmniejszanie zaufania społecznego państwa, wyłudzenia finansowe i wykradanie danych inwestycyjnych firm zajmujących się energetyką i transformacją energetyczną. Kluczowe jest także to, że liczba groźnych i poważnych ataków stale rośnie, a incydent z 2025 roku pokazał, że istnieje ryzyko bezpośredniego ataku na elektrownie.

Literatura

1. Abraham, D., Houmb, S. H., Erdodi, L. (2025). Cyber-Attacks on Energy Infrastructure-A Literature Overview and Perspectives on the Current Situation. *Applied Sciences*, *15*(17), 1-19. https://doi.org/10.3390/app15179233
2. Aparisi-Cerdá, I., Ribó-Pérez, D., García-Melón, M., D'Este, P., Poveda-Bautista, R. (2024). Drivers and barriers to the adoption of decentralised renewable energy technologies: A multi-criteria decision analysis. *Energy*, *305*, 1-13. https://doi.org/10.1016/j.energy.2024.132264
3. Awad, H., Bayoumi, E. H. E. (2025). Next-Generation Smart Inverters: Bridging AI, Cybersecurity, and Policy Gaps for Sustainable Energy Transition. *Technologies*, *13*(4), 1-31.
4. Blecking J. (2023). The Nuclear Option: Green Energy Goals in the European Energy Transition, *Wisconsin International Law Journal*, *41*(1), 1-32. https://doi.org/10.3390/technologies13040136
5. Carley, S., Konisky, D. M. (2020). The justice and equity implications of the clean energy transition. *Nature Energy*, *5*, 569-577. https://doi.org/10.1038/s41560-020-0641-6

6. CERT. (2015). *CERT Polska Raport 2014*. Warszawa: NASK.
7. CERT. (2016). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2015*. Warszawa: NASK.
8. CERT. (2017). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2016*. Warszawa: NASK.
9. CERT. (2018). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2017*. Warszawa: NASK.
10. CERT. (2019). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2018*. Warszawa: NASK.
11. CERT. (2020). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2019*. Warszawa: NASK.
12. CERT. (2021). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2020*. Warszawa: NASK.
13. CERT. (2022). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2021*. Warszawa: NASK.
14. CERT. (2023). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2022*. Warszawa: NASK.
15. CERT. (2024). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2023*. Warszawa: NASK.
16. CERT. (2025). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2025*. Warszawa: NASK.
17. Derugina, T. (2023). *The green transition, energy security and energy independence*. W: Ch. Gollier, D. Rohner (red.), *Peace not Pollution-How Going Green Can Tackle Both Climate Change and Toxic Politics* (185-191). Paryż: CEPR.
18. Duszczyk, M. (2014). *Cyberatak na polskie firmy energetyczne*. Pobrane z: https://energia.rp.pl/energetyka/art4985261-cyberatak-na-polskie-firmy-energetyczne? (dostęp: 12.02.2026).
19. Elbląskie Przedsiębiorstwo Energetyki Cieplnej. (2022). *Cyberatak: EPEC powiadamia UODO*. Pobrane z: https://epec.pl/aktualnosci/cyberatak-na-epec-spolka-powiadamia-urzad-ochrony-danych-osobowych (dostęp: 12.02.2026).
20. Gapiński, K. (2016). *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*. Pobrane z: https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym (dostęp: 12.02.2026).

21. Gov.pl (b.d.). *Rodzaje cyberzagrożeń – zagrożenia techniczne*. Pobrane z: https://www.gov.pl/web/baza-wiedzy/zagr-techniczne (dostęp: 12.02.2026).
22. Harichandan, S. i in. (2022). Energy transition research: A bibliometric mapping of current findings and direction for future research. *Cleaner Production Letters*, 3(100026), 1-17. https://doi.org/10.1016/j.clpl.2022.100026
23. Kędzierski, M., (2024). *Klucz do przyszłości Energiewende: wsparcie budowy nowych elektrowni*. Pobrane z: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-02-12/klucz-do-przyszlosci-energiewende-wsparcie-budowy-nowych (dostęp: 12.02.2026).
24. Klimczuk, O. (2025a). R*osjanie zaatakowali polską elektrownię i wodociąg*. Pobrane z: https://cyberdefence24.pl/cyberbezpieczenstwo/rosjanie-zaatakowali-polska-elektrownie-i-wodociag (dostęp: 12.02.2026).
25. Klimczuk, O. (2025b). *Polska elektrownia ponownie zaatakowana przez Rosję*. Pobrane z: https://cyberdefence24.pl/cyberbezpieczenstwo/polska-elektrownia-wodna-zaatakowana-po-raz-drugi (dostęp: 12.02.2026).
26. Malko, J. Wojciechowski, H. (2015). Sektor energetyczny i cyberbezpieczeństwo. *Nowa Energia*, *1*, 10-15.
27. Ministerstwo Klimatu i Środowiska. (2021). *Polityka Energetyczna Polski do 2040 r.* Warszawa: Ministerstwo Klimatu i Środowiska.
28. Muhire, F., Turyareeba, D., Adaramola, M. S., Nantongo, M., Atukunda, R., Olyanga, A. M. (2024). Drivers of green energy transition: A review. *Green Energy and Resources*, *2(4)*, 1-17. https://doi.org/10.1016/j.gerr.2024.100105
29. Nottingham, L., Young, M. (2019). *Cyber challenges to the energy transition*. Pobrane z: https://www.worldenergy.org/publications/entry/cyber-challenges-to-the-energy-transition (dostęp: 12.02.2026).
30. Nowosad, M. (2022). *Sieć ciepłownicza w Elblągu zaatakowana przez hakerów. Przepadła część danych klientów*. Pobrane z: https://radiogdansk.pl/wiadomosci/region/elblag/2022/06/30/siec-cieplownicza-w-elblagu-zaatakowana-przez-hakerow-przepadla-czesc-danych-klientow (dostęp: 12.02.2026).

31. Pepłowska, M. (2025). Climate neutrality in Poland: the role of the coal sector in achieving the 2050 goal. *Polityka Energetyczna – Energy Policy Journal*, *28*(1), 113-126. https://doi.org/ 10.33223/epj/202307
32. Pereira, S., Silva, C., Ferreira, L. M. (2025). Barriers to energy transition: Comparing developing with developed countries. *Energy for Sustainable Development*, *87*, 1-17. https://doi.org/10.1016/j.esd.2025.101753
33. Regeringen. (2024). *Energipolitikens långsiktiga inriktning*, Sztokholm: Rząd Królestwa Szwecji.
34. Röttinger, R. (2024). Cyberattacks on renewable energies: "how hackers are threatening the energy transition and which technologies can protect us". *European Journal of Engineering and Technology, 12*(1), 42-49.
35. Solomon, B., Krishna, D. (2011). The coming sustainable energy transition: History, strategies, and outlook. *Energy Policy*, *39*(11), 7422-7431. https://doi.org/10.1016/j.enpol.2011.09.009
36. Stankiewicz, M. (2014). *Cyberatak na Elbląskie Przedsiębiorstwo Energetyki Cieplnej*. Pobrane z: https://radioolsztyn.pl/cyberatak-na-elblaskie-przedsiebiorstwo-energetyki-cieplnej/01644460 (dostęp: 12.02.2026)
37. Szczęsny, J. (2022). *Koszmarny wyciek danych z polskiej instytucji. Kłamano odnośnie okoliczności*. Pobrane z: https://antyweb.pl/epec-atak-hakerski (dostęp: 12.02.2026).
38. Ukyab, K. T., Simonovich, L. (2025). *Powering cyber resilience in the energy sector*. Pobrane z: https://www.weforum.org/stories/2025/05/powering-cyber-resilience-energy-sector (dostęp: 12.02.2026).
39. Ustawa z 21.06.2002 r. o stanie wyjątkowym (Dz. U. z 2017 r. poz. 1928).
40. Wang, Q., Guo, J., Li, R., Jiang, X. (2023). Exploring the role of nuclear energy in the energy transition: A comparative perspective of the effects of coal, oil, natural gas, renewable energy, and nuclear power on economic growth and carbon emissions. *Environmental Research*, *221.* https://doi.org/10.1016/j.envres.2023.115290

Tomasz Grudniewski[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_14

BEZPIECZEŃSTWO ENERGETYCZNE PAŃSTWA W ERZE DECENTRALIZACJI DOSTAW

NATIONAL ENERGY SECURITY IN THE ERA OF DECENTRALISED SUPPLIES

Streszczenie

Bezpieczeństwo energetyczne państwa coraz silniej zależy od zdolności systemu elektroenergetycznego do integrowania rozproszonych źródeł energii (distributed energy resources – DER), elastyczności popytu oraz magazynów energii w warunkach rosnącej zmienności generacji i narastających ryzyk zakłóceniowych. Wirtualne elektrownie (Virtual Power Plants – VPP) stanowią warstwę agregacji i koordynacji wielu rozproszonych zasobów, umożliwiając ich udział w rynkach energii oraz świadczenie usług systemowych. W rozdziale przedstawiono ramy analityczne łączące wymiary bezpieczeństwa energetycznego (4A: availability, accessibility, affordability, acceptability) oraz odporność (resilience) z architekturą VPP i warstwami ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO). Zastosowano ustrukturyzowany przegląd literatury (2018-2026) oraz mapowanie funkcji VPP na mechanizmy wpływu na bezpieczeństwo energetyczne, uzupełnione perspektywą cyberbezpieczeństwa DER. Wynikiem jest (1) typologia mechanizmów

[1] https://doi.org/0000-0003-3394-8992 , e-mail: gisbourne2@gmail.com

wzmacniania bezpieczeństwa przez VPP, (2) propozycja zestawu wskaźników KPI oraz procesu oceny wkładu VPP w bezpieczeństwo energetyczne i (3) rekomendacje wdrożeniowe akcentujące interoperacyjność danych, koordynację DSO-TSO, pomiar i weryfikację (M&V) oraz podejście security-by-design. Wykazano, że VPP może wzmacniać adekwatność mocy, stabilność operacyjną i przystępność cenową, ale jednocześnie wprowadza zależności cyfrowe, które muszą być zarządzane jako element bezpieczeństwa dostaw.

Słowa kluczowe: bezpieczeństwo energetyczne, wirtualna elektrownia, agregacja DER, elastyczność, DERMS, ADMS, cyberodporność, zarządzanie popytem

Abstract

A country's energy security increasingly depends on its power system's ability to integrate distributed energy resources (DER), demand flexibility, and energy storage in the face of growing generation variability and increasing disruption risks. Virtual power plants (VPPs) provide a layer of aggregation and coordination for multiple distributed resources, enabling them to participate in energy markets and provide system services. The article author presents the dimensions of energy security (4A: availability, accessibility, affordability, acceptability) and resilience with the VPP architecture and ICT layers (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO). A structured literature review (2018-2026) and mapping of VPP functions to mechanisms influencing energy security, supplemented by a DER cybersecurity perspective, were used. The result is (1) a typology of mechanisms for strengthening security through VPPs, (2) a proposal for a set of KPIs and a process for assessing the contribution of VPPs to energy security, and (3) implementation recommendations emphasising data interoperability, DSO-TSO coordination, measurement and verification (M&V), and a security-by-design approach. It has been shown that VPPs can enhance capacity adequacy, operational stability, and affordability, but at the same time introduce digital dependencies that must be managed as part of security of supply.

Keywords: energy security, virtual power plant, DER aggregation, flexibility, DERMS, ADMS, cyber resilience, demand management

Wstęp

Bezpieczeństwo energetyczne jest pojęciem wielowymiarowym i silnie zależnym od kontekstu technologicznego, gospodarczego i instytucjonalnego. W literaturze często przywołuje się podejście „4A" – availability (dostępność), accessibility (dostęp), affordability (przystępność cenowa)

i acceptability (akceptowalność środowiskowo-społeczna) – jako podstawę budowy wskaźników i ram oceny (Siksnelyte-Butkiene i in., 2024). Współczesne ujęcia podkreślają jednak, że same „4A" nie domykają problemu, ponieważ rośnie znaczenie odporności (resilience), rozumianej jako zdolność systemu do absorpcji zakłóceń, adaptacji oraz odtworzenia funkcji krytycznych (Schmitz i in., 2025). Transformacja elektroenergetyki – wzrost udziału OZE, elektryfikacja transportu i ciepłownictwa, rozwój prosumeryzmu, magazynów i ładowania pojazdów elektrycznych – przenosi ciężar bezpieczeństwa z dużych, sterowalnych jednostek wytwórczych na zdolność systemu do elastycznego bilansowania i koordynacji zasobów rozproszonych. Wysoka zmienność generacji i popytu zwiększa wartość prognozowania, automatyzacji i zarządzania w czasie rzeczywistym, co oznacza, że bezpieczeństwo energetyczne państwa staje się w coraz większym stopniu „cyfrowe" (data-driven). Przeglądy dotyczące zastosowań AI i IoT w programach demand response wskazują, że cyfryzacja poprawia zdolność do predykcji i sterowania, ale równocześnie wymaga dojrzałego zarządzania jakością danych i cyberochrony (Algburi i in., 2025).

Wirtualna elektrownia (VPP) jest jednym z kluczowych rozwiązań organizacyjno-technicznych w tym krajobrazie. W sensie funkcjonalnym VPP agreguje heterogeniczne zasoby DER (generacja rozproszona, magazyny, pojazdy elektryczne, elastyczne obciążenia) i koordynuje je tak, aby zachowywały się jak jedna jednostka zdolna do: (a) sprzedaży energii (rynki day-ahead/intraday), (b) świadczenia usług bilansujących i rezerw, oraz (c) wsparcia pracy sieci (np. zarządzania ograniczeniami i redukcji curtailmentu OZE). Przeglądy pokazują jednocześnie szybkie dojrzewanie modeli VPP: rośnie zakres rynków, stopień automatyzacji, a także nacisk na wykonalność praktyczną, interoperacyjność i skalowalność (Esfahani i in., 2025; Roozbehani i in., 2022; Zare, Shafiyi, 2025). Jednocześnie VPP – jako platforma cyfrowa sterująca potencjalnie tysiącami urządzeń – zwiększa zależność systemu elektroenergetycznego od warstwy ICT oraz powiększa powierzchnię ataku. Koordynacja DER wymaga telemetrii, kanałów sterowania i integracji API w architekturze wielostronnej (agregator, operator, dostawcy technologii, właściciele urządzeń). Przeglądy cyberbezpieczeństwa DER podkreślają, że rosnąca skala i heterogeniczność urządzeń wprowadzają ryzyka fałszowania danych (false data injection), przejęć sterowania, a także

kaskadowych konsekwencji incydentów w systemie fizycznym (Chen i in., 2025; Hasan i in., 2022). W tym sensie VPP, choć wzmacnia elastyczność i odporność operacyjną, jednocześnie wymusza systemowe podejście do cyberodporności jako warunku bezpieczeństwa dostaw (Leszczyna, 2018).

Problem badawczy i cel

W literaturze VPP dominują dwa nurty: (1) modelowanie i optymalizacja udziału w rynkach (strategie ofertowania, zarządzanie niepewnością, value stacking) oraz (2) metody sterowania i integracji DER (architektury scentralizowane i zdecentralizowane). Mniej prac łączy te zagadnienia z wymiarami bezpieczeństwa energetycznego państwa w sposób operacjonalizowany (KPI, proces oceny, warunki brzegowe wdrożenia), szczególnie z uwzględnieniem cyberodporności jako integralnej części bezpieczeństwa dostaw. Równolegle literatura o systemach zarządzania DER (HEMS/EMS, DERMS, ADMS/SCADA) bywa analizowana „w oderwaniu" od ram bezpieczeństwa energetycznego.

Celem rozdziału jest: (1) zaproponowanie ram analitycznych łączących wymiary bezpieczeństwa energetycznego z architekturą VPP i systemami ICT, (2) zmapowanie funkcji VPP oraz warstw informatycznych na mechanizmy wzmacniania bezpieczeństwa, (3) zaproponowanie zestawu KPI i procesu oceny wkładu VPP w bezpieczeństwo energetyczne państwa z uwzględnieniem cyberryzyk. Pytania badawcze sformułowano następująco:
RQ1 – które mechanizmy VPP najsilniej wspierają poszczególne wymiary 4A + odporność?
RQ2 – jakie warstwy ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO) są krytyczne dla bezpiecznego skalowania VPP?
RQ3 – jakie ryzyka cyberfizyczne towarzyszą VPP i jak włączyć je do oceny bezpieczeństwa energetycznego?

Metody

Projekt badania

Zastosowano podejście mieszane: ustrukturyzowany przegląd literatury (scoping review) oraz analizę konceptualną opartą na mapowaniu funkcji i zależności. Przyjęto, że dla oceny bezpieczeństwa energetycznego

państwa istotna jest nie tylko poprawność modeli optymalizacyjnych VPP, lecz także zdolność do skalowania, interoperacyjności, weryfikowalności (measurement & verification – M&V) i odporności na ryzyka (w tym cybernetyczne). Z tego powodu analizą objęto prace z trzech obszarów: (a) VPP i agregacja DER, (b) systemy zarządzania zasobami rozproszonymi po stronie operatorów (DERMS/ADMS/EMS), (c) cyberbezpieczeństwo DER i systemów smart grid.

Dobór literatury i kryteria włączenia

Publikacje identyfikowano dla lat 2018-2026, ze szczególnym naciskiem na prace po 2021 r. Włączano materiały spełniające łącznie kryteria: (a) bezpośrednie odniesienie do VPP, agregacji DER, elastyczności, DERMS/ADMS/EMS lub cyberbezpieczeństwa DER, (b) możliwość powiązania z co najmniej jednym wymiarem bezpieczeństwa energetycznego (4A, resilience/cyber), (c) dostępny identyfikator DOI. Wykluczano publikacje bez DOI, czysto opisowe bez implikacji dla funkcji systemu lub niewystarczająco związane z elektroenergetyką.

Procedura analityczna

Dla każdej publikacji kodowano: (1) wymiar bezpieczeństwa energetycznego (availability, accessibility, affordability, acceptability, resilience/cyber), (2) funkcje VPP (prognozowanie, optymalizacja, dyspozycja, udział w rynkach, usługi systemowe, M&V), (3) warstwę systemów ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO), (4) typ ryzyka i środki kontroli (np. szyfrowanie, uwierzytelnianie, segmentacja, monitoring, ocena ryzyka). Następnie przeprowadzono syntezę tematyczną i opracowano mapowanie mechanizmów (Tabela 1) oraz porównanie warstw ICT (Tabela 2), a także dwa schematy koncepcyjne (Rysunki 1-2).

Wyniki

Mechanizmy, przez które VPP wzmacniają bezpieczeństwo energetyczne

Synteza literatury pozwala wyróżnić sześć klas mechanizmów łączących funkcje VPP i systemów ICT z bezpieczeństwem energetycznym państwa.

1. Adekwatność mocy i bilansowanie (availability). VPP zwiększa „efektywną" dyspozycyjność poprzez agregację wielu małych jednostek i zasobów elastyczności. Kluczowa jest zdolność sterowania w krótkim horyzoncie: strategie agregacji i dyspozycji w czasie rzeczywistym podnoszą zdolność regulacyjną i elastyczność VPP (Liu i in., 2024). Dla państwa oznacza to potencjał redukcji ryzyka niedoborów mocy w sytuacjach krytycznych – pod warunkiem, że elastyczność jest kontraktowalna, dostępna i zweryfikowana (M&V).
2. Usługi systemowe i stabilność (frequency/voltage). Integracja magazynów i elastycznych obciążeń umożliwia świadczenie usług regulacji częstotliwości i rezerw, a w pewnych konfiguracjach także wsparcie parametrów lokalnych (napięcia, przeciążenia). Przykładowo, mechanizmy zdecentralizowane mogą ograniczać zależność od jednego centrum sterowania oraz zmniejszać wąskie gardła obliczeniowe, co sprzyja odporności operacyjnej, pokazują to m.in. prace dotyczące zdecentralizowanego świadczenia regulacji częstotliwości przez VPP (Sun i in., 2023).
3. Redukcja kosztów i ryzyk cenowych (affordability). VPP umożliwia optymalizację portfela zasobów w wielu segmentach rynku („value stacking") oraz ograniczanie kosztów bilansowania i rezerw przez wykorzystanie elastyczności. Przeglądy VPP akcentują, że nowoczesne modele obejmują coraz szerszy zakres rynków i usług oraz łączą cele ekonomiczne z ograniczeniami technicznymi (Esfahani i in., 2025; Zare, Shafiyi, 2025). Dla państwa efekt jest pośredni: niższe koszty systemowe mogą stabilizować ceny energii i zmniejszać ekspozycję gospodarki na szoki, ale wymaga to poprawnego projektowania bodźców i zasad rozliczeń.
4. Dywersyfikacja i dostęp (accessibility). Agregacja rozproszona zmniejsza koncentrację ryzyka w pojedynczych punktach i technologiach. VPP może koordynować zasoby prosumenckie i lokalne magazyny, zwiększając udział energii lokalnej w bilansie oraz umożliwiając priorytetyzację odbiorów w sytuacjach kryzysowych (np. utrzymanie zasilania infrastruktury krytycznej na poziomie dystrybucji). W tym wymiarze krytyczne są rejestry zasobów, mechanizmy kwalifikacji urządzeń, a także integracja z DERMS, które „pilnuje" ograniczeń sieci.

5. Akceptowalność transformacji (acceptability). VPP ułatwia integrację OZE poprzez sterowanie popytem, magazyny i redukcję kosztów zmienności. Ograniczenie redukcji generacji OZE (curtailment) oraz poprawa wykorzystania lokalnych zasobów mogą zmniejszać potrzebę utrzymywania wysokoemisyjnych rezerw i ograniczać koszty społeczne transformacji. W ujęciu bezpieczeństwa energetycznego oznacza to jednoczesne wsparcie celów środowiskowych i kosztowych. W praktyce mechanizm ten jest wzmacniany przez narzędzia prognozowania i optymalizacji, które – jak wskazują przeglądy AI/IoT w DR – stają się coraz bardziej dostępne, ale wymagają nadzoru jakości danych i cyberochrony (Algburi i in., 2025).
6. Odporność i cyberbezpieczeństwo (resilience/cyber). Cyfrowa koordynacja zasobów zwiększa możliwości reagowania na zakłócenia (rekonfiguracja portfela, aktywacja DR, przejście w tryby awaryjne), ale jednocześnie powiększa powierzchnię ataku: urządzenia IoT i firmware, kanały łączności, interfejsy API, protokoły OT/IT, a także zależności w łańcuchu dostaw oprogramowania. Wzrost skali VPP oznacza, że incydent cybernetyczny może mieć konsekwencje systemowe, dlatego cyberodporność musi być traktowana jako część bezpieczeństwa dostaw (Schmitz i in., 2025). Przeglądy cyberbezpieczeństwa DER identyfikują zestaw środków obrony: segmentację stref OT/IT, zarządzanie tożsamością i uprawnieniami (IAM), szyfrowanie i uwierzytelnianie komunikacji, monitoring (SOC/IDS) oraz procedury reagowania na incydenty, uwzględniające współdziałanie wielu interesariuszy (Chen i in., 2025; Hasan i in., 2022). Ramy i standardy sektorowe stanowią w tym kontekście „szkielet" wymagań bezpieczeństwa (Leszczyna, 2018; Ustun, 2022), a adaptacje kryteriów oceny ryzyka do środowisk VPP są rozwijane także w pracach dotyczących oceny ryzyka dla wirtualnych elektrowni (Gkoktsis i in., 2023).

Poniżej (Tabela 1) przedstawiono mapę: wymiary bezpieczeństwa energetycznego, mechanizmy VPP/ICT oraz przykładowe KPI.

Tabela 1. Mapowanie wymiarów bezpieczeństwa energetycznego na funkcje VPP i systemów ICT

Wymiar bezpieczeństwa	Przykładowe ryzyko systemowe	Mechanizmy VPP (funkcje)	Warstwa ICT (przykłady)	Przykładowe KPI do oceny
Dostępność / adekwatność (availability)	Niedobór mocy, wysoki EENS/ LOLE, ograniczenia bilansowania	Agregacja DER, prognozy, optymalizacja portfela, dispatch w RT, rezerwy	Platforma VPP, integracja z EMS/TSO, DERMS/ADMS	LOLE, EENS, margines rezerw, dostępna elastyczność (MW/MWh), ramp rate (MW/ min), niezawodność aktywacji (%)
Stabilność operacyjna (frequency/voltage)	Odchylenia f/U, przeciążenia, ograniczenia OZE	Usługi regulacyjne, sterowanie magazynem i obciążeniem, lokalne wsparcie napięcia	ADMS/SCADA, DERMS, VPP	Czas i liczba naruszeń limitów f/U, wolumen usług pomocniczych, redukcja curtailment, liczba interwencji DSO
Przystępność cenowa (affordability)	Zmienność cen, koszty bilansowania, ubóstwo energetyczne	Value stacking, DR, arbitraż magazynem, optymalizacja kosztów	EMS/HEMS, VPP, rozliczenia/M&V	Koszt bilansowania i rezerw, zmienność cen (quantyle), koszty krańcowe elastyczności, oszczędność u odbiorców
Dostęp i dywersyfikacja (accessibility)	Zależność importowa, awarie punktów, wąskie gardła	Rozproszenie zasobów, lokalne bilansowanie, priorytetyzacja odbiorów	DERMS/ADMS, HEMS, rejestry	Udział energii lokalnej, dywersyfikacja portfela (HHI), czas przywrócenia, liczba krytycznych węzłów
Akceptowalność (acceptability)	Emisyjność rezerw, konflikty środowiskowe	Integracja OZE, redukcja emisji, ograniczenie pracy źródeł szczytowych	EMS/planowanie, analityka VPP	Emisje CO2e (kg/MWh), redukcja curtailment OZE, odsetek odbiorców w DR, proxy jakości powietrza
Odporność i cyber (resilience/cyber)	Blackout, incydent cyber, awaria łączności, manipulacja danymi	Rekonfiguracja portfela, tryby awaryjne, monitoring, M&V	SOC/monitoring, IAM, segmentacja, IDS, audyty	MTTR/MTBF usług cyfrowych, czas detekcji/reakcji, liczba incydentów, zgodność ze standardami, dostępność łączności

Źródło: opracowanie własne.

Warstwy informatyczne zarządzania a VPP: rola DERMS i ADMS

VPP nie działa w próżni: jej bezpieczeństwo i użyteczność zależą od integracji z warstwami sterowania i danych po stronie odbiorców (HEMS/EMS), operatorów dystrybucyjnych (DERMS + ADMS/SCADA) i operatora przesyłowego (EMS/TSO). W praktyce DERMS pełni rolę „tłumacza" między światem zasobów rozproszonych a wymaganiami bezpiecznej pracy sieci: łączy rejestr zasobów, obserwację stanu, zarządzanie ograniczeniami, a także interfejsy do agregatorów/VPP (Strezoski, 2023). ADMS/SCADA dostarcza obraz stanu sieci i narzędzia automatyki (np. rekonfiguracja), ważne dla odtwarzania zasilania.

Z perspektywy bezpieczeństwa energetycznego (Tabela 2) kluczowe są trzy konsekwencje tej architektury. Po pierwsze, aktywacja usług przez VPP musi uwzględniać ograniczenia sieci dystrybucyjnej (constraints), w przeciwnym razie elastyczność może generować lokalne ryzyka. Po drugie, parametry telemetrii i sterowania (czas reakcji, rozdzielczość danych, dostępność łączności) stają się elementem krytycznymi dla niezawodności usług. Po trzecie, integracja danych i interfejsów oznacza nowe wektory ataku, dlatego minimalne wymagania cyberbezpieczeństwa powinny obejmować cały łańcuch (urządzenia, łączność, VPP, integracje z DSO/TSO).

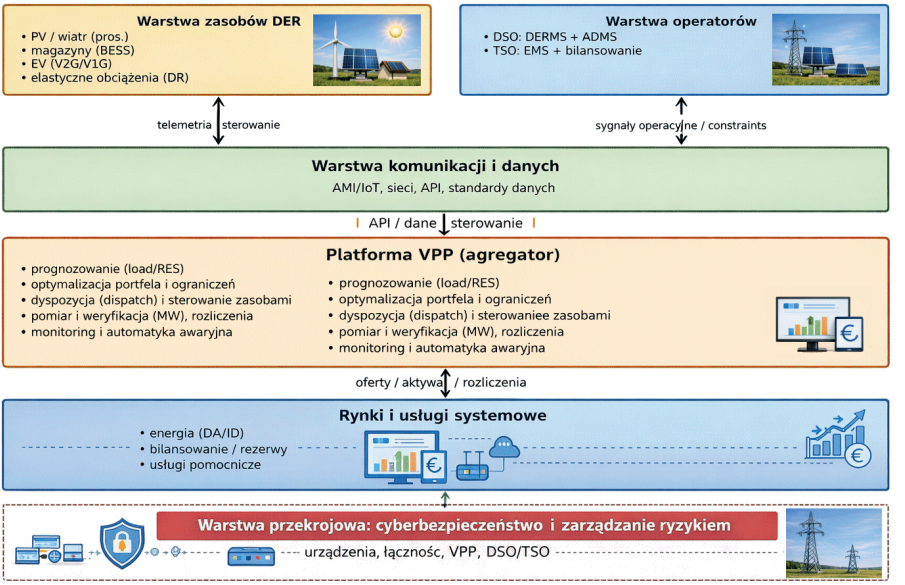
Tabela 2. Porównanie funkcji warstw ICT istotnych dla VPP i bezpieczeństwa energetycznego

Warstwa/system	Główny cel	Horyzont sterowania	Dane wejściowe (przykłady)	Kluczowe punkty integracji	Typowe ryzyka i kontrole
HEMS/EMS (budynek/zakład)	Optymalizacja lokalna (koszt/komfort), sterowanie urządzeniami	sekundy-godziny	smart meter, czujniki, taryfy, prognoza PV, stan magazynu/EV	integracja z VPP (API), lokalna automatyka	prywatność, błędy sterowania, uwierzytelnianie, aktualizacje, segmentacja sieci lokalnej
Platforma VPP (agregator)	Agregacja, prognozowanie, optymalizacja, udział w rynkach/usługach	minuty-dni	profile zasobów, prognozy, ograniczenia, ceny, sygnały TSO/DSO	integracja z DERMS/ ADMS i rynkami, M&V	single point of failure, manipulacja danymi, redundancja, audyt algorytmów, SOC, testy
DERMS (operator DSO)	Bezpieczna integracja DER z siecią, zarządzanie ograniczeniami	sekundy-godziny	topologia sieci, pomiary, zdolności elastyczności, constraints	integracja z ADMS/ SCADA i VPP	ataki na telemetrię, błędna estymacja, segmentacja OT/IT, monitoring, polityki dostępu
ADMS/SCADA (sieć dystrybucyjna)	Nadzór i automatyka sieci, przywracanie zasilania	sekundy-minuty	pomiary, stany łączników, sygnały zabezpieczeń, prognozy	współpraca z DERMS, interfejsy OT	incydenty cyber-fizyczne OT, hardening, separacja stref, testy, procedury IR
EMS/TSO (system przesyłowy)	Bilansowanie krajowe, usługi systemowe, bezpieczeństwo KSE	minuty-dni	prognozy obciążenia/ generacji, rezerwy, constraints	integracja z rynkami i agregatorami	błędy koordynacji, procedury operacyjne, rezerwy manualne, redundancja

Źródło: opracowanie własne.

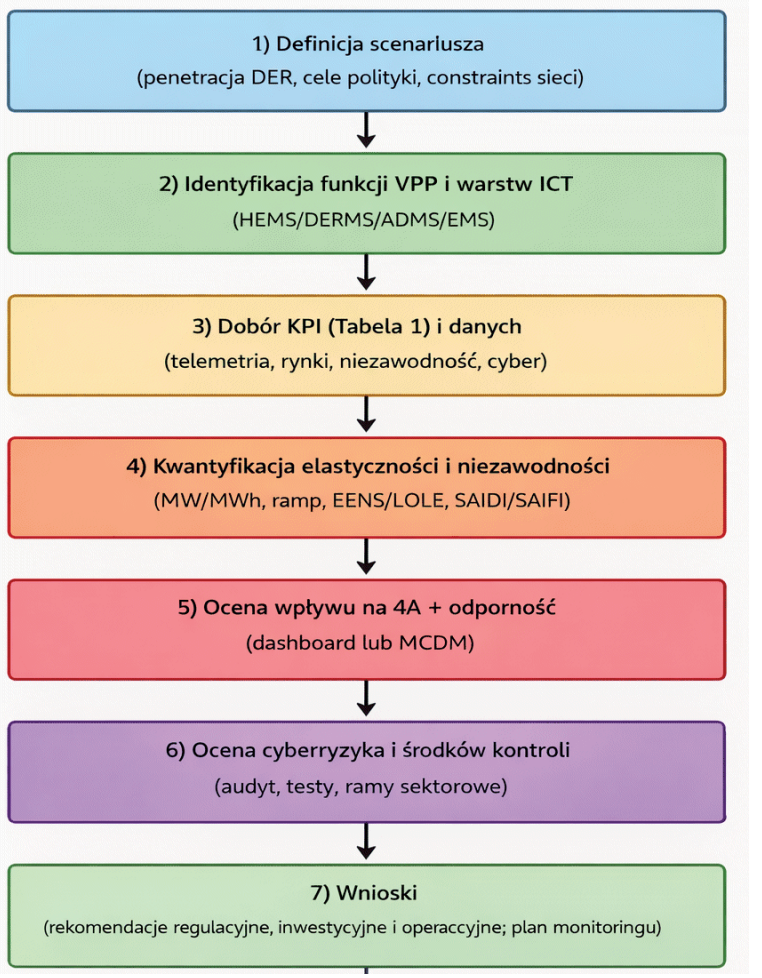
Modele graficzne: architektura i proces oceny

Poniżej przedstawiono dwa rysunki koncepcyjne: architekturę przepływów danych (Rysunek 1) oraz proces oceny wkładu VPP w bezpieczeństwo energetyczne (Rysunek 2).



Rysunek 1. Architektura VPP i systemów ICT w relacji do operatorów oraz rynków

Źródło: opracowanie własne.



Rysunek 2. Proces oceny wkładu VPP w bezpieczeństwo energetyczne
Źródło: opracowanie własne.

Dyskusja

VPP jako instrument bezpieczeństwa energetycznego

Wyniki sugerują, że VPP i systemy ICT mogą stać się narzędziem polityki bezpieczeństwa energetycznego, ale tylko wtedy, gdy są traktowane jako element ekosystemu operacyjnego i regulacyjnego, a nie wyłącznie jako rozwiązanie rynkowe. Włączenie VPP do planowania bezpieczeństwa wymaga powiązania wskaźników technicznych (EENS/LOLE, stabilność),

ekonomicznych (koszty bilansowania, zmienność cen) i środowiskowych (emisje) z odpornością cyfrową (czas detekcji, gotowość procedur, dostępność łączności). W praktyce państwo (regulator, operatorzy, instytucje ds. cyber) powinno traktować platformy VPP jako element infrastruktury krytycznej „z funkcji", nawet jeśli są własnością podmiotów komercyjnych.

Poziom techniczny. Aktywacja elastyczności przez VPP musi uwzględniać ograniczenia sieci dystrybucyjnej, w przeciwnym razie działania rynkowe mogą być technicznie niebezpieczne (np. kumulacja ładowania EV w słabym węźle). Dlatego rozwój VPP powinien iść w parze z rozwojem DERMS/ADMS, automatyki i procedur koordynacji DSO-TSO (Strezoski, 2023). Poziom ekonomiczny. Korzyści dla przystępności cenowej zależą od projektowania rynków elastyczności, transparentności rozliczeń i właściwej alokacji ryzyk, bez tego elastyczność może istnieć „na papierze", ale nie być dostępna w godzinach krytycznych (Esfahani i in., 2025).

Rekomendacje wdrożeniowe w skali państwa

Na podstawie syntezy można wskazać cztery grupy rekomendacji zwiększających prawdopodobieństwo, że VPP wzmocnią bezpieczeństwo energetyczne:

1. Interoperacyjność i governance danych: standardy danych, minimalna telemetria, rejestry zasobów, wymagania dla API oraz zasady jakości danych (kompletność, spójność, czasowość). W praktyce chodzi o to, by zasoby były „adresowalne" i „mierzalne" oraz by możliwy był audyt.
2. Koordynacja DSO-TSO: reguły priorytetyzacji (bezpieczeństwo sieci przed rynkiem), platformy wymiany constraints i mechanizmy unikania sprzecznych sygnałów do tych samych zasobów. W państwach o rosnącej penetracji DER koordynacja ta staje się warunkiem wykorzystania elastyczności bez pogorszenia niezawodności.
3. M&V jako filar bezpieczeństwa: weryfikacja wolumenów, parametrów dynamicznych (czas reakcji, ramp) i niezawodności usług, logowanie decyzji i ścieżek audytu (auditability). Im większy wpływ VPP na bilansowanie systemu, tym większa potrzeba formalizacji M&V.
4. Security-by-design: minimalne wymagania bezpieczeństwa dla urządzeń końcowych, łączności i platform, obejmujące m.in. segmentację

OT/IT, IAM, monitoring (SOC) i procedury IR obejmujące cały łańcuch interesariuszy. Przeglądy podkreślają, że bezpieczeństwo smart grid nie jest możliwe bez spójnych standardów i praktyk wdrażanych end-to-end (Chen i in., 2025; Leszczyna, 2018).

Rozdział ma charakter konceptualno-przeglądowy. Ograniczeniem jest brak empirycznej weryfikacji na danych krajowych oraz fakt, że literatura techniczna często opiera się na modelach testowych. Dalsze badania powinny łączyć: (a) analizę niezawodności i odporności (EENS/LOLE, scenariusze szoków i procesów długotrwałych), (b) modelowanie ekonomiczne rynków elastyczności oraz (c) ocenę cyberryzyka w architekturach wielostronnych, w tym wpływu pojedynczych platform na ryzyko systemowe. Szczególnie potrzebne są studia przypadków dużych VPP, które pokażą, w jakim stopniu „cyfrowe" KPI (dostępność łączności, jakość danych, dojrzałość SOC) korelują z KPI energetycznymi (np. niezawodność dostaw usług bilansujących).

Wnioski

VPP i powiązane systemy ICT mogą wzmacniać bezpieczeństwo energetyczne państwa w wielu wymiarach: od adekwatności mocy i stabilności pracy systemu, przez przystępność cenową i dywersyfikację, po akceptowalność środowiskową. Warunkiem jest jednak traktowanie VPP jako elementu infrastruktury krytycznej, w którym elastyczność jest mierzalna, weryfikowalna i bezpieczna cyfrowo. Proponowane w rozdziale mapowanie mechanizmów, KPI oraz proces oceny mogą stanowić podstawę do projektowania programów elastyczności i cyfryzacji w taki sposób, aby były one jednocześnie efektywne kosztowo i odporne na ryzyka zakłóceniowe.

Literatura

1. Algburi, S., Abed Al Kareem, S. S., Sapaev, I. B., Mukhitdinov, O., Hassan, Q., Khalaf, D. H., Jabbar, F. I. (2025). The role of artificial intelligence in accelerating renewable energy adoption for global energy transformation. *Unconventional Resources, 8*, 100229. https://doi.org/10.1016/j.uncres.2025.100229

2. Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Applied Energy, 383*, 125364. https://doi.org/10.1016/j.apenergy.2025.125364
3. Esfahani, M., Alizadeh, A., Cao, B., Kamwa, I., Xu, M. (2025). Bridging theory and practice: A comprehensive review of virtual power plant technologies and their real-world applications. *Renewable and Sustainable Energy Reviews, 222*, 115929. https://doi.org/10.1016/j.rser.2025.115929
4. Gkoktsis, G., Lauer, H., Jäger, L. (2023). Risk assessments in virtual power plants with NESCOR criteria, practical application, advantages and disadvantages. ARES 2023: *Proceedings of the 18Th International Conference on Availability, Reliability and Security*, 1-11. https://doi.org/10.1145/3600160.3605179
5. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., Razzaque, M. A. (2022). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications, 209*, 103540. https://doi.org/10.1016/j.jnca.2022.103540
6. Leszczyna, R. (2018). Standards and frameworks for cybersecurity in smart grid. *Computers Security, 79*, 1-15. https://doi.org/10.1016/j.cose.2018.03.011
7. Liu, X., Li, Y., Wang, L., Tang, J., Qiu, H., Berizzi, A., Valentin, I., Gao, C. (2024). Dynamic aggregation strategy for a virtual power plant to improve flexible regulation ability. *Energy, 297*, 131261. https://doi.org/10.1016/j.energy.2024.131261
8. Roozbehani, M. M., Heydarian-Forushani, E., Hasanzadeh, S., Elghali, S. B. (2022). Virtual power plant operational strategies: Models, markets, optimization, challenges, and opportunities. *Sustainability, 14*(19), 12486. https://doi.org/10.3390/su141912486
9. Schmitz, R., Flachsbarth, F., Plaga, L. S., Braun, M., Härtel, P. (2025). Energy security and resilience: Revisiting concepts and advancing planning perspectives for transforming integrated energy systems. *Energy Policy, 207*, 114796. https://doi.org/10.1016/j.enpol.2025.114796

10. Siksnelyte-Butkiene, I., Streimikiene, D., Lekavicius, V., Balezentis, T. (2024). Comprehensive analysis of energy security indicators and measurement of their integrity. *Technological Forecasting and Social Change, 200*, 123167. https://doi.org/10.1016/j.techfore.2023.123167
11. Strezoski, L. (2023). Distributed energy resource management systems (DERMS): State of the art and how to move forward. *WIREs Energy and Environment, 12*(1), e460. https://doi.org/10.1002/wene.460
12. Sun, X., Xie, H., Qiu, D., Xiao, Y., Bie, Z., Strbac, G. (2023). Decentralized frequency regulation service provision for virtual power plants: A best response potential game approach. *Applied Energy, 352*, 121987. https://doi.org/10.1016/j.apenergy.2023.121987
13. Ustun, T. S. (2022). Cybersecurity for smart grids. *Energies, 15*(15), 5458. https://doi.org/10.3390/en15155458
14. Zare, A., Shafiyi, M. A. (2025). Virtual power plant models and market participation: A deep dive into optimization and real-world applications. *Results in Engineering, 26*, 105548. https://doi.org/10.1016/j.rineng.2025.105548

Małgorzata Orłowska[1], Michał Mogilnicki[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103373_15

WYBRANE CYBERZAGROŻENIA W LOGISTYCE XXI W. WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI W OCHRONIE ŁAŃCUCHÓW DOSTAW

SELECTED CYBER THREATS IN 21ST-CENTURY LOGISTICS. THE USE OF ARTIFICIAL INTELLIGENCE IN SUPPLY CHAIN SECURITY

Streszczenie

Celem niniejszego rozdziału było ukazanie ewolucji logistyki w XXI w. w kontekście rosnącej podatności na zagrożenia cybernetyczne oraz analiza metod przeciwdziałania tym zagrożeniom, ze szczególnym uwzględnieniem zastosowania sztucznej inteligencji w ochronie łańcuchów dostaw. W pracy przeprowadzono kompleksową analizę wpływu cyberzagrożeń na funkcjonowanie logistyki, identyfikując kluczowe obszary ryzyka, w tym ataki na systemy zarządzania łańcuchem dostaw (SCM), zakłócenia w infrastrukturze teleinformatycznej oraz wykorzystanie dezinformacji jako narzędzia destabilizującego procesy logistyczne. Szczególną uwagę poświęcono zjawisku dezinformacji, które w dobie globalizacji i dynamicznego przepływu danych stanowi istotne zagrożenie dla bezpieczeństwa operacyjnego

[1] https://orcid.org/0000-0002-8446-8764, e-mail: m.orlowska@akademia.mil.pl
[2] https://orcid.org/0009-0003-2545-6266, e-mail: michalmogilnicki00@gmail.com

podmiotów logistycznych. Ponadto wskazano mechanizmy propagowania fałszywych informacji oraz ich wpływ na decyzje podejmowane w ramach zarządzania łańcuchem dostaw. Przeanalizowano również scenariusze manipulacji danymi i ich konsekwencje dla efektywności operacyjnej przedsiębiorstw logistycznych. W kontekście przeciwdziałania cyberzagrożeniom podjęto rozważania na temat wykorzystania sztucznej inteligencji jako jednego z narzędzi wykorzystywanych w ochronie łańcuchów dostaw. Omówiono zastosowanie algorytmów uczenia maszynowego w detekcji anomalii w systemach teleinformatycznych, wykrywaniu incydentów bezpieczeństwa oraz automatyzacji reakcji na potencjalne zagrożenia. Dodatkowo zwrócono uwagę na rolę sztucznej inteligencji w predykcji ryzyka oraz optymalizacji procesów logistycznych w kontekście zapewnienia ich odporności na cyberataki. Na podstawie przeprowadzonych analiz opracowano rekomendacje dotyczące wzmacniania cyberbezpieczeństwa w logistyce, ze szczególnym uwzględnieniem strategii integracji sztucznej inteligencji z tradycyjnymi metodami zarządzania bezpieczeństwem w łańcuchach dostaw. Wskazano kierunki przyszłych badań w obszarze ochrony systemów logistycznych przed zagrożeniami cybernetycznymi i dezinformacyjnymi. Całość opracowania zwieńczono podsumowaniem, w którym podkreślono wnioski dotyczące wyzwań i możliwości, jakie niesie XXI w. dla bezpieczeństwa logistyki w erze cyfrowej transformacji.

Słowa kluczowe: logistyka, zarządzanie, cyberbezpieczeństwo, dezinformacja, sztuczna inteligencja

Abstract

The aim of this chapter was to complete the evolution of logistics in the 21st century with respect to the application of cybersecurity vulnerabilities and analyse methods for preventing these threats, with a detailed application of artificial intelligence in supply chain protection. In a comprehensive approach to addressing the impact of cybersecurity threats on logistics operations, key threats were identified, including disruptions to the secure supply chain management (SCM) system, IT infrastructure disruptions, and the use of disinformation to destabilise logistics processes. Particular attention was paid to the phenomenon of disinformation, which in the era of globalisation and data exploitation constitutes a key safeguard for data security. Additionally, mechanisms for information propagation and its Impact on supply chain management decisions were identified. Data manipulation scenarios and their consequences for the operational efficiency of logistics companies were also analysed. In connection with countering cybersecurity threats, an assessment was conducted of the use of artificial intelligence to protect supply chains. Machine learning algorithms are used to detect anomalies in known ICT systems, detect security incidents, and automate risk responses. Additionally, attention is drawn to the risks posed by

artificial intelligence in threat prediction and logistics system optimisation, given their vulnerability to cyberattacks. Based on the analysis, recommendations were developed to strengthen cybersecurity in logistics by applying artificial intelligence strategies alongside traditional management methods for basic supplies. Information is provided on the implications of the research for protecting IT systems from cyber and disinformation threats. The concluding summary provides information on the significance of the conclusions regarding the opportunities and possibilities the 21st century offers for logistics security in the era of artificial transformation.

Keywords: logistics, military logistics, management, cybersecurity, disinformation, artificial intelligence

Wstęp

Rozważania na temat cyberzagrożeń w logistyce jako czynników negatywnie oddziałujących na cyberbezpieczeństwo branży wydają się uzasadnione. Bardzo mało jest publikacji poświęconych rozważaniom w tym zakresie. Sytuację problemową stanowiła próba ukazania, w jaki sposób cyberzagrożenia oraz dezinformacja wpływają na współczesną logistykę, a także jak sztuczna inteligencja może wspierać zapewnianie cyberbezpieczeństwa. Celem głównym opracowania było wyjaśnienie, co współcześnie stanowi wyzwanie dla cyberbezpieczeństwa logistyki (łańcuchów dostaw) oraz w jaki sposób można im przeciwdziałać. Z kolei celami szczegółowymi były ukazanie ewolucji logistyki, pod kątem wykorzystania technologii cyfrowych. Dokonanie analizy wybranych ryzyk, jakie są powszechnie obserwowane w logistyce, w wymiarze cyberbezpieczeństwa. Jak również, ukazanie dezinformacji jako istotnego cyberzagrożenia dla bezpieczeństwa logistyki. Hipotezę badawczą stanowił pogląd autorów, że możliwa jest synergia sztucznej inteligencji z personelem logistycznym, jeśli zrealizowane zostaną adekwatne działania przygotowawczo-edukacyjne w aspekcie zapewniania cyberbezpieczeństwa.

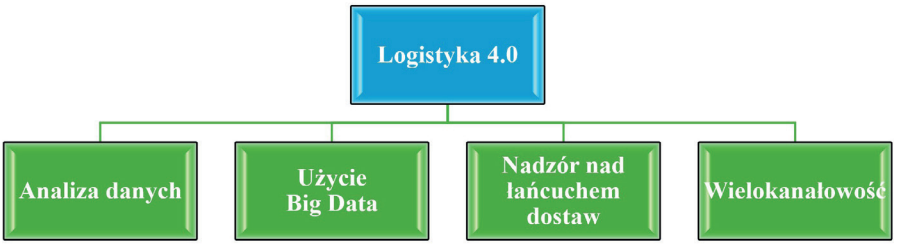
Cyfryzacja logistyki

W historii cywilizacji wyróżniono trzy ważne rewolucje przemysłowe, które doprowadziły do poważnych zmian gospodarczych i zwiększonej wydajności produkcji. Ich wynikiem był dynamiczny rozwój gospodarczy i poprawa jakości życia społeczeństw. Pierwsza rewolucja przemysłowa

była powiązana z rozpoczęciem wykorzystywania silników parowych, które pozwoliły na opracowanie narzędzi i maszyn, znacznie wydajniejszych od dotychczasowych. Druga rewolucja przemysłowa rozpoczęła się wraz z wynalezieniem maszyn zasilanych energią elektryczną, które przyczyniły się do tworzenia zarządzania produkcją i wprowadzenia masowej produkcji. Tymczasem trzecia rewolucja przemysłowa, opisana jako rewolucja naukowa i technologiczna, była oparta na automatyzacji procesów z wykorzystaniem informacji i technologii IT oraz zastosowaniu technologii IT w celu poprawy wydajności i jakości produkcji. Współcześnie coraz częściej mówi się o czwartej rewolucji przemysłowej, nazywanej Przemysłem 4.0 lub cyfrową transformacją (Płaczek, 2018).

Rozwój technologii cyfrowych zrewolucjonizował współczesną logistykę. Zauważalne są zmiany w sposobie zarządzania łańcuchem dostaw, procesami magazynowymi i transportowymi. Logistyka, podobnie jak przemysł, przeszła kilka etapów rozwoju, dostosowując się do zmian technologicznych i gospodarczych (Arvato, b.d.). Każda kolejna wersja logistyki odzwierciedlała coraz większy stopień automatyzacji i integracji w zarządzaniu łańcuchem dostaw. Logistyka 1.0 dotyczyła podstawowych operacji związanych z transportem, magazynowaniem i dystrybucją towarów. Realizowanych za pomocą papierowej dokumentacji i prostych metod zarządzania. Transport odbywał się głównie przy użyciu kolei i żeglugi, a jego głównym celem było przemieszczanie towarów z jednego punktu do drugiego (Tjahjono i in., 2017). Wraz z drugą rewolucją przemysłową i upowszechnieniem produkcji masowej logistyka zaczęła rozwijać się pod kątem optymalizacji procesów. W Logistyce 2.0 wprowadzono pierwsze systemy mechanizacji, takie jak przenośniki taśmowe i wózki widłowe, a także standaryzację transportu (np. konteneryzację). Dokumentacja wciąż była w większości papierowa, jednak zaczęły pojawiać się pierwsze systemy wspierające zarządzanie zapasami. Logistyka 3.0 stanowiła erę globalizacji i szerokiego wykorzystania technologii informatycznych. Wprowadzenie systemów zarządzania łańcuchem dostaw (SCM), systemów ERP oraz automatycznych systemów identyfikacji (np. kody kreskowe) pozwoliło na lepszą kontrolę i optymalizację procesów logistycznych (Orłowska, 2023). Powstały pierwsze systemy zarządzania magazynem (WMS) oraz systemy śledzenia przesyłek. Logistyka stała się kluczowym elementem strategii biznesowych, umożliwiając

firmom dostosowanie się do dynamicznych zmian rynkowych. Logistyka 4.0 odnosi się do wdrażania inteligentnych systemów oraz pełnej automatyzacji (Rysunek 1) (Sokołowska, 2024). Przy użyciu zaawansowanych technologii, takich jak sztucznej inteligencji (AI), Internetu Rzeczy (IoT), Big Daty, blockchainów, robotyzacji i autonomicznych pojazdów. Systemy zarządzania magazynem (WMS) i transportem (TMS) pracują w chmurze i są zintegrowane z innymi systemami w czasie rzeczywistym. Misją logistyki 4.0 jest dążenie do elastyczności, predykcyjnego zarządzania zapasami oraz minimalizacji kosztów operacyjnych (Barcik, Odlanicka-Poczobutt, 2020). Ponadto w logistyce 4.0 zyskały na znaczeniu: zrównoważony rozwój i ekologiczne rozwiązania, takie jak pojazdy elektryczne czy inteligentne zarządzanie flotą pojazdów przedsiębiorstwa.



Rysunek 1. Elementy Logistyki 4.0

Źródło: opracowanie własne na podstawie RedSteel, b.d.

Choć pojęcie Logistyki 5.0 nie jest jeszcze szeroko ugruntowane, pojawia się ono i wskazuje na kolejną fazę rozwoju. Zadaniem logistyki 5.0 ma być skupienie się na harmonijnym współdziałaniu ludzi i technologii, z naciskiem na zrównoważony rozwój oraz społeczną odpowiedzialność biznesu (Bielecki, 2022).

W dobie digitalizacji firmy logistyczne wdrożyły zaawansowane rozwiązania z obszaru technologii cyfrowych. Umożliwiło to tworzenie podstaw automatyzacji, optymalizacji i zwiększonej wydajności operacyjnej (Internet IoT), sztucznej inteligencji (AI), Big Data, Blockchain, Process Robotation – Logistics 4.0. Oczywiście, w oparciu głównie o narzędzia z obszaru cyber. Cyfryzacja logistyki umożliwia ciągłe monitorowanie i analizę danych w czasie rzeczywistym, co prowadzi do bardziej szczegółowego planowania transportu, zarządzania zapasami i zmniejszania kosztów operacyjnych.

Wykorzystanie cyfrowych, inteligentnych systemów analitycznych umożliwiło prognozowanie popytu, optymalizację tras oraz eliminację zbędnych przejazdów, co przekłada się na bardziej efektywne i ekologiczne zarządzanie flotą transportową (Ivanov i in., 2019).

Współczesne magazyny coraz częściej wykorzystują systemy automatyki, w tym autonomiczne roboty, drony oraz zaawansowane systemy identyfikacji towarów oparte na RFID i kodach kreskowych (Orłowska, Orłowski, 2024). Integracja tych technologii z systemami zarządzania magazynem (WMS) pozwala na zwiększenie precyzji operacji logistycznych, minimalizację błędów oraz redukcję czasu potrzebnego na kompletację zamówień. Cyfrowa transformacja logistyki ma również istotne znaczenie w kontekście zrównoważonego rozwoju. Inteligentne systemy monitorujące mogą optymalizować zużycie energii i paliwa, zmniejszając ślad węglowy transportu. Ponadto integracja systemów informatycznych umożliwia lepszą współpracę pomiędzy podmiotami w łańcuchu dostaw, zwiększając transparentność procesów i poprawiając efektywność logistyczną.

Widoczne zdaje się być, jak duże pole manewru mogą mieć cyberzagrożenia w obszarze logistyki. Z uwagi na to, jak istotne z punktu widzenia funkcjonowania państwa są branża i element gospodarki, należy mieć świadomość, że kluczowe jest zapewnienie ich bezpieczeństwa. Zarówno w wymiarze kinetycznym, jak i cybernetycznym. Każda ze wspomnianych wersji logistyki przynosiła dlań nowe zagrożenia dla bezpieczeństwa, a tym samym nowe zagrożenia dla podmiotu, wewnątrz którego „nowa logistyka" funkcjonowała. Obecnie zakorzeniająca się Logistyka 5.0 i jej istota skupiona wokół współdziałania systemów cybernetycznych oraz sztucznej inteligencji z ludźmi pozwalają przewidywać, że oprócz wielu szans będą pojawiać się zagrożenia cyberbezpieczeństwa podmiotów logistycznych. Zasadnym wydaje się podjąć rozważania na tym etapie dotyczące typów form ryzyka, z jakimi będzie już niedługo musiała się mierzyć logistyka w aspekcie cyberbezpieczeństwa.

Cyberzagrożenia procesów logistycznych – analiza współczesnych ryzyk

Zaawansowany już obecnie oraz ciągły i dynamiczny proces cyfryzacji logistyki niesie ze sobą liczne korzyści, jednak równolegle z rozwojem

technologii rośnie także liczba zagrożeń związanych z cyberbezpieczeństwem. Systemy logistyczne, zintegrowane z chmurą obliczeniową, Internetem Rzeczy (IoT) oraz sztuczną inteligencją (AI), stają się atrakcyjnym celem dla m.in. cyberprzestępców. Ataki mogą prowadzić do poważnych zakłóceń operacyjnych, strat finansowych oraz naruszenia poufności danych. Do najbardziej znanych cyberzagrożeń w logistyce należy zaliczyć ataki ransomware, czyli zastosowanie złośliwego oprogramowania szyfrującego dane w systemach zarządzania magazynem (WMS) lub transportem (TMS), wymagające okupu za ich odszyfrowanie. Przykładem takiego ataku było zdarzenie z roku 2017 w firmie Maersk, w trakcie którego unieruchomiono systemy globalnej logistyki morskiej. Co więcej, jako zagrożenia dla bezpieczeństwa z obszaru cyber należy rozumieć np. fałszywe e-maile i strony internetowe w celu wyłudzenia danych logowania do systemów logistycznych. Takie działania nazywane są phishingiem i socjotechnikami, które mogą doprowadzić do przejęcia kontroli nad łańcuchem dostaw lub manipulacji danymi dotyczącymi transportu i zapasów.

Kolejnym cyberzagrożeniem są ataki na IoT i inteligentne urządzenia ze względu na coraz większą liczbę procesów logistycznych zarządzanych przez zautomatyzowane systemy i urządzenia podłączone do Internetu. Niewłaściwie lub słabo zabezpieczone sieci mogą stanowić furtkę dla hakerów, którzy mogą np. przejąć kontrolę nad systemami monitorowania przesyłek lub autonomicznych pojazdów (Netbe.pl, b.d.).

Innym zagrożeniem jest złośliwe oprogramowanie (malware) wprowadzane do systemów ERP i SCM. Są to ataki wycelowane w zintegrowane systemy zarządzania łańcuchem dostaw (SCM) lub w systemy planowania zasobów przedsiębiorstwa (ERP). Ich działania mogą skutkować przejęciem kontroli nad procesami logistycznymi i wprowadzeniem nieautoryzowanych zmian w danych operacyjnych przedsiębiorstwa (Bartczak, 2022). Firmy logistyczne często współpracują z wieloma podmiotami zewnętrznymi oraz państwowymi, co zwiększa ryzyko ataków poprzez słabo zabezpieczone systemy partnerów. Przykładem zakłócenia łańcucha dostaw przez cyberatak na dostawcę był atak na firmę SolarWinds, który wpłynął na bezpieczeństwo wielu przedsiębiorstw na całym świecie (Vault-Tech, b.d.). Cyberzagrożenia mogą prowadzić do szeregu negatywnych skutków, takich jak np.: zakłócenia operacyjne – przestoje w magazynach, opóźnienia w dostawach, blokada

systemów śledzenia przesyłek, straty finansowe, koszty związane z usuwaniem skutków ataku, okup w przypadku ransomware, kary umowne za niewywiązanie się z kontraktów, naruszenie poufności danych, wyciek wrażliwych informacji o dostawcach, klientach i trasach transportowych, który może prowadzić do utraty zaufania klientów, manipulacja danymi, zmiana danych dotyczących dostaw, manipulacja trasami transportu czy sabotaż systemów logistycznych może mieć katastrofalne skutki.

Wskazane w tej części opracowania ryzyka zdają się podkreślać słuszność podjętych rozważań. Ryzyko jest stanem, w którym dany czynnik oddziaływujący lub podjęte działanie spowoduje negatywne dla podmiotu konsekwencje, stopień prawdopodobieństwa których jest wysoki. Procesom logistycznym oraz łańcuchom dostaw towarzyszy wiele rodzajów ryzyka, z których większość powoduje powstanie kolejnych, jeśli nie podejmie się adekwatnych działań, celem ich neutralizacji. Obecnie zagrożenia informacyjne zdają się przeżywać swój renesans. Warto podkreślić, że zagrożenia dla bezpieczeństwa informacyjnego mogą też mieć podłoże naturalne (Kitler, 2022). Brak kontroli oraz demokratyczny dostęp do tworzenia i upubliczniania treści użyźnił i zaorał pole pod rozkwit dezinformacji. Stanowi ona zagrożenie w każdym wymiarze bezpieczeństwa. W logistyce również, zarówno w ujęciu kinetycznym, jak i w ujęciu cyberbezpieczeństwa.

Dezinformacja jako wybrane zagrożenie dla logistyki i zarządzania łańcuchem dostaw

Aby przedstawić dezinformację, która obecnie coraz częściej stanowi właśnie cyberzagrożenie w sposób jak najbardziej jasny w opinii autorów, posłużyli się przykładem zarządzania łańcuchem dostaw. Jest to jeden z głównych, często realizowanych i bardzo ważnych, zwłaszcza w aspekcie działań zbrojnych i procesów logistycznych. Przykładów na słuszność tej tezy nie brakuje. W czasie II wojny światowej cele, zasięg oraz czas trwania operacji oraz ofensyw były uzależnione w dużej mierze od sprawności i bezpieczeństwa łańcucha dostaw dla nacierających związków taktycznych i operacyjnych. Niemal całkowite zatrzymanie pochodu Aliantów zachodnich jesienią 1944 r. było spowodowane kłopotami w łańcuchu dostaw. Nie dość, że początek łańcucha dostaw znajdował się nad północnym, francuskim wybrzeżem, to pojawiło się wiele niebezpieczeństw na każdym z jego

ogniw. Równocześnie w środkowej Polsce stanęła ofensywa w ramach operacji *Bagration*. Ten przymusowy postój również w dużej mierze spowodowany był wydłużeniem o kilkaset kilometrów łańcucha dostaw, a także koniecznością odnalezienia odbiorców dostaw i ustalenia, co, komu, ile i gdzie trzeba dostarczyć.

W tym miejscu zasadne wydaje się podkreślić, że jak zauważają Z. Piątkowski oraz W. Żebrowski, należy rozumieć, że logistyka w sferze zaopatrzenia dotyczy przepływów surowców, materiałów, detali, części, półproduktów od dostawców do magazynów zaopatrzeniowych lub magazynów przyjęcia w przedsiębiorstwie lub bezpośrednio do procesu produkcyjnego (Piątkowski, Żebrowski, 2008). Definicji samego łańcucha dostaw w literaturze przedmiotu zawiera wiele. Jest on bardzo często definiowany w kreślonych kontekstach prowadzonych badań. Inaczej definiuje się w aspekcie militarnym, przedsiębiorstw prywatnych, towarów niebezpiecznych czy produktów cyfrowych. W odniesieniu do pojęcia zarządzania również nie brakuje definicji tego procesu w licznych jego kontekstach. Najlepszą formą zdefiniowania procesu zarządzania łańcuchem dostaw, w odniesieniu do cyberzagrożeń i cyberbezpieczeństwa, wydaje się być następujące stwierdzenie. Zarządzanie łańcuchem dostaw to proces planowania, realizacji zaplanowanych działań oraz kontroli tych działań, mających na celu efektywny i wydajny przepływ towarów, surowców, zapasów w drodze oraz niezbędnej informacji i wiedzy z punktu wyjścia do punktu dostawy w celu zaspokojenia potrzeb i wymagań odbiorcy (Janczewski, 2018).

Łańcuch dostaw jest elementem logistyki. Prowadząc rozszerzone rozważania na temat logistyki w aspekcie poznawczym, jak i praktycznym, pominięcie zagadnienia łańcucha dostaw stanowiłoby kardynalne niedopatrzenie. Posiadanie ważnych, aktualnych, wiarygodnych oraz na bieżąco weryfikowanych informacji zdaje się być jednym z głównych narzędzi do ochrony bezpieczeństwa podmiotu. Zarówno w aspekcie zagrożeń tradycyjnych, jak i cyberzagrożeń. W tym momencie rozważań należy uwidocznić, w jaki sposób dezinformacja stanowi obecnie broń w podjętym temacie.

Dezinformacja to zjawisko, element komunikacji werbalnej i niewerbalnej, a także broń. Nie sposób określić moment w dziejach ludzkości, w którym pierwszy człowiek przekazał fałszywą informację w celu umyślnego wprowadzenia kogoś w błąd, a w konsekwencji samemu osiągając

zamierzone korzyści. Można pokusić się o stwierdzenie, iż dezinformacja stanowi stały element stosunków społecznych (w tym również biznesowych), bowiem jest mocno zakorzeniona w przeszłości, obecnie wykorzystywana na skalę jak nigdy wcześniej oraz prognozowanie jej udziału w szeroko pojętej przestrzeni informacyjnej jest raczej słuszne (Dela, 2022). Właśnie demokratyczny dostęp do przestrzeni informacyjnej innego przedsiębiorstwa logistycznego, zwłaszcza w obszarze cyber i poprzez Internet, daje możliwość upubliczniania w niej dowolnego rodzaju treści skierowanych do innych realizatorów łańcucha dostaw oraz innych procesów logistycznych, co stanowi narzędzie *par excellence* dla eskalacji skuteczności dezinformacji (Mogilnicki, 2024).

Dezinformację można rozumieć zarówno jako stan, jak i proces. Można ją stosować z wykorzystaniem różnorakich metod, zarówno oddzielnie, jak i synchronicznie (Brühl, 2019). Wszystko zależy od tego, zarówno w stanie, jak i w procesie, która forma jest bardziej korzystna. Proces dezinformowania, mający doprowadzić do stanu dezinformowania, wymaga stosowania dezinformacji jako działań (Osiecki, 2023): zaplanowanych, sprowadzających się do spreparowania i dostarczania odbiorcom informacji lub innego rodzaju danych częściowo lub w pełni fałszywych, realizowanych w cyberprzestrzeni, rozumianej jako obszar przetwarzania, publikowania i wymiany informacji z wykorzystaniem odpowiednich urządzeń i oprogramowania, posiadającej ukryty, znany tylko twórcy dezinformacji, cel.

W kontekście cyberbezpieczeństwa w logistyce i bezpieczeństwa łańcuchów dostaw te dwie opcje rozumienia dezinformacji, jawią się następująco. Dezinformacja jako stan odnosiła się do sparaliżowania zarządzania łańcuchem dostaw oraz innych procesów logistycznych w przeszłości. Innymi słowy, ten paraliż już się dokonał i trwa. Natomiast dezinformacja jako proces to wszystkie działania realizowane w czasie teraźniejszym jak i te zaplanowane na przyszłość. Są one ukierunkowane na doprowadzenie do przerwania łańcucha dostaw oraz uniemożliwienie zarządzania nim. Żadne z wielu pojedynczych działań nie spowoduje tego, lecz ujęte w zorganizowanych procesach dezinformowania już tak. Zarówno w aspekcie tradycyjnych zagrożeń bezpieczeństwa, jak i w aspekcie cyberzagrożeń.

Dezinformacja obecnie stanowi poważne zagrożenie dla skutecznego zarządzania łańcuchem dostaw, a także dla logistyki. Współczesność, jak

dowodzi praktyka, nie ograniczyła się jeszcze do działań jedynie w domenie cybernetycznej, ale ta domena odgrywa i będzie odgrywać coraz większą i ważniejszą rolę. W systematycznym budowaniu przewagi niekinetycznych cyfrowych form, metod i technik wykorzystania dezinformacji jako broni, pomaga wykorzystanie narzędzi opartych na sztucznej inteligencji. Aby przedstawić to zagadnienie, posłużono się opisami hipotetycznych, lecz bardzo prawdopodobnych sytuacji, jakie mogą mieć miejsce w rzeczywistości.

Po pierwsze, wykorzystanie dezinformacji może doprowadzić do przerwania łańcucha dostaw oraz spadku jego wydajności. W procesie działań dezinformacyjnych określone grupy dywersyjne mogą zniszczyć lub przestawiać znaki drogowe. To natychmiast i znacznie zakłóci zarządzanie łańcuchem dostaw i same dostawy, generując jednocześnie dodatkowe koszty, bo kierowcy będą spalać paliwo, aby wrócić na właściwą trasę przejazdu. W transporcie kolejowym lub lotniczym bardzo podobnie. Dodatkowo, jeśli maszynista otrzyma informację fałszywą (dezinformację), może ustawić lokomotywę na złym torze i zabrać zaopatrzenie przeznaczone dla odbiorcy „A", które zawiezie odbiorcy „B". Takie sytuacje wręcz paraliżują proces zarządzania łańcuchem dostaw oraz sam łańcuch. Opóźnienia oraz dodatkowe koszty mogą być gargantuiczne. Dodatkowo mogą mieć znaczny wpływ na wartości i cele najwyższe, takie jak bezpieczeństwo państwa. Zakłócenie lub paraliż łańcucha dostaw broni, amunicji, żołnierzy lub medykamentów do rejonu prowadzenia działań zbrojnych może mieć katastrofalne i nieodwracalne skutki.

Po drugie, wykorzystanie dezinformacji, w oparciu o sztuczną inteligencję może doprowadzić do likwidacji łańcucha dostaw, nawet przez podmiot od tegoż łańcucha uzależniony. Program o nazwie *Deepfake* zdaje się być jednym z obecnie najbardziej powszechnych oraz niebezpiecznych narzędzi. Ten program, który wykorzystuje sztuczną inteligencję, jest w stanie wytwarzać produkty audiowizualne, odtwarzające bardzo wiarygodnie wygląd oraz głos konkretnych osób. Wytworzenie np. filmu, w którym przedstawiciel podmiotu „A" zwraca się do przedstawiciela podmiotu „B" i wypowiada mu kontrakt na dostawy ekstremalnie ważnych surowców, urządzeń lub towarów. Utracenie dostaw w krótkim czasie doprowadzi do upadku podmiotu „A", który na dodatek będzie jeszcze musiał zapłacić karę

podmiotowi „B". Jeśli ktoś nie zorientowałby się, że to mistyfikacja i dywersja, doszłoby do wspomnianych skutków, a zorientowanie się wcale nie jest proste.

Po trzecie, dezinformacją można doprowadzić do przerwania łańcucha dostaw, poprzez samych jego realizatorów. Wszak w obecnym świecie, głównymi celami dezinformacji stały się społeczeństwa, które zajęły miejsce dowódców wojskowych, prominentnych polityków oraz wpływowych grup obywateli. Poprzez wykorzystanie sztucznej inteligencji do szerzenia informacji, można zasypać wręcz pracowników przedsiębiorstw logistycznych spreparowanymi treściami, które wywołają co najmniej strajk. Wykorzystanie trudnego okresu finansowego, żeby wtedy rozpowszechnić treści (np. wytworzone przez *Deepfake*), które informowałyby o lekkomyślnym rozporządzaniu aktywami przedsiębiorstwa, zamiast podnieść płace pracownikom, to recepta właśnie na to. Zasadnym wydaje się stwierdzić, że ochrona realizatorów łańcucha dostaw przed dezinformacją, to de facto ochrona samego łańcucha dostaw. Bezpieczeństwo informacyjne ludzi odpowiedzialnych za łańcuch, determinuje zarówno pośrednio, jak i bezpośrednio bezpieczeństwo łańcucha dostaw oraz innych procesów logistycznych.

Dezinformacja stanowi obecnie coraz poważniejsze zagrożenie dla bezpieczeństwa we wszystkich jego wymiarach, w tym także w branży logistycznej. To zagrożenie, choć powstało i wyewoluowało w prawdziwym świecie, obecnie jest spotykane głównie w przestrzeni cyfrowej. Sztuczna inteligencja to ogromne osiągnięcie techniki, ale też katalizator częstotliwości, kreatywności i liczby, z jaką dezinformacja jest szerzona. Dlatego warto się przyjrzeć, w jaki sposób może być wykorzystana w cyberbezpieczeństwie logistyki.

Sztuczna inteligencja w cyberbezpieczeństwie logistyki

Wskazano już, jak dużo zależy od bezpieczeństwa łańcucha dostaw, który jest elementem logistyki. O ile w tradycyjnym rozumieniu bezpieczeństwa logistyki i zagrożeń w logistyce trudno jest cokolwiek nowego wskazać, o tyle w aspekcie cyberbezpieczeństwa zdecydowanie tak. Tradycyjne, czyli kinetyczne, i inne już znane zagrożenia dla logistyki zostały już gruntownie zbadane. Zasadnym wydaje się wskazać, że mogą pojawić się nowe formy, lecz już nazwane i usystematyzowane typy zagrożeń logistycznych

stanowią prawie katalog zamknięty. Zupełnie inaczej ma się to w aspekcie zapewnienia cyberbezpieczeństwa w branży logistycznej, a także wykorzystania do tego sztucznej inteligencji. Bezpieczeństwo cyberprzestrzeni, czyli innymi słowy cyberbezpieczeństwo w ujęciu holistycznym, to brak ryzyka utraty danych lub informacji przechowywanych w cyberprzestrzeni (Pacek, Hoffmann, 2013). Można zatem stwierdzić, jak wykazuje praktyka, że jest to połączenie różnych narzędzi, technik oraz środków reagowania i ochrony danych nie tylko przed ich kradzieżą i utratą, ale też przed manipulowaniem ich treścią.

Zdaniem autorów, cyberbezpieczeństwo to stan braku zagrożeń utratą, kradzieżą oraz manipulacją danych przechowywanych trwale przez podmiot, a także brak zagrożenia manipulacją i kreowaniem własnej przestrzeni informacyjnej przez inny podmiot, za sprawą wykorzystania do tego narzędzi, metod oraz technik cyfrowych w przestrzeni cybernetycznej. Stan ten osiągany jest w wyniku realizacji procesów okresowych oraz ciągłych, mających na celu zbudowanie zdolności ochrony przed cyberzagrożeniami, a także stałe monitorowanie przestrzeni informacyjnej w poszukiwaniu destrukcyjnych i innych niepożądanych działań w tejże przestrzeni.

A zatem cyberbezpieczeństwo w logistyce należy rozumieć jako stan, w którym procesy logistyczne, cyfrowe dane niezbędne do niezakłóconej ich realizacji, a także ich planowania oraz ich kontrolowania pozostają wolne od zagrożeń, zarówno tych typowo cybernetycznych, jak i innych, które mogą być wywołane działaniami w cyberprzestrzeni (Microsoft, b.d.).

Tak jak wspomniano wcześniej, sztuczna inteligencja (AI) może generować i być narzędziem do wytwarzania zagrożeń dla cyberbezpieczeństwa w logistyce, a też może wspomagać utrzymywanie i polepszanie tego wymiaru bezpieczeństwa jako stanu. Obecnie coraz częściej powstają nowe programy, algorytmy oraz sposoby wykorzystania sztucznej inteligencji w procesie dbania o cyberbezpieczeństwo. Niektóre z nich ukierunkowane są na wykrywanie i zwalczanie pojawiających się zagrożeń, nawet stosując metaforyczny ogień kontrbateryjny, czyli niszcząc zdolności innego dezinformacyjnego programu czy algorytmu. Jednakże wykorzystanie sztucznej inteligencji, zwłaszcza w logistyce, nie ogranicza się jedynie do tego. Może być ona równie pożytecznie wykorzystywana w bieżącej obsłudze centrów logistycznych oraz np. w zarządzaniu łańcuchami dostaw. W kontekście

centrów logistycznych, znajduje ona zastosowanie np. w optymalizacji przestrzeni magazynowej, zarządzaniu zapasami zgromadzonymi w magazynach centrów logistycznych, przydzielaniu zadań pracownikom centrów logistycznych oraz poprawie efektywności tras na terenie samego magazynu, co przekłada się na efektywniejsze i bezpieczniejsze funkcjonowanie całego łańcucha dostaw. Natomiast w kontekście zarządzania łańcuchem dostaw, korzyści zastosowania sztucznej inteligencji, zdają jawić się następująco: ułatwia rutynową komunikację, zarówno w komunikacji wewnętrznej oraz z podmiotami zewnętrznymi, może udzielać automatycznie odpowiedzi na zapytania, które wprowadzane do systemu zintegrowanego z nią pojawiają się dość często, a odpowiedzi na nie zazwyczaj są podobne, potwierdza zamówienia i aktualizuje statusy dostaw, co skutecznie usprawnia komunikację i ogranicza opóźnienia w procesach, przyspiesza planowanie przepływów logistycznych w różnych horyzontach czasowych i przekrojach, skuteczniej koordynuje procesy logistyczne oraz inne operacje oraz prowadzi stały monitoring procesów logistycznych (Mroczko, 2023).

Biorąc pod uwagę zawarte powyżej wybrane możliwości zastosowania sztucznej inteligencji w logistyce oraz zarządzaniu łańcuchem dostaw, zasadnym wydaje się wskazać, jakie korzyści dla przedsiębiorstwa logistycznego oraz procesu zarządzania łańcuchem dostaw płyną za sprawą wykorzystania tego cybernetycznego narzędzia. Oczywiście, zachowując kontekst niniejszego opracowania, autorzy wymieniają jedynie te, które mają wpływ na cyberbezpieczeństwo, ale oddziałują na kluczowe aspekty w logistyce determinujące jej skuteczność. A są to: wyeliminowanie błędu ludzkiego, przy planowaniu zagospodarowania przestrzeni magazynowej, wyeliminowanie błędu ludzkiego przy obliczeniach stanu zapasów zgromadzonych w magazynie, wyeliminowanie ryzyka korupcji pracowników odpowiedzialnych lub biorących udział w realizacji procesów logistycznych, która może skłonić nich do szeroko rozumianego sabotażu, przydzielanie zadań pracownikom, w oparciu o znajomość wszystkich ich kompetencji, odnotowanych w systemie cyfrowym, a także precyzyjny ich dobór po porównaniu ze sobą co najmniej dwóch pracowników o podobnych ale nieidentycznych kompetencjach, prowadzone przez sztuczną inteligencję pojazdy na terenie magazynu wykonują przewóz towarów efektywniej oraz z większą częstotliwością w badanym czasie, niż gdy prowadzi je człowiek, odciąża i nie marnuje

czasu pracowników odpowiedzialnych za komunikację i aktualizację statusu dostaw, samodzielnie obsługuje systemy i nie dopuszcza się metod ani czynności (wchodzenia na niebezpieczne strony internetowe służbowym komputerem), które generują ryzyko oddziaływania cyberzagrożeń, wykrywa odpowiedzi udzielne na zapytania kierownictwa do realizatorów łańcucha dostaw, które są niezgodne z ustalonymi standardami, przez co natychmiast może zaalarmować o nieprawidłowości odpowiednią komórkę organizacji, może szybko i trafnie przewidywać potencjalne zagrożenia dla planu realizacji konkretnego łańcucha dostaw, w oparciu o całą wiedzę globalnej sieci internetowej, do której jest podłączona, analizuje i koreluje dane dotyczące zdarzeń w cyberprzestrzeni i cyberzagrożeń z wielu źródeł, przekształcając je w jasne i praktyczne szczegółowe informacje używane przez analityków ds. zabezpieczeń do dalszego badania i ograniczania ryzyka cyberataków.

Przedstawione możliwości wykorzystania sztucznej inteligencji w zapewnianiu cyberbezpieczeństwa logistyki, procesu zarządzania łańcuchem dostaw oraz bieżącego prowadzenia działalności centrum logistycznego, rzecz jasna, nie zawierają wszystkich możliwych jej zastosowań. Jednakże zasadnym wydaje się wskazać, że zbiór możliwości tutaj zaprezentowany, może śmiało stanowić wstęp i punkt wyjścia do dalszych badań nad rolą sztucznej inteligencji w cyberbezpieczeństwie logistyki oraz zarządzania łańcuchem dostaw.

Przyszłość cyberbezpieczeństwa w logistyce

Stałą w obszarze obronności wielu państw świata jest to, że przygotowują się do odparcia ataku, prowadzenia wojny oraz zgromadzenia zapasów i produkcji bieżącej w takich ilościach, jakie były niezbędne ostatnio, tj. w czasie ostatniej wojny tych państw. Cyberbezpieczeństwo, choć stosunkowo niedawno usystematyzowane, jest znacznie starsze od sztucznej inteligencji. Mogłoby się tak wydawać, jeśli rozumiemy je jako brak zagrożeń i ryzyka utraty ważnych informacji danej organizacji drogą cyfrową. Wykorzystywanie najnowocześniejszych w danym momencie technologii w działalności przedsiębiorstw, np. logistycznych, czy w obronności państwa nie jest niczym nowym. Oczywiście, w kontekście ochrony przed nieuprawnionym dostępem do treści planów, raportów z realizacji zadań,

danych osobowych personelu organizacji i wielu innych podobnych, przełomowe i bezpieczne technologie już powstawały.

Zatem, odpowiadając na pytanie problemowe opracowania, należy wskazać dwa procesy, które wydają się niezbędne do przygotowania branży logistycznej w aspekcie bezpieczeństwa, pod kątem rozważań zawartych w tym opracowaniu.

Po pierwsze, należy uświadomić całą branżę w ujęciu personalnym, a także na etapie edukacji uświadamiać młodych adeptów logistyki, na temat zagrożeń cyberbezpieczeństwa logistyki oraz zarządzania łańcuchami dostaw. Świadomość istnienia, fundamentalnych zasad działania i najczęstszych celów stosowania konkretnych typów zagrożeń, to inherentna część systemu odporności przed nimi.

Po drugie, należy już na etapie projektowania nowych cyfrowych systemów planowania, realizacji oraz nadzoru procesów logistycznych przewidywać włączenie w ich obsługę sztucznej inteligencji. Zdecydowanie ergonomicznie jest obsługiwać i przebywać w pojazdzie opancerzonym, który ma przewidziane miejsce na ewentualny, np. karabin maszynowy, czyli coś długiego, o pewnej szerokości, wyrzucający przedmioty (łuski) tylko w jednym możliwym kierunku, i można się o to jeszcze oparzyć. Przewidzenie włączenia sztucznej inteligencji do obsługi systemów logistycznych nie tylko nie spowoduje zakłóceń, np. w zarządzaniu łańcuchem dostaw, ale również skróci czas, w którym pewne podmioty mogłyby przypuścić cyberatak w związku z niepoprawnym działaniem systemu podczas czas dostosowywania go do sztucznej inteligencji.

Po trzecie, należy zoptymalizować czynnik ludzki z cyfrowym, aby zarówno ludzie nie bali się sztucznej inteligencji w swojej pracy, jak i sztuczna inteligencja przewidywała pewną tolerancję błędu, gdyż nadzoruje nie inny system, ale ludzi. Należy zrównoważenie budować podejście do sztucznej inteligencji w branży logistycznej, aby ona i ludzie ze sobą współpracowali, a nie rywalizowali. Tutaj też trzeba nadmienić świadomość. Koniecznym wydaje się dążenie do takiego stanu, w którym personel rozumie i widzi, że sztuczna inteligencja skutecznie dba o bezpieczeństwo ich pracy, również w obszarze cyberbezpieczeństwa. Postrzeganie przez branżę logistyczną w ujęciu personalnym sztucznej inteligencji jako zagrożenia spowoduje zwalczanie jej poprzez próby sabotażu jej poleceń. W efekcie

ani personel ani sztuczna inteligencja nie będą efektywne. Ucierpi na tym organizacja jako całość. Jak wynika z doświadczeń wojennych, np. w naszym kraju, gdzie dwóch się bije, tam korzysta partyzant. W rozpatrywanym kontekście takie zwalczanie się wytworzy dogodne warunki do ataków zewnętrznych na organizację, w tym w obszarze cyber. Konflikty wewnętrzne, niepokoje społeczne oraz dysfunkcyjność to okoliczności par excellence dla dezinformacji oraz katalizatory jej skuteczności.

Do głównych strategii ochrony przed cyberzagrożeniami w logistyce, zdaniem autorów, należy zaliczyć: zwiększenie świadomości pracowników poprzez szkolenia z zakresu cyberbezpieczeństwa oraz stosowanie polityk dotyczących bezpiecznego korzystania z poczty e-mail i systemów IT, segmentację sieci IT/OT, czyli oddzielenie systemów operacyjnych (OT) od klasycznych systemów IT, w celu ograniczenia możliwości rozprzestrzeniania się ataków. Regularne aktualizacje i łatki bezpieczeństwa, najnowsze wersje oprogramowania oraz systemów operacyjnych, które eliminują luki w zabezpieczeniach, monitorowanie zagrożeń i szybka reakcja poprzez wdrażanie systemów detekcji anomalii i SIEM (Security Information and Event Management) w celu wykrywania podejrzanych aktywności. Zabezpieczenie dostępu do systemów logistycznych poprzez stosowanie uwierzytelniania wieloskładnikowego (MFA), silnych haseł oraz ograniczonego dostępu do kluczowych systemów oraz backup danych, czyli tworzenie regularnych kopii zapasowych i ich przechowywanie w sposób odseparowany od głównej infrastruktury IT.

Podsumowanie

Współczesna logistyka, oparta na cyfryzacji i integracji systemów IT, jest coraz bardziej narażona na cyberzagrożenia. Ataki mogą prowadzić do poważnych zakłóceń operacyjnych, strat finansowych oraz naruszenia poufności danych. Dlatego też przedsiębiorstwa logistyczne muszą nieustannie inwestować w strategie cyberbezpieczeństwa, szkolenia pracowników oraz zaawansowane systemy ochrony, aby minimalizować ryzyko ataków i zapewnić stabilność operacyjną łańcucha dostaw. Kluczowa wydaje się być świadomość cyberzagrożeń oraz ukierunkowanie sztucznej inteligencji nie tylko na bieżące wsparcie procesów logistycznych, ale też na wykrywanie i przeciwdziałanie cyberzagrożeniom. Jednym z głównych zagrożeń dla

współczesnej logistyki, poza atakami cybernetycznymi, zdaje się być dezinformacja. Zarówno dla logistyki cywilnej, jak i wojskowej. Zatem, aby osiągnąć cyberbezpieczeństwo w tym obszarze, charakteryzujące się wysokim stopniem doskonałości, należy podejmować wiele różnych oraz nowych działań, jakie zostały ukazane w tym opracowaniu. Pełna synergia personelu ze sztuczną inteligencją wydaje się być determinującym czynnikiem rozwoju i szerszego stosowania jej w branży logistycznej. Stanowić ona musi narzędzie wspomagające, a nie eliminujące czynnika ludzkiego. Tylko wtedy będzie możliwy do wykorzystania cały jej potencjał. Zarówno w aspekcie poznawczym, jak i praktycznym. Zaproponowane działania przygotowawczo-edukacyjne zdają się dowodzić hipotezy postawionej przez autorów. Lecz wymagają one dużej finezji oraz jeszcze większej wiedzy ich realizatorów. Powierzchowne i niedokładne ich zrealizowanie na pewno nie poprawi poziomu cyberbezpieczeństwa w logistyce.

Literatura

1. Arvato. (b.d.). *Logistyka kiedyś i dziś: Ewolucja czy rewolucja*? Pobrane z: https://blog.arvato.pl/logistyka-kiedys-i-dzis-ewolucja-czy-rewolucja (dostęp: 24.02.2026).
2. Barcik, R., Odlanicka-Poczobutt, M. (2020). *Logistyka 4.0 – wybrane zastosowania*. Politechnika Śląska.
3. Bartczak, K. (2022). Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście cyfrowych platform technologicznych w logistyce. *Autobusy: Technika, Eksploatacja, Systemy Transportowe, 23*(12), 123-128.
4. Bielecki, M. (2022). *Total logistic management: Logistyka i łańcuchy dostaw 4.0.* Uniwersytet Łódzki.
5. Brühl, M. (2019). Wiedza a dezinformacja w społeczeństwie. W: A. Szczygielska (red.), *Zarządzanie wiedzą w kontekście zapewnienia bezpieczeństwa państwa* (s. 129-142). Akademia Sztuki Wojennej.
6. Dela, P. (2022). Informacja jako narzędzie i obiekt ataku w cyberprzestrzeni. W: W. Scheffs (red.), *Konteksty teoretyczne i praktyczne informacji w organizacji* (s. 279-300). Akademia Kaliska.
7. Ivanov, D., Dolgui, A., Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics.

International Journal of Production Research, 57(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

8. Janczewski, J. (2018). Zarządzanie łańcuchem dostaw. *Zarządzanie Innowacyjne w Gospodarce i Biznesie, 1*(26), 163-179.
9. Kitler, W. (2022). Przygotowanie systemu kierowania bezpieczeństwem narodowym RP: Zadania i organizacja administracji rządowej szczebla centralnego. *Wiedza Obronna, 278*(1), 11-34.
10. Microsoft. (b.d.). *Co to jest AI dla cyberbezpieczeństwa*? Pobrane z: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-ai-for-cybersecurity (dostęp: 24.02.2026).
11. Mogilnicki, M. (2024). Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą. *Cybersecurity and Cybercrime, 1*(4), 272-280.
12. Mroczko, F. Kowalczyk L., Mroczko F. (red.). (2023). *Prace naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu*, *53.* Wyższa Szkoła Zarządzania i Przedsiębiorczości.
13. Netbe.pl. (b.d*.). Specyfika ataków na urządzenia IoT: Jakie zagrożenia wiążą się z Internetem Rzeczy?* Pobrane z: https://netbe.pl/specyfika-atakow-na-urzadzenia-iot-jakie-zagrozenia-wiaza-sie-z-internetem-rzeczy/ (dostęp: 24.02.2026).
14. Orłowska, M. (2023). SAP ERP software as a tool for managing the logistics subsystems of an enterprise. *Zeszyty NaukowebPolitechniki Śląskiej. Organizacja i Zarządzanie, XXX*, 515-526.
15. Orłowska, M., Orłowski, D. (2024). Wyzwania i możliwości zastosowania dronów w logistyce miejskiej. *Gospodarka Materiałowa i Logistyka, 76*(3), 69-79.
16. Osiecki, M. (2023*).* Dezinformacja jako źródło współczesnych cyberzagrożeń. W: M. Marczyk, M. Stolarz, B. Terebiński (red.), *Cyberbezpieczeństwo w teorii i praktyce: Wybrane aspekty* (s. 199-210). Akademia Sztuki Wojennej.
17. Pacek, B., Hoffmann, R. (2013). *Działania sił zbrojnych w cyberprzestrzeni*. Akademia Obrony Narodowej.
18. Piątkowski, Z., Żebrowski, W. (2008). Logistyka w sferze zaopatrzenia. *Postępy Techniki Przetwórstwa Spożywczego,18* (2), 115-121.
19. Płaczek, E. (2018). Logistyka w erze Industry 4.0. *Przedsiębiorczość i Zarządzanie, 19*(11.3), 55-66.

20. RedSteel. (b.d.). *Logistyka 4.0 – trudne wyzwanie czy szansa na rozwój*? Pobrane z: https://redsteel.pl/logistyka-4-0-trudne-wyzwanie-czy-szansa-na-rozwoj/ (dostęp: 24.02.2026).
21. Sokołowska, M. (2024). Logistyka 4.0: *Powiedzmy sobie, o co tak naprawdę chodzi.* Pobrane z: https://www.trans.eu/pl/blog/logistyka-4-0/logistyka-4-0-powiedzmy-sobie-o-co-tak-naprawde-chodzi/ (dostęp: 24.02.2026).
22. Tjahjono, B., Esplugues, C., Ares, E., Pelaez, G. (2017). What does Industry 4.0 mean to supply chain? *Procedia Manufacturing, 13*, 1175-1182. https://doi.org/10.1016/j.promfg.2017.09.191
23. Vault-Tech. (b.d.). *Supply chain attack: Tak ataki na dostawców zagrażają bezpieczeństwu firm*. Pobrane z: https://vault-tech.pl/cyberbezpieczenstwo/supply-chain-attack/ (dostęp: 24.02.2026).

Zbigniew Piskor[1]
Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103373_16

EWOLUCJA CYBERZAGROŻEŃ TRANSPORTU LOTNICZEGO

THE EVOLUTION OF CYBER THREATS TO AIR TRANSPORT

Streszczenie

Rozdział porusza problematykę cyberzagrożeń w lotniczych systemach informatycznych jako ważnego czynnika prowadzącego do zagrożeń dla bezpieczeństwa transportu lotniczego, wykorzystującego urządzenia IT do prowadzenia większości swoich operacji przez internet. Na świecie obserwuje się stały wzrost liczby cyberataków na wszystkie sektory działalności lotniczej. Operacje w sieci muszą być chronione przy użyciu kompleksowych przepisów dotyczących cyberbezpieczeństwa. Celem jest analiza wpływu tego typu ryzyka na poziom bezpieczeństwa w transporcie lotniczym. Stosownie do przyjętego celu sformułowano główny problem badawczy: Jak niepoprawne działania w korzystaniu z urządzeń IT powodowane przez organizacje wpływają na poziom cyberbezpieczeństwa transportu lotniczego? Uzyskanie odpowiedzi na powyższe pytanie wymagało zastosowania metod badawczych, w tym dokonania krytycznej analizy aktów prawnych i wybranych pozycji literatury przedmiotu. Przeprowadzona analiza wskazuje, że aby poprawić działalność branży i organizacji lotniczych, należy rozważyć wprowadzenie odpowiednich

[1] https://orcid.org/0000-0002-4456-1104, e-mail: zbpis@wp.pl

środków oraz przyjąć wyznaczone kierunki zmian. Tezę tę potwierdzają statystyki zdarzeń cybernetycznych oraz liczne działania podejmowane przez państwa w celu zwalczania cyberzagrożeń.

Słowa kluczowe: cyberzagrożenia, lotnictwo, bezpieczeństwo, ochrona, statki powietrzne

Abstract

The article addresses the issue of cyber threats to aviation IT systems as an important factor contributing to security risks in air transport, which relies on devices to conduct most of its operations over the Internet. Worldwide, there is a steady increase in cyberattacks across all sectors of aviation activity. Network operations must be protected using comprehensive cybersecurity regulations. The goal is to analyse the impact of this type of security-related risk on security-related proceedings in air transport. In accordance with the adopted objective, the main research problem was formulated as follows: How do improper actions in the use of IT devices by the organisation affect the level of cybersecurity in air transport? Obtaining an answer to the above question required applying research methods, including a critical analysis of legal acts and selected literature in the field. The analysis of the indicated areas shows that to improve the operations of the aviation industry and organisations, it is necessary to implement appropriate measures and adopt the designated directions of change. This thesis is supported by statistics on cyber incidents and by numerous actions taken by countries to combat cyber threats.

Keywords: cybersecurity, hazards, aviation, safety, security, plane

Wstęp

Cyberprzestrzeń stanowi nieodłączny komponent współczesnego świata. Globalne lotnictwo ze swoją infrastrukturą cyfrową charakteryzuje się rozległymi wzajemnymi powiązaniami i złożonością oraz wysokim poziomem ekspozycji w mediach społecznych, a także kluczową rolą w rozwoju społeczno-gospodarczym krajów i państw. Poziom globalnych wzajemnych połączeń systemów i sieci stwarza bezprecedensowy rozwój technologicznych instrumentów charakteryzujących się powiązaniami i złożonością szeregu transformacji w wykorzystaniu mocy technologii w celu zwiększenia wydajności w przepływie danych, które wykraczają poza granice państw. Przeciwdziałanie zagrożeniom i ryzykom dla lotnictwa musi opierać się na współdziałaniu i współpracy między wszystkimi zainteresowanymi stronami.

W tym celu idealnym dla społeczności lotniczej jest Międzynarodowa Organizacja Lotnictwa Cywilnego przy ONZ która podejmując wysiłki na rzecz cyberbezpieczeństwa w lotnictwie były spójne, zharmonizowane, zgodne z priorytetami międzynarodowego lotnictwa cywilnego i obejmujące:

- opracowywanie (SARP) norm i zalecanych metod postępowania załącznika 17 – Ochrony lotnictwa cywilnego (Konwencja o międzynarodowym lotnictwie cywilnym, 1944),
- zapewnieniu, aby ramy międzynarodowego prawa lotniczego były odpowiednie do przeciwdziałania cyberatakom na lotnictwo cywilne,
- wspieranie dyskusji o cyberbezpieczeństwie w lotnictwie na szczeblu globalnym, regionalnym i krajowym,
- rozwijanie inicjatyw wspierających budowanie, wdrażanie zdolności z zakresu cyberbezpieczeństwa lotniczego dla społeczności lotniczej,
- podnoszenie świadomości na temat znaczenia rozwiązywania problemu ochrony cyberprzestrzeni dla lotnictwa cywilnego.

Strategia cybernetycznego bezpieczeństwa w lotnictwie stanowi podstawę wizji ICAO z którą globalne cywilne lotnictwo ma być odporne na cyberataki i wprowadzać innowacje. Zbudowana jest na siedmiu filarach:

1. Polityka w zakresie bezpieczeństwa cybernetycznego.
2. Przepisy ustawowe i wykonawcze.
3. Zarządzanie.
4. Zarządzanie incydentami, planowanie awaryjne.
5. Budowanie zdolności, szkolenia i kultury cyberbezpieczeństwa.
6. Współpraca międzynarodowa.
7. Wymiana informacji.

Rozwiązywanie problemu cyberbezpieczeństwa w cywilnym lotnictwie stało się na forum ICAO kwestią bezprecedensową najwyższej rangi, określone poprzez rezolucje Zgromadzenia:

- A39-19, dotyczącej cyberbezpieczeństwa w lotnictwie cywilnym – 2016 rok,
- A40-10, dotycząca problemu cyberbezpieczństwa w lotnictwie cywilnym – 2019 rok,
- A41-19, dotyczącej cyberbezpieczeństwa w lotnictwie cywilnym – 2022 rok,

zawierające klauzule, które uznają wzajemne powiązania między bezpieczeństwem, efektywnością, zarządzaniem, współpracą i współdziałaniem w rozwiązywaniu tak istotnych zagadnień w przeciwdziałaniu cyberatakom na lotnictwo cywilne. Wezwano państwa członkowskie do przyjęcia i wdrożenia Konwencji Pekińskiej z 2010 roku oraz Protokołu Pekińskiego (Żylicz, 2002; International Civil Aviation Organization, 2022).

Europejska Agencja Bezpieczeństwa Lotniczego opublikowała wymagania dotyczące zarządzania ryzykiem informacji – Rozporządzenie Part-IS, w którym zamieszczono wytyczne dostosowania Systemów Zarządzania Bezpieczeństwem Informacji opartych o ISO 27001. Rozporządzenie ma zastosowanie do organów odpowiedzialnych za certyfikację i nadzór nad organizacjami lotniczymi mogącymi mieć wpływ na bezpieczeństwo lotnicze. Ochrona poufności i integralności danych technologii informacyjnych wykorzystywanych w lotnictwie cywilnym. Jako kluczowy element kompleksowej strategii cyberbezpieczeństwa ma zastosowanie do różnych obszarów lotnictwa, podkreślając znaczenie informacji w lotnictwie. Nakłada na nadzory lotnicze oraz organizacje obowiązek stworzenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Organizacje powinny również spełniać wymagania NIS2 (Parlamentu Europejskiego). EASA Part IS oznacza wymagania dotyczące systemu zarządzania bezpieczeństwem informacji określone w rozporządzeniach Unii Europejskiej: Rozporządzenie Delegowane 2022/1645 i Rozporządzenie Wykonawcze 2023/203. Nadrzędnym celem ISMS jest kontrola ryzyka związanego z bezpieczeństwem informacji. Standardem dla ISMS jest ISO/IEC 27001:2022 oraz ISO/IEC 22301, których celem jest zmniejszenie prawdopodobieństwa wystąpienia zakłóceń w przypadku sytuacji kryzysowej, przygotowanie się na ewentualne zakłócenia i posiadanie zdolności do skutecznego reagowania na zakłócenia lub odtworzenia działania w określonym czasie, na wyznaczonym poziomie sprawności organizacji. Norma ISO 31000 Zarządzanie Ryzykiem stanowi wsparcie poprzez zbiór zasad i wytycznych, dobrych praktyk, które należy zastosować w celu utrzymania i udoskonalania skuteczności procesu zarządzania ryzykiem (Syta, 2025, s. 122). Raport dotyczący Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), uzupełnia obecny system zarządzania bezpieczeństwem w zakresie bezpieczeństwa informacji elementami:

- zarządzanie ryzykiem związanym z bezpieczeństwem informacji,
- obsługą incydentów związanych z informacjami,
- obsługą zgłaszanych zdarzeń związanych z bezpieczeństwem informacji,
- strategią zarządzania bezpieczeństwem informacji w branży lotniczej.

Ma na celu ustanowienie najlepszych praktyk w zapewnieniu spójności informacji oraz zmniejszenie nakładów związanych z audytem dla zainteresowanych stron. Ma również na celu dostarczenie dodatkowych wytycznych do Part-IS: Acceptable Means of Complince (AMC) & Guidance Materials (GM). Rozporządzenie Part IS jest obowiązujące dla DOA, POA, lotnisk i operatorów lotniskowych od 16.10.2025. Dla Władzy Lotniczej i pozostałych organizacji lotniczych od 22.02.2026 roku.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, świadczenie usług cyfrowych i kluczowych poprzez osiągnięcie poziomu bezpieczeństwa systemów informacyjnych do świadczenia usług oferowanych, zapewnienie obsługi zgodnie z obowiązującymi ustawami w ww. zakresie przez CSIRT GOV, MON, NASK.

Cyberbezpieczeństwo staje się priorytetem dla gospodarki narodowej, stanowi kluczowy temat, który obejmuje w całej branży ochronę systemów informatycznych portów lotniczych, przewoźników lotniczych, danych pasażerów, krytycznej infrastruktury lotniczej przed cyberzagrożeniami. Świat lotniczy we wszystkich aspektach wszedł w nowoczesne technologie informatyczne, a co za tym idzie, również w zagrożenia cybernetyczne. Według prognoz Międzynarodowego Zrzeszenia Przewoźników Powietrznych IATA transport lotniczy kreuje i przyspiesza procesy globalizacji. Wraz z technologią informacyjną określany jest mianem fundamentu i filaru podstawy, przy czym sam tym procesom podlega. Nowe technologie wiążą się z koniecznością zabezpieczenia przed cyberatakami. Społeczne synonimy definiowane jako branżowy zestaw wartości, odczuć, przekonań, a także zachowań organizacji odnoszących się do problemu bezpieczeństwa. Muszą się opierać na wysokim poziomie szacunku i zaufania na linii przełożony–podwładny. Działania te powinny sprowadzać się do pragmatycznych formuł w zakresie kultury elastyczności, sprawiedliwego traktowania, raportowania i uczenia się.

Priorytetyzacja działań prewencyjnych pozwala na lepsze przewidywanie przyszłych zagrożeń, efektywniejszą reakcję już na zaistniałe zdarzenia i incydenty. Poznanie przeciwnika jest fundamentem nowoczesnej cyberobrony.

Sytuacja geopolityczna w transporcie lotniczym

Komunikacja lotnicza jest najdynamiczniej rozwijającą się gałęzią transportu. Latanie stało się normalną częścią naszego życia. Szacuje się, iż zaledwie 5% światowej populacji kiedykolwiek leciało samolotem, z usług transportu lotniczego korzysta coraz więcej podróżnych. Globalny rozwój transportu lotniczego determinowany jest przemianami i trendami w rozwoju światowej gospodarki przy przewidywanym wzroście ruchu o 4,3% rocznie do roku 2035. Lotniska bez stanowisk check-in? Zdalne wieże zarządzania ruchem lotniczym na lotniskach? W przyszłości czekają nas orbitalne loty pasażerskie, czy loty statkami autonomicznymi. Dziś kupno biletu załatwiamy kliknięciem w smartfonie. Korzystając z usług z portu lotniczego za które zapłacimy kartą bądź blikiem. Odprawę bagażu na niektórych lotniskach możemy dokonać w domu. Na lotnisku przechodzimy przez automatyczną bramkę. W samolocie zakładamy słuchawki i surfujemy w internecie. Jedynie dobra organizacja jest w stanie dać dobre produkty i usługi. Stwarza się konieczność wypracowania i stosowania działań globalnych w budowaniu strategii i bezpieczeństwa personalnego w sektorze branży lotniczej. Liczba wszystkich lotów na całym świecie w 2024 roku wyniosła około 100 mln, co oznacza wzrost o 4,3% do roku 2023. ACI (Airports Council International, Międzynarodowe Zrzeszenie Portów Lotniczych) jest organizacją obejmującą 2181 lotnisk w 170 krajach i, według analiz przeprowadzonych, wskazuje, że pierwsze 10 największych lotnisk odpowiada za 9 procent globalnego ruchu lotniczego, przy czym prym wiodą lotniska USA, takie jak Hartsfield-Jackson w Atlancie, Chicago-O'Hare i Dallas. Fort Worth (Airports Council International, 2025). W Europie znajduje się londyńskie Heathrow. Pod względem największego ruchu towarowego znajdują się lotniska w Hongkongu, Szanghaju oraz Memphis w amerykańskim stanie Tennessee. Szacuje się, że wolumen ładunków przewożonych drogą lotniczą wzrósł o 8,4% do 124 mln ton. Lotnisko Szanghaj Pudong awansowało z 21 pozycji w 2023 r. na dziesiątą pozycję w rankingu 2024 roku. Przewidywany wzrost w globalnym ruchu pasażerskim w 2030 roku przekroczy

12 mld pasażerów, natomiast w 2042 roku ma osiągnąć 19,5 mld, co oznacza dwukrotny wzrost w porównaniu z obecnym rokiem, spowodowany rozwojem międzynarodowych rynków w regionie Azji i Pacyfiku oraz Bliskiego Wschodu. Jesteśmy połączeni systemami satelitarnymi w każdej dziedzinie życia. Dla przykładu, w 2018 roku linie lotnicze British Airways zostały ukarane rekordową grzywną w wysokości 183 mln funtów za wyciek danych około 500 tys. pasażerów (Sweney, 2019). Podatność amatorskich i profesjonalnych systemów na zakłócenia czy zakłócanie sygnału GNSS jest faktem. Wykrywanie anomalii GNSS – jammingu i spoofingu – stało się najbardziej odczuwalne w obszarach działań wojennych i terytoriach okupowanych i zaczepnych. Działania poprzez ataki nie są wykonywane na oślep, rozszerzone o ataki jednostkowe, kierunkowe, stają się coraz bardziej wyrafinowane, a obszar FIR Warszawa stał się cywilnym polem walki bez strzelania. Zakłócenia częstotliwości nawigacji satelitarnych, zgodnie z ITU (International Telecommunication Union), nie powinny być zakłócane, a stają się coraz bardziej agresywne i bezwzględne. Przeloty w rejonie tych obszarów stają się niemożliwe z powodu zakłóceń generowanych przez sygnały również naziemne.

Techniki ogólnego zakłócania

Atak jest zdefiniowany jako próba zniszczenia, kradzieży czy uzyskania nieautoryzowanego dostępu czy użycia aktywów (Krawiec, 2019). Cyberprzestępcy wykorzystują różne techniki, aby zdobyć dane do logowania i inne wrażliwe informacje. Ewoluujące taktyki, techniki i procedury stosowane przez cyberprzestępców w działaniu różnorodnych grup przestępczych działających na skalę globalną obejmują zarówno narzędzia, złośliwe oprogramowanie, jak i sposoby poruszania się w sieci. Cyberprzestępcy stosują szeroką gamę taktyk, aby wyłudzić od użytkownika dane dotyczące logowania do kont, nakłonić użytkownika do udostępnienia informacji, pobrania szkodliwych plików. Wzrost złośliwych reklam jest jednym z niepokojących trendów, ponieważ atakujący ukrywają złośliwe oprogramowanie w reklamach internetowych w popularnych wyszukiwarkach – to malvertising polegający na umieszczeniu złośliwego oprogramowania. W przeciwieństwie do ataków phishingowych, które wykorzystują wiadomości e-mailowe, złośliwe reklamy mogą pojawiać się w standardowych wynikach wyszukiwania,

co sprawia, że czujnym okiem użytkownika trudno je wykryć. Umożliwia to pominięcie typowych środków bezpieczeństwa i rozprzestrzenianie złośliwego oprogramowania. Słabe dane uwierzytelniające pozostają głównymi metodami nieautoryzowanego dostępu do sieci. Staje się kluczowym elementem w budowaniu proaktywnych strategii obronnych przez współczesne organizacje. Raport Malwarebytes ujawnił 42% wzrost incydentów związanych ze złośliwym oprogramowaniem tylko w USA, przy czym ataki były wymierzone w popularne marki do wyłudzenia informacji czy dostarczenia złośliwego oprogramowania (Greenberg, 2024). Przestępcy umieszczają złośliwe reklamy, które nie są do odróżnienia od legalnych, co utrudnia ich identyfikację.

Źródłem największej liczby zakłóceń o małej mocy i na niewielką skalę geograficzną są „chuligani elektroniczni", jak złodzieje najczęściej drogich samochodów, kierowcy samochodów ciężarowych, taksówkarze, by nie było ich widać w systemie, hakerzy oraz służby – nie mówią, do jakich celów. Stosują anteny kierunkowe do zakłócania poszczególnych czy wybranych sygnałów samolotów. Przy użyciu dużych mocy ukierunkowane zasięgi mają kilkaset kilometrów. Większość ataków nie dociera do powierzchni ziemi. Atakują wszystkie konstelacje. Włamują się do cywilnej sieci AFTN; widzą, wiedzą, co i kiedy leci. Zakłócenia stały się poważnym problemem bezpieczeństwa lotniczego i geopolitycznego w Europie. Najwięcej incydentów odnotowuje się na wschodniej granicy NATO, na Bliskim Wschodzie oraz na szlakach morskich. Lotnictwo cywilne korzysta z urządzeń VOR, ILS, INS (Inertial Navigation System) / DME oraz procedur awaryjnych w ograniczaniu ryzyka zakłóceń. Europa poprzez wdrażanie OSNMA (Open Service Navigation Message Authentication) w Galileo wzmacnia raportowanie i koordynację działań.

Cyberatak na międzynarodowego dostawcę oprogramowania lotniskowego, firmę Collins, obsługującą system boardingu i odprawy bagażowych, na lotniskach europejskich (Berlin, Bruksela, Londyn, Heathrow) spowodował, że część rejsów została opóźniona lub odwołana – trzeba było przejść na system ręczny „papierzany". Cyberatak na oprogramowanie jest testem ciągłości działania lotnisk w momencie awarii krytycznego elementu (Associated Press, 2025).

Już uzależniliśmy się od urządzeń IT, w tym satelitarnych, co skutkuje atakami na wiele systemów, a co w przyszłości może spowodować skutki

katastrofalne. „System of systems", kontynuując monitorowanie anomalii GNSS (Global Navigation Satellite System) z systemów monitorowania w powietrzu, na ziemi oraz transponderów, umożliwia skuteczne zdiagnozowanie technik i źródeł jammingu i spoofingu (Narkiewicz, 2007).

Spoofing to wirtualne przemieszczanie samolotu w powietrzu przy wykorzystaniu agresywnej techniki „jammowania" w pierwszej kolejności, a następnie podłożenia sfałszowanego sygnału satelitarnego, mówiąc o manipulowaniu sygnałem tak, aby zmienić pozycję i czas. Jest to subiektywne i trudne w pierwszym momencie do jednoznacznej identyfikacji – ikonka ilustrująca liczbę satelitów będzie najprawdopodobniej biała przy zmniejszeniu dostępnych satelit. Pierwsze takie skutki załogi odczuły w trakcie przelotu w rejonie Bliskiego Wschodu. Urządzenia pokładowe przekierowały samolot w rejon Iranu – góry na północ od Teheranu. Spoofing komunikacji VHF, z wykorzystaniem AI do naśladowania służb ATC i pilotów jest zagadnieniem coraz „modniejszym". Natomiast jamming to zakłócanie sygnału. Wystarczy tylko chwila, aby znaleźć się w zainfekowanym obszarze, a powrót do normalności może zająć minutę, co w trakcie lotu – 60 sekund – jest bardzo długim czasem. Nieodpowiedzialnych bawiących się, świadomych i nieświadomych swoich działań, bawiących się tanimi jammerami. Również przy drogach ekspresowych i autostradach. Ataki napędzające falę cyberwymuszeń to:

- Ransomware, polegający na szyfrowaniu danych ofiary i żądaniu okupu za ich odblokowanie, pozostaje najpoważniejszym, najbardziej destrukcyjnym zagrożeniem cybernetycznym, napędzanym przez innowacyjne działania cyberprzestępców, zakłócając krytyczne usługi pasażerskie. Pociąga za sobą konsekwencje regulacyjne, reputacyjne, operacyjne. Przykład awarii na lotniskach pokazuje, jak wiele mamy jeszcze do zrobienia. Zakłócenia świadczą o powszechnym uzależnieniu od dostawcy usług. Odprawy i nadawanie bagażu, stosowane przez linie lotnicze, lotniska, zostały zaszyfrowane przez oprogramowanie ransomware. Pociągnęło to za sobą konsekwencje operacyjne poprzez wyłączenie automatycznych punktów odprawy i systemów nadawania bagażu. Lotniska odwołały dziesiątki lotów i stanęły w obliczu utraty reputacji, kolejek i niepewności; podkreśliły bezpośredni wpływ

incydentów cybernetycznych na biznes. Wstępne dochodzenia wskazują, że jest to kampania ransomware motywowana finansowo.

- Ransomware-as-a-Service (RaaS) – model ten znacząco obniżył barierę wejścia dla atakujących, nieposiadających zaawansowanych umiejętności technicznych w tworzeniu złośliwego oprogramowania, działających na zasadzie podziału zysków poprzez oferowanie gotowego do użycia zestawu narzędzi do infiltracji danych.
- RansomHub – oferująca swym partnerom intratne warunki podziału zysków zapłaconego okupu, co sprzyja pojawianiu się licznych nowych grup ransomware.

Stojący za atakami cyberprzestępcy, stosując bardziej wyrafinowane metody wymuszania, działają w zorganizowany sposób, wykorzystując modele biznesowe, specjalizując się w poszczególnych atakach, co zwiększa ich efektywność i skalę działania. Poprzez zastosowanie sztucznej inteligencji ataki stały się bardziej wyrafinowane, a inwestorzy inwestują w nowe technologie, a przy tym dywersyfikują swoje zyski w inwestycjach legalnych i półlegalnych, co utrudnia władzom wykrycie takich działań. Kluczowe pozostają budowa odporności oraz plan odzyskiwania danych. Firmy muszą dostosowywać strategie cyberbezpieczeństwa organizacji do rozwiązań predykcyjnych i zarządzania ryzykiem.

Czynnik ludzki w organizacjach, w tym kadra zarządzająca, partnerzy biznesowi, służby lotniskowe, pozostaje jednym z najsłabszych i najczęściej atakowanych ogniw w systemach bezpieczeństwa informatycznego. Błędy czy też celowe złośliwe działania pracowników przyczyniły się do około 60% wszystkich potwierdzonych naruszeń bezpieczeństwa. Nieostrożne kliknięcia w wiadomościach phishingowych stwarzają podatność na wyrafinowane techniki inżynierii społecznej – vishing, protexting, jak też błędne wysłanie wrażliwych danych do nieuprawnionych odbiorców, stosowanie słabych haseł, nieprzestrzeganie polityk bezpieczeństwa. Powyższe zagrożenia mogą być przypadkowe, wynikające z braku wiedzy, niedbalstwa, pośpiechu, a może celowe działanie pracownika motywowane chęcią zemsty, na zlecenie konkurencji, obcego wywiadu, aby osiągnąć zysk finansowy. Legalne konta pracownicze przejęte przez zewnętrznych hakerów w wyniku phishingu lub malware'u są szczególnie podstępne i trudne do wykrycia, ponieważ omijają środki bezpieczeństwa, jak systemy IDS/IPS, dzięki

posiadaniu zaufanego dostępu do systemów w organizacji. Szkolenia z zakresu cyberbezpieczeństwa są skutecznym środkiem zaradczym, zarówno teoretycznym, jak i praktycznym, dotyczące rozpoznawania ataków i prób phishingu, są skłonni do prawidłowego zidentyfikowania i zgłaszania takich prób służbom bezpieczeństwa. Budowanie kultury bezpieczeństwa jest kluczowym elementem w redukcji ryzyka i w podnoszeniu świadomości pracowników organizacji lotniczej.

Współczesna cyberprzestępczość staje się coraz bardziej podzielona na specjalizację oraz tworzenie grup do przeprowadzania określonych typów ataków – phishing kits, exploit kits. Wymusza to stosowanie strategii bezpieczeństwa, które adresują nie tylko etap końcowy ataku. Konieczne stają się aktywne monitorowanie aktywności dostępu, analiza trendów, które dadzą obraz złożoności ekosystemu, przewidywalność we wskazaniach nowych wektorów zagrożeń cybernetycznych (Krawiec, 2019; Syta, 2025).

Nie można wykluczyć również degradacji sygnału GNSS (Global Magnetic Storm Index) spowodowanej czynnikami naturalnymi, tak jak wybuchami na Słońcu – wysokim indeksem Kp, niekorzystne ustawienie konstelacji, odbiciowość sygnału nawigacji satelitarnej od przeszkód, załamanie sygnału od przeszkód, zakłócenia przemysłowe.

Kolejnym problemem w przestrzeni powietrznej nad lotniskami są niezidentyfikowane drony zmuszające zarządzających do podjęcia działań w odpowiednich procedurach bezpieczeństwa, w tym do tymczasowego zamknięcia lotnisk. Lotnictwo w dobie wojny hybrydowej stawia wyzwania dla bezpieczeństwa lotnictwa i wymaga weryfikacji procedur. Trzeba balansować między neutralizacją dronów a zachowaniem bezpieczeństwa lotów, co wiąże się z potencjalnymi opóźnieniami i koniecznością zmian w planach pasażerów.

Monitorowanie anomalii GNSS

Postęp cyfrowy naraża sektor na cyberzagrożenia ze wszystkich stron, co ma wpływ na reputację, ciągłość usług, bezpieczeństwo ludzi i obiektów, a w ostateczności na finanse. Raporty CERT.PL pokazują, że liczba ataków odnotowanych w polskiej cyberprzestrzeni drastycznie wzrasta, co stanowi wyzwanie i wiąże się z pojawiającymi się wyzwaniami, takimi jak przeciwdziałanie (CERT Polska, 2025). Zagrożenia dla bezpieczeństwa w cyberprzestrzeni wpływają na działania państwa, dając możliwość wprowadzenia stanów

nadzwyczajnych (Jelonek, 2024). Aby skutecznie móc monitorować, jak też interpretować anomalie, należy wykorzystać w tym celu czujniki naziemne umieszczone nad powierzchnią, a dane z ADS-B poprzez czujniki umieszczone w statkach powietrznych są bardzo pomocne i wiarygodne. Skuteczność zakłócania na ziemi jest ograniczona przede wszystkim rzeźbą terenu, lasami i budynkami. Dużą liczbę czujników i dysponując algorytmami multilateracji, możemy precyzyjnie określić miejsce oraz sposób przemieszczania się źródła zakłóceń. Przeciwnik sprytnie wykorzystuje swoją wirtuozerię i kunszt, przebiegłość i bezwzględność działania, tworząc nowy rozdział wojny hybrydowej. Inteligentny spoofing da się wdrożyć na Bliskim Wschodzie na kilkusetkilometrowym obszarze, a co gdyby takie niepożądane działanie działo się w miejscu o olbrzymim natężeniu ruchu lotniczego – jakie konsekwencje.

Używając merytorycznych przesłanek, wiemy, że temat zakłóceń sygnałów GNSS i spoofingu jest coraz częściej powtarzającym się. Załogi tracą integralność danych GNSS, raportując zagregowane anomalie w określaniu pozycji i integralności danych. Różnorodność standardów i skomplikowany system przy niejednoznacznym systemie interpretacji powoduje, że wyciągnięcie wniosków nastręcza trudności, wskazując na trzy typy wskaźników jakości danych dla systemu ADS-B:

1. Wskaźnik niepewności – wartości parametrów wskazują, że co najmniej 95% pomiarów mieści się w dopuszczalnych granicach niepewności,
2. Wskaźnik dokładności – zastępują wskaźnik niepewności, również wskazują, że co najmniej 95% pomiarów mieści się w dozwolonych granicach dokładności,
3. Wskaźnik integralności – zastępuje wskaźnik niepewności z wersji 0.

W zależności od specyfiki urządzeń, standardów ADS-B, od sytuacji, czy od fazy lotu. Dane oparte na błędach pozycji – (NIC – Navigational Integrity Category), (NACp – Navigation Accuracy Code for position) oraz NUCr, NACv muszą być analizowane z (SIL – Source Integrity Level) w kontekście (ESASSP – EUROCONTROL Specification for ATM Surveillance System Performance). Z danych ADS-B bez dogłębnej analizy stwierdzamy, że coś jest nie tak i wymaga szczegółowej dogłębnej analizy. Dla załóg lotniczych są publikowane depesze NOTAM FIR EPWW – „ANOMALIES IN GNSS SIGNAL MAY BE EXPECTED IN AREA NORTH OF LINE, DEFINED

BY POINTS: 1….N….E, 2….N….E." Zgłoszenia zdarzeń lotniczych związanych z zakłóceniami sygnału GPS w różnych obszarach geograficznych i przedziale czasowym należy raportować w ECCAIRS. Wykorzystanie luk prawnych i działanie za pośrednictwem pozorantów to praktyki stosowane w utrudnianiu działań organów bezpieczeństwa.

W celu zapewnienia cyberbezpieczeństwa stosuje się testy penetracyjne systemów lotniczych w celu wykrycia słabości polegających na symulacji ataków w kontrolowanych warunkach, aby wykryć i naprawić słabości, mając na uwadze aspekty tego procesu, jak:

1. Cel testów penetracyjnych – w identyfikacji słabości systemów, przeprowadzeniu oceny odporności na potencjalne ataki czy zagrożenia, dla wzmocnienia zabezpieczeń przed rzeczywistymi atakami;
2. Zakres testów – dla zarządzania lotami systemów nawigacji i komunikacji powiązany infrastrukturą sieci IT z uwzględnieniem systemów cyberbezpieczeństwa i ochrony;
3. Etapy testów – obejmujące planowanie w tym zakresie i celach oraz metodologię, jak również zbieranie informacji o systemach i infrastrukturze, wykrywanie słabości z użyciem narzędzi do identyfikacji luk. Prowadzenie analizy i raportowanie wyników w tym rekomendacje naprawcze;
4. Metody i narzędzia – z wykorzystaniem ręcznych i automatycznych technik penetracyjnych w symulacji ataków typu phishing, malware, DDoS (Distributed Denial of Service), na poziomie aplikacji i urządzeń;
5. Bezpieczeństwo i zgodność – współpraca z odpowiednimi organami w zapewnieniu minimalizacji ryzyka zakłóceń operacyjnych za pomocą testów przez certyfikowanych specjalistów;
6. Działania naprawcze, wnioski – wdrażanie rekomendowanych zabezpieczeń przez regularne testy, audyty, monitorowanie postępów, analizę wyników.

Szczególne warunki muszą spełniać osoby zajmujące kierownicze stanowiska w organizacjach lotniczych w obszarach wysokiego ryzyka w sektorze bezpieczeństwa – ochrony. Decyzje w szczególnie trudnych warunkach będą podejmowane pod dużą presją, w stresie, co stanowi istotną cechę przywództwa zorientowanego na zadanie (Klich, 2011; Jelonek, 2024).

Podsumowanie

Podstawą cyberbezpieczeństwa jest czynnik ludzki mający wiedzę i praktykę przekładające się na doświadczenie. Mimo rosnących nakładów, nowych regulacji, coraz doskonalszych narzędzi, rosnącej świadomości potrzeby ochrony przed cyberatakami, trudno się oprzeć wrażeniu, że w przyszłości w znaczący sposób wzrośnie ryzyko przetwarzania informacji. Rosnące światowe wydatki na IT wskazują, że w coraz większym stopniu uzależniliśmy się od technologii teleinformatycznych. Dlatego organizacje lotnicze muszą podjąć konkretne kroki w celu zwiększenia liczby personelu posiadającego wiedzę z zakresu cyberbezpieczeństwa i lotnictwa poprzez ciągłą edukację, a poprzez innowacyjne sposoby łączenia ścieżek kariery w dziedzinie technologii informacyjnych z karierą w lotnictwie dla rozwoju umiejętności potrzebnych dla cyberbezpieczeństwa w łączeniu branż lotnictwa cywilnego, obronnego z pozostałymi.

Nie ma dnia ani tygodnia, abyśmy nie byli zaskoczeni czymś nowym. Ataki hakerskie na lotniska poprzez włamania do punktów odprawy bagażu czy wyciek danych personalnych pasażerów na różne sposoby i metody, przy tak rozbudowanej technice, wykorzystujące wszelkie oficjalne i nieoficjalne metody, w tym dostęp do powszechnie stosowanych urządzeń i sieci, muszą być na wszechmiar kontrolowane i zabezpieczone. W obliczu wyzwań kluczowe pozostają ciągłe doskonalenie rozwiązań bezpieczeństwa i płynność ruchu lotniczego.

Standardy cyberbezpieczeństwa w dobie XXI wieku mają szerokie znaczenie w dzisiejszych firmach branży lotniczej, które wykorzystują technologię IT do prowadzenia operacji w sieci. Nie wystarczy umieścić cyberbezpieczeństwo w ustawie o IT, ale aby zmaksymalizować swoje zyski, korporacje wykorzystują technologię w działalności operacyjnej, która musi być chroniona we wszystkich aspektach działalności biznesowej. W wielu przypadkach różniące się pod wieloma względami standard bezpieczeństwa cybernetycznego nie jest optymalny dla zmniejszenia ryzyka. Należy zastanowić się, w jaki sposób przestrzegać przepisów z cyberbezpieczeństwa. Cyberatak na system boardingu i odpraw bagażowych dowodzi, jak ważne jest tworzenie i testowanie procedur awaryjnych. Należy utrzymywać podręczniki ręcznej odprawy i nadawania bagażu na wypadek awarii IT. Rezerwowy dodatkowy

personel w celu zmniejszenia wąskich gardeł. Weryfikacja segmentacji sieci i plany ograniczania incydentów dla połączeń innych firm. Przeprowadzać ćwiczenia odporności okresowe na całym lotnisku, symulując ataki ransomware'a. Przetestować koordynację pod presją, uwzględniając linie lotnicze, obsługę naziemną. Usprawnić udostępnianie informacji w czasie rzeczywistym za pośrednictwem kanałów społecznościowych, oznakowań, aplikacji. Weryfikacja sieci oraz plany ograniczania incydentów.

Przemysł lotniczy jest kluczowy dla gospodarki narodowej, a inwestycje w rozwój technologii i innowacji są niezbędne, aby sprostać rosnącym wymaganiom rynku oraz wyzwaniom związanym ze zrównoważonym rozwojem branży lotniczej. Załącznik 19 ICAO wskazuje nam, że bezpieczeństwo w lotnictwie jest stawiane na pierwszym miejscu. Eksperci wskazują, że aby uchronić się przed utratą danych, należy zachować zdrowy rozsądek i nie pozwolić wywierać na siebie presję. Weryfikować tożsamość autora wiadomości, próbując skontaktować się za pomocą innego urządzenia. Dyskusje w zróżnicowanym i wielokulturowym środowisku na temat „Flying Tomorrow: Enhancing Aviation Security for a Sustainable Future", przygotowując się do rozmów na temat ewolucji bezpieczeństwa lotniczego. Polski rząd zwiększył do rekordowej kwoty 4 mld zł budżet na cyberbezpieczeństwo w 2025 roku.

Literatura

1. Airports Council International. (2025). T*he busiest airports in the world defy global uncertainty and hold top rankings*.
2. Associated Press. (2025). *Cyberattack disrupts check-in systems at major European airports*. AP News. Pobrane z: https://apnews.com/article/29b6d890baf7ac3a22f0f2b2f169b890 (dostęp: 24.02.2026).
3. CERT Polska. (2025). *Raport roczny z działalności CERT Polska w 2024 roku*. CERT Polska.
4. Greenberg, A. (2024). *Malicious ads in search results are driving new generations of scams.* Wired. Pobrane z: https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams (dostęp: 24.02.2026).
5. International Civil Aviation Organization. (2022). *Aviation cybersecurity strategy*.

6. Jelonek, A. (2024). *Współczesne zagrożenia bezpieczeństwa*. Akademia Sztuki Wojennej.
7. Klich, E. (2011). *Bezpieczeństwo lotów.* Instytut Technologii Eksploatacji – PIB.
8. Konwencja o międzynarodowym lotnictwie cywilnym, podpisana w Chicago dnia 7 grudnia 1944 r. (1944).
9. Komisja Europejska. (2022). *Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji*. Dz.Urz. UE L 248 z 26.09.2022.
10. Komisja Europejska. (2023). *Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji*. Dz.Urz. UE L 31 z 2.02.2023.
11. Krawiec, J. (2019). *Cyberbezpieczeństwo: Podejście systemowe*. Oficyna Wydawnicza Politechniki Warszawskiej.
12. Narkiewicz, J. (2007). *GPS i inne satelitarne systemy nawigacyjne*. Wydawnictwa Komunikacji i Łączności.
13. Parlament Europejski i Rada UE. (2022). *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.* Dz.Urz. UE L 333 z 27.12.2022, s. 80-152.
14. Rada Ministrów. (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.*
15. Sweney, M. (2019). *BA faces £183m fine over passenger data breach*. The Guardian. Pobrane z: https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways (dostęp: 24.02.2026).
16. Syta, J. (2025). *Zarządzanie cyberbezpieczeństwem*. Wydawnictwo Naukowe PWN.
17. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20).
18. Żylicz, M. (2002). *Prawo lotnicze międzynarodowe, europejskie i krajowe*. Wydawnictwo Prawnicze LexisNexis.

Sławomir Żurawski[1]
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Marek Ciekanowski[2]
Społeczna Akademia Nauk filia w Warszawie
Rafał Parczewski[3]
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Warszawa

https://doi.org/10.29316/9788368103373_17

ZARZĄDZANIE BEZPIECZEŃSTWEM TRANSPORTU PUBLICZNEGO W AGLOMERACJACH MIEJSKICH W POLSCE

PUBLIC TRANSPORT SAFETY MANAGEMENT IN URBAN AREAS IN POLAND

Streszczenie

Celem rozdziału jest analiza poziomu bezpieczeństwa transportu publicznego w wybranych aglomeracjach miejskich w Polsce, ze szczególnym uwzględnieniem liczby wypadków, incydentów pasażerskich oraz strategii zarządzania ryzykiem podejmowanych przez operatorów i administrację miejską. Badanie ma na celu ocenę

[1] https://orcid.org/ 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl
[2] https://orcid.org/0009-0009-1271-0652, e-mail: marek@ciekanowski.pl
[3] https://orcid.org/0000-0002-2603-0596

skuteczności wdrożonych rozwiązań oraz wskazanie dobrych praktyk możliwych do replikacji w innych jednostkach miejskich. W rozdziale zastosowano podejście oparte na analizie danych ilościowych i jakościowych. Wykorzystano oficjalne statystyki Policji, GUS, ZTM oraz raporty miejskie dotyczące wypadków i kolizji z udziałem pojazdów komunikacji zbiorowej. Uzupełnieniem analizy statystycznej była analiza treści dokumentów strategicznych i operacyjnych dotyczących bezpieczeństwa transportu, a także przegląd wybranych wdrożeń technologicznych i organizacyjnych (np. monitoring, ITS, szkolenia, kampanie społeczne). Problem badawczy sformułowano: Jak zmienia się poziom bezpieczeństwa transportu publicznego w polskich aglomeracjach w ostatnich latach i które strategie zarządzania ryzykiem okazują się najskuteczniejsze? Odpowiednio sformułowano hipotezę badawczą: Systematyczne wdrażanie zintegrowanych działań technicznych, organizacyjnych i cyfrowych w zarządzaniu bezpieczeństwem transportu publicznego przyczynia się do ograniczenia liczby wypadków i incydentów oraz poprawy poczucia bezpieczeństwa pasażerów.

Słowa kluczowe: bezpieczeństwo, transport publiczny, zarządzanie, aglomeracja miejska, zagrożenia

Abstract

The aim of the article is to analyse the level of public transport safety in selected urban agglomerations in Poland, with particular emphasis on the number of accidents, passenger incidents and risk management strategies undertaken by operators and municipal administration. The aim of the study is to assess the effectiveness of the implemented solutions and to indicate good practices that can be replicated in other urban units. The article uses an approach based on the analysis of quantitative and qualitative data. Official statistics of the Police, the Central Statistical Office, the Statistical Office of the Republic of Poland and city reports on accidents and collisions involving public transport vehicles were used. The statistical analysis was complemented by an analysis of the content of strategic and operational documents on transport safety, as well as an overview of selected technological and organisational initiatives (e.g., monitoring, ITS, training, social campaigns). The research problem is formulated: How has the level of public transport safety in Polish agglomerations changed in recent years, and which risk management strategies turn out to be the most effective? The research hypothesis was formulated accordingly: The systematic implementation of integrated technical, organisational, and digital activities in public transport safety management contributes to reducing the number of accidents and incidents and to improving passengers' sense of safety.

Keywords: safety, public transport, management, urban agglomeration, threats

Wstęp

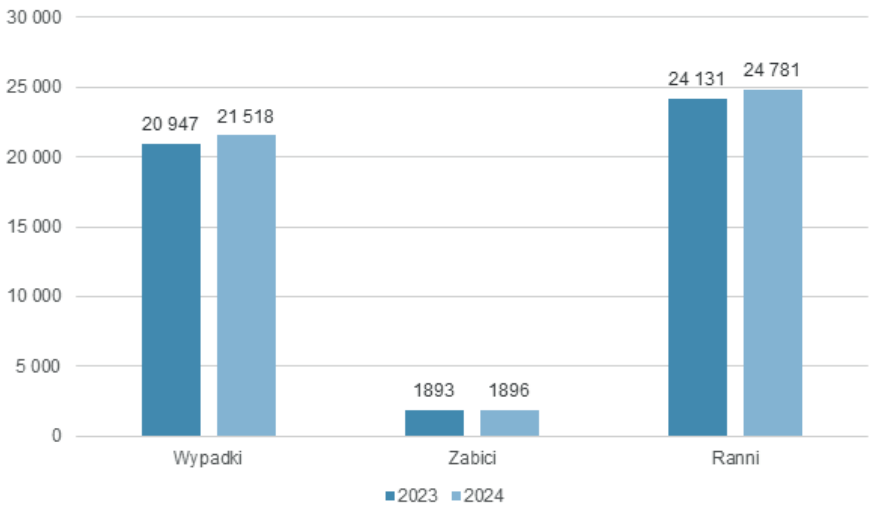
Bezpieczeństwo transportu publicznego stanowi jeden z kluczowych elementów funkcjonowania współczesnych aglomeracji miejskich. Systemy komunikacji zbiorowej obsługują codziennie miliony pasażerów, a ich niezawodność i bezpieczeństwo mają bezpośredni wpływ na jakość życia mieszkańców, sprawność logistyki miejskiej oraz poziom zaufania społecznego do instytucji publicznych. W miarę jak miasta stają się coraz bardziej złożone i zurbanizowane, rośnie również znaczenie skutecznego zarządzania bezpieczeństwem w przestrzeni transportowej – zarówno w aspekcie prewencyjnym, jak i reagowania na incydenty. Transport publiczny jest środowiskiem narażonym na różnorodne zagrożenia: techniczne (np. wypadki drogowe, awarie pojazdów), społeczne (np. agresja, przestępstwa, wandalizm), zdrowotne (zasłabnięcia, zakażenia), a także organizacyjne (niewydolność służb, braki kadrowe, przeciążenie infrastruktury). Szczególnym wyzwaniem dla systemów zarządzania bezpieczeństwem okazały się ostatnie lata, naznaczone m.in. pandemią COVID-19, zmianami w strukturze mobilności miejskiej, wzrostem liczby pasażerów po okresie lockdownów, a także zwiększoną liczbą zdarzeń o charakterze kryzysowym w przestrzeni publicznej.

Celem niniejszego rozdziału jest analiza poziomu bezpieczeństwa transportu publicznego w wybranych aglomeracjach miejskich w Polsce, ze szczególnym uwzględnieniem występujących incydentów oraz działań operacyjnych podejmowanych przez odpowiedzialne instytucje. Badanie obejmuje zarówno analizę danych statystycznych dotyczących wypadków, interwencji służb i incydentów pasażerskich, jak i przegląd strategii zarządzania ryzykiem stosowanych w największych miastach. Podjęta analiza ma na celu odpowiedź na pytanie, w jaki sposób zmieniał się poziom bezpieczeństwa w transportach miejskich w ostatnich latach i które działania okazały się najskuteczniejsze z perspektywy zarządzania kryzysowego i operacyjnego. Opracowanie ma charakter interdyscyplinarny i łączy podejścia zarządcze, statystyczne i operacyjne. Stanowi próbę połączenia wiedzy teoretycznej z zakresu zarządzania bezpieczeństwem publicznym z analizą praktycznych rozwiązań stosowanych w warunkach polskich aglomeracji. Wyniki niniejszego badania mogą znaleźć zastosowanie zarówno w planowaniu polityk miejskich, jak i w doskonaleniu systemów reagowania kryzysowego w transporcie zbiorowym.

Statystyczny obraz zagrożeń w transporcie publicznym

Bezpieczeństwo transportu publicznego stanowi jeden z kluczowych komponentów zarządzania bezpieczeństwem miejskim (Płachecka, 2016, s. 22). Wraz z dynamicznym rozwojem aglomeracji i wzrostem mobilności mieszkańców rośnie również znaczenie efektywnego monitorowania i zarządzania ryzykiem w systemach komunikacji zbiorowej. Dobrze zorganizowany transport zapewnia efektywny przepływ zasobów umożliwiający rozwój gospodarczy danego obszaru (Janczarska-Bergel, 2021, s. 97).

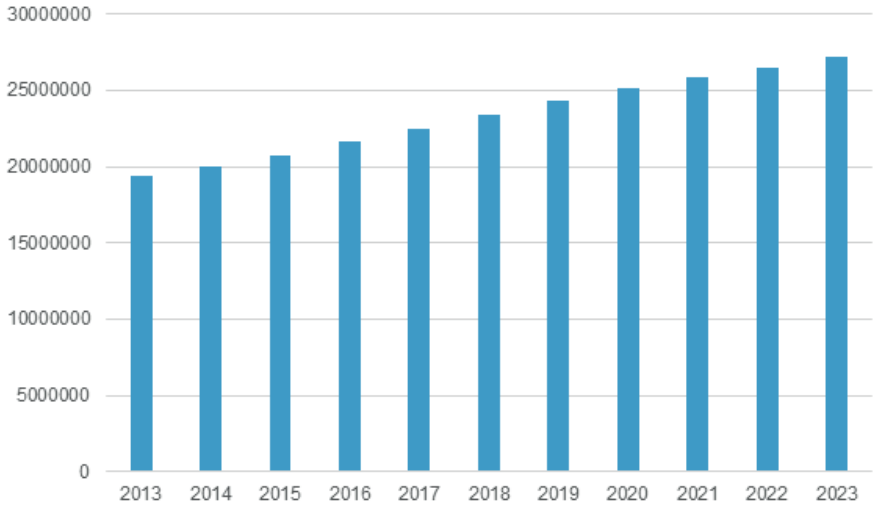
Transport publiczny – obejmujący autobusy, tramwaje, metro oraz inne środki przewozu pasażerskiego – jest środowiskiem o podwyższonym poziomie zagrożeń zarówno technicznych, jak i społecznych (Ochyra-Żurawska i in., 2024). Wypadki drogowe, kolizje, awarie taboru, przypadki agresji pasażerskiej, kradzieże kieszonkowe, zasłabnięcia czy sytuacje kryzysowe związane z masowymi wydarzeniami lub katastrofami naturalnymi – wszystkie te zdarzenia mogą znacząco obniżać poczucie bezpieczeństwa użytkowników transportu i wpływać na sprawność działania systemu komunikacyjnego miasta. Poniżej przedstawiono liczbę wypadków drogowych w Polsce w 2023 i 2024 roku (Rysunek 1).



Rysunek 1. Liczba wypadków drogowych w Polsce, liczba rannych i ofiar śmiertelnych w 2023 i 2024 roku

Źródło: Wydział Ruchu Drogowego Komendy Stołecznej Policji, 2025.

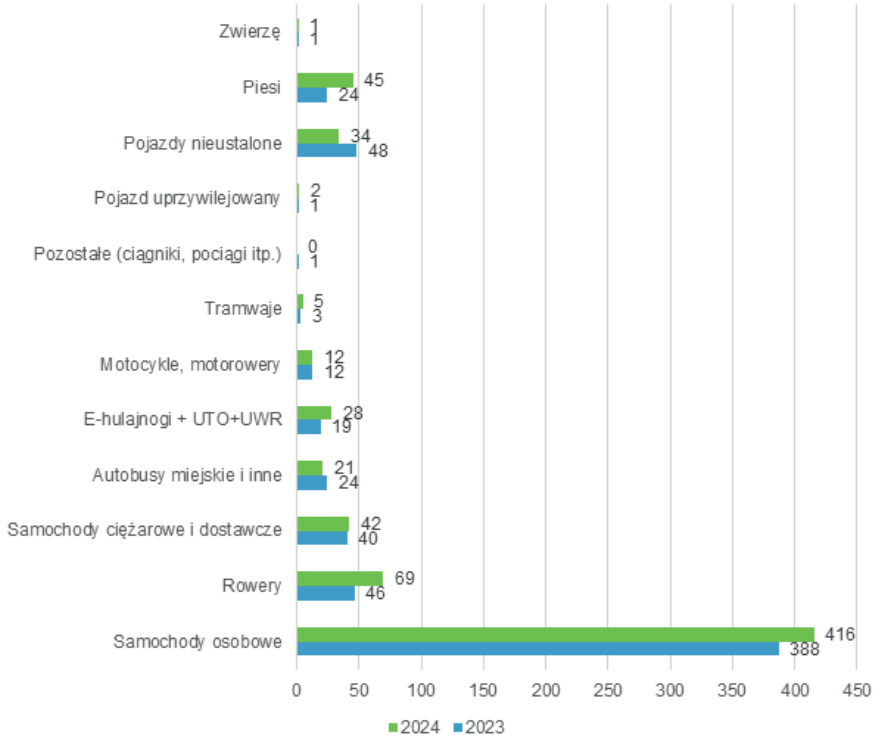
Według wstępnych danych szacunkowych, w 2024 roku na terenie Polski zaistniało 21518 wypadków drogowych (o 571 więcej niż w 2023 r.), w wyniku których 1896 osób poniosło śmierć (o 3 więcej niż w 2023 r.), a 24781 osób doznało obrażeń ciała (o 650 więcej). Odnotowano też 390581 kolizji drogowych (o 23346 więcej) (Wydział Ruchu Drogowego Komendy Stołecznej Policji, 2025). Jednym z czynników jest fakt, iż w ciągu ostatnich dwudziestu lat liczba samochodów osobowych w Polsce znacznie wzrosła (Glanert, 2024, s. 58). Poniżej przedstawiono liczbę samochodów osobowych w latach 2013-2023 (Rysunek 2).



Rysunek 2. Zestawienie liczby samochodów osobowych w latach 2013-2023
Źródło: opracowanie własne na podstawie danych GUS, b.d.

W latach 2013-2023 liczba samochodów osobowych w Polsce systematycznie rosła. W 2013 roku zarejestrowanych było nieco poniżej 20 milionów pojazdów, natomiast w 2023 roku liczba ta przekroczyła 27 milionów. Wzrost miał charakter stały i liniowy, bez żadnych spadków, nawet w okresie pandemii COVID-19. Średnio każdego roku przybywało od 0,5 do 1 miliona nowych samochodów. Trend ten wskazuje na rosnącą motoryzację społeczeństwa i zwiększone obciążenie infrastruktury drogowej, co wiąże się z wyzwaniami dla transportu publicznego, środowiska i bezpieczeństwa ruchu drogowego.

W literaturze przedmiotu przyjmuje się, że skuteczne zarządzanie bezpieczeństwem transportu zbiorowego wymaga podejścia systemowego i wielowymiarowego. Obejmuje ono zarówno działania prewencyjne, jak i operacyjne, a także monitoring efektywności zastosowanych rozwiązań (Żukowska, 2013, s. 2301). Elementami składającymi się na taki system są m.in. rozwinięta infrastruktura techniczna (np. systemy CCTV, przyciski alarmowe, inteligentne zarządzanie ruchem), kompetencje i zachowania pracowników (szkolenia z zakresu reagowania kryzysowego, procedury ewakuacji), współpraca z jednostkami policji, straży miejskiej i pogotowia ratunkowego oraz sprawna komunikacja z pasażerami. W ostatnich latach wzrasta również znaczenie narzędzi cyfrowych i analityki danych w zarządzaniu ryzykiem – umożliwiają one m.in. prognozowanie incydentów, analizę zachowań pasażerów oraz optymalizację tras i interwencji. Działania te muszą być jednak oparte na rzetelnej diagnozie sytuacji bezpieczeństwa w danym systemie transportowym. Analiza danych statystycznych pozwala nie tylko na identyfikację głównych zagrożeń i obszarów ryzyka, ale także na ocenę skuteczności polityk zarządzania. Zestawienie danych z lat 2020-2024 obejmujących liczbę wypadków drogowych z udziałem pojazdów komunikacji miejskiej, incydentów pasażerskich, interwencji służb porządkowych i medycznych oraz zmiennych związanych z sytuacjami nadzwyczajnymi (takimi jak pandemia COVID-19 czy wydarzenia masowe) pozwala dostrzec zmieniające się wzorce zagrożeń i potrzeby operacyjne. Poniżej przedstawiono liczbę wypadków poprzez poszczególne grupy sprawców wypadków wg środków transportu w Warszawie w 2023 i 2024 roku (Rysunek 3).

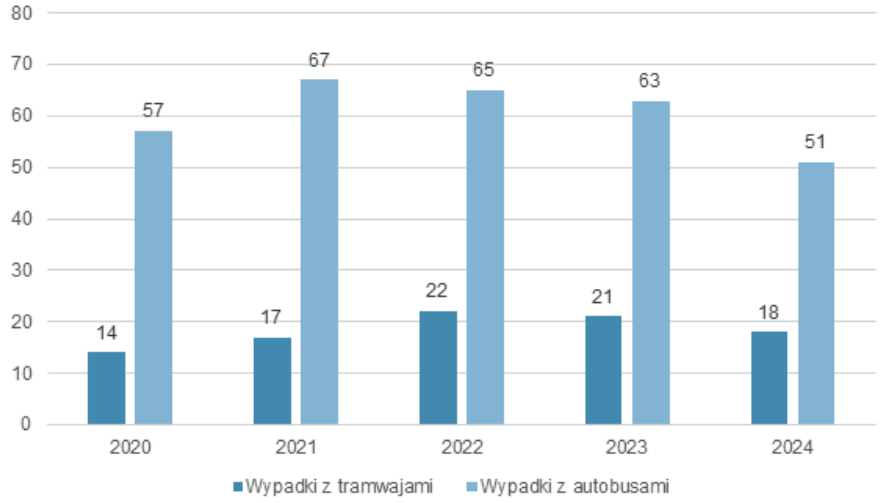


Rysunek 3. Sprawcy wypadków wg środków transportu w 2023 i 2024 roku
Źródło: Zarząd Dróg Miejskich, 2024.

Kierowcy samochodów osobowych są co roku sprawcami największej liczby wypadków. Wyraźną tendencją jest rosnąca liczba wypadków spowodowanych przez rowerzystów oraz osoby kierujące hulajnogami elektrycznymi. Łącznie kierujący rowerami, e-hulajnogami, urządzeniami transportu osobistego (UTO) oraz urządzeniami wspomagającymi ruch (UWR), byli w 2024 r. sprawcami aż 98 wypadków.

Dane z Warszawy wskazują również, że w 2024 roku zarejestrowano łącznie 69 wypadków oraz 122 kolizje, w których uczestniczyły pojazdy transportu zbiorowego. W jednym ze zdarzeń brały udział jednocześnie autobus i tramwaj komunikacji miejskiej. W wyniku tych wypadków śmierć poniosło 6 osób, co stanowiło 23% wszystkich ofiar śmiertelnych odnotowanych w zdarzeniach drogowych, a 78 osób odniosło obrażenia (w tym 9 ciężkich i 69 lekkich). Autobusy miejskie uczestniczyły w 51 wypadkach

i 99 kolizjach, natomiast tramwaje brały udział w 18 wypadkach i 24 kolizjach. Warto zaznaczyć, że część drobnych kolizji z udziałem pojazdów komunikacji publicznej nie jest zgłaszana policji, dlatego przedstawione dane mogą nie odzwierciedlać pełnej skali incydentów. Poniżej przedstawiono wypadki z tramwajami i autobusami w latach 2020-2024 (Rysunek 4).



Rysunek 4. Wypadki z tramwajami i autobusami w latach 2020-2024
Źródło**:** Zarząd Dróg Miejskich, 2024.

W porównaniu z rokiem 2023 nastąpił spadek liczby wypadków z udziałem komunikacji miejskiej o 17,8%, z 84 do 69 przypadków. Analiza przyczyn wskazuje, że kierowcy autobusów i motorniczowie rzadko są bezpośrednio odpowiedzialni za tego rodzaju zdarzenia. W 2024 roku spowodowali łącznie 24 wypadki, w których obrażenia odniosło 30 osób, jednak nie odnotowano żadnych ofiar śmiertelnych. Zdecydowaną większość – 45 wypadków, czyli 65% wszystkich tego typu zdarzeń – spowodowali inni uczestnicy ruchu drogowego.

Powyższe dane pokazują, że transport publiczny w aglomeracjach miejskich, mimo wdrażanych rozwiązań zwiększających bezpieczeństwo, nadal stanowi przestrzeń narażoną na różnorodne zagrożenia. W 2024 roku odnotowano spadek liczby wypadków z udziałem pojazdów komunikacji miejskiej, jednak liczba osób rannych oraz powaga niektórych zdarzeń świadczą o utrzymującym się ryzyku dla pasażerów i uczestników ruchu

drogowego. Zdecydowana większość wypadków wynika z winy innych uczestników ruchu, co podkreśla potrzebę nie tylko doskonalenia procedur i szkoleń wewnętrznych operatorów transportu, lecz także prowadzenia szeroko zakrojonych działań edukacyjnych i prewencyjnych w całym systemie komunikacyjnym miasta. Statystyka potwierdza również znaczenie monitorowania incydentów oraz konieczność dalszego rozwijania narzędzi analizy danych dla skuteczniejszego zarządzania bezpieczeństwem transportu zbiorowego.

Strategie zarządzania ryzykiem i poprawy bezpieczeństwa w transporcie zbiorowym

Bezpieczne funkcjonowanie transportu publicznego w dużych aglomeracjach wymaga nie tylko reagowania na zaistniałe zdarzenia, ale przede wszystkim wdrażania skutecznych strategii zarządzania ryzykiem. Praktyka wielu miast pokazuje, że bezpieczeństwo w komunikacji zbiorowej jest efektem działania złożonego systemu środków technicznych, organizacyjnych i społecznych, które – odpowiednio skoordynowane – mogą znacząco ograniczyć liczbę incydentów oraz zwiększyć poczucie bezpieczeństwa wśród pasażerów.

Jednym z podstawowych filarów tego systemu są narzędzia monitoringu i detekcji zagrożeń. W większości dużych polskich miast pojazdy transportu miejskiego oraz przystanki i węzły przesiadkowe wyposażone są w systemy monitoringu wizyjnego (CCTV), które służą zarówno do prewencji przestępstw, jak i jako narzędzie dowodowe w przypadku incydentów. Dodatkowo wiele pojazdów posiada przyciski alarmowe i systemy bezpośredniego kontaktu z centralą, co umożliwia szybką reakcję służb technicznych lub porządkowych. W niektórych aglomeracjach, jak Warszawa czy Kraków, rozwinięto systemy powiadamiania służb miejskich i policji bezpośrednio z poziomu kabiny kierowcy lub pasażera.

Istotnym uzupełnieniem są działania o charakterze prewencyjnym, których celem jest zapobieganie zagrożeniom poprzez edukację, podnoszenie kompetencji personelu oraz zwiększanie świadomości pasażerów (Abryelewicz, Sadłowska-Wrzesińska, 2014). Operatorzy transportu organizują szkolenia z zakresu reagowania kryzysowego, procedur ewakuacyjnych, rozpoznawania zachowań agresywnych oraz udzielania pierwszej pomocy.

Przeprowadzane są również kampanie społeczne promujące bezpieczne zachowania w pojazdach i na przystankach, np. w zakresie ustępowania miejsca osobom starszym, zachowania czujności wobec kradzieży czy sposobów zgłaszania zagrożeń. W niektórych miastach (np. Poznań, Łódź) funkcjonują programy współpracy z wolontariuszami lub NGO, które wspierają działania prewencyjne, zwłaszcza wobec osób narażonych na przemoc lub marginalizację.

Kolejnym istotnym aspektem są procedury reagowania kryzysowego i plany awaryjne, których celem jest zapewnienie sprawnego działania w sytuacjach nadzwyczajnych, takich jak wypadki, pożary, ataki agresji czy zagrożenia chemiczno-biologiczne. Przewoźnicy posiadają zatwierdzone plany ewakuacji i scenariusze reagowania na incydenty, a w niektórych aglomeracjach organizowane są ćwiczenia symulacyjne we współpracy z PSP, Policją i Pogotowiem Ratunkowym. Tego typu działania pozwalają nie tylko na sprawdzenie skuteczności procedur, ale także na ich bieżącą aktualizację i korektę w oparciu o doświadczenia operacyjne.

W ostatnich latach rosnące znaczenie w zarządzaniu bezpieczeństwem transportu publicznego zyskuje cyfryzacja i zastosowanie inteligentnych systemów zarządzania ruchem (ITS) (Kasprzyk, 2025, s. 167). Dzięki integracji danych z GPS, kamer, sygnalizacji świetlnej i czujników ruchu możliwe jest dynamiczne sterowanie flotą, przewidywanie zatłoczenia, a także wczesne wykrywanie potencjalnych zagrożeń. Wdrożenia takie jak systemy analizy wideo w czasie rzeczywistym, monitorowanie stanu technicznego pojazdów czy predykcyjne zarządzanie rozkładami jazdy stają się standardem w dużych miastach – m.in. w Warszawie, Gdańsku i Wrocławiu. Dodatkowo niektóre miasta wdrażają mobilne aplikacje umożliwiające pasażerom zgłaszanie incydentów i uwag dotyczących bezpieczeństwa w czasie rzeczywistym (np. aplikacja „Warszawa 19115") (Miasto Stołeczne Warszawa, b.d.).

W powyższej analizie można również wskazać szereg dobrych praktyk i innowacyjnych rozwiązań, które przyniosły pozytywne efekty. Przykładem mogą być pilotażowe patrole rowerowe Straży Miejskiej w okolicach przystanków i pętli tramwajowych, programy obejmujące montaż dodatkowego oświetlenia i punktów SOS czy partnerstwa z organizacjami pozarządowymi, jak np. współpraca ZTM z fundacjami przeciwdziałającymi przemocy wobec kobiet i dzieci. Takie działania, choć często lokalne i ograniczone

budżetowo, stanowią ważny element kultury bezpieczeństwa i zwiększają społeczne zaangażowanie w tworzenie bezpiecznego transportu. Poniżej w Tabeli 1 przedstawiono strategie zarządzania bezpieczeństwem w transporcie zbiorowym i ich efekty.

Tabela 1. Strategie zarządzania bezpieczeństwem w transporcie zbiorowym i ich efekty

RODZAJ STRATEGII	OPIS DZIAŁAŃ	PRZYKŁADOWE EFEKTY
Techniczne środki zabezpieczeń	Monitoring CCTV, przyciski alarmowe, komunikacja z centralą	Spadek liczby incydentów wandalizmu i agresji, szybsze reagowanie na zdarzenia
Działania prewencyjne	Kampanie społeczne, szkolenia kierowców, informowanie pasażerów	Większa świadomość zagrożeń, ograniczenie przypadków agresji i zachowań ryzykownych
Procedury awaryjne i plany kryzysowe	Ewakuacja, współpraca z PSP i Policją, symulacje zdarzeń	Skrócenie czasu reakcji na wypadki, lepsze skoordynowanie działań między służbami
Cyfryzacja i systemy ITS	Inteligentne sterowanie ruchem, analiza wideo, predykcja incydentów	Optymalizacja tras, wczesne wykrywanie zagrożeń, poprawa punktualności i koordynacji
Wdrażanie dobrych praktyk i innowacji	Patrole rowerowe, aplikacje mobilne, współpraca z NGO	Wzrost poczucia bezpieczeństwa pasażerów, większe zaangażowanie społeczne

Źródło: opracowanie własne.

Zebrane przykłady pokazują, że skuteczne zarządzanie bezpieczeństwem w transporcie zbiorowym wymaga nie tylko inwestycji infrastrukturalnych, ale również długofalowej polityki prewencyjnej, ciągłego doskonalenia procedur oraz współpracy między różnymi podmiotami: przewoźnikami, służbami porządkowymi, samorządem i społecznością lokalną. Analiza strategii wdrażanych w polskich aglomeracjach może stanowić podstawę do formułowania rekomendacji i standaryzacji działań w skali krajowej.

Ocena skuteczności działań i rekomendacje

Analiza wdrożonych w polskich aglomeracjach strategii zarządzania bezpieczeństwem w transporcie publicznym pozwala stwierdzić, że wiele z nich przyniosło wymierne efekty, choć ich skuteczność w dużym stopniu zależała od stopnia koordynacji działań i poziomu zaawansowania organizacyjnego poszczególnych miast (Klonowska i in., 2022). Działania

o charakterze technicznym, takie jak rozwój systemów monitoringu wizyjnego (CCTV) oraz montaż przycisków alarmowych w pojazdach i na przystankach, znacząco przyczyniły się do ograniczenia aktów wandalizmu, kradzieży oraz agresji wobec pasażerów i pracowników transportu. Obecność kamer działała nie tylko odstraszająco, lecz także pozwalała na szybkie reagowanie w przypadku wystąpienia incydentu oraz dokumentowanie przebiegu zdarzenia.

Dużą rolę w poprawie bezpieczeństwa odegrały również działania prewencyjne. Kampanie informacyjne skierowane do pasażerów, jak i specjalistyczne szkolenia dla kierowców i motorniczych z zakresu reagowania w sytuacjach kryzysowych, udzielania pierwszej pomocy czy obsługi trudnych pasażerów, zwiększyły kompetencje personelu i ograniczyły ryzyko eskalacji zagrożeń. W wielu miastach wzrosła też świadomość społeczna w zakresie reagowania na niebezpieczne sytuacje, co przełożyło się na większą liczbę zgłoszeń oraz szybszą identyfikację incydentów. Wielkie katastrofy nie zdarzają się często, dlatego też trudno oczekiwać stałej presji społeczeństwa, by utworzyć niezależną instytucję zajmującą się kontrolą stanu systemu bezpieczeństwa w transporcie, a gdy katastrofa się wydarzy, obiektywnych badań jej przyczyn i okoliczności (Krystek i in., 2008, s. 435).

Istotnym elementem zarządzania ryzykiem w transporcie zbiorowym okazały się procedury awaryjne oraz plany reagowania kryzysowego. W aglomeracjach takich jak Warszawa, Kraków czy Gdańsk regularnie organizowano ćwiczenia z udziałem służb ratunkowych i przewoźników, pozwalające na sprawdzenie sprawności ewakuacji, komunikacji między jednostkami oraz weryfikację aktualności procedur. Działania te skutkowały skróceniem czasu reakcji na zdarzenia i lepszym przygotowaniem załóg do sytuacji nagłych.

Coraz większe znaczenie w ocenie skuteczności działań odgrywały rozwiązania cyfrowe i inteligentne systemy zarządzania ruchem (ITS). Wdrożenie systemów GPS, czujników w pojazdach, dynamicznych tablic informacyjnych oraz integracja danych w czasie rzeczywistym umożliwiły lepsze planowanie kursów, szybsze reagowanie na zakłócenia oraz dokładniejszy monitoring bezpieczeństwa. W niektórych miastach, takich jak Wrocław czy Poznań, zastosowano także rozwiązania mobilne – aplikacje umożliwiające pasażerom zgłaszanie incydentów, opóźnień czy zagrożeń

bezpośrednio do centrów operacyjnych. Na szczególną uwagę zasługują również innowacyjne rozwiązania i lokalne inicjatywy zwiększające zaangażowanie społeczne. Patrole rowerowe Straży Miejskiej w okolicach przystanków z dodatkowymi punktami alarmowymi oraz partnerstwa z organizacjami pozarządowymi na rzecz przeciwdziałania przemocy w przestrzeni publicznej – to działania, które w sposób pośredni, lecz bardzo efektywny, wpływały na poprawę poczucia bezpieczeństwa i kultury podróżowania.

Zgromadzone dane oraz obserwacje funkcjonowania poszczególnych systemów pozwalają sformułować kilka podstawowych rekomendacji. Po pierwsze, wskazana jest dalsza standaryzacja systemów monitoringu i systemów alarmowych w pojazdach oraz na infrastrukturze przystankowej, co pozwoli na pełniejszą integrację analiz i szybszą reakcję służb. Po drugie, konieczne jest kontynuowanie i rozwijanie działań edukacyjnych – zarówno wśród pasażerów, jak i wśród pracowników transportu – poprzez regularne szkolenia i kampanie społeczne. Po trzecie, warto inwestować w cyfryzację i narzędzia analityczne, w tym aplikacje do zgłaszania zagrożeń i integrację danych w czasie rzeczywistym, które wspierają podejmowanie decyzji operacyjnych. Po czwarte, zalecane jest dalsze prowadzenie ćwiczeń kryzysowych we współpracy z odpowiednimi służbami, co pozwoli doskonalić procedury i budować odporność operacyjną systemu. Wreszcie, warto rozwijać partnerstwa lokalne i społeczne formy zaangażowania w bezpieczeństwo, które budują współodpowiedzialność i zaufanie do instytucji publicznych.

Skuteczne zarządzanie bezpieczeństwem w transporcie publicznym wymaga podejścia zintegrowanego, opartego na synergii technologii, kompetencji, organizacji i współpracy społecznej. Kierunki przyszłych badań powinny także obejmować strategie integracji transportu miejskiego z regionalnym oraz krajowym, aby stworzyć spójny system komunikacyjny odpowiadający na potrzeby zarówno mieszkańców, jak również osób dojeżdżających do pracy czy odwiedzających miasto (Handzel, 2023, s. 52). Wdrożenie Systemu Zarządzania Bezpieczeństwem przez przewoźników komunikacji zbiorowej nie powinno być postrzegane wyłącznie jako obowiązek wynikający z przepisów prawa czy rekomendacji instytucji unijnych, lecz przede wszystkim jako odpowiedź na rosnące oczekiwania społeczne wobec zapewnienia wysokiego poziomu bezpieczeństwa w transporcie publicznym (Sitarz, Chruzik, 2012, s. 26).

Ocena działań wdrożonych w polskich miastach potwierdza, że kompleksowe i wielowymiarowe strategie zarządzania ryzykiem przynoszą mierzalne efekty i powinny być rozwijane w sposób systemowy, z uwzględnieniem lokalnych uwarunkowań oraz perspektywy użytkowników systemu.

Podsumowanie

Bezpieczeństwo transportu publicznego w aglomeracjach miejskich stanowi jedno z kluczowych wyzwań współczesnego zarządzania miejskiego. Przeprowadzona analiza wykazała, że systematyczny wzrost liczby pasażerów, zwiększone nasycenie przestrzeni miejskiej pojazdami oraz złożoność zagrożeń stawiają wysokie wymagania wobec instytucji odpowiedzialnych za organizację i funkcjonowanie komunikacji zbiorowej.

Dane statystyczne potwierdzają utrzymującą się skalę zagrożeń związanych z wypadkami drogowymi, kolizjami, incydentami pasażerskimi i interwencjami służb porządkowych. Choć w ostatnim roku odnotowano spadek liczby wypadków, to nadal wysoka liczba poszkodowanych oraz znaczny udział innych uczestników ruchu jako sprawców wskazują na konieczność dalszych działań systemowych. W tym kontekście niezwykle istotne okazują się strategie zarządzania ryzykiem – zarówno oparte na technologiach (monitoring, systemy ITS), jak i na działaniach organizacyjnych, edukacyjnych i społecznych.

Ocena skuteczności wdrożonych rozwiązań wykazała, że największe efekty przynosi zintegrowane podejście łączące infrastrukturę, szkolenia, procedury awaryjne, cyfrowe narzędzia zarządzania oraz współpracę z mieszkańcami i organizacjami pozarządowymi. Wdrożenie inteligentnych systemów transportowych, aplikacji do zgłaszania zagrożeń, a także lokalnych inicjatyw bezpieczeństwa znacząco poprawia poziom ochrony pasażerów i wpływa na kształtowanie kultury bezpiecznego podróżowania.

Wnioski z przeprowadzonych analiz prowadzą do konkluzji, że skuteczne zarządzanie bezpieczeństwem w transporcie publicznym wymaga stałego monitoringu sytuacji, elastyczności działań, wzmacniania współpracy instytucjonalnej oraz aktywnego włączania użytkowników systemu. Tylko kompleksowe i adaptacyjne podejście do zagrożeń pozwoli na stworzenie odpornych, dostępnych i bezpiecznych systemów transportowych w polskich miastach.

Literatura

1. Gabryelewicz, I., Sadłowska-Wrzesińska, J. (2014). Systemowe zarządzanie bezpieczeństwem w transporcie drogowym. *Logistyka, 5*, 442-452.
2. Glanert, K. (2024). *Innowacje w bezpieczeństwie transportu miejskiego: Nowe technologie i praktyki.* W: S. Skiba (red.), *Współczesne trendy w transporcie* (s. 56-66). Uniwersytet Morski w Gdyni.
3. GUS. (b.d.). *Bank Danych Lokalnych: Pojazdy samochodowe i ciągniki*. Główny Urząd Statystyczny. Pobrane z: https://bdl.stat.gov.pl/ (dostęp: 22.02.2026).
4. Handzel, L. (2023). Bezpieczeństwo transportu jako element zarządzania miastem: Wyzwania i rozwiązania na przykładzie Nowego Sącza. W: K. Dymura (red.), *Wyzwania dla bezpieczeństwa ruchu drogowego – aspekty prawne i społeczne* (s. 43-52). Akademia Nauk Stosowanych w Nowym Sączu.
5. Janczarska-Bergel, K. (2021). Poziom bezpieczeństwa transportu zbiorowego jako jeden z głównych elementów jakości usług transportowych na przykładzie Krakowa. *Prace Komisji Geografii Przemysłu Polskiego Towarzystwa Geograficznego, 35*(1), 96-108.
6. Kasprzyk, Z. (2025). Zagadnienie modelowania bezpieczeństwa wymiany informacji w inteligentnych środkach transportu. *Journal of KONBiN, 55*(2), 157-170.
7. Klonowska, I., Lubiewski, P., Kuczyńska, E., Foryś, Ł. (2022). *Wybrane aspekty bezpieczeństwa ruchu drogowego: Obsługa zdarzeń drogowych przez Policję*. Instytut Wydawniczy EuroPrawo.
8. Krystek, R., Sitarz, M., Żurek, J., Gucma, S. (2008). Zintegrowany system bezpieczeństwa transportu. *Journal of KONBiN, 1*(1-4), 429-436.
9. Miasto Stołeczne Warszawa. (b.d.). *O aplikacji mobilnej – Warszawa 19115*. Pobrane z: https://warszawa19115.pl/o-aplikacji-mobilnej (dostęp: 22.02.2026).
10. Ochyra-Żurawska, K., Błażejewska, B., Spinek, B., Żurawski, S. (2024). Społeczne aspekty bezpieczeństwa w ruchu drogowym. *Studia Społeczne, 4*(47), 43-54.

11. Płachecka, M. (2016). Efekty działań na rzecz poprawy bezpieczeństwa w transporcie publicznym w Polsce. *Autobusy, 10*, 20-23.
12. Sitarz, M., Chruzik, K. (2012). System zarządzania bezpieczeństwem transportu zbiorowego. *Transport Miejski i Regionalny, 6*, 25-28.
13. Wydział Ruchu Drogowego Komendy Stołecznej Policji. (2025). *Analiza roczna stanu bezpieczeństwa w ruchu drogowym za 2024 rok.*
14. Zarząd Dróg Miejskich. (2024). *Raport o stanie bezpieczeństwa drogowego w Warszawie w 2024 roku.* Pobrane z: https://zdm.waw.pl/wp-content/uploads/2025/06/Raport-ZDM-2024__Online.pdf (dostęp: 22.02.2026).
15. Żukowska, J. (2013). Innowacyjne narzędzia zarządzania bezpieczeństwem transportu drogowego na poziomie regionalnym. *Autobusy. Technika, Eksploatacja, Systemy Transportowe, 3,* 2293-2303.

Ewelina Melaniuk[1]
Akademia Bialska im. Jana Pawł II, Biała Podlaska

https://doi.org/10.29316/9788368103373_18

TAKSONOMIA INCYDENTÓW RANSOMWARE 2024-2025

TAXONOMY OF RANSOMWARE INCIDENTS 2024-2025

Streszczenie

Ransomware pozostaje jednym z najbardziej dynamicznych zagrożeń w cyberprzestrzeni, a lata 2024-2025 przyniosły nowe, złożone formy ataków, w tym modele Ransomware-as-a-Service (RaaS), podwójne wymuszenia oraz złośliwe oprogramowanie wspomagane sztuczną inteligencją. Celem rozdziału jest opracowanie taksonomii incydentów ransomware w tym okresie. Analiza opiera się na raportach instytucjonalnych, dokumentach branżowych oraz literaturze naukowej. W badaniu wyróżniono cztery wymiary klasyfikacyjne: technikę ataku, wektor początkowego dostępu, strukturę organizacyjną sprawców oraz sektor ofiary. Dyskusja wyników obejmuje przykłady konkretnych incydentów oraz wskazuje na rosnącą adaptacyjność zagrożeń. Opracowana taksonomia może wspierać zespoły SOC, CERT oraz decydentów w monitorowaniu i reagowaniu na incydenty ransomware.

Słowa kluczowe: ransomware, taksonomia incydentów, RaaS, podwójne wymuszenia, cyberbezpieczeństwo, analiza zagrożeń

[1] https://orcid.org/0009-0002-9434-6258, e-mail: e.melaniuk@dyd.akademiabialska.pl

Abstract

Ransomware remains one of the most dynamic cyber threats, with 2024-2025 witnessing increasingly complex attacks, including Ransomware-as-a-Service (RaaS), double extortion, and AI-assisted malware. The aim of this chapter is to propose a taxonomy of ransomware incidents during this period. The analysis is based on institutional reports, industry documents, and scientific literature. Four classification dimensions were identified: attack technique, initial access vector, organisational structure of perpetrators, and victim sector. The discussion includes concrete examples and highlights the growing adaptability of ransomware threats. The proposed taxonomy can support SOC teams, CERTs, and decision-makers in monitoring and responding to ransomware incidents.

Keywords: ransomware, incident taxonomy, RaaS, double extortion, cybersecurity, threat analysis

Wstęp

Ransomware od ponad dekady pozostaje jednym z najbardziej destrukcyjnych i dynamicznie ewoluujących zagrożeń w cyberprzestrzeni. Jego istota polega na połączeniu technicznych mechanizmów sabotażu informacyjnego z klasycznym wymuszeniem finansowym, co czyni go szczególnie skutecznym narzędziem cyberprzestępczym (ENISA, 2024). W latach 2024-2025 zagrożenie to nie tylko nie uległo osłabieniu, lecz przyjęło nowe, bardziej złożone formy organizacyjne i technologiczne, obejmujące m.in. model Ransomware-as-a-Service (RaaS), strategię podwójnego i potrójnego wymuszenia oraz coraz częstsze wykorzystanie narzędzi sztucznej inteligencji (IBM Security, 2024; Raz i in., 2025).

Zgodnie z danymi przedstawionymi w raporcie *Worldwide Ransomware 2024*, liczba globalnych incydentów ransomware w 2024 r. utrzymywała się na wysokim poziomie, pomimo intensyfikacji działań organów ścigania oraz międzynarodowych operacji wymierzonych w infrastrukturę przestępczą (Cyber Threat Intelligence Integration Center [CTIIC], 2025). Jednocześnie w 2025 r. zaobserwowano dalszą fragmentację ekosystemu ransomware, polegającą na wzroście liczby mniejszych, krótkotrwałych grup przestępczych, co znacząco utrudnia ich identyfikację i neutralizację (ESET, 2025). Istotnym problemem badawczym pozostaje brak jednolitej, aktualnej taksonomii incydentów ransomware, która uwzględniałaby współczesne

kryteria klasyfikacyjne, takie jak technika ataku, wektor początkowego dostępu, struktura organizacyjna sprawców czy sektor ofiary. Dotychczasowe ujęcia koncentrowały się głównie na aspektach technicznych złośliwego oprogramowania, pomijając kontekst operacyjny i ekonomiczny ataków (ENISA, 2024). Tymczasem raporty branżowe wskazują, że skuteczna analiza i reagowanie na incydenty ransomware wymagają podejścia wielowymiarowego, łączącego perspektywę techniczną, organizacyjną oraz sektorową (IBM Security, 2024).

Celem niniejszego rozdziału jest zaproponowanie systematycznej taksonomii incydentów ransomware z lat 2024-2025, która umożliwi uporządkowanie obserwowanych zjawisk oraz identyfikację dominujących trendów zagrożeń. Przyjęta klasyfikacja opiera się na analizie raportów instytucji międzynarodowych, firm zajmujących się cyberbezpieczeństwem oraz literatury naukowej, w tym najnowszych badań dotyczących automatyzacji i wykorzystania modeli językowych w tworzeniu złośliwego oprogramowania (CTIIC, 2025, Raz i in., 2025). Wyniki zaproponowanej taksonomii mogą stanowić istotne wsparcie dla zespołów SOC, CERT oraz decydentów odpowiedzialnych za zarządzanie ryzykiem cybernetycznym, a także przyczynić się do dalszych badań nad predykcją i ograniczaniem skutków ataków ransomware w środowiskach krytycznych.

Metodologia badań

W niniejszym rozdziale zastosowano jakościowo-ilościowe podejście badawcze, którego celem było opracowanie aktualnej i wielowymiarowej taksonomii incydentów ransomware w latach 2024-2025. Metodologia opiera się na analizie wtórnej danych pochodzących z raportów instytucjonalnych, dokumentów branżowych oraz literatury naukowej, co jest powszechnie stosowaną praktyką w badaniach nad zagrożeniami cybernetycznymi (ENISA, 2024).

Podstawowym źródłem danych były raporty o zagrożeniach ransomware publikowane przez instytucje międzynarodowe oraz firmy zajmujące się cyberbezpieczeństwem, w szczególności: raport *Worldwide Ransomware 2024* przygotowany przez Cyber Threat Intelligence Integration Center (CTIIC, 2025), *ENISA Threat Landscape 2024*, *IBM X-Force Threat Intelligence Index 2024* i raporty analityczne ESET z 2025 r. Źródła te zostały

wybrane ze względu na ich wysoką wiarygodność, cykliczność publikacji oraz szeroki zakres danych empirycznych, obejmujących analizę techniczną incydentów, a także kontekst organizacyjny i sektorowy (IBM Security, 2024; ESET, 2025).

Uzupełniająco wykorzystano publikacje naukowe, w tym prace poświęcone automatyzacji ataków i zastosowaniu sztucznej inteligencji w cyberprzestępczości, co pozwoliło na identyfikację nowych kategorii zagrożeń, takich jak ransomware wspomagane przez modele językowe (Raz i in., 2025).

Proces badawczy składał się z czterech etapów:

1. Selekcja i normalizacja danych – wyodrębniono opisy incydentów ransomware z lat 2024-2025, eliminując duplikaty oraz przypadki niejednoznacznie zaklasyfikowane w źródłach pierwotnych (CTIIC, 2025).
2. Analiza porównawcza – przeprowadzono porównanie sposobów klasyfikacji stosowanych w poszczególnych raportach, identyfikując wspólne oraz rozbieżne kryteria opisu incydentów (ENISA, 2024).
3. Kodowanie kategorii – na podstawie analizy jakościowej wyodrębniono kluczowe zmienne klasyfikacyjne, takie jak: technika ataku, wektor początkowego dostępu, model organizacyjny sprawców, sektor ofiary oraz potencjalny wpływ incydentu. Takie podejście odpowiada rekomendacjom dotyczącym badań nad złożonymi zagrożeniami cybernetycznymi (IBM Security, 2024).
4. Synteza i budowa taksonomii – na podstawie zakodowanych danych zaproponowano spójną strukturę taksonomiczną, umożliwiającą jednoczesną analizę techniczną i kontekstową incydentów ransomware (ENISA, 2024).

W części ilościowej wykorzystano analizę częstości występowania poszczególnych typów incydentów oraz trendów czasowych, zgodnie z danymi zagregowanymi w raportach branżowych (ESET, 2025). Część jakościowa obejmowała analizę treści opisów incydentów oraz strategii grup ransomware, co pozwoliło na identyfikację nowych wzorców działania, w tym fragmentacji grup przestępczych i adaptacyjnych modeli RaaS (CTIIC, 2025).

Zastosowana metodologia opiera się na danych wtórnych, co oznacza zależność od zakresu i jakości raportów źródłowych. Ponadto, ze względu na

niejawny charakter wielu incydentów ransomware, rzeczywista skala zjawiska może być niedoszacowana (ENISA, 2024). Niemniej jednak triangulacja źródeł pozwala na zwiększenie rzetelności i wiarygodności zaproponowanej taksonomii (IBM Security, 2024).

Wyniki i dyskusja

Analiza danych z lat 2024-2025 pozwoliła na wyodrębnienie kilku kluczowych kategorii incydentów ransomware oraz identyfikację dominujących trendów w tym okresie. Na podstawie raportów CTIIC (2025), ENISA (2024), IBM Security (2024) oraz ESET (2025) opracowano taksonomię obejmującą cztery wymiary klasyfikacyjne: technikę ataku, wektor początkowego dostępu, strukturę organizacyjną sprawców oraz sektor ofiary.

Technika ataku

Technika ataku definiuje sposób działania ransomware w systemach ofiary. Obejmuje metody szyfrowania danych, strategie wymuszeń oraz adaptacje do systemów obronnych. Analiza incydentów z lat 2024-2025 wskazuje, że współczesne ransomware ewoluuje w kierunku coraz bardziej złożonych i wielowarstwowych technik.

1. Encryption ransomware (szyfrujące).

Klasyczny wariant ransomware, w którym złośliwe oprogramowanie szyfruje pliki ofiary, uniemożliwiając dostęp do danych bez zapłaty okupu, nadal pozostaje istotnym zagrożeniem. Przykład stanowi atak grupy Conti na amerykańską firmę logistyczną w 2024 r., gdzie zaszyfrowano systemy magazynowe, powodując poważne zakłócenia w łańcuchu dostaw. Incydent ten pokazuje, że nawet w przypadku tradycyjnych technik, skala i precyzja ataków mogą generować ogromne straty finansowe i operacyjne (ENISA, 2024).

2. Double extortion ransomware (podwójne wymuszenie).

Wariant podwójnego wymuszenia stał się dominujący w 2024-2025 r. Atakujący nie tylko szyfrują dane, ale również kradną wrażliwe informacje i grożą ich ujawnieniem w przypadku braku zapłaty, zwiększając presję na ofiarę. Przykładem jest incydent grupy LockBit na rumuński szpital w 2025 r., gdzie oprócz szyfrowania dokumentacji medycznej, sprawcy grozili publikacją danych pacjentów w sieci. Ten typ ataku pokazuje rosnącą

rolę strategii psychologicznych w wymuszaniu okupu oraz potrzebę rozbudowanych procedur bezpieczeństwa danych (IBM Security, 2024).

3. AI-assisted ransomware (wspomagane sztuczną inteligencją).

Nowoczesne kampanie ransomware wykorzystują sztuczną inteligencję do automatyzacji ataków i generowania spersonalizowanego phishingu. W 2025 r. eksperymentalne kampanie w USA wykazały, że AI mogła tworzyć e-maile phishingowe dostosowane do profili zawodowych pracowników korporacji finansowej, zwiększając skuteczność infekcji. Ransomware wspomagany AI może również adaptować swoje działanie w czasie rzeczywistym, np. omijać antywirusy i systemy monitoringu, co podkreśla rosnącą złożoność i trudność w wykrywaniu takich zagrożeń (Raz i in., 2025).

4. Multi-stage attacks (wieloetapowe ataki).

W 2024-2025 r. coraz częściej obserwowano wieloetapowe kampanie, w których ransomware był tylko jednym z elementów ataku. Przykładem jest kampania grupy Akira w Hiszpanii, w której najpierw włamano się do systemu poprzez niezaktualizowaną podatność, następnie przejęto konta administracyjne, a dopiero w końcowej fazie wprowadzono złośliwe oprogramowanie szyfrujące dane. Takie podejście umożliwia sprawcom maksymalizację zysków oraz minimalizację ryzyka wykrycia w początkowych etapach ataku (ENISA, 2024).

5. Targeted ransomware campaigns (atakowane precyzyjnie sektory).

Coraz częściej obserwuje się ataki skoncentrowane na określonych sektorach, np. szpitalach, administracji publicznej czy instytucjach edukacyjnych. Przykład: atak grupy REvil na uniwersytet w Wielkiej Brytanii w 2024 r., w którym ransomware został dostosowany do środowiska sieciowego uczelni i zabezpieczeń serwerów. Skierowane kampanie pozwalają sprawcom zoptymalizować kod malware, zwiększając jego skuteczność i maksymalizując straty ofiary (ESET, 2025).

Analiza wskazuje, że współczesne ransomware nie jest już jednorodnym zagrożeniem. Trendy w latach 2024-2025 pokazują:

- rosnącą rolę strategii podwójnego wymuszenia i presji psychologicznej na ofiarach,
- wprowadzenie AI i automatyzacji w procesach ataków, zwiększających skuteczność i adaptacyjność malware,

- coraz częstsze stosowanie wieloetapowych kampanii i technik hybrydowych, łączących phishing, eksploatację podatności i przejęcie poświadczeń,
- dopasowanie ataków do specyfiki sektorów ofiary, co zwiększa ich skuteczność i skalę strat (ENISA, 2024; IBM Security, 2024; Raz i in., 2025).

Wyniki te podkreślają, że skuteczna obrona wymaga wielowarstwowej ochrony, obejmującej systemy detekcji i reakcji, edukację użytkowników, szybkie aktualizacje oprogramowania oraz monitorowanie hybrydowych i zautomatyzowanych ataków.

Wektor początkowego dostępu

Wektor początkowego dostępu to metoda, za pomocą której ransomware infiltruje system ofiary, inicjując cały proces ataku. Analiza danych z lat 2024-2025 wskazuje, że pomimo rozwoju technik obronnych nadal phishing i spear-phishing pozostają dominującymi punktami wejścia, odpowiadającymi za 38-40% wszystkich incydentów (ESET, 2025). Przykładem jest atak grupy REvil na firmę usługową w Wielkiej Brytanii w 2024 r., w którym pracownik nieświadomie otworzył złośliwy link w e-mailu podszywającym się pod komunikat bankowy, umożliwiając zainstalowanie się ransomware na firmowych serwerach. Incydent ten ilustruje, że techniki socjotechniczne pozostają skuteczne nawet w organizacjach z częściową świadomością zagrożeń.

Drugim istotnym wektorem są ataki oparte na eksploatacji podatności w systemach i aplikacjach, w tym zarówno tzw. zero-day, jak i n-day vulnerabilities. W 2024 r. grupa Akira przeprowadziła atak na administrację miejską w Hiszpanii, wykorzystując niezaktualizowaną podatność w oprogramowaniu serwera WWW, co pozwoliło na zdalną instalację ransomware i szyfrowanie danych krytycznych. Ten przypadek pokazuje, że brak systematycznej aktualizacji systemów operacyjnych i aplikacji stanowi wciąż istotny punkt wejścia dla cyberprzestępców (ENISA, 2024).

Kolejnym coraz częściej wykorzystywanym kanałem jest kompromitacja poświadczeń, w tym ataki typu brute force lub credential stuffing na zdalny dostęp (RDP, VPN). Przykład ataku na szpital w USA w 2025 r. pokazuje, że przejęcie loginów administratora VPN umożliwiło sprawcom

nieograniczony dostęp do wewnętrznych sieci i danych pacjentów, co podkreśla znaczenie silnej polityki haseł oraz mechanizmów uwierzytelniania wieloskładnikowego (IBM Security, 2024).

W ostatnich latach wyraźnie wzrasta znaczenie ataków poprzez łańcuchy dostaw i dostawców usług trzecich. Przykładem jest incydent w 2025 r., w którym atak na dostawcę oprogramowania księgowego doprowadził do infekcji ransomware u kilkudziesięciu klientów firmy. Ten przypadek pokazuje, że współczesne zagrożenia są coraz bardziej powiązane z globalnymi sieciami powiązań biznesowych i że bezpieczeństwo organizacji nie zależy wyłącznie od własnych systemów, ale także od zabezpieczeń partnerów i dostawców (CTIIC, 2025).

Struktura organizacyjna sprawców

Analiza struktury sprawców ransomware w latach 2024-2025 pokazuje, że rynek cyberprzestępczy pozostaje zróżnicowany i dynamiczny. Dominują wciąż duże, zorganizowane grupy ransomware, takie jak LockBit i Akira, prowadzące długofalowe, kompleksowe kampanie ataków. Przykładem jest kampania LockBit 3.0 w USA w 2024 r., obejmująca kilkadziesiąt instytucji finansowych i usługowych. Incydent ten pokazał profesjonalizację tych grup, w tym posiadanie dedykowanych zespołów ds. programowania malware, działów marketingu w celu koordynowania afiliacji i skutecznego egzekwowania wymuszeń finansowych. Skala i precyzja ataku dowodzą, że nowoczesne grupy ransomware funkcjonują niemal jak legalne przedsiębiorstwa o rozbudowanej strukturze operacyjnej (CTIIC, 2025).

Jednocześnie rozwój modelu Ransomware-as-a-Service (RaaS) umożliwia mniej doświadczonym przestępcom przeprowadzanie ataków na szeroką skalę, co w praktyce oznacza demokratyzację narzędzi przestępczych. Przykład RaaS „Hive" w 2025 r. pokazuje, że nawet pojedynczy afiliant w Europie lub Ameryce Południowej mógł przeprowadzić atak na szkoły, małe przedsiębiorstwa i instytucje kulturalne, przy czym twórcy RaaS pobierali procent od okupów. Ten model zwiększa globalną penetrację rynku ransomware, a jednocześnie utrudnia identyfikację faktycznych sprawców, ponieważ grupa tworząca malware i grupa realizująca atak mogą być całkowicie oddzielne (ENISA, 2024).

Kolejnym istotnym trendem jest wzrost liczby małych, efemerycznych grup przestępczych, takich jak CyberVolk w Niemczech w 2025 r. Takie grupy działają sezonowo, przez kilka tygodni lub miesięcy, celując w lokalne przedsiębiorstwa i wykorzystując luki w zabezpieczeniach często niedostrzegane przez większe grupy. Fragmentacja rynku sprawców zwiększa trudność w monitorowaniu zagrożeń oraz wymaga od zespołów bezpieczeństwa adaptacyjnych strategii reagowania, które obejmują szybką identyfikację nowych podmiotów oraz aktualizację reguł detekcji (ESET, 2025; Raz i in., 2025). Dodatkowo w literaturze wskazuje się na elastyczne i hybrydowe struktury organizacyjne, w których grupy RaaS współpracują z niezależnymi programistami malware, ekspertami od phishingu i brokerami danych. Taka modularna organizacja umożliwia szybkie skalowanie kampanii, testowanie nowych technik ataku i szybką adaptację do działań organów ścigania. Przykładem jest międzynarodowa kampania LockBit w 2024 r., w której do ataków użyto afiliantów w Europie Wschodniej i Ameryce Północnej, a infrastruktura do wymuszeń była koordynowana centralnie przez grupę macierzystą (CTIIC, 2025).

Wnioski płynące z obserwacji struktury sprawców wskazują, że skuteczna obrona wymaga ścisłego monitorowania ekosystemu cyberprzestępczego, w tym rozpoznawania nowych grup RaaS, śledzenia afiliantów oraz reagowania na hybrydowe modele ataków. Zrozumienie organizacyjnej dynamiki sprawców pozwoli przewidywać skalę i kierunki ataków oraz opracowywać strategie prewencji i wczesnego ostrzegania dla instytucji publicznych i prywatnych.

Sektor ofiary

Analiza sektorów ofiar w latach 2024-2025 wskazuje, że największe zagrożenie dotyczy infrastruktury krytycznej, administracji publicznej i sektora edukacyjnego. Przykładem jest atak na rumuńską stację wodociągową w 2025 r., w wyniku którego tymczasowo wstrzymano dystrybucję wody w kilku miastach. Incydent ten podkreśla wysokie potencjalne skutki społeczne ransomware'u i istotną rolę infrastruktury krytycznej w funkcjonowaniu państwa i społeczeństwa (ENISA, 2024). Podobnie w sektorze energetycznym, ataki na lokalne elektrownie i sieci przesyłowe wykazały, że

ransomware może sparaliżować systemy zarządzania, powodując przestoje produkcji i ryzyko dla bezpieczeństwa publicznego (CTIIC, 2025).

W sektorze prywatnym ransomware powoduje poważne straty finansowe i operacyjne, szczególnie w przedsiębiorstwach logistycznych, produkcyjnych i finansowych. Atak na firmę logistyczną w USA w 2025 r. doprowadził do zatrzymania systemów magazynowych i spedycyjnych, generując straty liczone w milionach dolarów. W takich przypadkach konieczne były również pilne inwestycje w systemy bezpieczeństwa IT oraz audyty infrastruktury, co pokazuje długofalowy koszt incydentów (IBM Security, 2024).

Nowym trendem w latach 2024-2025 jest celowanie w instytucje kultury, badań i archiwa cyfrowe, które dotychczas były traktowane jako mniej atrakcyjne cele. Przykładem jest atak na bibliotekę narodową w Europie Środkowej w 2025 r., gdzie zaszyfrowano katalogi cyfrowe i dokumenty historyczne. Atak ten pokazuje, że cyberprzestępcy rozszerzają pole działania na podmioty, które posiadają wartościowe zasoby, ale często dysponują słabszymi mechanizmami ochrony (ESET, 2025). Dodatkowo w literaturze branżowej zauważono rosnącą liczbę ataków sektorowo ukierunkowanych, w których ransomware jest dostosowany do specyfiki infrastruktury ofiary. Przykładem jest kampania grupy LockBit 3.0 w 2024 r., skierowana do instytucji edukacyjnych i uczelni wyższych w Europie, gdzie kod malwaru był zoptymalizowany do działania w środowisku sieciowym kampusów, omijając standardowe zabezpieczenia serwerów edukacyjnych. Takie celowane podejście pozwala sprawcom na zwiększenie skuteczności ataków oraz maksymalizację presji finansowej na ofiary (ENISA, 2024; IBM Security, 2024).

Analiza sektorów ofiar wskazuje, że różnorodność celów rośnie, a nowoczesne kampanie ransomware nie ograniczają się już do dużych firm czy instytucji publicznych. Zrozumienie specyfiki ataków w poszczególnych sektorach umożliwia priorytetyzację zasobów obronnych i opracowanie strategii prewencji dostosowanej do rodzaju działalności, potencjalnych strat i wartości danych (CTIIC, 2025; ESET, 2025).

Dyskusja i wnioski

Wyniki badań wskazują, że zagrożenia ransomware w latach 2024-2025 cechują się wielowymiarową dynamiką, obejmującą ewolucję

techniczną i zmiany w strukturze organizacyjnej sprawców. Wyodrębnione w rozdziale kategorie klasyfikacyjne – technika ataku, wektor początkowego dostępu, struktura przestępcza oraz sektor ofiary – pozwalają uporządkować istniejące incydenty i jednocześnie identyfikować predyktory przyszłych zagrożeń, takie jak rosnące wykorzystanie sztucznej inteligencji w kampaniach ransomware czy fragmentacja ekosystemu przestępczego (ENISA, 2024; Raz i in., 2025).

Analiza wskazuje, że techniki ataku ewoluują w kierunku podwójnych i zautomatyzowanych wymuszeń. Ataki typu double extortion, w których oprócz szyfrowania danych następują kradzież i groźba publikacji, stają się standardem w działaniach grup takich jak LockBit czy Conti (IBM Security, 2024). W 2025 r. pojawienie się AI-assisted ransomware umożliwiało automatyzację generowania spersonalizowanych wiadomości phishingowych i adaptacyjne omijanie systemów ochrony, co zwiększa skuteczność ataków i trudność w ich wykrywaniu (Raz i in., 2025).

Wektory początkowego dostępu również stają się coraz bardziej złożone. Phishing, wykorzystanie podatności w systemach (zero-day i n-day) oraz ataki przez łańcuchy dostaw i dostawców usług trzecich umożliwiają sprawcom różnorodne ścieżki infiltracji, co zwiększa skuteczność kampanii ransomware i utrudnia obronę (CTIIC, 2025; ESET, 2025). Przykłady ataków na dostawcę oprogramowania księgowego w 2025 r. pokazują, że nawet organizacje o wysokim poziomie zabezpieczeń mogą zostać dotknięte pośrednio przez słabsze ogniwa w globalnych sieciach biznesowych.

Struktury sprawców stają się coraz bardziej zróżnicowane i elastyczne. Dominują duże, profesjonalne grupy, takie jak LockBit i Akira, prowadzące długofalowe kampanie, a także mniejsze, efemeryczne podmioty działające sezonowo, często korzystające z modeli RaaS (ENISA, 2024; ESET, 2025). Fragmentacja ekosystemu sprawców zwiększa trudność monitorowania i wymaga od zespołów SOC i CERT szybkiej adaptacji, np. poprzez śledzenie afiliantów RaaS i identyfikowanie nowych grup przestępczych.

Sektor ofiary determinuje charakter strat i skutki społeczne incydentów. W przypadku infrastruktury krytycznej, stacji wodociągowych czy elektrowni ransomware może prowadzić do zakłóceń w dostępie do podstawowych usług publicznych (ENISA, 2024). W sektorze prywatnym skutki są przede wszystkim finansowe, np. w ataku na firmę logistyczną w USA

w 2025 r., gdzie zatrzymanie systemów spedycyjnych wygenerowało straty liczone w milionach dolarów (IBM Security, 2024). Warto również zauważyć trend atakowania instytucji kultury i badań, takich jak biblioteki cyfrowe, gdzie straty mają charakter niematerialny, ale o dużej wartości historycznej i edukacyjnej (ESET, 2025).

Taksonomia opracowana w rozdziale stanowi narzędzie praktyczne dla zespołów SOC i CERT, umożliwiające skuteczniejsze monitorowanie, klasyfikowanie i raportowanie incydentów ransomware. Może również służyć jako podstawa dla badań prognostycznych, pozwalających przewidywać kierunki rozwoju zagrożeń i identyfikować potencjalne cele ataków (Raz i in., 2025; ESET, 2025).

Wyniki badań podkreślają również konieczność kompleksowego podejścia do zarządzania ryzykiem cybernetycznym, obejmującego:

- wdrożenie i aktualizację oprogramowania zabezpieczającego,
- edukację użytkowników i szkolenia z zakresu bezpieczeństwa informacji,
- monitorowanie łańcuchów dostaw i bezpieczeństwa partnerów biznesowych,
- współpracę międzynarodową oraz wymianę informacji wywiadowczych między podmiotami publicznymi i prywatnymi.

Tylko strategia wielowarstwowa, uwzględniająca aspekty techniczne i organizacyjne, może skutecznie ograniczyć ryzyko i konsekwencje ataków ransomware, zwłaszcza w sektorach najbardziej narażonych (CTIIC, 2025; ENISA, 2024; IBM Security, 2024).

Podsumowanie wniosków

1. Ransomware rozwija się w kierunku podwójnych wymuszeń i automatyzacji, w tym z użyciem AI.
2. Wektory początkowego dostępu są coraz bardziej złożone i obejmują phishing, podatności systemowe oraz łańcuchy dostaw.
3. Struktury sprawców są zróżnicowane – od dużych, profesjonalnych grup po efemeryczne podmioty korzystające z RaaS.
4. Sektor ofiary determinuje charakter strat i wymusza różne strategie obrony.

5. Kompleksowa strategia ochrony obejmująca technologie, edukację, monitoring partnerów oraz współpracę międzynarodową jest kluczowa dla ograniczenia skutków incydentów.

Literatura

1. Cyber Threat Intelligence Integration Center. (2025). *Worldwide ransomware, 2024: Increasing rate of attacks tempered by law enforcement disruptions.* Office of the Director of National Intelligence. Pobrane z: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf (dostęp: 22.02.2026).
2. ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. Pobrane z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 22.02.2026).
3. ESET. (b.d.). *Polska najczęściej na świecie atakowana ransomware w 2025 roku.* Pobrane z: https://www.eset.com/pl/about/newsroom/press-releases/news/polska-najczesciej-na-swiecie-atakowana-ransomware-w-2025-roku/ (dostęp: 22.02.2026).
4. IBM Security. (2024). *X-Force threat intelligence index 2024. IBM Corporation*. Pobrane z: https://www.ibm.com/reports/threat-intelligence (dostęp: 22 lutego 2026).
5. Raz, M., Udeshi, M., Sai Charan, P. V., Krishnamurthy, P., Khorrami, F., Karri, R. (2025). *Ransomware 3.0: Self-composing and LLM-orchestrated. arXiv.* https://doi.org/10.48550/arXiv.2508.20444

Elżbieta Cygnar[1]
Akademia Nauk Stosowanych w Nowym Sączu
Agata Bubenko[2]
Sławomir Żurawski[3]
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

https://doi.org/10.29316/9788368103373_19

CYBERBEZPIECZEŃSTWO DZIECI I MŁODZIEŻY W DOBIE WSPÓŁCZESNYCH ZAGROŻEŃ

CYBERSECURITY FOR CHILDREN AND YOUNG PEOPLE IN THE AGE OF MODERN THREATS

Streszczenie

Celem rozdziału jest przedstawienie i omówienie współczesnych wyzwań dotyczących ochrony dzieci i młodzieży w środowisku cyfrowym. W pierwszej części rozdziału omówiono istotę cyberprzestrzeni jako nowego środowiska życia, nauki i rozwoju dzieci oraz młodzieży. Autorzy analizują definicje pojęcia „cyberprzestrzeń", wskazując na jej dynamiczny, interaktywny i wirtualny charakter, który w znacznym stopniu wpływa na sposób komunikacji i funkcjonowania młodego pokolenia. W kolejnej części opisano główne zagrożenia, na jakie narażone są dzieci i młodzież w cyberprzestrzeni. Zjawiska te zostały poparte wynikami badań i raportów

[1] https://orcid.org/0009-0004-5377-9588, e-mail: ecygnar@ans-ns.edu.pl
[2] https://orcid.org/0009-0005-3152-9884
[3] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet,pl

międzynarodowych instytucji, takich jak NASK, EU Kids Online, WHO czy Europol. Następna część rozdziału poświęcona została analizie aspektów prawnych i instytucjonalnych związanych z ochroną dzieci w sieci. Problem badawczy został sformułowany w następujący sposób: w jaki sposób można skutecznie chronić dzieci i młodzież przed współczesnymi zagrożeniami w cyberprzestrzeni? Przyjęta hipoteza badawcza zakłada, że skuteczna ochrona najmłodszych użytkowników Internetu wymaga zintegrowanego podejścia, łączącego działania edukacyjne, profilaktyczne i prawne z rozwijaniem kompetencji cyfrowych oraz współpracą szkoły, rodziny i instytucji publicznych. W ramach metodyki badań wykorzystano analizę literatury przedmiotu, aktów prawnych, raportów instytucji zajmujących się bezpieczeństwem cyfrowym, a także analizę porównawczą wybranych programów edukacyjnych realizowanych w Polsce i na świecie. Z przeprowadzonej analizy wynika, że ochrona dzieci i młodzieży w środowisku cyfrowym wymaga podejścia interdyscyplinarnego, łączącego wiedzę z zakresu pedagogiki, psychologii, technologii informacyjnych i prawa. Kluczową rolę odgrywają edukacja cyfrowa, rozwijanie świadomości zagrożeń, kształtowanie odpowiedzialnych postaw wśród uczniów, rodziców i nauczycieli oraz budowanie empatii i odpowiedzialności w kontaktach online.

Słowa kluczowe: cyberbezpieczeństwo, dzieci i młodzież, cyberprzemoc, edukacja cyfrowa, ochrona prawna

Abstract

The aim of the article is to present and discuss contemporary challenges regarding the protection of children and young people in the digital environment. The first part of the article presents the essence of cyberspace as a new environment for the living, learning and development of children and young people. The authors analyse the definitions of the term "cyberspace", highlighting its dynamic, interactive, and virtual character, which significantly affects how the younger generation communicates and functions. The next part describes the main threats to which children and young people are exposed in cyberspace. Each of these phenomena has been supported by research findings and reports from international institutions such as NASK, EU Kids Online, WHO, and Europol. The next part of the article analyses the legal and institutional aspects of protecting children online. The research problem was formulated in: how can children and young people be effectively protected from modern threats in cyberspace? The adopted research hypothesis assumes that effective protection of the youngest Internet users requires an integrated approach, combining educational, preventive and legal activities with the development of digital competences and cooperation between the school, family and public institutions. As part of the research methodology, an analysis of the literature on the subject, legal acts, reports of institutions dealing with digital security, and a comparative analysis of selected educational programs implemented in Poland and around the world were used. The

analysis shows that protecting children and young people in the digital environment requires an interdisciplinary approach that combines knowledge from pedagogy, psychology, information technology, and law. Digital education plays a key role, developing awareness of risks, shaping responsible attitudes among students, parents and teachers, and building empathy and responsibility in online contacts.

Keywords: cybersecurity, children and young people, cyberbullying, digital education, legal protection

Wstęp

Współczesny świat rozwija się w niewyobrażalnie szybkim tempie. Szczególny wpływ ma na to stale postępujący proces globalizacji, który sprawia, iż staje się on jedną wielką informacyjną wioską. Dynamiczny rozwój technologii informacyjno-komunikacyjnych (TIK) w ostatnich dekadach w sposób zasadniczy przekształcił codzienne funkcjonowanie jednostki w społeczeństwie. Internet stał się powszechnym narzędziem komunikacji, edukacji, pracy i rozrywki, a jego dostępność sprawiła, że również dzieci i młodzież coraz częściej korzystają z zasobów cyfrowego świata. Młode pokolenie, dorastające w warunkach cyfrowej immersji, określane mianem „cyfrowych tubylców", cechuje się wysokim poziomem kompetencji technicznych, lecz nierzadko niską świadomością zagrożeń wynikających z aktywności online. Rozwój technologii informacyjno-komunikacyjnych zrewolucjonizował życie człowieka, usprawnił jego funkcjonowanie w wielu obszarach, jednakże znacząco poszerzył katalog istniejących zagrożeń. Jako że tzw. cyberprzestrzeń stała się głównym obszarem funkcjonowania dużej części społeczeństwa, istotną jest zatem kwestia wszelkich zagrożeń płynących z nieograniczonych wręcz możliwości przebywania w tejże „cyberprzestrzeni".

Wzrost obecności przede wszystkim młodych użytkowników w przestrzeni wirtualnej niesie ze sobą liczne ryzyka, takie jak cyberprzemoc, kontakt z niepożądanymi treściami, uzależnienie od mediów cyfrowych, nadużywanie mediów społecznościowych, manipulacja informacyjna czy nieuprawnione przetwarzanie danych osobowych. Problemy te mają charakter interdyscyplinarny, obejmujący aspekty psychologiczne, społeczne, pedagogiczne i prawne, co sprawia, że kwestia cyberbezpieczeństwa najmłodszych staje się jednym z kluczowych wyzwań współczesnej edukacji i polityki bezpieczeństwa informacyjnego.

Cyberprzestrzeń jako środowisko rozwoju dzieci i młodzieży

Termin „cyberprzestrzeń" pojawił się po raz pierwszy w 1984 roku w opowiadaniu „Wypalić Chrom" autorstwa pisarza *science fiction* Williama Gibsona, według którego jest to konsensusowa halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników, niejako graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Określenie „cyberprzestrzeń" zostało przeniesione zatem z literackiej formy na kształtującą się nową rzeczywistość w świecie (Konieczniak, 2011). Pierre Lévy charakteryzuje cyberprzestrzeń jako przestrzeń możliwości otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie. Podkreśla fundamentalną cechę cyberprzestrzeni, czyli jej cyfrowy charakter, który jest „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny" (Lévy, 2002).

Definiując cyberprzestrzeń, należy zwrócić przede wszystkim uwagę na znaczenia słów składających się na jej nazwę – cyber i przestrzeń. Bowiem termin cyber pochodzi od cybernetyki, czyli nauki o sterowaniu i komunikacji w systemach oraz przetwarzaniu informacji w tych systemach, zapoczątkowanej przez Norberta Wienera. Natomiast Margaret Mead uważa, iż: „cybernetyka – to forma interdyscyplinarnej myśli, która umożliwiła członkom różnych dyscyplin komunikację między sobą w języku zrozumiałym dla wszystkich". Zatem cyberprzestrzeń może być rozumiana jako przestrzeń komunikacji, gdzie sprzężenie zwrotne informacji pozwala na regulację systemów, wzajemne między nimi relacje, dynamiczny rozwój i wytyczanie szlaków (Konieczniak, 2011).

Cyberprzestrzeń często pojmowana jest po prostu jako rzeczywistość wirtualna, którą można wytłumaczyć, korzystając z angielskiej definicji słowa „wirtualny" – to jest: „symulowany, pełniący funkcję czegoś, co w istocie nie istnieje". Wobec powyższego, Piotr Sitarski dochodzi do stwierdzenia, że rzeczywistość wirtualna ma wszystkie cechy prawdziwego świata, oprócz jednej: istnienia (Konieczniak, 2011). Natomiast dynamika rozwoju Internetu i głębokie osadzenie współczesnego społeczeństwa w cyberprzestrzeni wskazują, iż ludzie zatracają się w tym nieprawdziwym świecie, bowiem wszystko dociera poprzez media, człowiek przenosi swoje życie do cyberprzestrzeni, a rzeczywistość realna i wirtualna przenikają się.

Zatem chyba najbardziej praktyczną definicją dla terminu „cyberprzestrzeń" jest dyrektywa 54 National Security Presidential, według której pojęcie to jest rozumiane jako wirtualne środowisko informacji i interakcji między ludźmi. Owe interakcje to bogaty zbiór odzwierciedlający zarówno pozytywne, jak i negatywne strony ludzkiej natury, wahający się od cyberautokreacji i autoekspresji do działań przestępczych prowadzących również do aktów terrorystycznych oraz możliwych konfliktów cybernetycznych. Dzieje się tak z powodu głównych cech cyberprzestrzeni, którymi są: brak granic, dynamiczne procesy i zjawiska oraz anonimowość użytkowników (Wochnowicz, 2023).

Internet jest aktualnie przestrzenią pracy i edukacji, ale również środowiskiem socjalizacji, rozrywki i samoekspresji. Zjawisko to szczególnie dotyczy dzieci i młodzieży, które dorastają w rzeczywistości cyfrowej, korzystając z technologii w sposób naturalny i intuicyjny, bowiem cyberprzestrzeń staje się miejscem, w którym młodzież kształtuje swoje relacje społeczne, tożsamość i kompetencje cyfrowe, to powoduje, że granice między światem realnym a wirtualnym stają się płynne, z zatem relacje, edukacja, rozrywka i komunikacja coraz częściej odbywają się w przestrzeni cyfrowej (Solecki, 2017). Współczesna młodzież określana jest często mianem cyfrowych tubylców (digital natives), czyli pokoleniem, które od najmłodszych lat funkcjonuje w otoczeniu technologicznym. Młodzi ludzie, to tubylcy „zamieszkali" w cyfrowym świecie. Cyberprzestrzeń stanowi dla nich całkowicie naturalne środowisko, do którego nie muszą się adaptować, bo postrzegają je jako „ojczyste". Po raz pierwszy tego terminu użył w swoim rozdziale w 2001 roku Marc Prensky, opisując pokolenie osób, które urodziły się w czasach, gdy technologie informatyczne dynamicznie się upowszechniały i zaczęły wkraczać w codzienne życie zwykłego człowieka. Internet przestawał powoli być domeną elit i pojawiał się w licznych gospodarstwach domowych, przeobrażając dotychczasową rzeczywistość i zapraszając do tej nowej – wirtualnej (Jabłońska, 2018).

Dzisiaj dzieci i nastolatki nie znają świata bez komputera, a Internet istniał dla nich „od zawsze", bowiem już kilkumiesięczne dzieci dostają do ręki smartfona i szybko uczą się go obsługiwać. Internet oferuje młodym ludziom niemal nieograniczone możliwości rozwoju, ale równocześnie naraża ich na szereg zagrożeń związanych z kontaktem z niepożądanymi treściami

czy cyberprzemocą. Aktualnie dla dzieci Internet pełni funkcję socjalizacyjną, edukacyjną i kulturową, ułatwia samokształcenie, rozwój zainteresowań oraz nabywanie kompetencji cyfrowych, które stanowią niezbędny element funkcjonowania w społeczeństwie wiedzy, oraz pozwala na stały kontakt z rówieśnikami. Jednocześnie należy zauważyć, że cyberprzestrzeń jest środowiskiem ambiwalentnym – sprzyja rozwojowi, ale także rodzi liczne zagrożenia. Nadmierna ekspozycja na bodźce cyfrowe może prowadzić do rozproszenia uwagi, spłycenia procesów poznawczych oraz obniżenia zdolności koncentracji. Istnieje również ryzyko uzależnienia od Internetu, które – jak wskazują badania – może skutkować izolacją społeczną, obniżeniem nastroju, a nawet zaburzeniami emocjonalnymi. Cyberprzemoc, hejt czy kontakt z nieodpowiednimi treściami stanowi kolejne czynniki negatywnie oddziałujące na rozwój psychospołeczny młodych użytkowników.

Pedagodzy zwracają uwagę, że proces kształtowania tożsamości w epoce cyfrowej nabiera nowych wymiarów. Media społecznościowe stały się przestrzenią autoprezentacji i poszukiwania akceptacji, więc młodzież często konstruuje w sieci alternatywne obrazy własnego ja, które nie zawsze są zgodne z rzeczywistością offline, ale pozytywny odbiór i wirtualna aprobata dają rzeczywiste emocjonalne zaspokojenie potrzeb (Solecki, 2017). „Ten „realny świat cyfrowy" jest praktycznie zsynchronizowany z ich dobrostanem społecznym, psychicznym, somatycznym i nie jest to oddziaływanie marginalne, niszowe, ale nabrało cech zjawiska pokoleniowego" (NASK, 2023). Z perspektywy wychowawczej oznacza to konieczność wspierania dzieci w rozwijaniu kompetencji cyfrowych, medialnych i emocjonalnych.

Współczesne zagrożenia w cyberprzestrzeni

Rozwój Internetu i technologii mobilnych wprowadził dzieci i młodzież w przestrzeń, w której tradycyjne formy relacji społecznych, nauki i rozrywki uległy znaczącym przemianom. Dla najmłodszych użytkowników, charakteryzujących się ograniczoną dojrzałością emocjonalną i poznawczą, zagrożenia te mogą przybrać szczególnie dotkliwe formy. W literaturze naukowej oraz w raportach instytucji publicznych wskazuje się na kilka najczęściej występujących zjawisk: cyberprzemoc, grooming, sexting, uzależnienie od Internetu, dezinformację oraz nadużycia danych osobowych.

Cyberbullying, czyli tzw. cyberprzemoc, to forma agresji realizowanej przy użyciu technologii informacyjno-komunikacyjnych. Cyberbullying definiowany jest najczęściej jako ciąg aktów agresji. Są one w sposób celowy i powtarzalny kierowane przeciwko innej osobie, która nie może się obronić, doświadcza bowiem bezradności w tym zakresie, co wynika z charakteru tych aktów agresji, które są: anonimowe, niewidoczne, asynchroniczne i tekstualne. Otóż brak bezpośredniego kontaktu sprawcy z jego ofiarą uniemożliwia wystąpienie mechanizmów hamujących agresję i poczucie empatii wobec osoby krzywdzonej (Fundacja Orange, 2019). Pojęcie cyberbullyingu powstało na podstawie terminu „*bullying"*, który w literaturze był wykorzystywany przez badaczy najczęściej do wyjaśniania zjawiska agresji rówieśniczej w szkole i poza nią. Bullying charakteryzuje się triadą cech: intencjonalnością, powtarzalnością i nierównością sił. Wykorzystanie do agresji rówieśniczej technologii komunikacyjnych przyniosło nowy typ bullyingu – cyberbullying, który obejmuje działania takie jak: wyzywanie, ośmieszanie, upokarzanie, rozpowszechnianie kompromitujących zdjęć lub filmów, podszywanie się pod kogoś, a także wykluczanie z grup internetowych (Pyżalski, 2012)

Według raportu *Nastolatki 3.0* przygotowanego przez NASK, aż 29,7% polskich uczniów doświadczyło wyzywania w sieci, 22,8% było obiektem ośmieszania, a 10,5% – szantażu lub gróźb w środowisku internetowym. Zjawisko to wywołuje poważne skutki psychologiczne: obniżenie samooceny, poczucie wstydu, izolację, a w skrajnych przypadkach – zaburzenia depresyjne i próby samobójcze (NASK, 2023).

Cyberprzemoc jest szczególnie niebezpieczna, gdyż jej oddziaływanie jest potencjalnie nieograniczone – materiał opublikowany w Internecie może być wielokrotnie udostępniany i niełatwo go usunąć. Jak zauważa prof. Jacek Pyżalski: Internet sprzyja wzmacnianiu agresji poprzez anonimowość i brak bezpośredniego kontaktu z ofiarą, co obniża empatię sprawcy (Pyżalski, 2012).

Innym zagrożeniem dla młodych użytkowników Internetu jest g*rooming*, czyli proces nawiązywania relacji przez osobę dorosłą z dzieckiem w celu jego wykorzystania seksualnego lub emocjonalnego. Sprawca stosuje manipulację, wzbudza zaufanie, wykorzystuje potrzebę akceptacji, a następnie doprowadza do uzyskania intymnych treści lub spotkania w świecie rzeczywistym. Zjawisko to stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa dzieci w sieci. W raporcie EUROPOL zwrócono uwagę,

że pandemia COVID-19 doprowadziła do nasilenia aktywności sprawców przestępstw na tle seksualnym w Internecie. Grooming często odbywa się poprzez komunikatory, gry online lub media społecznościowe, a dzieci – ze względu na brak świadomości zagrożeń – rzadko informują o takich kontaktach dorosłych (Europol, 2022).

W Polsce art. 200a § 2 Kodeksu karnego penalizuje nawiązywanie kontaktu z małoletnim w celu jego wykorzystania seksualnego (Kodeks karny, 1997; Fundacja Instytut Cyberbezpieczeństwa, 2023). Jednak praktyka pokazuje, że wykrywalność takich czynów jest niska, co wynika z trudności w identyfikacji sprawców działających anonimowo.

Sexting, definiowany jako przesyłanie lub publikowanie własnych treści erotycznych – zdjęć, filmów lub wiadomości – jest coraz częściej obserwowanym zjawiskiem wśród młodzieży. Dla wielu nastolatków stanowi on formę flirtu lub wyraz zaufania, jednak konsekwencje mogą być dramatyczne, bowiem udostępnione materiały mogą zostać upublicznione bez zgody ich autora, co prowadzi do upokorzenia, szantażu, a w konsekwencji nawet prób samobójczych. Według raportu *EU Kids Online Polska 2018*, ok. 11% młodych użytkowników Internetu przyznało, że wysyłało lub otrzymywało zdjęcia o charakterze intymnym (Fundacja Orange, 2019). Natomiast niespełna tylko 2% rodziców zadeklarowało, iż wie o tego typu aktywności swojego dziecka w sieci (NASK, 2023). Sexting wśród nieletnich bywa też traktowany jako przestępstwo – zgodnie z art. 202 § 3 Kodeksu karnego zakazane jest posiadanie lub rozpowszechnianie treści pornograficznych z udziałem małoletnich (Kodeks karny, 1997). Tym samym, działania podejmowane przez młodzież w sposób nieświadomy mogą skutkować odpowiedzialnością karną. Jak podkreśla prof. Jadwiga Izdebska: „wczesna edukacja seksualna i cyfrowa powinna kształtować świadomość granic prywatności, odpowiedzialności i wzajemnego szacunku w relacjach online" (Izdebska, 2020).

Nadmierne korzystanie z Internetu i gier sieciowych prowadzi do tzw. uzależnienia behawioralnego. Światowa Organizacja Zdrowia (WHO) w 2019 r. uznała *gaming disorder* za jednostkę chorobową, charakteryzującą się utratą kontroli nad czasem spędzanym w grze, zaniedbywaniem obowiązków i pogorszeniem relacji społecznych (WHO, 2019).

Badania polskich uczniów wskazują, że ponad 10% młodych osób przejawia symptomy uzależnienia od Internetu. Skutkami są problemy

z koncentracją, zaburzenia snu, izolacja społeczna, a także obniżenie wyników w nauce. W opinii Anny Andrzejewskiej uzależnienie od mediów cyfrowych jest współczesną formą ucieczki od rzeczywistości, w której młody człowiek poszukuje kompensacji emocjonalnej i poczucia kompetencji (Andrzejewska, 2014). Profilaktyka wymaga zatem nie tylko ograniczania czasu przed ekranem, lecz także rozwijania umiejętności społecznych i wsparcia psychologicznego dzieci i młodzieży. Wraz z rozwojem mediów społecznościowych pojawiło się zjawisko tzw. *infodemii* – nadmiaru niezweryfikowanych informacji. Dzieci i młodzież, pozbawione umiejętności krytycznego myślenia medialnego, stają się łatwym celem manipulacji i dezinformacji.

Według badań EU Kids Online, aż 46% polskich nastolatków miało kontakt z treściami zawierającymi przemoc, a 29% – z mową nienawiści (Fundacja Orange, 2019). Wzmacnia to postawy agresywne, prowadzi do desensytyzacji, czyli znieczulenia emocjonalnego i sprzyja polaryzacji społecznej. Ponadto młodzież narażona jest na kontakt z treściami promującymi autodestrukcję, zaburzenia odżywiania, samookaleczanie czy ekstremizm. Jak zauważa prof. Maciej Tanaś: media elektroniczne kreują świat bez wartości granicznych, w którym młody człowiek bez właściwego przygotowania nie jest w stanie odróżnić dobro od zła (Tanaś, 2024).

Dzieci i młodzież są szczególnie narażone na manipulacje socjotechniczne – podszywanie się pod znajomych, wyłudzanie danych, haseł, a nawet pieniędzy. Brak doświadczenia i ufność wobec innych użytkowników sprawiają, że młodzi internauci stają się łatwym celem cyberprzestępców.

Z raportu CERT Polska wynika, że liczba prób phishingu i kradzieży danych osobowych rośnie z roku na rok, a część ataków kierowana jest bezpośrednio do młodzieży w grach online i mediach społecznościowych (CERT Polska, 2024). Zagrożenia te mają nie tylko wymiar finansowy, lecz także psychologiczny – utrata kontroli nad danymi prowadzi do lęku, poczucia wstydu i utraty zaufania do otoczenia. Dlatego edukacja w zakresie bezpiecznego korzystania z sieci, ochrony haseł i danych osobowych powinna stanowić kluczowy element programów profilaktycznych.

Aspekty prawne i instytucjonalne ochrony dzieci w sieci

Rozwój usług cyfrowych oraz rosnąca aktywność dzieci i młodzieży w Internecie powodują, że tradycyjne instrumenty ochrony prawnej wymagają

adaptacji. Pojawiają się szczególne zagrożenia: kontakty z predatoryjnymi sprawcami, rozpowszechnianie materiałów seksualnych z udziałem nieletnich, cyberbullying, manipulowanie, targetowanie reklamowe oraz naruszenia prywatności. Prawo musi równocześnie chronić dzieci i respektować ich prawa, np. prawo do wyrażania poglądów, co stawia wyzwania wykładni i stosowania norm. Konwencja o prawach dziecka ustanawia ramę wartościową, natomiast państwa mają obowiązek zapewnić ochronę i środki zapobiegawcze wobec zagrożeń dla dzieci (Konwencja o prawach dziecka, 1989).

Polski Kodeks karny przewiduje szereg przestępstw, które w praktyce obejmują także zachowania w cyberprzestrzeni związane z krzywdzeniem małoletnich. Wśród kluczowych typów znajdują się: seksualne wykorzystanie małoletniego (art. 200), elektroniczna korupcja seksualna małoletniego (art. 200a), propagowanie pedofilii (art. 200b), jak również ogólne typy przestępstw, takie jak groźby, znieważenie czy stalking, gdy są popełniane wobec nieletnich za pomocą środków komunikacji elektronicznej. W praktyce ściganie tych czynów wymaga współpracy służb ścigania z operatorami platform oraz specjalistycznych procedur dowodowych.

W Polsce obowiązują też akty regulujące działalność usług internetowych i ochronę danych osobowych: ustawa o świadczeniu usług drogą elektroniczną reguluje obowiązki usługodawców, w tym zasady obsługi zgłoszeń dotyczących nielegalnych treści oraz kwestie odpowiedzialności usługodawców (Ustawa o świadczeniu usług drogą elektroniczną, 2002).

Ponadto istnieje ustawa o ochronie danych osobowych (UODO) (wdrożenie RODO/GDPR do porządku krajowego) oraz akty wykonawcze i wytyczne Prezesa UODO, które dotyczą przetwarzania danych dzieci (np. publikowanie zdjęć dzieci, profilowanie reklamowe skierowane do małoletnich) (Ustawa o ochronie danych osobowych, 2018).

Rozporządzenie Unii Europejskiej 2016/679 (RODO/GDPR) zawiera szczególne uregulowania dotyczące dzieci, przede wszystkim art. 8 – warunki zgody w odniesieniu do usług społeczeństwa informacyjnego: przetwarzanie danych osobowych dziecka jest zgodne z prawem, gdy dziecko ma co najmniej 16 lat; państwa członkowskie mogą obniżyć ten próg do nie mniej niż 13 lat (Unia Europejska, 2016). W praktyce Polska zachowała próg 16 lat, to znaczy, że osoba poniżej 16 lat wymaga zgody przedstawiciela ustawowego przy korzystaniu z usług on-line wymagających zgody. Przepisy

RODO wprowadzają też zasady szczególnej ochrony dzieci. Problematyczne jednak w praktyce są mechanizmy weryfikacji wieku i potwierdzania zgody rodzica.

Unia Europejska regulowała też obszar przeciwdziałania seksualnemu wykorzystywaniu dzieci – np. dyrektywa 2011/93/UE w sprawie zwalczania nadużyć seksualnych i pornografii dziecięcej, instrumenty te wymagają od państw członkowskich penalizacji określonych zachowań oraz współpracy transgranicznej (w tym z Europolem) (Dyrektywa 2011/93/UE, 2011). W praktyce dyrektywa kształtuje krajowe kody karne i współpracę międzynarodową w ściganiu przestępstw seksualnych wobec dzieci.

Konwencja z 1989 r. (UNCRC) ustanawia ramę praw dziecka, z obowiązkiem państw stron do zapewnienia odpowiedniej ochrony, edukacji i środków zapobiegawczych. W kontekście cyfrowym Komitet Praw Dziecka oraz wytyczne ONZ podkreślają obowiązek państw do aktualizacji prawa w celu ochrony dzieci przed zagrożeniami w sieci, przy jednoczesnym poszanowaniu ich praw do informacji i wyrażania poglądów (Komitet Praw Dziecka ONZ, 2021).

W polskim porządku prawnym przestępstwa przeciwko wolności seksualnej i obyczajności oraz przestępstwa związane z rozpowszechnianiem treści pornograficznych z udziałem nieletnich stanowią szczególnie surowo penalizowane kategorie (art. 197-201 k.k., w tym art. 200, 200a, 200b). Przestępstwa te obejmują czyny dokonywane online, takie jak: grooming, elektroniczne nakłanianie do czynności seksualnych, produkcja i udostępnianie materiałów. Ponadto przestępstwa powszechne (np. stalking, groźby, zniesławienie) mogą przybrać formę cyberprzestępstw, gdy są popełniane w sieci wobec małoletnich (Kodeks karny, 1997).

Skuteczne ściganie wymaga umiejętnego gromadzenia dowodów elektronicznych, międzynarodowej współpracy oraz współdziałania z platformami cyfrowymi w zakresie dostępu do danych i treści. DSA oraz instrumenty UE mają ułatwić współpracę i wymianę informacji, ale w praktyce bariery proceduralne utrudniają działania (Unia Europejska, 2022). Polskie przepisy przewidują sankcje karne, takie jak: kara pozbawienia wolności, grzywna, zakazy działalności za czyny przeciwko małoletnim. W orzecznictwie i praktyce karnej coraz częściej pojawiają się środki prewencyjne i zabezpieczające, czyli nadzór, zakazy kontaktu z dziećmi, ale istnieje potrzeba

lepszej specjalizacji organów ścigania i sądownictwa w sprawach cyberprzestępczości wobec dzieci.

Ochrona dzieci w cyberprzestrzeni wymaga kompleksowego podejścia łączącego normy karne, ochronę danych, regulacje sektorowe oraz instrumenty międzynarodowe. RODO i DSA stworzyły istotne narzędzia prawne, lecz istnieją realne luki – techniczne, proceduralne i międzynarodowe – które utrudniają pełne zabezpieczenie małoletnich. Konieczne są zarówno techniczne innowacje zgodne z prawami człowieka, jak i polityczne decyzje wzmacniające współpracę międzynarodową i egzekucję odpowiedzialności platform.

Podsumowanie

Cyberbezpieczeństwo dzieci i młodzieży stanowi jedno z najważniejszych wyzwań współczesnego społeczeństwa informacyjnego. Rozdział ukazuje, że rozwój technologii cyfrowych, choć niesie ogromne możliwości edukacyjne i komunikacyjne, jednocześnie stwarza liczne zagrożenia dla najmłodszych użytkowników Internetu. Zjawiska takie jak cyberprzemoc, sexting, grooming, uzależnienie od mediów cyfrowych, dezinformacja czy manipulacje danymi osobowymi stają się coraz bardziej powszechne, wpływając negatywnie na rozwój emocjonalny, społeczny i moralny młodego pokolenia.

Autorzy podkreślają, że skuteczna ochrona dzieci i młodzieży w przestrzeni cyfrowej wymaga zintegrowanego i wielowymiarowego podejścia, łączącego aspekty edukacyjne, prawne, psychologiczne i technologiczne. Niezbędne jest systemowe włączenie edukacji cyfrowej do programów nauczania oraz rozwijanie kompetencji medialnych, krytycznego myślenia i świadomości zagrożeń zarówno wśród uczniów, jak i dorosłych rodziców oraz nauczycieli. Współpraca pomiędzy szkołą, rodziną, instytucjami publicznymi i organizacjami społecznymi stanowi warunek skutecznego przeciwdziałania cyberzagrożeniom.

Z perspektywy prawnej konieczne jest dalsze doskonalenie przepisów krajowych i unijnych oraz usprawnienie mechanizmów egzekwowania prawa w zakresie ochrony małoletnich użytkowników sieci. Jednocześnie podkreśla się znaczenie działań profilaktycznych, kampanii informacyjnych i wsparcia psychologicznego dla dzieci dotkniętych cyberprzemocą lub innymi formami nadużycia.

Podsumowując, bezpieczeństwo cyfrowe dzieci i młodzieży nie może opierać się wyłącznie na technicznych narzędziach ochronnych, lecz wymaga kształtowania dojrzałych postaw, empatii i odpowiedzialności w korzystaniu z technologii. Tylko poprzez kompleksowe i długofalowe działania możliwe jest stworzenie środowiska cyfrowego, które sprzyja rozwojowi młodego człowieka, a jednocześnie skutecznie chroni go przed zagrożeniami współczesnego świata.

Literatura

1. Andrzejewska, A. (2014). *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych: aspekty teoretyczne i empiryczne*. Difin.
2. CERT Polska. (2024*). Raport roczny z działalności CERT Polska w 2023 roku.* CERT Polska.
3. *Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej oraz zastępująca decyzję ramową Rady 2004/68/WSiSW*. (2011). Dz.Urz. UE L 335 z 17.12.2011.
4. Europol. (2022). *Internet Organised Crime Threat Assessment 2022* (IOCTA). Europol.
5. Fundacja Instytut Cyberbezpieczeństwa. (2023). *Problematyka tzw. „child grooming" – okiem prawnika*. Fundacja Instytut Cyberbezpieczeństwa.
6. Fundacja Orange. (2019). *Polskie badanie EU Kids Online 2018*. Fundacja Orange.
7. Izdebska, J. (2020). *Dziecko w świecie mediów elektronicznych: Teoria, badania, edukacja medialna*. Wydawnictwo Trans Humana.
8. Jabłońska, M. R. (2018). *Człowiek w cyberprzestrzeni: Wprowadzenie do psychologii Internetu.* Wydawnictwo Uniwersytetu Łódzkiego.
9. Komitet Praw Dziecka ONZ. (2021*). Komentarz ogólny nr 25 (2021) w sprawie praw dziecka w środowisku cyfrowym.*
10. Konieczniak, M. (2011). Poszukiwanie tożsamości w cyberprzestrzeni: Implikacje pedagogiczne. *Edukacja i Dialog, 5/6*, 8-19.
11. Konwencja o prawach dziecka. (1989). *Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne ONZ dnia 20 listopada 1989 r.* (Dz. U. z 1991 r. Nr 120, poz. 526).

12. Lévy, P. (2002). Drugi potop. W: M. Hopfinger (red.), *Nowe media w komunikacji społecznej w XX wieku*: *Antologia* (s. 373-390). Oficyna Naukowa.
13. NASK. (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów i rodzic*ów. NASK – Państwowy Instytut Badawczy.
14. Pyżalski, J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży.* Oficyna Wydawnicza „Impuls".
15. Unia Europejska. (2016). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w sprawie swobodnego przepływu takich danych* (Dz. Urz. UE L 119 z 4.05.2016).
16. Unia Europejska. (2022). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).* Dz.Urz. UE L 277 z 27.10.2022, s. 1-102.
17. Solecki, R. (2017). *Aktywność młodzieży w cyberprzestrzeni: Profilaktyka patologicznego używania Internetu*. Oficyna Wydawnicza Von Velke.
18. Tanaś, M. (red.). (2024). *Pedagogika, środki informatyczne i media*. Oficyna Wydawnicza Impuls.
19. Ustawa o ochronie danych osobowych. (2018). *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. z 2018 r. poz. 1000).
20. Ustawa o świadczeniu usług drogą elektroniczną. (2002). *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.).
21. *Ustawa z dnia 6 czerwca 1997 r.* – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).
22. WHO. (2019). *International Classification of Diseases, 11th Revision (ICD-11).* World Health Organization.
23. Wochnowicz, A. (2023). Cyberprzestrzeń w systemie militarnym bezpieczeństwa państwa. *Cybersecurity and Law, 2*(10), 51-69.

Dorota Charkiewicz[1]
Warszawski Uniwersytet Medyczny
Marcin Czosnek[2]
Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu

https://doi.org/10.29316/9788368103373_20

PRAWO PACJENTA DO OCHRONY TAJEMNICY MEDYCZNEJ W ŚWIETLE USTAWY O PRAWACH PACJENTA I RZECZNIKU PRAW PACJENTA

THE PATIENT'S RIGHT TO MEDICAL CONFIDENTIALITY UNDER THE ACT ON PATIENTS' RIGHTS AND THE COMMISSIONER FOR PATIENTS' RIGHTS

Streszczenie

Rozdział poświęcony jest analizie instytucji tajemnicy medycznej w świetle ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Tajemnica medyczna została przedstawiona jako jeden z kluczowych elementów systemu ochrony praw pacjenta oraz fundamentalna zasada wykonywania zawodów medycznych. W opracowaniu przedstawiono jej znaczenie prawne, etyczne i praktyczne,

[1] https://orcid.org/0000-0002-1068-7569, e-mail: dorotacharkiewicz5@gmail.com
[2] https://orcid.org/0000-0002-1623-4720, e-mail: czosnek.marcin@gmail.com

a także wskazano relacje między obowiązkiem zachowania poufności a prawem pacjenta do prywatności i autonomii informacyjnej. Analiza obejmuje zarówno zakres podmiotowy, jak i przedmiotowy obowiązku zachowania tajemnicy, a także katalog ustawowych wyjątków dopuszczających jej uchylenie, w tym sytuacje wynikające z zagrożenia życia lub zdrowia, zgody pacjenta czy potrzeby wymiany informacji między osobami wykonującymi zawody medyczne. W rozdziale omówiono również podstawy odpowiedzialności karnej za naruszenie tajemnicy medycznej w świetle art. 266 § 1 Kodeksu karnego. Wyniki przeprowadzonych rozważań prowadzą do wniosku, że obowiązujący system prawny zapewnia spójną i wystarczającą ochronę tajemnicy medycznej, jednak jej efektywność w praktyce uzależniona jest od świadomości prawnej i etycznej personelu medycznego oraz skuteczności instytucjonalnego nadzoru. Zachowanie poufności informacji o pacjencie stanowi nie tylko obowiązek prawny, lecz także wyraz poszanowania jego godności, prywatności i praw człowieka w demokratycznym państwie prawnym.

Słowa kluczowe: tajemnica medyczna, prawa pacjenta, poufność, ustawa o prawach pacjenta, Rzecznik Praw Pacjenta, dane medyczne, ochrona prywatności, prawo medyczne

Abstract

The article focuses on the analysis of medical confidentiality under the Act of 6 November 2008 on Patients' Rights and the Commissioner for Patients' Rights. Medical confidentiality is presented as a key element in protecting patients' rights and as a fundamental principle governing the medical profession. The paper examines its legal, ethical, and practical dimensions, emphasising the relationship between the duty of confidentiality and the patient's right to privacy and informational autonomy. The analysis covers both the subjective and objective scope of the duty to maintain medical secrecy, as well as the statutory exceptions that allow for its disclosure, including situations involving a threat to life or health, the patient's explicit consent, or the need to exchange information among healthcare professionals involved in the provision of medical services. The article also addresses criminal liability for breaches of medical confidentiality under Article 266 § 1 of the Polish Penal Code. The findings indicate that the current legal framework provides a coherent and adequate foundation for protecting medical confidentiality. Nevertheless, its effectiveness in practice depends largely on healthcare professionals' legal and ethical awareness and on the efficiency of institutional oversight mechanisms. The maintenance of medical secrecy should therefore be regarded not only as a legal duty but also as an expression of respect for human dignity, privacy, and fundamental rights in a democratic state governed by the rule of law.

Keywords: medical confidentiality, patients' rights, privacy, Patients' Rights Act, Commissioner for Patients' Rights, medical data, legal protection, medical law

Wstęp

Prawo pacjenta do zachowania w tajemnicy informacji dotyczących jego stanu zdrowia, rozpoznania, leczenia oraz wszelkich innych danych ujawnionych w związku z udzielaniem świadczeń zdrowotnych stanowi jeden z fundamentów współczesnego prawa medycznego oraz zasad etyki zawodowej personelu medycznego. Tajemnica medyczna pełni funkcję gwarancyjną wobec pacjenta, chroniąc jego godność, prywatność i autonomię, a jednocześnie buduje niezbędne zaufanie w relacji pacjent-personel medyczny. W polskim porządku prawnym jej podstawową regulację stanowi ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581), w szczególności przepisy art. 13 i 14, które określają zarówno zakres prawa pacjenta do zachowania w tajemnicy informacji o nim, jak i dopuszczalne wyjątki od tej zasady.

Celem niniejszego opracowania jest szczegółowa analiza prawna instytucji tajemnicy medycznej w świetle przepisów wskazanej ustawy, ze szczególnym uwzględnieniem relacji pomiędzy ochroną poufności a realizacją obowiązków informacyjnych i administracyjnych podmiotów leczniczych. Autor stawia tezę, iż regulacja zawarta w art. 13-14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta stanowią wystarczającą i spójną podstawę prawną ochrony tajemnicy medycznej, jednak jej praktyczna skuteczność jest uzależniona od właściwej interpretacji przepisów, świadomości personelu medycznego oraz skutecznego nadzoru instytucjonalnego.

W opracowaniu zastosowano przede wszystkim metodę dogmatyczno-prawną, polegającą na analizie przepisów prawa krajowego w ich brzmieniu obowiązującym oraz w kontekście zasad konstytucyjnych i norm prawa europejskiego. Uzupełniająco wykorzystano metodę analizy orzecznictwa sądowego oraz analizy doktryny prawa medycznego, co pozwoliło na pogłębioną interpretację znaczenia tajemnicy medycznej w praktyce stosowania prawa. Praca ma charakter teoretyczno-praktyczny, łącząc refleksję prawniczą z odniesieniami do aktualnych problemów funkcjonowania systemu ochrony zdrowia w Polsce.

Pojęcie i znaczenie tajemnicy medycznej w prawie pacjenta

Tajemnica medyczna stanowi od wieków jeden z fundamentalnych obowiązków osób udzielających pomocy medycznej. W ujęciu historycznym postrzegano ją przede wszystkim jako powinność lekarzy (Bosek, 2025). Już w Przysiędze Hipokratesa pojawia się bowiem wyraźny nakaz zachowania dyskrecji: „*Cokolwiek bym podczas leczenia czy poza nim w życiu ludzkim ujrzał lub usłyszał, czego nie należy rozgłaszać, będę milczał, zachowując to w tajemnicy*". (Kapłan, 2002, s. 45).

Tajemnica medyczna odgrywa szczególną rolę, ponieważ stanowi fundament zaufania pacjentów do osób wykonujących zawody medyczne, co bezpośrednio przekłada się zarówno na jakość udzielanych świadczeń zdrowotnych, jak i na sprawne funkcjonowanie całego systemu opieki zdrowotnej (Denic, 2018). W samym systemie prawa brak jest legalnej definicji tajemnicy medycznej (Szymczak, 1989), ale przyjmuje się, że są to wszystkie informacje, które lekarz lub inna osoba wykonująca zawód medyczny pozyskała o pacjencie (Dubisz, 2003). W systemie ochrony zdrowia tajemnica medyczna odgrywa rolę nie tylko prawną, lecz także etyczną i kliniczną i stanowi podstawę relacji opartej na wzajemnym zaufaniu między pacjentem a personelem medycznym, które jest warunkiem skutecznego przebiegu procesu diagnostyczno-terapeutycznego (Sobczak, 2016).

Zgodnie z art. 24 Kodeksu etyki lekarskiej lekarz ma obowiązek zachowania tajemnicy lekarskiej (Kodeks Etyki Lekarskiej, 2024). Tajemnicą objęte są informacje związane z pacjentem, uzyskane przez lekarza w związku z wykonywanymi czynnościami zawodowymi. Śmierć chorego nie zwalnia od obowiązku dochowania tajemnicy lekarskiej. Kodeks uznaje tajemnicę lekarską za integralny element relacji opartej na zaufaniu, bez którego nie jest możliwe skuteczne leczenie ani budowanie właściwej więzi terapeutycznej. Obowiązek zachowania tajemnicy ma charakter nieograniczony w czasie i obejmuje nie tylko informacje o stanie zdrowia pacjenta, lecz także wszelkie dane dotyczące jego życia prywatnego, rodzinnego i społecznego, które lekarz pozyskał w związku z wykonywaniem czynności zawodowych.

Zagadnienia związane z ochroną tajemnicy medycznej zostały także ujęte w regulacjach o charakterze konstytucyjnym, co podkreśla ich fundamentalne znaczenie w systemie prawnym. Zgodnie z art. 47 Konstytucji

Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.) każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Przepis ten ustanawia dwa odrębne prawa podmiotowe: prawo jednostki do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz prawo do samodzielnego decydowania o swoim życiu osobistym (Tuleja, 2023). Pojęcie prywatności, chronione na gruncie tego przepisu, ma charakter szeroki i obejmuje kilka wzajemnie powiązanych sfer – życie prywatne, rodzinne, a także ochronę czci i dobrego imienia (Tuleja, 2023). Wskazane elementy nie stanowią zamkniętego ani rozłącznego katalogu, lecz wyznaczają jedynie podstawowy zakres konstytucyjnie gwarantowanej ochrony prywatności jednostki (Tuleja, 2023). Prawo do ochrony informacji (danych) osobistych stanowi jeden z elementów prawa do prywatności, jednak ustawodawca konstytucyjny zdecydował się ująć je w odrębnym przepisie art. 51 Konstytucji (Garlicki, Zubik, 2016). Taki zabieg należy interpretować jako wyraz dostrzeżenia szczególnych zagrożeń, jakie wiążą się z przetwarzaniem danych jednostki, oraz potrzeby zapewnienia jej w tym zakresie wzmocnionej ochrony prawnej (Garlicki, Zubik, 2016).

Przepis art. 51 Konstytucji Rzeczypospolitej Polskiej ustanawia prawo jednostki do ochrony danych osobowych, formułując jednocześnie podstawowe zasady dotyczące gromadzenia i przetwarzania informacji o obywatelach (Konstytucja RP, 1997). Zgodnie z jego treścią, nikt nie może być zobowiązany do ujawniania informacji dotyczących swojej osoby inaczej niż na podstawie ustawy. Władze publiczne mają natomiast zakaz pozyskiwania, gromadzenia i udostępniania danych o obywatelach w szerszym zakresie niż jest to konieczne w demokratycznym państwie prawnym. Każdemu przysługuje prawo dostępu do urzędowych dokumentów i zbiorów danych, które go dotyczą, przy czym ewentualne ograniczenia tego prawa mogą być wprowadzone wyłącznie ustawą. Konstytucja przyznaje również jednostce uprawnienie do żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych bądź uzyskanych z naruszeniem prawa oraz wskazuje, że szczegółowe zasady i tryb gromadzenia oraz udostępniania danych osobowych powinny być określone w przepisach ustawowych.

Tajemnica lekarska jako element praw pacjenta

Zgodnie z art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta z dnia 6 listopada 2008 r. (t.j. Dz. U. z 2024 r. poz. 581 ze zm.) pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego.

Regulacja dotycząca obowiązku zachowania tajemnicy lekarskiej, zawarta w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, ujmuje tajemnicę medyczną z perspektywy uprawnienia pacjenta, stanowiąc jednocześnie odpowiednik obowiązku po stronie podmiotów udzielających świadczeń zdrowotnych (Bosek, 2025). Ze względu na jej uniwersalny charakter oraz zastosowanie wobec wszystkich osób wykonujących zawody medyczne, właściwe wydaje się posługiwanie się terminem „tajemnica medyczna" bez zawężania go do określonych grup zawodowych, jak w przypadku pojęcia „tajemnicy lekarskiej" (Bosek, 2025). Brzmienie omawianego przepisu jednoznacznie wskazuje, że ustawodawca, mając świadomość otwartego charakteru katalogu zawodów medycznych, nałożył obowiązek zachowania tajemnicy medycznej na wszystkie osoby uczestniczące w procesie diagnostyczno-terapeutycznym pacjenta (Klich, 2022).

Jak wskazuje orzecznictwo, w oparciu o kryterium podmiotowe zakres tajemnicy lekarskiej obejmuje zarówno informacje uzyskane przez lekarza samodzielnie lub przekazane mu przez innego lekarza jak i dane ujawnione przez pacjenta bądź inne osoby działające na jego prośbę (Klich, 2022). Ochroną tajemnicy objęte są w szczególności wyniki badań, postawiona na ich podstawie diagnoza, dokumentacja medyczna, przebieg i metody leczenia, a także informacje dotyczące wcześniejszych lub współistniejących chorób, hospitalizacji oraz stosowanych leków (Haberko, Kocyłowski, 2006). Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 15 grudnia 2017 r. II SA/Kr 1206/17 tajemnica medyczna *„rozciąga się to również na wszelkie materiały związane z postawieniem diagnozy lub leczeniem, a więc na zaświadczenia, notatki, kartoteki"* (Wojewódzki Sąd Administracyjny w Krakowie, 2017).

Tajemnica lekarska stanowi formę tajemnicy zawodowej i pełni rolę istotnej gwarancji ochrony praw pacjenta, będąc zarazem fundamentalnym

elementem wykonywania zawodu lekarza w wymiarze prawnym i etycznym (Sobczak, 2016). Obowiązek jej przestrzegania spoczywa nie tylko na lekarzach, lecz również na całym personelu medycznym oraz podmiotach realizujących działalność leczniczą i udzielających świadczeń zdrowotnych (Sobczak, 2016).

System ochrony tajemnicy medycznej opiera się na zasadzie wzajemnej korelacji praw i obowiązków. Z jednej strony pacjentowi przysługuje prawo do poufności informacji o jego stanie zdrowia, z drugiej – na osobach wykonujących zawody medyczne spoczywa obowiązek zachowania tej tajemnicy. W ten sposób ustawodawca tworzy spójny mechanizm gwarantujący poszanowanie prywatności pacjenta w procesie udzielania świadczeń zdrowotnych (Bosek, 2020). Zgodnie z art. 14 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta – osoby wykonujące zawód medyczny, realizując prawo pacjenta do tajemnicy informacji, są obowiązane zachować w tajemnicy informacje związane z pacjentem, w szczególności ze stanem zdrowia pacjenta. Zatem prawu pacjenta do zachowania w tajemnicy informacji dotyczących jego stanu zdrowia odpowiada obowiązek zachowania tej tajemnicy, nałożony na osoby wykonujące zawody medyczne i inne podmioty uczestniczące w udzielaniu świadczeń zdrowotnych.

Jednym z aspektów, na który należy zwrócić również uwagę, jest systematyczny wzrost liczby postępowań sądowych inicjowanych przez pacjentów przeciwko przedstawicielom zawodów medycznych, co stanowi konsekwencję rosnącej świadomości społecznej w zakresie praw pacjenta oraz nagłaśniania przypadków tzw. błędów medycznych (Klich, 2022). Zgodnie z art. 261 § 2 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2024 r. poz. 1568 ze zm.) świadek może odmówić odpowiedzi na zadane mu pytanie, jeżeli zeznanie mogłoby narazić jego lub jego bliskich, wymienionych w paragrafie poprzedzającym, na odpowiedzialność karną, hańbę lub dotkliwą i bezpośrednią szkodę majątkową albo jeżeli zeznanie miałoby być połączone z pogwałceniem istotnej tajemnicy zawodowej (Kodeks postępowania cywilnego, 1964).

Przepis ten upoważnia zatem przedstawiciela zawodu medycznego do odmowy odpowiedzi na zadawane pytania w postępowaniu cywilnym sądowym, jeśli jego wypowiedź mogłaby prowadzić do naruszenia tajemnicy medycznej (Marciniak, 2019), jednocześnie jednak obarcza np. lekarza

odpowiedzialnością za każdorazową ocenę, czy w konkretnej sytuacji może dojść do naruszenia tajemnicy medycznej. Inaczej sytuacja przedstawia się w postępowaniu karnym w którym zgodnie z art. 180 § 2 k.p.k. osoby obowiązane do zachowania m.in. tajemnicy lekarskiej mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu (Kodeks postępowania karnego, 1997). Jednocześnie nie można utożsamiać sytuacji, w której określona okoliczność mająca znaczenie dla rozstrzygnięcia sprawy ma zostać ustalona na podstawie dowodu wymagającego zwolnienia z tajemnicy zawodowej z automatycznym spełnieniem przesłanki niezbędności dla dobra wymiaru sprawiedliwości. Z tego względu należy przyjąć, że przesłanka niezbędności dla dobra wymiaru sprawiedliwości musi mieć charakter kwalifikowany i obejmować sytuacje wyjątkowe, w których ujawnienie informacji objętych tajemnicą stanowi jedyny sposób ustalenia istotnych dla sprawy okoliczności.

Jednakże jak wskazał Europejski Trybunał Praw Człowieka w wyroku z dnia 6 czerwca 2013 r. (1585/09 Avilkina i inni v. Rosja) nad interesami pacjenta i całego społeczeństwa związanymi z ochroną poufności danych medycznych przeważyć może jawność postępowania sądowego, jeżeli wykazane zostanie jej większe znaczenie (należy jednak wykazać taki prymat) (Cnota, Grabowski, Gura, Kurowska, 2016). Zaznaczył jednak, że zdrowie publiczne to ważny cel publiczny, lecz sam w sobie nie uzasadnia aż tak poważnego naruszenia prawa do poufności danych medycznych pacjentów. Informacje dotyczące stanu zdrowia pacjenta mają charakter poufny, a ich ujawnienie może nastąpić wyłącznie za świadomą i jednoznaczną zgodą osoby, której dotyczą. Naruszenie tej zasady stanowi ingerencję w prawo pacjenta do poszanowania życia prywatnego, chronione m.in. przez art. 8 Europejskiej Konwencji Praw Człowieka (Europejski Trybunał Praw Człowieka, 2013).

Okoliczności legalizujące ujawnienie informacji medycznych dotyczących pacjenta

Obowiązek dyskrecji medycznej, mimo swego doniosłego znaczenia i prawnych gwarancji, nie jest nieograniczony. Ujawnienie informacji może być dopuszczalne za zgodą pacjenta, w jego interesie lub dla ochrony

innych, ważniejszych dóbr (Bosek, 2020). Tego rodzaju sytuacje stanowią tzw. dyspensy od tajemnicy medycznej (Bosek, 2020).

Wprowadzając wyjątki umożliwiające ujawnianie danych medycznych pacjentów, należy pamiętać, że zgodnie z art. 31 ust. 1 Konstytucji ograniczenia praw i wolności mogą być ustanawiane wyłącznie w ustawie oraz tylko wtedy, gdy są niezbędne w demokratycznym państwie prawnym – w szczególności dla ochrony bezpieczeństwa, porządku publicznego, zdrowia, moralności lub praw i wolności innych osób. Nie mogą one jednak prowadzić do naruszenia istoty tych praw (Bosek, 2020).

Przepis art. 14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta dopuszcza możliwość wyjątków od obowiązku zachowania tajemnicy medycznej w sytuacji w której po pierwsze tak stanowią przepisy odrębnych ustaw, zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób, pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, bądź zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń.

Możliwość ujawnienia danych medycznych przewidziana w przepisach szczególnych innych ustaw sprawia, że wyjątki od obowiązku zachowania tajemnicy medycznej mają zróżnicowany charakter i podstawy prawne (Bosek, 2020). Najczęściej uzasadnione są one potrzebą ochrony interesu publicznego, który w określonych sytuacjach przeważa nad prawem pacjenta do poufności (Bosek, 2020). Jako przykład można wymienić przepis art. 27 ust. 1 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, zgodnie z którym lekarz lub felczer, który podejrzewa lub rozpoznaje zakażenie, chorobę zakaźną lub zgon z powodu zakażenia lub choroby zakaźnej, jest obowiązany do zgłoszenia tego faktu właściwemu państwowemu inspektorowi sanitarnemu (Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, 2008). Również przepis art. 11 ust. 8 ustawy z dnia 31 stycznia 1959 roku o cmentarzach i chowaniu zmarłych przewiduje wyjątek od obowiązku zachowania tajemnicy medycznej (Ustawa o cmentarzach i chowaniu zmarłych, 1959). Zarówno lekarz, jak i inne osoby powołane do dokonywania oględzin zwłok, jeżeli przy dokonaniu tej czynności powezmą pewność lub uzasadnione

podejrzenie, że przyczyną zgonu była choroba zakaźna, podlegająca obowiązkowemu zgłoszeniu, powinni zawiadomić o tym natychmiast właściwego inspektora sanitarnego. W przypadku uzasadnionego podejrzenia, że przyczyną zgonu było przestępstwo, lekarz, jak i inne osoby powołane do oględzin zwłok powinni zawiadomić o tym natychmiast właściwego prokuratora lub najbliższy posterunek policji.

Przepisy dopuszczają również ujawnienie informacji o stanie zdrowia pacjenta, gdy zachowanie tajemnicy mogłoby stanowić zagrożenie dla życia lub zdrowia jego samego bądź innych osób. W takich sytuacjach lekarz powinien ocenić, czy istnieje realne i bezpośrednie niebezpieczeństwo, którego nieusunięcie lub nieograniczenie mogłoby prowadzić do poważnych skutków dla zdrowia lub życia, co uzasadnia odstąpienie od tajemnicy medycznej (Cnota, Grabowski, Gura, Kurowska, 2016).

Ponieważ ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta, nie zawiera definicji pojęcia „zagrożenia dla życia lub zdrowia pacjenta bądź innych osób", przy jego interpretacji pomocne może być odwołanie się do art. 160 § 1 Kodeksu karnego (Kodeks karny, 1997). Przepis ten stanowi, że odpowiedzialność ponosi ten, kto naraża człowieka na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, co pozwala na zbliżone rozumienie pojęcia „zagrożenia" w kontekście tajemnicy medycznej. Przestępstwa określone w art. 160 § 1 Kodeksu karnego dotyczą ochrony życia i zdrowia człowieka. Ich znamiona zostają spełnione już przez samo stworzenie sytuacji, w której choćby jedna osoba zostaje narażona na bezpośrednie niebezpieczeństwo utraty życia lub doznania ciężkiego uszczerbku na zdrowiu (Stefański, 2025).

Zgodnie z art. 14 ust. 2 pkt 3 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta tajemnica medyczna przestaje obowiązywać, jeśli pacjent lub jego przedstawiciel ustawowy wyrazi zgodę na jej ujawnienie. Zgoda pacjenta na ujawnienie informacji objętych tajemnicą medyczną nie niweczy samego faktu naruszenia poufności, lecz wyłącza jego bezprawność. Stanowi ona świadomy i dobrowolny akt woli, wyrażający zgodę na ujawnienie określonych danych. Może być udzielona w sposób wyraźny lub dorozumiany, na przykład poprzez brak sprzeciwu, o ile pacjent miał realną możliwość swobodnego jego wyrażenia i mimo to pozostawił decyzję bez reakcji.

Wprawdzie przepisy ustawy, jak i inne akty wykonawcze nie precyzują formy zgody, pozostawiając jej wyrażenie w dowolnej formie, to jednak nieprecyzyjne określenie formy zgody nie uprawnia do jej domniemania i z całą pewnością musi zostać wyrażona w sposób niebudzący wątpliwości, co oznacza, że:

- udzielanie informacji osobom nieupoważnionym jest niedopuszczalne, a pracownik medyczny nie może zakładać, że osoby z najbliższego otoczenia pacjenta posiadają z góry prawo dostępu do danych dotyczących jego stanu zdrowia,
- nie należy przyjmować, że osoba towarzysząca pacjentowi ma z samego faktu obecności prawo dostępu do jego danych medycznych,
- nie można zakładać, że pacjent wyraża zgodę na ujawnianie informacji o charakterze poufnym podczas przeprowadzania wywiadu w salach, w których przebywają inne osoby (Bosek, 2025).

Przekazanie niezbędnych informacji o pacjencie innym osobom wykonującym zawód medyczny stanowi również wyjątek od obowiązku zachowania tajemnicy medycznej. Jest on jednak uzasadniony dobrem pacjenta, gdyż umożliwia szybsze i skuteczniejsze udzielanie świadczeń zdrowotnych, zwłaszcza w sytuacjach wymagających natychmiastowej interwencji lub konsultacji (Bosek, 2025). Takie rozwiązanie pozwala na naruszenie poufności w zakresie niezbędnym do ochrony życia i zdrowia pacjenta (Bosek, 2025).

Udostępnienie dokumentacji medycznej innemu lekarzowi – w szczególności w celach konsultacyjnych – mieści się w granicach dopuszczalnego przekazywania informacji o pacjencie osobom wykonującym zawód medyczny, uczestniczącym w procesie udzielania świadczeń zdrowotnych. Tego rodzaju działanie, nawet jeśli formalnie narusza przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, nie jest co do zasady postrzegane jako naruszenie tajemnicy lekarskiej w stopniu godzącym w dobra osobiste pacjenta.

Odpowiedzialność karna za naruszenie tajemnicy medycznej w systemie ochrony zdrowia

Prawo pacjenta do zachowania w tajemnicy informacji dotyczących jego osoby, stanu zdrowia oraz przebiegu leczenia stanowi jedno

z podstawowych praw określonych w art. 13 ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta, 2008). W szerszym kontekście uprawnienie to jest implikacją konstytucyjnego prawa do prywatności i ochrony danych osobowych. Podmiotowo, obowiązek przestrzegania tajemnicy obciąża wszystkie osoby wykonujące zawód medyczny, a zatem nie tylko lekarzy, lecz także pielęgniarki, położne, ratowników medycznych czy diagnostów laboratoryjnych. Przedmiotowo, tajemnica medyczna obejmuje szeroki zakres informacji i danych przekazywanych albo utrwalonych w dowolnej formie – zarówno ustnie, jak i w dokumentacji medycznej. Zawiera się w dokumentacji medycznej dotyczącej stawianej diagnozy lub leczenia, w tym w zaświadczeniach, zapiskach, kartotekach, ale też w wynikach badań, historii choroby, użytych w leczeniu metodach oraz osiąganych postępach, opisach schorzeń współistniejących, przebytych hospitalizacjach i zażywanych lekach. W związku z tym tajemnica medyczna obejmuje ogół informacji uzyskiwanych od pacjenta. Warto zauważyć, że mogą zakresem wykraczać poza sferę zdrowia i obejmować elementy działalności zawodowej, stanu majątkowego albo życia osobistego (Burdzik i in., 2019). Dysponentem tajemnicy jest pacjent, który może upoważnić inne osoby do uzyskania informacji o swoim stanie zdrowia i wglądu w dokumentację medyczną. Czasowo konieczność zachowania tajemnicy nie dezaktualizuje śmierć pacjenta, chyba że osoba najbliższa wyrazi zgodę na jej ujawnienie. Choć sama ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta nie przewiduje sankcji karnych za naruszenie tego obowiązku, jego złamanie może rodzić odpowiedzialność karną w oparciu o przepisy ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 ze zm.). W art. 266 § 1 Kodeksu karnego, kryminalizacją objęte jest zachowanie sprawcy polegające na wykorzystaniu lub ujawnieniu wbrew przepisom ustawy (Kodeks karny, 1997). Przestępstwo należy do kategorii indywidualnie właściwych, przez co może być popełnione tylko przez osobę mającą określone właściwości lub cechy. W poruszanym kontekście musi być zobowiązana na podstawie przywołanego już art. 13 o prawach pacjenta i Rzeczniku Praw Pacjenta – do zachowania w tajemnicy informacji związanych z wykonywaniem określonej pracy, pełnioną funkcją albo wykonywaną działalnością publiczną. Jest to przestępstwo o charakterze bezwzględnie wnioskowym. Oznacza to, że aby doszło do wszczęcia

lub kontynuowania postępowania, konieczne jest w myśl § 3 art. 266 k.k. złożenie przez pokrzywdzonego wniosku o ściganie karne. Brak wniosku uniemożliwia postępowanie (art. 17 § 1 pkt 10 k.p.k.), przez co prowadzi do uchybienia określonego w art. 439 § 1 pkt 9 k.p.k. W zakresie znamienia „ujawniać" należy wskazać, że oznacza ono przekazywanie informacji innej osobie nieuprawnionej, do której nie miała wcześniej dostępu. Wykorzystywać to używać takiej informacji w ten sposób, że wiedza o niej była asumptem do działania, a zostało to zrealizowane w jakimś celu. Czyn może być popełniony tylko umyślnie w zamiarze bezpośrednim lub wynikowym (Sobański, 2024). Odpowiedzialność sprawcy, nie zaistnieje w szczególności, gdy wynika to z przepisów odrębnych ustaw lub jeśli zachowanie tajemnicy mogłoby stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta albo innych osób, bądź też zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń. Szczególnym przejawem tajemnicy medycznej jest tajemnica lekarska, która dotyczy wyłącznie lekarzy. W procesie karnym, legalna możliwość pozyskania danych objętych tajemnicą lekarską – poza zgodą pacjenta – realizowana jest na podstawie art. 180 § 2 k.p.k., za zgodą sądu. Uzyskanie zezwolenia sądu jest możliwe, gdy wymaga tego dobro wymiaru sprawiedliwości i jednocześnie udowodnienie danej okoliczności nie jest możliwe przy wykorzystaniu innego dowodu. Z tego rodzaju zasadą subsydiarności zwolnienia z tajemnicy wiąże się także możliwość dowiedzenia danej okoliczności nie tylko za pomocą innego dowodu, ale także w inny sposób niż poprzez zwolnienie z tajemnicy przez Sąd.

Tajemnica medyczna stanowi jeden z podstawowych instrumentów ochrony prywatności pacjenta, a jej naruszenie może prowadzić do odpowiedzialności karnej na podstawie art. 266 § 1 k.k., przy czym ustawowe wyjątki od obowiązku jej zachowania mają charakter ściśle ograniczony.

Podsumowanie

Tajemnica medyczna stanowi jeden z fundamentalnych filarów systemu ochrony praw pacjenta oraz podstawową zasadę etyki zawodowej osób wykonujących zawody medyczne. Jej znaczenie wykracza poza wymiar prawny – pełni funkcję gwarancyjną wobec pacjenta, chroniąc jego

godność, prywatność oraz autonomię informacyjną, a zarazem tworzy niezbędny fundament zaufania w relacji terapeutycznej. Analiza regulacji zawartych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, prowadzi do wniosku, że ustawodawca w sposób systemowy i spójny ukształtował obowiązek zachowania tajemnicy medycznej, jednocześnie przewidując zamknięty katalog przesłanek uzasadniających jej uchylenie.

Odstępstwa od obowiązku zachowania tajemnicy mogą mieć miejsce wyłącznie w przypadkach ściśle określonych w przepisach prawa – w szczególności na podstawie zgody pacjenta, w jego interesie, dla ochrony życia lub zdrowia jego samego bądź innych osób, bądź w przypadkach wynikających z regulacji szczególnych. Każde ujawnienie informacji medycznych wymaga zachowania najwyższej staranności i proporcjonalności, albowiem nieuprawnione naruszenie poufności może rodzić wielopłaszczyznową odpowiedzialność – cywilną, zawodową oraz karną, w tym w oparciu o art. 266 § 1 Kodeksu karnego.

Wyniki przeprowadzonej analizy wskazują, iż skuteczność ochrony tajemnicy medycznej zależy nie tylko od precyzji obowiązujących norm prawnych, ale również od poziomu świadomości prawnej i etycznej przedstawicieli zawodów medycznych oraz od sprawności instytucjonalnych mechanizmów nadzoru. Zachowanie poufności informacji o pacjencie należy zatem postrzegać jako integralny element poszanowania jego praw podmiotowych, a zarazem jako istotny wyznacznik profesjonalizmu i odpowiedzialności w praktyce medycznej.

Literatura

1. Bosek, L. (red.). (2020). *Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta: Komentarz*. Wydawnictwo C.H. Beck.
2. Bosek, L. (red.). (2025). *Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta: Komentarz*. Wydawnictwo C.H. Beck.
3. Burdzik, M., Chowaniec, C., Nowak, A. (2019). Tajemnica lekarska w świetle nowelizacji Kodeksu postępowania karnego z 10.06.2016 r. *Państwo i Prawo, 9*, 128-145.
4. Cnota, Z., Grabowski, T., Gura, G., Kurowska, E. (2016). *Zasady i tryb ustalania świadczeń/roszczeń (odszkodowania i zadośćuczynienia)*

w przypadku zdarzeń medycznych: Komentarz. Wydawnictwo C.H. Beck.

5. Denic, D. (2018). Medical secret as a basis of medical confidence in relation doctor–patient – Healthcare system of the Republic of Serbia. *JAHR, 9*(2). 205-222. https://doi.org/10.21860/j.9.2.4
6. Dubisz, S. (red.). (2003). *Uniwersalny słownik języka polskiego. Tom 4.* Wydawnictwo Naukowe PWN.
7. Europejski Trybunał Praw Człowieka. (2013). *Wyrok z dnia 6 czerwca 2013 r. w sprawie Avilkina i inni przeciwko Rosji, skarga nr 1585/09*.
8. Garlicki, L., Zubik, M. (red.). (2016). *Konstytucja Rzeczypospolitej Polskiej: Komentarz. II.* Wydawnictwo Sejmowe.
9. Haberko, J., Kocyłowski, R. (2006). Szczególna postać tajemnicy lekarskiej w przypadku stosowania technik wspomaganego medycznie rozrodu. *Prawo i Medycyna, 23*(2). 18-32.
10. Kapłan, W. (tłum.). (2002). *Hipokrates. Wybór pism*. Wydawnictwo Naukowe PWN.
11. Klich, A. (2022). Ochrona tajemnicy zawodów medycznych w procesie sądowym. W: K. Flaga-Gieruszyńska, V. Nekrošius (red.), *Tajemnica prawnie chroniona w prawie materialnym i procesowym* (s. 21-44). Wydawnictwo C.H. Beck.
12. Kodeks Etyki Lekarskiej. (2024). *Załącznik do uchwały nr 5 Nadzwyczajnego XVI Krajowego Zjazdu Lekarzy z dnia 18 maja 2024 r.*
13. Kodeks karny. (1997). *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz. U. z 2025 r. poz. 383, tekst jednolity).
14. Kodeks postępowania cywilnego. (1964). *Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego* (Dz. U. z 2024 r. poz. 1568, tekst jednolity).
15. Kodeks postępowania karnego. (1997). *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (Dz. U. z 2025 r. poz. 46, tekst jednolity).
16. Konstytucja RP. (1997). *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.).
17. Marciniak, A. (red.) (2019). *Kodeks postępowania cywilnego*. *Tom II: Komentarz*. Wydawnictwo C.H. Beck.

18. Sobański, P. (2024). Odpowiedzialność karna za naruszenie tajemnicy dyplomatycznej – wybrane aspekty. *Europejski Przegląd Prawa i Stosunków Międzynarodowych, 1*(69), 109-119. https://doi.org/10.52097/eppism.8891
19. Sobczak, J. (2016). Tajemnica lekarska. *Medyczna Wokanda*, *8*, 57-72.
20. Stefański, R. A. (red.). (2025). *Kodeks karny: Komentarz*. Wydawnictwo C.H. Beck.
21. Szymczak, M. (red.). (1989). *Słownik języka polskiego. Tom 3*. Państwowe Wydawnictwo Naukowe.
22. Tuleja, P. (red.). (2023). *Konstytucja Rzeczypospolitej Polskiej: Komentarz*. Wolter Kluwer.
23. Ustawa o cmentarzach i chowaniu zmarłych. (1959). *Ustawa z dnia 31 stycznia 1959 r. o cmentarzach i chowaniu zmarłych* (Dz. U. z 2024 r. poz. 576).
24. Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta. (2008). *Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta* (Dz. U. z 2024 r. poz. 581).
25. Ustawa o zawodach lekarza i lekarza dentysty. (1996). *Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty* (Dz. U. z 2024 r. poz. 1287).
26. Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi. (2008). *Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi* (Dz. U. z 2024 r. poz. 924)
27. Wojewódzki Sąd Administracyjny w Krakowie. (2017). *Wyrok z dnia 15 grudnia 2017 r., II SA/Kr 1206/17, Legalis nr 1729645.*

Ireneusz Fura[1]
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie

https://doi.org/10.29316/9788368103373_21

WYBRANE ZAGROŻENIA BEZPIECZEŃSTWA GLOBALNEGO

SELECTED GLOBAL SECURITY THREATS

Streszczenie

Bezpieczeństwo globalne jest obecnie kształtowane pod wpływem szeregu wyzwań i zagrożeń w różnych aspektach. Problematykę zarządzania globalnym bezpieczeństwem można rozpatrywać w kilku aspektach/sferach. Mogą to być sfery: geostrategiczna, technologiczna, klimatyczna i demograficzna, które nazywane są również siłami konstrukcyjnymi. Aktualne wyniki badań wielu ośrodków eksperckich wykazują dwie kluczowe perspektywy globalne – krótkoterminową i długoterminową. Perspektywa krótkoterminowa obejmowała lata 2024-2025, natomiast perspektywa długoterminowa sięga do roku 2034. Szczególne znaczenie w aspekcie globalnego bezpieczeństwa zajmuje oddziaływanie sił strukturalnych na klimat i technologie sztucznej inteligencji. Zmiany klimatu są już faktem i, niezatrzymane, będą generować nieodwracalne skutki w środowisku naturalnym oraz zmiany demograficzne. Natomiast technologie sztucznej inteligencji, oprócz niewątpliwie ogromnego pozytywnego wpływu na rozwój cywilizacyjny, niosą ze sobą jeszcze niezbadane ryzyko. Nasilać się będą odrębne podejścia podmiotów rządowych i pozarządowych

[1] https://orcid.org/0000-0003-0649-2395, e-mail: irekfura@poczta.onet.pl

co do celów w zakresie polityki klimatycznej, wykorzystania nowoczesnych technologii i sposobów ich osiągnięcia. Stosując metody analizy i krytyki piśmiennictwa oraz metodę badań dokumentów, autor rozdziału wykazał, że oba te zagrożenia są dostrzegane przez respondentów, lecz ich negatywne skutki są inaczej postrzegane zarówno w bliższej, jak i dalszej perspektywie czasowej.

Słowa kluczowe: bezpieczeństwo globalne, zagrożenia, siły strukturalne, klimat, nowoczesne technologie, sztuczna inteligencja

Abstract

Global security faces a number of challenges and threats across its various aspects. The issue of global security management can be considered in several aspects/spheres. These may be the following spheres: geostrategic, technological, climate and demographic, which are also called structural forces. Current research results from many expert centres show, briefly, two key global perspectives in the long term. The short-term perspective covers the years 2024-2025, while the long-term perspective reaches until 2034. Of particular importance for global security are the impacts of structural forces on the climate and on artificial intelligence technologies. Climate threats and artificial intelligence technologies are of particular importance for global security. Climate change is already a fact, and if left unchecked, it will have irreversible effects on the natural environment and on demographics. However, artificial intelligence technologies, apart from undoubtedly having a huge positive impact on the development of civilisation, also carry unexplored risks. Separate approaches by government entities will intensify, and non-governmental organisations will focus on climate policy goals, the use of modern technologies, and ways to achieve them. Using the methods of literary analysis and criticism and document research, the author of the article showed that both threats are recognised by respondents, but their negative effects are perceived differently in the short and long term.

Keywords: global security, threats, structural forces, climate, modern technologies, artificial intelligence

Wstęp

Otaczająca nas rzeczywistość cechuje się gwałtownym przyspieszeniem zmian technologicznych i niepewności gospodarczej oraz niebezpiecznymi kryzysami o charakterze klimatycznym i konfliktowym, w tym zbrojnym.

Wiele regionów świata ogarniętych jest napięciami mającymi charakter geopolityczny, z wybuchem aktywnych działań wojennych włącznie.

Współczesność cechuje się niestabilnością porządku globalnego charakteryzującego się polaryzującymi narracjami, erozją zaufania i brakiem bezpieczeństwa. Wysiłki i zasoby w zakresie przystosowania się do zmiany klimatu są niewystarczające w stosunku do rodzaju, skali i intensywności zdarzeń związanych z klimatem, które już mają miejsce, co powoduje, że w tym samym czasie wiele regionów świata zmaga się ze skutkami ekstremalnych zjawisk pogodowych. Duża część świata poddana jest presji związanej z kosztami utrzymania w warunkach uporczywie podwyższonej inflacji i stóp procentowych oraz utrzymującej się niepewności gospodarczej. Globalne możliwości komunikacji pozwalają systematycznie przekazywać aktualne informacje o sytuacjach polityczno-gospodarczo-militarnych, które w wielu przypadkach są powodem frustracji społeczeństw. Sytuacja taka pozwala na skuteczne rozprzestrzenianie się dezinformacji – w społeczeństwach, które już w ostatnich latach zostały osłabione politycznie i gospodarczo.

Rozdział ten jest próbą analizy globalnego krajobrazu ryzyka w tej fazie transformacji oraz przeciążenia systemów zarządzania bezpieczeństwem. Analizie poddane zostały najpoważniejsze postrzegane zagrożenia dla gospodarek i społeczeństw do dziesięciu lat, tj. do ok. 2035 r. Rozdział jest oczywiście materiałem dyskusyjnym, w którym można domniemywać o czekającej nas rzeczywistości w świecie o temperaturze wyższej o 3°C. Możemy zadać sobie kilka pytań natury egzystencjalnej: czy właśnie osiągamy szczyt rozwoju społecznego dużej części światowej populacji, biorąc pod uwagę pogarszające się zadłużenie i warunki geoekonomiczne? Czy będziemy świadkami bezpardonowej walki państw o pozycję w świecie, rozwoju przestępczości i korupcji, które żywią się bardziej wrażliwymi państwami i bardziej bezbronnymi populacjami? Czy wykorzystanie w wyścigu zbrojeń nowych technologii będzie stanowiło egzystencjalne zagrożenie dla ludzkości?

Należy się liczyć z tym, że z tymi ponadnarodowymi zagrożeniami coraz trudniej będzie sobie poradzić w miarę pogłębiającej się erozji globalnej współpracy. Wiele ośrodków badawczych przewiduje, że w ciągu najbliższych 10 lat dominować będzie wielobiegunowy porządek, ponieważ średnie i wielkie mocarstwa będą ustalać i egzekwować – ale także kwestionować – obecne zasady i normy egzystencji. W rozdziale poddane zostały analizie konsekwencje tego rozdrobnionego świata, w którym gotowość na

globalne zagrożenia jest coraz bardziej wątpliwa i utrudniona przez brak konsensusu i współpracy między podmiotami międzynarodowymi. Przedstawiono w nim również ogólne ramy koncepcyjne dotyczące przeciwdziałania globalnym zagrożeniom, określając zakres „minimalnego realnego wysiłku" w zakresie działania, w zależności od charakteru ryzyka.

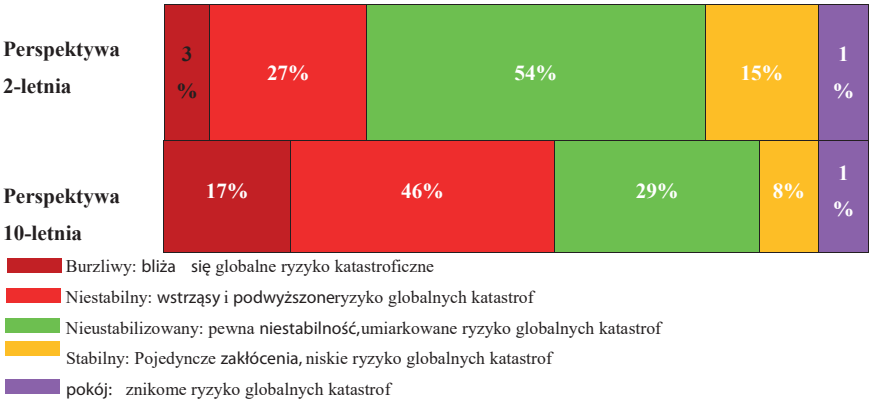
W rozdziale autor koncentrował się przede wszystkim na analizie najważniejszych zagrożeń, które mogą pojawić się w ciągu następnej dekady w kontekście zmian geostrategicznych, klimatycznych, technologicznych i demograficznych. Część pierwsza rozdziału skupia się na analizie wyników badań w zakresie wpływu tzw. sił konstrukcyjnych na systemy Ziemi i na rozwój nowych technologii. Spostrzeżenia zawarte w tym rozdziale opierają się na badaniach ośrodków analitycznych, między innymi Global Risks Perception Survey (GRPS), a także środowisk akademickich, biznesu, rządu, społeczności międzynarodowej i społeczeństwa obywatelskiego. Wykorzystane zostały również prognozy ekspertów tematycznych, w tym specjalistów ds. ryzyka, którzy tworzą Radę Doradczą ds. Globalnych Raportów o Ryzykach, Global Future Council on Complex Risks oraz Społeczność Dyrektorów ds. Ryzyka a także Marsh McLennan i Zurich Insurance Group.

Kluczowe zagadnienia bezpieczeństwa środowiska globalnego

Analizując aktualny stan bezpieczeństwa środowiska globalnego, należy uwzględnić wydarzenia z ostatnich lat, a przede wszystkim z 2023 roku. Należy zdawać sobie sprawę, że wiele wydarzeń przyciągnęło uwagę ludzi na całym świecie – podczas gdy inne zostały poddane minimalnej analizie. Zagrożone populacje zmagały się ze śmiertelnymi konfliktami, od Ukrainy po Gazę i Izrael, a także z rekordowymi upałami, suszami, pożarami i powodziami. Niezadowolenie społeczne było wyczuwalne w wielu krajach, a cykle informacyjne były zdominowane przez polaryzację, gwałtowne protesty, zamieszki i strajki. Należy stwierdzić, że w znacznej mierze uniknięto destabilizujących skutków na całym świecie – takich jak te, które pojawiły się przy pandemii COVID-19 czy w początkowym okresie wybuchu wojny rosyjsko-ukraińskiej – w długoterminowych perspektywach tych wydarzeń należy się liczyć z dalszymi globalnymi wstrząsami.

Analizując rok 2024, wyniki GRPS podkreślały głównie negatywne perspektywy dla świata w latach 2024-2025 w zakresie globalnych katastrof,

które mają się pogorszyć w ciągu następnej dekady (Rysunek 1). W badaniu przeprowadzonym we wrześniu 2023 r. większość respondentów (54 proc.) przewidywała pewną niestabilność i umiarkowane ryzyko globalnych katastrof, a kolejne 30 proc. spodziewała się jeszcze bardziej burzliwych warunków. Perspektywy w kolejnych latach są znacznie bardziej negatywne w horyzoncie 10 lat, a prawie dwie trzecie respondentów spodziewa się burzliwych perspektyw (World Economic Forum, 2024).



Rysunek 1. Krótko i długoterminowe perspektywy globalne

Źródło: World Economic Forum, 2024.

Analiza perspektyw obejmuje cztery siły konstrukcyjne, które będą kształtować zarządzanie globalnym ryzykiem w ciągu następnej dekady. Są to długoterminowe zmiany w układzie i relacjach między czterema systemowymi elementami globalnego krajobrazu:

1. Globalne ocieplenie i związane z nim konsekwencje dla systemów Ziemi (zmiana klimatu).
2. Demografia i związane z nią zmiany w wielkości, wzroście i strukturze populacji na całym świecie.
3. Nowe technologie i perspektywy ich rozwoju.
4. Dominacja geopolityczna, ewolucja koncentracji i źródeł władzy geopolitycznej (przesunięcia geostrategiczne).

Należy spodziewać się, że dziedziny te w najbliższej dekadzie kształtować będą nowe warunki globalne, a ich przemiany będą charakteryzować się niepewnością i zmiennością. W miarę jak społeczeństwa będą się starały

dostosować do tych zmieniających się sił, wpłynie to na ich zdolność do przygotowania się na globalne zagrożenia i reagowania na nie.

Krytyczne punkty zagrożenia dla środowiska

Z przeprowadzonych badań wynika, że w perspektywie najbliższych 10 lat nadal dominować będą zagrożenia środowiskowe (Rysunek 2).

Badania wykonane przez Global Risks Perception Survey wykazały, że respondenci nie zgadzają się jednak co do pilności zagrożeń środowiskowych, w szczególności utraty różnorodności biologicznej i załamania się ekosystemów oraz krytycznych zmian w systemach Ziemi. Okazuje się, że młodsi respondenci w porównaniu ze starszymi grupami wiekowymi, postrzegają te zagrożenia za znacznie bardziej niebezpieczne w perspektywie krótkoterminowej (dwóch lat). Natomiast starsi respondenci, choć nie kwestionują problemów środowiskowych, dostrzegają je dopiero w perspektywie kolejnych 10 lat. Podobne postrzeganie zagrożeń środowiskowych prezentują podmioty prywatne w odróżnieniu od respondentów reprezentujących społeczeństwa obywatelskie lub rządy. Sytuacja taka nie jest pożądana, gdyż może powodować brak optymalizacji wysiłków zmierzających do przeciwdziałania tym zagrożeniom, co do czasu, miejsca i zakresu działań.



Rysunek 2. Globalne ryzyko uszeregowane według dotkliwości w perspektywie krótko i długoterminowej

Źródło: World Economic Forum, 2024.

Badania GRPS wykazały, że nie wykluczone jest przekroczenie co najmniej jednego „klimatycznego punktu krytycznego" w ciągu następnej dekady. Ostatnie badania GRPS sugerują, że próg wywołania długoterminowych, potencjalnie nieodwracalnych i samonapędzających się zmian w wybranych układach planetarnych prawdopodobnie zostanie przekroczony w momencie globalnego ocieplenia o 1,5°C lub wcześniej, co obecnie przewiduje się już na początek lat 2030. W takiej sytuacji należy spodziewać się, że wiele państw będzie nieprzygotowanych na skutki potencjalnie wywołanych kilku powiązanych ze sobą zagrożeń społeczno-środowiskowych, które mogą przyspieszyć zmianę klimatu poprzez uwolnienie dwutlenku węgla i wzmocnić powiązane skutki, zagrażając grupom społecznym wrażliwym na zmianę klimatu. Poziom rozwoju państw jest tak zróżnicowany, że trzeba liczyć się z tym, że skala potencjalnych skutków i wymagań w zakresie inwestycji w infrastrukturę ograniczającą degradację środowiska naturalnego może być nie do udźwignięcia przez wiele społeczeństw. Skutkiem tego mogą być problemy gospodarczo-ekonomiczne wielu państw,

niepokoje społeczne i wzrost znaczenia sił populistycznych. Finalnym efektem tego zjawiska może się stać zachwianie systemu bezpieczeństwa międzynarodowego.

Świat w 2034 roku

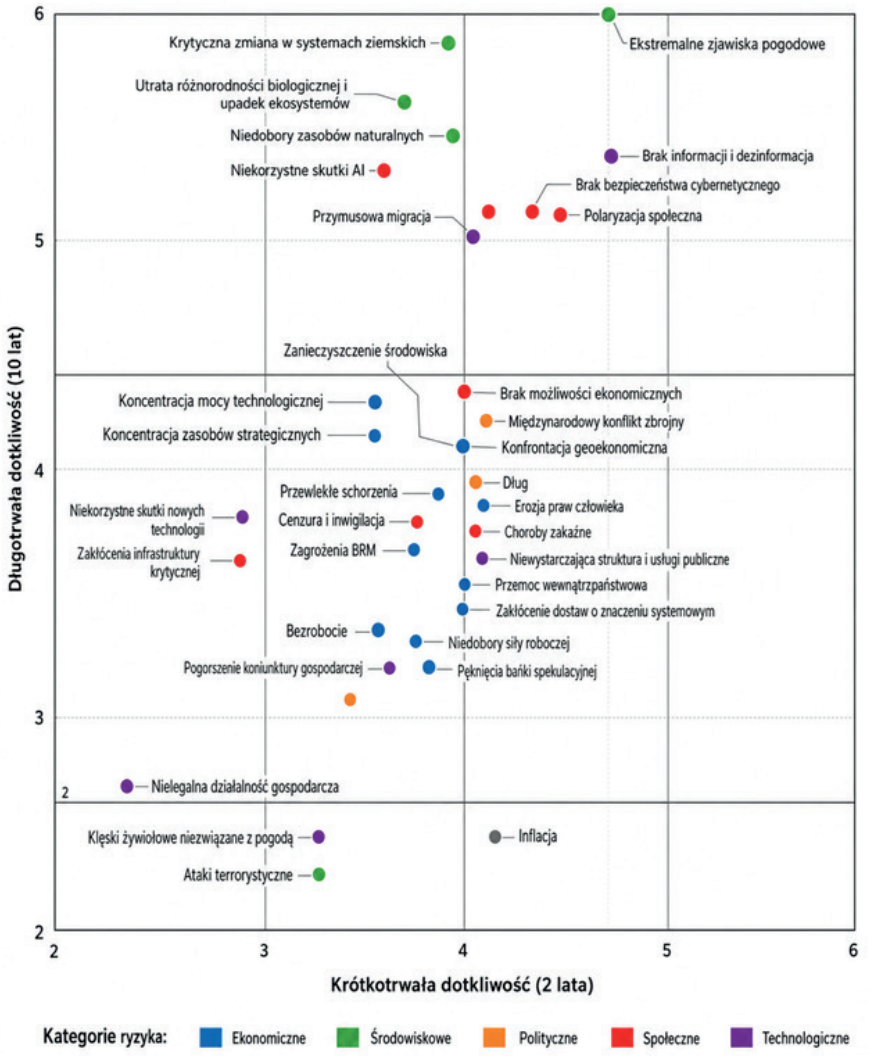
Należy oczekiwać, że do 2034 r. ryzyko środowiskowe i technologiczne ulegnie radykalnemu pogorszeniu i zdominuje długoterminowy krajobraz zagrożeń globalnych (Rysunek 2). Prawdopodobnie nasilą się ekstremalne zjawiska pogodowe, które staną się jeszcze bardziej dotkliwe, jako najwyżej oceniane ryzyko w ciągu następnej dekady. Badania wykazały, że w najbliższych 10 latach krytyczne zmiany w systemach Ziemi (poz. 2) i niedobory zasobów naturalnych (poz. 4) są postrzegane jako istotnie pogarszające się, przyczyniając się do ich wejścia do rankingu 10 największych zagrożeń w ciągu najbliższej dekady, podczas gdy związane z tym ryzyko mimowolnej migracji wzrośnie o jedno miejsce na poz. 7, a na przykład zanieczyszczenie środowiska pozostaje na 10 miejscu.

Przedstawione wyniki badań świadczą o dostrzeganiu przez respondentów zagrożeń dla środowiska. Utrata różnorodności biologicznej i załamanie się ekosystemów oraz krytyczne zmiany w systemach Ziemi pojawiają się na wysokich pozycjach w długoterminowych rankingach zagrożeń.

Wyraźnie widoczne są również obawy dotyczące możliwych skutków najnowszych osiągnięć technologicznych. Przewiduje się, że negatywne skutki technologii sztucznej inteligencji doświadczą jednego z największych pogorszeń dotkliwości (poz. 6). Pojawia się możliwy systemowy lub nawet egzystencjalny charakter powiązanych zagrożeń, gdy sztuczna inteligencja przenika do systemów gospodarczych, społecznych i politycznych. Pomimo pogarszających się wyników dotkliwości w tym okresie, najbardziej widoczne zagrożenia technologiczne w perspektywie krótkoterminowej, czyli brak informacji i dezinformacja oraz brak bezpieczeństwa cybernetycznego, spadły w rankingu, ale w dłuższej perspektywie pozostają w pierwszej dziesiątce, odpowiednio na 5. i 8. miejscu. Związane z tym ryzyko polaryzacji społecznej również spada z 3. miejsca w perspektywie krótkoterminowej na 9. w horyzoncie długoterminowym.

Następna dekada zapoczątkuje okres znaczących zmian, które rozciągną zdolności adaptacyjne ludzkości do granic możliwości. Wyniki badań

GRPS są znacznie mniej optymistyczne co do perspektyw dla świata w dłuższej perspektywie niż w perspektywie krótkoterminowej. Dwie trzecie (63%) respondentów GRPS przewiduje burzliwe perspektywy, z wstrząsami i w najlepszym razie podwyższonym ryzykiem globalnych katastrof.



Rysunek 3. Względna dotkliwość ryzyka w okresie 2 i 10 lat

Źródło: World Economic Forum, 2024.

Porównanie dwu- i dziesięcioletnich okresów czasowych wskazuje na tendencję do zwiększających się ryzyk w wielu badanych obszarach.

Trzydzieści trzy z 34 globalnych zagrożeń zwiększa swoją dotkliwość w dłuższej perspektywie, co odzwierciedla obawy respondentów dotyczące zwiększonej częstotliwości lub intensywności tych zagrożeń w ciągu 10 lat (Rysunek 3). Należy się liczyć z tym, że największemu pogorszeniu w okresie najbliższych dziesięciu lat ulegnie środowisko naturalne (np. ekstremalne zjawiska pogodowe staną się jeszcze bardziej dotkliwe) oraz znacznie wzrośnie ryzyko związane z nowymi technologiami. Prawie wszystkie zagrożenia środowiskowe znalazły się w rankingu 10 najważniejszych zagrożeń na nadchodzącą dekadę (Rysunek 2).

Należy stwierdzić, że zdecydowanie dostrzegana jest możliwość utraty różnorodności biologicznej i załamania ekosystemu, w tym krytyczne zmiany w systemach Ziemi czy niedobory zasobów naturalnych. Natomiast ryzyko mimowolnej migracji postrzegane jest podobnie jak w perspektywie krótkoterminowej jako zjawisko zanieczyszczenia środowiska. Z kolei klęski żywiołowe niezwiązane z pogodą nie są postrzegane jako kluczowe zagrożenia zarówno w dwuletnim okresie czasu, jak i w najbliższej dekadzie. Prawdopodobną przyczyną takiego punktu widzenia jest charakter takiego ryzyka i często geograficznie odizolowany charakter tych zdarzeń.

Zagrożenia środowiska, utraty różnorodności biologicznej i załamania ekosystemów uznawane są jako priorytetowe przez ludzi młodszych, natomiast reprezentanci sektora prywatnego, w przeciwieństwie do respondentów reprezentujących społeczeństwo obywatelskie lub rząd, uważają, że większość zagrożeń środowiskowych zmaterializuje się w dłuższym okresie czasu. Taka sytuacja jest bardzo niebezpieczna, gdyż oznaczać może, że to biznes będzie odgrywał kluczowe znaczenie w aspekcie ochrony szeroko rozumianego środowiska naturalnego i tym samym komplikuje się wskazanie ośrodka decyzyjnego oraz czas decyzji i działania w tym zakresie. Należy zwrócić uwagę, że znacznie wzrosły obawy społeczeństwa przed skutkami najnowszych osiągnięć technologicznych. Przewiduje się, że technologie korzystające ze sztucznej inteligencji staną się szczególnie dotkliwe dla ludzkości. W perspektywie najbliższych 10 lat możliwe jest wystąpienie zagrożeń związanych z tymi technologiami, które stanowić będą wręcz egzystencjalny problem ludzkości. Brak informacji czy dezinformacja w perspektywie 10-letniej, zdaniem badanych, będzie mieć mniejsze znaczenie niż obecnie; dotyczy to również braku bezpieczeństwa cybernetycznego

i ryzyka polaryzacji społecznej (Rysunek 2). Należy zauważyć, że społeczne ryzyka związane z ekonomią, gospodarką czy inflacją w perspektywie 10 lat, zdaniem badanych, tracą na znaczeniu. Pogląd ten dotyczy zarówno respondentów ze środowisk społeczeństwa obywatelskiego, jak i ze środowisk akademickich. Rozbieżność w stosunku do postrzegania sektora publicznego – który nie klasyfikuje tego ryzyka w pierwszej dziesiątce – w połączeniu z długoterminowymi, skumulowanymi skutkami świata o niskich szansach dla następnego pokolenia sprawia, że stanowi to ryzyko dla sektora prywatnego.

Z badań GRPS wynika, że inflacja jest prawdopodobnie jedynym ryzykiem, którego dotkliwość może ulec poprawie w ciągu następnej dekady. W rzeczywistości większość ryzyk ekonomicznych gwałtownie spada w rankingach porównawczych percepcji ryzyka w ciągu następnej dekady. Może to odzwierciedlać fakt, że konfrontacja geoekonomiczna, kluczowy czynnik wielu ryzyk gospodarczych, znacznie zmniejszyła postrzeganą dotkliwość w obu horyzontach czasowych w porównaniu z wynikami z lat 2022-2023. Faktem jest, że ryzyko geopolityczne jest nieobecne w rankingu dziesięciu kluczowych ryzyk w ciągu następnej dekady.

Warto jednak zauważyć, że ataki terrorystyczne są znacznie słabiej postrzegane pod względem dotkliwości zarówno w perspektywie krótkoterminowej, jak i długoterminowej (Rysunek 3). Chociaż najnowsze dostępne dane wskazują, że ogólna śmiertelność pozostaje ograniczona w porównaniu z innymi zagrożeniami, przy 6 701 ofiarach śmiertelnych na całym świecie w 2022 r., terroryzm może wywołać szersze konflikty i niepokoje, takie jak obecny konflikt na Bliskim Wschodzie (Institute for Economics, Peace, 2023).

Siły konstrukcyjne kształtujące zarządzanie globalnym ryzykiem

Problematykę zarządzania globalnym bezpieczeństwem można rozpatrywać w kilku aspektach/sferach. Mogą to być sfery: geostrategiczna, technologiczna, klimatyczna i demograficzna, które nazywane są również siłami konstrukcyjnymi (World Economic Forum, 2024).

Zmiany warunków i parametrów tych sfer warunkować będą zagrożenia, których należy spodziewać się w ciągu następnej dekady. Siły te mogą mieć istotny wpływ na szybkość, rozprzestrzenianie się lub zakres globalnych

ryzyk i będą na siebie nawzajem wpływać. Siły konstrukcyjne będą mieć także największy wpływ na globalny krajobraz ryzyka i obejmować będą: przyspieszenie technologiczne; zmiany geostrategiczne; zmiany klimatu; rozwidlenie demograficzne. Trzeba mieć świadomość, że gdy wszystkie cztery siły mają globalne konsekwencje, jedna z nich, jaką jest zmieniający się klimat, jest bardziej wielokierunkowa w swoim rozwoju, co może mieć wpływ na rozwój kilku potencjalnych kierunków rozwoju ludzkości. Inna siła – zmiany geostrategiczne mogą prowadzić do braku zgodności między mocarstwami, co w konsekwencji może prowadzić do konfliktów, nie wykluczając wojen. Natomiast skutki przyspieszenia technologicznego nie są łatwe do zdefiniowania w perspektywie długoterminowej. Można założyć, że będzie ono sprzyjać nowym odkryciom, które będą szybko przekształcać wiele systemów, ale zarówno pozytywnie, jak i negatywnie.

Tabela 1. Siły konstrukcyjne

Przyspieszenie technologiczne odnosi się do ścieżek rozwoju technologii. Przewiduje się, że w ciągu najbliższych 10 lat podzbiór kluczowych technologii, w tym sztuczna inteligencja ogólnego przeznaczenia, doświadczy znacznego, przyspieszonego rozwoju. Biorąc pod uwagę sam zakres rozwoju pionierskiego i zastosowań ogólnych, może pojawić się wiele trajektorii. Na przykład obliczenia kwantowe mogą pozwolić na gwałtowny wzrost mocy obliczeniowej i, oprócz oczekiwanych korzyści, szybko spowodować nowe globalne zagrożenia. Eksperymenty technologiczne, takie jak interfejsy mózg-komputer, mogą zatrzeć granice między technologią a ludzkością, z niespotykanymi skutkami.	**Zmiana klimatu** obejmuje szereg możliwych trajektorii globalnego ocieplenia i konsekwencji dla systemów Ziemi. W tegorocznej analizie zmiana klimatu została scharakteryzowana jako zmiana systemowa, ponieważ przewiduje się, że próg 1,5°C powyżej temperatury sprzed epoki przemysłowej, określony w porozumieniu paryskim z 2015 r., zostanie przekroczony na początku lub w połowie lat 30. Jednak na ścieżki globalnego ocieplenia nadal będzie miało wpływ tempo, w jakim odbywają się dekarbonizacja i wdrażanie rozwiązań klimatycznych. Degradacja systemów środowiskowych może również przyspieszyć szacowane trajektorie, do tego stopnia, że „w sposób naturalny" przyczyniają się one do globalnego ocieplenia i związanych z nim skutków (takich jak odwrócenie pochłaniaczy dwutlenku węgla).

Zmiany geostrategiczne odnoszą się do ewoluujących źródeł i koncentracji władzy geopolitycznej. To z kolei wpływa na ułożenie porządku geopolitycznego, wpływając na powiązane sojusze i dynamikę, a także na ofensywną i defensywną projekcję miękkiej i twardej siły w ciągu następnej dekady. Władza gospodarcza staje się coraz bardziej rozproszona, na przykład odzwierciedlając zmiany w zależności walutowej, źródłach energii, dostępnym kapitale i wielkości rynków konsumenckich. Koncentracja siły gospodarczej i militarnej jest również silnie związana z zasobami technologicznymi i surowcowymi. Podczas gdy alternatywna przyszłość jest możliwa, szereg mocarstw prawdopodobnie potwierdzi swoją dominację na arenie globalnej w wielobiegunowym świecie.	**Bifurkacja demograficzna** odnosi się do zmian w wielkości, wzroście i strukturze populacji na całym świecie. Przepaść demograficzna pogłębia się. Polaryzacja wzrostu na górnym i dolnym końcu piramidy populacji oraz między krajami i regionami będzie miała materialne implikacje dla powiązanych systemów społeczno-gospodarczych i politycznych. Azja nadal dominuje pod względem bezwzględnego wzrostu liczby ludności. Większość krajów będzie nadal borykać się ze starzeniem się społeczeństwa, łącząc długoterminowy wzrost średniej długości życia ze spadkiem współczynnika dzietności. Z kolei Afryka stoi przed radykalnie innym wyzwaniem politycznym: oczekuje się, że do 2030 r. młodzi Afrykanie będą stanowić 42% światowej młodzieży.

Źródło: World Economic Forum, 2024.

Siły konstrukcyjne stale oddziałują na siebie i tym samym stają się źródłem globalnych zagrożeń, które stale ewaluują – Tabela 1). W ciągu następnych 10 lat należy liczyć się że zagrożenia te będą mogły oddziaływać między innymi na:

1. Systemy Ziemi: badania wykazały, że stanowi jedno z najpoważniejszych zagrożeń, z jakimi będziemy musieli się zmierzyć w ciągu następnej dekady (Rysunek 2, poz. 2). Działania ludzkości mogą doprowadzić do zmian klimatycznych poza punkt krytyczny, do którego ludzie nie będą się w stanie przystosować.
2. Technologie sztucznej inteligencji: prawdopodobnie do 2034 roku gwałtownie wzrośnie liczba niekorzystnych skutków wykorzystania technologii sztucznej inteligencji (Rysunek 2, poz. 7). Należy liczyć się z tym, że nowoczesne technologie będą mogły służyć do destabilizacji globalnej gospodarki i bezpieczeństwa.
3. Rozwój społeczny: w latach 2024-2025 występujący jako główne ryzyko w perspektywie kolejnej dekady tuż poza pierwszą dziesiątką zagrożeń. Prawdopodobny brak możliwości gospodarczych może być

stałym, ale mniej priorytetowym ryzykiem dla globalnych decydentów w dłuższym horyzoncie czasowym.

4. Rozwój przestępczości zorganizowanej: jednym z najniżej ocenianych zagrożeń w globalnej sieci zagrożeń jest nielegalna działalność gospodarcza. Istnieje jednak ryzyko, że ponadnarodowe sieci przestępcze podporządkują sobie niestabilne państwa i wrażliwe populacje, wykorzystując wysoce destrukcyjne działania.

Spodziewana przyszłość przedstawiona w każdym z poniższych punktów to tylko jeden z wielu możliwych scenariuszy i jego prawdopodobne skutki. Zadaniem właściwych decydentów należy umieć we właściwym czasie zidentyfikować te, które będą stanowić realne zagrożenie dla ludzkości i odpowiednio przeciwstawić się im – a jeżeli już nastąpią, to właściwie i skutecznie reagować.

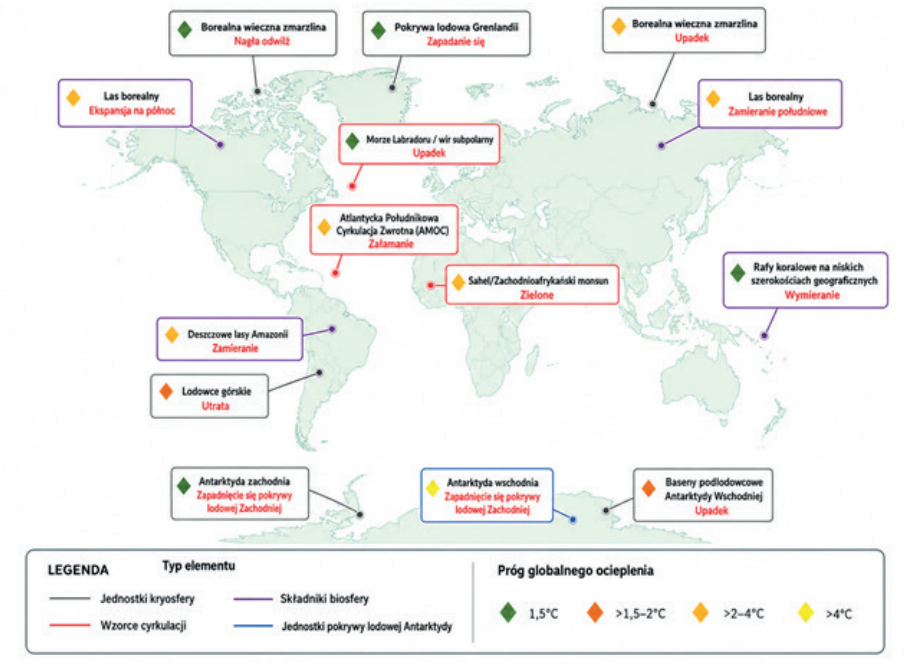
Zmiany klimatyczne

Długoterminowe, potencjalnie nieodwracalne i samonapędzające się zmiany w krytycznych systemach Ziemi, w wyniku przekroczenia krytycznego progu lub „punktu krytycznego" na poziomie regionalnym lub globalnym, mają nagły i poważny wpływ na środowisko naturalne i na stan zdrowia oraz dobrobyt ludzi. Obejmują między innymi topnienie i zapadanie się lodowców, podnoszenie się poziomu mórz, zmiany prądów oceanicznych lub atmosferycznych czy uwalnianie węgla z topniejącej wiecznej zmarzliny.

Aktualne prognozy globalnego ocieplenia wskazują, że w ciągu najbliższej dekady może zostać przekroczony co najmniej jeden „klimatyczny punkt krytyczny" (lub próg, przy którym następuje długoterminowa, potencjalnie nieodwracalna i samonapędzająca się zmiana w systemie planetarnym). Przy obecnym poziomie globalnego ocieplenia (~1,1°C) pięć systemów klimatycznych mogłoby teoretycznie przekroczyć punkty krytyczne, w tym: rafy koralowe na niskich szerokościach geograficznych; wieczna zmarzlina; pokrywy lodowe Grenlandii i Antarktydy Zachodniej; oraz konwekcja morska Labrador-Irminger. Przy ociepleniu o 1,5°C zagrożonych może być kolejnych pięć: lasy borealne (północ i południe); Atlantycki Obieg M.O. (AMOC); lód morski Barentsa; i lodowce górskie (McKay, 2022). W prawie wszystkich scenariuszach Międzyrządowego Zespołu ds.

Próg zmian klimatu (IPCC) 1,5°C zostanie przekroczony na początku lat 2030 (Intergovernmental Panel on Climate Change [IPCC], 2022).

Najnowsze badania wskazują, że prawdopodobnie co najmniej cztery systemy Ziemi przekroczą krytyczny próg przy podwyższeniu średniej temperatury o 1,5°C (Rysunek 4): wymieranie raf koralowych na niskich szerokościach geograficznych (wysoki poziom ufności), zapadanie się pokrywy lodowej Grenlandii i Antarktydy Zachodniej (wysoki poziom ufności) oraz nagłe topnienie wiecznej zmarzliny (średni poziom ufności). Istnieją również nowe dowody sugerujące, że cyrkulacja wiru subpolarnego na Północnym Atlantyku może być dodatkowo zagrożona przy temperaturze 1,5°C, podczas gdy lasy borealne, namorzyny i łąki trawy morskiej również zaczną stawać się wrażliwe (Lenton i in., 2023).



Rysunek 4. Przykłady globalnych i regionalnych punktów krytycznych
Źródło: World Economic Forum, 2024.

Należy przyjąć, że krytyczne zmiany w systemach ziemskich stają się jednym z głównych elementów globalnych zagrożeń, z jakimi będziemy

musieli się zmierzyć w ciągu najbliższych 10 lat. Skutki tych zmian są już odczuwalne na poziomie systemowym, wywierając wpływ na światowe bezpieczeństwo żywnościowe i zdrowotne. Wszystko na to wskazuje, że zmiany klimatyczne będą wymuszać dalsze prace i stosowanie geoinżynierii czy produkcji żywności genetycznie zmodyfikowanej.

Badania wykazują, że klimatyczne punkty krytyczne są dobrze znane zarówno decydentom, jak i społeczeństwom obywatelskim, ale nie do końca są przez nich postrzegane jako realne zagrożenie, szczególnie jeżeli mowa o nich w dłuższej perspektywie. Sytuacja taka jest bardzo niebezpieczna, gdyż przekroczenie punktów krytycznych może nastąpić w sposób i w czasie nieoczekiwanym oraz nie w pełni dostrzegalny. Zbyt późne, konkretne i systemowe przeciwdziałanie skutkować będzie brakiem możliwości przystosowania się ludzkości do nowych warunków egzystencji. Należy liczyć się z tym, że do 2034 r. wiele gospodarek będzie słabo przygotowanych do nieliniowych skutków zmian klimatycznych, a taka sytuacja będzie grozić koniecznością powstania i zaakceptowania nowych struktur społeczno-ekonomicznych. Przekroczenie klimatycznych punktów krytycznych będzie pogłębiało i tak silne aktualne zagrożenia, znacznie przybliżając do sytuacji kryzysowych w zakresie społecznym i środowiskowym. Efektami tych zmian będą prawdopodobnie: załamanie się ekosystemów, zachwianie różnorodności biologicznej, zanieczyszczenie środowiska i nasilenie się ekstremalnych zjawisk pogodowych, które będą mogły powodować deficyt i utrudniony oraz ograniczony dostęp do zasobów naturalnych. Kolejnymi skutkami tych zjawisk będą pogorszenie sytuacji gospodarczej i zdrowotnej wielu państw, co będzie powodować zintensyfikowanie wymuszonej migracji oraz pandemie.

Możliwość przeciwstawienia się tym skutkom będzie prawdopodobnie utrudniona przez kilka czynników:

- Należy liczyć się z tym, że do 2034 r. Działania mające na celu przygotowanie się do nowej rzeczywistości będą nieskuteczne, szczególnie w krajach, które są najbardziej narażone na skutki zmian klimatycznych. Będą to państwa ubogie, niestabilne gospodarczo, z nierozwiązanymi konfliktami wewnętrznymi. Działania zmierzające do adaptacji krajów rozwijających będą uzależnione między innymi od finansów czy potrzeb infrastrukturalnych. Konflikty wewnętrzne i spory graniczne

o zasoby, np. wody pitnej czy złóż naturalnych, będą prawdopodobnie się nasilać, odstraszając tym samym potencjalnych inwestorów. Skutki problemów społeczno-ekonomicznych państw szczególnie nieodpornych na zmiany klimatyczne pośrednio odczuwane będą także w państwach znacznie lepiej przystosowanych, np. poprzez zaniechanie inwestycji czy porzucenie już funkcjonujących.

- Zmniejszenie wydajności rolnictwa i prawdopodobne znaczne zmniejszenie jego wydajności w niektórych ważnych regionach Ziemi. Na przykład niektóre badania sugerują, że utrata znacznej masy lodu z pokrywy lodowej Grenlandii może prowadzić do susz i strat w rolnictwie w regionie Sahelu, w północnej Afryce, jednocześnie zmniejszając pierwotną produktywność mórz na północnym Atlantyku (Kwiatkowski, 2019). Problem braku bezpieczeństwa żywnościowego, w tym wody pitnej, jest kluczowym źródłem narażenia – lub dźwigni – dla kilku światowych i regionalnych potęg: Chin, Korei Południowej, Japonii, Rosji i Arabii Saudyjskiej, które należą do największych importerów netto żywności i produktów rolnych, podczas gdy Argentyna, Australia, Brazylia, Kanada, Nowa Zelandia, Tajlandia i Stany Zjednoczone należą do jednych z największych eksporterów (Huang i in., 2018).
- Spory o zasoby zmniejszających się źródeł wody pitnej, gruntów ornych i obszarów mieszkalnych mogą być przyczynami konfliktów krajowych, a na arenie międzynarodowej mogą powodować zmiany zasad światowego handlu i zmieniać sojusze polityczno-gospodarcze czy militarne. Mogą również wymiernie wpływać na politykę migracyjną wielu krajów.
- Spodziewane będą zapewne problemy w adaptacji społeczeństw do nowych warunków klimatycznych i ich skutków; dotyczyć to będzie również tych, wydawałoby się, dobrze przygotowanych. Sytuacje takie prawdopodobnie zwiększą skalę przesiedleń czy migracji. Na przykład lodowiec Thwaites, który odgrywa kluczową rolę w stabilizacji pokrywy lodowej Antarktydy Zachodniej, mógł już przekroczyć nieodwracalny punkt krytyczny. Thwaites rozciąga się na 120 kilometrów szerokości (jest mniej więcej wielkości Florydy). Gdyby cały lodowiec wpadł do oceanu, poziom mórz podniósłby się o 65 centymetrów. Stanowi to największe na świecie zagrożenie dla poziomu mórz w ciągu

najbliższych 80 lat (Gramling, 2022). Chociaż badania ewoluują, a ramy czasowe wpływu są wysoce niepewne, może to spowodować podniesienie się poziomu morza o ponad pół metra lub destabilizację pokrywy lodowej Antarktydy Zachodniej, według niektórych szacunków, nawet o 3,2 metra w dłuższej perspektywie czasowej (World Economic Forum, 2024).

- dramatycznie zmieniając linie brzegowe i zatapiając niektóre państwa wyspiarskie. Przykłady ilustruje Rysunek 5.

W przypadku realnych perspektyw przekroczenia krytycznych progów należy liczyć, że będzie rosła presja na szybkie działanie na dużą skalę, a punkt ciężkości programu Net Zero będzie coraz bardziej wykraczał poza dekarbonizację na „odwrócenie" zmian klimatycznych poprzez nowoczesne rozwiązania technologiczne, takie jak geoinżynieria. Jednak te powstające technologie mogą same w sobie stwarzać poważne skutki zewnętrzne, rodząc złożone pytania dotyczące odpowiedzialności. Obserwacja zmian zachodzących na Ziemi i ich przyczyn wskazuje, że geoinżynieria ma możliwość przeciwstawiania się najważniejszym czynnikom powodującym zmiany klimatu, a tym samym ich wpływom na środowisko naturalne, np. niektóre jej obszary umożliwią usuwanie dwutlenku węgla z atmosfery, podczas gdy inne oddziałują na ochłodzenie klimatu (Felgenhauer, 2022).



Rysunek 5. Orientacyjny wzrost poziomu mórz, wybrane kraje
Źródło: World Economic Forum, 2024.

Należy zauważyć, że wdrażanie technologii geoinżynieryjnych nie jest i nie będzie całkowicie bezdyskusyjne. Trzeba przyznać, że technologie te będą przynosić globalne korzyści, ale także wiązać się z zagrożeniami na poziomie globalnym, regionalnym czy lokalnym. Trzeba również mieć na uwadze, że inwestowanie i wprowadzanie tzw. emisji „zredukowanych"

(emisje z paliw kopalnych wychwytywanych za pomocą technologii) będą powodować lokowanie w nich środków finansowych, a tym samym spowolnienie rozwoju wielu gospodarek.

Jednocześnie nie należy zapominać, że możliwości i skutki wykorzystania nowych technologii nie są jeszcze do końca poznane i zbadane, a wyniki ich zastosowania są w wielu przypadkach całkowicie nieznane, np. jak twierdzą B. Sovacool i M. B. Chad, geologiczne składowanie węgla grozi przyszłym tzw. „odpowietrzeniem", z potencjalnie szkodliwymi konsekwencjami dla pobliskich społeczności (Sovacool, Baum, 2022). Należy mieć również na uwadze, że pojawić się mogą wątpliwości natury prawnej w zakresie odpowiedzialności za zmiany klimatyczne. Wszelkiego rodzaju powstałe straty i szkody związane ze zmianami klimatycznymi mogą być przedmiotem sporów sądowych wobec rządów wielu krajów. Wprowadzenie nowych technologii przez niektóre podmioty prawne może być powodem protestów społecznych i wysuwania roszczeń finansowych wobec rządów. Należy liczyć się z tym, że w wielu przypadkach koszty zmian geoinżynieryjnych wywołanych nowoczesnymi technologiami mogą być wyższe niż spodziewane lokalne skutki zmiany klimatu, co doprowadzić będzie mogło do napięć społecznych, włączając również konflikty transgraniczne.

Wydaje się, że w ciągu najbliższych 10 lat bardzo mało prawdopodobne jest jednostronne i niekontrolowane wdrożenie technologii manipulacji klimatem, w tym przez jeden kraj, podmioty niepaństwowe, takie jak filantropi, lub przez przedsiębiorstwa w celu uzyskania korzyści komercyjnych. Chociaż niektóre technologie mają jedynie tymczasowe skutki, istnieje duża niepewność co do ich skutków, nawet w perspektywie krótkoterminowej.

Należy być świadomym, że działania przeciwstawiające się ryzyku krytycznych zmian w systemach Ziemi wymagają rozwiniętego całościowego podejścia do zarządzania ryzykiem klimatycznym i podejmowania decyzji. Należy na poziomie geopolitycznym mieć na uwadze skutki społeczne i ekonomiczne zmian w systemie Ziemi. Konieczne wydaje się zintensyfikowanie prac badawczo-rozwojowych zarówno w odniesieniu do krytycznych zmian w systemach ziemskich, jak i niekorzystnych skutków pionierskich technologii, w tym geoinżynierii. Konieczne jest również rozwinięcie możliwości stymulowania działań mających na celu ograniczenie ingerencji ludzi w systemy Ziemi.

Najbardziej pilnym działaniem w zakresie zmian klimatycznych i ich złagodzenia będzie redukcja emisji. Ważnym aspektem będzie dostęp do istniejących rozwiązań adaptacyjnych, w tym systemów wczesnego ostrzegania i zdecentralizowanej energii odnawialnej, aby wzmocnić pozycję lokalnych społeczności. Państwa i banki rozwoju będą musiały ściśle współpracować, aby zmniejszyć ryzyko inwestycji dla sektora prywatnego w priorytetowych obszarach i na odpowiednich rynkach.

Technologie sztucznej inteligencji

Rozwój technologii sztucznej inteligencji jest zjawiskiem niezwykle dynamicznie rozwijającym się i należy liczyć się, że w najbliższych 10 latach technologie te będą miały ogromne znaczenie dla rozwoju społeczeństw poszczególnych krajów i ich gospodarek. Technologie związane ze sztuczną inteligencją będą generowały nie tylko korzyści czy zyski tych gospodarek, np. w zakresie ochrony zdrowia, ale z całą pewnością przyczynią się do postępu innych technologii, ale będą również źródłem wielu zagrożeń społecznych, w tym z samodoskonalającymi się modelami sztucznej inteligencji, które sprawują coraz większą kontrolę nad światem fizycznym, wywołując zmiany w strukturach społeczno-ekonomicznych.

Niekorzystne skutki technologii sztucznej inteligencji są jednym z 10 najważniejszych w najbliższej dekadzie (Rysunek 2, poz. 6) z tendencją do jeszcze bardziej znacznego negatywnego wpływu w dalszej perspektywie czasowej. Wyniki badań GRPS wskazują, że oprócz możliwości osiągnięcia przez jednostkę ogólnej sztucznej inteligencji (AGI) – uczenia się wykonywania wszelkich zadań związanych z ludźmi lub zwierzętami – kluczowe obawy wymieniane przez respondentów GRPS obejmują: dezinformację, utratę pracy i wysiedlenie, wykorzystanie przestępcze i cyberataki, uprzedzenia i dyskryminacje, wykorzystanie w podejmowaniu krytycznych decyzji zarówno przez organizacje, jak i państwa oraz integracja sztucznej inteligencji z bronią i działaniami wojennymi.

Trzeba zauważyć, że przy pracach nad sztuczną inteligencją zachwiana została zasada ostrożności (ostrożność w obliczu niepewności). Sytuacja ta wynikała w dużej mierze z zachłyśnięcia się nowymi możliwościami tej technologii i właściwe organy regulacyjne nie dostrzegły w porę potencjalnych niebezpieczeństw jej wykorzystania. Dynamiczny rozwój sztucznej

inteligencji, potrzeby rynku w zakresie jej wykorzystania będą dalej wyzwaniem dla instytucji zarządzających etycznym i prawnym jej wykorzystaniem. Wykorzystanie przez sektor prywatny sztucznej inteligencji zarówno na cele cywilne, jak i militarne sprawia, że problematyka regulacji jej wykorzystania staje się niezwykle ważna.

Brak bezpieczeństwa cybernetycznego i koncentracja mocy technologicznej są jedynymi czynnikami ryzyka powodującymi niekorzystne skutki technologii sztucznej inteligencji. Zdaniem wielu ekspertów, produkcja technologii sztucznej inteligencji jest wysoce skoncentrowana, w pojedynczym, globalnie zintegrowanym łańcuchu dostaw, który faworyzuje kilka firm i krajów (Ye, 2023). Sytuacja taka jest niekorzystna w nadchodzącej dekadzie z punktu widzenia np.: zapewnienia ciągłości dostaw w danym kraju, między innymi zaawansowanych półprzewodników, tworzenia się luk zabezpieczenia w systemach cybernetycznych, a tym samym bezpośrednio wpływać na bezpieczeństwo infrastruktury krytycznej.

Przyjmując, że technologie sztucznej inteligencji stają się dla każdego państwa wartością strategiczną, ich głównym beneficjentem będzie bezpieczeństwo narodowe. Rządy państw będą priorytetowo traktować bezpieczeństwo dostaw produktów i usług służących do zapewnienia bezpieczeństwa danego kraju. Przykładem mogą być Chiny, które kontrolują własne łańcuchy dostaw, jednocześnie blokując możliwość dostępu do szczególnie zaawansowanych technologii elektronicznych (chipów półprzewodnikowych) (Allen, 2023). Należy spodziewać się, że będą takie państwa, które będą dążyć do uzyskania wysokich zysków gospodarczych związanych z wykorzystaniem technologii sztucznej inteligencji, gdy inne dążyć będą do rozwiązania problemu koncentracji, potencjalnie kosztem innowacji (Haeck, 2023). Wobec takiej perspektywy, należy rozważyć konieczność podjęcia przez podmioty międzynarodowe (np. Unię Europejską) działań zwalczających (ograniczających) praktyki antykonkurencyjne w sektorze technologicznym.

Jest prawdopodobne, że selektywnie, mimo protekcjonizmu państwowego, jednak niektóre gałęzie produkcji pozostaną mocno skoncentrowane, a próby wejścia na dany rynek innych podmiotów będą niezwykle trudne, wręcz niemożliwe. Należy się liczyć z tym, że w dalszym ciągu dotychczas uznane i rozpoznawalne firmy będą wciąż odgrywać zasadniczą rolę na światowych rynkach.

Zasadnym wydaje się przypuszczenie, że system kontroli regulacyjnej dotyczącej zastosowań technologii sztucznej inteligencji niższych szczebli mógłby jeszcze bardziej umocnić pozycję rynkową istniejących wiodących podmiotów tej branży, a ich licencjonowanie może tylko te podmioty wzmocnić. Podmioty rządowe z reguły starają się w dużej mierze mieć pod kontrolą aplikacje o wyższym ryzyku. Jednak posiadacze technologii służących do tworzenia tych aplikacji siłą rzeczy będą mieć realny wpływ na procesy legislacyjne. Także istotne jest, że to nie sprawy publiczne, a komercyjne będą siłą napędową rozwoju technologii sztucznej inteligencji. Konsekwencje komercyjnego rozwoju sztucznej inteligencji mogą być widoczne w ciągu najbliższej dekady, szczególnie w obszarze militarnym, opieki zdrowotnej, finansów czy prawa. Rozwój komputerów kwantowych może naruszyć tajemnice handlowe z wielu branż, w tym farmaceutycznej i sprzętu technologicznego, podobnie jak krytycznie wrażliwe dane, takie jak dostęp do elektronicznej dokumentacji medycznej. Sparaliżowana może zostać globalna infrastruktura bankowa, energetyczna czy szpitalna. Jednak chyba najbardziej kosztowne może być zachwianie systemu bezpieczeństwa globalnego czy regionalnego.

Prognozowana rzeczywistość w zakresie rozwoju technologii sztucznej inteligencji może doprowadzić do podziału na podmioty wyraźnie zyskujące i na te, które w tej rywalizacji będą ulegać. Dotyczyć to będzie zarówno gospodarek wysoko rozwiniętych, jak i tych rozwijających się. Sytuacja taka może doprowadzić w ciągu najbliższych dziesięciu lat do wyraźnych różnic w rozwoju społeczeństw. Kraje już obecnie borykające się z trudnościami ekonomiczno-gospodarczymi jeszcze bardziej odczują efekty dostępu i stosowania technologii sztucznej inteligencji między innymi w zakresie, gospodarki, finansów, ochrony zdrowia, bezpieczeństwa wewnętrznego i zewnętrznego czy ochrony środowiska.

W związku z tym należy liczyć się z tym, że dostęp do technologii sztucznej inteligencji będzie szczególnie istotny i będzie źródłem rywalizacji międzynarodowej, aby umocnić swoje wpływy. Sztuczna inteligencja będzie narzędziem do osiągnięcia następnego przełomu technologicznego i producenci jej elementów z całą pewnością będą bezwzględnie z tych zasobów i możliwości korzystać. Eksperci uważają, że takie państwa jak: Australia, Kanada, Indonezja, Maroko, Wietnam czy Chile będą mogły

wymiernie korzystać z możliwości dostaw minerałów krytycznych, a z korzyści z posiadanych własności intelektualnych czerpać będą państwa takie jak Japonia i Korea Południowa lub posiadające kapitał, takie jak Norwegia czy Singapur.

W związku z tym, że firmy zajmujące się nowoczesnymi technologiami mają tak naprawdę ponadnarodowy charakter, niebezpieczne może być to, że oficjalny dostęp do tych technologii będzie utrudniony, ale w wielu przypadkach będzie się odbywał poza kontrolą władz państwowych. Szczególnie istotna będzie kwestia dostępu do technologii sztucznej inteligencji ogólnego przeznaczenia o podwójnym zastosowaniu. Przykładem jednostronnych działań podmiotów prywatnych w tym zakresie mogą być: systemowe wykorzystanie w wojnie w Ukrainie satelitów cywilnych czy różne formy dezinformacji. Rozwój i wykorzystanie technologii sztucznej inteligencji do celów wojskowych w ciągu następnej dekady mogą zagrozić globalnej stabilności, a włączenie sztucznej inteligencji do procesu podejmowania decyzji w konfliktach stanowić może poważne ryzyko.

Technologie sztucznej inteligencji bez wątpienia zwiększą skuteczność wojny w cyberprzestrzeni, umożliwiając tworzenie całych systemów ofensywnych i defensywnych, które mogą działać autonomicznie, z nieprzewidywalnym wpływem na sieci i połączoną infrastrukturę. Jeśli chodzi o wojnę kinetyczną, światowe i regionalne mocarstwa zainwestowały znaczne środki w rozwój systemów uzbrojenia opartych na sztucznej inteligencji, a stopień autonomii im przyznany wzrasta: broń lądowa, powietrzna i morska może już prowadzić nadzór i działania bez udziału człowieka (Adler, 2023). Podjęte zostały próby ustanowienia międzynarodowego zarządzania jej użyciem, jednak porozumienia nie zostały jeszcze zawarte. Godnym uwagi było w 2023 roku wstrzymanie się od głosu i głosowanie przeciwko projektowi rezolucji ONZ w sprawie autonomicznych systemów uzbrojenia, w tym Chiny, Korea Północna, Iran, Izrael, Turcja, Zjednoczone Emiraty Arabskie, Indie i Rosja. W związku z tym powstaje realne ryzyko, że systemy sztucznej inteligencji mogłyby zostać zastosowane do autonomicznego podejmowania decyzji w sprawie działań kinetycznych, w tym określania i wyboru celów. Uprawnienia takie obarczone będą dużym marginesem potencjalnych błędów rodzących poważne ryzyka, od niekontrolowanego rozpoczęcia konfliktu zbrojnego, a kończąc na nieprzewidywalnych decyzjach dotyczących

działań śmiercionośnych, w tym wykorzystania broni jądrowej. Podczas gdy rządy wskazały, że ludzka kontrola nad systemami broni jądrowej zostanie utrzymana, w zasadzie sztuczna inteligencja może zapewnić najlepszą obronę poprzez skrócenie czasu podejmowania decyzji (Parke, 2023). Pamiętać należy, że systemy startowe wykorzystujące sztuczną inteligencję mogą podważyć stabilność strategiczną, biorąc pod uwagę ich teoretyczny potencjał do atakowania zasobów jądrowych i zdolność do drugiego uderzenia. Jeżeli państwa powiążą technologie AI z bronią jądrową, to w ciągu następnej dekady znacząco wzrośnie ryzyko konfliktu nuklearnego.

Badania wykonane przez Global Risks Perception Survey (GRPS) identyfikują świadomość społeczną i edukację jako jedne z najskuteczniejszych mechanizmów reagowania na wypadek zagrożeń i ograniczania niepożądanych skutków technologii sztucznej inteligencji oraz jako kluczowe narzędzie zarządzania lokalnymi skutkami, a także budowania zdolności w zakresie zarządzania i odporności społecznej. Umiejętność korzystania z generatywnej sztucznej inteligencji ma zasadnicze znaczenie zarówno dla organów regulacyjnych jak i dla szerszego społeczeństwa. Umiejętność korzystania z AI powinna zostać włączona do publicznych systemów edukacji i szkoleń dla dziennikarzy i decydentów, aby nie tylko zrozumieć możliwości systemów sztucznej inteligencji, ale także zidentyfikować wiarygodne źródła informacji, co będzie coraz większym wyzwaniem.

Respondenci GRPS podkreślają również potrzebę wprowadzenia przepisów krajowych i lokalnych. Chociaż wysiłki na szczeblu krajowym niekoniecznie zapobiegną szybkiemu globalnemu rozprzestrzenianiu się sztucznej inteligencji i powiązanym zagrożeniom, solidne, ale elastyczne ustanawianie norm może pomóc w zapewnieniu dostosowania rozwoju i wdrażania technologii do potrzeb społecznych. Wydaje się, że aby sprostać nowym wyzwaniom związanym z generatywną sztuczną inteligencją, aktualne prawodawstwa w zakresie własności intelektualnej, zatrudnienia, polityki konkurencji, ochrony danych, prywatności i praw człowieka będą musiały ewoluować, dostosowując się do nowych rzeczywistości i oczekiwań. Problematyka regulacji prawnych, która powinna być pilnie zrealizowana, powinna obejmować: identyfikację produktów wytwarzanych przez sztuczną inteligencję, blokowanie lub ograniczenia w odniesieniu do najbardziej ryzykownych zastosowań oraz ustalenie odpowiedzialności za szkody

spowodowane przez sztuczną inteligencję. Proponowane rozwiązania obejmują między innymi: rejestrację i licencjonowanie najpotężniejszych wersji technologii, wielopoziomowy dostęp do mocy obliczeniowej, wdrożenie systemów pochodzenia i/lub znaków wodnych, procedury „Znaj swojego klienta" i obowiązkowe ujawnianie incydentów oraz stworzenie solidnego systemu audytu i certyfikacji.

Niezwykle istotną kwestią są globalne traktaty i porozumienia w zakresie zarządzania zarówno niekorzystnymi skutkami technologii sztucznej inteligencji, jak i koncentracją władzy technologicznej. Problematyka zarządzania sztuczną inteligencją na szczeblu globalnym została już poddana częściowej regulacji poprzez pierwsze zarządzenia w tym zakresie, np.: ostatnie ustalenia grupy G-7 z Hiroszimy (19-21 maja 2023 r.) w sprawie generatywnej sztucznej inteligencji, a także deklarację z Bletchley (5 listopada 2023 r.). W 2023 roku pojawiły się głosy postulujące powołania Międzyrządowego Zespołu ds. Sztucznej Inteligencji (IPCC) (Suleyman, Schmidt, 2023). Zdaniem autorów koncepcji powołania tego Zespołu, jego celem byłoby połączenie wysiłków podmiotów prywatnych i rządowych w zakresie przeciwdziałania zagrożeniom stwarzanym przez technologie sztucznej inteligencji. Zespół ten mógłby przedstawiać prognozy organizacyjnych i systemowych (sprzętowych) rozwiązań oraz rekomendować właściwym organom/decydentom skuteczne środki przeciwdziałania szkodliwemu wykorzystaniu sztucznej inteligencji. Innym obszarem działania tego Zespołu mogłoby być również nadzór nad sprawozdawczością dotyczącą baz danych i rejestrowanie kluczowych systemów sztucznej inteligencji. Zmaterializowanie tej koncepcji wymagać będzie jednak ogólnego konsensusu liczących się mocarstw światowych, co przy obecnej sytuacji geopolitycznej jest i zapewne będzie niezwykle trudne.

Podsumowanie

Analiza wybranych zagrożeń bezpieczeństwa globalnego wskazuje, że współczesne środowisko bezpieczeństwa charakteryzuje się wysokim poziomem złożoności oraz dynamicznymi zmianami wynikającymi z oddziaływania wielu wzajemnie powiązanych czynników. Do najistotniejszych należą przede wszystkim zmiany klimatyczne, rozwój technologii – w tym szczególnie sztucznej inteligencji – a także przemiany demograficzne oraz

uwarunkowania geostrategiczne kształtujące relacje międzynarodowe. Czynniki te tworzą tzw. siły strukturalne, które w sposób bezpośredni lub pośredni wpływają na stabilność systemu bezpieczeństwa globalnego.

Przeprowadzona analiza literatury oraz dokumentów strategicznych wskazuje, że zagrożenia te będą w najbliższych latach narastać, a ich konsekwencje będą odczuwalne zarówno w wymiarze regionalnym, jak i globalnym. W krótkiej perspektywie czasowej szczególnie istotne są napięcia geopolityczne, rozwój technologii informacyjnych oraz rosnące znaczenie cyberprzestrzeni jako nowego obszaru rywalizacji państw. Z kolei w dłuższej perspektywie znaczącego wpływu na bezpieczeństwo międzynarodowe należy oczekiwać ze strony zmian klimatycznych, migracji ludności, transformacji energetycznej oraz rozwoju zaawansowanych technologii cyfrowych.

Istotnym wnioskiem wynikającym z przeprowadzonych rozważań jest również fakt, że postrzeganie zagrożeń przez różne podmioty – zarówno państwowe, jak i pozarządowe – nie zawsze jest jednakowe. Różnice te wynikają z odmiennych interesów politycznych, gospodarczych i społecznych, a także z różnej oceny skali oraz czasu występowania potencjalnych zagrożeń. W konsekwencji utrudnia to wypracowanie spójnych i skutecznych mechanizmów przeciwdziałania zagrożeniom na poziomie globalnym.

Wobec powyższego szczególnego znaczenia nabiera rozwijanie międzynarodowej współpracy w zakresie zarządzania bezpieczeństwem, wzmacnianie instytucji odpowiedzialnych za monitorowanie zagrożeń oraz rozwój systemów wczesnego ostrzegania. Konieczne jest również prowadzenie pogłębionych badań naukowych dotyczących wpływu nowych technologii, w tym sztucznej inteligencji, na funkcjonowanie systemów bezpieczeństwa państw oraz organizacji międzynarodowych.

Podsumowując, można stwierdzić, że bezpieczeństwo globalne w nadchodzących latach będzie w coraz większym stopniu determinowane przez oddziaływanie czynników technologicznych, środowiskowych i społecznych. Skuteczne reagowanie na te wyzwania wymaga podejścia interdyscyplinarnego, integrującego wiedzę z zakresu nauk o bezpieczeństwie, stosunków międzynarodowych, ekonomii, technologii oraz nauk społecznych. Tylko takie podejście pozwoli na właściwe identyfikowanie zagrożeń oraz budowanie długofalowej odporności systemu bezpieczeństwa globalnego.

Literatura

1. Adler, N. (2023). *Are killer robots the future of war?* Al Jazeera. Pobrane z: https://www.aljazeera.com/features/2023/5/16/are-killer-robots--the-future-of-war (dostęp: 12.02.2026).
2. Allen, G. C. (2023). *China's new strategy for waging the microchip tech war. Center for Strategic & International Studies*. Pobrane z: https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech--war (dostęp: 12.02.2026).
3. Felgenhauer, T. (2022). *Solar radiation modification: A risk-risk analysis. Carnegie Climate Governance Initiative*. Pobrane z: https://www.c2g2.net/wp-content/uploads/202203-C2GRR-Full.pdf (dostęp: 12.02.2026).
4. Gramling, C. (2022). *The "Doomsday" glacier may soon trigger a dramatic sea-level rise. Science News Explores*. Pobrane z: https://www.snexplores.org/article/antarctica-thwaites-glacier-ice-shelf-collapse-climate-5-years (dostęp: 12.02.2026).
5. Haeck, P. (2023). *With Apple's iPhone 15, the EU wins the charger war*. Politico. Pobrane z: https://www.politico.eu/article/apple-iphone-15-european-union-regulations-charger-usbc-lightning/ (dostęp: 12.02.2026).
6. Huang, J., Piñeiro, M., Piñeiro, V. (2018). *Global food security and market stability: The role and concerns of large net food importers and exporters. International Food Policy Research Institute.* Pobrane z: https://www.ifpri.org/publication/brief-2-global-food-security-and-market-stability-role-and-concerns-large-net-food (dostęp: 12.02.2026).
7. Institute for Economics & Peace. (2023). *Global Terrorism Index 2023: Measuring the impact of terrorism*. Pobrane z: https://www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf (dostęp: 12.02.2026).
8. Intergovernmental Panel on Climate Change. (2022). *Climate change 2022: Impacts, adaptation and vulnerability*. Pobrane z: https://www.ipcc.ch/report/sixth-assessment-report-working-group-ii/ (dostęp: 12.02.2026).
9. Kwiatkowski, L. (2019). Decline in Atlantic primary production accelerated by Greenland ice sheet melt. *Geophysical Research Letters, 46*(20), 11347-11357. https://doi.org/10.1029/2019GL085267

10. Lenton, T. M., Armstrong McKay, D. I., Loriani, S., Abrams, J. F., Lade, S. J., Donges, J. F., Milkoreit, M., Powell, T., Smith, S. R., Zimm, C., Buxton, J. E., Bailey, E., Laybourn, L., Ghadiali, A., Dyke, J. G. (red.). (2023). *The Global Tipping Points Report 2023*. University of Exeter. Pobrane z: https://global-tipping-points.org/ (dostęp: 12.02.2026).
11. McKay, D. I. A., Staal, A., Abrams, J. F., Winkelmann, R., Sakschewski, B., Loriani, S., Fetzer, I., Cornell, S. E., Rockström, J., Lenton, T. M. (2022). Exceeding 1.5°C global warming could trigger multiple climate tipping points. *Science, 377*(6611), eabn7950. https://doi.org/10.1126/science.abn7950
12. Parke, M. (2023). *Zapobieganie nuklearnemu Armagedonowi. Project Syndicate*. Pobrane z: https://www.project-syndicate.org/commentary/dangers-of-artificial-intelligence-ai-applications-nuclear-weapons-by-melissa-parke-2023-11 (dostęp: 12.02.2026).
13. Sovacool, B. K., Baum, C. M. (2022). *Ensuring the environmental sustainability of emerging technologies for carbon dioxide removal. EPFL International Risk Governance Center*. Pobrane z: https://www.epfl.ch/research/domains/irgc/wp-content/uploads/2022/12/IRGC-2022-Ensuring-the-environmental-sustainability-of-emerging-technologies-for-carbon-dioxide-removal.pdf (dostęp: 12.02.2026).
14. Suleyman, M., Schmidt, E. (2023). *Mustafa Suleyman and Eric Schmidt: We need an AI equivalent of the IPCC*. Financial Times. Pobrane z: https://www.ft.com/content/d84e91d0-ac74-4946-a21f-5f82eb4f1d2d (dostęp: 12.02.2026).
15. World Economic Forum. (2024). *The Global Risks Report 2024: 19th edition*. Pobrane z: https://www.weforum.org/publications/global-risks-report-2024/ (dostęp: 12.02.2026).
16. Ye, J. (2023). *How Huawei plans to rival Nvidia in the AI chip business*. Reuters. Pobrane z: https://www.reuters.com/technology/how-huawei-plans-rival-nvidia-ai-chip-business-2023-11-07/ (dostęp: 12.02.2026).

Zbigniew Ciekanowski[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska
Wiesława Załoga[2]
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Warszawa
Martyna Zaroślak[3]
Uniwersytet w Siedlcach

https://doi.org/10.29316/9788368103373_22

ROLA WOJSK OBRONY CYBERPRZESTRZENI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA WOBEC ZAGROŻEŃ HYBRYDOWYCH

THE ROLE OF CYBER DEFENCE FORCES IN THE NATIONAL SECURITY SYSTEM IN THE FACE OF HYBRID THREATS

Streszczenie

Celem rozdziału jest określenie rzeczywistej roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa oraz zbadanie, czy są one jedynie wyspecjalizowanym komponentem militarnym, czy też pełnią funkcję węzłową w krajowym ekosystemie odporności na zagrożenia hybrydowe. Problem badawczy dotyczy zagadnienia, w jakim stopniu Wojska Obrony Cyberprzestrzeni wzmacniają zdolność

[1] https://orcid.org/0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl
[2] https://orcid.org/0000-0001-7758-0187, e-mail: wieslawa.zaloga@wat.edu.pl
[3] https://orcid.org/0000-0001-7693-8327, e-mail: martynazaroslak@gmail.com

państwa do zapobiegania, wykrywania, neutralizowania oraz odtwarzania skutków złożonych kampanii hybrydowych, obejmujących działania w cyberprzestrzeni, manipulację informacyjną, presję na infrastrukturę krytyczną oraz operacje prowadzone poniżej progu wojny. Zastosowano jakościową analizę instytucjonalno-prawną, krytyczny przegląd literatury polsko- i anglojęzycznej, analizę wtórną danych statystycznych z raportów CERT Polska i CSIRT GOV za lata 2020-2024 oraz studium przypadku incydentu dezinformacyjno-cybernetycznego związanego z fałszywą depeszą PAP z 31 maja 2024 r. Analiza potwierdza, że skuteczność Wojsk Obrony Cyberprzestrzeni nie wynika wyłącznie z posiadania zdolności technicznych, lecz z ich integracji z całym systemem bezpieczeństwa państwa, w tym z krajowymi CSIRT-ami, administracją publiczną, infrastrukturą krytyczną, sektorem prywatnym i strukturami sojuszniczymi. Empirycznie widoczny wzrost liczby incydentów w polskiej cyberprzestrzeni oraz narastanie zagrożeń mieszanych wskazują, że Wojska Obrony Cyberprzestrzeni powinny być traktowane jako komponent obrony państwa, odporności systemowej i wsparcia operacji połączonych, a nie wyłącznie jako narzędzie ochrony sieci resortu obrony.

Słowa kluczowe: bezpieczeństwo państwa, cyberbezpieczeństwo, zagrożenia hybrydowe, Wojska Obrony Cyberprzestrzeni, odporność, CSIRT, infrastruktura krytyczna

Abstract

The aim of chapter is to define the actual role of the Cyberspace Defence Forces in the state security system and to verify whether they should be understood merely as a specialised military component or rather as a nodal actor in the national resilience ecosystem against hybrid threats. The research problem concerns the extent to which the Cyberspace Defence Forces enhance the state's ability to prevent, detect, neutralise, and recover from complex hybrid campaigns involving cyber operations, information manipulation, pressure on critical infrastructure, and activities conducted below the threshold of war. The study uses qualitative institutional and legal analysis, a critical review of Polish- and English-language literature, secondary statistical analysis based on CERT Polska and CSIRT GOV reports for 2020-2024, and a case study of the cyber-disinformation incident related to the false PAP mobilisation dispatch on 31 May 2024. Findings: The study shows that the effectiveness of the Cyberspace Defence Forces depends not only on their technical capabilities but above all on their integration with the broader state security architecture, including national CSIRTs, public administration, critical infrastructure operators, the private sector and allied structures.

Keywords: state security, cybersecurity, hybrid threats, Cyberspace Defence Forces, resilience, CSIRT, critical infrastructure

Wstęp

Współczesne środowisko bezpieczeństwa jest kształtowane przez zjawiska, które wymykają się klasycznemu podziałowi na pokój i wojnę. W praktyce rośnie znaczenie działań prowadzonych poniżej progu otwartego konfliktu zbrojnego, łączących presję polityczną, operacje informacyjne, sabotaż, wrogą aktywność w cyberprzestrzeni i uderzenia w infrastrukturę krytyczną. Unia Europejska definiuje zagrożenia hybrydowe jako skoordynowane działania wymierzone w państwo lub instytucję przy użyciu zróżnicowanych, często łączonych środków, takich jak manipulacja informacyjna, cyberataki, presja ekonomiczna czy groźba użycia siły. Z kolei NATO uznaje cyberobronę za element odstraszania i obrony zbiorowej, a od szczytu w Warszawie w 2016 r. traktuje cyberprzestrzeń jako domenę operacyjną, w której Sojusz musi bronić się równie skutecznie jak na lądzie, morzu i w powietrzu. W sensie strategicznym oznacza to, że państwo nie może już oddzielać bezpieczeństwa militarnego od cyfrowego i informacyjnego, przeciwnie, musi myśleć o nich jako o jednym polu współzależnych oddziaływań (Bachmann i in., 2023; Hoffman, 2007).

W przypadku Polski skala wyzwania jest wyraźnie widoczna w danych operacyjnych. Według rocznego sprawozdania o cyberbezpieczeństwie w 2024 r. krajowe zespoły CSIRT zarejestrowały łącznie 111 660 incydentów bezpieczeństwa teleinformatycznego; sam CSIRT NASK odnotował 103 449 przypadków, CSIRT GOV 3 991, a CSIRT MON 4 220 (Ministerstwo Cyfryzacji, 2025). Oznacza to dalszy wzrost presji na państwowy ekosystem bezpieczeństwa oraz pokazuje, że problem cyberzagrożeń nie ma już charakteru niszowego, lecz systemowego. W warunkach utrzymującego się podwyższonego poziomu zagrożenia w cyberprzestrzeni oraz obowiązywania stopnia alarmowego CHARLIE-CRP zdolności obronne muszą być rozpatrywane w kategoriach stałej gotowości, a nie wyłącznie doraźnej reakcji (Ministerstwo Cyfryzacji, 2025). W tym kontekście kluczowego znaczenia nabiera wyspecjalizowany komponent militarny odpowiedzialny za ochronę i działania w cyberprzestrzeni. Zgodnie z informacjami Ministerstwa Obrony Narodowej, Wojska Obrony Cyberprzestrzeni realizują zadania w kluczowych obszarach związanych z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów teleinformatycznych (Ministerstwo Obrony Narodowej, 2022; Ministerstwo Obrony Narodowej, b.d.). W ich strukturze

znajduje się 12 podporządkowanych jednostek wojskowych, w tym wyspecjalizowane jednostki działań w cyberprzestrzeni „A" i „B", od 2024 r. trwa również formowanie jednostki „C" we Wrocławiu. WOC odpowiadają także za świadczenie usług teleinformatycznych na rzecz Sił Zbrojnych RP oraz za zapewnienie prawidłowego funkcjonowania CSIRT MON, prowadzącego całodobowy monitoring sieci resortu obrony. Przyjęte rozwiązania instytucjonalne potwierdzają, że Wojska Obrony Cyberprzestrzeni nie są jedynie uzupełnieniem klasycznych rodzajów sił zbrojnych, lecz stanowią istotny filar ochrony cyfrowego wymiaru działań militarnych oraz cyfrowego zaplecza państwa (Kuś, 2023).

Celem niniejszego rozdziału jest zatem odpowiedź na pytanie, jaka jest rzeczywista rola Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa wobec zagrożeń hybrydowych. Przyjęto hipotezę, że skuteczność WOC zależy przede wszystkim od stopnia ich integracji z szerszym systemem bezpieczeństwa państwa, a nie wyłącznie od własnych zdolności technicznych. Weryfikacja tej hipotezy wymaga połączenia perspektywy prawno-instytucjonalnej, strategicznej i empirycznej, dlatego w dalszej części zestawiono ustalenia literatury z aktualnymi rozwiązaniami organizacyjnymi oraz danymi o zagrożeniach i incydentach.

Przegląd literatury

W literaturze przedmiotu pojęcie zagrożeń hybrydowych ujmowane jest szeroko, jednak jego wspólny rdzeń stanowi łączenie środków wojskowych i pozawojskowych, jawnych i ukrytych, a także kinetycznych i niekinetycznych. Frank G. Hoffman wskazywał, że wojny hybrydowe charakteryzują się równoczesnym wykorzystaniem zróżnicowanych instrumentów oddziaływania, przy czym ich skuteczność wzrasta wraz z umiejętnym zacieraniem granic między stanem wojny a stanem pokoju. Nowsze ujęcia tego zagadnienia akcentują znaczenie tzw. szarej strefy działań, rozumianej jako przestrzeń celowych operacji prowadzonych poniżej progu formalnej wojny, lecz zarazem dostatecznie intensywnych, aby wpływać na decyzje polityczne, odporność społeczną oraz ciągłość funkcjonowania państwa. W tym kontekście Dominika Dziwisz trafnie lokuje cyberprzestrzeń w centrum rosyjskiej perspektywy działań typu grey zone, wskazując, że operacje cyfrowe są szczególnie użyteczne w sytuacji, gdy państwo dąży do osiągania efektów

strategicznych bez uruchamiania pełnoskalowej eskalacji (Dziwisz, 2024; Hoffman, 2007).

Drugi istotny nurt badań koncentruje się na relacji między wojną hybrydową a cyberoperacjami. Alan Brill i John Bennett podkreślają, że współczesne zagrożenia w cyberprzestrzeni stają się coraz bardziej złożone, wielowarstwowe oraz maskujące swój rzeczywisty cel, co utrudnia zarówno ich atrybucję, jak i szybkie podjęcie adekwatnej reakcji. Z kolei analizy dotyczące wojny rosyjsko-ukraińskiej wskazują, że cyberoperacje rzadko stanowią autonomiczne narzędzie rozstrzygające konflikt, lecz regularnie pełnią funkcję wzmacniającą wobec innych instrumentów oddziaływania: wspierają rozpoznanie, wpływają na świadomość społeczną, zakłócają świadczenie usług, obciążają administrację publiczną oraz generują presję psychologiczną. Matthias Schulze, analizując użyteczność działań cybernetycznych na poziomie strategicznym, operacyjnym i taktycznym, dochodzi do wniosku, że ich największa skuteczność ujawnia się w ścisłym powiązaniu z innymi narzędziami polityki państwa. Podobny kierunek interpretacyjny odnaleźć można u Wróblewskiego i Wiśniewskiego, którzy wskazują, że konflikt w Ukrainie istotnie zwiększył ryzyko cyberataków, dezinformacji i agresji informacyjnej, oddziałujących również na sektor publiczny oraz społeczeństwo w Polsce (Brill, Bennett, 2022; Schulze, 2020; Wróblewski, Wiśniewski, 2024).

Trzeci obszar badań obejmuje problematykę odporności oraz współpracy cywilno-wojskowej. Raport Joint Research Centre Komisji Europejskiej wskazuje, że odporność na zagrożenia hybrydowe nie może być budowana w sposób punktowy, lecz powinna mieć charakter systemowy, uwzględniający zależności i współzależności między poszczególnymi segmentami państwa i społeczeństwa. W praktyce oznacza to konieczność integrowania komponentów militarnego, administracyjnego, infrastrukturalnego oraz prywatnego. Csaba Krasznay podkreśla natomiast, że wojna rosyjsko-ukraińska unaoczniła szczególną podatność infrastruktury krytycznej, której ochrona w wielu przypadkach opiera się na zdolnościach cywilnych podmiotów cyberbezpieczeństwa. W konsekwencji skuteczna obrona wymaga rozwiniętej wymiany informacji, wspólnych standardów oraz mechanizmów integrujących wojskowe i cywilne zdolności ochronne. Obserwacja ta ma szczególne znaczenie dla Wojsk Obrony Cyberprzestrzeni, ponieważ ich

efektywność zależy nie tylko od potencjału technicznego jednostek wojskowych, lecz także od jakości współdziałania z instytucjami cywilnymi oraz sektorem prywatnym (Jungwirth i in., 2023; Krasznay, 2024). W polskiej literaturze problematyka organizacyjno-prawnej roli sił zbrojnych w obszarze cyberbezpieczeństwa została wyraźnie zarysowana przez Bartosza Kusia, jednak nadal brakuje opracowań łączących perspektywę normatywną, instytucjonalną i empiryczną w odniesieniu do zmian po 2024 r., w szczególności po przyjęciu nowej Strategii Cyberbezpieczeństwa RP oraz nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa w 2026 r. W rezultacie pozostaje dostrzegalna luka badawcza pomiędzy klasycznym ujęciem Wojsk Obrony Cyberprzestrzeni jako wyspecjalizowanego komponentu Sił Zbrojnych a analizą ich rzeczywistej funkcji w państwowym systemie reagowania na zagrożenia hybrydowe. Niniejszy rozdział zmierza do wypełnienia tej luki poprzez zestawienie ustaleń literatury przedmiotu z aktualnymi dokumentami strategicznymi oraz danymi operacyjnymi (Kuś, 2023).

Część empiryczna

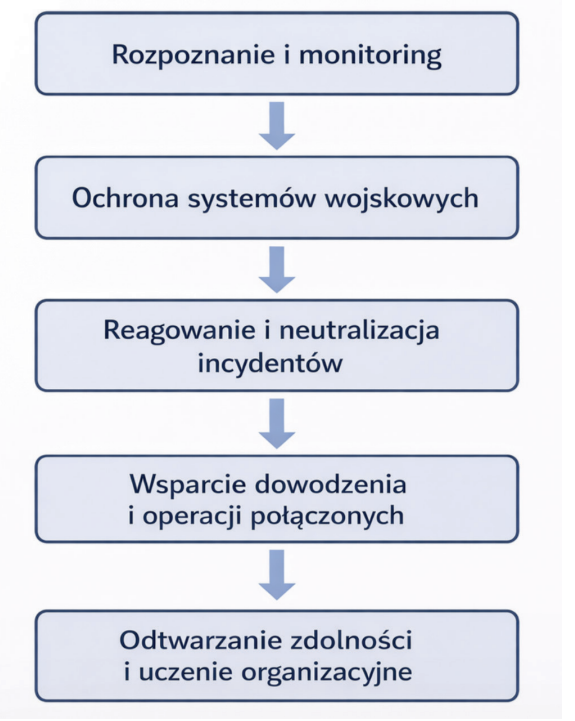
Część empiryczną oparto na triangulacji trzech typów materiału badawczego. Po pierwsze, przeprowadzono analizę instytucjonalno-prawną aktualnych dokumentów państwowych i sojuszniczych, obejmującą m.in. informacje dotyczące statusu Wojsk Obrony Cyberprzestrzeni, nowej Strategii Cyberbezpieczeństwa RP oraz zmian w krajowym systemie cyberbezpieczeństwa. Po drugie, wykorzystano wtórną analizę danych statystycznych zawartych w raportach CERT Polska i CSIRT GOV za lata 2020-2024. Po trzecie, zastosowano metodę studium przypadku, odnosząc ją do incydentu z 31 maja 2024 r., kiedy w oficjalnym serwisie PAP opublikowano fałszywą depeszę dotyczącą mobilizacji, zakwalifikowaną w oficjalnych materiałach jako cyberatak o istotnym wymiarze informacyjnym. Tak dobrany materiał badawczy pozwala ujmować Wojska Obrony Cyberprzestrzeni nie jako abstrakcyjny konstrukt organizacyjny, lecz jako podmiot funkcjonujący w konkretnym środowisku zagrożeń.

Punktem wyjścia analizy jest status formalnoprawny tej formacji. Ustawa o obronie Ojczyzny wskazuje Wojska Obrony Cyberprzestrzeni jako wyspecjalizowany komponent Sił Zbrojnych Rzeczypospolitej Polskiej, właściwy do realizacji pełnego spektrum działań w cyberprzestrzeni

(Rysunek 1). Na poziomie praktycznym oznacza to zdolność do prowadzenia działań obronnych, rozpoznawczych i ofensywnych, a zarazem odpowiedzialność za utrzymywanie oraz monitorowanie sieci i systemów teleinformatycznych Sił Zbrojnych RP, zarówno jawnych, jak i niejawnych. Dodatkowo, Wojska Obrony Cyberprzestrzeni zapewniają funkcjonowanie CSIRT MON, stanowiącego element krajowego systemu reagowania na incydenty odpowiedzialnego za obszar resortu obrony narodowej. Istotne znaczenie ma również logika programu CYBER.MIL 2.0, opartego na pięciu filarach: budowie struktur i infrastruktury, edukacji i szkoleniu, rekrutacji oraz aktywnej rezerwie, współpracy międzynarodowej, a także pozyskiwaniu narzędzi umożliwiających prowadzenie pełnego spektrum działań w cyberprzestrzeni. W ujęciu praktycznym wskazuje to, że Wojska Obrony Cyberprzestrzeni są projektowane jako formacja integrująca funkcje obronne, operacyjne, kadrowe i innowacyjne (Kuś, 2023).

W perspektywie systemowej rola Wojsk Obrony Cyberprzestrzeni wykracza poza ochronę wewnętrznych sieci wojskowych i obejmuje szerszy zakres funkcji istotnych z punktu widzenia bezpieczeństwa państwa. W tym kontekście można wyróżnić co najmniej cztery wzajemnie powiązane obszary ich oddziaływania. Po pierwsze, Wojska Obrony Cyberprzestrzeni zabezpieczają zdolność Sił Zbrojnych RP do zachowania ciągłości procesów dowodzenia, łączności, logistyki oraz zarządzania zasobami (Tabela 1). Po drugie, poprzez funkcjonowanie CSIRT MON stanowi istotny element krajowego systemu reagowania na incydenty cybernetyczne. Po trzecie, wzmacniają odporność państwa dzięki ochronie kluczowych technologii oraz rozwijaniu współpracy krajowej i międzynarodowej w obszarze cyberbezpieczeństwa. Po czwarte, pełnią funkcję odstraszającą, gdyż posiadanie wyspecjalizowanego komponentu cybernetycznego zwiększa koszt i ryzyko działań podejmowanych przez potencjalnego przeciwnika. Taki sposób ujmowania roli Wojsk Obrony Cyberprzestrzeni koresponduje z kierunkami wyznaczonymi w Strategii Cyberbezpieczeństwa RP z 10 marca 2026 r., przewidującej rozwój krajowej kryptografii i technologii kwantowych, rozwiązań chmurowych dla potrzeb cyberbezpieczeństwa, bezpieczeństwa łańcucha dostaw oraz centralnej ochrony przed atakami DDoS dla instytucji publicznych, w tym Sił Zbrojnych RP (Rada Ministrów, 2026; Ministerstwo Cyfryzacji, 2026). W konsekwencji, Wojska Obrony Cyberprzestrzeni

należy postrzegać jako istotny element szerszego programu budowy suwerenności technologicznej i cyberodporności państwa.



Rysunek 1. Model roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa

Źródło: opracowanie własne na podstawie Ministerstwo Cyfryzacji, 2025, 2026; Ministerstwo Obrony Narodowej, 2022, b.d.; NATO, 2016, 2024; Rada Unii Europejskiej, 2026.

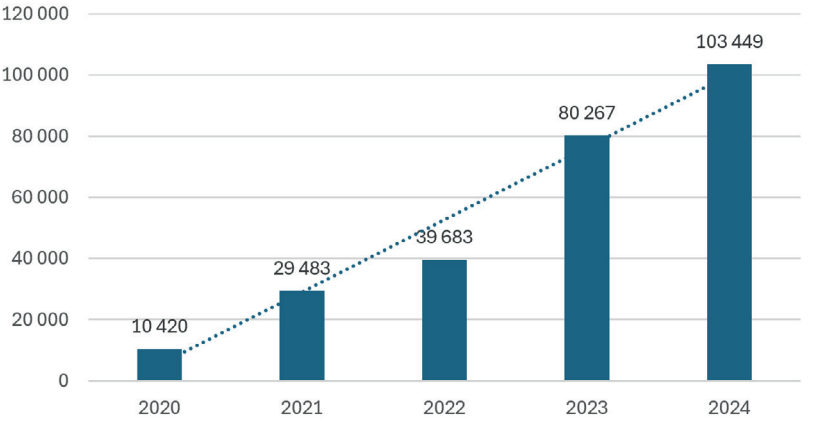
Tabela 1. Główne wymiary roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa

Wymiar roli	Treść funkcji	Główni partnerzy instytucjonalni	Przykładowy efekt bezpieczeństwa
Strategiczny	budowa zdolności, planowanie, rozwój narzędzi, współpraca sojusznicza	MON, NATO, instytucje rządowe	wzrost odstraszania I odporności państwa
Operacyjny	monitorowanie, reagowanie, obsługa incydentów, wsparcie operacji połączonych	CSIRT MON, inne CSIRT-y poziomu krajowego, PCOC	skrócenie czasu wykrycia I reakcji

Wymiar roli	Treść funkcji	Główni partnerzy instytucjonalni	Przykładowy efekt bezpieczeństwa
Ochronny	ochrona sieci, systemów I łączności Sił Zbrojnych RP	jednostki wojskowe, logistyka, dowodzenie	utrzymanie ciągłości działania wojska
Systemowy	współpraca cywilno-wojskowa, wsparcie infrastruktury krytycznej, wymiana informacji	administracja publiczna, sektor prywatny, operatorzy IK	ograniczenie skutków kampanii hybrydowych
Kadrowo-rozwojowy	edukacja, szkolenia, aktywna rezerwa, rozwój kompetencji	uczelnie, partnerzy technologiczni, program CYBER.MIL	zwiększenie podaży specjalistów I zdolności adaptacyjnych

Źródło: opracowanie własne na podstawie Ministerstwo Cyfryzacji, 2025, 2026; Ministerstwo Obrony Narodowej, 2022, b.d.; NATO, 2016, 2024; Jungwirth i in., 2023; Krasznay, 2024.

Znaczenie Wojsk Obrony Cyberprzestrzeni staje się jeszcze bardziej widoczne, gdy zestawi się je z dynamiką incydentów odnotowywanych w polskiej cyberprzestrzeni. Dane CERT Polska wskazują na bardzo wyraźny wzrost liczby obsłużonych incydentów w latach 2020-2024: od 10 420 w 2020 r., przez 29 483 w 2021 r., 39 683 w 2022 r. i 80 267 w 2023 r., aż do 103 449 w 2024 r. Oznacza to, że w ciągu czterech lat liczba incydentów wzrosła niemal dziesięciokrotnie. Tendencji tej nie należy interpretować wyłącznie w kategoriach ilościowych. Tak wysokie tempo wzrostu świadczy o nasilającej się presji wywieranej na państwo przez aktywność wrogą, przestępczą oraz haktywistyczną, a więc przez zjawiska charakterystyczne dla współczesnego środowiska zagrożeń hybrydowych. W tej perspektywie Wojska Obrony Cyberprzestrzeni powinny być oceniane nie tylko przez pryzmat ich bezpośrednich działań operacyjnych, lecz również przez pryzmat zdolności do odciążania i wzmacniania całej architektury bezpieczeństwa cyfrowego państwa. Na Rysunku 2 przedstawiono dynamikę liczby incydentów obsłużonych przez CERT Polska w latach 2020-2024, ukazującą wyraźną tendencję wzrostową w analizowanym okresie.



Rysunek 2. Dynamika liczby incydentów obsłużonych przez CERT Polska w latach 2020-2024

Źródło: opracowanie własne na podstawie CERT Polska, 2025; Ministerstwo Cyfryzacji, 2025.

Na szczególną uwagę zasługuje sytuacja sektora publicznego. Z danych CERT Polska wynika, że w 2024 r. CSIRT NASK obsłużył 3 450 incydentów w podmiotach publicznych, co oznacza wzrost o 58% w porównaniu z rokiem poprzednim, przy czym najwyższą liczbę odnotowano w administracji publicznej – 1 911 przypadków. Z perspektywy nauk o bezpieczeństwie ustalenie to ma istotne znaczenie, ponieważ wskazuje, że ciężar zagrożeń nie koncentruje się wyłącznie w sektorze finansowym czy komercyjnym, lecz w coraz większym stopniu dotyczy struktur odpowiedzialnych za ciągłość funkcjonowania państwa. W konsekwencji wzrasta znaczenie komponentu militarnego zdolnego zarówno do współpracy z administracją publiczną, jak i do ochrony własnych systemów dowodzenia, zwłaszcza w sytuacji, gdy presja wywierana na sektor publiczny może stanowić element przygotowania pola pod szerszą operację hybrydową (Gaie, Karpiuk, Spaziani, 2025; Gaie, Karpiuk, Strizzolo, 2025). Szczególnie wymowne pozostaje studium przypadku fałszywej depeszy dotyczącej mobilizacji, opublikowanej 31 maja 2024 r. w oficjalnym serwisie PAP. W raporcie o stanie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej wskazano wprost, że doszło do dwukrotnego zamieszczenia fałszywej depeszy odnoszącej się do mobilizacji w Polsce. Znaczenie tego incydentu wykracza poza klasycznie rozumianą kategorię naruszenia systemu informatycznego, ponieważ jego potencjalnym skutkiem mogło być wywołanie paniki

informacyjnej, podważenie zaufania do oficjalnych kanałów komunikacji oraz wygenerowanie wtórnych efektów psychologicznych. Przypadek ten stanowi modelowy przykład splotu warstwy cybernetycznej i informacyjnej, a więc dokładnie tego rodzaju zjawiska, wobec którego niewystarczające byłyby zarówno wyłącznie techniczne zdolności typu SOC, jak i samodzielnie funkcjonujący aparat komunikacji strategicznej. Właśnie w takich sytuacjach niezbędny jest podmiot zdolny do równoczesnego rozumienia militarnego, technicznego i strategicznego wymiaru ataku.

Dopełnieniem tego obrazu jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa z 2026 r. Wprowadza ona Połączone Centrum Operacyjne Cyberbezpieczeństwa jako organ pomocniczy Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, rozszerza kompetencje krajowych CSIRT-ów, umożliwia tworzenie sektorowych CSIRT-ów oraz ustanawia krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Z punktu widzenia roli Wojsk Obrony Cyberprzestrzeni jest to zmiana szczególnie istotna, ponieważ wzmacnia mechanizmy koordynacji pomiędzy elementami systemu i przesuwa debatę z poziomu pytania o to, kto odpowiada za cyberbezpieczeństwo, na poziom pytania o sposób integrowania zdolności resortowych, sektorowych i narodowych w jeden spójny system działania. W tym sensie można stwierdzić, że otoczenie instytucjonalne dojrzewa do logiki, w jakiej Wojska Obrony Cyberprzestrzeni zostały powołane.

Dyskusja

Przeprowadzona analiza prowadzi do wniosku, że rola Wojsk Obrony Cyberprzestrzeni jest wyraźnie szersza niż tradycyjnie rozumiana ochrona wojskowych sieci teleinformatycznych. W ujęciu funkcjonalnym WOC pełnią co najmniej trzy równoległe role: podmiotu odpowiedzialnego za ochronę wojskowej ciągłości działania, komponentu państwowego systemu reagowania na incydenty oraz narzędzia wzmacniania odporności strategicznej państwa. Ujęcie to pozostaje zgodne z sojuszniczym rozumieniem cyberobrony, w którym cyberprzestrzeń traktowana jest jako domena operacyjna, a odpowiedź na zagrożenia powinna integrować poziomy polityczny, wojskowy i techniczny. Oznacza to, że w warunkach zagrożeń hybrydowych WOC nie powinny być sytuowane na obrzeżach państwowego systemu bezpieczeństwa, lecz w jego centrum, jako komponent integrujący wojskowe i pozawojskowe wektory odporności (NATO, 2024).

Jednocześnie materiał empiryczny wskazuje, że sama specjalizacja wojskowa nie jest wystarczająca. Współczesne cyberoperacje często dotyczą infrastruktury i usług, które formalnie pozostają poza resortem obrony, lecz mają zasadnicze znaczenie zarówno dla bezpieczeństwa państwa, jak i dla sprawności sił zbrojnych. Krasznay trafnie zauważa, że ochrona infrastruktury krytycznej bardzo często wymaga ścisłej koordynacji z cywilnymi dostawcami usług bezpieczeństwa oraz z sektorem prywatnym. Analogiczny kierunek wzmacnia dyrektywa NIS2, która rozszerza ramy ochrony na osiemnaście sektorów krytycznych i nakłada na państwa obowiązek budowy strategii, zdolności oraz mechanizmów współpracy i raportowania. W przypadku Polski oznacza to, że WOC muszą funkcjonować w środowisku gęstej sieci relacji z krajowymi CSIRT-ami, sektorowymi CSIRT-ami, administracją publiczną, operatorami usług kluczowych oraz partnerami prywatnymi. Im silniejsze są te relacje, tym większa jest skuteczność WOC, im słabsze, tym większe staje się ryzyko, że formacja pozostanie wprawdzie bardzo sprawna technicznie, lecz operacyjnie odizolowana (Krasznay, 2024).

Drugim istotnym problemem pozostają zasób kadrowy oraz transfer kompetencji. Program CYBER.MIL 2.0 już w 2022 r. eksponował rekrutację i aktywną rezerwę jako jeden z pięciu filarów rozwoju, co należy interpretować jako pośrednie przyznanie, że zdolności cybernetyczne nie mogą być budowane wyłącznie w klasycznej logice etatowej i koszarowej. Wysoko wykwalifikowani specjaliści funkcjonują bowiem na rynku cywilnym, w ośrodkach badawczych, firmach technologicznych i organizacjach eksperckich, a wojskowy komponent cyberbezpieczeństwa musi być zdolny do przyciągania, czasowego angażowania i utrzymywania tego zasobu. Z tej perspektywy WOC są nie tylko formacją operacyjną, lecz również platformą organizacyjną służącą łączeniu środowiska wojskowego, technologicznego i naukowego. W przeciwnym razie nawet najlepiej zaprojektowana struktura prawna nie przełoży się na rzeczywistą zdolność działania w warunkach gwałtownej ewolucji zagrożeń.

Trzecia kwestia dotyczy prawno-strategicznej logiki działań prowadzonych poniżej progu wojny. Definicje zagrożeń hybrydowych eksponują ich niejednoznaczność, trudność atrybucji oraz celowe utrzymywanie się poniżej progu, który wywoływałby jednoznaczną reakcję zbrojną. To właśnie sprawia, że WOC muszą działać w przestrzeni szczególnie wymagającej:

wystarczająco stanowczo, aby chronić państwo, a jednocześnie w zgodzie z krajowymi i międzynarodowymi ograniczeniami użycia siły oraz w ścisłej współpracy z władzami cywilnymi. NATO dopuszcza, że skumulowany efekt istotnych złośliwych działań cybernetycznych może w określonych okolicznościach zostać uznany za zbrojną napaść, jednak każdorazowo ocena ta ma charakter polityczno-strategiczny. Z perspektywy polskiej oznacza to potrzebę dalszego rozwijania doktryn, procedur decyzyjnych oraz zasad współdziałania WOC z innymi instytucjami państwa w sytuacjach niejednoznacznych, typowych dla presji hybrydowej (Dziwisz, 2024; NATO, 2024).

Czwarty wątek ma charakter rozwojowy i odnosi się do państwowej suwerenności technologicznej. Strategia Cyberbezpieczeństwa RP z 2026 r. akcentuje rozwój krajowej kryptografii, migrację do kryptografii postkwantowej, bezpieczeństwo łańcucha dostaw oraz rozwój rodzimych technologii. Z punktu widzenia WOC jest to zmiana o znaczeniu fundamentalnym. Formacja ta nie może być bowiem oceniana wyłącznie przez pryzmat bieżącego reagowania na incydenty, lecz również jako uczestniczka długofalowej polityki budowy narodowych kompetencji technologicznych. W warunkach rywalizacji geopolitycznej zależność od zewnętrznych rozwiązań, nieprzejrzystych łańcuchów dostaw czy obcych standardów kryptograficznych może sama w sobie stać się źródłem podatności. W tym sensie rozwój WOC oznacza jednocześnie rozwój wojskowych zdolności operacyjnych oraz wzmacnianie państwowej autonomii technologicznej.

Wyniki badania pozwalają zatem uznać hipotezę roboczą za potwierdzoną. O skuteczności WOC nie decyduje wyłącznie poziom militarnej specjalizacji ani liczba jednostek organizacyjnych, lecz zdolność do działania w logice sieciowej, obejmującej współpracę z administracją, krajowymi i sektorowymi CSIRT-ami, operatorami infrastruktury krytycznej, partnerami technologicznymi oraz strukturami sojuszniczymi. Innymi słowy, WOC są najskuteczniejsze wtedy, gdy pozostają jednocześnie formacją wojskową i instytucją systemową.

Wnioski

Przeprowadzona analiza prowadzi do kilku podstawowych wniosków. Wojska Obrony Cyberprzestrzeni należy traktować jako trwały i konieczny element systemu bezpieczeństwa państwa, a nie jedynie wyspecjalizowaną

strukturę ochrony teleinformatycznej resortu obrony. Ich rola ma charakter wielopoziomowy i obejmuje zarówno obronę infrastruktury wojskowej, wsparcie krajowego reagowania na incydenty, udział w budowie odporności państwa, jak i wzmacnianie odstraszania. Dynamika incydentów odnotowywanych w latach 2020-2024 dowodzi, że zagrożenia wobec Polski mają charakter systemowy i ciągły, co uzasadnia dalsze wzmacnianie wyspecjalizowanych zdolności wojskowych w cyberprzestrzeni. Przypadki takie jak fałszywa depesza PAP pokazują ponadto, że współczesne ataki coraz częściej łączą wymiar cybernetyczny i informacyjny, a skuteczna odpowiedź wymaga integracji zasobów militarnych, technicznych i komunikacyjnych. Przyszła skuteczność Wojsk Obrony Cyberprzestrzeni będzie natomiast zależała od jakości współpracy cywilno-wojskowej, rozwoju kadr, budowy krajowych technologii oraz efektywnego włączenia formacji w rozwijającą się architekturę krajowego systemu cyberbezpieczeństwa i Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (Kancelaria Sejmu, 2018; Rada Ministrów, 2026; Ministerstwo Cyfryzacji, 2026)

Z perspektywy praktycznej oznacza to potrzebę dalszego rozwoju wspólnych ćwiczeń z administracją publiczną i operatorami usług kluczowych, doprecyzowania zasad wymiany informacji między komponentami wojskowym i cywilnym, budowy mechanizmów szybkiego pozyskiwania kompetencji eksperckich oraz wdrożenia mierników oceny skuteczności WOC, wykraczających poza prostą statystykę incydentów. W naukach o bezpieczeństwie rozdział wzmacnia tezę, że cyberbezpieczeństwo państwa w epoce zagrożeń hybrydowych nie jest sumą odrębnych działań technicznych, lecz rezultatem zdolności do organizacyjnego integrowania narzędzi wojskowych, administracyjnych, prawnych i społecznych. To właśnie w tej przestrzeni Wojska Obrony Cyberprzestrzeni odgrywają rolę strategicznie pierwszoplanową.

Literatura

1. Bachmann, S.-D. D., Putter, D., Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy, 14*(5), 858-869. https://doi.org/10.1111/1758-5899.13257
2. Brill, A., Bennett, J. (2022). Understanding hybrid warfare in cyberspace: Building resilience through understanding. W: *Building cyber*

resilience against hybrid threats. *NATO Science for Peace and Security Series D: Information and Communication Security*. IOS Press. https://doi.org/10.3233/NICSP220016

3. CERT Polska. (2025). *Annual report 2024*. NASK – Państwowy Instytut Badawczy.
4. CSIRT GOV. (2025). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*. Agencja Bezpieczeństwa Wewnętrznego.
5. Dziwisz, D. (2024). Rethinking future conflicts: The cyber grey zone from the Russian perspective. *Politeja, 21*(5), 281-309. https://doi.org/10.12797/Politeja.21.2024.92.13
6. Gaie, C., Karpiuk, M., Spaziani, A. (2025). Cybersecurity in France, Poland and Italy. *Studia Iuridica Lublinensia, 34*(1), 73-95. https://doi.org/10.17951/sil.2025.34.1.73-95
7. Gaie, C., Karpiuk, M., Strizzolo, N. (2025). Cybersecurity of public sector institutions. *Prawo i Więź, 53*(6), 347-362. https://doi.org/10.36128/PRIW.VI53.1129
8. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
9. Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., Giannopoulos, G. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. Publications Office of the European Union. https://doi.org/10.2760/37899
10. Kancelaria Sejmu. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1560 z późn. zm.)
11. Krasznay, C. (2024). The role of civilian cybersecurity companies in military cyber operations. *Land Forces Academy Review, 29*(1), 1-10. https://doi.org/10.2478/raft-2024-0001
12. Kuś, B. (2023). Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo: Zagadnienia organizacyjno-prawne. *Cybersecurity and Law, 10*(2), 32-50. https://doi.org/10.35467/cal/174908
13. Ministerstwo Cyfryzacji. (2025). *Krajobraz cyberprzestrzeni: Roczne sprawozdanie o cyberbezpieczeństwie*. Pobrane z: https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie (dostęp: 12.02.2026).

14. Ministerstwo Cyfryzacji. (2026). *Nowa strategia cyberbezpieczeństwa: Polska wzmacnia ochronę przed cyberatakami*. Pobrane z: https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami (dostęp: 12.02.2026).
15. Ministerstwo Obrony Narodowej. (2022). *Wojska Obrony Cyberprzestrzeni rozpoczynają działalność*. Pobrane z: https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc (dostęp: 12.02.2026).
16. Ministerstwo Obrony Narodowej. (b.d.). *Wojska Obrony Cyberprzestrzeni*. Pobrane z: https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni (dostęp: 12.02.2026).
17. NATO. (2016). *Warsaw Summit Communiqué. North Atlantic Treaty Organization*. Pobrane z: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique (dostęp: 12.02.2026).
18. NATO. (2024). *Cyber defence. North Atlantic Treaty Organization*. Pobrane z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (dostęp: 12.02.2026).
19. Rada Ministrów. (2026). *Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Monitor Polski, poz. 309. Pobrane z: https://monitorpolski.gov.pl/MP/2026/309 (dostęp: 12.02.2026).
20. Rada Unii Europejskiej. (2026). *Hybrid threats*. Pobrane z: https://www.consilium.europa.eu/en/policies/hybrid-threats/ (dostęp: 12.02.2026).
21. Schulze, M. (2020). Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. W: *2020 12th International Conference on Cyber Conflict* (s. 183-197). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon49761.2020.9131733
22. Wróblewski, W., Wiśniewski, M. (2024). Cybersecurity in the context of hybrid warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. *Central European Journal of Security Studies, 1*(1), 48-60. https://doi.org/10.15804/CEJSS.2023105

Marta Chodyka[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_23

MODEL ZARZĄDZANIA INCYDENTEM CYBERBEZPIECZEŃSTWA W ADMINISTRACJI ODPOWIEDZIALNEJ ZA OCHRONĘ GRANIC

A MODEL FOR MANAGING CYBERSECURITY INCIDENTS IN THE ADMINISTRATION RESPONSIBLE FOR BORDER PROTECTION

Streszczenie

Rozdział przedstawia model zarządzania incydentem cyberbezpieczeństwa w administracji odpowiedzialnej za ochronę granic. Punktem wyjścia jest założenie, że incydent w systemach granicznych nie jest wyłącznie zdarzeniem technicznym, lecz zdarzeniem wpływającym na ciągłość funkcji państwa: identyfikację osób, kontrolę przepływów, wymianę danych, komunikację kryzysową oraz zaufanie do decyzji administracyjnych. Problem badawczy dotyczy sposobu ujęcia procesu obsługi incydentu tak, aby obejmował jednocześnie wymiar techniczny, operacyjny, prawny i komunikacyjny. Celem opracowania jest zaproponowanie modelu interpretacyjno-aplikacyjnego, który łączy fazy reagowania na incydent z wymaganiami

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl

cyberodporności i ciągłości działania. Zastosowano analizę dokumentów prawnych, standardów i literatury oraz modelowanie koncepcyjne oparte na scenariuszu referencyjnym. Wyniki wskazują, że skuteczność reakcji zależy od jasnych progów eskalacji, wspólnego obrazu sytuacji, integracji ról, zdolności do pracy w stanie kontrolowanej degradacji oraz wykorzystania wniosków po incydencie do wzrostu dojrzałości organizacyjnej.

Słowa kluczowe: incydent cyberbezpieczeństwa, zarządzanie incydentem, administracja publiczna, ochrona granic, cyberodporność, ciągłość działania

Abstract

The chapter presents a model for managing a cybersecurity incident in public administration responsible for border protection. It assumes that an incident in border-management systems is not merely a technical event, but one that affects the continuity of state functions: identity verification, control of flows, data exchange, crisis communication, and trust in administrative decisions. The research problem concerns how to frame incident handling to cover the technical, operational, legal, and communication dimensions simultaneously. The aim of the study is to propose an interpretative and application-oriented model that integrates incident response phases with the requirements of cyber resilience and business continuity. The study applies legal document analysis, standards and literature review, and conceptual model design based on a reference scenario. The findings indicate that an effective response depends on clear escalation thresholds, a common operational picture, role integration, the ability to operate in a controlled-degraded mode, and the use of post-incident lessons to increase organisational maturity.

Keywords: cybersecurity incident, incident management, public administration, border protection, cyber resilience, business continuity

Wstęp

Administracja odpowiedzialna za ochronę granic funkcjonuje w środowisku, w którym incydent cyberbezpieczeństwa może szybko uzyskać znaczenie wykraczające poza obszar teleinformatyczny. Zakłócenie systemu odpraw, bazy danych, kanału łączności, systemu identyfikacji albo komunikacji publicznej może wpływać na zdolność państwa do wykonywania funkcji granicznej. W tym sensie incydent nie jest jedynie problemem administratora systemu, lecz zdarzeniem administracyjnym i operacyjnym, które wymaga decyzji kierowniczych, prawnych, organizacyjnych i komunikacyjnych. Podstawowy kontekst instytucjonalny wyznaczają przepisy

krajowego systemu cyberbezpieczeństwa oraz regulacje unijne dotyczące zarządzania ryzykiem, raportowania incydentów i współpracy między podmiotami (Kancelaria Sejmu, 2018). Dyrektywa NIS 2 wzmacnia podejście oparte na zarządzaniu ryzykiem, odpowiedzialności kierownictwa, ciągłości działania i współpracy transgranicznej (Dyrektywa (UE) 2022/2555, 2022). W administracji granicznej wymagania te powinny być interpretowane przez pryzmat funkcji publicznej, ponieważ skutki incydentu mogą dotyczyć nie tylko dostępności systemu, ale także legalności decyzji, integralności danych, bezpieczeństwa personelu i zaufania do instytucji.

Problem badawczy opracowania można sformułować następująco: jaki model zarządzania incydentem cyberbezpieczeństwa odpowiada potrzebom administracji odpowiedzialnej za ochronę granic, jeżeli incydent wpływa jednocześnie na systemy teleinformatyczne, procesy operacyjne, przepływ informacji, komunikację i ciągłość funkcji państwa? Problem ten ma charakter teoretyczno-aplikacyjny. Teoretycznie dotyczy relacji między cyberbezpieczeństwem, cyberodpornością, zarządzaniem kryzysowym i bezpieczeństwem państwa (Kitler, 2011; Wiśniewski, 2013). Aplikacyjnie wymaga określenia ról, progów eskalacji, przepływów informacji, trybów pracy awaryjnej i mechanizmów uczenia się po incydencie. Celem naukowym jest opracowanie modelu zarządzania incydentem, który łączy klasyczne fazy obsługi incydentu z wymaganiami administracji publicznej i specyfiką systemów granicznych. Celem szczegółowym jest wskazanie, jak w jednym modelu powiązać detekcję techniczną, kwalifikację wpływu na funkcję graniczną, decyzję o eskalacji, utrzymanie procesu w stanie ograniczonej sprawności, odtworzenie usług i analizę po incydencie. Celem praktycznym jest zaproponowanie ram, które mogą zostać wykorzystane przy tworzeniu planów reagowania, playbooków, ćwiczeń, audytów i szkoleń. Metodologia ma charakter jakościowy i diagnostyczno-projektowy. Wykorzystano analizę dokumentów prawnych, standardów i literatury, a następnie modelowanie koncepcyjne. Analiza dokumentów jest zasadna, ponieważ badany problem obejmuje źródła o różnym statusie: akty prawne, standardy, raporty instytucjonalne, publikacje naukowe i opracowania metodyczne (Bowen, 2009; Mayring, 2000). Modelowanie pozwala przekształcić wymagania formalne i ustalenia literatury w uporządkowaną procedurę zarządzania incydentem. W badaniu przyjęto także scenariusz referencyjny: zakłócenie dostępności

systemu wspierającego odprawę, połączone z fałszywą informacją o zamknięciu przejścia oraz koniecznością pracy w trybie awaryjnym. Taki scenariusz łączy wymiar techniczny, operacyjny, prawny i komunikacyjny. Dobór źródeł podporządkowano trzem kryteriom. Uwzględniono literaturę z zakresu bezpieczeństwa państwa i funkcjonowania instytucji publicznych (Żurawski i in., 2025). Wykorzystano standardy dotyczące reagowania na incydenty, cyberodporności i ciągłości działania (Nelson i in., 2025). Dodatkowo włączono publikacje dotyczące bezpieczeństwa danych, zarządzania incydentami, systemów bezpieczeństwa w organizacjach publicznych oraz sprawności działania w warunkach kryzysowych (Chodyka, 2025; Wołejszo i in., 2021; Żurawski i in., 2025).

Incydent cyberbezpieczeństwa jako zdarzenie administracyjne i operacyjne

W klasycznym ujęciu cyberbezpieczeństwa ochronę informacji opisuje się przez pryzmat poufności, integralności i dostępności. W systemach granicznych znaczenie tych kategorii należy interpretować w związku z funkcją publiczną. Naruszenie poufności może oznaczać ujawnienie danych osobowych, dokumentowych lub biometrycznych. Naruszenie integralności może prowadzić do decyzji podjętych na podstawie danych błędnych, niepełnych albo zmanipulowanych (Chodyka, Dalba-Gołaszewska, 2025). Naruszenie dostępności może skutkować opóźnieniem odprawy, wzrostem kolejek, koniecznością pracy manualnej i zwiększeniem ryzyka błędu operacyjnego (Ciekanowski, Wojciechowska-Filipek, 2019).

Incydent cyberbezpieczeństwa w administracji granicznej powinien być zatem kwalifikowany nie tylko według typu technicznego, ale przede wszystkim według wpływu na funkcję graniczną. Ten sam problem techniczny może mieć różne skutki w zależności od natężenia ruchu, miejsca wystąpienia, dostępności procedur zastępczych, znaczenia przetwarzanych danych oraz stopnia zależności od systemów zewnętrznych. Krótkotrwała niedostępność aplikacji pomocniczej może pozostać zdarzeniem technicznym, natomiast krótkotrwała niedostępność systemu referencyjnego w godzinach szczytu może wymagać decyzji operacyjnej i komunikacyjnej. NIST SP 800-61 Rev. 3 ujmuje reagowanie na incydenty jako element szerszego zarządzania ryzykiem cyberbezpieczeństwa i wiąże je z funkcjami NIST

Cybersecurity Framework 2.0 (Nelson i in., 2025; NIST, 2024). To przesunięcie jest istotne dla administracji publicznej, ponieważ obsługa incydentu nie może być izolowana od zarządzania ryzykiem, odpowiedzialności kierownictwa, komunikacji i odtwarzania funkcji. Z perspektywy systemów granicznych szczególne znaczenie ma powiązanie reagowania i odtwarzania z funkcją zarządzania, ponieważ bez jasnych ról decyzyjnych można przywrócić komponent techniczny, ale nie odtworzyć procesu operacyjnego.

Incydent w systemie granicznym ma co najmniej cztery wymiary. Wymiar techniczny dotyczy systemów, sieci, kont, logów, konfiguracji, danych i dostępności usług. Wymiar operacyjny obejmuje odprawę, kontrolę, kolejki, bezpieczeństwo personelu i decyzje o trybie pracy. Wymiar prawny dotyczy ochrony danych, zabezpieczenia dowodów, obowiązków raportowych i zgodności działań z procedurami. Wymiar komunikacyjny obejmuje informowanie personelu, podróżnych, partnerów instytucjonalnych oraz reagowanie na dezinformację (Ciekanowski i in., 2025). Dopiero łączna ocena tych wymiarów pozwala ustalić rzeczywisty poziom incydentu. Z tego względu zasadne jest wyróżnienie kilku poziomów wpływu. Poziom monitorowania obejmuje zdarzenia techniczne bez istotnego wpływu na funkcję graniczną. Poziom operacyjny dotyczy zdarzeń ograniczających sprawność procesu, na przykład wydłużających odprawę lub wymagających pracy w trybie zastępczym. Poziom prawny pojawia się wtedy, gdy istnieje podejrzenie naruszenia danych lub konieczność zabezpieczenia materiału dowodowego. Poziom informacyjny dotyczy sytuacji, w których incydentowi towarzyszy dezinformacja, presja medialna albo rozbieżność komunikatów. Poziom krytyczny występuje wtedy, gdy zakłócona zostaje podstawowa zdolność realizacji funkcji granicznej. Takie ujęcie jest spójne z prakseologicznym rozumieniem sprawności działania w organizacjach odpowiedzialnych za bezpieczeństwo. W warunkach kryzysu istotne jest nie tylko posiadanie zasobów, lecz także zdolność ich skoordynowanego użycia, utrzymania kontroli nad procesem i podejmowania decyzji przy niepełnej informacji (Wołejszo, Feltynowski, 2023; Wołejszo i in., 2021). W administracji granicznej oznacza to konieczność projektowania reakcji nie jako sekwencji czynności technicznych, lecz jako procesu dowodzenia, koordynacji i utrzymania funkcji publicznej.

Model zarządzania incydentem w administracji odpowiedzialnej za ochronę granic

Proponowany model ma charakter fazowy i funkcjonalny. Fazy porządkują przebieg reakcji, natomiast funkcjonalność modelu wynika z odniesienia każdej fazy do utrzymania zadania publicznego. Model obejmuje osiem faz: przygotowanie, wykrycie, kwalifikację, eskalację, ograniczenie skutków, utrzymanie funkcji, odtwarzanie oraz uczenie się. Fazy te nie zawsze występują liniowo. W praktyce część działań może przebiegać równolegle, szczególnie wtedy, gdy zespół techniczny izoluje incydent, pion operacyjny uruchamia tryb ograniczony, a komórka komunikacyjna przygotowuje komunikat etapowy. Przygotowanie obejmuje wskazanie ról, list kontaktowych, kanałów zapasowych, playbooków, procedur pracy awaryjnej, zasad komunikacji i scenariuszy ćwiczeń. Bez tej fazy pozostałe etapy stają się improwizacją. Wykrycie powinno obejmować zarówno sygnały techniczne, jak i sygnały operacyjne z terenu. Alert z systemu monitoringu ma inne znaczenie, jeżeli równocześnie rośnie kolejka, pojawia się niespójność danych albo w przestrzeni informacyjnej rozpowszechniany jest fałszywy komunikat. Kwalifikacja polega na ocenie wpływu zdarzenia na funkcję graniczną. Nie wystarcza ustalenie, czy wystąpił atak, awaria lub błąd konfiguracji. Konieczne jest ustalenie, czy zdarzenie wpływa na identyfikację osób, weryfikację dokumentów, wymianę informacji, dostępność danych referencyjnych, bezpieczeństwo personelu, ochronę danych albo komunikację publiczną. Eskalacja powinna wynikać z wcześniej ustalonych progów, a nie z uznaniowej oceny pojedynczej osoby. Progi mogą dotyczyć czasu niedostępności, liczby dotkniętych stanowisk, podejrzenia naruszenia danych, konieczności przejścia na tryb manualny, ryzyka dezinformacji albo potrzeby powiadomienia CSIRT i kierownictwa.

Ograniczenie skutków obejmuje działania techniczne i organizacyjne. Do działań technicznych należą między innymi izolacja segmentu, blokada kont, zabezpieczenie logów, przełączenie usług i ograniczenie propagacji zakłócenia. Do działań organizacyjnych należy zmiana organizacji ruchu, uruchomienie procedury manualnej, wzmocnienie obsady, przekazanie instrukcji personelowi, przygotowanie komunikatu oraz ustalenie zasad dokumentowania decyzji. Faza utrzymania funkcji jest szczególnie ważna z perspektywy cyberodporności. Celem nie jest natychmiastowy powrót do

pełnej automatyzacji, lecz bezpieczne utrzymanie minimalnej funkcji na akceptowalnym poziomie (ISO, 2019). Odtwarzanie obejmuje przywrócenie usług, weryfikację integralności danych, synchronizację rekordów powstałych w trybie awaryjnym, analizę logów, potwierdzenie bezpieczeństwa środowiska i decyzję o powrocie do normalnego trybu pracy. Działania po incydencie powinny obejmować raport, przegląd decyzji, identyfikację luk, aktualizację procedur, korektę konfiguracji, wnioski szkoleniowe oraz ocenę relacji z dostawcami. NIST SP 800-184 podkreśla, że odzyskiwanie po zdarzeniu wymaga nie tylko odtworzenia usług, lecz także walidacji i komunikacji (Bartock i in., 2016). Fazy modelu przedstawiono w Tabeli 1. Model wymaga również jednoznacznego przypisania ról. Rola techniczna odpowiada za analizę systemów, logów, konfiguracji i zabezpieczeń. Rola operacyjna odpowiada za wpływ incydentu na odprawę, decyzje w terenie i organizację pracy. Rola prawna odpowiada za ochronę danych, obowiązki raportowe, zabezpieczenie dowodów i zgodność działań. Rola komunikacyjna odpowiada za przekaz do personelu, podróżnych, mediów i partnerów. Rola kierownicza odpowiada za priorytety, akceptację ryzyka resztkowego, przejście między trybami pracy i decyzję o powrocie do normalnego działania. Przepływ informacji powinien być dwukierunkowy. Zespół techniczny przekazuje informacje o naturze zdarzenia, ale pion operacyjny informuje o rzeczywistym wpływie na proces graniczny. Komunikacja publiczna raportuje sygnały z otoczenia informacyjnego, a prawnicy określają ograniczenia publikacji, raportowania i przetwarzania danych. Bez takiego przepływu decyzje mogą być podejmowane na podstawie niepełnego obrazu sytuacji. Dlatego model powinien opierać się na jednej karcie incydentu, aktualizowanej w czasie i obejmującej status techniczny, wpływ operacyjny, decyzje, komunikaty, ryzyka prawne i kolejne kroki.

Progi eskalacji i tryby pracy są elementami łączącymi model z praktyką. Tryb normalny oznacza pełną funkcjonalność systemów. Tryb podwyższonej czujności oznacza zwiększony monitoring i gotowość zespołów. Tryb degradacji kontrolowanej oznacza ograniczenie automatyzacji i uruchomienie procedur zastępczych przy zachowaniu rozliczalności decyzji. Tryb krytyczny oznacza minimalny zakres funkcji oraz priorytet bezpieczeństwa osób, danych i procesu. Takie tryby powinny być opisane przed incydentem, ponieważ w warunkach presji czasu trudniej uzgadniać kryteria działania.

Tabela 1. Fazy modelu zarządzania incydentem cyberbezpieczeństwa w administracji granicznej

Faza	Cel	Decyzja kluczowa	Dowód wykonania
Przygotowanie	zapewnienie gotowości ról, procedur, kanałów i playbooków	zatwierdzenie planu reagowania i trybów pracy	aktualny plan, lista kontaktowa, scenariusze ćwiczeń
Wykrycie	rozpoznanie anomalii technicznej lub operacyjnej	czy zdarzenie wymaga kwalifikacji jako incydent	alert, zgłoszenie, zapis w rejestrze zdarzeń
Kwalifikacja	ocena wpływu na funkcję graniczną i dane	poziom incydentu i zakres oddziaływania	wstępny obraz sytuacji, ocena skutków
Eskalacja	uruchomienie właściwych ról i podmiotów	kogo powiadomić i kto podejmuje decyzję	lista powiadomień, decyzja kierownicza
Ograniczenie skutków	zatrzymanie propagacji zakłócenia i zabezpieczenie dowodów	co izolować, co utrzymać, co wyłączyć	logi, decyzje techniczne, zapis działań
Utrzymanie funkcji	zapewnienie minimalnej zdolności odprawy i komunikacji	tryb degradacji kontrolowanej albo tryb krytyczny	karta incydentu, instrukcje dla personelu
Odtwarzanie	przywrócenie usług i integralności procesu	czy system może wrócić do pracy normalnej	raport odtworzeniowy, walidacja danych
Uczenie się	zwiększenie dojrzałości organizacyjnej po zdarzeniu	jakie procedury, umowy i szkolenia zmienić	raport poincydentowy, plan działań korygujących

Źródło: opracowanie własne.

Znaczenie progów eskalacji wzmacniają regulacje unijne dotyczące poważnych zagrożeń i incydentów. Akt w sprawie cybersolidarności rozwija unijne podejście do wykrywania, przygotowania i reagowania na zagrożenia cybernetyczne i incydenty, co potwierdza, że zarządzanie incydentem nie jest wyłącznie sprawą wewnętrzną pojedynczej jednostki (Rozporządzenie (UE) 2025/38, 2025). W systemach granicznych ma to szczególne znaczenie, ponieważ zakłócenie lokalne może wpływać na współpracę z partnerami, wymianę danych i zaufanie do procesu transgranicznego.

Wyniki analizy i zastosowanie modelu

Przeprowadzona analiza prowadzi do pięciu zasadniczych wyników. Po pierwsze, zarządzanie incydentem w administracji granicznej wymaga połączenia modelu technicznego i modelu misji. Samo przywrócenie aplikacji, serwera lub łączności nie oznacza jeszcze przywrócenia funkcji granicznej.

Konieczne jest odtworzenie danych, kolejki operacyjnej, komunikacji, ścieżki audytu i zdolności do uzasadnienia decyzji podjętych w czasie zakłócenia. Po drugie, skuteczna reakcja wymaga wspólnego obrazu sytuacji. W incydencie granicznym informacje pochodzą z wielu źródeł: logów, stanowisk odpraw, zgłoszeń personelu, komunikacji publicznej, dostawców, partnerów zewnętrznych i mediów. Jeżeli każda komórka organizacyjna posiada własną wersję zdarzenia, rośnie ryzyko opóźnienia, sprzecznych decyzji i niespójnych komunikatów. Ćwiczenia Cyber Europe wskazują, że koordynacja i wspólny obraz sytuacji są kluczowe dla gotowości i odporności cyberbezpieczeństwa (ENISA, 2024). Po trzecie, centralnym elementem modelu jest praca w stanie degradacji kontrolowanej. Cyberodporność nie polega na założeniu, że wszystkie systemy będą zawsze dostępne. Polega na tym, że instytucja wie, które funkcje utrzymać, jakie dane są minimalnie niezbędne, kiedy przejść na tryb manualny lub częściowo manualny, jak dokumentować decyzje i jak później zsynchronizować zaległe dane. W tym sensie odporność jest zdolnością operacyjną, a nie wyłącznie stanem infrastruktury. Po czwarte, szczególnego znaczenia nabiera integralność danych i rozliczalność procesu. Decyzja podjęta na podstawie danych błędnych, niepełnych lub niespójnych może być formalnie zgodna z procedurą, a jednocześnie wadliwa z punktu widzenia funkcji bezpieczeństwa. Dlatego plan reagowania powinien obejmować walidację danych, zabezpieczenie logów, odtworzenie ścieżki decyzji, kontrolę wpisów dokonanych w trybie offline i mechanizmy ponownej weryfikacji spraw po przywróceniu systemu. Po piąte, działania po incydencie powinny prowadzić do wzrostu dojrzałości organizacyjnej. Raport poincydentowy nie może być wyłącznie dokumentem zamykającym sprawę. Powinien wskazywać, które decyzje były spóźnione, jakie dane były niedostępne, które role były niejasne, jakie umowy z dostawcami wymagają doprecyzowania i które scenariusze ćwiczeń należy zmienić. Badania nad skutecznością systemów zarządzania incydentami bezpieczeństwa informacji wskazują, że efektywność reakcji zależy nie tylko od technologii, lecz także od automatyzacji, kompetencji, skrócenia czasu detekcji i reakcji oraz integracji zarządzania incydentami ze strategią bezpieczeństwa.

Model może być zastosowany w planach reagowania na incydenty. Plan powinien obejmować role, listę kontaktową, progi eskalacji, tryby pracy, zasady komunikacji wewnętrznej i zewnętrznej, procedury zabezpieczenia

dowodów, kryteria przejścia na tryb awaryjny oraz kryteria powrotu do normalnego działania. Nie powinien być dokumentem wyłącznie formalnym. Jego użyteczność zależy od tego, czy może zostać wykorzystany w pierwszych minutach incydentu, kiedy informacje są niepełne, a presja operacyjna rośnie. Drugim zastosowaniem są playbooki scenariuszowe. W administracji granicznej powinny one obejmować co najmniej niedostępność systemu odpraw, podejrzenie naruszenia danych, niespójność danych referencyjnych, fałszywy komunikat w mediach społecznościowych, awarię dostawcy oraz konieczność pracy w trybie manualnym. Każdy playbook powinien wskazywać pierwsze działania, role, kanały komunikacji, decyzje progowe, minimalne dane, zasady dokumentowania i kryteria zakończenia. Trzecim zastosowaniem są ćwiczenia. Ćwiczenie typu tabletop pozwala sprawdzić role, decyzje i progi eskalacji. Ćwiczenie techniczne pozwala sprawdzić logi, kopie, izolację i odtwarzanie. Ćwiczenie zintegrowane łączy oba wymiary i jest najbardziej użyteczne, ponieważ ujawnia problemy na styku zespołów. Scenariusz nie powinien ograniczać się do ogólnego hasła o cyberataku. Powinien opisywać sekwencję zdarzeń: opóźnienia w odprawie, alert z monitoringu, zgłoszenia funkcjonariuszy, fałszywy komunikat, pytania mediów, decyzję o trybie manualnym i synchronizację danych po odtworzeniu systemu. Czwartym zastosowaniem jest audyt dojrzałości. Instytucja może ocenić, czy posiada aktualne playbooki, czy zna zależności od dostawców, czy ma kanały zapasowe, czy personel zna procedurę zgłoszenia, czy potrafi odtworzyć dane po pracy offline i czy wyniki ćwiczeń prowadzą do korekty planów. Badania dotyczące systemów zarządzania bezpieczeństwem w organizacjach publicznych wskazują, że wyższa dojrzałość systemu zarządzania wiąże się z lepszą zdolnością reagowania i większą odpornością organizacyjną (Chodyka i in., 2026). Piątym zastosowaniem są szkolenia i komunikacja wewnętrzna. Personel operacyjny powinien wiedzieć, jak rozpoznać objawy incydentu, kiedy eskalować problem, jak pracować w trybie ograniczonym i jak dokumentować decyzje. Personel techniczny powinien rozumieć skutki operacyjne swoich działań, na przykład izolacji komponentu lub wyłączenia usługi. Kierownictwo powinno być przygotowane do podejmowania decyzji przy niepełnej informacji. Komórka komunikacyjna powinna dysponować komunikatami etapowymi, które informują o ograniczeniach, nie ujawniają szczegółów wrażliwych i ograniczają ryzyko dezinformacji.

Szóstym zastosowaniem jest zarządzanie relacjami z dostawcami. Umowy powinny określać czasy reakcji, tryb wsparcia podczas incydentu, obowiązek informowania o podatnościach, dostęp do logów, udział w ćwiczeniach, procedury odtworzeniowe i zasady współpracy w sytuacji awaryjnej. W systemach granicznych dostawca nie jest wyłącznie podmiotem serwisowym. W czasie incydentu staje się elementem łańcucha reakcji i może wpływać na zdolność utrzymania funkcji publicznej. Znaczenie bezpieczeństwa infrastruktury krytycznej i zależności międzysektorowych potwierdzają także analizy dotyczące zarządzania bezpieczeństwem w warunkach rosnących cyberzagrożeń (Chodyka i in., 2025).

Model może być wdrażany przez minimalny pakiet operacyjny obejmujący kartę incydentu, matrycę eskalacji, listę kontaktową, playbooki scenariuszowe i formularz wniosków po incydencie. Dokumenty te powinny być krótkie, aktualne, dostępne offline i testowane w ćwiczeniach. Ich celem nie jest zwiększenie biurokracji, lecz zapewnienie podstawy do szybkiej, rozliczalnej i skoordynowanej decyzji. Ocena modelu powinna obejmować zarówno metryki ilościowe, jak i jakościowe. Użyteczne są wskaźniki czasu wykrycia, czasu kwalifikacji, czasu eskalacji, czasu przejścia na tryb awaryjny, czasu odtworzenia funkcji oraz liczby decyzji wymagających korekty. Nie powinny one jednak zastępować oceny jakości decyzji. Szybkość reakcji nie zawsze oznacza adekwatność. Decyzja powinna być terminowa, udokumentowana, proporcjonalna, zgodna z procedurą i ukierunkowana na utrzymanie funkcji państwa.

Wnioski z raportów krajowych i europejskich potwierdzają, że zarządzanie incydentami wymaga nie tylko narzędzi technicznych, lecz także zdolności organizacyjnych, współpracy, świadomości zagrożeń i gotowości do działania w warunkach presji (CERT Polska, 2026). W administracji granicznej oznacza to konieczność traktowania zarządzania incydentem jako część polityki cyberodporności, a nie wyłącznie jako procedury technicznej.

Wnioski

Incydent cyberbezpieczeństwa w administracji odpowiedzialnej za ochronę granic jest zdarzeniem wielowymiarowym. Jego obsługa wymaga integracji zespołów technicznych, operacyjnych, prawnych, komunikacyjnych i kierowniczych. Brak tej integracji zwiększa ryzyko opóźnienia,

niespójności działań, błędów decyzyjnych oraz utraty zaufania do procesu. Zaproponowany model ośmiu faz pozwala połączyć obsługę incydentu z wymaganiami cyberodporności i ciągłości działania. Najważniejszym elementem modelu jest utrzymanie funkcji granicznej w stanie kontrolowanej degradacji. Oznacza to zdolność do pracy przy ograniczonej dostępności systemów, zachowania minimalnych danych, dokumentowania decyzji i późniejszego odtworzenia integralności procesu.

Model ma zastosowanie w planach reagowania, playbookach, ćwiczeniach, audytach dojrzałości, szkoleniach i zarządzaniu relacjami z dostawcami. Jego wartość polega na tym, że przenosi zarządzanie incydentem z poziomu reakcji technicznej na poziom funkcji państwa. W praktyce oznacza to, że skuteczność reakcji powinna być oceniana nie tylko przez czas usunięcia awarii, ale także przez zdolność utrzymania odprawy, ochrony danych, komunikacji i rozliczalności decyzji. Zaproponowany model ma charakter interpretacyjno-aplikacyjny. Nie zastępuje audytu konkretnej architektury systemowej ani oceny procedur wdrożonych w poszczególnych jednostkach organizacyjnych, lecz wyznacza ramy takiej analizy. Dalsze badania powinny obejmować walidację modelu przez studia przypadków, wywiady eksperckie, ćwiczenia typu tabletop i cyber range, analizę danych incydentowych oraz pomiar skuteczności trybów pracy awaryjnej w różnych typach punktów granicznych. Szczególnie istotne będzie ustalenie, w jakim stopniu model pozwala identyfikować luki odpowiedzialności, zależności krytyczne, słabe punkty komunikacji oraz ryzyka wynikające z pracy na danych niepełnych lub niespójnych.

Literatura

1. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K. (2016). *Guide for cybersecurity event recovery (NIST SP 800-184).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184
2. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027
3. CERT Polska. (2026). *Raport roczny z działalności CERT Polska w 2025 roku*. NASK – Państwowy Instytut Badawczy.

4. Chodyka, M. (2025). Bezpieczeństwo baz danych jako element odporności cybernetycznej Sił Zbrojnych. W D. Brążkiewicz, M. Chodyka, T. Grudniewski, J. Nowicka (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część 1* (s. 123-140). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103199_7
5. Chodyka, M., Dalba-Gołaszewska, A. (2025). Database security in the face of contemporary threats. Przegląd Naukowo-Metodyczny. *Edukacja dla Bezpieczeństwa, 18*(4/69), 29-44.
6. Chodyka, M., Wojciechowska-Filipek, S., Ciekanowski, Z., Chrząszcz, A. E., Żurawski, S. (2026). The effectiveness of security management systems in public organizations: A cybersecurity perspective. *European Research Studies Journal, 29*(1), 478-489. https://doi.org/10.35808/ersj/4323
7. Chodyka, M., Żurawski, S., Wojciechowska-Filipek, S., Ciekanowski, Z., Mazur, S. (2025). Critical infrastructure security management in the era of cyber threats. *European Research Studies Journal, 28*(2), 610-621. https://doi.org/10.35808/ersj/4000
8. Ciekanowski, M., Chodyka, M., Żurawski, S., Parczewska, W. (2025). Bezpieczeństwo teleinformatyczne w zarządzaniu kryzysowym. W: D. Brążkiewicz, M. Chodyka, T. Grudniewski, S. Żurawski (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część 2* (s. 159-174). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103205_8
9. Ciekanowski, Z., Wojciechowska-Filipek, S. (2019). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: Jednostki – organizacji – państwa*. CeDeWu.
10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. (2022). Dz.Urz. UE L 333 z 27.12.2022, s. 80-152.
11. ENISA. (2024). *Cyber Europe 2024: After Action Report. European Union Agency for Cybersecurity*. Pobrane z: https://www.enisa.europa.eu/publications/cyber-europe-2024-after-action-report
12. ISO. (2019). *ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements*. International Organization for Standardization.

13. Kitler, W. (2011). *Bezpieczeństwo narodowe RP: Podstawowe kategorie, uwarunkowania, system*. Akademia Obrony Narodowej.
14. Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung Forum: Qualitative Social Research, 1*(2). https://doi.org/10.17169/fqs-1.2.1089
15. NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
16. Nelson, A., Rekhi, S., Souppaya, M., Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
17. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694. (2025). Dz.Urz. UE L 2025/38 z 15.01.2025.
18. Kancelaria Sejmu. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (t.j. Dz. U. z 2026 r. poz. 20, 252 z późn. zm.).
19. Wiśniewski, B. (2013). *System bezpieczeństwa państwa: Konteksty teoretyczne i praktyczne*. Wydawnictwo WSPol.
20. Wołejszo, J., Feltynowski, M. (2023). Efficiency of the control and command system in crisis management. *Polish Political Science Yearbook, 52*(3), 85-100. https://doi.org/10.15804/ppsy202381
21. Wołejszo, J., Malasiewicz, K., Prusiński, N. (red.). (2021). *Prakseologia w naukach o bezpieczeństwie: Sprawność działania w zarządzaniu kryzysowym*. Wydawnictwo Naukowe Akademii Kaliskiej im. Prezydenta Stanisława Wojciechowskiego.
22. Żurawski, S., Chrząszcz, A. E., Ciekanowski, Z., Pauliuchuk, Y., Pietrzyk, S., Wyrzykowska, B. (2025). Effectiveness of information security incident management systems: Identifying practices, challenges and development perspectives. *European Research Studies Journal, 28*(1), 575-588. https://doi.org/10.35808/ersj/3922

Tomasz Grudniewski[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_24

BEZPIECZEŃSTWO ENERGETYCZNE PAŃSTWA A DETEKCJA ANOMALII Z WYKORZYSTANIEM LSTM AUTOENCODER I DANYCH ENTSO-E

NATIONAL ENERGY SECURITY AND THE DETECTION OF ANOMALIES USING LSTM AUTOENCODERS AND ENTSO-E DATA

Streszczenie

Celem rozdziału jest ocena możliwości wykorzystania modelu LSTM Autoencoder do detekcji anomalii w godzinowych danych obciążenia krajowego systemu elektroenergetycznego Polski. Badanie osadzono w kontekście bezpieczeństwa energetycznego państwa, rozumianego jako zdolność do zapewnienia stabilnych dostaw energii oraz wczesnego identyfikowania nietypowych zjawisk mogących wskazywać na błędy danych, zakłócenia techniczne lub zdarzenia systemowe. Materiał badawczy stanowiły publiczne dane ENTSO-E obejmujące obciążenie systemu elektroenergetycznego Polski w latach 2022-2024. Dane poddano oczyszczeniu, normalizacji oraz podziałowi chronologicznemu na zbiory uczące, walidacyjne i testowe. Model

[1] https://orcid.org/0000-0003-3394-8992, e-mail: gisbourne2@gmail.com

uczono rekonstrukcji typowych tygodniowych przebiegów obciążenia, a detekcję oparto na wartości błędu rekonstrukcji. W części testowej zastosowano syntetyczne scenariusze anomalii: skok dodatni, spadek, flatline oraz dryf. Wyniki wskazują, że model najlepiej identyfikuje gwałtowne spadki obciążenia, częściowo wykrywa skoki dodatnie, natomiast słabiej reaguje na zmiany wolno narastające oraz przebiegi typu flatline. Uzyskane rezultaty potwierdzają przydatność podejścia rekonstrukcyjnego jako narzędzia wspierającego monitoring systemu elektroenergetycznego, przy jednoczesnej konieczności walidacji operatorskiej oraz uzupełnienia modelu o dodatkowe zmienne kontekstowe, takie jak pogoda, generacja OZE i prognozy zapotrzebowania.

Słowa kluczowe: bezpieczeństwo energetyczne, system elektroenergetyczny, detekcja anomalii, LSTM Autoencoder, ENTSO-E, obciążenie elektroenergetyczne, sztuczna inteligencja

Abstract

The aim of this chapter is to assess the potential of using the LSTM Autoencoder model for anomaly detection in hourly load data from Poland's national power system. The study is set within the context of national energy security, understood as the ability to ensure stable energy supplies and to identify at an early stage any unusual phenomena that may indicate data errors, technical disruptions or system events. The research data consisted of publicly available ENTSO-E data on Poland's power system load for 2022-2024. The data were cleaned, normalised, and chronologically split into training, validation, and test sets. The model was trained to reconstruct typical weekly load profiles, and detection was based on the reconstruction error value. In the test phase, synthetic anomaly scenarios were used: positive spike, drop, flatline and drift. The results indicate that the model best identifies sudden drops in load, partially detects positive spikes, but reacts less effectively to slowly rising changes and flatline patterns. The results obtained confirm the usefulness of the reconstruction approach as a tool supporting power system monitoring, whilst acknowledging the need for operator validation and the supplementation of the model with additional contextual variables, such as weather, renewable energy generation and demand forecasts.

Keywords: energy security, power system, anomaly detection, LSTM Autoencoder, ENTSO-E, power load, artificial intelligence

Wstęp

Bezpieczeństwo państwa zależy obecnie w szczególnym stopniu od stabilnych dostaw energii (Sovacool, Mukherjee, 2011; Winzer, 2012). Jednym z elementów wspierających bezpieczeństwo energetyczne państwa jest systematyczna analiza zużycia energii, obciążenia systemu oraz detekcja anomalii jako potencjalnych sygnałów zagrożenia (Chandola i in., 2009; Pang i in., 2021). Obciążenie pokazuje, jakie jest zapotrzebowanie odbiorców na moc w analizowanym oknie czasowym, np. w danej godzinie (ENTSO-E, b.d.-a; Kardi i in., 2021). Nagły skok albo spadek może oznaczać błąd danych lub nietypowe zdarzenie systemowe (Karkhaneh, Ozgoli, 2022). Może też wskazywać anomalie obciążenia systemu elektroenergetycznego krajowego. Anomalia oznacza przebieg, który wyraźnie odbiega od zwykłego. Takie odchylenie może wskazywać na błąd danych albo zdarzenie. By pozyskać dane do analizy, zdecydowano się na ENTSO-E (European Network of Transmission System Operators for Electricity). Platforma ENTSO-E udostępnia publiczne dane o obciążeniu krajów (ENTSO-E b.d.-c). Dzięki temu badanie można odtworzyć wyłącznie na podstawie publicznie dostępnych i sprawdzonych danych (Wiese i in., 2019). Badanie sprawdza, czy prosty model AI może zostać użyty do wskazywania podejrzanych okien czasowych. LSTM Autoencoder to autoenkoder wykorzystujący sieć typu Long Short-Term Memory, uczący się reprezentacji typowych przebiegów obciążenia (Hochreiter, Schmidhuber, 1997; Sakurada, Yairi, 2014). Potem próbuje odtworzyć nowe okna z danych testowych. Gdy odtworzenie jest słabe, błąd modelu rośnie wyraźnie. Błąd rekonstrukcji pokazuje, jak źle model odtworzył okno. Duży błąd oznacza, że przebieg wygląda nietypowo dla modelu. Tak powstaje sygnał do dalszego sprawdzenia danych systemowych. Model nie zastępuje operatora, lecz wskazuje okna czasowe wymagające kontroli technicznej (Hochreiter, Schmidhuber, 1997; Pang i in., 2021).

Okno tygodniowe obejmuje rytm dnia oraz tygodnia systemu. To ważne, bo zużycie prądu zmienia się regularnie. Podział chronologiczny chroni badanie przed przeciekiem informacji czasowej. Celem badania była ocena, czy model LSTM Autoencoder może wskazywać anomalie w godzinowych danych obciążenia krajowego systemu elektroenergetycznego. Sprawdzono, czy błąd rekonstrukcji pozwala odróżnić okna z anomaliami syntetycznymi od okien typowych.

Materiał i metody

Dane pochodziły z publicznych zasobów ENTSO-E dla Polski (ENTSO-E, b.d.-d). Obejmowały trzy lata godzinowych wartości obciążenia systemu krajowego. Po oczyszczeniu zostało dwadzieścia sześć tysięcy trzysta cztery obserwacje. Trzy braki uzupełniono interpolacją, trzy duplikaty uśredniono przed analizą. w danych ENTSO-E Polska jako obszar elektroenergetyczny jest identyfikowana specjalnym kodem: EIC 10YPL-AREA-----S (ENTSO--E, b.d.-b). Zastosowano dane publiczne, ponieważ każdy może sprawdzić zastosowaną procedurę (Wiese i in., 2019). To ułatwia powtórzenie badania bez systemów operatora sieci. Każde okno miało tydzień, czyli sto sześćdziesiąt osiem godzin (Karkhaneh, Ozgoli 2022). Okno przesuwano co dobę, aby zmniejszyć obliczenia modelu. Najpierw dane przeskalowano tylko na części uczącej modelu. Potem tak samo przekształcono walidację oraz test modelu. To zmniejsza ryzyko podpowiadania modelowi przyszłych wyników danych. Autoenkoder uczył się odtwarzać zwykłe okna obciążenia systemu (Lin i in., 2024). Alarm powstawał wtedy, gdy błąd odtworzenia przekraczał próg. Próg ustalano na podstawie wyników części walidacyjnej danych. Próg percentylowy wybiera granicę z danych walidacyjnych modelu. Niższy próg daje więcej alarmów i większą czułość. Wyższy próg daje mniej alarmów i mniejszą czułość. Najważniejsze dane zestawiono w Tabeli 1. Tabela 2 pokazuje ustawienia użytego modelu w badaniu.

Tabela 1. Charakterystyka wykorzystanych danych

Parametr	Wartość
Źródło	ENTSO-E Power Statistics, Monthly Hourly Load Values
Powiązanie ze źródłem głównym	zestaw oparty na agregacjach Transparency Platform
Obszar	Poland / PL
Kod EIC	10YPL-AREA-----S
Okres	2022-01-01 00:00 UTC – 2024-12-31 23:00 UTC
Jednostka	MW
Liczba obserwacji po oczyszczeniu	26 304
Braki uzupełnione interpolacją	3
Duplikaty uśrednione	3
Podział train / validation / test	17520 / 4368 / 4416

Źródło: opracowanie własne na podstawie ENTSO-E, b.d.-b, b.d.-c, b.d.-d.

Tabela 2. Parametry procedury uczenia i detekcji

Parametr	Wartość
Model	LSTM Autoencoder
Długość okna	168 h
Krok okna	24 h
Liczba cech wejściowych	1
Warstwa kodera	LSTM, 8 jednostek ukrytych
Warstwa dekodera	LSTM, 8 jednostek ukrytych
Normalizacja	MinMax, dopasowanie tylko na zbiorze train
Funkcja straty	MAE
Optymalizator	Adam
Epoki	8
Wskaźnik detekcji	maksymalny błąd bezwzględny rekonstrukcji w oknie

Źródło: opracowanie własne.

Wyniki

Scenariusze testowe dodano sztucznie, aby znać położenie anomalii. Skok oznacza nagły wzrost wartości w krótkim czasie (Chandola i in., 2009). Spadek oznacza nagłe zmniejszenie obciążenia w badanym oknie. Dryf oznacza powolną zmianę poziomu obciążenia w czasie. Taki przebieg może być trudniejszy do wykrycia (Pang i in., 2021). Zmiana rozłożona w czasie często nie tworzy wysokiego błędu rekonstrukcji modelu. Model może uznać dryf za zmianę dopuszczalną. Dlatego jego wykrycie wymaga często dodatkowych cech albo niższego progu detekcji. Flatline oznacza okres bez widocznej zmiany obciążenia danych. Tabela 3 pokazuje rodzaj, czas oraz siłę zmian.

Tabela 3. Scenariusze anomalii syntetycznych

Scenariusz	Początek	Czas trwania	Modyfikacja
Skok dodatni	2024-09-10 08:00 UTC	6 h	+35 procent
Spadek	2024-10-22 18:00 UTC	12 h	-35 procent
Flatline	2024-11-15 00:00 UTC	24 h	stała wartość
Dryf	2024-12-03 00:00 UTC	24 h	od 0 do +25 procent

Źródło: opracowanie własne.

Precision oznacza odsetek alarmów, które naprawdę wskazały anomalię. Recall oznacza odsetek anomalii, które model faktycznie znalazł. F1 łączy oba wyniki w jedną ocenę jakości. Uczenie zakończono po ośmiu epokach pracy modelu testowego. Najniższa strata walidacyjna wyniosła około 0,170 w tej próbie. Próg główny nie dawał fałszywych alarmów w teście. Jednocześnie wykrył tylko część okien z anomaliami syntetycznymi. Najlepiej rozpoznano spadek obciążenia o trzydzieści pięć procent. Skok dodatni wykryto częściowo, a dryfu nie wykryto. Flatline także nie przekroczył przyjętego progu alarmowego modelu. Niższy próg zwiększył recall bez fałszywych alarmów testowych. Wyższy próg zmniejszył liczbę wykrytych anomalii w testach. Czwarta tabela pokazuje wyniki dla progów detekcji modelu. Piąta tabela pokazuje skuteczność dla typów anomalii testowych.

Tabela 4. Wyniki detekcji dla progów percentylowych

Próg	Wartość progu	Precision	Recall	F1	FP	FN
0.950	0.513685	1.000	0.621	0.766	0	11
0.990	0.545169	1.000	0.345	0.513	0	19
0.995	0.546137	1.000	0.345	0.513	0	19
0.999	0.548783	1.000	0.310	0.474	0	20

Źródło: opracowanie własne.

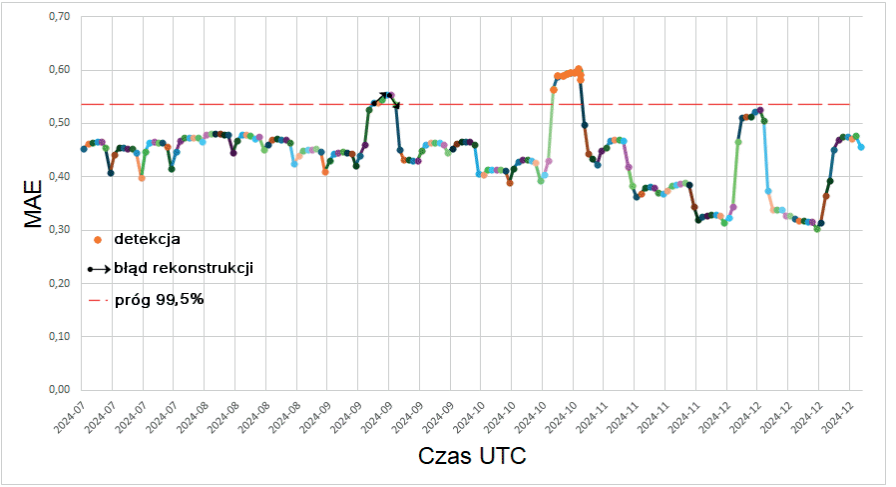
Niższy próg zwiększa czułość detektora anomalii. Próg 0,950 dał najwyższy recall bez fałszywych alarmów testowych w modelu. Wyższe progi ograniczały liczbę wykrytych przypadków. Porównanie pokazuje kompromis między ostrożnością alarmu a kompletnością detekcji anomalii testowych (Tabela 5).

Tabela 5. Wykrywalność według typu anomalii przy progu 0,995

Typ	Godziny	Okna dodatnie	Okna wykryte	Recall okien
skok_plus_35	6	7	3	0.429
spadek_minus_35	12	8	7	0.875
flatline_24h	24	7	0	0.000
dryf_plus_25	24	7	0	0.000

Źródło: opracowanie własne.

Najlepiej wykrywano spadek obciążenia systemu krajowego. Skok dodatni został wykryty częściowo, a dryf pozostał niewykryty w teście. Flatline nie przekroczył przyjętego progu alarmowego. Wyniki wskazują potrzebę dodatkowych cech dla wolniejszych zmian obciążenia systemu krajowego. Rysunek 1 pokazuje zmiany błędu rekonstrukcji w czasie. Próg pokazuje wartość, powyżej której model zgłasza potencjalną anomalię okna testowego danych. Największe piki błędu odpowiadają wykrytym zakłóceniom testowym. Brak przekroczenia progu oznacza, że dane nie uruchomiły alarmu detekcyjnego modelu automatycznie. Wykres ułatwia ocenę zachowania detektora w czasie. Pozwala też porównać reakcję modelu z położeniem wcześniej dodanych anomalii syntetycznych testowych.



Rysunek 1. Błąd rekonstrukcji i detekcje w zbiorze testowym

Źródło: opracowanie własne na podstawie ENTSO-E, b.d.-d.

Dyskusja

Wynik trzeba rozumieć jako sygnał wstępny, nie diagnozę. Dane godzinowe są zbyt ogólne, aby wskazać przyczynę (Kardi i in., 2021). Operator powinien sprawdzić alarm razem z innymi danymi. Sam alarm nie wystarcza do oceny zagrożenia energetycznego (Winzer, 2012). Model najlepiej reagował na szybkie zmiany wielkości obciążenia. Powolne zmiany mogły wyglądać dla niego zwyczajnie w danych. Dlatego dryf nie został wykryty

w tej próbie. Podobnie flatline nie przekroczył głównej granicy alarmowej modelu. Uzyskane wyniki potwierdzają użyteczność rekonstrukcji w monitoringu obciążenia systemu. Jednocześnie pokazują, że sama wartość błędu nie opisuje przyczyn zakłóceń w sieci. Model najlepiej reaguje na nagłe zmiany amplitudy sygnału obciążenia. Słabsza detekcja dryfu wskazuje na potrzebę uwzględnienia cech długookresowych szeregu czasowego w modelu. Flatline wymaga osobnej interpretacji, ponieważ nie zawsze zwiększa błąd. W praktyce podobny przebieg może oznaczać awarię pomiaru albo stabilny odczyt systemowy. Dlatego detekcja powinna być zawsze łączona z wiedzą operatorską. Dodatkowe zmienne mogłyby ograniczyć liczbę niejednoznacznych alarmów w ocenie systemu przez operatora. Szczególnie istotne są temperatura, generacja OZE oraz prognozy zapotrzebowania (ENTSO-E, b.d.-a; Shrestha i in., 2024). Takie dane pomagają odróżnić nietypowość techniczną od normalnej reakcji odbiorców energii elektrycznej. Wyniki należy traktować jako etap walidacji koncepcji badawczej modelu. Przed wdrożeniem potrzebne są testy na zdarzeniach potwierdzonych przez operatora systemu krajowego. Do dalszych badań warto dodać pogodę oraz produkcję OZE. Można także użyć prognozy zapotrzebowania na energię elektryczną. Lepsze dane pomogłyby odróżnić błąd od zdarzenia systemowego. Metoda wspiera monitoring, ale wymaga rozsądnej interpretacji eksperta. Bezpieczeństwo energetyczne dotyczy dostaw, danych oraz decyzji państwa. Właśnie dlatego wynik modelu powinien wspierać decyzję człowieka. Nie powinien samodzielnie przesądzać o stanie systemu krajowego.

Wnioski

LSTM Autoencoder może pomagać w prostym monitoringu obciążenia (Nam i in., 2020). Najpierw wskazuje miejsca, które warto sprawdzić dokładniej technicznie. Nie wyjaśnia jednak, dlaczego pojawiła się dana anomalia. W pilotażu najlepiej wykrywał spadki godzinowego obciążenia systemu. Dryf i flatline wymagają innych cech albo progów. Przed użyciem operacyjnym potrzebna jest walidacja operatorska metody. Najbezpieczniej traktować wynik jako listę spraw do kontroli. Model potwierdza przydatność rekonstrukcji w monitoringu obciążenia systemowego. Nie stanowi jednak samodzielnego narzędzia diagnozy pracy krajowej sieci elektroenergetycznej w praktyce. Największą skuteczność uzyskano dla gwałtownych

spadków obciążenia systemu. Słabsze wyniki dla dryfu pokazują ograniczenia prostej detekcji rekonstrukcyjnej w analizie operacyjnej. Próg alarmowy wymaga dostosowania do potrzeb operatora systemu. Zbyt niski próg może zwiększać liczbę zgłoszeń wymagających kontroli technicznej przez operatora. Zastosowanie operacyjne wymaga walidacji systemu na zdarzeniach rzeczywistych. Dalsze badania powinny uwzględnić pogodę, OZE oraz prognozy zapotrzebowania dla krajowego systemu. Metoda może wspierać priorytetyzację kontroli dużych zbiorów danych. Ostateczna decyzja powinna łączyć wynik modelu z oceną eksperta oraz kontekstem operatorskim.

Literatura

1. Chandola, V., Banerjee, A., Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
2. ENTSO-E. (b.d.-a). *Actual total load & day-ahead total load forecast*. Pobrane z: 18 maja 2026 https://transparencyplatform.zendesk.com/hc/en-us/articles/15885757679124-Actual-Total-Load-Day-ahead-Total--Load-Forecast-6-1-A-B (dostęp: 18.05.2026).
3. ENTSO-E. (b.d.-b). *EIC approved codes*. Pobrane z: https://www.entsoe.eu/data/energy-identification-codes-eic/eic-approved-codes/ (dostęp: 18.05.2026).
4. ENTSO-E. (b.d.-c). *Electricity market transparency*. Pobrane z: https://www.entsoe.eu/data/transparency-platform/ (dostęp: 18.05.2026).
5. ENTSO-E. (b.d.-d). *Monthly hourly load values. Power statistics*. Pobrane z: https://www.entsoe.eu/publications/data/power-stats/ (dostęp: 18.05.2026).
6. Hochreiter, S., Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735
7. Kardi, M., AlSkaif, T., Tekinerdogan, B., Catalão, J. P. S. (2021). *Anomaly detection in electricity consumption data using deep learning*. 2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe. https://doi.org/10.1109/EEEIC/ICPSEurope51590.2021.9584650

8. Karkhaneh, M., Ozgoli, S. (2022). Anomalous load profile detection in power systems using wavelet transform and robust regression. *Advanced Engineering Informatics, 53*, Article 101639. https://doi.org/10.1016/j.aei.2022.101639
9. Lin, R., Chen, S., He, Z., Wu, B., Zou, H., Zhao, X., Li, Q. (2024). Electricity behavior modeling and anomaly detection services based on a deep variational autoencoder network. *Energies, 17*(16), Article 3904. https://doi.org/10.3390/en17163904
10. Nam, G., Jeong, H., Park, P. (2020). *An anomaly detection scheme based on LSTM autoencoder for energy management.* International Conference on Information and Communication Technology Convergence. https://doi.org/10.1109/ICTC49870.2020.9289226
11. Pang, G., Shen, C., Cao, L., van den Hengel, A. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys, 54*(2), Article 38. https://doi.org/10.1145/3439950
12. Sakurada, M., Yairi, T. (2014). *Anomaly detection using autoencoders with nonlinear dimensionality reduction*. Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis. https://doi.org/10.1145/2689746.2689747
13. Shrestha, R., Mohammadi, M., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., Sanz, A., Nowroozi, E., Lindgren, A. (2024). Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. *Journal of Parallel and Distributed Computing, 193*, Article 104951. https://doi.org/10.1016/j.jpdc.2024.104951
14. Sovacool, B. K., Mukherjee, I. (2011). Conceptualizing and measuring energy security: A synthesized approach. *Energy, 36*(8), 5343-5355. https://doi.org/10.1016/j.energy.2011.06.043
15. Wiese, F., Schlecht, I., Bunke, W.-D., Gerbaulet, C., Hirth, L., Jahn, M., Kunz, F., Lorenz, C., Mühlenpfordt, J., Reimann, J., Schill, W.-P. (2019). Open Power System Data – Frictionless data for electricity system modelling. *Applied Energy, 236*, 401-409. https://doi.org/10.1016/j.apenergy.2018.11.097
16. Winzer, C. (2012). Conceptualizing energy security. *Energy Policy, 46*, 36-48. https://doi.org/10.1016/j.enpol.2012.02.067



ISBN 978-83-68103-37-3