PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335
e-ISSN 2720-0841

Punkty MEiN: 20

Numer zamknięto i oddano do druku w kwietniu 2026 r.

Recenzji są poddawane materiały zamieszczone w dziale Artykuły oraz
artykuły recenzyjne zamieszczone w dziale Artykuły recenzyjne / recenzje

Artykuły wyrażają poglądy autorów

Deklaracja o wersji pierwotnej

Wersja drukowana czasopisma jest jego wersją pierwotną
Wersja online czasopisma jest dostępna na stronie:
https://ejournals.eu/czasopismo/przeglad-bezpieczenstwa-wewnetrznego

Wersje językowe

Język polski (wersja drukowana i elektroniczna).
Tłumaczenie na język angielski (wersja elektroniczna).

Indeksacja w bazach danych

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się w bazach:
Index Copernicus Journal Master List z liczbą 100 punktów, ERIH PLUS,
Central European Journal of Social Science and Humanities
i Polska Bibliografia Naukowa (PBN)

Zgłaszanie tekstów

Materiały do PBW należy składać przez panel redakcyjny dostępny pod adresem:
https://ojs.ejournals.eu/PBW/about/submissions

SPIS TREŚCI

ARTYKUŁY

ARTYKUŁY RECENZYJNE / RECENZJE

PRACE KONKURSOWE

Szanowni Państwo!

Cieszę się, że mogę zarekomendować kolejny numer „Przeglądu Bezpieczeństwa Wewnętrznego". W tym wydaniu wiele uwagi poświęciliśmy działalności różnych formacji mundurowych w Polsce. Nasi autorzy piszą m.in. o ratownictwie specjalistycznym w Państwowej Straży Pożarnej, zagadnieniach związanych z polityką kadrową w Straży Granicznej i Siłach Zbrojnych RP, jak również o trudnych doświadczeniach żołnierzy i funkcjonariuszy chroniących w 2021 r. wschodnią granicę naszego kraju w czasie rosyjsko-białoruskiej operacji „Śluza".

Sytuacja geopolityczna w Europie Środkowo-Wschodniej, na którą duży wpływ ma konflikt zbrojny w Ukrainie, generuje nowe wymagania dla systemów reagowania na zagrożenia, w tym CBRNE, czyli chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe. Mobilne laboratoria CBRNE, w które została wyposażona Państwowa Straż Pożarna, odgrywają ważną rolę w zapewnianiu bezpieczeństwa w Polsce. Dr inż. Grzegorz Bugaj przeanalizował efektywność operacyjną tych laboratoriów w świetle przepisów prawnych i założeń Krajowego Systemu Ratowniczo-Gaśniczego, a także wskazał wyzwania i ograniczenia związane z ich wykorzystaniem. Jednym z takich wyzwań jest pozyskanie i utrzymanie wysoko wykwalifikowanej kadry wymaganej do obsługi tak zaawansowanych technologicznie rozwiązań.

O potrzebie zapewnienia optymalnie liczebnej i dobrze wyszkolonej kadry w formacjach mundurowych, umożliwiającej realizację zadań na odpowiednio wysokim poziomie, piszą dr Radosław Wiśniewski i Denis Tomala. Przedstawiają wyniki badań dotyczących retencji funkcjonariuszy Straży Granicznej. Badacze szukali odpowiedzi na pytania o to, jaki wpływ na odejście bądź pozostanie funkcjonariuszy mają czynniki indywidualne i organizacyjne oraz jakie rozwiązania mogłyby nie tylko zwiększyć zainteresowanie służbą

w Straży Granicznej – i w ogóle w formacjach mundurowych – lecz także zoptymalizować warunki do jej pełnienia przez wiele lat. Obecność w zespole ludzi doświadczonych, poza wieloma innymi korzyściami, przynosi pożądany efekt w postaci właściwie przebiegającego procesu zastępowalności kadr. Wiedza płynąca z prezentowanych badań pozwala doskonalić wewnętrzne rozwiązania kadrowe i zwiększać stabilność formacji, a także bezpieczeństwo państwa. Warto się z nią zapoznać.

Problematyki polityki kadrowej, ale w strukturach Sił Zbrojnych RP, dotyczy artykuł mjr. dr. Mariusza Domżalskiego. Omawia on kwestie związane z zakazem podejmowania pracy zarobkowej i prowadzenia działalności gospodarczej przez żołnierza zawodowego. Należy mieć na uwadze, że sytuacja na rynku pracy staje się coraz bardziej złożona i pojawiają się nowe formy zarobkowania. Może to wymagać – jak słusznie zauważa autor – doprecyzowania pojęcia pracy zarobkowej i wydania rozporządzeń wykonawczych dotyczących ograniczeń zawodowych dla osób służących w formacjach mundurowych.

Norbert Łucarz opisuje operację „Śluza" i proceder instrumentalizacji migrantów w polityce Federacji Rosyjskiej i Republiki Białorusi. W wyniku tej operacji polskie służby mundurowe chroniące granicę polsko-białoruską stały się obiektem agresji ze strony migrantów oraz wspierających ich białoruskich funkcjonariuszy. Operacji „Śluza" towarzyszyły wrogie działania propagandowe i dezinformacyjne – pojawiły się narracje, w których polskie służby przedstawiano w wyjątkowo negatywnym świetle. Efektem tych działań była narastająca polaryzacja polskiego społeczeństwa. Jednym z wyrazów sprzeciwu wobec tych wydarzeń była akcja „Murem za polskim mundurem". Miała ona na celu wyrażenie poparcia dla ludzi, którzy wykonując swoje zadania służbowe, musieli mierzyć się z silną presją fizyczną i psychiczną.

O atakach na nienaruszalność polskiej granicy z Białorusią pisze także Agata Rytel, która podejmuje temat działań hybrydowych ze strony Federacji Rosyjskiej, wymierzonych w latach 2021–2024 w polską przestrzeń informacyjną i cyberprzestrzeń. Autorka dowodzi, że zdarzenia te miały bezpośredni związek z wojną w Ukrainie i były intencjonalną ingerencją Rosji i Białorusi. To kolejny przykład, jak złożony charakter mają współczesne ataki, w których agresor łączy różne rodzaje działań i prowadzi je w wielu domenach.

Jednym z częściej wybieranych celów ataków jest sektor finansowy. Dr hab. Kamil Mroczka i Paweł Piekutowski piszą o zwiększaniu odporności cyfrowej podmiotów z tego sektora w związku z obowiązkami wynikającymi z rozporządzenia DORA (Digital Operational Resilience Act). Wskazują testy TLPT (threat-led penetration testing), czyli testy penetracyjne oparte na zagrożeniach, jako skuteczną metodę wzmacniania tej odporności. Zadaniem tych testów jest jak najwierniejsze odzwierciedlenie rzeczywistych scenariuszy ataków, aby precyzyjnie zidentyfikować słabe miejsca w systemie ochrony cybernetycznej organizacji i poprawić jej zdolność do wykrywania cyberzagrożeń. Autorzy uważają, że testy TLPT są bardzo potrzebne, gdyż pozwalają na zweryfikowanie nie tylko środków technicznych, lecz także zachowań personelu.

Problematyka testowania odporności pojawia się również w artykule Klaudii Maciaty poświęconym morskim farmom wiatrowym, istotnym dla bezpieczeństwa energetycznego państwa. Ich specyficzna lokalizacja zwiększa podatność na zagrożenia hybrydowe, w tym w cyberprzestrzeni. Potrzebne jest zatem wielotorowe testowanie odporności tych farm. W sferze cybernetycznej będą to m.in. ćwiczenia red teaming, czyli symulowane ataki odzwierciedlające taktyki i techniki wykorzystywane przez cyberprzestępców. Zdaniem autorki, aby zwiększyć poziom bezpieczeństwa farm wiatrowych, należy połączyć działania legislacyjne, technologiczne i organizacyjne.

Duży wpływ na rozwój zagrożeń cybernetycznych ma pojawienie się sztucznej inteligencji. Traktuje o tym artykuł Jakuba Gajeckiego. Postęp w zakresie AI i uczenia maszynowego spowodował, że zagrożenia stały się bardziej złożone, dynamiczne i trudniejsze do wykrycia. W tym kontekście autor analizuje i ocenia istniejące strategie obronne. Zwraca uwagę na rolę współpracy międzynarodowej w zwalczaniu cyberprzestępczości i potrzebę bieżącego aktualizowania przepisów. Większość z nich powstała bowiem w okresie, gdy technologie AI nie były wykorzystywane w działaniach cybernetycznych na tak szeroką skalę.

W tym numerze pojawia się także istotny z punktu widzenia zarządzania kryzysowego i obronności RP wątek dotyczący zapewnienia ciągłości funkcjonowania państwa. W dziale „Prace konkursowe" prezentujemy tekst Davida Cybulskiego na temat łączności i komunikacji administracji państwowej w przypadku zagrożenia bezpieczeństwa narodowego. Wdrożenie Systemu Bezpiecznej

Łączności Państwowej, który jest nadzorowany przez ministra właściwego do spraw wewnętrznych, ma przełożyć się na skrócenie czasu reakcji administracji, służb bezpieczeństwa i usprawnienie ratownictwa w sytuacjach kryzysowych.

„Przegląd Bezpieczeństwa Wewnętrznego" to periodyk służby specjalnej o profilu kontrwywiadowczym, nie mogło więc zabraknąć odwołania do problematyki oscylującej wokół art. 130 Kodeksu karnego. Dr hab. Tomasz Safjański zrecenzował dla nas monografię pt. *Szpiegostwo. Studium kryminologiczne*. Jej autor, dr hab. Piotr Chlebowicz, podjął się całościowej analizy kryminologicznej zjawiska szpiegostwa w Polsce w latach 1990–2022. Publikacja ta jest podsumowaniem jego wieloletnich dociekań, opartych na badaniach aktowych, archiwalnych, wywiadach swobodnych i literaturze przedmiotu. Zdaniem recenzenta jest to praca wybitna i powinna stać się lekturą obowiązkową dla kryminologów, karnistów, analityków, a także polityków i innych osób odpowiedzialnych za bezpieczeństwo narodowe. Ja również zachęcam do lektury tej wyjątkowej książki!

Kończąc, chciałabym podziękować autorom, recenzentom, członkom Rady Naukowej i zespołu redakcyjnego za współtworzenie czasopisma, którym kieruję. To dla mnie przyjemność i zobowiązanie. Wierzę, że poruszane przez nas tematy są dla Państwa interesujące, a nasz wkład w popularyzację problematyki bezpieczeństwa jest potrzebny i dostrzegany.

Redaktor naczelny
dr Daria Olender

ARTYKUŁY

Przegląd Bezpieczeństwa Wewnętrznego

2026, nr 34, s. 13–35

 https://doi.org/10.4467/20801335PBW.26.001.23363

ARTYKUŁ

Testy threat-led penetration testing (TLPT) – nowe podejście do testowania cyfrowej odporności podmiotów finansowych w Polsce w kontekście obowiązków wynikających z rozporządzenia Digital Operational Resilience Act (DORA)

Threat-led penetration testing (TLPT) – a new approach to testing digital resilience of financial entities in Poland in the perspective of requirements under the Digital Operational Resilience Act (DORA)

KAMIL MROCZKA

Wydział Nauk Politycznych i Studiów Międzynarodowych,
Uniwersytet Warszawski

https://orcid.org/0000-0003-3809-3479

PAWEŁ PIEKUTOWSKI

Departament Cyberbezpieczeństwa,
Urząd Komisji Nadzoru Finansowego

https://orcid.org/0009-0001-5861-7367

Abstrakt

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA) wprowadziło do unijnego, a tym samym i krajowego, porządku prawnego nowy model testowania cyfrowej odporności podmiotów finansowych działających na polskim rynku finansowym. Zasadniczym celem artykułu jest omówienie i ocena modelu threat-led penetration

testing (TLPT), czyli testów penetracyjnych opartych na zagrożeniach. Testy TLPT mogą obejmować zarówno techniczne, jak i socjotechniczne elementy. Hipotezą artykułu jest twierdzenie, że testy TLPT powinny wpłynąć pozytywnie na zwiększanie cyfrowej odporności podmiotów finansowych, gdyż są zaprojektowane tak, aby imitować rzeczywiste cyberataki, co umożliwia organizacjom zrozumienie swojej odporności na zagrożenia oraz podjęcie odpowiednich działań naprawczych. Uzyskane rezultaty analizy potwierdzają postawioną hipotezę badawczą. Wynika to z faktu, że głównym założeniem testów TLPT jest jak najwierniejsze odzwierciedlenie rzeczywistych scenariuszy ataków. Stwarza to możliwość bardziej rzetelnej i szczegółowej oceny poziomu bezpieczeństwa organizacji. Autorzy podkreślają, że takie podejście pozwala nie tylko na weryfikację skuteczności zabezpieczeń infrastruktury teleinformatycznej, lecz także na ocenę odporności procesów operacyjnych oraz poziomu świadomości pracowników w obszarze cyberzagrożeń.

Słowa kluczowe testy TLPT, DORA, Komisja Nadzoru Finansowego, cyfrowa odporność, cyberbezpieczeństwo

Abstract

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA) launched a new model for testing the digital resilience of financial services operating in the Polish financial market into the EU and thus into the domestic legal framework. The primary purpose of this article is to discuss and evaluate the Threat-Led Penetration Testing (TLPT) model. TLPT tests can include both technical and sociotechnical components. The hypothesis of the article is that TLPT testing will have a positive impact on enhancing the digital resilience of financial stakeholders because these tests are designed to simulate real-world cyber attacks, enabling organisations to understand their resilience to threats and initiate relevant countermeasures. The results obtained from the analysis confirm the validity of the proposed research hypothesis. This follows from the fact that the fundamental premise of TLPT testing is to replicate real-world attack scenarios as accurately as possible, thereby enabling a more reliable and detailed assessment of organisation's security posture. The authors emphasise that such an approach allows not only for the verification of the effectiveness of information system safeguards, but also for the evaluation of the resilience of operational processes and the level of employee awareness regarding cyber threats.

Keywords TLPT tests, DORA, Polish Financial Supervision Authority, digital resilience, cybersecurity

Wprowadzenie

Technologie informacyjno-komunikacyjne (information and communication technologies, ICT[1]) są obecne niemal w każdym obszarze funkcjonowania państw i ich gospodarek[2]. Stanowią realne wsparcie dla złożonych systemów wykorzystywanych w codziennych działaniach. Technologie te napędzają polską gospodarkę i jej najważniejsze sektory, w tym sektor finansowy, oraz wzmacniają funkcjonowanie rynku wewnętrznego Unii Europejskiej. Gęstniejąca sieć wzajemnych powiązań między interesariuszami rynku finansowego, dostawcami usług finansowych i klientami tego rynku wraz z postępującą cyfryzacją systemów finansowych zwiększają podatność na różnego rodzaju ryzyko, w tym wynikające z cyberzagrożeń i zakłóceń w funkcjonowaniu ICT. Niezbędne jest zatem podejmowanie działań mających na celu zwiększanie odporności cyfrowej podmiotów finansowych.

W motywie 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (dalej: rozporządzenie DORA)[3] jednoznacznie podkreślono, że (…) *w ostatnich dziesięcioleciach korzystanie z ICT zaczęło odgrywać zasadniczą rolę, jeżeli chodzi o świadczenie usług finansowych, do tego stopnia, że obecnie ICT mają krytyczne znaczenie dla wykonywania typowych codziennych funkcji wszystkich podmiotów finansowych*. W piśmiennictwie słusznie się zauważa, że obowiązujące od stycznia 2025 r. rozporządzenie DORA zobowiązało podmioty finansowe oraz zewnętrznych dostawców usług ICT do stosowania najlepszych praktyk w zakresie cyberbezpieczeństwa. Za jeden z zaawansowanych środków prowadzących do zwiększenia odporności cyfrowej podmiotów finansowych uznano testy penetracyjne oparte na zagrożeniach (threat-led penetration testing, TLPT). Będą one wykorzystywane do oceny stanu cyberbezpieczeństwa tych podmiotów[4].

Nie wchodząc w tym miejscu w pogłębioną analizę zakresu znaczeniowego terminu „threat-led penetration testing", należy podkreślić, że jest to technika oceny

---

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

[2] W artykule wykorzystano publikację jednego z autorów przygotowaną na potrzeby procesu wdrażania rozporządzenia DORA. Zob. *Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji*, Komisja Nadzoru Finansowego, 14 VII 2025 r., https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [dostęp: 9 II 2026].

[3] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*.

[4] M.L. Dozsa, *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, praca magisterska, Oslo 2024, s. ii.

cyberbezpieczeństwa służąca do symulacji realistycznych scenariuszy cyberataków, których celem są krytyczne systemy i infrastruktura organizacji. W przeciwieństwie do tradycyjnych testów penetracyjnych, mogących opierać się na standardowej liście podatności, metoda TLPT koncentruje się na naśladowaniu konkretnych aktorów, technik i taktyk, których zaistnienie w organizacji jest najbardziej prawdopodobne ze względu na jej unikalny profil ryzyka. Testy TLPT są przeprowadzane, aby zidentyfikować słabości, zweryfikować istniejące środki bezpieczeństwa i zwiększyć zdolności organizacji do wykrywania rzeczywistych cyberzagrożeń, reagowania na nie i odzyskiwania danych[5].

Głównym celem artykułu jest krytyczna analiza modelu TLPT jako instrumentu oceny cyfrowej odporności podmiotów finansowych w Polsce w kontekście wymogów rozporządzenia DORA, ze szczególnym uwzględnieniem różnic między testami TLPT a klasycznymi testami penetracyjnymi, roli instytucji nadzorczych oraz implikacji wdrożeniowych.

Autorzy artykułu przyjęli następującą hipotezę: testy TLPT powinny wpłynąć pozytywnie na zwiększanie cyfrowej odporności podmiotów finansowych, gdyż są zaprojektowane tak, aby imitować rzeczywiste cyberataki, co umożliwia organizacjom zrozumienie swojej odporności na zagrożenia oraz podjęcie odpowiednich działań naprawczych.

Na potrzeby prowadzonych rozważań wykorzystano metodę prawnoporównawczą, analizę instytucjonalną oraz krytyczną analizę piśmiennictwa naukowego. Zastosowano również obserwację uczestniczącą wynikającą z doświadczeń zawodowych autorów. Wskazane metody pozwoliły na ustalenie roli i kompetencji podmiotów odpowiedzialnych za cyberbezpieczeństwo rynku finansowego, a także na identyfikację różnic w podejściu do testowania odporności cyfrowej, ocenę stopnia harmonizacji regulacyjnej oraz zasygnalizowanie obszarów, w których polski model nadzoru nad cyberbezpieczeństwem rynku finansowego może wymagać doprecyzowania lub dalszego rozwoju.

Testy TLPT – definicja

Definiując testy TLPT, eksperci z zakresu cyberbezpieczeństwa podkreślają, że jest to (…) *zaawansowana forma testów penetracyjnych, która wykracza poza standardowe podejście, symulując rzeczywiste ataki cybernetyczne z wykorzystaniem taktyk, technik i procedur (TTP) stosowanych przez prawdziwych cyberprzestępców.*

[5] B. Riaz, Z. Younas, *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024, s. 26.

W przeciwieństwie do tradycyjnych testów penetracyjnych, TLPT koncentruje się na analizie konkretnych zagrożeń, na które narażona jest dana organizacja, dostosowując symulacje ataków do jej specyficznego profilu ryzyka[6].

Definicję legalną testów TLPT zawarto w art. 3 pkt 17 rozporządzenia DORA. Zgodnie z tym przepisem testy te oznaczają (…) *ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają dostarczenie kontrolowanych, dostosowanych do podmiotu, wynikających z analizy zebranych danych (red team) testów działających na bieżąco krytycznych systemów produkcyjnych podmiotu finansowego*[7].

Testy penetracyjne a testy TLPT – najważniejsze różnice

Głównym celem realizacji testów TLPT jest ocena realnej odporności instytucji na zagrożenia i mogące zaistnieć scenariusze ataków. Test penetracyjny skupia się bardziej na identyfikacji technicznych podatności i błędów konfiguracyjnych w systemach informatycznych.

Uszczegóławiając, można wskazać następujące różnice:

1) zakres realizacji testu – testy penetracyjne koncentrują się zazwyczaj na ściśle określonych elementach infrastruktury IT – pojedynczych systemach, aplikacjach czy komponentach sieci. Ich celem jest przede wszystkim wykrycie podatności technicznych w zdefiniowanym obszarze. To podejście pozwala na ocenę bezpieczeństwa konkretnego systemu, ale nie daje pełnego obrazu, jak organizacja poradziłaby sobie ze złożonym cyberatakiem. W testach TLPT podchodzi się do tematu znacznie szerzej. Obejmują one nie tylko systemy i technologie, lecz także procesy operacyjne i ludzi. Celem jest sprawdzenie całego ekosystemu cyberobrony organizacji i odpowiedź na pytania: jak działa monitorowanie bezpieczeństwa? Jak przebiega komunikacja wewnętrzna? Jak zespół reaguje na incydenty? Jakie są ścieżki eskalacji? Testy TLPT pozwalają zobaczyć, czy organizacja jest przygotowana na atak nie tylko teoretycznie, lecz także w praktyce. Umożliwia to zwiększenie odporności całego „organizmu", a nie tylko pojedynczego elementu;

---

[6] *Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA*, Bankowe ABC, 2 I 2025 r., https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [dostęp: 19 IV 2025].

[7] Zob. także: J. Kurek-Sobieraj, Komentarz do art. 3, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 85–86.

2) scenariusze ataków – testy penetracyjne opierają się głównie na znanych podatnościach i skupiają się bardziej na identyfikacji potencjalnych zagrożeń w określonym systemie informatycznym. Testy TLPT są realizowane na podstawie scenariuszy opracowanych przez specjalny zespół threat intelligence. Ma on zidentyfikować najbardziej realistyczne cyberzagrożenia i scenariusze ataków, z którymi może mieć do czynienia dana organizacja. Scenariusze te mogą bazować na raportach dotyczących ogólnej analizy cyberzagrożeń (generic threat intelligence) dla danego sektora. W raporcie opublikowanym przez zespół reagowania na incydenty bezpieczeństwa komputerowego Komisji Nadzoru Finansowego (CSIRT KNF) zostały opisane potencjalne rodzaje ataków, kategorie adwersarzy i trendy w realizacji cyberataków[8]. Duży nacisk położono w nim na możliwy rozwój zagrożeń związanych z wykorzystaniem technik i narzędzi opartych na sztucznej inteligencji, a także na niebezpieczeństwa wynikające z ataków na łańcuchy dostaw. Istotnymi aspektami są również intensyfikacja ataków ransomware, coraz częściej realizowanych w modelu ransomware as a service, oraz rozwój zjawiska haktywizmu, który przybrał na sile po wybuchu wojny w Ukrainie;
3) środowisko testowe i podejście do ryzyka – testy penetracyjne są realizowane najczęściej w odpowiednich środowiskach testowych, aby uniknąć zakłóceń w funkcjonowaniu systemów. W testach TLPT duży nacisk jest położony na kompleksowe zbadanie faktycznego poziomu bezpieczeństwa organizacji, dlatego są one przeprowadzane na środowiskach produkcyjnych. Oznacza to dodatkowe ryzyko związane z możliwością zakłócenia ciągłości działania systemów i procesów biznesowych. W związku z tym podczas testów TLPT niezbędne jest prowadzenie analizy ryzyka pozwalającej na mitygację zakłóceń, które mogłyby się pojawić podczas ich realizacji;
4) przebieg testów i poufność – cechą charakterystyczną testów TLPT jest wymóg zachowania ich w tajemnicy przed większością organizacji. Jedynie wąska grupa pracowników ma świadomość ich realizacji. Intencją jest zweryfikowanie reakcji organizacji na cyberzagrożenie. Bada się nie tylko cyfrową odporność systemów teleinformatycznych, lecz także przygotowanie zespołów bezpieczeństwa oraz funkcjonowanie odpowiednich procesów wewnątrz organizacji. Zachowanie poufności testów stanowi duże wyzwanie dla organizacji ze względu na złożoność wielu procesów biznesowych;

[8] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025*, CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 19 I 2026].

5) wyniki i raportowanie – istotnym elementem realizacji testów TLPT są ćwiczenia typu purple team, które odbywają się po zakończeniu fazy ataków. Są to ćwiczenia, w ramach których zespół symulujący ataki oraz zespół odpowiedzialny za obronę wspólnie omawiają przeprowadzone scenariusze, identyfikują słabości w procesach i systemach, a także wypracowują rozwiązania pozwalające na zwiększenie poziomu cyberodporności organizacji. Następnie jest przygotowywany plan działań naprawczych;
6) częstotliwość testu – testy penetracyjne mogą być realizowane z większą częstotliwością. Testy TLPT są przeprowadzane zdecydowanie rzadziej ze względu na poziom ich skomplikowania oraz koszty.

Obowiązek testowania cyfrowej odporności podmiotów finansowych w świetle art. 26 rozporządzenia DORA

Rozporządzenie DORA zobowiązuje podmioty finansowe (z pewnymi wyłączeniami wskazanymi w art. 16 ust. 1 akapit pierwszy rozporządzenia DORA) do przeprowadzania testów TLPT nie rzadziej niż co trzy lata. Na podstawie profilu ryzyka danego podmiotu finansowego i z uwzględnieniem okoliczności operacyjnych właściwy organ może jednak, w razie potrzeby, zwrócić się do tego podmiotu o zmniejszenie lub zwiększenie częstotliwości przeprowadzania testów TLPT. W piśmiennictwie stwierdza się, że może to nastąpić w przypadku (…) *pozyskania przez właściwy organ uzasadnionych podejrzeń, że w organizacji doszło do nieprawidłowego zarządzania ryzykiem (np. przez pojawienie się ofert sprzedaży danych organizacji na czarnym rynku)*[9].

Niezwykle ważny z perspektywy wymagań dotyczących jakości jest ust. 2 przywołanego przepisu. Stanowi on, że: *każdy test penetracyjny ukierunkowany przez analizę zagrożeń obejmuje kilka krytycznych lub istotnych funkcji podmiotu finansowego lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje.* Pierwszym krokiem do rzetelnego przeprowadzenia testów TLPT jest określenie wszelkich stosownych systemów bazowych. Następnie podmioty finansowe powinny ustalić wszystkie procesy i technologie ICT wspierające krytyczne lub istotne funkcje. Ostatnie działanie polega na określeniu, które usługi ICT, w tym systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcje i usługi, zostały zlecone w drodze outsourcingu zewnętrznym dostawcom usług ICT lub są przedmiotem umowy z takimi dostawcami.

[9] C. Cichocki, Komentarz do art. 26, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 280.

W doktrynie słusznie podkreśla się, że profesjonalny proces gromadzenia tych informacji i danych wymaga wiedzy biznesowej o funkcjonowaniu organizacji oraz przełożenia jej na wiedzę technologiczną i techniczną. Do takich działań można wykorzystać różne narzędzia ICT, np. systemy klasy CMDB (computer management database)[10]. W praktyce badanie może dotyczyć wszystkich lub tylko wybranych systemów czy funkcjonalności. Mając na uwadze wysoki poziom współzależności systemów i narzędzi ICT w podmiotach finansowych, zaleca się kompleksowe badania. Na podstawie informacji i danych uzyskanych z analizy podmioty te mają obowiązek dokonania oceny, które krytyczne lub istotne funkcje należy objąć testami TLPT. Ocenę tę zatwierdzają właściwe organy. W polskim porządku prawnym jest to Komisja Nadzoru Finansowego, o czym będzie mowa w dalszej części artykułu.

W przypadku gdy zakres TLPT obejmuje zewnętrznych dostawców usług ICT, podmiot finansowy stosuje niezbędne środki i zabezpieczenia, aby wzięli oni udział w testach, i przez cały czas ponosi pełną odpowiedzialność za zapewnianie zgodności z rozporządzeniem DORA. Wymóg ten jest krytycznie istotny w kontekście praktyki funkcjonowania podmiotów finansowych, gdyż wszystkie korzystają z usług zewnętrznych dostawców.

Prawodawca unijny, świadomy skali działania dostawców usług ICT, wprowadza pewne odstępstwa od generalnej zasady ich udziału w testach TLPT. Zgodnie z brzmieniem art. 26 ust. 4 rozporządzenia DORA:

> (…) w przypadku gdy można racjonalnie przewidywać, że udział zewnętrznego dostawcy usług ICT w TLPT (…) będzie miał negatywny wpływ na jakość lub bezpieczeństwo usług świadczonych przez tego zewnętrznego dostawcę usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia lub na poufność danych związanych z takimi usługami, dany podmiot finansowy i dany zewnętrzny dostawca usług ICT mogą uzgodnić na piśmie, że ten zewnętrzny dostawca usług ICT zawrze ustalenia umowne bezpośrednio z testerem zewnętrznym w celu przeprowadzenia – pod kierownictwem jednego wyznaczonego podmiotu finansowego – zbiorczych TLPT z udziałem kilku podmiotów finansowych (testowania zbiorczego), na rzecz których dany zewnętrzny dostawca usług ICT świadczy usługi ICT.
>
> Takie testowanie zbiorcze obejmuje odpowiedni zakres usług ICT wspierających krytyczne lub istotne funkcje będące przedmiotem zawartej przez te podmioty finansowe umowy z tym zewnętrznym dostawcą usług ICT. Testowanie zbiorcze uznaje się za TLPT przeprowadzone przez podmioty finansowe biorące udział w tym testowaniu zbiorczym.

[10] Tamże.

Liczba podmiotów finansowych uczestniczących w takim testowaniu jest odpowiednio dostosowana i uwzględnia stopień złożoności i rodzaj usług nim objętych. Po zakończeniu testów, uzgodnieniu sprawozdań i planów naprawczych podmiot finansowy i w stosownych przypadkach testerzy zewnętrzni przedstawiają właściwemu organowi podsumowanie ustaleń, plany naprawcze i dokumentację wykazującą, że testy przeprowadzono zgodnie z wymogami rozporządzenia. Na tej podstawie właściwe organy wydają podmiotom finansowym poświadczenie, które potwierdza przeprowadzenie testów zgodnie z wymaganiami określonymi w dokumentacji. Umożliwia ono organom wzajemne uznawanie testów TLPT, przy czym nie zwalnia podmiotów finansowych z odpowiedzialności za wyniki tych testów.

Na podmioty finansowe nałożono obowiązek zawarcia umów, których celem jest przeprowadzenie testów TLPT. Jeżeli podmiot finansowy dysponuje zespołami testerów wewnętrznych, rozporządzenie DORA nakłada wymóg zrealizowania tego rodzaju testów przez testera zewnętrznego co trzy testy, czyli najrzadziej co dziewięć lat. Wyjątek od tej zasady dotyczy instytucji kredytowych sklasyfikowanych jako istotne zgodnie z art. 6 ust. 4 rozporządzenia Rady UE nr 1024/2013[11]. Podmioty te mają obowiązek korzystania wyłącznie z testerów zewnętrznych.

Rozporządzenie DORA definiuje również kryteria, które są stosowane przez właściwe organy do określania podmiotów objętych obowiązkiem testowania TLPT. W ocenie uwzględnia się:

- czynniki związane z wpływem, zwłaszcza zakres, w jakim świadczone usługi i działania podejmowane przez podmiot finansowy mają wpływ na sektor finansowy,
- ewentualne obawy dotyczące stabilności finansowej, w tym systemowy charakter podmiotu finansowego na poziomie unijnym lub krajowym,
- specyficzny profil ryzyka związanego z ICT, poziom zaawansowania podmiotu finansowego pod względem ICT lub zastosowane rozwiązania technologiczne.

Syntetyzując analizę przedmiotową i podmiotową art. 26 rozporządzenia DORA, należy wskazać, że przepis ten daje państwom członkowskim możliwość wyznaczenia jednego organu publicznego w sektorze finansowym, który na szczeblu krajowym będzie odpowiedzialny za kwestie związane z testami TLPT w tym sektorze. Organowi temu powierza się wszystkie kompetencje i zadania w tym zakresie.

[11] *Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi*, s. 63.

Wymogi dotyczące testerów zewnętrznych i wewnętrznych

W art. 27 rozporządzenia DORA zostały zdefiniowane podstawowe wymagania dotyczące testerów przeprowadzających testy TLPT. Ustęp 1 tego przepisu stanowi, że podmioty finansowe korzystają w tym przypadku wyłącznie z usług testerów zewnętrznych, którzy:

a) są najbardziej odpowiedni do tego zadania i cieszą się największą renomą;
b) posiadają zdolności techniczne i organizacyjne oraz wykazują się szczególną wiedzą fachową w zakresie analizy zagrożeń, testów penetracyjnych i testów z udziałem zespołów typu red team;
c) posiadają certyfikat wydany przez jednostkę akredytującą w państwie członkowskim lub przystąpili do formalnych kodeksów postępowania lub ram etycznych;
d) przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z przeprowadzaniem TLPT, w tym należytej ochrony poufnych informacji podmiotu finansowego i mitygacji ryzyka biznesowego podmiotu finansowego;
e) są należycie i w pełni objęci odpowiednimi ubezpieczeniami od odpowiedzialności cywilnej z tytułu wykonywania zawodu, w tym od ryzyka uchybień i zaniedbań.

W doktrynie słusznie podkreśla się, że (…) *trafność i rzetelność testów TLPT jest traktowana przez ustawodawcę jako kluczowa, bowiem poszczególne organizacje finansowe powinny ufać certyfikatom okazywanym przez inne podmioty z branży. Również dla organu właściwego dla kontroli, istotny jest poziom zaufania do testerów zewnętrznych lub wewnętrznych*[12].

Prawodawca unijny dopuszcza możliwość korzystania z testerów wewnętrznych. Stawia jednak dodatkowe wymogi, poza przywołanymi powyżej w odniesieniu do testerów zewnętrznych. W art. 27 ust. 2 rozporządzenie DORA stanowi, że podmioty finansowe korzystające z testerów wewnętrznych zapewniają spełnienie następujących warunków:

a) takie korzystanie z testerów wewnętrznych zostało zatwierdzone przez odpowiedni właściwy organ lub przez jeden organ publiczny wyznaczony zgodnie z art. 26 ust. 9 i 10;
b) odpowiedni właściwy organ sprawdził, że dany podmiot finansowy dysponuje wystarczającymi zasobami przeznaczonymi na ten cel i że zapewnił unikanie konfliktów interesów na wszystkich etapach projektowania i wykonywania testu; oraz

[12] C. Cichocki, Komentarz do art. 27, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 284.

c) dostawca analizy zagrożeń jest podmiotem zewnętrznym względem danego podmiotu finansowego.

W art. 27 ust. 3 rozporządzenia DORA zwraca się uwagę na kwestie bezpieczeństwa informacji i danych wynikających z testów TLPT. Podmioty finansowe mają zapewnić, aby umowy zawarte z testerami zewnętrznymi zobowiązywały tych testerów do (…) *należytego zarządzania wynikami TLPT oraz aby żadne przetwarzanie danych pochodzących z tych wyników, w tym generowanie, przechowywanie, agregowanie, sporządzanie, zgłaszanie, przekazywanie lub niszczenie, nie stwarzały ryzyka dla podmiotu finansowego*.

Cezary Cichocki słusznie podnosi, że dane uzyskane w wyniku testów TLPT należy traktować jako szczególnie wrażliwe z uwagi na to, że jeśli (…) *wpadną w ręce osób niepowołanych, to stanowić będą rodzaj przewodnika po podatnościach w systemach organizacji finansowej i znacznie ułatwią potencjalnemu intruzowi atak. Ryzyko ujawnienia tych danych polega na tym, że pomiędzy ujawnieniem zagrożeń w ramach testów TLPT a ich mitygacją może minąć pewien interwał czasu, który stanie się oknem ataku w wypadku ujawnienia danych z testów osobom nieuprawnionym*[13].

Testowanie cyfrowej odporności podmiotów finansowych na gruncie prawa krajowego

Rozporządzenie DORA wykreowało nowe otoczenie regulacyjne dla podmiotów finansowych oraz KNF jako organu odpowiedzialnego za nadzór nad jego przestrzeganiem. Przepisy rozporządzenia są stosowane bezpośrednio, jednak niektóre z nich wymagają wprowadzenia zmian w krajowym porządku prawnym, zwłaszcza w odniesieniu do wyznaczenia organów właściwych oraz nałożenia obowiązków na podmioty finansowe[14].

Pierwszy projekt ustawy wdrażający przywołane regulacje prawa unijnego został przedłożony przez Ministra Finansów w kwietniu 2024 r.[15] Proces legislacyjny trwał ponad rok, co budzi pytania w kontekście pilności wprowadzenia tej regulacji. Opieszałość decydentów spowodowała, że pod koniec marca 2025 r. Komisja Europejska

[13] Tamże, s. 285.

[14] *Ustawa wdrażająca DORA do prawa polskiego*, „Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [dostęp: 12 IV 2025].

[15] *Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji*, druk nr UC11, Rządowe Centrum Legislacji, Warszawa 2025.

wezwała Polskę i 12 innych państw unijnych do pełnego wdrożenia rozporządzenia DORA w ramach krajowych systemów prawnych[16]. Rządowy proces legislacyjny zakończył się w kwietniu 2025 r. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego został zaakceptowany przez Stały Komitet Rady Ministrów. Ustawę wdrażającą rozporządzenie DORA uchwalono w czerwcu 2025 r.[17]

Z perspektywy celu tego artykułu najważniejsze zmiany dotyczą wprowadzenia art. 18zk do *Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym*. Przepis ten reguluje zadania KNF w zakresie przeprowadzenia testów, o których mowa w art. 26 rozporządzenia DORA, oraz sposób postępowania podmiotów finansowych zobowiązanych do ich przeprowadzania. Na mocy tego przepisu organ nadzoru stał się organem odpowiedzialnym za realizację obowiązków organu właściwego, wskazanych w art. 26 i art. 27 rozporządzenia DORA. W świetle powyższego KNF wyposażono w ustawowe uprawnienie do wyznaczania – w drodze decyzji – podmiotu finansowego zobowiązanego do przeprowadzenia testów TLPT. Artykuł 18zk powiela kryteria wyboru podmiotów obowiązanych do przeprowadzenia tych testów z uwzględnieniem zasady proporcjonalności (art. 4 ust. 2 rozporządzenia DORA).

Podmioty, w stosunku do których KNF wydała wspomnianą decyzję, są zobowiązane do przekazywania organowi nadzoru, w celu zatwierdzenia, wyniku oceny dokonanej zgodnie z art. 26 ust. 2 akapit trzeci rozporządzenia DORA. Wynik ten wskazuje, które krytyczne lub istotne funkcje należy objąć testami TLPT. Po ich przeprowadzeniu, uzgodnieniu sprawozdań i planów naprawczych podmiot finansowy i – w stosownych przypadkach – testerzy zewnętrzni będą zobowiązani do przedstawienia KNF podsumowania ustaleń, planów naprawczych i dokumentacji potwierdzającej, że testy TLPT zostały zrealizowane zgodnie z wymogami rozporządzenia DORA. Obowiązkiem organu nadzoru – w świetle art. 18zk ust. 4 – będzie potwierdzanie tej zgodności. Ma to umożliwić wzajemne uznawanie testów penetracyjnych przez właściwe organy.

Komisji Nadzoru Finansowego przyznano również kompetencje w zakresie zmniejszania lub zwiększenia częstotliwości przeprowadzania testów TLPT oraz legitymację do zatwierdzania zamiaru korzystania przez podmiot finansowy z usług testerów wewnętrznych. Jej odpowiedzialnością jest ponadto weryfikacja, czy testerzy wewnętrzni spełniają wymagania rozporządzenia DORA. Realizacja tego

[16] Na liście państw, które nie wdrożyły rozporządzenia, znalazły się również: Belgia, Bułgaria, Dania, Grecja, Hiszpania, Francja, Litwa, Łotwa, Malta, Portugalia, Rumunia i Słowenia.

[17] *Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji*.

obowiązku – w świetle nieostrych wymagań art. 27 rozporządzenia DORA – może powodować istotne problemy. Można jednak założyć, że w interesie podmiotów finansowych leży zapewnienie odpowiedniej jakości zasobów do realizacji testów TLPT. Jakość tych testów wpływa bowiem na zwiększenie poziomu odporności cyfrowej, a tym samym na szeroko pojęte bezpieczeństwo podmiotu finansowego.

Regulacyjne standardy techniczne w zakresie testów TLPT

W art. 26 ust. 11 rozporządzenia DORA prawodawca unijny zdecydował, że europejskie urzędy nadzoru (EUN) w porozumieniu z Europejskim Bankiem Centralnym opracują wspólne projekty regulacyjnych standardów technicznych (regulatory technical standards, RTS)[18] zgodne z ramami frameworku TIBER-EU (European framework for threat intelligence-based ethical red teaming). W RTS mają zostać doprecyzowane następujące elementy:

- kryteria wykorzystywane do celów stosowania ust. 8 akapit drugi rozporządzenia DORA,
- kryteria określające sposoby identyfikacji i notyfikacji podmiotów zobowiązanych do realizacji testów TLPT,
- role i obowiązki poszczególnych zespołów uczestniczących w testach,
- wymogi i standardy regulujące korzystanie z testerów wewnętrznych,
- wymogi dotyczące:
  - zakresu TLPT,
  - metodyki testowania i podejścia, które należy stosować na każdym konkretnym etapie testowania,
  - etapów testów odnoszących się do wyników, zamykania testów oraz środków naprawczych,
- rodzaj współpracy w zakresie nadzoru i inne odpowiednie rodzaje współpracy potrzebne do przeprowadzenia testów TLPT i do ułatwienia wzajemnego uznawania takiego testowania w kontekście podmiotów finansowych, które działają w więcej niż jednym państwie członkowskim. Ma to umożliwić odpowiedni poziom zaangażowania organów nadzoru i elastyczne

[18] Regulacyjne standardy techniczne nakładają szczegółowe wymagania techniczne dotyczące wdrożenia przepisów. Są bardziej normatywne i koncentrują się na praktycznych aspektach implementacji rozporządzenia DORA. Z kolei wykonawcze standardy techniczne (implementing technical standards, ITS) zajmują się ujednoliceniem i standaryzacją procesów wdrażania tych przepisów w UE i mają charakter bardziej proceduralny. Skupiają się dużo bardziej na odpowiednim sposobie raportowania do właściwych organów nadzoru.

wdrażanie, uwzględniające specyfikę podsektorów finansowych lub lokalnych rynków finansowych.

W lipcu 2024 r. EUN zaprezentowały finalny raport z konsultacji RTS w sprawie testów TLPT[19].

Testy TLPT a TIBER-EU

Zanim zostaną omówione zależności między testami TLPT a TIBER-EU[20], konieczne jest krótkie scharakteryzowanie założeń tego dokumentu. Framework TIBER-EU został powołany w 2018 r. przez Europejski Bank Centralny w celu usystematyzowania i ujednolicenia podejścia i realizacji realistycznych testów penetracyjnych w organizacjach z sektora finansowego państw członkowskich UE[21]. TIBER-EU definiuje model testów/operacji red teamowych poprzedzonych przeprowadzeniem rozpoznania i analizy danych na temat zagrożeń ukierunkowanych na testowany podmiot. Stanowi on fundament wymagań dotyczących realizacji testów TLPT. W początkowym etapie istniały różnice pomiędzy założeniami tego dokumentu a wymaganiami określonymi w rozporządzeniu DORA. Główna polegała na odmiennym podejściu do przeprowadzania testów z udziałem testerów wewnętrznych. TIBER-EU pierwotnie nie dopuszczał takiego rozwiązania, a w testach TLPT jest ono akceptowalne pod warunkiem spełnienia określonych kryteriów. Framework TIBER-EU został zaktualizowany w 2025 r. i jego obecna wersja odzwierciedla wymagania wynikające z rozporządzenia DORA[22]. Można zatem uznać, że aktualny TIBER-EU to podręcznik do realizacji testów TLPT. Podczas gdy

[19] *Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554*, European Banking Authority, 17 July 2024.

[20] Na temat założeń TIBER-EU zob. szerzej: T. Valkeasuo, *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023; M. Bayle de Jessé, *The Eurosystem's cyber resilience strategy for financial market infrastructures*, „Cyber Security: A Peer-Reviewed Journal" 2019, t. 2, nr 4, s. 294–302. https://doi.org/10.69554/DFBJ2963; B.F. Scott, *Red teaming financial crime risks in the banking sector*, „Journal of Financial Crime" 2021, t. 28, nr 1, s. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

[21] *TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym*, Z-LABS, 8 VII 2024 r., https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [dostęp: 19 IV 2025].

[22] *TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [dostęp: 9 II 2026].

rozporządzenie DORA określa, co musi zostać wykonane w ramach testów TLPT, TIBER-EU wskazuje, jak należy to zrobić.

Framework TIBER-EU również zakłada możliwość lokalnej implementacji, żeby lepiej dopasować go do specyfiki danego kraju[23]. Według stanu na kwiecień 2025 r. na implementację zdecydowały się m.in.: Austria, Belgia, Holandia, Francja, Niemcy, Dania, Finlandia, Szwecja i Norwegia.

Dokumentacja TIBER-EU obejmuje liczne opracowania, które mogą być przydatne w trakcie realizacji zarówno testów TLPT, jak i TIBER-EU. Do najważniejszych można zaliczyć:

- *TIBER-EU Guidance for Service Provider Procurement*[24] – zbiór dobrych praktyk w zakresie realizacji procesów zamówień usług red team oraz threat intelligence provider,
- *TIBER-EU Purple-Teaming Guidance*[25] – zbiór dobrych praktyk dotyczących realizacji ćwiczeń purple team, które odbywają się po testach red team,
- *TIBER-EU Scope Specification Document Guidance*[26] – wytyczne odnośnie do odpowiedniego doboru zakresu testów,
- *TIBER-EU Test Summary Report Guidance*[27] – wytyczne na temat opracowania raportu podsumowującego testy.

Główne założenia TIBER-EU to:

- testy oparte na rzeczywistych zagrożeniach (threat intelligence) – scenariusze testowe uwzględniające aktualne informacje o zagrożeniach,
- symulacja rzeczywistych ataków (red teaming) – kontrolowany test, w którym red team symuluje działania cyberprzestępców,
- ochrona krytycznych funkcji – sprawdzenie odporności na ataki dotyczące najważniejszych funkcji biznesowych,

---

[23] *Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce*, Komisja Nadzoru Finansowego, 27 I 2025 r., https://www.knf.gov.pl/?articleId=91971&p_id=18 [dostęp: 19 IV 2025].

[24] *TIBER-EU Guidance for Service Provider Procurement*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [dostęp: 19 IV 2025].

[25] *TIBER-EU Purple Teaming Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [dostęp: 19 IV 2025].

[26] *TIBER-EU Scope Specification Document Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [dostęp: 19 IV 2025].

[27] *TIBER-EU Test Summary Report Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [dostęp: 19 IV 2025].

- współpraca i zgoda – instytucja finansowa dobrowolnie zgadza się na udział w testach,
- standaryzacja i możliwość wdrożenia w różnych krajach UE – model ramowy adaptowany na poziomie krajowym,
- uczenie się i poprawa – faza analizy i nauki (lessons learned) jako istotny element TIBER-EU.

Zespoły realizujące testy TLPT

Jak już wspomniano, testy TLPT cechują się wysoką złożonością. Wymagają różnych kompetencji i umiejętności członków zespołu. Bardzo ważne jest precyzyjne określenie ról, odpowiedzialności i obowiązków zaangażowanych osób i zespołów. Zwiększa to szansę, że każdy aspekt testu będzie dobrze zarządzony, a kolejne działania będą realizowane zgodnie z przyjętym harmonogramem. Precyzyjne zdefiniowanie i przypisanie ról to lepsza koordynacja działań, minimalizacja ryzyka błędów oraz szybkie zidentyfikowanie i odpowiednie zaadresowanie każdego problemu.

Podstawowy model podziału ról, odpowiedzialności i obowiązków zakłada istnienie następujących zespołów:

- TLPT cyber team (TCT),
- control team (CT) znany również jako white team,
- blue team (BT),
- threat intelligence provider (TIP),
- red team (RT),
- purple team (PT).

TLPT cyber team – jest wyznaczany przez uprawniony organ nadzorujący test. Odpowiada za monitorowanie i ocenę prawidłowości przeprowadzania testów, a także ich rzetelne i bezpieczne wykonanie. Powinien zadbać również o to, aby wszystkie aspekty testu były zrealizowane zgodnie z planem, co minimalizuje ryzyko błędów i nieprawidłowości.

Control team (white team) – odgrywa kluczową rolę, gdyż odpowiada za koordynowanie realizacji testów po stronie podmiotu finansowego – planowanie, monitorowanie i zarządzanie ich wszystkimi aspektami. W pracach CT uczestniczą menadżerowie wyższego szczebla i eksperci, którzy dysponują wiedzą na temat infrastruktury oraz procesów operacyjnych organizacji. Zespół odpowiada także za ochronę integralności i stabilności systemów produkcyjnych podczas testowania. Jako jedyny ma informacje na temat szczegółów testów, co pozwala mu na obiektywną ocenę reakcji pracowników organizacji na symulowane zagrożenia.

Blue team – odpowiada za zarządzanie cyberbezpieczeństwem wewnętrznym organizacji i zapewnienie jego odpowiedniego poziomu. Najważniejszym zadaniem tego zespołu jest monitorowanie potencjalnych zagrożeń i reagowanie na nie w czasie rzeczywistym oraz utrzymywanie ochrony systemów i danych przed cyberatakami. Zespół ten nie jest informowany o szczegółach realizowanych testów, co ma pozwolić na przeprowadzenie symulacji w warunkach jak najbardziej zbliżonych do rzeczywistych. Dzięki temu można ocenić reakcje zespołu organizacji na zagrożenia oraz sprawdzić skuteczność istniejących procedur i mechanizmów obronnych, a tym samym lepiej zrozumieć rzeczywisty poziom przygotowania organizacji na incydenty związane z ICT.

Threat intelligence provider – odpowiada za zbieranie informacji o zagrożeniach dotyczących organizacji, przy czym korzysta z metod takich jak OSINT (open source intelligence). Gromadzi dane wywiadowcze, analizuje dostępne źródła publiczne oraz inne źródła informacji, aby stworzyć kompleksowy obraz zagrożeń mogących wpłynąć na organizację. Zespół TIP ma dostarczyć dokładne i aktualne informacje, które pomogą w opracowaniu realistycznych scenariuszy ataków realizowanych przez RT. Dzięki temu testy są lepiej dopasowane do zagrożeń, z jakimi może się zmierzyć organizacja.

Red team – realizuje testy bezpieczeństwa zgodnie z przyjętymi i zaakceptowanymi scenariuszami, wykorzystując informacje, materiały i dane dostarczone przez TIP. Głównym zadaniem RT jest symulowanie rzeczywistych ataków na systemy organizacji, aby ocenić, jak skutecznie potrafią one wykrywać zagrożenia i reagować na nie. Testowane są zarówno zabezpieczenia techniczne, jak i organizacyjne. Holistyczne podejście ma umożliwić identyfikację potencjalnych słabości i luk w zabezpieczeniach organizacji. Red team wykorzystuje różne techniki i metody ataków, aby testy były jak najbardziej realistyczne i skuteczne. Od jakości pracy RT zależy wiarygodność uzyskanych wyników testów. Im ta jakość jest wyższa, tym większa jest szansa na eliminację potencjalnych zagrożeń, mitygację zidentyfikowanych ryzyk oraz wzmocnienie poziomu bezpieczeństwa w kontekście funkcjonowania organizacji.

Purple team – składa się z członków zespołów RT i BT. Zadaniem PT jest analizowanie wyników uzyskanych z testów, identyfikowanie obszarów do poprawy oraz formułowanie rekomendacji, które pomogą wzmocnić zabezpieczenia organizacji. Dzięki współpracy obu zespołów można trafniej ocenić skuteczność istniejących mechanizmów obronnych i zaproponować konkretne działania usprawniające zarówno techniczne, jak i proceduralne aspekty bezpieczeństwa.

Etapy realizacji testów TLPT

Z uwagi na skomplikowaną i wieloaspektową naturę testów TLPT są one realizowane w trzech kolejnych etapach: przygotowanie do testów, ich zrealizowanie i podsumowanie. Podejście to zwiększa szanse przeprowadzenia rzetelnej i pogłębionej oceny odporności organizacji na różne typy zagrożeń.

W etapie pierwszym, czyli przygotowawczym, są przeprowadzane następujące działania:

- spotkania wstępne podmiotu realizującego testy z organem nadzorującym i zespołem TCT, aby omówić i uzgodnić szczegóły dotyczące testów, w tym cele, metodologię oraz kryteria oceny;
- określenie zakresu testu, tj. obszarów do testowania oraz potencjalnych zagrożeń, które mają zostać uwzględnione. W tym kroku również są ustalane cele testu, a także oczekiwane wyniki;
- procesy zakupowe, aby wyłonić odpowiednie zespoły RT oraz TIP. Wybór tych zespołów ma decydujące znaczenie dla zapewnienia wysokiej jakości testów i realistycznych scenariuszy ataków;
- przygotowanie dokumentacji, w której są określone wszystkie aspekty testów, w tym harmonogram, zasady komunikacji oraz procedury bezpieczeństwa. Dokumentacja ta stanowi podstawę dla kolejnych etapów testowania i potwierdza, że wszystkie strony są zgodne co do oczekiwań i obowiązków.

Etap drugi, w ramach którego są realizowane główne działania testowe, obejmuje:

- opracowanie raportu TTI (targeted threat intelligence) i scenariuszy ataku – zespół TIP przygotowuje raport dotyczący ukierunkowanych zagrożeń TTI oraz wstępne scenariusze ataku. Raport ten zawiera szczegółowe informacje na temat potencjalnych zagrożeń oraz wektorów ataków mogących wpływać na organizację. Na tej podstawie zespół TIP tworzy realistyczne scenariusze ataków, które będą wykorzystywane w dalszej części testowania;
- przeprowadzenie testów przez RT z uwzględnieniem scenariuszy opracowanych przez zespół TIP, co pozwala na dokładną ocenę odporności systemów i procedur organizacji. Red team wykorzystuje różne techniki i metody ataków, aby sprawdzić, jak skutecznie organizacja radzi sobie z zagrożeniami.

Etap trzeci to podsumowanie i analiza uzyskanych wyników testów, a także opracowanie rekomendacji. Składa się na to:

- opracowanie raportów przez zespoły RT i BT. Zawierają one analizy wyników, opis przeprowadzonych scenariuszy ataku oraz ocenę efektywności reakcji i obrony. Dokumenty te są podstawą do dalszej analizy i wniosków dotyczących bezpieczeństwa organizacji;
- przeprowadzenie warsztatów purple teaming, w ramach których zespoły RT i BT omawiają zrealizowane scenariusze ataku, aby wymienić między sobą informacje i doświadczenia. Pozwala to na lepsze zrozumienie skuteczności testów oraz identyfikację obszarów do poprawy, jak również pomaga w opracowaniu praktycznych rekomendacji oraz planów usprawnień;
- przygotowanie końcowego raportu z realizacji testów TLPT na podstawie raportów zespołów RT i BT oraz wyników warsztatów. Obejmuje on podsumowanie całokształtu przeprowadzonych działań, wnioski z testów oraz zalecenia dotyczące poprawy zabezpieczeń. Dokument jest przekazywany organizacji i stanowi podstawę do wdrażania zmian w zakresie bezpieczeństwa.

Podsumowanie i wnioski

Jak wykazano w artykule, podstawowym założeniem testów TLPT jest jak najwierniejsze odwzorowanie rzeczywistych ataków. Umożliwia to sprawdzenie nie tylko efektywności zabezpieczeń systemów informatycznych, lecz także poziomu bezpieczeństwa procesów operacyjnych i świadomości pracowników w zakresie cyberzagrożeń, co zwiększa precyzję oceny odporności systemów i procedur organizacji. Ze względu na złożoność i różnorodność testów TLPT ich wdrożenie może jednak stanowić wyzwanie dla organizacji. Wymagają one starannego przygotowania i odpowiednich procedur, które zapewnią zarówno skuteczność testów, jak i bezpieczeństwo organizacji podczas ich realizacji.

Analiza przeprowadzona na potrzeby artykułu prowadzi do wniosku, że wdrożenie testów TLPT jako standardu dla podmiotów finansowych było krokiem w dobrym kierunku. Nie ulega bowiem wątpliwości, że w złożonym środowisku cyfrowym konieczne jest rozwijanie skutecznych mechanizmów zarządzania ryzykiem opartych na rzeczywistych czynnikach i wyzwaniach, a nie wyłącznie tych definiowanych na potrzeby budowania odpowiednich modeli. Autorzy podzielają stanowisko Europejskiego Banku Centralnego, który podkreśla, że testy TLPT pozwalają na weryfikowanie nie tylko środków technicznych, lecz także personelu i procesów. Bank ten słusznie zwraca uwagę, że (…) *wyniki tych testów mogą znacząco podnieść świadomość bezpieczeństwa wśród kadry kierowniczej wyższego*

szczebla testowanych podmiotów[28]. Rację ma także Wojciech Dworakowski, wskazując, że TLPT to inwestycja w bezpieczeństwo, która się zwraca, ponieważ lepiej działać proaktywnie, niż naprawiać skutki cyberataku[29].

W perspektywie kolejnych lat kluczowe będzie zapewnienie konsekwentnego i proporcjonalnego stosowania testów TLPT w całym sektorze finansowym UE. Nadzór finansowy powinien tę możliwość wykorzystywać, wspierając podmioty w przygotowaniu do tych testów oraz w rozwijaniu zdolności obrony przed cyberatakami. Weryfikacja odporności organizacji za pomocą realistycznych scenariuszy ataków powinna istotnie przyczynić się do poprawy cyberodporności całego rynku finansowego.

Bibliografia

Bayle de Jessé M., *The Eurosystem's cyber resilience strategy for financial market infrastructures*, „Cyber Security: A Peer-Reviewed Journal" 2019, t. 2, nr 4, s. 294–302. https://doi.org/10.69554/DFBJ2963.

Cichocki C., Komentarz do art. 26, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 276–282.

Cichocki C., Komentarz do art. 27, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 283–286.

Dozsa M.L., *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, praca magisterska, Oslo 2024.

Kurek-Sobieraj J., Komentarz do art. 3, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 69–106.

[28] *Opinia Europejskiego Banku Centralnego z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (CON/2021/20)*, s. 1.

[29] W. Dworakowski, *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?*, Securing, 28 II 2025 r., https://www.securing.pl/pl/threat-led-penetration-testing-tlpt-jak-byc-zgodnym-z-dora-w-2025-roku-2/#Czym-s%C4%85-testy-TLPT-i-dlaczego-s%C4%85-kluczowe-dla-DORA [dostęp: 18 IV 2025].

Riaz B., Younas Z., *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024.

Scott B.F., *Red teaming financial crime risks in the banking sector*, „Journal of Financial Crime" 2021, t. 28, nr 1, s. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

Valkeasuo T., *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023.

Źródła internetowe

Dworakowski W., *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?*, Securing, 28 II 2025 r., https://www.securing.pl/pl/threat-led-penetration-testing-tlpt-jak-byc-zgodnym-z-dora-w-2025-roku-2/#Czym-s%C4%85-testy-TLPT-i-dlaczego-s%C4%85-kluczowe-dla-DORA [dostęp: 18 IV 2025].

Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce, Komisja Nadzoru Finansowego, 27 I 2025 r., https://www.knf.gov.pl/?articleId=91971&p_id=18 [dostęp: 19 IV 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025, CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 19 I 2026].

Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA, Bankowe ABC, 2 I 2025 r., https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [dostęp: 19 IV 2025].

Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji, Komisja Nadzoru Finansowego, 14 VII 2025 r., https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [dostęp: 9 II 2026].

TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [dostęp: 9 II 2026].

TIBER-EU Guidance for Service Provider Procurement, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [dostęp: 19 IV 2025].

TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym, Z-LABS, 8 VII 2024 r., https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [dostęp: 19 IV 2025].

TIBER-EU Purple Teaming Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff-75caf6e644af0fd757415aee [dostęp: 19 IV 2025].

TIBER-EU Scope Specification Document Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [dostęp: 19 IV 2025].

TIBER-EU Test Summary Report Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [dostęp: 19 IV 2025].

Ustawa wdrażająca DORA do prawa polskiego, „Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [dostęp: 12 IV 2025].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 2022 r., ze zm.).

Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz. Urz. UE L 287 z 2013 r.).

Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (DzU z 2025 r. poz. 1069).

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. DzU z 2025 r. poz. 640, ze zm.).

Inne dokumenty

Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554, European Banking Authority, 17 July 2024.

Opinia Europejskiego Banku Centralnego z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (CON/2021/20) – (Dz. Urz. UE C 343/1 z 2021 r.).

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji, druk nr UC11, Rządowe Centrum Legislacji, Warszawa 2025.

Dr hab. Kamil Mroczka

Doktor habilitowany nauk społecznych w zakresie nauk o polityce i administracji, adiunkt w Katedrze Nauk o Państwie i Administracji Publicznej Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, absolwent programu Executive MBA. Ma wieloletnie doświadczenie na stanowiskach kierowniczych w administracji publicznej oraz w sektorze prywatnym. Obecnie zatrudniony jako Chief Compliance Officer w Santander Bank Polska.

Kontakt: ks.mroczka@uw.edu.pl

Paweł Piekutowski

Absolwent Wojskowej Akademii Technicznej. Ma wieloletnie doświadczenie w zakresie cyberbezpieczeństwa, zwłaszcza w obszarze testów penetracyjnych. Obecnie pełni funkcję zastępcy dyrektora Departamentu Cyberbezpieczeństwa w Urzędzie Komisji Nadzoru Finansowego.

Kontakt: pawel.piekutowski@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 37–56

https://doi.org/10.4467/20801335PBW.26.002.23364

ARTYKUŁ

Aspekty prawne zakazu podejmowania pracy zarobkowej i prowadzenia działalności gospodarczej przez żołnierza zawodowego

Legal aspect of prohibition on taking up gainful employment and conducting business activities by a professional soldier

MARIUSZ DOMŻALSKI

Dowództwo 18 Dywizji Zmechanizowanej
im. gen. broni Tadeusza Buka

https://orcid.org/0000-0002-7749-2598

Abstrakt

Stosunek służbowy żołnierza zawodowego odróżnia go od osób świadczących pracę ze stosunku pracy nie tylko wieloma uprawnieniami, lecz także licznymi ograniczeniami. Zawodowa służba wojskowa wymaga dyspozycyjności i charakteryzuje się m.in. podległością służbową. Jednym z ograniczeń jest także powstrzymywanie się od podejmowania zajęć zarobkowych poza służbą bez zezwolenia dowódcy jednostki wojskowej, w której żołnierz pełni służbę. W artykule dokonano analizy regulacji związanych z podejmowaniem pracy zarobkowej i prowadzeniem działalności gospodarczej przez żołnierza zawodowego. Instytucja ta została określona w art. 335 *Ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny* oraz w *Rozporządzeniu Ministra Obrony Narodowej z dnia 13 czerwca 2023 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych*. Autor porównał przepisy obowiązujące w przedmiotowym zakresie z *Ustawą z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych*.

Następnie odpowiedział na pytanie badawcze: czy ustawa o obronie Ojczyzny i powiązane z nią akty wykonawcze w odpowiedni sposób porządkują omawianą problematykę? W przeprowadzonej analizie aktów prawnych autor wykorzystał metodę formalno-dogmatyczną uzupełnioną o metodę teoretyczno-prawną. W podsumowaniu wskazał zapisy, które jego zdaniem wymagają doprecyzowania lub uzupełnienia.

Słowa kluczowe Siły Zbrojne, stosunek służbowy, dodatkowa praca zarobkowa

Abstract

The employment relationship of a professional soldier distinguishes him from persons working under an employment contract not only by numerous rights, but also by numerous restrictions. Professional military service requires availability and is characterised, among other things, by subordination in the service. One of the restrictions is also refraining from taking up additional gainful employment outside of service without the permission of the commander of the military unit in which the soldier serves. This article aims to analyse the regulations related to taking up paid employment and conducting business activity by professional soldiers. This institution is defined in Article 335 of the *Act of 11 March 2022 on the Defence of the Homeland* and in the *Regulation of the Minister of National Defence of 13 June 2023 on the performance of paid employment or conducting business activity by professional soldiers*. The author compared the applicable regulations in this regard with the repealed *Act of 11 September 2003 on the military service of professional soldiers*. He then answered the research question whether the *Act on the Defence of the Homeland* and related implementing regulations adequately regulate the discussed issues? In the analysis of legal acts, the author used a formal-dogmatic method supplemented by a theoretical-legal method. In summary, he pointed out provisions which, in his opinion, require clarification of supplementation.

Keywords Armed Forces, employment relationship, additional gainful employment

Wprowadzenie

Możliwość wykonywania dodatkowej pracy zarobkowej i prowadzenia działalności gospodarczej przez żołnierza zawodowego należy traktować jako wyjątek od zasady całkowitego poświęcenia się pełnionej zawodowej służbie wojskowej, która to zasada wynika z funkcji sił zbrojnych w państwie. Znajduje to odzwierciedlenie w art. 65 ust. 1 w związku z art. 31 ust. 3 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. Zgodnie z tymi przepisami każdemu zapewnia się wolność wyboru i wykonywania zawodu oraz wyboru miejsca pracy, a (…) *ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw*. Dopuszczalne jest zatem istnienie pewnych kategorii zatrudnionych, wobec których ograniczenia będą większe ze względu na charakter pełnionych przez nich funkcji[1]. Do tych osób należą żołnierze zawodowi. W ich przypadku ograniczenia korzystania z konstytucyjnych wolności wynikają z charakteru służby i specyfiki armii jako pracodawcy, która polega na hierarchicznym podporządkowaniu, rozkazodawstwie oraz jednoosobowym dowodzeniu[2]. Zakaz dodatkowej pracy jest konsekwencją uwarunkowań takich jak dyspozycyjność, apolityczność oraz prestiż służby.

Zgodnie z art. 335 ust. 1 *Ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny* (dalej: ustawa o obronie Ojczyzny) żołnierzowi zawodowemu nie wolno podejmować pracy zarobkowej i prowadzić działalności gospodarczej. Analogiczną regulację zawierała obowiązująca wcześniej *Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych* (dalej: ustawa o służbie wojskowej).

Praca zarobkowa żołnierza zawodowego

Praca w znaczeniu świadczenia usług czy produkcji dóbr nie prowadzi bezpośrednio do księgowego ujęcia aktywów w bilansie podmiotu świadczącego pracę, np. pracownika. Z jego perspektywy jest to zazwyczaj zamiana czasu i umiejętności na dochód (płacę), który następnie może, ale nie musi, zostać przekształcony w aktywa

[1] P. Pakuła-Gawarecka, *Zakres przedmiotowy i podmiotowy zakazu podejmowania dodatkowych zajęć przez funkcjonariuszy Policji*, „Roczniki Administracji i Prawa" 2015, nr 15(2), s. 282.

[2] M. Domżalski, *Neutralność polityczna sił zbrojnych w wymiarze prawnokonstytucyjnym*, „Wrocławskie Studia Politologiczne" 2023, nr 32, s. 13. https://doi.org/10.19195/1643-0328.32.1.

trwałe lub obrotowe. Dopiero otrzymana płaca staje się aktywami obrotowymi, czyli gotówką lub środkami na rachunku bankowym. Moment powstania aktywów jest przesunięty w czasie względem samego aktu pracy (od wykonania usługi do otrzymania zapłaty). Jednocześnie należy podkreślić, że nie każde działanie żołnierza, którego efektem będzie otrzymanie dochodu, jest traktowane jako praca zarobkowa.

Przykładowo pracą zarobkową nie jest przysporzenie wynikające z rozporządzania swoim majątkiem, takie jak np. zakładanie rachunków oszczędnościowych i inne formy przewidziane prawem bankowym, a mające na celu osiągnięcie korzyści finansowych. Mimo że głównym celem tego typu działań jest uzyskanie dochodu, należy je traktować jako formę inwestycji posiadanych aktywów pieniężnych. Innymi słowy, dochód w tym przypadku nie ma związku z działalnością żołnierza, a powstaje na skutek powierzenia instytucji finansowej pewnej sumy pieniędzy w zamian za otrzymanie dochodu.

Definicja pojęcia zatrudnienia występuje w art. 2 pkt 51 *Ustawy z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia*. Wskazuje się tam, że jest to (…) *wykonywanie pracy na podstawie stosunku pracy, stosunku służbowego lub umowy o pracę nakładczą*. W orzecznictwie termin „praca zarobkowa" jest rozumiany jako wszelkie formy zatrudnienia połączone z uzyskiwaniem dochodów, czyli działalność gospodarcza, stosunek pracy, stosunek służbowy oraz każdy rodzaj umowy cywilnoprawnej, jak również członkostwo w organach statutowych jakichkolwiek instytucji, jeżeli jest to połączone z uzyskiwaniem stałych lub okresowych dochodów pieniężnych. Pracą zarobkową będzie również świadczenie pracy za wynagrodzeniem bez podpisania umowy, która precyzowałaby warunki wykonywanej działalności[3].

Niezbędnym elementem zakwalifikowania czynności realizowanych przez żołnierza do działalności zarobkowej jest otrzymywanie przez niego wynagrodzenia lub świadczeń pieniężnych za wykonaną pracę. Standardem w tym zakresie są gwarancje wynikające z prawa pracownika do godziwego wynagrodzenia. To pojęcie występuje w aktach prawa międzynarodowego, do których należą: Powszechna Deklaracja Praw Człowieka z 1948 r. (art. 23)[4], Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych z 1966 r. (art. 7)[5], Europejska Karta Społeczna z 1961 r.

[3] Wyrok Wojewódzkiego Sądu Administracyjnego (dalej: WSA) w Szczecinie z 7 V 2008 r., sygn. II SA/Sz 99/08, LEX nr 515274; wyrok WSA w Szczecinie z 25 I 2017 r., sygn. II SA/Sz 1395/16, LEX nr 2237739; wyrok WSA w Poznaniu z 8 X 2015 r., sygn. IV SA/Po 467/15, LEX nr 1933084.

[4] *Powszechna Deklaracja Praw Człowieka*, Paryż, 10 XII 1948 r., https://libr.sejm.gov.pl/tek01/txt/onz/1948.html [dostęp: 1 VII 2025].

[5] *Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.*

(art. 4)[6] oraz konwencje Międzynarodowej Organizacji Pracy[7]. Co do zasady w przypadku stosunku pracy pracodawca ma prawo korzystania z pracy świadczonej przez pracownika, w zamian za co jest zobowiązany do wypłaty mu wynagrodzenia (art. 22 § 1 *Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy*). Wynagrodzenie za pracę obejmuje wszystkie świadczenia, zarówno pieniężne, jak i niepieniężne, otrzymywane przez pracownika od pracodawcy z tytułu pozostawania w stosunku pracy. Kodeks pracy stanowi o odpłatnym charakterze stosunku pracy, co odróżnia stosunki pracy od stosunków cywilnoprawnych[8], np. umowy o dzieło czy umowy zlecenia. Świadczenia z tego tytułu mają charakter świadczeń cywilnych, stąd też nie podlegają rygorom oraz ochronie przewidzianej przez przepisy prawa pracy[9].

Działalność gospodarcza żołnierza zawodowego

Zgodnie z art. 3 *Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* (dalej: ustawa Prawo przedsiębiorców) działalnością gospodarczą jest zorganizowana działalność zarobkowa, wykonywana we własnym imieniu i w sposób ciągły. Sąd Najwyższy w jednej ze swoich uchwał stwierdził, że (…) *działalnością gospodarczą jest działalność wykazująca zawodowy, a więc stały charakter, podporządkowanie regułom opłacalności i zysku lub zasadzie racjonalnego gospodarowania, działanie na własny rachunek oraz uczestnictwo w obrocie gospodarczym*[10].

Zorganizowany charakter działalności gospodarczej oznacza wpisanie obranego rodzaju działalności w formalne ramy organizacyjne, które (…) *oznaczają np. ustanowienie określonej formy prawnej, utworzenie siedziby, zorganizowanie biura bądź innych pomieszczeń do prowadzenia działalności, zatrudnianie pracowników i ustanowienie wewnątrzzakładowych uregulowań prawnych*[11]. W orzecznictwie sądowym utrwalił się pogląd, że w ocenie, czy mamy do czynienia z prowadzeniem działalności gospodarczej, należy uwzględnić takie cechy jak ciągłość i zorganizowanie, bez względu na to, czy podmiot faktycznie jest zarejestrowany. Wymienione

---

6 *Europejska Karta Społeczna sporządzona w Turynie dnia 18 października 1961 r.*

7 K. Prokop, *Konstytucyjne prawo do godziwego wynagrodzenia za pracę*, „Białostockie Studia Prawnicze" 2021, t. 26, nr 2, s. 120. https://doi.org/10.15290/bsp.2021.26.02.08.

8 M. Liskowski, *Pojęcie wynagrodzenia za pracę w Kodeksie pracy*, „Pracownik i Pracodawca" 2016, nr 2, s. 35. https://doi.org/10.12775/PiP.2016.012; zob. także: E. Beck-Krala, *Wynagrodzenie pracowników w organizacji. Teoria i praktyka*, Kraków 2013.

9 A. Górnicz-Mulcahy, *„Własność" wynagrodzenia za pracę*, w: *Własność w prawie i gospodarce*, U. Kalina-Prasznic (red.), Wrocław 2017, s. 162.

10 Uchwała Sądu Najwyższego (dalej: SN) z 23 II 2005 r., sygn. III CZP 88/04, LEX nr 143136, s. 5–6.

11 Wyrok SN z 6 IV 2017 r., sygn. II UK 98/16, LEX nr 2307127.

cechy działalności są kategorią obiektywną, niezależną od tego, jak daną czynność ocenia wykonujący ją podmiot[12].

Kolejną cechą odróżniającą działalność gospodarczą od innych aktywności jest jej zarobkowy charakter. *Dana działalność jest zarobkowa, jeżeli jest prowadzona w celu osiągnięcia dochodu (zarobku) rozumianego jako nadwyżka przychodów nad poniesionymi kosztami. Działalność pozbawiona tego aspektu jest działalnością charytatywną, społeczną, kulturalną i inną (określaną mianem non profit)*[13].

Działalność gospodarcza ma być wykonywana we własnym imieniu, czyli samodzielnie, na własne ryzyko oraz na własną odpowiedzialność. Osobę fizyczną, która prowadzi działalność samodzielnie i niezależnie od innych podmiotów, można uznać za odrębny podmiot gospodarczy[14].

Ostatnią z przesłanek warunkujących zakwalifikowanie działalności jako działalności gospodarczej jest jej ciągłość. *Przedsiębiorcą będzie więc tylko ten, kto wykonuje czynności powtarzalne i w taki sposób, że tworzą one pewną całość, a nie stanowią oderwanego świadczenia czy świadczeń określonych rzeczy lub usług. Jeżeli takie działania mają charakter gospodarczy lub zawodowy, istnieją podstawy do uznania, że podejmujący je podmiot jest przedsiębiorcą*[15]. Sporadyczna działalność nie jest działalnością gospodarczą[16]. Granica między sporadycznym wykonywaniem czynności a planowym (zorganizowanym), ale przerywanym prowadzeniem działalności gospodarczej, opiera się w Polsce na definicji działalności gospodarczej (ciągłość, zorganizowanie, cel zarobkowy) oraz limitach przychodów dla działalności nieewidencjonowanej. Do zachowania ciągłości wystarczy, aby z całokształtu okoliczności wynikał zamiar powtarzania określonego zespołu konkretnych działań w celu osiągnięcia zarobku. Powinna to być działalność stała, planowa (celowa), przy czym obojętne jest, czy plan obejmuje dłuższy czy krótszy okres. Nie jest natomiast wymagane nieprzerwane prowadzenie działalności[17].

Aby określona aktywność została uznana za działalność gospodarczą, wskazane przesłanki (działalność zorganizowana, ciągła, prowadzona we własnym imieniu i dla osiągnięcia zysku) muszą być spełnione łącznie. Brak którejkolwiek z nich oznacza, że danej działalności nie można zakwalifikować do kategorii działalności gospodarczej.

---

[12] Wyrok WSA w Opolu z 7 V 2008 r., sygn. I SA/Op 18/08, LEX nr 484040.

[13] Wyrok Naczelnego Sądu Administracyjnego (dalej: NSA) z 26 IX 2008 r., sygn. II FSK 789/07, LEX nr 495147. Por. wyrok WSA w Warszawie z 8 X 2004 r., sygn. II SA 3673/03, LEX nr 159913.

[14] Wyrok NSA z 1 X 1997 r., sygn. II SA 1811/96, LEX nr 33310.

[15] Postanowienie Sądu Apelacyjnego w Szczecinie z 7 VIII 2006 r., sygn. I ACz 441/06, LEX nr 279953.

[16] Wyrok NSA z 17 IX 1997 r., sygn. II SA 1089/96, LEX nr 31312.

[17] Wyrok WSA we Wrocławiu z 27 IV 2005 r., sygn. I SA/Wr 3237/03, LEX nr 496830.

Inne formy pracy zarobkowej żołnierza zawodowego

Na kanwie analizowanej problematyki interesujące jest zagadnienie działalności nieewidencjonowanej uregulowanej w art. 5 ustawy Prawo przedsiębiorców. Działalność nieewidencjonowana jest definiowana przez trzy przesłanki:

1) podmiotową, która odwołuje się do faktu wykonywania działalności przez osobę fizyczną;
2) przychodową, opierającą się na zastrzeżeniu, że przychód należny z tej działalności nie przekracza w żadnym kwartale 225% kwoty minimalnego wynagrodzenia, o którym mowa w *Ustawie z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę*;
3) formalną, czyli wykazania, że podmiot, który wykonuje taką działalność, w ciągu ostatnich 60 miesięcy nie wykonywał działalności gospodarczej.

Działalność nieewidencjonowana formalnie nie jest działalnością gospodarczą, ale jest działalnością zarobkową, jest wykonywana osobiście oraz może naruszać warunki wymienione w art. 335 ust. 3 ustawy o obronie Ojczyzny, np. kolidować z wykonywaniem zadań służbowych czy naruszać prestiż żołnierza zawodowego. Dlatego nawet przy działalności nieewidencjonowanej, chociaż przepisy nie wymagają na nią zgody dowódcy, żołnierz musi brać pod uwagę ograniczenia wynikające z przywołanego artykułu. Jednocześnie należy pamiętać, że zgodnie z art. 5 ust. 3 ustawy Prawo przedsiębiorców, jeśli w danym kwartale przychód przekroczy 225% minimalnego wynagrodzenia, działalność nieewidencjonowana z mocy prawa staje się działalnością gospodarczą od dnia, w którym nastąpiło przekroczenie tej kwoty. W takiej sytuacji żołnierz zawodowy musi otrzymać zgodę dowódcy jednostki wojskowej. Jej brak jest naruszeniem art. 335 ust. 1 ustawy o obronie Ojczyzny, co może skutkować postępowaniem dyscyplinarnym lub cofnięciem – jeśli wcześniej była udzielona – zgody na inne formy działalności. Jeżeli żołnierz uzyska zgodę na prowadzenie działalności gospodarczej, może w jej ramach dalej wykonywać czynności, które do tej pory wykonywał jako działalność nieewidencjonowaną.

Dodatkowe zarobkowanie żołnierza zawodowego de iure

Ustawodawca przewidział możliwość podjęcia przez żołnierza zawodowego dodatkowej pracy zarobkowej i prowadzenia działalności gospodarczej pod warunkiem złożenia przez niego wniosku o udzielenie na to zgody do dowódcy swojej jednostki wojskowej. Zgodnie z definicją zawartą w art. 2 ustawy o obronie Ojczyzny dowódca jednostki wojskowej to osoba kierująca lub dowodząca jednostką wojskową,

w której żołnierz zajmuje stanowisko służbowe lub do której został skierowany w ramach pełnienia zawodowej służby wojskowej w dyspozycji.

Szczegółowe warunki i tryb postępowania w sprawach udzielania żołnierzom zawodowym zezwoleń na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej oraz dane, jakie ma zawierać wniosek żołnierza o zezwolenie na pracę lub prowadzenie działalności gospodarczej, określa *Rozporządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2023 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych* (dalej: rozporządzenie w sprawie wykonywania pracy). Na podstawie delegacji zawartej w art. 56 ustawy o służbie wojskowej wydano *Rozporządzenie Ministra Obrony Narodowej z dnia 7 października 2009 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych*.

Pisemny wniosek o zezwolenie na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej żołnierz zawodowy składa wyłącznie w swoim imieniu drogą służbową. Oznacza to, że tego działania nie może podjąć ustanowiony przez żołnierza pełnomocnik, jak również nie można go przeprowadzić w imieniu lub interesie osoby trzeciej. Droga służbowa oznacza zaopiniowanie wniosku przez każdego przełożonego wnioskującego żołnierza, dzięki czemu bezpośredni przełożony, który ma najpełniejszą wiedzę na temat żołnierza, może stwierdzić, czy dodatkowa działalność podwładnego nie będzie kolidowała z wykonywanymi przez niego obowiązkami służbowymi[18].

Warto zauważyć, że brakuje podstawy prawnej do rozstrzygania przez dowódcę jednostki wojskowej w sprawie wniosku żołnierza zawodowego o udzielenie zgody na wykonywanie pracy zarobkowej w drodze decyzji administracyjnej, tj. w trybie przepisów *Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego* (dalej: k.p.a.). Ta sprawa należy do spraw wewnętrznych wynikających z podległości służbowej i powinna zostać załatwiona na drodze służbowej, a nie w formie decyzji administracyjnej. Od rozstrzygnięcia (decyzji) dowódcy jednostki wojskowej nie przysługuje odwołanie do organu wyższego stopnia, a w konsekwencji jego rozpoznanie w trybie skargi złożonej do sądu administracyjnego[19]. Decyzja dotycząca załatwienia sprawy ze stosunku służbowego żołnierza zawodowego musi wynikać z obowiązującego przepisu, a nie z k.p.a.[20] W rozporządzeniu w sprawie

[18] P. Gacek, *Dodatkowe zajęcie zarobkowe poza służbą (art. 62 ust. 1 ustawy o Policji) – wybrane zagadnienia proceduralne*, „Ius et Administratio" 2017, nr 1, s. 6.

[19] Wyrok WSA w Bydgoszczy z 22 I 2013 r., sygn. II SA/Bd 1012/12, LEX nr 1351366.

[20] Postanowienie NSA z 23 VIII 2012 r., sygn. I OSK 1649/12, LEX nr 1331525; postanowienie NSA z 26 IV 2006 r., sygn. I OSK 303/06, LEX nr 203585; postanowienie WSA w Poznaniu z 15 I 2010 r., sygn. II SA/Po 882/09, LEX nr 635705; postanowienie WSA w Białymstoku z 19 III 2013 r., sygn. II SA/Bk 171/13, LEX nr 1301609.

wykonywania pracy nie podano terminu, w którym trzeba zakończyć procedurę udzielenia zgody bądź odmowy na prowadzenie pracy zarobkowej lub prowadzenie działalności gospodarczej. Należy jednak uznać, że dowódca jednostki wojskowej powinien podjąć decyzję przed datą wskazaną przez żołnierza we wniosku jako data rozpoczęcia pracy/działalności gospodarczej, z tym zastrzeżeniem, że wniosek musi zostać złożony odpowiednio wcześniej.

W § 3 ust. 2 pkt 1 rozporządzenia w sprawie wykonywania pracy wskazano, że w przypadku pracy zarobkowej wniosek zawiera:

a) stopień, imię i nazwisko żołnierza,
b) nazwę podmiotu, u którego będzie świadczona praca zarobkowa, i adres jego siedziby albo imię i nazwisko osoby, u której będzie świadczona praca zarobkowa, i miejsce zamieszkania tej osoby,
c) podstawę wykonywanej pracy (w ramach stosunku pracy lub na podstawie innego tytułu),
d) miejsce wykonywania pracy,
e) okres, na jaki podmiot, o którym mowa w lit. b, zamierza zawrzeć umowę o pracę lub umowę na podstawie innego tytułu,
f) wymiar czasu pracy,
g) rozkład czasu służby w tygodniu wraz z ustaleniem zadań służbowych w ramach 40 godzin w 5-dniowym tygodniu służby,
h) charakter wykonywanej pracy,
i) termin rozpoczęcia pracy.

Zgodnie z § 3 ust. 2 pkt 2 rozporządzenia w sprawie wykonywania pracy wniosek o uzyskanie zgody na prowadzenie działalności gospodarczej zawiera:

a) stopień, imię i nazwisko żołnierza,
b) określenie przedmiotu prowadzonej działalności gospodarczej, zgodnie z Polską Klasyfikacją Działalności, i adres siedziby lub miejsce zamieszkania podmiotu prowadzącego działalność gospodarczą,
c) adres, pod którym będzie wykonywana działalność gospodarcza,
d) formę prawną wykonywanej działalności gospodarczej,
e) wymiar czasu niezbędny do wykonywania działalności gospodarczej,
f) termin rozpoczęcia wykonywania działalności gospodarczej.

W myśl § 3 ust. 2 pkt 3 rozporządzenia w sprawie wykonywania pracy razem z wnioskiem żołnierz składa obowiązkowe oświadczenie, że (…) *prowadzona działalność gospodarcza lub działalność podmiotu, u którego będzie świadczona praca, nie dotyczy wyrobów, o których mowa w przepisach w sprawie klasyfikacji wyrobów obronnych oraz dostaw, robót budowlanych i usług, przeznaczonych na zamówienie jednostek wojskowych*. Szczegółowe zasady kodyfikacji wyrobów obronnych określa *Decyzja Nr 115/MON Ministra Obrony Narodowej z dnia 18 września 2024 r.*

w sprawie Systemu Kodyfikacji Wyrobów Obronnych. Jest to regulacja późniejsza w stosunku do ustawy. Ani w ustawie o służbie wojskowej, ani w ustawie o obronie Ojczyzny nie przewidziano możliwości prowadzenia działalności zarobkowej związanej z wyrobami obronnymi oraz dostawami, robotami budowlanymi i usługami przeznaczonymi na zamówienie jednostek wojskowych. Nie wymagano też od żołnierza złożenia oświadczenia w tym zakresie.

W art. 56 ust. 3 ustawy o służbie wojskowej oraz w art. 335 ust. 3 ustawy o obronie Ojczyzny ustawodawca wskazał, że dowódca jednostki wojskowej może zezwolić żołnierzowi na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, jeżeli:

1) nie koliduje to z wykonywaniem zadań służbowych przez żołnierza;
2) wpływa na podwyższenie jego kwalifikacji;
3) nie narusza to prestiżu żołnierza zawodowego;
4) prowadzona działalność gospodarcza lub działalność podmiotu, u którego będzie świadczona praca, nie dotyczy wyrobów, o których mowa w przepisach w sprawie klasyfikacji wyrobów obronnych oraz dostaw, robót budowlanych i usług, przeznaczonych na zamówienie jednostek wojskowych.

Dodatkowa praca żołnierza nie może zatem negatywnie wpływać na jego dyspozycyjność, powinna natomiast podwyższać jego kwalifikacje. Daje to np. praca w charakterze wykładowcy czy ratownika medycznego.

W jednym z orzeczeń sądów administracyjnych na kanwie ustawy o służbie wojskowej wskazano negatywną przesłankę w postaci naruszenia prestiżu żołnierza zawodowego:

> Służba wojskowa żołnierza zawodowego, jak sama nazwa wskazuje, nie jest pracą zawodową[,] lecz służbą charakteryzującą się zdyscyplinowaniem, lojalnością i poświęceniem. Żołnierze zawodowi są żołnierzami w czynnej służbie wojskowej. Ich wymiar czasu służby jest określany zadaniami służbowymi trudnymi do przewidzenia i zaplanowania. Posyłani są na najtrudniejsze odcinki zabezpieczające niepodległość Ojczyzny, ale także zapewniają bezpieczeństwo obywateli z gotowością poniesienia ofiary życia włącznie. Ich podstawy powinności określa Konstytucja Rzeczypospolitej i ustawa o służbie wojskowej żołnierzy zawodowych. Nie można zatem zgodzić się ze skarżącym, że prowadzona przez niego działalność gospodarcza nie koliduje ze służbą wojskową i że status sprzedawcy w sklepie komputerowym posiada taki sam prestiż jak żołnierz zawodowy[21].

[21] Wyrok WSA w Gorzowie Wielkopolskim z 25 XI 2009 r., sygn. II SA/Go 676/09, LEX nr 589116.

Na podstawie § 3 ust. 4 rozporządzenia w sprawie wykonywania pracy, dowódca jednostki wojskowej może zwrócić się do przyszłego pracodawcy żołnierza o udzielenie (…) *informacji dotyczących charakteru pracy, jaka będzie wykonywana przez żołnierza, stosowanego rozkładu czasu pracy oraz możliwości wykonywania na polecenie pracodawcy zadań służbowych poza stałym miejscem pracy, w tym poza granicami kraju*.

Przy podejmowaniu decyzji dowódca jednostki wojskowej musi rozważyć wszelkie przesłanki warunkujące wydanie zgody, zarówno pozytywne, jak i negatywne dla wnioskodawcy. Musi przy tym pamiętać, że najważniejsze jest zabezpieczenie bieżącej działalności jednostki wojskowej, którą dowodzi[22]. Stwierdzenie, czy rodzaj działalności zarobkowej wykonywanej przez żołnierza koliduje z wykonywaniem przez niego obowiązków służbowych, należy wyłącznie do dowódcy jednostki wojskowej[23].

Gdy dojdzie do naruszenia warunków uzyskania zgody, dowódca jednostki wojskowej bezzwłocznie cofa zezwolenie na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, przy czym zapewnia żołnierzowi czas potrzebny do rozwiązania umowy o pracę lub innej umowy, na podstawie której żołnierz wykonuje pracę zarobkową[24], albo do zakończenia prowadzenia działalności gospodarczej (§ 10 rozporządzenia w sprawie wykonywania pracy). W rozporządzeniu tym są wskazane warunki odmowy lub cofnięcia zezwolenia na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej. Różnica między aktualnie obowiązującym rozporządzeniem a wcześniejszymi przepisami polega na tym, że dowódca cofa zezwolenie bezzwłocznie, czyli jest to obligatoryjne. W poprzednich regulacjach wskazano, że dowódca może cofnąć zgodę, więc było to uprawnienie realizowane uznaniowo.

W przypadku pracy zarobkowej podejmowanej przez żołnierza w ramach umowy o pracę lub prowadzenia działalności gospodarczej dowódca jednostki wojskowej musi wyrazić na nią zgodę niezależnie od okresu, na jaki zostanie zawarta umowa o pracę lub przewidywanego okresu prowadzenia działalności. W przypadku innego tytułu, np. umowy zlecenia czy umowy o dzieło, obowiązek uzyskania zgody będzie dotyczył umów zawartych na okres dłuższy niż miesiąc.

W poprzednio obowiązujących przepisach nie przewidziano konieczności informowania dowódcy jednostki wojskowej, w której żołnierz zajmuje stanowisko służbowe, o nazwie podmiotu, u którego ten żołnierz wykonywał odpłatne prace

---

[22] P. Palka, *Dodatkowa praca zarobkowa żołnierzy zawodowych (uwagi de lege lata)*, „Wojskowy Przegląd Prawniczy" 2006, nr 2, s. 35; M. Czechowski, *Prawny charakter zatrudnienia żołnierzy zawodowych*, Toruń 2016, s. 224–227.

[23] Wyrok NSA z 9 II 2001 r., sygn. II SA 3072/00, LEX nr 53672.

[24] Wyrok WSA w Warszawie z 14 IV 2008 r., sygn. II SA/Wa 1842/07, LEX nr 480072.

przez okres nie dłuższy niż miesiąc, w terminie nie dłuższym niż miesiąc od dnia rozpoczęcia wykonywania tych prac. Obecnie nie trzeba informować o rodzaju pracy, wynagrodzeniu i wymiarze pracy – obowiązkowe jest jedynie wskazanie podmiotu, wobec którego żołnierz świadczył pracę.

Warto zauważyć, że praca zarobkowa nie może być wykonywana przez żołnierza zawodowego w innej jednostce wojskowej, chyba że uzyska on zgodę Ministra Obrony Narodowej na podjęcie tej pracy, z wyłączeniem zatrudnienia w uczelni wojskowej jako wykładowcy prowadzącego zajęcia dydaktyczne. Zgodnie z definicją zawartą w art. 2 ustawy o obronie Ojczyzny przez jednostkę wojskową należy rozumieć (…) *jednostkę organizacyjną Sił Zbrojnych oraz komórkę organizacyjną funkcjonujące na podstawie nadanego przez Ministra Obrony Narodowej etatu, posługujące się pieczęcią urzędową z godłem Rzeczypospolitej Polskiej i nazwą (numerem) jednostki*. Żołnierz zawodowy nie może wykonywać dodatkowej pracy zarobkowej w jednostce wojskowej, w której pełni służbę.

W sytuacji gdy praca zarobkowa, którą podejmuje żołnierz, ma być wykonywana w innej jednostce wojskowej, zgodnie z § 4 rozporządzenia w sprawie wykonywania pracy żołnierz musi złożyć wniosek (…) *do Ministra Obrony Narodowej za pośrednictwem dowódcy jednostki wojskowej, w której zajmuje stanowisko służbowe lub do której został skierowany w ramach pełnienia zawodowej służby wojskowej w dyspozycji. Dowódca przesyła wniosek wraz ze swoją opinią na jego temat do Ministra Obrony Narodowej za pośrednictwem kierownika komórki organizacyjnej Ministerstwa Obrony Narodowej właściwej do spraw kadr*. Decyzja ministra o wyrażeniu lub niewyrażeniu zgody jest przekazywana żołnierzowi również przez dowódcę. Dodatkowo, już po uzyskaniu przez żołnierza zezwolenia na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, dowódca jednostki wojskowej może zażądać od niego (…) *przedstawienia do wglądu umowy o pracę lub innej umowy, na podstawie której żołnierz wykonuje pracę zarobkową, lub wydruków z rejestru przedsiębiorców Krajowego Rejestru Sądowego, lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej* (§ 5 rozporządzenia w sprawie wykonywania pracy).

W ustawie o służbie wojskowej dodatkowa praca zarobkowa żołnierza w jednostce wojskowej była uregulowana w odmienny sposób. Zgodnie z art. 56 ust. 3a i 3b przywołanej ustawy, taka praca nie mogła być wykonywana przez żołnierza zawodowego w jednostce wojskowej, w której żołnierz ten pełnił służbę, oraz jednostce wojskowej bezpośrednio podległej, z zastrzeżeniem sytuacji, gdy praca była podejmowana w jednostce niebędącej jednostką budżetową, na podstawie innej niż umowa o pracę. W opinii autora obecne przepisy w tej materii są bardziej przejrzyste – wniosek musi zostać złożony do Ministra Obrony Narodowej, podczas gdy wcześniej decyzję o zgodzie na dodatkową pracę mógł podejmować organ, który równocześnie mógł być dodatkowym pracodawcą żołnierza.

Zgodnie z § 9 ust. 1 rozporządzenia w sprawie wykonywania pracy:

> W przypadku wyznaczenia żołnierza, któremu wydano zezwolenie na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, na stanowisko służbowe w innej jednostce wojskowej lub w przypadku skierowania go do innej jednostki wojskowej w ramach pełnienia zawodowej służby wojskowej w dyspozycji żołnierz zainteresowany kontynuacją wykonywania pracy zarobkowej lub prowadzeniem działalności gospodarczej występuje z wnioskiem do tego dowódcy jednostki wojskowej w terminie 14 dni od dnia objęcia obowiązków na stanowisku służbowym lub dnia stawienia się w jednostce wojskowej w ramach pełnienia zawodowej służby wojskowej w dyspozycji. Do czasu wydania przez dowódcę jednostki wojskowej lub Ministra Obrony Narodowej rozstrzygnięcia w tej sprawie żołnierz wykonuje pracę lub prowadzi działalność gospodarczą na podstawie dotychczasowego zezwolenia.

Podobnie jak w przypadku cofnięcia zezwolenia na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, dowódca jednostki wojskowej zapewnia żołnierzowi odpowiedni czas potrzebny do rozwiązania umowy o pracę lub innej umowy, na podstawie której żołnierz wykonuje pracę zarobkową, albo do zakończenia prowadzenia działalności gospodarczej (§ 10 ust. 3 rozporządzenia w sprawie wykonywania pracy). W ustawie o służbie wojskowej oraz w *Rozporządzeniu Ministra Obrony Narodowej z dnia 7 października 2009 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych* brakowało regulacji w tym zakresie. Niewątpliwie ta zmiana korzystnie wpływa na stabilność finansową żołnierza. W tym miejscu warto zauważyć, że ruchy kadrowe w Siłach Zbrojnych RP są bardzo częste, stąd też ta regulacja nabiera szczególnego wymiaru praktycznego.

Zgodnie z § 6 rozporządzenia w sprawie wykonywania pracy:

1. Żołnierz, który uzyskał zezwolenie na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej, niezwłocznie powiadamia na piśmie dowódcę jednostki wojskowej o:
   1) niepodjęciu pracy zarobkowej;
   2) przerwaniu pracy zarobkowej;
   3) zakończeniu pracy zarobkowej;
   4) niepodjęciu prowadzenia działalności gospodarczej;
   5) zakończeniu prowadzenia działalności gospodarczej;
   6) zawieszeniu prowadzenia działalności gospodarczej;
   7) wznowieniu prowadzenia działalności gospodarczej.
2. W przypadkach, o których mowa w pkt 1–5, dowódca jednostki wojskowej stwierdza wygaśnięcie zezwolenia na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej.

Ustawodawca odmiennie uregulował wykonywanie przez żołnierza zawodowego odpłatnych prac przez okres krótszy niż miesiąc. W takim przypadku żołnierz zawodowy jest obowiązany przekazać dowódcy jednostki wojskowej, w której zajmuje stanowisko służbowe, informację o nazwie podmiotu, u którego wykonywał te prace, w terminie nie dłuższym niż miesiąc od dnia rozpoczęcia ich wykonywania. Pomimo formalnego braku konieczności posiadania zgody od dowódcy jednostki wojskowej żołnierzowi zawodowemu nie wolno wykonywać odpłatnych prac w okresach krótszych niż miesiąc, jeżeli kolidowałoby to z wykonywaniem przez niego zadań służbowych, naruszało prestiż służby lub praca dotyczyłaby wyrobów, o których mowa w przepisach w sprawie klasyfikacji wyrobów obronnych oraz dostaw, robót budowlanych i usług, przeznaczonych na zamówienie jednostek wojskowych.

Należy zwrócić uwagę, że zgodnie z art. 547 ustawy o obronie Ojczyzny w razie ogłoszenia mobilizacji, ogłoszenia stanu wojennego i w czasie wojny do żołnierzy zawodowych nie stosuje się m.in. art. 335 dotyczącego możliwości podjęcia przez nich dodatkowej pracy zarobkowej. Jest to odzwierciedlenie priorytetu interesu państwa nad indywidualnym interesem żołnierza, szczególnie w momencie wystąpienia stanów zagrożenia.

Zgodnie z art. 353 ust. 1 ustawy o obronie Ojczyzny: (…) *naruszenie dyscypliny wojskowej stanowi czyn żołnierza polegający na zachowaniu godzącym w dobre imię lub interes Sił Zbrojnych, zawinionym przekroczeniu uprawnień albo niewykonaniu obowiązków wynikających z przepisów prawa, w tym z rozkazów i poleceń wydanych przez przełożonych uprawnionych na podstawie tych przepisów*. Natomiast art. 353 ust. 2 pkt 2 wspomnianej ustawy stanowi, że naruszeniem dyscypliny wojskowej jest w szczególności: (…) *niedopełnienie obowiązków żołnierza wynikających ze złożonej przysięgi wojskowej, a także z przepisów prawa, regulaminów wojskowych i zasad etyki wojskowej*. Wobec tych regulacji należy uznać, że podjęcie przez żołnierza zawodowego dodatkowej pracy zarobkowej bądź prowadzenie działalności gospodarczej bez zgody dowódcy jednostki wojskowej jest deliktem dyscyplinarnym. Warto w tym miejscu przytoczyć wyrok – wydany co prawda na kanwie ustawy o Policji, ale sentencja będzie miała odniesienie również do żołnierzy zawodowych – Wojewódzkiego Sądu Administracyjnego w Lublinie:

> (…) zgodnie z art. 62 ust. 1 ustawy o Policji, policjant nie może podejmować zajęcia zarobkowego poza służbą bez pisemnej zgody przełożonego ani wykonywać czynności lub zajęć sprzecznych z obowiązkami wynikającymi z ustawy lub podważających zaufanie do Policji. Zgodnie zaś z zapisem art. 132 ust. 1 i 2 ustawy o Policji, policjant odpowiada dyscyplinarnie za popełnienie przewinienia dyscyplinarnego polegającego na naruszeniu dyscypliny służbowej lub nieprzestrzeganiu zasad etyki zawodowej. Naruszeniem dyscypliny służbowej jest czyn policjanta polegający na zawinionym przekroczeniu uprawnień lub

niewykonaniu obowiązków wynikających z przepisów prawa lub rozkazów i poleceń wydanych przez przełożonych uprawnionych na podstawie tych przepisów[25].

Norma dyscyplinarna należy do szerszego zbioru regulacji dotyczących statusu służbowego żołnierzy zawodowych i jest typowym przykładem ograniczeń znanych również w innych formacjach mundurowych, np. w Policji, Agencji Bezpieczeństwa Wewnętrznego czy Straży Granicznej. Jej zadania to m.in.: eliminowanie konfliktu interesów, minimalizacja ryzyka korupcyjnego oraz zabezpieczenie zdolności operacyjnych sił zbrojnych.

Podsumowanie

Wstępując do zawodowej służby wojskowej, żołnierz musi mieć świadomość rezygnacji z niektórych uprawnień, które przysługiwały mu jako cywilowi. Wynika to z konieczności wysokiej dyspozycyjności oraz hierarchiczności występujących w armii. Jednym z takich ograniczeń jest obowiązek powstrzymania się przez żołnierza zawodowego od podejmowania zajęcia zarobkowego poza służbą bez pisemnej zgody dowódcy jednostki wojskowej. Ustawodawca przewidział możliwość uzyskania takiej zgody pod określonymi warunkami. Żołnierz musi złożyć drogą służbową wniosek, który zawiera dane enumeratywnie wymienione w rozporządzeniu w sprawie wykonywania pracy. Ustawodawca przewidział również możliwość cofnięcia zgody, ale tylko w przypadkach wymienionych w ustawie o obronie Ojczyzny. Istotne jest, że wobec procedury wydania zarówno zgody, jak i odmowy, a także cofnięcia zgody nie będą miały zastosowania przepisy dotyczące procedury administracyjnej.

Poprzednio obowiązująca ustawa o służbie wojskowej również zakazywała podejmowania pracy zarobkowej oraz prowadzenia działalności gospodarczej przez żołnierza zawodowego. Definicja pracy zarobkowej jest analogiczna w obu ustawach, z tym zastrzeżeniem, że w ustawie o obronie Ojczyzny jest przewidziana konieczność poinformowania dowódcy jednostki wojskowej o wykonywaniu odpłatnych prac w okresach krótszych niż miesiąc. Podobnie jak wcześniej, na wniosek żołnierza jest możliwe udzielenie mu zgody przez dowódcę jednostki na podjęcie pracy lub działalności gospodarczej, jeśli zostaną spełnione warunki braku jej kolidowania ze służbą, podnoszenia kwalifikacji, nienaruszania prestiżu oraz braku działalności w sektorze obronnym. Tryb uzyskania zgody jest identyczny w obu regulacjach. Zarówno w ustawie o obronie Ojczyzny, jak i w ustawie o służbie

[25] Wyrok WSA w Lublinie z 25 X 2007 r., sygn. III SA/Lu 422/07, LEX nr 492288.

wojskowej zostały określone procedura wniosku oraz ocena przesłanek do wydania zgody. Artykuł 335 ustawy o obronie Ojczyzny rozszerza – w porównaniu z art. 56 ustawy o służbie wojskowej – kontrolę i ograniczenia w przypadku pracy zarobkowej żołnierza w innych jednostkach wojskowych – nie wolno jej wykonywać, chyba że żołnierz uzyska zgodę Ministra Obrony Narodowej. Wyjątek stanowi praca wykładowcy na uczelni wojskowej. Niewątpliwie ten wyjątek jest formą wzmacniania potencjału edukacyjnego sił zbrojnych. W opinii autora brak jest przy tym możliwości pracy w jednostce wojskowej, w której żołnierz pełni służbę.

Należy wskazać, że przepisy pragmatyki oraz aktu wykonawczego do niej w przedmiotowej materii są uregulowane w dość jednoznaczny sposób i mają na względzie prymat służby nad indywidualnym interesem żołnierza. Większość obowiązujących przepisów dotyczących zakazu dodatkowej pracy zarobkowej żołnierzy zawodowych się nie zmieniła. Ustawa o obronie Ojczyzny wprowadza jednak w art. 335 większą precyzję i nowe uwarunkowania, np. te dotyczące pracy zarobkowej w innej jednostce wojskowej. Może to ograniczyć praktyki zatrudniania żołnierzy na dodatkowych umowach w ramach sił zbrojnych. Istotne jest również to, że w przypadku naruszenia zasad wykonywania dodatkowej pracy dowódca jednostki wojskowej jest zobowiązany do cofnięcia zezwolenia na wykonywanie pracy zarobkowej lub prowadzenie działalności gospodarczej. W opinii autora regulacje wprowadzone w ustawie o obronie Ojczyzny spowodowały korzystne – w porównaniu z ustawą o służbie wojskowej – zmiany, które wpływają na transparentność i przejrzystość udzielania zgód na dodatkową pracę. Pozostaje jednak niedosyt w tym względzie. W zakresie udzielania zgody istnieje duża uznaniowość dowódcy. Przepis nie definiuje bowiem metody oceny kolizji pracy z obowiązkami służbowymi, co może prowadzić do różnic w praktyce dowódców różnych jednostek. Problemów interpretacyjnych może nastręczać również ocena prestiżu żołnierza w kontekście wykonywanej pracy. Jest to klauzula generalna, która wymaga wytycznych interpretacyjnych. Przepis dopuszcza pracę w uczelniach wojskowych, lecz nie wskazuje wprost na uczelnie cywilne, co prowadzi do konieczności wydawania zgód i wzmożonego nadzoru służbowego. Warto zwrócić uwagę na fakt, że realia rynku pracy stają się coraz bardziej złożone i pojawiają się nowe, elastyczne formy zarobkowania, np. freelancing, praca platformowa, gig economy, które mogą w przyszłości wymagać doprecyzowania pojęcia pracy zarobkowej lub wydania rozporządzeń wykonawczych.

Podsumowując, art. 335 ustawy o obronie Ojczyzny jest ważnym elementem stabilizującym strukturę służby zawodowej i chroniącym bezpieczeństwo państwa oraz przeciwdziałającym nadużyciom w służbie. Z naukowego punktu widzenia przepis ten spełnia wymogi konstytucyjne i wpisuje się w standardy dotyczące ograniczeń zawodowych dla członków służb mundurowych.

Bibliografia

Beck-Krala E., *Wynagrodzenie pracowników w organizacji. Teoria i praktyka*, Kraków 2013.

Czechowski M., *Prawny charakter zatrudnienia żołnierzy zawodowych*, Toruń 2016.

Domżalski M., *Neutralność polityczna sił zbrojnych w wymiarze prawnokonstytucyjnym*, „Wrocławskie Studia Politologiczne" 2023, nr 32, s. 7–20. https://doi.org/10.19195/1643-0328.32.1.

Gacek P., *Dodatkowe zajęcie zarobkowe poza służbą (art. 62 ust. 1 ustawy o Policji) – wybrane zagadnienia proceduralne*, „Ius et Administratio" 2017, nr 1, s. 1–25.

Górnicz-Mulcahy A., *„Własność" wynagrodzenia za pracę*, w: *Własność w prawie i gospodarce,* U. Kalina-Prasznic (red.), Wrocław 2017, s. 161–173.

Liskowski M., *Pojęcie wynagrodzenia za pracę w Kodeksie pracy*, „Pracownik i Pracodawca" 2016, nr 2, s. 32–42. https://doi.org/10.12775/PiP.2016.012.

Pakuła-Gawarecka P., *Zakres przedmiotowy i podmiotowy zakazu podejmowania dodatkowych zajęć przez funkcjonariuszy Policji*, „Roczniki Administracji i Prawa" 2015, nr 15(2), s. 281–298.

Palka P., *Dodatkowa praca zarobkowa żołnierzy zawodowych (uwagi de lege lata)*, „Wojskowy Przegląd Prawniczy" 2006, nr 2, s. 31–43.

Prokop K., *Konstytucyjne prawo do godziwego wynagrodzenia za pracę*, „Białostockie Studia Prawnicze" 2021, t. 26, nr 2, s. 119–135. https://doi.org/10.15290/bsp.2021.26.02.08.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (DzU z 1977 r. nr 38 poz. 169).

Europejska Karta Społeczna sporządzona w Turynie dnia 18 października 1961 r. (DzU z 1999 r. nr 8 poz. 67).

Powszechna Deklaracja Praw Człowieka, Paryż, 10 XII 1948 r., https://libr.sejm.gov.pl/tek01/txt/onz/1948.html [dostęp: 1 VII 2025].

Ustawa z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia (DzU z 2025 r. poz. 620, ze zm.).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2025 r. poz. 825, ze zm.).

Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU z 2025 r. poz. 1480, ze zm.).

Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (t.j. DzU z 2022 r. poz. 536).

Ustawa z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (t.j. DzU z 2024 r. poz. 1773).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. DzU z 2025 r. poz. 277, ze zm.).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. DzU z 2025 r. poz. 1691).

Rozporządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2023 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych (DzU z 2023 r. poz. 1217).

Rozporządzenie Ministra Obrony Narodowej z dnia 7 października 2009 r. w sprawie wykonywania pracy zarobkowej lub prowadzenia działalności gospodarczej przez żołnierzy zawodowych (DzU z 2009 r. nr 176 poz. 1366).

Decyzja Nr 115/MON Ministra Obrony Narodowej z dnia 18 września 2024 r. w sprawie Systemu Kodyfikacji Wyrobów Obronnych (Dz. Urz. MON z 2024 r. poz. 145).

Orzecznictwo

Uchwała Sądu Najwyższego z 23 II 2005 r., sygn. III CZP 88/04, LEX nr 143136.

Wyrok Sądu Najwyższego z 6 IV 2017 r., sygn. II UK 98/16, LEX nr 2307127.

Postanowienie Sądu Apelacyjnego w Szczecinie z 7 VIII 2006 r., sygn. I ACz 441/06, LEX nr 279953.

Wyrok Naczelnego Sądu Administracyjnego z 26 IX 2008 r., sygn. II FSK 789/07, LEX nr 495147.

Wyrok Naczelnego Sądu Administracyjnego z 9 II 2001 r., sygn. II SA 3072/00, LEX nr 53672.

Wyrok Naczelnego Sądu Administracyjnego z 1 X 1997 r., sygn. II SA 1811/96, LEX nr 33310.

Wyrok Naczelnego Sądu Administracyjnego z 17 IX 1997 r., sygn. II SA 1089/96, LEX nr 31312.

Postanowienie Naczelnego Sądu Administracyjnego z 23 VIII 2012 r.,
sygn. I OSK 1649/12, LEX nr 1331525.

Postanowienie Naczelnego Sądu Administracyjnego z 26 IV 2006 r.,
sygn. I OSK 303/06, LEX nr 203585.

Wyrok Wojewódzkiego Sądu Administracyjnego w Bydgoszczy z 22 I 2013 r.,
sygn. II SA/Bd 1012/12, LEX nr 1351366.

Wyrok Wojewódzkiego Sądu Administracyjnego w Gorzowie Wielkopolskim z 25 XI 2009 r., sygn. II SA/Go 676/09, LEX nr 589116.

Wyrok Wojewódzkiego Sądu Administracyjnego w Lublinie z 25 X 2007 r.,
sygn. III SA/Lu 422/07, LEX nr 492288.

Wyrok Wojewódzkiego Sądu Administracyjnego w Opolu z 7 V 2008 r.,
sygn. I SA/Op 18/08, LEX nr 484040.

Wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 8 X 2015 r.,
sygn. IV SA/Po 467/15, LEX nr 1933084.

Wyrok Wojewódzkiego Sądu Administracyjnego w Szczecinie z 25 I 2017 r.,
sygn. II SA/Sz 1395/16, LEX nr 2237739.

Wyrok Wojewódzkiego Sądu Administracyjnego w Szczecinie z 7 V 2008 r.,
sygn. II SA/Sz 99/08, LEX nr 515274.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 14 IV 2008 r.,
sygn. II SA/Wa 1842/07, LEX nr 480072.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 8 X 2004 r.,
sygn. II SA 3673/03, LEX nr 159913.

Wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z 27 IV 2005 r.,
sygn. I SA/Wr 3237/03, LEX nr 496830.

Postanowienie Wojewódzkiego Sądu Administracyjnego w Białymstoku z 19 III 2013 r.,
sygn. II SA/Bk 171/13, LEX nr 1301609.

Postanowienie Wojewódzkiego Sądu Administracyjnego w Poznaniu z 15 I 2010 r.,
sygn. II SA/Po 882/09, LEX nr 635705.

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO
2026, nr 34, s. 37–56

Mjr dr Mariusz Domżalski

Radca prawny w Dowództwie 18 Dywizji Zmechanizowanej im. gen. broni Tadeusza Buka.

Kontakt: mariuszdomzalski89@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 57–77

https://doi.org/10.4467/20801335PBW.26.003.23365

ARTYKUŁ

Funkcjonalność mobilnego laboratorium CBRNE Państwowej Straży Pożarnej w świetle przepisów prawnych oraz założeń operacyjnych Krajowego Systemu Ratowniczo-Gaśniczego

Functionality of the mobile CBRNE laboratory of the State Fire Service in the context of legal regulations and operational assumptions of the National Firefighting and Rescue System

GRZEGORZ BUGAJ

Stowarzyszenie Specjalistów ds. Bezpieczeństwa CBRNE

https://orcid.org/0000-0003-1650-023X

Abstrakt

W artykule przeanalizowano funkcjonalność mobilnego laboratorium CBRNE Państwowej Straży Pożarnej (PSP) w kontekście obowiązujących przepisów prawnych oraz założeń operacyjnych Krajowego Systemu Ratowniczo-Gaśniczego. Laboratorium to, zaprojektowane jako najwyższy poziom gotowości operacyjnej (poziom L) w strukturze ratownictwa chemicznego i ekologicznego, stanowi istotne wzmocnienie zdolności analitycznych PSP do reagowania na zagrożenia chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe. W pracy przedstawiono charakterystykę techniczną laboratorium – jego konstrukcję modułową, zaawansowane systemy filtracyjne i dekontaminacyjne oraz wyposażenie analityczne zgodne ze standardami Organizacji Traktatu Północnoatlantyckiego. Omówiono scenariusze operacyjne wykorzystania laboratorium, z uwzględnieniem identyfikacji przesyłek niebezpiecznych, oceny skażeń środowiskowych oraz reagowania

na zagrożenia radiacyjne. Przeanalizowano również wyzwania związane z funkcjonowaniem mobilnych laboratoriów, w tym kwestie formalne dotyczące klasyfikacji BSL-3, wymagania kadrowe oraz aspekty logistyczne. Podkreślono strategiczne znaczenie mobilnych laboratoriów CBRNE dla bezpieczeństwa Polski jako państwa granicznego Unii Europejskiej i NATO, zwłaszcza w świetle doświadczeń z konfliktu w Ukrainie, które wskazują, że ryzyko uwolnienia substancji toksycznych w wyniku działań wojennych jest realne.

Słowa kluczowe mobilne laboratorium CBRNE, Państwowa Straż Pożarna, bezpieczeństwo CBRNE, ratownictwo chemiczne, zagrożenia radiacyjne

Abstract The article analyses the functionality of the mobile CBRNE laboratory of the State Fire Service in the context of applicable legal regulations and operational assumptions of the National Firefighting and Rescue System. This laboratory, designed as the highest (L) level of operational readiness in the chemical and ecological rescue structure, significantly strengthens the analytical capabilities of the State Fire Service to respond to chemical, biological, radiological, nuclear and explosive threats. The paper presents a detailed technical characteristics of the laboratory, including its modular construction, advanced filtration and decontamination systems, and analytical equipment compliant with NATO standards. Operational scenarios for the laboratory's use are discussed, with particular emphasis on the identification of dangerous shipments, assessment of environmental contamination, and response to radiological threats. The article also analyses challenges related to the operation of mobile laboratories, including formal issues regarding BSL-3 classification, staffing requirements, and logistical aspects. The strategic importance of mobile CBRNE laboratories for Poland's security as a border state of the EU and NATO is emphasised, especially in light of experiences from the conflict in Ukraine, indicating the real risk of releasing toxic substances as a result of warfare.

Keywords mobile CBRNE laboratory, State Fire Service, CBRNE security, chemical rescue, radiological threats

Wprowadzenie

Zagrożenia chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe (ang. *chemical, biological, radiological, nuclear, and explosive*, CBRNE) należą do najpoważniejszych wyzwań, przed jakimi stoją współczesne systemy bezpieczeństwa powszechnego. W literaturze przedmiotu można zauważyć systematyczny wzrost zainteresowania tą problematyką, czego wyrazem jest rosnąca liczba publikacji naukowych[1].

Mobilne laboratoria CBRNE stały się przedmiotem szczegółowych badań już na początku XXI w. Przykładem mogą być projekty włoskich laboratoriów mobilnych[2] czy koncepcje Deployable Mobile CBRN Laboratory[3], rozwijane dzięki inwestycjom zwiększonym po atakach terrorystycznych w Stanach Zjednoczonych i Japonii. W Finlandii opracowano mobilne laboratorium diagnostyczne umożliwiające prowadzenie analiz w warunkach polowych. Jego przydatność oceniło NATO[4]. Rozwiązania te wpisują się w globalny trend zwiększania mobilnych zdolności analitycznych, nasilony po 2001 r. W odniesieniu do sprzętu stosowanego w mobilnych laboratoriach badania międzynarodowe koncentrują się na miniaturyzacji urządzeń analitycznych oraz zwiększaniu ich skuteczności[5]. Prowadzone są

---

1 Por. m.in.: *CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapons*, A. Richardt i in. (red.), Weinheim 2013; M. Gawlik-Kobylińska, M. Urban, G. Gudzbeler, *The EU-SENSE System as a Tool to Support Airport Security*, w: *Reliability and Statistics in Transportation and Communication: Human Sustainability and Resilience in the Digital Age*, I. Kabashkin, I. Yatskiv, O. Prentkovskis (red.), s. 597–605, seria: Lecture Notes in Networks and Systems, t. 1337, Cham 2025. https://doi.org/10.1007/978-3-031-87532-8_53; M. Urban, *Protection of Airports against the Threat of CBRNE*, „Studia Bezpieczeństwa Narodowego" 2023, t. 29, nr 3, s. 7–34. https://doi.org/10.37055/sbn/171016; *Przeciwdziałanie zagrożeniom CBRNE – aspekty teoretyczne i praktyczne*, Ł. Jureńczyk, A. Pieczywok, M. Urban (red.), Bydgoszcz 2024; A. Rabajczyk i in., *Monitoring of Selected CBRN Threats in the Air in Industrial Areas with the Use of Unmanned Aerial Vehicles*, „Atmosphere" 2020, nr 11, 1373. https://doi.org/10.3390/atmos11121373.

2 G. Mari i in., *CBRN mobile laboratories in Italy*, „Proceedings SPIE 7304, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing X" 2009, t. 7304. https://doi.org/10.1117/12.819445.

3 C. Toader i in., *Mobile Deployable Laboratory – Chemical Module*, „International Conference KNOWLEDGE-BASED ORGANIZATION" 2016, t. 22, nr 3, s. 677–680. https://doi.org/10.1515/kbo-2016-0116.

4 P.M. Kinnunen i in., *Mobile Diagnostic CBRN Field Laboratory: NATO evaluated Finnish Design*, „Challenge – Medical CBRN Defence International" 2012, nr 1.

5 Por. m.in.: D. Di Giovanni i in., *Design of Miniaturized Sensors for a Mission-Oriented UAV Application: A New Pathway for Early Warning*, „International Journal of Safety and Security Engineering" 2021, t. 11, nr 4, s. 435–444. https://doi.org/10.18280/ijsse.110417; M. Gawlik-Kobylińska i in., *The EU-SENSE System for Chemical Hazards Detection, Identification, and Monitoring*, „Applied Sciences" 2021, t. 11, nr 21, 10308. https://doi.org/10.3390/app112110308; Ł. Szklarski, *Diagnoza*

również analizy dotyczące wykorzystania mobilnych laboratoriów jako narzędzi wspierających działania ratownicze. Badania wskazują, że mobilne zdolności analityczne mają decydujące znaczenie dla skrócenia czasu reakcji i poprawy jakości decyzji operacyjnych. Potwierdzają to zarówno doświadczenia płynące z wykorzystania laboratoriów mobilnych podczas epidemii wirusa Ebola w Afryce[6], jak i wyniki projektu MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU) finansowanego przez Unię Europejską. Celem tego projektu było rozwijanie zdolności oceny zagrożeń CBRN bezpośrednio w miejscu ich wystąpienia[7].

Mobilne laboratoria CBRNE są przedmiotem systematycznych badań prowadzonych nie tylko w ramach programów ramowych UE, lecz także inicjatyw NATO. Projekty takie jak PRACTICE (Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment) czy EU-SENSE (European Sensor System for CBRN Applications) służą rozwijaniu nowych koncepcji mobilnych systemów analitycznych[8].

Sytuacja geopolityczna w Europie Środkowo-Wschodniej, na którą ma wpływ zwłaszcza konflikt w Ukrainie, generuje nowe wymagania dla systemów reagowania na zagrożenia CBRNE. Nie wszystkie kwestie zostały w pełni uwzględnione w badaniach. Literatura przedmiotu nie zawiera pogłębionych analiz dotyczących integracji mobilnych laboratoriów z systemami ratownictwa w Polsce oraz ich zgodności z krajowymi przepisami prawa i normami technicznymi. Brakuje również opracowań analizujących rzeczywiste bariery operacyjne tych laboratoriów. Możliwości urządzeń analitycznych są szczegółowo opisywane w literaturze technicznej, ale nie ma badań poświęconych wyzwaniom kadrowym, proceduralnym, logistycznym oraz organizacyjnym, które mogą mieć duży wpływ na efektywność wykorzystania w praktyce tych zaawansowanych technologicznie rozwiązań[9]. Uwagę skupia się

potrzeb w zakresie usprawnienia technologii i sprzętu służącego reagowaniu na incydenty o charakterze CBRN. Zarys problemu z perspektywy europejskich straży pożarnych, „Zeszyty Naukowe SGSP" 2021, t. 2, nr 80, s. 142–160. https://doi.org/10.5604/01.3001.0015.6474.

[6] A. Parsons i in., *Examining the utility and readiness of mobile and field transportable laboratories for biodefence and global health security-related purposes*, „Global Security: Health, Science and Policy" 2018, t. 3, nr 1, s. 1–13. https://doi.org/10.1080/23779497.2018.1480403.

[7] *Final Report Summary – MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU)*, CORDIS – EU research results, 9 II 2016 r., https://cordis.europa.eu/project/id/312885/reporting [dostęp: 25 IX 2025].

[8] Ł. Szklarski, *CBRN threats, EU-SENSE system: Paving the way for future national security systems – an assessment of the suitability of the concept for the future of national security*, „Zeszyty Naukowe SGSP" 2024, t. 2, nr 89, s. 139–156. https://doi.org/10.5604/01.3001.0054.3833.

[9] R. Jankowski, P. Wereski, *CBRNE lab*, Przegląd Pożarniczy, https://www.ppoz.pl/czytelnia/ratownictwo-i-ochrona-ludnosci/CBRNE-lab/idn:2828 [dostęp: 25 IX 2025].

przede wszystkim na ogólnych zagadnieniach z zakresu bezpieczeństwa chemicznego i ratownictwa specjalistycznego, za mało jest natomiast szczegółowych analiz poświęconych nowoczesnym rozwiązaniom technicznym wdrożonym w strukturach Państwowej Straży Pożarnej (PSP).

Problemem badawczym, z którym zmierzył się autor artykułu, było pytanie o rzeczywistą efektywność operacyjną mobilnych laboratoriów CBRNE PSP, rozumianą jako realne możliwości ich wykorzystania w działaniach ratowniczych, w kontekście rozbieżności między formalnymi wymaganiami techniczno-prawnymi a uwarunkowaniami kadrowymi, proceduralnymi, logistycznymi oraz organizacyjnymi. Rozbieżności te mogą znacznie ograniczać zdolność do skutecznego reagowania na incydenty CBRNE. Celem badań była kompleksowa analiza funkcjonalności mobilnych laboratoriów CBRNE PSP przez udzielenie odpowiedzi na następujące pytania badawcze:

1. W jakim stopniu mobilne laboratoria CBRNE PSP spełniają wymagania prawne i normatywne?
2. Jakie są rzeczywiste możliwości operacyjne mobilnych laboratoriów CBRNE PSP w kontekście założeń Krajowego Systemu Ratowniczo-Gaśniczego (KSRG)?
3. Jakie są główne wyzwania i ograniczenia w funkcjonowaniu mobilnych laboratoriów CBRNE PSP?

Autor przyjął hipotezę, że zaawansowanie technologiczne mobilnych laboratoriów CBRNE może generować wyzwania organizacyjne i operacyjne, którym sprostanie wymaga wdrożenia adekwatnych rozwiązań systemowych. Artykuł ma charakter przyczynkarski, stanowiąc studium funkcjonalności mobilnych laboratoriów CBRNE PSP, które otwiera pole do dalszych badań empirycznych nad optymalizacją wykorzystania tych laboratoriów w systemie bezpieczeństwa państwa.

Metody badawcze

Badanie oparto na analizie jakościowej dokumentów prawnych, norm technicznych oraz dokumentacji technicznej mobilnych laboratoriów CBRNE PSP. Zastosowano metodę analizy treści oraz analizę porównawczą w celu oceny zgodności rozwiązań technicznych z wymaganiami normatywnymi.

W badaniu wykorzystano następujące źródła danych:

- akty prawne: ustawa o Państwowej Straży Pożarnej oraz rozporządzenia wykonawcze dotyczące organizacji i funkcjonowania KSRG,
- dokumenty operacyjne: *Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym*,

- normy techniczne,
- dokumentację techniczną producenta laboratoriów,
- materiały audiowizualne prezentujące funkcjonalność laboratoriów.

Ocenę funkcjonalności laboratoriów CBRNE PSP przeprowadzono według następujących kryteriów:

- zgodność z przepisami prawa krajowego,
- zgodność z normami technicznymi,
- zdolności operacyjne w kontekście zadań KSRG,
- interoperacyjność z systemami krajowymi i międzynarodowymi,
- ograniczenia techniczne i organizacyjne.

Badanie opierało się głównie na analizie dokumentów i nie objęło badań empirycznych działania laboratoriów w warunkach rzeczywistych. Dostęp do niektórych dokumentów operacyjnych był ograniczony ze względu na ich niejawny charakter. Z tego faktu wynikają ograniczenia metodologiczne.

Ramy prawne i normatywne funkcjonowania w Polsce mobilnych laboratoriów CBRNE PSP

Działalność mobilnych laboratoriów CBRNE PSP jest osadzona w złożonym systemie regulacji prawnych, obejmującym zarówno przepisy krajowe, jak i normy międzynarodowe. Podstawę prawną stanowi ustawa o Państwowej Straży Pożarnej[10], która określa organizację i zakres jej działania, w tym realizację zadań z zakresu ratownictwa chemicznego i ekologicznego. Przepisy wykonawcze do tej ustawy, przede wszystkim rozporządzenie dotyczące szczegółowej organizacji KSRG, definiują zagrożenia CBRNE jako: (…) *zagrożenia powodowane przez czynniki chemiczne, biologiczne, radioaktywne, nuklearne oraz wybuchowe, które ze względu na swoje właściwości zostały użyte lub mogły zostać użyte w sposób celowy do wywołania zagrożenia dla życia i zdrowia ludzi, zwierząt oraz środowiska naturalnego*[11].

Równie istotne są *Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym*[12], które określają strukturę organizacyjną i zadania specjalistycznych grup ratownictwa chemiczno-ekologicznego

[10] *Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej*.

[11] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego*.

[12] *Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym*, Warszawa 2025.

(SGRChem-Eko) na różnych poziomach gotowości operacyjnej. W tym dokumencie wprowadzono podział na pięć poziomów gotowości:

1) poziom A – zabezpieczenie chemiczne,
2) poziom B – rozpoznanie chemiczne,
3) poziom C – rozpoznanie specjalne,
4) poziom D – dekontaminacja,
5) poziom L – analiza laboratoryjna.

Wdrożone mobilne laboratoria CBRNE PSP odpowiadają najwyższemu poziomowi gotowości (L). Analiza laboratoryjna obejmuje działania wymagające użycia zaawansowanych metod i środków analitycznych, przewyższających możliwości poziomów rozpoznania chemicznego i rozpoznania specjalnego. SGRChem-Eko poziomu gotowości L dzięki wykwalifikowanemu personelowi zapewnia wsparcie merytoryczne w interpretacji danych o zdarzeniu i wyników analizy uzyskanych przez podmioty KSRG[13].

Zakres zadań laboratorium obejmuje:

– bezpośredni udział w działaniach na miejscu zdarzenia,
– wykonanie analizy próbek dostarczonych przez jednostki włączone do KSRG,
– zdalną interpretację przesłanych wyników analizy chemicznej.

Laboratoria CBRNE PSP były projektowane zgodnie z przepisami krajowymi i normami międzynarodowymi, w tym:

– normami dotyczącymi infrastruktury laboratoryjnej i wyposażenia (PN-EN 13150:2004[14], PN-EN 14175[15], PN-EN 14727:2006[16]),
– normami dla wody, pomieszczeń czystych i dekontaminacji (PN-EN ISO 3696:1999[17], PN-EN ISO 14644[18]),

[13] Tamże, pkt 3.2.L, s. 14.

[14] PN-EN 13150:2004 – Stoły robocze dla laboratoriów – Wymiary, wymagania bezpieczeństwa i metody badań, Polski Komitet Normalizacyjny, Warszawa 2004.

[15] PN-EN 14175 (części 1–6) – Wyciągi laboratoryjne, Polski Komitet Normalizacyjny, Warszawa.

[16] PN-EN 14727:2006 – Meble laboratoryjne – Meble laboratoryjne do przechowywania – Wymagania i metody badań, Polski Komitet Normalizacyjny, Warszawa 2006.

[17] PN-EN ISO 3696:1999/Ap1:2004 – Woda stosowana w laboratoriach analitycznych – Wymagania i metody badań, Polski Komitet Normalizacyjny, Warszawa 1999/2004.

[18] PN-EN ISO 14644 – Pomieszczenia czyste i związane z nimi środowiska kontrolowane, Polski Komitet Normalizacyjny, Warszawa.

– normami biotechnologicznymi i bezpieczeństwa biologicznego (PN-EN 12128:2000[19], PN-EN 12740:2002[20], PN-EN 12469:2002[21]),
– normą dotyczącą systemów zasilania i automatyki (PN-EN 62040[22]),
– normami eksploatacyjnymi zbiorników i urządzeń pomocniczych (PN-EN 13311-1:2004[23], PN-EN 12347:2002[24]),
– normami międzynarodowymi i specjalistycznymi (DIN 16892:2000-07[25], DIN 19541:2004-09[26]).

Zgodnie z deklaracją producenta[27] mobilne laboratoria CBRNE PSP uwzględniają również standardy NATO, w tym:

– STANAG 4632[28] – Deployable NBC Analytical Laboratory,
– AEP-66[29] – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA),
– DD/3.8(B)[30] – Obrona przed bronią masowego rażenia w operacjach połączonych,

---

[19] PN-EN 12128:2000/Ap1:2001 – Biotechnologia – Laboratoria badawcze, rozwoju i analizy – Stopnie hermetyczności laboratoriów mikrobiologicznych, strefy ryzyka i wymagania względem lokalizacji i bezpieczeństwa fizycznego, Polski Komitet Normalizacyjny, Warszawa 2000/2001.

[20] PN-EN 12740:2002 – Biotechnologia – Laboratoria badawcze, rozwojowe i analityczne – Wytyczne do postępowania z odpadami, ich inaktywacji i kontroli, Polski Komitet Normalizacyjny, Warszawa 2002.

[21] PN-EN 12469:2002 – Biotechnologia – Kryteria działania komór bezpiecznej pracy mikrobiologicznej, Polski Komitet Normalizacyjny, Warszawa 2002.

[22] PN-EN 62040 – Systemy bezprzerwowego zasilania (UPS), Polski Komitet Normalizacyjny, Warszawa.

[23] PN-EN 13311-1:2004 – Biotechnologia – Kryteria eksploatacji zbiorników – Część 1: Ogólne kryteria eksploatacji; PN-EN 13311-5:2004 – Biotechnologia – Kryteria eksploatacji zbiorników – Część 5: Zbiorniki do inaktywacji, Polski Komitet Normalizacyjny, Warszawa 2004.

[24] PN-EN 12347:2002 – Biotechnologia – Kryteria działania sterylizatorów parowych i autoklawów, Polski Komitet Normalizacyjny, Warszawa 2002.

[25] DIN 16892:2000-07 – Kunststoff-Rohrleitungssysteme aus vernetztem Polyethylen (PE-X) – Allgemeine Güteanforderungen, Prüfungen, Deutsches Institut für Normung, Berlin 2000.

[26] DIN 19541:2004-09 – Abscheideranlagen für Leichtflüssigkeiten, Deutsches Institut für Normung, Berlin 2004.

[27] *PEX DEFENCE POLSKA – Prezentacja produktu Laboratorium CBRNE*, YouTube, 15 XI 2024 r., https://www.youtube.com/watch?app=desktop&v=ClJ9FZuZGQM [dostęp: 18 V 2025].

[28] STANAG 4632 (Edition 1) – *Deployable NBC Analytical Laboratory*, NATO Standardization Agency, Brussels 2005.

[29] AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA), NATO Standardization Agency, Brussels 2015.

[30] DD/3.8(B) – Obrona przed bronią masowego rażenia w operacjach połączonych, Ministerstwo Obrony Narodowej, Sztab Generalny Wojska Polskiego, Warszawa 2013.

– DD 4.10(A)[31] – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej.

Charakterystyka techniczna mobilnych laboratoriów CBRNE PSP

Laboratorium zostało zaprojektowane jako kompletny, samowystarczalny system analityczny, zdolny do realizacji pełnego procesu badawczego w warunkach terenowych. Kluczowym założeniem projektowym było skrócenie czasu między poborem próbki a uzyskaniem wiarygodnych wyników analizy, co w sytuacjach zagrożenia ma decydujące znaczenie. System podzielono na pięć głównych obszarów funkcjonalnych.

1. Czas rozstawienia i osiągnięcia gotowości operacyjnej – konstrukcja umożliwia uzyskanie wymaganych warunków klimatycznych i gotowości analitycznej w czasie nieprzekraczającym 45 minut od momentu rozstawienia (nie dotyczy urządzeń wymagających dłuższego czasu stabilizacji).
2. Kompleksowość realizowanych analiz – wyposażenie umożliwia detekcję i identyfikację substancji chemicznych, biologicznych, radiacyjnych i promieniotwórczych przy użyciu zaawansowanych urządzeń analitycznych (GC-MS, FTIR, Raman, PCR, XRF, IMS, HPGe, FPD)[32].
3. Autonomiczność i logistyka – zapewniają je agregat prądotwórczy o mocy 80 kW, systemy UPS, dekontaminacji i gospodarki ściekami, które umożliwiają długotrwałą pracę bez dostępu do infrastruktury zewnętrznej.
4. Bezpieczeństwo operatorów i środowiska – spełnienie wymagań dotyczących laboratoriów bezpieczeństwa biologicznego klasy BSL-3 (ang. *biosafety level* 3) obowiązujących przy pracy z mikroorganizmami o wysokim stopniu ryzyka, przenoszonymi drogą powietrzną. Uzyskano to dzięki zastosowaniu hermetycznych śluz osobowych, komór rękawicowych klasy III, systemów wentylacyjnych z filtrami HEPA klasy H14 oraz redundantnych zabezpieczeń.

[31] DD 4.10(A) – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2015.

[32] GC-MS (ang. *gas chromatography-mass spectrometry*) – chromatografia gazowa sprzężona ze spektrometrią mas; FTIR (ang. *Fourier transform infrared spectroscopy*) – spektroskopia w podczerwieni z transformacją Fouriera; Raman – spektroskopia Ramana; PCR (ang. *polymerase chain reaction*) – reakcja łańcuchowa polimerazy; XRF (ang. *X-ray fluorescence*) – fluorescencyjna analiza rentgenowska; IMS (ang. *ion mobility spectrometry*) – spektrometria ruchliwości jonów; HPGe – wysokorozdzielczy detektor germanowy do spektrometrii promieniowania gamma; FPD (ang. *flame photometric detector*) – płomieniowy detektor fotometryczny, selektywny m.in. względem związków siarki i fosforu, powszechnie wykorzystywany w analizie środków bojowych i toksycznych związków organicznych.

5. Interoperacyjność i zdolność integracji z innymi służbami – zgodność ze standardami NATO w zakresie rozpoznania CBRNE, zdolność do pracy na podstawie procedur SIBCRA (pobieranie próbek i identyfikacja czynników biologicznych, chemicznych i radiologicznych) oraz działania w trybie CBRN Reachback (zdalna wymiana danych, ekspertyz i konsultacji między jednostkami terenowymi a centrami analitycznymi i eksperckimi w zakresie zagrożeń CBRN).

Konstrukcja i podział funkcjonalny

Laboratorium zostało zbudowane na trzyosiowej naczepie z zawieszeniem pneumatycznym, umożliwiającej bezpieczny transport wrażliwych urządzeń analitycznych. Naczepa jest wyposażona w hydrauliczne podpory stabilizujące, pozwalające na pracę w trybie stacjonarnym bez ciągnika siodłowego.

Układ funkcjonalny laboratorium składa się z czterech głównych przedziałów.

1. Przedział operacyjny (A) – rozsuwany segment naczepy przeznaczony do zarządzania systemami pokładowymi, pełniący funkcję centrum nadzoru i bufora klimatycznego. Po rozstawieniu pojazdu konstrukcja wysuwana zwiększa przestrzeń roboczą.
2. Przedział biologiczny (B) – laboratorium spełniające warunki hermetyczności klasy BSL-3, wyposażone w komorę rękawicową klasy III, dygestorium, autoklaw, system dekontaminacji, system HVAC (ang. *heating, ventilation, air conditioning*) oraz śluzy podawczą i osobową.
3. Przedział chemiczny (C) – centralna część laboratorium przeznaczona do analiz fizykochemicznych, wyposażona w chromatografy, spektrometry, dygestorium przeciwwybuchowe oraz zlew laboratoryjny z systemem odpływu do zbiorników odpadów.
4. Strefy techniczne – zawierające instalacje wspierające (filtry, wentylacja, systemy zasilania).

Infrastruktura techniczna laboratorium obejmuje zaawansowane systemy zasilania, teleinformatyki oraz monitoringu środowiska.

Systemy filtracyjne, wentylacyjne i dekontaminacyjne

Laboratorium dysponuje zaawansowanymi układami filtracji i kontroli przepływu powietrza, dzięki którym jest zapewnione bezpieczeństwo pracy z materiałami niebezpiecznymi. System wentylacyjny został zintegrowany z zespołem filtrowentylacyjnym i generuje precyzyjnie kontrolowaną kaskadę ciśnień. Przepływ powietrza odbywa się zgodnie z zasadami strefowości i nie ma możliwości kontaminacji krzyżowej. Powietrze dostarczane do przestrzeni laboratoryjnej przechodzi przez wielostopniowy układ oczyszczania. W jego skład wchodzą filtry

wstępne oraz wysokowydajne filtry węglowe HEPA H14, spełniające wymagania normy PN 1822:2009[33]. Obudowy filtrów są zgodne z wytycznymi normy PN-EN ISO 14644-3:2020[34], co zapewnia kontrolę upływu i szczelności montażu. Konstrukcja umożliwia dekontaminację obudowy filtrów przy użyciu nadtlenku wodoru.

Centrala wentylacyjna obsługuje przepływ 1500 m^3/h, wykorzystując wyłącznie powietrze zewnętrzne. System utrzymuje precyzyjną kaskadę ciśnień – śluza osobowa funkcjonuje przy ciśnieniu odniesienia 0 Pa, a przedział biologiczny pracuje przy podciśnieniu -30 Pa.

Przedział biologiczny wyposażono w zaawansowany system dekontaminacji gazowej wykorzystujący nadtlenek wodoru. Umożliwia to pełną sterylizację przedziału, komory rękawicowej oraz elementów systemu filtracyjnego. Dekontaminacja personelu odbywa się w specjalnej śluzie osobowej z prysznicem wodnym i odzieżą ochronną. System interlock zapobiega jednoczesnemu otwarciu drzwi do stref skażenia i strefy czystej.

Wyposażenie analityczne

Mobilne laboratorium CBRNE PSP jest wyposażone w zaawansowany sprzęt analityczny umożliwiający identyfikację szerokiego spektrum zagrożeń chemicznych, biologicznych i radiacyjnych. Przy doborze aparatury kierowano się zdolnością do szybkiej i precyzyjnej identyfikacji substancji niebezpiecznych w zróżnicowanych matrycach środowiskowych.

Moduł chemiczny jest wyposażony w:

- chromatograf gazowy GC-MS z detektorami FPD i FTIR do detekcji i identyfikacji środków bojowych, pestycydów, związków aromatycznych i chlorowcopochodnych,
- spektrometr FTIR/ATR[35] wyposażony w przystawki do analizy gazów i cieczy,
- spektrofotometr UV-VIS do oznaczania zanieczyszczeń w wodzie i glebie,
- chromatograf jonowy do ilościowego oznaczania anionów i kationów w próbkach wodnych, ściekach,

[33] PN-EN 1822-1:2009 – Wysokoskuteczne filtry powietrza (EPA, HEPA i ULPA) – Część 1: Klasyfikacja, badanie parametrów, znakowanie, Polski Komitet Normalizacyjny, Warszawa 2009.

[34] PN-EN ISO 14644-3:2020 – Pomieszczenia czyste i związane z nimi środowiska kontrolowane – Część 3: Metody badań, Polski Komitet Normalizacyjny, Warszawa 2020. Norma określa metody weryfikacji szczelności, integralności montażu oraz kontroli upływów w systemach wentylacyjno-filtracyjnych, w tym badania obudów filtrów HEPA/ULPA, przepływów powietrza i różnic ciśnień.

[35] FTIR/ATR (ang. *Fourier transform infrared spectroscopy with attenuated total reflectance*) – technika spektroskopii w podczerwieni umożliwiająca bezpośrednią analizę powierzchni próbek bez ich przygotowania.

– mikroskop i ręczne spektrometry Ramana do analizy substancji stałych i materiałów wybuchowych,
– zestawy PID i IMS/AP4C do szybkiego rozpoznania substancji niebezpiecznych w powietrzu,
– spektrometry XRF do analizy składu pierwiastkowego.

Moduł biologiczny jest wyposażony w:

– urządzenie do wykrywania techniką PCR – zaawansowany system, który izoluje materiał genetyczny (DNA lub RNA[36]) i analizuje go pod kątem patogenów. Pozwala na jednoczesną identyfikację co najmniej dziesięciu różnych czynników biologicznych (uznawanych za broń biologiczną). Urządzenie jest przystosowane do bezpiecznej pracy wewnątrz komory rękawicowej w warunkach podciśnienia,
– jednorazowe testy kolorymetryczne do szybkiej, wstępnej oceny próbek, przeznaczone głównie do analizy proszków i substancji sypkich, umożliwiające wykrywanie białek, spor bakteryjnych oraz określenie odczynu pH,
– bioluminometr do wykrywania ATP[37] na powierzchniach i w próbkach ciekłych, umożliwiający szybką ocenę stopnia zanieczyszczenia biologicznego,
– homogenizator mechaniczny do przygotowania próbek biologicznych w hermetycznie zamykanych, jednorazowych probówkach, co ogranicza ryzyko uwolnienia materiału zakaźnego podczas obróbki,
– systemy przygotowania próbek, obejmujące wirówki laboratoryjne, wytrząsarki do mieszania małych objętości oraz zestaw automatycznych pipet z filtrami przystosowanych do sterylizacji w autoklawie.

Do identyfikacji zagrożeń radiacyjnych i nuklearnych służą:

– spektrometr promieniowania Polimaster (detekcja promieniowania alfa, beta, gamma i neutronów),
– przenośny spektrometr promieniowania gamma oparty na detektorze półprzewodnikowym HPGe, identyfikujący ponad 400 różnych izotopów.

Pomiary spektrometryczne są prowadzone zgodnie ze standardowymi procedurami operacyjnymi Międzynarodowej Agencji Energii Atomowej (International Atomic Energy Agency) i NATO, z czasami akwizycji od 1–5 minut (szybkie skanowanie) do 15–60 minut (dokładne analizy ilościowe). Urządzenia te są w pełni

[36] DNA (ang. *deoxyribonucleic acid*, kwas deoksyrybonukleinowy) oraz RNA (ang. *ribonucleic acid*, kwas rybonukleinowy) stanowią materiał genetyczny organizmów i wirusów. Jest on wykorzystywany w diagnostyce molekularnej do identyfikacji czynników biologicznych.

[37] ATP (ang. *adenosine triphosphate*, adenozynotrifosforan) jest uniwersalnym nośnikiem energii występującym w żywych komórkach. Jego oznaczanie metodą bioluminescencyjną stanowi niespecyficzny, szybki wskaźnik obecności aktywnego materiału biologicznego na powierzchniach i w próbkach ciekłych. Jest wykorzystywany w analizach przesiewowych skażenia biologicznego.

kompatybilne z procedurami SIBCRA oraz systemami wymiany danych w ramach CBRN Reachback.

Scenariusze operacyjne i obszary zastosowania mobilnych laboratoriów CBRNE PSP

Mobilne laboratorium CBRNE PSP zostało przewidziane do wykorzystania w następujących scenariuszach operacyjnych:

1) identyfikacja przesyłek niebezpiecznych oraz nieznanych substancji – realizowana zgodnie z procedurami Komendy Głównej PSP, obejmującymi pełny protokół zabezpieczenia materiału, jego transport i analizę[38],
2) ocena skażenia – prowadzenie analiz gleby, powietrza i wody, w tym oznaczanie obecności lotnych związków organicznych i metali ciężkich,
3) zabezpieczanie imprez masowych oraz wydarzeń wysokiego ryzyka – prewencyjne badania środowiskowe i kontrola obecności substancji niebezpiecznych,
4) wsparcie działań organów ścigania – identyfikacja materiałów wybuchowych, środków odurzających, dopalaczy oraz innych substancji.

Zgodnie z *Zasadami organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym* podczas dysponowania do bezpośrednich działań ratowniczych SGRChem-Eko poziomu gotowości L każdorazowo jest dysponowana również SGRChem-Eko poziomu gotowości B. Ma to na celu zapewnienie kompleksowego podejścia do identyfikacji zagrożeń – grupa rozpoznania chemicznego (B) wspiera działania analityczne laboratorium (L).

Szczególnym obszarem zastosowania mobilnego laboratorium CBRNE jest identyfikacja zagrożeń radiacyjnych, która polega na:

- weryfikacji na miejscu zdarzenia zgłoszenia o zagrożeniu,
- wykonaniu pomiarów radiometrycznych w celu określenia poziomu narażenia,
- wyznaczeniu obszaru, w którym występuje moc dawki promieniowania jonizującego powyżej 100 μSv/h i/lub występują skażenia promieniotwórcze,
- identyfikacji izotopów promieniotwórczych,
- współpracy z innymi służbami uczestniczącymi w działaniach.

[38] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r…*, § 16; *Zasady organizacji ratownictwa chemicznego i ekologicznego…*, załącznik nr B.2: *Zasady działań Państwowej Straży Pożarnej podczas wystąpienia zagrożenia z niezidentyfikowaną przesyłką oraz organizacja transportu materiałów biologicznych do laboratorium*.

Wyposażenie radiacyjne mobilnego laboratorium CBRNE PSP, obejmujące spektrometry promieniowania oraz detektory HPGe, umożliwia precyzyjną identyfikację izotopów promieniotwórczych, co ma zasadnicze znaczenie dla określenia charakteru zagrożenia i wyboru właściwych metod neutralizacji.

Wyzwania i ograniczenia związane z wykorzystaniem mobilnych laboratoriów CBRNE PSP

Pomimo zaawansowanych rozwiązań technicznych i wysokiego poziomu zgodności z normami wykorzystanie mobilnych laboratoriów CBRNE PSP wiąże się z pewnymi wyzwaniami i ograniczeniami. Konieczne jest ich uwzględnienie w planowaniu operacyjnym. Jedno z najważniejszych ograniczeń wynika z tego, że pomimo zaprojektowania przedziału biologicznego zgodnie z wymogami bezpieczeństwa dla laboratoriów BSL-3 mobilne laboratorium nie może być formalnie sklasyfikowane jako pełnoprawna jednostka tej klasy. Według definicji normatywnych laboratoria tego typu muszą być trwałą, nieruchomą konstrukcją budowlaną. Naczepa nie spełnia tego wymogu. Brak jest również certyfikacji walidacyjnej zgodnie z normą PN-EN ISO 14644-3:2020. Ponadto laboratorium CBRNE PSP zostało zaprojektowane do działań krótkoterminowych (akcji ratowniczych, zabezpieczeń), a nie do długotrwałego prowadzenia hodowli, badań patogenów czy pracy ze szczepami wysokiego ryzyka. Układ funkcjonalny i wykorzystane w nim technologie umożliwiają jednak skuteczne wykonywanie w warunkach terenowych analiz próbek wysokiego ryzyka, zgodnie z najlepszymi praktykami bezpieczeństwa biologicznego.

Istotnym wyzwaniem jest zapewnienie odpowiedniej kadry specjalistów do obsługi laboratorium. Według *Zasad organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym* wyznaczeni ratownicy chemiczni ze SGRChem-Eko poziomu gotowości L powinni dodatkowo mieć wykształcenie wyższe kierunkowe z chemii, fizyki lub biologii. Pozyskanie i utrzymanie tak wysoko wykwalifikowanej kadry w strukturach PSP może stanowić wyzwanie organizacyjne i finansowe. SGRChem-Eko poziomu gotowości L powinna składać się z co najmniej 12 strażaków lub ratowników, w tym z co najmniej:

1) 12 ratowników chemicznych,
2) 12 ratowników chemicznych z uprawnieniami do obsługi sprzętu specjalistycznego stanowiącego wyposażenie grupy poziomu L,
3) 6 ratowników chemicznych z uprawnieniami do obsługi pojazdów samochodowych,

4) 9 ratowników chemicznych mających wykształcenie wyższe kierunkowe z zakresu chemii, fizyki lub biologii[39].

Zapewnienie ciągłości funkcjonowania grupy przy tak wysokich wymaganiach kompetencyjnych wymaga długofalowego planowania kariery funkcjonariuszy oraz systemowego podejścia do ich rozwoju zawodowego.

Mobilne laboratorium CBRNE PSP, chociaż zaprojektowane jako jednostka autonomiczna, wymaga odpowiedniego zaplecza logistycznego. W przypadku wystąpienia skażenia spowodowanego działaniami wojennymi lub atakiem terrorystycznym laboratorium musi być w stanie operować w warunkach ograniczonego dostępu do zasobów takich jak woda czy paliwo. Wymaga to szczegółowego planowania operacyjnego i zabezpieczenia logistycznego. Realizacja zadań analitycznych w warunkach ograniczonych zasobów jest dużym wyzwaniem, zwłaszcza w kontekście możliwości zaistnienia zagrożeń chemicznych, np. w strefie działań wojennych lub w jej pobliżu. W przypadku poważniejszych incydentów z udziałem materiałów niebezpiecznych może być konieczne zadysponowanie większej liczby specjalistów oraz wykorzystanie dodatkowych zasobów analitycznych. Podjęcie bezpośrednich działań ratowniczych przez SGRChem-Eko w poziomie gotowości L jest warunkowane – jak już wspomniano – obecnością na miejscu zdarzenia SGRChem-Eko poziomu gotowości B. Takie podejście zapewnia komplementarność działań, ale wymaga koordynacji między różnymi poziomami gotowości operacyjnej i różnymi jednostkami PSP. Koniecznością są wspólne ćwiczenia i szkolenia tych jednostek. Ich brak może prowadzić do problemów komunikacyjnych, nieznajomości procedur operacyjnych oraz nieefektywnego wykorzystania zaawansowanego sprzętu analitycznego podczas rzeczywistych zdarzeń CBRNE. Tym samym potencjał mobilnego laboratorium może nie być w pełni wykorzystany, a czas reakcji na zagrożenie wydłużony. Regularne ćwiczenia integrujące różne poziomy gotowości SGRChem-Eko są niezbędnym elementem budowania spójnego i skutecznego systemu reagowania na zdarzenia z udziałem materiałów niebezpiecznych.

Perspektywy rozwoju mobilnych laboratoriów CBRNE w systemie bezpieczeństwa RP

Wdrożenie mobilnych laboratoriów CBRNE PSP stanowi ważny krok w rozwoju krajowych zdolności analitycznych, gdyż umożliwia szybką i precyzyjną identyfikację zagrożeń bezpośrednio na miejscu zdarzenia. Rozwój tych zdolności

[39] *Zasady organizacji ratownictwa chemicznego i ekologicznego*…, pkt 3.4.L, s. 19.

powinien opierać się zarówno na doświadczeniach krajowych, jak i międzynarodowych trendach w obszarze reagowania na incydenty CBRNE. Priorytetem na najbliższe lata wydaje się pogłębienie integracji mobilnych laboratoriów z wielopoziomowym systemem zarządzania kryzysowego. Dzięki zgodności z kluczowymi standardami NATO (STANAG 4632, AEP-66) oraz zdolności do współdziałania w ramach Unijnego Mechanizmu Ochrony Ludności (EU Civil Protection Mechanism) laboratoria PSP mogą efektywnie funkcjonować w europejskiej sieci reagowania kryzysowego. Taka integracja zapewnia nie tylko możliwość otrzymania międzynarodowego wsparcia w przypadku incydentów na dużą skalę, lecz także pozwala na udzielanie specjalistycznej pomocy innym państwom członkowskim UE. Szczególną wartość w kontekście rozproszonych geograficznie zasobów analitycznych ma zdolność do działania w systemie CBRN Reachback. Aby w pełni wykorzystać ten potencjał, należy rozwijać dedykowaną infrastrukturę teleinformatyczną oraz standaryzować protokoły wymiany danych analitycznych. Rozwój mobilnych laboratoriów CBRNE powinien zatem uwzględniać eksplorację nowych zastosowań i integrację z istniejącą infrastrukturą, co może znacznie zwiększyć skuteczność działań ratowniczych w przypadku incydentów związanych z materiałami CBRNE. Istotne jest, aby równolegle z rozwojem integracji systemowej modernizować wyposażenie analityczne. Ewolucja zagrożeń CBRNE, obejmująca nowe substancje i metody ich wykorzystania, wymaga ciągłego dostosowywania możliwości detekcyjnych. Kierunki rozwoju powinny uwzględniać zaawansowane techniki pomiarowe, rozwiązania wykorzystujące sztuczną inteligencję do interpretacji złożonych danych oraz systemy integrujące informacje z różnego rodzaju czujników i sensorów.

Z uwagi na położenie Polski mobilne laboratoria CBRNE nabierają dodatkowego znaczenia strategicznego. Doświadczenia płynące z wojny w Ukrainie uwypuklają wagę mobilnych zdolności analitycznych. Przypadki niszczenia infrastruktury przemysłowej, zwłaszcza w regionach zurbanizowanych, pokazują realność ryzyka uwolnienia na dużą skalę toksycznych substancji chemicznych. Zdolność do szybkiej detekcji i identyfikacji tych substancji może mieć decydujące znaczenie dla ochrony ludności cywilnej. Jako państwo graniczne zarówno UE, jak i NATO Polska może odegrać szczególną rolę w budowie regionalnego systemu reagowania na zagrożenia CBRNE. Zaawansowane zdolności analityczne mogą być elementem współpracy transgranicznej. W tym kontekście mobilne laboratoria stanowią nie tylko element krajowego systemu bezpieczeństwa, lecz także komponent potencjalnego wsparcia międzynarodowego, wzmacniający kolektywną odporność na zagrożenia asymetryczne w Europie Środkowo-Wschodniej.

Wnioski

Przeprowadzona analiza wykazała, że mobilne laboratoria PSP spełniają kluczowe wymagania normatywne oraz charakteryzują się wysokim potencjałem operacyjnym. Rozwiązania techniczne zastosowane w tych laboratoriach są zgodne z obowiązującymi przepisami prawa, normami technicznymi oraz standardami NATO, co wzmacnia interoperacyjność PSP w wymiarze krajowym i międzynarodowym. Integracja zaawansowanych systemów filtracji, hermetycznych przedziałów roboczych oraz specjalistycznego wyposażenia analitycznego umożliwia prowadzenie działań w różnych warunkach.

Zdaniem autora wyniki badań potwierdzają hipotezę, że wysoki poziom zaawansowania technologicznego mobilnych laboratoriów CBRNE powoduje wyzwania organizacyjne i operacyjne, którym sprostanie wymaga wdrożenia adekwatnych rozwiązań systemowych. Należy do nich zaliczyć konieczność zapewnienia wysoko wykwalifikowanej kadry, rozwój procedur integrujących różne poziomy SGRChem-Eko, stabilnych mechanizmów utrzymania sprzętu oraz systematycznych ćwiczeń poprawiających współdziałanie.

W obliczu dynamiki zagrożeń asymetrycznych mobilne laboratoria należy postrzegać nie tylko jako technologiczny przełom, lecz przede wszystkim jako strategiczną inwestycję w bezpieczeństwo państwa i ochronę ludności. Rozwój możliwości wykorzystania tych laboratoriów powinien obejmować modernizację aparatury, wdrażanie rozwiązań z zakresu sztucznej inteligencji oraz pogłębianie współpracy międzynarodowej, co pozwoli w pełni wykorzystać ich potencjał w systemie reagowania kryzysowego.

Bibliografia

CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapons, A. Richardt, B. Hülseweh, B. Niemeyer, F. Sabath (red.), Weinheim 2013.

Di Giovanni D., Fumian F., Chierici A., Bianchelli M., Martellucci L., Carminati G., Malizia A., d'Errico F., Gaudio P., *Design of Miniaturized Sensors for a Mission-Oriented UAV Application: A New Pathway for Early Warning*, „International Journal of Safety and Security Engineering" 2021, t. 11, nr 4, s. 435–444. https://doi.org/10.18280/ijsse.110417.

Gawlik-Kobylińska M., Gudzbeler G., Szklarski Ł., Kopp N., Koch-Eschweiler H., Urban M., *The EU-SENSE System for Chemical Hazards Detection, Identification, and Monitoring*, „Applied Sciences" 2021, t. 11, nr 21, 10308. https://doi.org/10.3390/app112110308.

Gawlik-Kobylińska M., Urban M., Gudzbeler G., *The EU-SENSE System as a Tool to Support Airport Security*, w: *Reliability and Statistics in Transportation and Communication: Human Sustainability and Resilience in the Digital Age*, I. Kabashkin, I. Yatskiv, O. Prentkovskis (red.), s. 597–605, seria: Lecture Notes in Networks and Systems, t. 1337, Cham 2025. https://doi.org/10.1007/978-3-031-87532-8_53.

Kinnunen P.M., Haataja T., Hemmila H., Maatela P., Teho K., Elo M., Raijas T., Nikkari S., *Mobile Diagnostic CBRN Field Laboratory: NATO evaluated Finnish Design*, „Challenge – Medical CBRN Defence International" 2012, nr 1.

Mari G., Giraudi G., Bellino M., Pazienza M., Garibaldi C., Lancia C., *CBRN mobile laboratories in Italy*, „Proceedings SPIE 7304, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing X" 2009, t. 7304. https://doi.org/10.1117/12.819445.

Parsons A., Matero P., Adams M., Yeh K., *Examining the utility and readiness of mobile and field transportable laboratories for biodefence and global health security-related purposes*, „Global Security: Health, Science and Policy" 2018, t. 3, nr 1, s. 1–13. https://doi.org/10.1080/23779497.2018.1480403.

Przeciwdziałanie zagrożeniom CBRNE – aspekty teoretyczne i praktyczne, Ł. Jureńczyk, A. Pieczywok, M. Urban (red.), Bydgoszcz 2024.

Rabajczyk A., Zboina J., Zielecka M., Fellner R., *Monitoring of Selected CBRN Threats in the Air in Industrial Areas with the Use of Unmanned Aerial Vehicles*, „Atmosphere" 2020, nr 11, 1373. https://doi.org/10.3390/atmos11121373.

Szklarski Ł., *CBRN threats, EU-SENSE system: Paving the way for future national security systems – an assessment of the suitability of the concept for the future of national security*, „Zeszyty Naukowe SGSP" 2024, t. 2, nr 89, s. 139–156. https://doi.org/10.5604/01.3001.0054.3833.

Szklarski Ł., *Diagnoza potrzeb w zakresie usprawnienia technologii i sprzętu służącego reagowaniu na incydenty o charakterze CBRN. Zarys problemu z perspektywy europejskich straży pożarnych*, „Zeszyty Naukowe SGSP" 2021, t. 2, nr 80, s. 142–160. https://doi.org/10.5604/01.3001.0015.6474.

Toader C., Epure G., Moşteanu D., Epure C., Iorga O., Florin I., *Mobile Deployable Laboratory – Chemical Module*, „International Conference KNOWLEDGE-BASED ORGANIZATION" 2016, t. 22, nr 3, s. 677–680. https://doi.org/10.1515/kbo-2016-0116.

Urban M., *Protection of Airports against the Threat of CBRNE*, „Studia Bezpieczeństwa Narodowego" 2023, t. 29, nr 3, s. 7–34. https://doi.org/10.37055/sbn/171016.

Źródła internetowe

Final Report Summary – MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU), CORDIS–EU research results, 9 II 2016 r., https://cordis.europa.eu/project/id/312885/reporting [dostęp: 25 IX 2025].

Jankowski R., Wereski P., *CBRNE lab*, Przegląd Pożarniczy, https://www.ppoz.pl/czytelnia/ratownictwo-i-ochrona-ludnosci/CBRNE-lab/idn:2828 [dostęp: 25 IX 2025].

PEX DEFENCE POLSKA – Prezentacja produktu Laboratorium CBRNE, YouTube, 15 XI 2024 r., https://www.youtube.com/watch?app=desktop&v=ClJ9FZuZGQM [dostęp: 18 V 2025].

Akty prawne

Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (t.j. DzU z 2025 r. poz. 1312, ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego (DzU z 2021 r. poz. 1737).

Inne dokumenty

AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA), NATO Standardization Agency, Brussels 2015.

DD/3.8(B) – Obrona przed bronią masowego rażenia w operacjach połączonych, Ministerstwo Obrony Narodowej, Sztab Generalny Wojska Polskiego, Warszawa 2013.

DD 4.10(A) – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2015.

STANAG 4632 (Edition 1) – Deployable NBC Analytical Laboratory, NATO Standardization Agency, Brussels 2005.

Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym, Warszawa 2025.

Normy polskie

PN-EN 12469:2002 – Biotechnologia – Kryteria działania komór bezpiecznej pracy mikrobiologicznej, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 12347:2002 – Biotechnologia – Kryteria działania sterylizatorów parowych i autoklawów, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 13311-1:2004 – Biotechnologia – Kryteria eksploatacji zbiorników – Część 1: Ogólne kryteria eksploatacji.

PN-EN 13311-5:2004 – Biotechnologia – Kryteria eksploatacji zbiorników – Część 5: Zbiorniki do inaktywacji, Polski Komitet Normalizacyjny, Warszawa 2004.

PN-EN 12740:2002 – Biotechnologia – Laboratoria badawcze, rozwojowe i analityczne – Wytyczne do postępowania z odpadami, ich inaktywacji i kontroli, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 12128:2000/Ap1:2001 – Biotechnologia – Laboratoria badawcze, rozwoju i analizy – Stopnie hermetyczności laboratoriów mikrobiologicznych, strefy ryzyka i wymagania względem lokalizacji i bezpieczeństwa fizycznego, Polski Komitet Normalizacyjny, Warszawa 2000/2001.

PN-EN 14727:2006 – Meble laboratoryjne – Meble laboratoryjne do przechowywania – Wymagania i metody badań, Polski Komitet Normalizacyjny, Warszawa 2006.

PN-EN ISO 14644 – Pomieszczenia czyste i związane z nimi środowiska kontrolowane, Polski Komitet Normalizacyjny, Warszawa.

PN-EN 13150:2004 – Stoły robocze dla laboratoriów – Wymiary, wymagania bezpieczeństwa i metody badań, Polski Komitet Normalizacyjny, Warszawa 2004.

PN-EN 62040 – Systemy bezprzerwowego zasilania (UPS), Polski Komitet Normalizacyjny, Warszawa.

PN-EN ISO 3696:1999/Ap1:2004 – Woda stosowana w laboratoriach analitycznych – Wymagania i metody badań, Polski Komitet Normalizacyjny, Warszawa 1999/2004.

PN-EN 14175 (części 1–6) – Wyciągi laboratoryjne, Polski Komitet Normalizacyjny, Warszawa.

PN-EN 1822-1:2009 – Wysokoskuteczne filtry powietrza (EPA, HEPA i ULPA) – Część 1: Klasyfikacja, badanie parametrów, znakowanie, Polski Komitet Normalizacyjny, Warszawa 2009.

Normy niemieckie

DIN 19541:2004-09 – Abscheideranlagen für Leichtflüssigkeiten, Deutsches Institut für Normung, Berlin 2004.

DIN 16892:2000-07 – Kunststoff-Rohrleitungssysteme aus vernetztem Polyethylen (PE-X) – Allgemeine Güteanforderungen, Prüfungen, Deutsches Institut für Normung, Berlin 2000.

St. bryg. w st. spocz. dr inż. Grzegorz Bugaj

Były Prorektor-Zastępca Komendanta Szkoły Głównej Służby Pożarniczej (obecnie Akademia Pożarnicza), wieloletni dowódca Specjalistycznej Grupy Ratownictwa Chemicznego i Jednostki Ratowniczo-Gaśniczej nr 6 w Warszawie oraz dowódca modułu „CBRN Det. Mazowsze" w Mechanizmie Ochrony Ludności UE. Ma ponadtrzydziestoletnie doświadczenie operacyjne w Państwowej Straży Pożarnej, przede wszystkim na terenie m.st. Warszawy. Absolwent Szkoły Głównej Służby Pożarniczej oraz Akademii Pożarniczej, Uniwersytetu Łódzkiego (Wydział Biologii i Ochrony Środowiska), Akademii Medycznej w Poznaniu i Centralnego Instytutu Ochrony Pracy. Obecnie prowadzi działalność ekspercką i szkoleniową.

Kontakt: g.bugaj@cbrne.org.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 79–110

https://doi.org/10.4467/20801335PBW.26.004.23366

ARTYKUŁ

Badanie retencji funkcjonariuszy Straży Granicznej w kontekście bezpieczeństwa kadrowego formacji

Study on the retention of Border Guard officers in the context of staff level security within the formation

RADOSŁAW WIŚNIEWSKI

Wyższa Szkoła Straży Granicznej

https://orcid.org/0009-0005-0751-9002

DENIS TOMALA

Wyższa Szkoła Straży Granicznej

https://orcid.org/0009-0008-0169-1612

Abstrakt

Celem badania było określenie, w jakim stopniu czynniki indywidualne i organizacyjne wpływają na retencję funkcjonariuszy Straży Granicznej. Przeanalizowano wpływ satysfakcji ze służby, zaangażowania organizacyjnego oraz wytrwałości na intencję pozostania w służbie oraz intencję odejścia z niej. Badanie przeprowadzono za pomocą kwestionariusza ankiety wśród 184 funkcjonariuszy Straży Granicznej. Zastosowano modelowanie równań strukturalnych metodą najmniejszych kwadratów cząstkowych (PLS-SEM), co umożliwiło jednoczesną analizę wielu zależności. Opracowany model charakteryzuje się dobrym dopasowaniem i wysoką mocą wyjaśniającą – zmienne ujęte w modelu tłumaczą ponad 50% wariancji intencji odejścia ze służby. Stwierdzono, że satysfakcja ze służby,

zaangażowanie organizacyjne i wytrwałość istotnie zwiększają intencję pozostania w formacji, co warto uwzględniać w rozwiązaniach przeciwdziałających odchodzeniu funkcjonariuszy ze służby.

Słowa kluczowe retencja, zaangażowanie organizacyjne, satysfakcja, wytrwałość, PLS-SEM, Straż Graniczna

Abstract The aim of the study was to determine the extent to which individual and organisational factors influence the retention of Border Guard officers. The impact of job satisfaction, organisational commitment, and perseverance on the intention to remain in service and the intention to leave service was analysed. The study was conducted among 184 Border Guard officers using a questionnaire survey. Partial least squares structural equation modeling (PLS-SEM) was used, which enabled the simultaneous analysis of multiple relationships. The developed model is characterised by a good fit and high explanatory power – the variables included in the model explain over 50% of the variance in the intention to leave the service. It was found that job satisfaction, organisational commitment, and perseverance significantly increase the intention to remain in the force, which should be taken into account in solutions to counteract the departure of officers.

Keywords retention, organisational commitment, satisfaction, perseverance, PLS-SEM, Border Guard

Wprowadzenie

Zmiany demograficzne w Polsce związane ze spadkiem liczby ludności i starzeniem się społeczeństwa powodują zmniejszanie się puli osób w wieku produkcyjnym. Efektami tych zmian są rywalizacja o kandydatów do pracy i służby oraz tworzenie rozwiązań wpływających na retencję (z łac. *retentio* – 'zatrzymanie'[1]) personelu. Zapewnienie odpowiednio liczebnej i wyszkolonej kadry koniecznej do realizacji

[1] Jeśli nie oznaczono inaczej, wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

ustawowych zadań poszczególnych formacji mundurowych stanowi zatem wyzwanie w aspekcie bezpieczeństwa kadrowego warunkującego bezpieczeństwo państwa. Problem retencji personelu jest uniwersalny i dotyczy zarówno krajowych, jak i zagranicznych służb mundurowych, które zmagają się z przedwczesnymi odejściami ze służby oraz wakatami kadrowymi. Sytuacja ta skłania do poszukiwania rozwiązań nie tylko zwiększających zainteresowanie służbą w formacjach mundurowych, lecz także optymalizujących warunki do jej pełnienia przez wiele lat. Te intencje wybrzmiewają m.in. w treści rozkazu szefa Sztabu Armii Stanów Zjednoczonych[2] oraz w poleceniu sekretarza stanu Ministerstwa Spraw Wewnętrznych i Administracji RP[3], odnoszących się do problemu utrzymania personelu. Konieczność zapewnienia bezpieczeństwa kadrowego sprawiła, że w służbach mundurowych podjęto różne inicjatywy i projekty badawcze. W armii USA są prowadzone badania retencji, które dotyczą już kilku milionów żołnierzy[4] i mają na celu ustalenie przyczyn odchodzenia ze służby. Wśród kadetów elitarnej Akademii West Point[5] identyfikowano natomiast czynniki wpływające na ukończenie nauki lub rezygnację z niej. Ponadto zespół zadaniowy państw NATO pracował nad pełnym zbadaniem mechanizmów wpływających na wyniki rekrutacji i retencję[6].

W polskich służbach mundurowych brakuje podobnych badań, dlatego też podjęcie tej problematyki wydaje się wysoce uzasadnione w odniesieniu do bezpieczeństwa kadrowego formacji i państwa oraz wydatkowania na ten cel znacznych środków budżetowych. W artykule zostały opisane badania zrealizowane w Wyższej Szkole Straży Granicznej (WSSG), przeprowadzone wśród 184 funkcjonariuszy Straży Granicznej (SG), z uwzględnieniem ich opinii, ocen oraz zamiarów związanych z kontynuacją służby lub jej zakończeniem. Problem badawczy to pytanie: jakie czynniki indywidualne i organizacyjne wpływają na intencję pozostania w służbie oraz intencję odejścia ze służby? Celem badania było zidentyfikowanie i pomiar zmiennych wpływających na intencję pozostania w służbie oraz

---

2 W.J. Strickland, *A Longitudinal Examination of First Term Attrition and Reenlistment Among FY1999 Enlisted Accessions*, https://apps.dtic.mil/sti/tr/pdf/ADA448564.pdf, s. V [dostęp: 10 I 2025].

3 Najwyższa Izba Kontroli, *Informacja o wynikach kontroli pt. Realizacja programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2017–2020*, https://www.nik.gov.pl/plik/id,21396,vp,24037.pdf, s. 158 [dostęp: 12 II 2025].

4 J.V. Marrone, *Predicting 36-Month Attrition in the U.S. Military. A Comparison Across Service Branches*, Santa Monica 2020, s. 11. https://doi.org/10.7249/RR4258.

5 D.R. Kelly, M.D. Matthews, P.T. Bartone, *Grit and Hardiness as Predictors of Performance Among West Point Cadets*, „Military Psychology" 2014, t. 26, nr 4, s. 327–342. https://doi.org/10.1037/mil0000050.

6 North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel. Final Report of Research Task Group HFM-107*, https://apps.dtic.mil/sti/tr/pdf/ADA476488.pdf [dostęp: 11 I 2025].

intencję odejścia z niej. Cel osiągnięto za pomocą metody częściowo ustrukturyzowanego wywiadu ankietowego oraz modelowania równań strukturalnych metodą najmniejszych kwadratów cząstkowych (partial least squares structural equation modeling, PLS-SEM).

Przegląd literatury

Przegląd literatury dotyczącej badań retencji personelu w służbach oraz podmiotach cywilnych pozwolił na wybór odpowiedniej metodyki i zmiennych. Analiza wykazała, że w badaniach retencji personelu jest stosowane dwukierunkowe podejście, w którym identyfikuje się czynniki wpływające na chęć pozostania w organizacji, a także ujawnia czynniki wpływające na chęć odejścia z niej[7]. Takie ujęcie problematyki bazuje na założeniach teorii planowanego zachowania (theory of planned behaviour)[8], która łączy intencje zachowania z rzeczywistym zachowaniem – co potwierdzono empirycznie[9]. Badania prowadzi się wśród osób aktualnie pracujących w instytucji czy pełniących służbę, które są pytane o zamiary pozostania w organizacji lub odejścia z niej oraz o czynniki na to wpływające. To rozwiązanie przyjęto ze względu na doświadczenia wskazujące, że osoby, które zwolniły się z organizacji, niechętnie wypowiadają się na temat przyczyn tej decyzji.

Retencja personelu jest zatem określana na podstawie deklarowanej intencji pozostania (intention to stay), rozumianej – za Robertem P. Tettem i Johnem P. Meyerem – jako zamiar odnoszący się do świadomej i celowej woli pracowników pozostania w organizacji[10], oraz intencji odejścia (intention to leave), definiowanej przez Williama H. Mobleya, Stanleya O. Hornera, Abnera T. Hollingswortha jako świadome i celowe pragnienie opuszczenia organizacji w niedalekiej

[7] Zob. m.in.: M.C. Lytell, F. Drasgow, *"Timely" Methods: Examining Turnover Rates in the U.S. Military*, „Military Psychology" 2009, t. 21, nr 3, s. 334–350. https://doi.org/10.1080/08995600902914693; T.W. Lee, T.R. Mitchell, *The unfolding effects of organizational commitment and anticipated job satisfaction on voluntary employee turnover*, „Motivation and Emotion" 1991, t. 15, nr 1, s. 99–121. https://doi.org/10.1007/BF00991478.

[8] I. Ajzen, *From Intentions to Actions: A Theory of Planned Behawior*, w: *Action Control: From Cognition to Behavior*, J. Kuhl, J. Beckmann (red.), Berlin 1985, s. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2.

[9] B.H. Sheppard, J. Hartwick, P.R. Warshaw, *The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research,* „Journal of Consumer Research" 1988, t. 15, nr 3, s. 325–343. https://doi.org/10.1086/209170.

[10] R.P. Tett, J.P. Meyer, *Job satisfaction, organizational commitment, turnover intention, and turnover: Path analyses based on meta-analytic findings*, „Personnel Psychology" 1993, t. 46, nr 2, s. 259–293. https://doi.org/10.1111/j.1744-6570.1993.tb00874.x.

przyszłości[11]. Intencja odejścia jest uznawana za bezpośredni predyktor rzeczywistej rotacji w modelach retencji (retention models)[12], co również zostało potwierdzone empirycznie[13].

Najlepiej przebadanymi i statystycznie potwierdzonymi zmiennymi wpływającymi na intencje pozostania lub odejścia (zarówno w służbach, jak i podmiotach cywilnych) są satysfakcja z pracy/służby (job satisfaction) oraz zaangażowanie organizacyjne (organizational commitment)[14]. W literaturze nie istnieje jedna ogólnie przyjęta definicja tych pojęć, a ich zakres znaczeniowy bywa zróżnicowany. Paul E. Spector definiuje satysfakcję z pracy jako odczucie dotyczące pracy i jej różnych aspektów[15], które – według Edwina A. Locke'a – zależy od tego, czy praca pozwala zaspokajać ważne dla pracownika potrzeby[16]. W badaniach satysfakcji z pracy

---

[11] W.H. Mobley, S.O. Horner, A.T. Hollingsworth, *An evaluation of precursors of hospital employee turnover*, „Journal of Applied Psychology" 1978, t. 63, nr 4, s. 408–414. https://doi.org/10.1037/0021-9010.63.4.408.

[12] D. Pitts, J. Marvel, S. Fernandez, *So Hard to Say Goodbye? Turnover Intention among U.S. Federal Employees*, „Public Administration Review" 2011, t. 71, nr 5, s. 751–760. https://doi.org/10.1111/j.1540-6210.2011.02414.x; R.W. Griffeth, P.W. Hom, S. Gaertner, *A Meta-Analysis of Antecedents and Correlates of Employee Turnover: Update, Moderator Tests, and Research Implications for the Next Millennium*, „Journal of Management" 2000, t. 26, nr 3, s. 463–488. https://doi.org/10.1177/014920630002600305.

[13] Y.J. Cho, G.B. Lewis, *Turnover Intention and Turnover Behavior: Implications for Retaining Federal Employees*, „Review of Public Personnel Administration" 2011, t. 32, nr 1, s. 4–23. https://doi.org/10.1177/0734371X11408701; A.H. Huffman i in., *The Impact of Operations Tempo on Turnover Intentions of Army Personnel*, „Military Psychology" 2005, t. 17, nr 3, s. 175–202. https://doi.org/10.1207/s15327876mp1703_4.

[14] Zob. m.in.: North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel*… s. 329; H.M. Weiss i in., *Retention in the Armed Forces: Past Approaches and New Research Directions*, https://www.mfri.purdue.edu/wp-content/uploads/2018/03/Retention-in-the-Armed-Forces.pdf [dostęp: 17 I 2025]; W.J. Strickland, *A Longitudinal Examination*…, s. 9; R.W. Griffeth, P.W. Hom, S. Gaertner, *A Meta-Analysis of Antecedents*…; D.B Currivan, *The Causal Order of Job Satisfaction and Organizational Commitment in Models of Employee Turnover*, „Human Resource Management Review" 1999, t. 9, nr 4, s. 495–524. https://doi.org/10.1016/S1053-4822(99)00031-5; T.W. Lee, T.R. Mitchell, *The unfolding effects of organizational commitment*…; S. Gaertner, *Structural Determinants of Job Satisfaction and Organizational Commitment in Turnover Models*, „Human Resource Management Review" 1999, t. 9, nr 4, s. 479–493. https://doi.org/10.1016/S1053-4822(99)00030-3; P.W. Hom i in., *A meta-analytical structural equations analysis of a model of employee turnover*, „Journal of Applied Psychology" 1992, t. 77, nr 6, s. 890–909. https://doi.org/10.1037/0021-9010.77.6.890.

[15] P.E. Spector, *The Nature of Job Satisfaction*, w: tegoż, *Job Satisfaction: Application, Assessment, Causes, and Consequences*, London 1997, s. 2. https://doi.org/10.4135/9781452231549.n1.

[16] E.A. Locke, *The Nature and Causes of Job Satisfaction*, College Park 1976, https://www.researchgate.net/publication/238742406_The_Nature_and_Causes_of_Job_Satisfaction, s. 1307 [dostęp: 13 I 2025].

często przywołuje się teorię motywacyjno-higieniczną Fredericka Herzberga, wskazującą wpływ czynników motywujących (motywatorów) na poziom satysfakcji oraz czynników higienicznych (demotywatorów) na brak satysfakcji, które łącznie wpływają na retencję personelu[17]. John P. Meyer i Natalie J. Allen określają zaangażowanie organizacyjne jako stan psychiczny charakteryzujący relację pracownika z organizacją i mający wpływ na decyzję o kontynuowaniu lub zaprzestaniu członkostwa w organizacji[18]. Składa się on z trzech wymiarów: afektywnego, kontynuacyjnego i normatywnego. Komponent afektywny odnosi się do emocjonalnego przywiązania pracownika do organizacji, identyfikacji z nią i zaangażowania w jej działalność. Komponent kontynuacyjny (kalkulacyjny) dotyczy przywiązania opartego na kosztach, jakie pracownik wiąże z opuszczeniem organizacji, komponent normatywny natomiast jest związany z poczuciem obowiązku pozostania w organizacji[19]. Dodatkowo Richard T. Mowday, Richard M. Steers i Lyman W. Porter wskazali, że zaangażowanie organizacyjne obejmuje gotowość do wysiłku na rzecz organizacji oraz wiarę w jej wartości i akceptację jej celów[20].

Obok tradycyjnie uwzględnianych czynników w badaniach retencji personelu, takich jak satysfakcja z pracy i zaangażowanie organizacyjne, pojawiły się nowe czynniki badane zarówno w służbach, jak i podmiotach cywilnych. Jednym z nich jest wytrwałość (grit). Konstrukt ten zdefiniowano jako dążenie do osiągnięcia długoterminowych celów z wytrwałością i pasją[21], a wyniki badań wykazały, że osoby o wyższym poziomie wytrwałości miały istotnie niższą skłonność do dobrowolnej rezygnacji z wymagającego 24-dniowego kursu Army Special Operations Forces

[17] F. Herzberg, B. Mausner, B.B. Snyderman, *The Motivation to Work*, New York 1959, https://api.pageplace.de/preview/DT0400.9781351504430_A30546568/preview-9781351504430_A30546568.pdf [dostęp: 18 I 2025]; H. Dogonyaro, F. Nwosu, *Exploring Employee Retention in the Hospitality Industry Through Herzberg's Two-Factor Motivation Theory*, preprint. https://doi.org/10.13140/RG.2.2.34721.93287; L.C. Chiat, S.A. Panatik, *Perceptions of Employee Turnover Intention by Herzberg's Motivation-Hygiene Theory: A Systematic Literature Review*, „Journal of Research in Psychology" 2019, t. 1, nr 2, s. 10–15. https://doi.org/10.31580/jrp.v1i2.949.

[18] J.P. Meyer, N.J. Allen, *A three-component conceptualization of organizational commitment*, „Human Resource Management Review" 1991, t. 1, nr 1, s. 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z.

[19] N.J. Allen, J.P. Meyer, *The measurement and antecedents of affective, continuance and normative commitment to the organization*, „Journal of Occupational Psychology" 1990, t. 63, nr 1, s. 1–18. https://doi.org/10.1111/j.2044-8325.1990.tb00506.x.

[20] R.T. Mowday, R.M. Steers, L.W. Porter, *The measurement of organizational commitment*, „Journal of Vocational Behavior" 1979, t. 14, nr 2, s. 224–247. https://doi.org/10.1016/0001-8791(79)90072-1.

[21] A.L. Duckworth i in., *Grit: Perseverance and passion for long-term goals*, „Journal of Personality and Social Psychology" 2007, t. 92, nr 6, s. 1087–1101. https://doi.org/10.1037/0022-3514.92.6.1087.

(ARSOF)[22] niż osoby o niższym poziomie wytrwałości[23]. Badanie przeprowadzone wśród 1558 kadetów Akademii West Point również potwierdziło, że wytrwałość była solidnym predyktorem rezygnacji – wyższy poziom wytrwałości znacznie zwiększał szansę ukończenia czteroletniego szkolenia w akademii[24]. Wytrwałość wskazywana jest zatem jako obiecujący predyktor retencji, który mógłby być wykorzystywany w służbach mundurowych, choć wymaga to dalszych badań dla pełnego potwierdzenia[25].

Scharakteryzowane zmienne przyjęto również w projekcie badawczym zrealizowanym w WSSG i zestawiono w tabeli 1.

Tabela 1. Definicje zmiennych przyjętych w badaniu.

Nazwa zmiennej	Definicja	Źródła
Satysfakcja z pracy	Odczucie dotyczące pracy i jej różnych aspektów. Zależne od tego, czy praca pozwala zaspokajać ważne dla pracownika potrzeby	P.E. Spector (1997) E.A. Locke (1976) F. Herzberg (1959)
Zaangażowanie organizacyjne	Stan psychiczny charakteryzujący relację pracownika z organizacją i mający wpływ na decyzję o kontynuowaniu lub zaprzestaniu członkostwa w organizacji. Gotowość do wysiłku na rzecz organizacji oraz wiara w jej wartości i cele i ich akceptacja	J.P. Meyer, N.J. Allen (1991) R.T. Mowday, R.M. Steers, L.W. Porter (1979)
Wytrwałość	Dążenie do osiągnięcia długoterminowych celów z wytrwałością i pasją	A.L. Duckworth, C. Peterson, M.D. Matthews, D.R. Kelly (2007)
Intencja pozostania w organizacji	Zamiar odnoszący się do świadomej i celowej woli pracowników pozostania w organizacji	R.P. Tett, J.P. Meyer (1993)
Intencja odejścia z organizacji	Świadome i celowe pragnienie opuszczenia organizacji w niedalekiej przyszłości	W.H. Mobley, S.O. Horner, A.T. Hollingsworth (1978)

Źródło: opracowanie własne na podstawie literatury przedmiotu.

[22] Szkolenie ARSOF koncentruje się na intensywnych testach sprawności fizycznej i psychicznej, przywództwie, rozwiązywaniu problemów i adaptacji kulturowej w celu wyłonienia kandydatów gotowych na wyjątkowe wymagania sił specjalnych. Jego istotą jest rygorystyczna selekcja i identyfikacja osób potrafiących opanować nieregularne działania wojenne, niekonwencjonalne taktyki i działać globalnie.

[23] L. Eskreis-Winkler i in., *The grit effect: predicting retention in the military, the workplace, school and marriage*, „Frontiers in Psychology" 2014, t. 5, nr 36. https://doi.org/10.3389/fpsyg.2014.00036.

[24] D.R. Kelly, M.D. Matthews, P.T. Bartone, *Grit and Hardiness*…

[25] K.N. Roach, *Leveraging Grit in Military Research: A Comprehensive Review*, https://apps.dtic.mil/sti/trecms/pdf/AD1211251.pdf [dostęp: 20 I 2025].

Metodyka badawcza

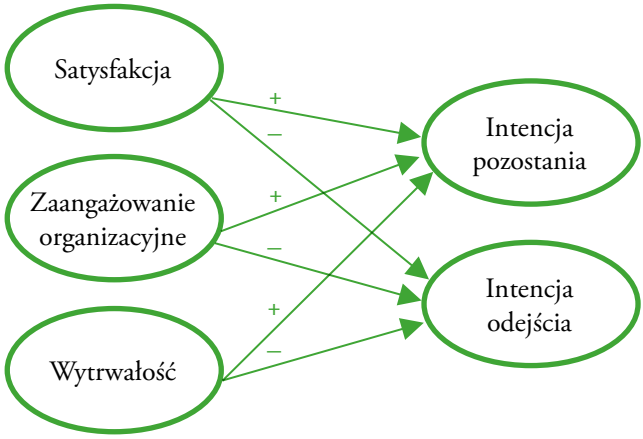
Przyjęta metodyka i organizacja badań były inspirowane projektem A Longitudinal Examination of First Term Attrition and Reenlistment among FY1999 Enlisted Accessions realizowanym w Armii Stanów Zjednoczonych przez United States Army Research Institute for the Behavioral and Social Sciences. Projekt opisywał podejście i narzędzia badawcze oraz najistotniejsze wyniki zarządzania retencją personelu. Projektem badawczym formalnie zatwierdzonym w WSSG objęto funkcjonariuszy w służbie stałej szkolących się w tej uczelni. Kryterium doboru do próby badawczej była dostępność osób, a etycznymi uwarunkowaniami badania – dobrowolność udziału oraz zachowanie anonimowości respondentów. Finalna próba badawcza objęła 184 funkcjonariuszy w służbie stałej z co najmniej trzyletnim stażem służby, zróżnicowanych pod względem płci, wieku, stażu oraz reprezentowanych jednostek i stanowisk służbowych. Dane badawcze były zbierane od lutego do września 2024 r.

Przegląd literatury przedmiotu, realizowanych projektów i potrzeb służbowych z zakresu retencji personelu umożliwił wyznaczenie głównego celu badania: zidentyfikowanie i pomiar zmiennych wpływających na intencję pozostania w służbie oraz intencję odejścia z niej.

Kierunki poszukiwań badawczych zostały odzwierciedlone w następujących hipotezach oraz przedstawionym modelu koncepcyjnym (rysunek 1):

H1: Satysfakcja, zaangażowanie organizacyjne, wytrwałość będą istotnie i pozytywnie wpływać na intencję pozostania w służbie.

H2: Satysfakcja, zaangażowanie organizacyjne, wytrwałość będą istotnie i negatywnie wpływać na intencję odejścia ze służby.



Rysunek 1. Podstawowy model koncepcyjny badania retencji funkcjonariuszy Straży Granicznej.

Źródło: opracowanie własne na podstawie przeglądu literatury.

W badaniu wykorzystano metodę częściowo ustrukturyzowanego wywiadu ankietowego oraz modelowania równań strukturalnych metodą najmniejszych kwadratów cząstkowych (PLS-SEM).

Kwestionariusz ankiety obejmował następujące zmienne z pierwotną liczbą związanych z nimi pytań: satysfakcja z pracy (45 pozycji), zaangażowanie organizacyjne (18 pozycji), wytrwałość (12 pozycji), intencja pozostania w organizacji (3 pozycje), intencja odejścia z organizacji (3 pozycje). Dodatkowo kwestionariusz ankiety zawierał półotwarty katalog 45 potencjalnych powodów rezygnacji ze służby z możliwością wpisania innych niewymienionych powodów oraz swobodnej wypowiedzi respondenta.

Wszystkie pytania miały 5-punktową skalę odpowiedzi typu Likerta, na której wartość 1 oznaczała skrajnie negatywną opinię lub całkowitą niezgodę z twierdzeniem, 3 – postawę neutralną, wartość 5 natomiast wskazywała skrajnie pozytywną opinię lub pełną zgodę z twierdzeniem. Zawartość narzędzia badawczego skonsultowano z psychologami związanymi ze służbą pod kątem zrozumiałości, kompletności i poprawności użytych sformułowań.

Badanie docelowe poprzedzono pilotażem kwestionariusza wśród 50 funkcjonariuszy szkolących się w WSSG, którzy nie należeli do finalnej próby badawczej. Respondenci potwierdzili zrozumiałość pytań i twierdzeń zawartych w ankiecie, co znalazło odzwierciedlenie w wysokiej zgodności odpowiedzi z powtórzonym po dwóch tygodniach testem powtórnym (tabela 2), świadczącym o dobrej stabilności narzędzia[26].

Tabela 2. Wyniki korelacji test-retest dla komponentów narzędzia badawczego.

Nazwa konstruktu	Test-retest (badanie pilotażowe) n = 50
Satysfakcja ze służby	0,83
Zaangażowanie afektywne	0,65
Zaangażowanie normatywne	0,84
Zaangażowanie kontynuacyjne	0,96
Wytrwałość	0,65
Intencja pozostania w organizacji	0,77
Intencja odejścia z organizacji	0,68

Źródło: opracowanie własne na podstawie przeprowadzonego testu statystycznego.

[26] K.S. Jankowski, M. Zajenkowski, *Metody szacowania rzetelności pomiaru testem*, w: *Psychometria – podstawowe zagadnienia*, K. Fronczyk (red.), Warszawa 2009, s. 84–110.

Kierując się zasadą ekonomiki badań, zredukowano liczbę pytań w ankiecie bez uszczerbku dla wartości poznawczej i parametrów statystycznych, co umożliwiło skrócenie czasu wypełnienia ankiety i ograniczyło pracochłonność. Na wstępie obliczono współczynnik Kaisera–Meyera–Olkina (KMO). Jego wysoka wartość (> 0,8) potwierdziła zasadność przeprowadzenia eksploracyjnej analizy czynnikowej (exploratory factor analysis, EFA), na podstawie której dla zmiennej satysfakcja z pracy wyłoniono sześć czynników: S1 – relacje interpersonalne, S2 – wynagrodzenia, S3 – stabilność zawodowa, S4 – możliwość awansu, S5 – samorealizacja, S6 – poczucie bezpieczeństwa. Zredukowano liczbę pytań związanych z tą zmienną z 45 do 18 najbardziej istotnych pozycji. Analogicznie zmniejszono liczbę pytań dotyczących zaangażowania organizacyjnego z 18 do 9 oraz wyodrębniono trzy czynniki tego zaangażowania: zaangażowanie afektywne, zaangażowanie normatywne, zaangażowanie kontynuacyjne. Podobnie postąpiono w przypadku wytrwałości, dla której zredukowano liczbę pytań z 12 do 5 najistotniejszych. Wymiary dla poszczególnych zmiennych wyłoniono za pomocą analizy czynnikowej, w której uzyskano zadowalające parametry – wszystkie ładunki czynnikowe przekroczyły wartość 0,5, a skumulowana wyjaśniona wariancja przekroczyła 60%. Ze względu na jednowymiarowość intencji pozostania i intencji odejścia oraz małą liczbę pytań ich dotyczących nie zmniejszano ich liczby. W katalogu potencjalnych powodów odejścia ze służby nie wyłaniano czynników i nie redukowano liczby pytań z powodu różnorodności odpowiedzi otwartych uzyskanych w tym obszarze.

Intencja zbudowania modelu strukturalnego retencji funkcjonariuszy, rozkłady odbiegające od normalnego oraz potrzeba jednoczesnej analizy wielu zależności skłoniły do wykorzystania w badaniu PLS-SEM. Zastosowanie PLS-SEM do badania zachowań personelu jest współcześnie zalecane przez wiodące europejskie czasopisma z dziedziny zarządzania (m.in. „Journal of Business Research", „European Management Journal")[27]. Model równań strukturalnych pozwala zobrazować i zmierzyć wpływ zmiennych takich jak satysfakcja, zaangażowanie organizacyjne czy wytrwałość na intencję pozostania oraz intencję odejścia ze służby – co można wykorzystać do wyjaśnienia oraz predykcji zachowań funkcjonariuszy związanych z pozostaniem w SG bądź odejściem z niej. Wszystkie obliczenia przeprowadzono w środowisku R[28], a zbudowany konstrukt wyższego rzędu miał charakter

[27] Zob. M. Ratzmann, S.P. Gudergan, R. Bouncken, *Capturing heterogeneity and PLS-SEM prediction ability: Alliance governance and innovation*, „Journal of Business Research" 2016, t. 69, nr 10, s. 4593–4603. https://doi.org/10.1016/j.jbusres.2016.03.051; N.F. Richter i in., *European management research using partial least squares structural equation modeling (PLS-SEM)*, „European Management Journal" 2016, t. 34, nr 6, s. 589–597. https://doi.org/10.1016/j.emj.2016.08.001.

[28] R – interpretowany język programowania oraz środowisko do obliczeń statystycznych i wizualizacji wyników. Wykorzystano wersję 4.5.1 i pakiet SEMinR w wersji 2.3.4.

refleksyjno-refleksyjny (reflective-reflective higher-order construct) i został estymowany w ramach rozłącznego podejścia dwuetapowego (disjoint two-stage approach). PLS-SEM, w odróżnieniu od wielu innych technik statystycznych, pozostaje stosunkowo odporny na naruszenie założenia normalności rozkładów i dobrze sprawdza się przy umiarkowanej liczebności próby, co czyniło go właściwym narzędziem w niniejszych analizach.

Wyniki badań

Satysfakcja z poszczególnych czynników motywacyjnych

Analiza uzyskanych wyników dotyczących ocen indywidualnych motywatorów wskazuje, że najbardziej satysfakcjonującym czynnikiem dla funkcjonariuszy była stabilność zawodowa, najmniej satysfakcjonujący natomiast okazał się czynnik dotyczący wynagrodzeń, którego wartość wyniosła 3,11 (tabela 3). Ogólny poziom satysfakcji ze wszystkich 18 badanych motywatorów wyniósł 3,51 w skali pięciopunktowej, co oznacza, że respondenci generalnie pozytywnie ocenili system motywacyjny składający się z analizowanych elementów. Na tym tle poziom satysfakcji z wynagrodzenia może sugerować potencjalne ryzyko dla retencji personelu i być podstawą do rozważenia wprowadzenia ulepszeń.

Tabela 3. Poziom satysfakcji z poszczególnych czynników motywacyjnych (n = 184).

Czynniki satysfakcji	Średnia arytmetyczna	Odchylenie standardowe
Stabilność zawodowa (3 motywatory)	3,88	0,99
Samorealizacja (3 motywatory)	3,74	0,88
Relacje interpersonalne (3 motywatory)	3,60	1,02
Poczucie bezpieczeństwa (3 motywatory)	3,56	1,05
Możliwość awansu (3 motywatory)	3,19	1,16
Wynagrodzenie (3 motywatory)	3,11	1,12
Ogólny poziom satysfakcji ze wszystkich 18 badanych motywatorów	3,51	1,04

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Zaangażowanie organizacyjne i wytrwałość

Poziom zaangażowania organizacyjnego badanych funkcjonariuszy okazał się umiarkowany – osiągnęło ono średnią 2,93, czyli wartość zbliżoną do neutralnej 3,00 (tabela 4). Wynik ten sugeruje, że ogólne poczucie więzi respondentów z organizacją nie było ani wyraźnie pozytywne, ani wyraźnie negatywne. W ramach poszczególnych wymiarów zaangażowania organizacyjnego najwyższy poziom odnotowano dla zaangażowania afektywnego – średnia 3,41. Ten wymiar – mierzony m.in. twierdzeniami: *Straż Graniczna ma dla mnie bardzo duże znaczenie osobiste*, *Odczuwam silne poczucie przynależności do SG*, *Czuję emocjonalny związek z SG* – świadczy o dość silnym emocjonalnym związku respondentów z organizacją oraz identyfikacji z jej wartościami. Z kolei zaangażowanie kontynuacyjne i zaangażowanie normatywne uzyskały znacznie niższe średnie, odpowiednio: 2,72 i 2,67. Rezultat ten może świadczyć o relatywnie słabym poczuciu lojalności wobec organizacji (wymiar normatywny) i przywiązaniu wynikającym z kosztów odejścia (wymiar kontynuacyjny).

Średni deklarowany poziom wytrwałości w działaniu wyniósł 4,05, co oznacza, że badani ocenili siebie jako osoby dążące do osiągania długoterminowych celów z nieco ponadprzeciętną pasją i determinacją. Jest to umiarkowanie wysoki poziom wytrwałości, który może dobrze rokować w kontekście kontynuacji służby w SG i braku chęci jej porzucenia – osoby bardziej wytrwałe z reguły trudniej zniechęcić do realizacji obranej drogi zawodowej.

Tabela 4. Poziom zaangażowania organizacyjnego i wytrwałości (n = 184).

Nazwa konstruktu	Średnia arytmetyczna	Odchylenie standardowe
Zaangażowanie organizacyjne całościowe	2,93	1,12
Zaangażowanie afektywne	3,41	1,01
Zaangażowanie kontynuacyjne	2,72	1,21
Zaangażowanie normatywne	2,67	1,13
Wytrwałość	4,05	0,83

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Przedstawione wyniki wskazują newralgiczne obszary dla badanych funkcjonariuszy SG, które należy monitorować i uwzględniać w działaniach zarządczych, aby uniknąć niepożądanej dużej rotacji personelu. Z jednej strony stosunkowo niski poziom zaangażowania organizacyjnego (zwłaszcza normatywnego i kontynuacyjnego) sugeruje potrzebę wzmacniania różnymi środkami poczucia lojalności

i przywiązania funkcjonariuszy do formacji. Z drugiej strony stosunkowo wysoka wytrwałość badanych stanowi pozytywny prognostyk – może sprzyjać wytrwaniu w służbie pomimo ewentualnych trudności.

Potencjalne powody odejścia ze służby

Zdaniem badanych funkcjonariuszy najistotniejszym potencjalnym powodem rezygnacji ze służby (tzw. demotywatorem) w SG jest niekorzystna zmiana przepisów dotyczących uposażeń, świadczeń lub systemu emerytalnego (tabela 5). W pierwszej dziesiątce najwyżej sklasyfikowanych powodów rezygnacji znalazły się aż trzy związane z systemem wynagrodzeń (wspomniana niekorzystna zmiana przepisów płacowych; zbyt niskie uposażenie; rzadkie i niskie podwyżki uposażenia). Dwa powody należą do kategorii związanej z równowagą praca–życie (work-life balance): brak czasu na życie prywatne (z powodu nadmiernej liczby zadań służbowych) oraz trudności w godzeniu obowiązków służbowych z życiem rodzinnym (ciągłe napięcie przy próbach równoważenia tych sfer). Dwa kolejne powody można powiązać z relacjami z przełożonymi: niesprawiedliwe ukaranie oraz nierówne traktowanie. Ponadto wskazano jeden powód natury interpersonalnej: brak szacunku ze strony przełożonego i współpracowników, a także jeden dotyczący stabilności zawodowej: przeniesienia służbowe między jednostkami/komórkami organizacyjnymi SG (przymusowe relokacje). Listę uzupełnia jeden czynnik rynkowy – lepsza oferta zatrudnienia u innego pracodawcy.

Tabela 5. Dziesięć najważniejszych potencjalnych powodów rezygnacji funkcjonariuszy ze służby w Straży Granicznej (n = 184).

Lp.	Potencjalny powód odejścia ze służby w Straży Granicznej	Średnia arytmetyczna	Odchylenie standardowe
1.	Niekorzystna zmiana przepisów dot. uposażeń/świadczeń/emerytur itp.	4,29	1,00
2.	Przeniesienia służbowe między jednostkami/komórkami organizacyjnymi SG	4,06	1,07
3.	Niesprawiedliwe ukaranie	4,06	1,13
4.	Brak czasu na życie prywatne spowodowany zbyt dużą liczbą zadań	4,05	1,05
5.	Napięcie związane z równoważeniem relacji rodzinnych i wymagań służbowych	4,02	1,02
6.	Nierówne traktowanie	3,96	1,11

Lp.	Potencjalny powód odejścia ze służby w Straży Granicznej	Średnia arytmetyczna	Odchylenie standardowe
7.	Zbyt niskie uposażenie	3,95	1,07
8.	Rzadkie i niskie podwyżki uposażenia	3,91	1,20
9.	Lepsza oferta zatrudnienia u innego pracodawcy	3,91	1,04
10.	Brak szacunku do mnie ze strony przełożonego i współpracowników	3,91	1,05

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Wyniki dotyczące powodów odejścia wskazują obszary problemowe, na których SG jako pracodawca powinna się skoncentrować, aby zmniejszyć ryzyko utraty funkcjonariuszy. Szczególnie mocno rysuje się kwestia wynagrodzeń i świadczeń – aż trzy z dziesięciu najważniejszych powodów dotyczą sfery finansowej. Zarówno system płac, jak i przewidywalność ścieżki zawodowej (problem przeniesień) czy relacje z przełożonymi wymagają uwagi decydentów. Identyfikacja tych czynników stwarza możliwość podjęcia ukierunkowanych działań zarządczych zapobiegających odejściom.

Intencja pozostania oraz intencja odejścia

Chęć pozostania w służbie bądź odejścia z niej była sondowana przez badanie deklaracji funkcjonariuszy w tym zakresie, co pozwoliło na zmierzenie zarówno potencjalnego poziomu retencji, jak i rotacji personelu, których to poziomów nie traktowano jako komplementarne względem siebie. Zgodnie z pięciostopniową skalą zastosowaną w narzędziu badawczym neutralnym progiem rozgraniczającym odpowiedzi była wartość 3,00 (tabela 6). Intencja pozostania (poziom retencji) była na dobrym poziomie – średnia deklaracji wyniosła 3,89, czyli osiągnęła wartość wyraźnie powyżej progu 3,00. Spośród 184 badanych osób 38 miało intencję pozostania poniżej neutralnego poziomu, co w przeliczeniu na procenty daje rezultat 21% i określa retencję na poziomie 79%.

Poziomy intencji odejścia i rotacji były niskie, gdyż średnia wartość dla intencji odejścia wyniosła 2,00. Tylko 25 osób spośród 184 miało intencję odejścia powyżej neutralnego poziomu, co określa rotację na poziomie 14%.

Tabela 6. Poziom intencji pozostania/odejścia oraz retencji/rotacji funkcjonariuszy Straży Granicznej.

Wyszczególnienie	Intencja pozostania	Intencja odejścia
Średnia arytmetyczna	3,89	2,00
Poziom retencji w %	79	-
Poziom rotacji w %	-	14
Odchylenie standardowe	1,08	1,06

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

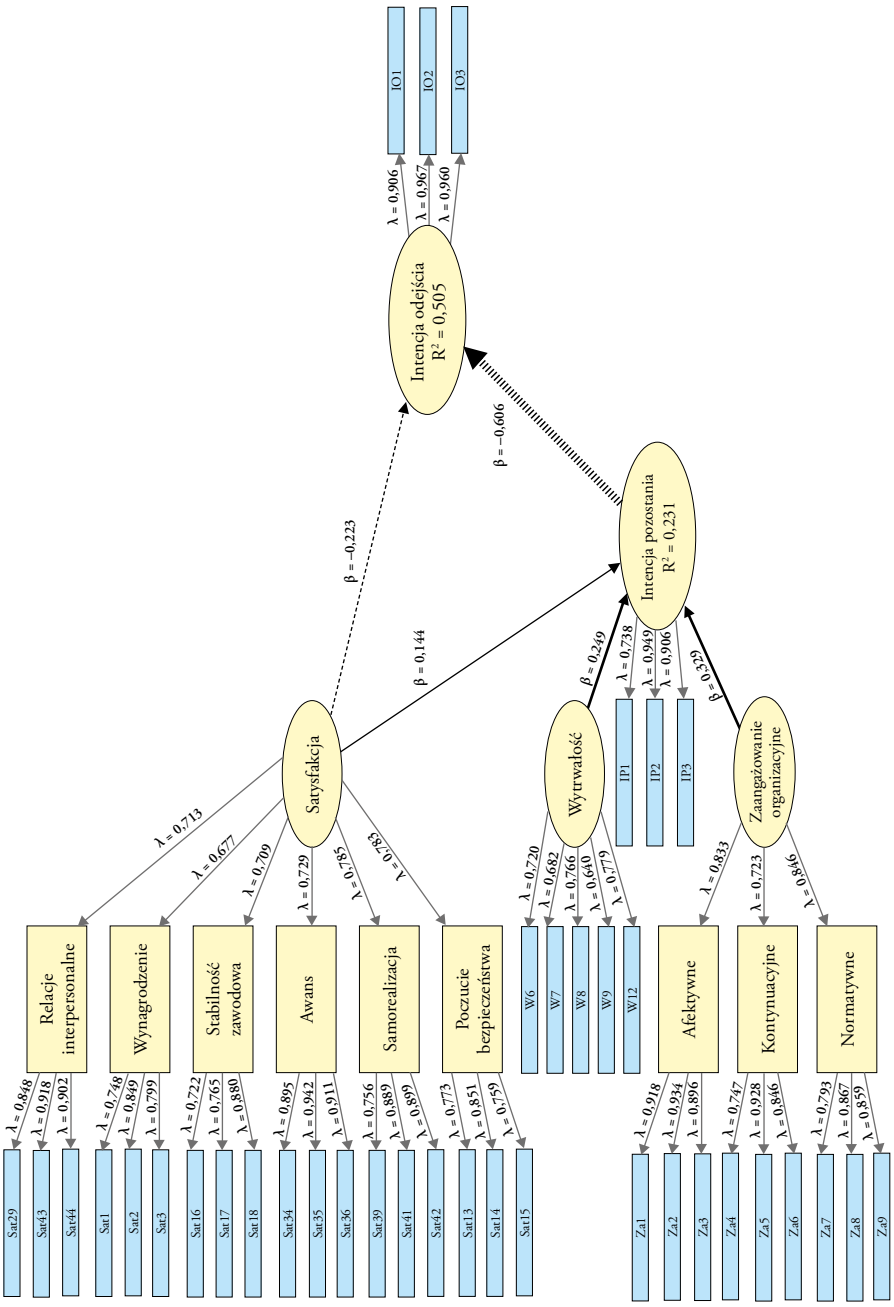
Przedstawione wyniki oznaczają, że SG ma wysoką zdolność zatrzymania funkcjonariuszy w służbie, gdyż ich zdecydowana większość planuje w niej pozostać, a nad odejściem mogą się zastanawiać pojedyncze osoby.

Wyniki modelu strukturalnego PLS-SEM

Najważniejszym zamierzeniem badawczym było zastosowanie do badania retencji personelu w polskich służbach mundurowych modelowania strukturalnego PLS-SEM i opracowanie modelu (rysunek 2).

Kształty eliptyczne w modelu przedstawiają zmienne ukryte: satysfakcję, zaangażowanie organizacyjne, wytrwałość, intencję pozostania, intencję odejścia, a wartości R^2 wpisane w intencje informują, w ilu procentach są one wyjaśniane przez zmienne na nie oddziałujące. Kierunek tego oddziaływania wskazują zwroty strzałek, dodatnie lub ujemne wartości β odpowiadają natomiast sile oddziaływania.

Prostokątne kształty w kolorze żółtym przedstawiają poszczególne wymiary wyłonione w strukturze danej zmiennej. Przykładowo, zmienna zaangażowanie organizacyjne ma swoje odzwierciedlenie w trzech wymiarach, z których wymiar zaangażowania normatywnego ma największy udział (λ = 0,846) w poziomie zaangażowania organizacyjnego w porównaniu z zaangażowaniem afektywnym (λ = 0,833) i zaangażowaniem kontynuacyjnym (λ = 0,723). Z kolei na ogólny poziom satysfakcji ze służby najbardziej wpływają wymiary samorealizacji (λ = 0,785) i poczucia bezpieczeństwa (λ = 0,783).



Rysunek 2. Model strukturalny PLS-SEM retencji funkcjonariuszy Straży Granicznej.

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Wyniki uzyskane w modelu retencji funkcjonariuszy SG są satysfakcjonujące, gdyż wszystkie współczynniki determinacji R^2 przekroczyły próg 0,20[29], a badana kluczowa zmienna – intencja odejścia – została wyjaśniona w ponad 50% ($R^2 = 0,505$) przez zmienne: intencję pozostania i satysfakcję oraz pośrednio przez zaangażowanie organizacyjne i wytrwałość. Oznacza to, że ponad połowę zróżnicowania w skłonności do odejścia w tej grupie można tłumaczyć mierzonymi zmiennymi, co potwierdza słuszność ich doboru oraz istotność.

Wyniki badania wskazały na bardzo silny negatywny wpływ intencji pozostania na intencję odejścia, gdyż wzrost intencji pozostania o 1 odchylenie standardowe przekłada się na spadek intencji odejścia o 0,606 odchylenia standardowego. Potwierdza to logikę rozumowania, że budowanie wśród funkcjonariuszy chęci pozostania w SG bezpośrednio redukuje ryzyko ich odejścia. Okazało się również, że intencja odejścia jest determinowana zarówno przez intencję pozostania, jak i poziom satysfakcji ($\beta = -0,223$), przy czym intencja pozostania oddziałuje silniej na intencję odejścia niż satysfakcja. Można to interpretować następująco: im bardziej ktoś jest niezadowolony z warunków, tym bardziej myśli o odejściu, ale jeszcze ważniejsze jest ogólne nastawienie – sam zamiar pozostania w służbie. Osoby, które mimo pewnych braków satysfakcji chcą zostać, np. z lojalności czy poczucia misji, są mniej skłonne do rozmyślań o odejściu. Wysoka satysfakcja może natomiast powstrzymywać tych, którzy zamierzali odejść. Intencja pozostania w tym modelu jest z kolei wyjaśniana w ponad 23% ($R^2 = 0,231$) przez zmienne: zaangażowanie organizacyjne ($\beta = 0,329$), wytrwałość ($\beta = 0,249$) oraz satysfakcję ($\beta = 0,144$), z których najsilniej oddziałuje zaangażowanie organizacyjne. Jest to istotny, choć umiarkowany efekt, sugerujący, że dla funkcjonariuszy budowanie identyfikacji z organizacją i lojalności jest czynnikiem silniej wpływającym na realne plany pozostania w służbie niż wytrwałość i satysfakcja. Podsumowując tę część badania, można stwierdzić, że model strukturalny dla funkcjonariuszy potwierdził dużą rolę zaangażowania organizacyjnego i satysfakcji w utrzymaniu personelu. Wskazał też, że najsilniejszym czynnikiem powstrzymującym przed odejściem ze służby jest silna intencja pozostania wynikająca z przywiązania do organizacji. Zatem działania wzmacniające

[29] A. Kacprzak, *Modelowanie strukturalne w analizie zachowań konsumentów: porównanie metod opartych na analizie kowariancji (CB-SEM) i częściowych najmniejszych kwadratów (PLS-SEM)*, „Handel Wewnętrzny" 2018, t. 1, nr 6, s. 255; R.F. Frank, N.B. Miller, *A Primer for Soft Modeling*, Ohio 1992; J.F. Hair i in., *An assessment of the use of partial least squares structural equation modeling in marketing research*, „Journal of the Academy of Marketing Science" 2012, t. 40, s. 414–433. https://doi.org/10.1007/s11747-011-0261-6; J.F. Hair Jr. i in., *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*, seria: Classroom Companion: Business, Cham 2021, s. 76–78. https://doi.org/10.1007/978-3-030-80519-7.

identyfikację funkcjonariuszy z SG (poczucie misji, dumy, więzi) oraz dbanie o ich satysfakcję w różnych aspektach mogą ograniczać zjawisko odejść ze służby.

Ocena parametrów statystycznych modelu strukturalnego PLS-SEM

Testowanie rzetelności i trafności pomiarowej zastosowanego modelu strukturalnego PLS-SEM potwierdziło, że charakteryzuje się on dobrymi parametrami psychometrycznymi, co prezentuje tabela 7. Wartości miar rzetelności – zarówno współczynnika Alfa Cronbacha, wskaźnika rho_A, jak i rzetelności kompozytowej (composite reliability, CR) – dla większości konstruktów znalazły się w przedziale 0,70–0,95[30]. Wyjątek stanowił konstrukt intencji odejścia, dla której wartość CR wyniosła 0,961. Tak wysoki wynik może sugerować redundancję wskaźników, tj. ich nadmierne podobieństwo treściowe. Jednakże, biorąc pod uwagę, że intencja odejścia jest konstruktem jednorodnym, mierzonym za pomocą trzech wskaźników, a wartość rho_A pozostaje na akceptowalnym poziomie, można uznać ten rezultat za uzasadniony i niebudzący zastrzeżeń. Dodatkowo średnia wyjaśniona wariancja (average variance extracted, AVE) dla każdego konstruktu wyniosła powyżej 0,50[31], co świadczy o wysokiej zbieżności zawartych w nich wskaźników.

Tabela 7. Trafność i rzetelność miar modelu strukturalnego PLS-SEM – wskaźniki dla konstruktów latentnych.

Wyszczególnienie	Alfa Cronbacha	rho_A	CR	AVE
Intencja odejścia	0,939	0,944	0,961	0,892
Intencja pozostania	0,837	0,888	0,902	0,756
Satysfakcja	0,829	0,834	0,875	0,538
Wytrwałość	0,771	0,790	0,842	0,517
Zaangażowanie organizacyjne	0,723	0,732	0,844	0,644

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

W celu sprawdzenia trafności dyskryminacyjnej konstruktów obliczono także współczynniki heterotrait-monotrait (heterotrait-monotrait ratio of correlations, HTMT) dla każdej pary zmiennych latentnych. W tabeli 8 przedstawiono wartości HTMT – we wszystkich przypadkach mieszczą się one wyraźnie poniżej przyjętego

[30] J.F. Hair Jr. i in., *Partial Least Squares*…, s. 77–78, 80.

[31] Tamże, s. 78, 80.

kryterium 0,85[32], co świadczy o dobrej rozdzielności poszczególnych konstruktów – żadne z nich nie mierzą tego samego zjawiska. Innymi słowy, zmienne latentne zastosowane w modelu są wzajemnie dyskretne i nie następuje niepożądane nakładanie się ich znaczeń.

Tabela 8. Macierz współczynników HTMT – trafność dyskryminacyjna konstruktów modelu strukturalnego PLS-SEM.

Nazwa konstruktu	Zaangażowanie organizacyjne	Satysfakcja	Wytrwałość	Intencja pozostania	Intencja odejścia	Relacje interpersonalne	Wynagrodzenie	Stabilność zawodowa	Awans	Samorealizacja	Poczucie bezpieczeństwa	Zaangażowanie afektywne	Zaangażowanie kontynuacyjne
Satysfakcja	0,59												
Wytrwałość	0,27	0,18											
Intencja pozostania	0,44	0,37	0,28										
Intencja odejścia	0,46	0,47	0,20	0,76									
Relacje interpersonalne	0,38	*	0,13	0,20	0,34								
Wynagrodzenie	0,55	*	0,12	0,35	0,30	0,43							
Stabilność zawodowa	0,40	*	0,24	0,31	0,41	0,46	0,54						
Awans	0,37	*	0,06	0,22	0,31	0,52	0,57	0,41					
Samorealizacja	0,46	*	0,15	0,27	0,32	0,72	0,62	0,50	0,68				
Poczucie bezpieczeństwa	0,55	*	0,20	0,34	0,46	0,57	0,51	0,81	0,57	0,65			
Zaangażowanie afektywne	*	0,47	0,20	0,36	0,30	0,29	0,43	0,30	0,24	0,42	0,49		
Zaangażowanie kontynuacyjne	*	0,30	0,33	0,32	0,38	0,17	0,36	0,21	0,23	0,17	0,26	0,34	
Zaangażowanie normatywne	*	0,53	0,14	0,28	0,31	0,37	0,43	0,38	0,35	0,45	0,44	0,74	0,57

* Nie oceniamy trafności różnicowej między satysfakcją i zaangażowaniem organizacyjnym a ich komponentem niższego rzędu, ponieważ naruszenie trafności różnicowej między tymi konstruktami jest oczekiwane.

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

[32] J. Henseler, Ch.M. Ringle, M. Sarstedt, *A new criterion for assessing discriminant validity in variance-based structural equation modeling*, „Journal of the Academy of Marketing Science" 2015, t. 43, s. 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Wszystkie wartości współczynnika inflacji wariancji (variance inflation factor, VIF) dla modelu wewnętrznego[33] (tabela 9) są znacznie poniżej powszechnie akceptowanych progów[34], co wskazuje na niewystępowanie znaczącej współliniowości między konstruktami w modelu strukturalnym PLS-SEM. Niskie wartości VIF dla modelu wewnętrznego sugerują, że konstrukty są stosunkowo niezależne od siebie, co pozwala na bardziej wiarygodną interpretację współczynników ścieżek.

Tabela 9. Wartości VIF – ocena współliniowości modelu wewnętrznego.

Wyszczególnienie	VIF
Intencja pozostania → intencja odejścia	1,12
Satysfakcja → intencja odejścia	1,12
Satysfakcja → intencja pozostania	1,31
Wytrwałość → intencja pozostania	1,04
Zaangażowanie organizacyjne → intencja pozostania	1,30

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

W modelu strukturalnym PLS-SEM za pomocą bootstrappingu (10 000 iteracji) oszacowano 95% przedział ufności (confidence interval, CI) dla wszystkich ścieżek, których wartości prezentuje tabela 10. Interpretacja tych przedziałów potwierdza istotność większości zależności w modelu. Dla każdej ścieżki, jeśli cały przedział ufności znajduje się powyżej lub poniżej zera, oznacza to efekt statystycznie istotny (przy $p < 0,05$). W analizowanym modelu wszystkie główne ścieżki okazały się istotne.

Tabela 10. Współczynniki ścieżek, poziom istotności, przedział ufności modelu strukturalnego PLS-SEM.

Ścieżka	Oryginalna próba	Średnia z prób	Odchylenie standardowe	Stat. t	2,5% CI	97,5% CI
Zaangażowanie organizacyjne → intencja pozostania	0,329	0,342	0,079	4,184	0,196	0,494

[33] Prezentowany model strukturalny PLS-SEM składa się z modelu zewnętrznego i wewnętrznego. Model zewnętrzny obejmuje konstrukty niższego rzędu wpływające na konstrukty wyższego rzędu. Model wewnętrzny obejmuje konstrukty wyższego rzędu: satysfakcję, zaangażowanie, wytrwałość, intencję odejścia, intencję pozostania.

[34] J-M. Becker i in., *How collinearity affects mixture regression results*, „Marketing Letters" 2015, t. 26, nr 4, s. 643–659. https://doi.org/10.1007/s11002-014-9299-9.

Ścieżka	Oryginalna próba	Średnia z prób	Odchylenie standardowe	Stat. t	2,5% CI	97,5% CI
Satysfakcja → intencja pozostania	0,144	0,151	0,073	1,962	0,007	0,293
Satysfakcja → intencja odejścia	–0,223	–0,228	0,075	–2,972	–0,375	–0,082
Wytrwałość → intencja pozostania	0,249	0,259	0,083	2,994	0,110	0,407
Intencja pozostania → intencja odejścia	–0,606	–0,605	0,077	–7,867	–0,751	–0,450

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Oprócz efektów bezpośrednich uwzględnionych w modelu przeanalizowano również efekty pośrednie (mediacje) kluczowych zmiennych predykcyjnych na zmienne wynikowe. Wyniki tej analizy przedstawia tabela 11. Dane pokazują, że satysfakcja z pracy wywiera istotny pośredni wpływ zarówno na intencję odejścia, jak i na intencję pozostania. Efekt pośredni satysfakcji na intencję odejścia wynosi –0,087, co oznacza, że satysfakcja zmniejsza skłonność do odejścia przez swój wpływ na intencję pozostania.

Zaangażowanie organizacyjne oraz wytrwałość również wykazują negatywne efekty pośrednie na intencję odejścia, odpowiednio –0,199 oraz –0,151, co wskazuje, że czynniki te redukują skłonność do porzucenia służby pośrednio, przez wzmacnianie intencji pozostania.

Tabela 11. Efekty pośrednie wybranych zmiennych w modelu strukturalnym PLS-SEM.

Ścieżka	Efekt pośredni
Zaangażowanie organizacyjne → intencja odejścia	–0,199
Satysfakcja → intencja odejścia	–0,087
Wytrwałość → intencja odejścia	–0,151

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Jak wynika z danych przedstawionych w tabeli 12, największy całkowity wpływ na intencję odejścia mają kolejno: intencja pozostania (–0,606), satysfakcja (–0,310), zaangażowanie organizacyjne (–0,199) i wytrwałość (–0,151).

Tabela 12. Efekty całkowite wybranych zmiennych w modelu strukturalnym PLS-SEM (bootstrapping – 10 000 iteracji, $p < 0,05$).

Ścieżka	Oryginalna próba	Średnia z prób	Odchylenie standardowe	Stat. t	2,5% CI	97,5% CI
Zaangażowanie organizacyjne → intencja pozostania	0,329	0,342	0,079	4,18	0,196	0,494
Zaangażowanie organizacyjne → intencja odejścia	–0,199	–0,210	0,065	–3,05	–0,347	–0,097
Satysfakcja → intencja pozostania	0,144	0,151	0,073	1,96	0,007	0,293
Satysfakcja → intencja odejścia	–0,310	–0,320	0,076	–4,07	–0,465	–0,166
Wytrwałość → intencja pozostania	0,249	0,259	0,083	2,99	0,110	0,407
Wytrwałość → intencja odejścia	–0,151	–0,157	0,056	–2,71	–0,266	–0,061
Intencja pozostania → intencja odejścia	–0,606	–0,605	0,077	–7,87	–0,751	–0,450

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Wskaźnik f^2 mierzy, o ile wzrasta R^2 zmiennej objaśnianej, gdy uwzględnimy konkretny predyktor lub gdy go usuniemy. Wszystkie wartości f^2 uzyskały wartość progową 0,02 wskazaną przez Jacoba Cohena[35], co świadczy o ich praktycznej istotności (tabela 13).

Tabela 13. Siła efektów f^2 dla relacji w modelu strukturalnym PLS-SEM.

Nazwa konstruktu	Intencja pozostania	Intencja odejścia
Zaangażowanie organizacyjne	0,111	-
Satysfakcja	0,020	0,089

[35] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, New York 1988, s. 413. https://doi.org/10.4324/9780203771587.

Nazwa konstruktu	Intencja pozostania	Intencja odejścia
Wytrwałość	0,077	-
Intencja pozostania	-	0,663

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Wyniki te potwierdzają konieczność uwzględnienia w modelu intencji pozostania, satysfakcji, zaangażowania organizacyjnego i wytrwałości jako predyktorów wpływających bezpośrednio lub pośrednio na intencję odejścia.

Za pomocą funkcji PLSpredict – podejścia bezpośrednich poprzedników (direct antecedents approach) wykonano 10-krotną walidację krzyżową. Uzyskane wartości błędów predykcji RMSE (root mean square error) i MAE (mean absolute error) dla modelu strukturalnego PLS-SEM były niższe niż w modelu regresji liniowej, co wskazuje na wysoką moc predykcyjną[36]. Wyniki zostały przedstawione w tabeli 14.

Tabela 14. Wyniki walidacji krzyżowej przeprowadzonej za pomocą funkcji PLSpredict.

Miary jakości predykcji PLS dla danych poza próbą						
	IP1	IP2	IP3	IO1	IO2	IO3
RMSE	1,067	0,980	0,966	0,969	0,688	0,717
MAE	0,774	0,734	0,767	0,718	0,502	0,521
Miary jakości predykcji modelu regresji liniowej (LM) dla danych poza próbą						
	IP1	IP2	IP3	IO1	IO2	IO3
RMSE	1,096	1,001	0,974	1,004	0,714	0,728
MAE	0,815	0,757	0,767	0,759	0,522	0,532

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

[36] G. Shmueli i in., *Predictive model assessment in PLS-SEM: guidelines for using PLSpredict*, „European Journal of Marketing" 2019, t. 53, nr 11, s. 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189.

Porównanie wyników modelu strukturalnego PLS-SEM z innymi badaniami

Obliczono korelację konstruktów wyższego rzędu i dokonano analizy porównawczej w zakresie oceny siły i kierunku zależności między zmiennymi (tabela 15), aby odnieść wyniki niniejszego badania do badań przeprowadzonych w zagranicznych służbach mundurowych.

Tabela 15. Macierz korelacji konstruktów wyższego rzędu.

Nazwa konstruktu	Zaangażowanie organizacyjne	Satysfakcja	Wytrwałość	Intencja pozostania	Intencja odejścia
Zaangażowanie organizacyjne	1,000	-	-	-	-
Satysfakcja	0,463	1,000	-	-	-
Wytrwałość	–0,075	0,118	1,000	-	-
Intencja pozostania	0,377	0,325	0,241	1,000	-
Intencja odejścia	–0,378	–0,420	–0,180	–0,679	1,000

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Analiza korelacji danych z tabeli 15 wskazuje, że określone kierunki zależności są zgodne z kierunkami przyjętymi w hipotezach badawczych. Wyniki wskazują, że intencja odejścia – kluczowy dla badań konstrukt – jest skorelowana najsilniej negatywnie z intencją pozostania (–0,679), następnie z satysfakcją (–0,420) i zaangażowaniem organizacyjnym (–0,378) oraz wytrwałością (–0,180). Oznacza to, że wraz ze wzrostem któregokolwiek z konstruktów: intencji pozostania, satysfakcji, zaangażowania organizacyjnego czy wytrwałości mocno lub średnio będzie się zmniejszać intencja odejścia. Ustalenie to dostarcza statystycznego dowodu na możliwość zmniejszania liczby niepożądanych odejść ze służby funkcjonariuszy przez optymalizację warunków służby wpływających na te konstrukty.

Ze względu na brak informacji o krajowych badaniach w tym zakresie porównania wyników projektu można było dokonać jedynie z wynikami projektów zagranicznych. W badaniu 400 nowozelandzkich policjantów wykazano istotną korelację

między satysfakcją ze służby a intencją odejścia, która wyniosła r = –0,43[37], co jest bardzo zbliżonym rezultatem do uzyskanego w niniejszym projekcie r = –0,42. Z kolei w badaniu, w którym wzięło udział 3580 holenderskich żołnierzy, korelacja zaangażowania organizacyjnego i intencji odejścia wyniosła r = –0,34[38], co również stanowi rezultat zbliżony do wyniku przedmiotowego badania r = –0,38.

W badaniu 450 kanadyjskich żołnierzy wskaźnik regresji wielorakiej pomiędzy satysfakcją a intencją odejścia wyniósł β = –0,28[39], podczas gdy w niniejszym modelu współczynnik ścieżkowy wyniósł β = –0,22, a efekt całkowity –0,31. Wyniki te potwierdzają ujemny kierunek zależności oraz zbliżony rząd wielkości efektu uzyskany w niniejszym badaniu.

Na podstawie porównania wyników można przypuszczać, że satysfakcja i zaangażowanie organizacyjne istotnie wpływają na intencję odejścia w całej populacji osób pracujących w służbach mundurowych, a kierunki i rząd wielkości efektu oddziaływania kluczowych zmiennych na siebie będą podobne.

Podsumowanie i wnioski

Wyniki modelowania strukturalnego PLS-SEM pozytywnie weryfikują postawione hipotezy H1 i H2. Satysfakcja z pracy, zaangażowanie organizacyjne oraz wytrwałość istotnie sprzyjają pozostaniu w służbie – wpływają dodatnio na intencję pozostania i przeciwdziałają odejściu – wpływają ujemnie (bezpośrednio lub pośrednio) na intencję odejścia. Co więcej, w modelu uwidacznia się kluczowa rola intencji pozostania jako czynnika bezpośrednio zmniejszającego intencję odejścia.

Mając na uwadze uzyskane wyniki badań z udziałem funkcjonariuszy SG, można rozważyć następujące rozwiązania praktyczne:

1. Zwiększanie retencji personelu przez koncentrację na rozwiązaniach dotyczących najważniejszych potencjalnych powodów rezygnacji ze służby, a także zapewnienie stabilności przepisów regulujących uposażenia/

[37] P. Brough, R. Frame, *Predicting Police Job Satisfaction and Turnover Intentions: The role of social support and police organisational variables*, „New Zealand Journal of Psychology" 2004, t. 33, nr 1, https://www.psychology.org.nz/journal-archive/NZJP-Vol331-2004-2-Brough.pdf, s. 8–16 [dostęp: 5 V 2025].

[38] M.W. van Eetveldt i in., *The Importance of Career Insecurity for Turnover Intentions in the Dutch Military*, „Military Psychology" 2013, t. 25, nr 5, s. 489–501. https://psycnet.apa.org/doi/10.1037/mil0000016.

[39] K.E. Dupré, A.L. Day, *The effects of supportive management and job quality on the turnover intentions and health of military personnel*, „Human Resource Management" 2007, t. 46, nr 2, s. 185–201. https://doi.org/10.1002/hrm.20156.

świadczenia/emerytury oraz waloryzację ich wysokości. Służy temu stosowanie obiektywnych i sprawiedliwych kryteriów przeniesień służbowych, uwzględniających sytuację funkcjonariusza przed podjęciem decyzji o przeniesieniu, a także szkolenia dla przełożonych i ocena przez podwładnych ich kompetencji miękkich. Planowanie pracy służb powinno uwzględniać potrzeby funkcjonariuszy, w tym regenerację ich sił.

2. Zaproponowanie jednostkom organizacyjnym SG oraz innym polskim służbom mundurowym przyjęcia przedstawionej metodyki i narzędzia badawczego do prowadzenia cyklicznych badań dotyczących satysfakcji z pracy, zaangażowania organizacyjnego, wytrwałości oraz intencji pozostania i intencji odejścia wśród funkcjonariuszy i żołnierzy w służbie stałej. Regularne monitorowanie tych wskaźników pozwoli na szybkie identyfikowanie problemów i optymalizację rozwiązań zarządczych związanych z retencją, co korzystnie wpłynie na bezpieczeństwo kadrowe i państwowe.
3. Podkreślanie w szkoleniach przeznaczonych dla kadry kierowniczej znaczenia zaangażowania organizacyjnego (oraz jego poszczególnych komponentów) jako zmiennej mogącej wymiernie wpływać na chęć kontynuacji służby. Należy rozwijać kompetencje kadry kierowniczej w zakresie kształtowania i wzmacniania zaangażowania organizacyjnego podwładnych – zwłaszcza w wymiarze afektywnym – przez odpowiedni styl przywództwa i komunikacji oraz budowanie identyfikacji z misją formacji.
4. Włączenie do procedur rekrutacyjnych i kwalifikacyjnych elementów oceny wytrwałości kandydatów do służby, np. opracowanie pytań behawioralnych lub testów pozwalających ocenić poziom wytrwałości kandydatów już na etapie naboru. Wytrwałość jest predyktorem pozostania w służbie, a osoby o wysokiej wytrwałości lepiej znoszą trudy służby i rzadziej przedwcześnie z niej rezygnują.
5. Analizowanie czynników wpływających na intencję odejścia oraz intencję pozostania w poszczególnych jednostkach SG. Jednostki organizacyjne SG mogłyby okresowo analizować, które czynniki (np. zidentyfikowane w niniejszym badaniu) najsilniej oddziałują na plany odejścia ich funkcjonariuszy, a które sprzyjają ich pozostaniu. Pozwoli to dostosować i doskonalić wewnętrzne rozwiązania kadrowe (np. programy motywacyjne, szkolenia, wsparcie psychologiczne).
6. Rozważenie zmian w systemie wynagradzania funkcjonariuszy SG. Wyniki jednoznacznie wskazują, że kwestie płacowe stanowią istotny słaby punkt wpływający na niezadowolenie funkcjonariuszy i ich skłonność do odejścia. Dostosowanie systemu wynagrodzeń – aby odczuwali oni

sprawiedliwość płac i realny wzrost wynagrodzeń wraz ze stażem i osiągnięciami – może znacznie poprawić poziom retencji.

Badanie retencji personelu stanowi wyzwanie. Warto je podejmować, gdyż uzyskane wyniki mogą pomóc w zwiększaniu bezpieczeństwa kadrowego oraz realizowaniu celów danej formacji. Bezpieczeństwo państwa wymaga zatem prowadzenia projektów badawczych pozwalających monitorować za pomocą metod statytycznych zmienne wpływające na pozostanie w służbie lub rezygnację z niej.

Osiągnięcie celu badań w postaci zidentyfikowania i pomiaru zmiennych wpływających na intencję pozostania w służbie oraz intencję odejścia ze służby pozwoliło wyłonić istotne zmienne: satysfakcję, zaangażowanie organizacyjne, wytrwałość oraz powiązać je z powodami decyzji i zasugerować inicjatywy wspierające działania zarządcze.

Metodyka, skonstruowany model strukturalny i rekomendowane rozwiązania przedstawione w artykule mogą stanowić wytyczne dla polskich służb mundurowych w zakresie pokonywania obecnych oraz minimalizowania przyszłych wyzwań związanych z retencją kadrową. Wdrożenie proponowanych inicjatyw – takich jak systematyczne monitorowanie satysfakcji, zaangażowania organizacyjnego i wytrwałości, doskonalenie warunków służby oraz rozwój kompetencji przywódczych kadry – powinno się przełożyć na poprawę retencji funkcjonariuszy SG, a tym samym na wzmocnienie potencjału tej formacji w zapewnianiu bezpieczeństwa państwa.

Opisane badania można byłoby przeprowadzić we wszystkich polskich służbach mundurowych z uwzględnieniem ich specyfiki, co w skali kraju pozwoliłoby uzyskać efekt synergii w zakresie bezpieczeństwa.

Bibliografia

Ajzen I., *From Intentions to Actions: A Theory of Planned Behawior*, w: *Action Control: From Cognition to Behavior*, J. Kuhl, J. Beckmann (red.), Berlin 1985, s. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2.

Allen N.J., Meyer J.P., *The measurement and antecedents of affective, continuance and normative commitment to the organization*, „Journal of Occupational Psychology" 1990, t. 63, nr 1, s. 1–18. https://doi.org/10.1111/j.2044-8325.1990.tb00506.x.

Becker J-M., Ringle Ch.M., Sarstedt M., Völckner F., *How collinearity affects mixture regression results*, „Marketing Letters" 2015, t. 26, nr 4, s. 643–659. https://doi.org/10.1007/s11002-014-9299-9.

Chiat L.C., Panatik S.A., *Perceptions of Employee Turnover Intention by Herzberg's Motivation-Hygiene Theory: A Systematic Literature Review*, „Journal of Research in Psychology" 2019, t. 1, nr 2, s. 10–15. https://doi.org/10.31580/jrp.v1i2.949.

Cho Y.J., Lewis G.B., *Turnover Intention and Turnover Behavior: Implications for Retaining Federal Employees*, „Review of Public Personnel Administration" 2011, t. 32, nr 1, s. 4–23. https://doi.org/10.1177/0734371X11408701.

Cohen J., *Statistical Power Analysis for the Behavioral Sciences*, New York 1988. https://doi.org/10.4324/9780203771587.

Currivan D.B., *The Causal Order of Job Satisfaction and Organizational Commitment in Models of Employee Turnover*, „Human Resource Management Review" 1999, t. 9, nr 4, s. 495–524. https://doi.org/10.1016/S1053-4822(99)00031-5.

Hair J.F. Jr., Hult G.T.M., Ringle Ch.M., Sarstedt M., Danks N.P., Ray S., *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*, seria: Classroom Companion: Business, Cham 2021. https://doi.org/10.1007/978-3-030-80519-7.

Dogonyaro H., Nwosu F., *Exploring Employee Retention in the Hospitality Industry Through Herzberg's Two-Factor Motivation Theory*, preprint. https://doi.org/10.13140/RG.2.2.34721.93287.

Duckworth A.L., Peterson C., Matthews M.D., Kelly D.R., *Grit: Perseverance and passion for long-term goals*, „Journal of Personality and Social Psychology" 2007, t. 92, nr 6, s. 1087––1101. https://doi.org/10.1037/0022-3514.92.6.1087.

Dupré K.E., Day A.L., *The effects of supportive management and job quality on the turnover intentions and health of military personnel*, „Human Resource Management" 2007, t. 46, nr 2, s. 185–201. https://doi.org/10.1002/hrm.20156.

Eetveldt M.W. van, Ven N. van de, Tooren M. van den, Versteeg R.C., *The Importance of Career Insecurity for Turnover Intentions in the Dutch Military*, „Military Psychology" 2013, t. 25, nr 5, s. 489–501. https://psycnet.apa.org/doi/10.1037/mil0000016.

Eskreis-Winkler L., Shulman E.P., Beal S.A., Duckworth A.L., *The grit effect: predicting retention in the military, the workplace, school and marriage*, „Frontiers in Psychology" 2014, t. 5, nr 36. https://doi.org/10.3389/fpsyg.2014.00036.

Falk R.F., Miller N.B., *A Primer for Soft Modeling*, Ohio 1992.

Gaertner S., *Structural Determinants of Job Satisfaction and Organizational Commitment in Turnover Models*, „Human Resource Management Review" 1999, t. 9, nr 4, s. 479–493. https://doi.org/10.1016/S1053-4822(99)00030-3.

Griffeth R.W., Hom P.W., Gaertner S., *A Meta-Analysis of Antecedents and Correlates of Employee Turnover: Update, Moderator Tests, and Research Implications for the Next Millennium*, „Journal of Management" 2000, t. 26, nr 3, s. 463–488. https://doi.org/10.1177/014920630002600305.

Hair J.F., Sarstedt M., Ringle Ch.M., Mena J.A., *An assessment of the use of partial least squares structural equation modeling in marketing research*, „Journal of the Academy of Marketing Science" 2012, t. 40, s. 414–433. https://doi.org/10.1007/s11747-011-0261-6.

Henseler J., Ringle Ch.M., Sarstedt M., *A new criterion for assessing discriminant validity in variance-based structural equation modeling*, „Journal of the Academy of Marketing Science" 2015, t. 43, s. 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hom P.W., Caranikas-Walker F., Prussia G.E., Griffeth R.W., *A meta-analytical structural equations analysis of a model of employee turnover*, „Journal of Applied Psychology" 1992, t. 77, nr 6, s. 890–909. https://doi.org/10.1037/0021-9010.77.6.890.

Huffman A.H., Adler A.B., Dolan C.A., Castro C.A., *The Impact of Operations Tempo on Turnover Intentions of Army Personnel*, „Military Psychology" 2005, t. 17, nr 3, s. 175–202. https://doi.org/10.1207/ s15327876mp1703_4.

Jankowski K.S., Zajenkowski M., *Metody szacowania rzetelności pomiaru testem*, w: *Psychometria – podstawowe zagadnienia*, K. Fronczyk (red.), Warszawa 2009, s. 84–110.

Kacprzak A., *Modelowanie strukturalne w analizie zachowań konsumentów: porównanie metod opartych na analizie kowariancji (CB-SEM) i częściowych najmniejszych kwadratów (PLS-SEM)*, „Handel Wewnętrzny" 2018, t. 1, nr 6, s. 247–261.

Kelly D.R., Matthews M.D., Bartone P.T., *Grit and Hardiness as Predictors of Performance Among West Point Cadets*, „Military Psychology" 2014, t. 26, nr 4, s. 327–342. https://doi.org/10.1037/mil0000050.

Lee T.W., Mitchell T.R., *The unfolding effects of organizational commitment and anticipated job satisfaction on voluntary employee turnover*, „Motivation and Emotion" 1991, t. 15, nr 1, s. 99–121. https://doi.org/10.1007/BF00991478.

Lytell M.C., Drasgow F., *"Timely" Methods: Examining Turnover Rates in the U.S. Military*, „Military Psychology" 2009, t. 21, nr 3, s. 334–350. https://doi.org/10.1080/08995600902914693.

Marrone J.V., *Predicting 36-Month Attrition in the U.S. Military: A Comparison Across Service Branches*, Santa Monica 2020. https://doi.org/10.7249/RR4258.

Meyer J.P., Allen N.J., *A three-component conceptualization of organizational commitment*, „Human Resource Management Review" 1991, t. 1, nr 1, s. 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z.

Mobley W.H., Horner S.O., Hollingsworth A.T., *An evaluation of precursors of hospital employee turnover*, „Journal of Applied Psychology" 1978, t. 63, nr 4, s. 408–414. https://doi.org/10.1037/0021-9010.63.4.408.

Mowday R.T., Steers R.M., Porter L.W., *The measurement of organizational commitment*, „Journal of Vocational Behavior" 1979, t. 14, nr 2, s. 224–247. https://doi.org/10.1016/0001-8791(79)90072-1.

Pitts D., Marvel J., Fernandez S., *So Hard to Say Goodbye? Turnover Intention among U.S. Federal Employees*, „Public Administration Review" 2011, t. 71, nr 5, s. 751–760. https://doi.org/10.1111/j.1540-6210.2011.02414.x.

Ratzmann M., Gudergan S.P., Bouncken R., *Capturing heterogeneity and PLS-SEM prediction ability: Alliance governance and innovation*, „Journal of Business Research" 2016, t. 69, nr 10, s. 4593–4603. https://doi.org/10.1016/j.jbusres.2016.03.051.

Richter N.F., Cepeda G., Roldán J.L., Ringle Ch.M., *European management research using partial least squares structural equation modeling (PLS-SEM)*, „European Management Journal" 2016, t. 34, nr 6, s. 589–597. https://doi.org/10.1016/j.emj.2016.08.001.

Sheppard B.H., Hartwick J., Warshaw P.R., *The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research*, „Journal of Consumer Research" 1988, t. 15, nr 3, s. 325–343. https://doi.org/10.1086/209170.

Shmueli G., Sarstedt M., Hair J.F., Cheah J-H., Ting H., Vaithilingam S., Ringle Ch.M., *Predictive model assessment in PLS-SEM: guidelines for using PLSpredict*, „European Journal of Marketing" 2019, t. 53, nr 11, s. 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189.

Spector P.E., *The Nature of Job Satisfaction*, w: tegoż, *Job Satisfaction: Application, Assessment, Causes, and Consequences*, London 1997. https://doi.org/10.4135/9781452231549.n1.

Tett R.P., Meyer J.P., *Job satisfaction, organizational commitment, turnover intention, and turnover: Path analyses based on meta-analytic findings*, „Personnel Psychology" 1993, t. 46, nr 2, s. 259–293. https://doi.org/10.1111/j.1744-6570.1993.tb00874.x.

Źródła internetowe

Brough P., Frame R., *Predicting Police Job Satisfaction and Turnover Intentions: The role of social support and police organisational variables*, „New Zealand Journal of Psychology" 2004, t. 33, nr 1, https://www.psychology.org.nz/journal-archive/NZJP-Vol331-2004-2-Brough.pdf, s. 8–16 [dostęp: 5 V 2025].

Herzberg F., Mausner B., Snyderman B.B., *The Motivation to Work*, New York 1959, https://api.pageplace.de/preview/DT0400.9781351504430_A30546568/preview-9781351504430_A30546568.pdf [dostęp: 18 I 2025].

Locke E.A., *The Nature and Causes of Job Satisfaction*, College Park 1976, https://www.researchgate.net/publication/238742406_The_Nature_and_Causes_of_Job_Satisfaction [dostęp: 13 I 2025].

Strickland W.J., *A Longitudinal Examination of First Term Attrition and Reenlistment Among FY1999 Enlisted Accessions*, https://apps.dtic.mil/sti/tr/pdf/ADA448564.pdf [dostęp: 10 I 2025].

Inne dokumenty

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli pt. Realizacja programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2017–2020*, https://www.nik.gov.pl/plik/id,21396,vp,24037.pdf [dostęp: 12 II 2025].

North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel. Final Report of Research Task Group HFM-107*, https://apps.dtic.mil/sti/tr/pdf/ADA476488.pdf [dostęp: 11 I 2025].

Roach K.N., *Leveraging Grit in Military Research: A Comprehensive Review*, https://apps.dtic.mil/sti/trecms/pdf/AD1211251.pdf [dostęp: 20 I 2025].

Weiss H.M., MacDermid S.M., Strauss R., Kurek K.E., Le B., Robbins D., *Retention in the Armed Forces: Past Approaches and New Research Directions*, https://www.mfri.purdue.edu/wpcontent/uploads/2018/03/Retention-in-the-Armed-Forces.pdf [dostęp: 17 I 2025].

Dr Radosław Wiśniewski

Funkcjonariusz Straży Granicznej, pełni służbę w Wyższej Szkole Straży Granicznej w Koszalinie. Absolwent Uniwersytetu Szczecińskiego, w którym w 2015 r. uzyskał stopień naukowy doktora nauk ekonomicznych w dyscyplinie nauki o zarządzaniu. W WSSG wykłada zagadnienia dotyczące zarządzania zasobami ludzkimi oraz realizuje projekty badawcze, m.in. „Badanie skuteczności i efektywności systemu motywacyjnego funkcjonariuszy Straży Granicznej oraz preferencji motywacyjnych potencjalnych kandydatów do służby z tzw. pokolenia Z", „Kohortowe badanie retencji funkcjonariuszy Straży Granicznej".

Kontakt: radekwisniewski@poczta.onet.pl

Denis Tomala

Funkcjonariusz pełniący służbę w Wyższej Szkole Straży Granicznej w Koszalinie, wcześniej funkcjonariusz Policji. Absolwent kierunków inżynieria środowiska oraz geodezja i kartografia na Wydziale Inżynierii Lądowej, Środowiska i Geodezji Politechniki Koszalińskiej. Zajmuje się wykorzystaniem analizy danych i metod statystycznych do badania zagadnień zarządczych i społecznych w obszarze bezpieczeństwa.

Kontakt: denis8908@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 111–131

https://doi.org/10.4467/20801335PBW.26.005.23367

ARTYKUŁ

Morskie farmy wiatrowe jako infrastruktura krytyczna w dobie zagrożeń hybrydowych – nowy wymiar bezpieczeństwa energetycznego Polski

Offshore wind farms as critical infrastructure in the era of hybrid threats – a new dimension of Poland's energy security

KLAUDIA MACIATA

Politechnika Gdańska

https://orcid.org/0000-0001-6227-2851

Abstrakt

Morskie farmy wiatrowe (offshore wind farms, OWFs) stają się kluczowym elementem bezpieczeństwa energetycznego Polski. Z uwagi na lokalizację i charakter są one podatne na zagrożenia hybrydowe. Autorka artykułu omówiła OWFs jako nowy komponent infrastruktury krytycznej w kontekście incydentów na Morzu Bałtyckim od 2022 r. oraz przeanalizowała stopień odporności OWFs w aspekcie zagrożeń hybrydowych. Opisała luki prawne i organizacyjne w polskim systemie ochrony infrastruktury, wskazała dobre praktyki stosowane na świecie oraz rekomendacje dla administracji i operatorów w Polsce. Zwróciła uwagę na potrzebę testowania odporności OWFs z wykorzystaniem symulacji digital twin i ćwiczeń red teaming. Postulatem autorki jest złożone podejście do bezpieczeństwa OWFs – integrujące działania legislacyjne, technologiczne i organizacyjne. Artykuł stanowi wkład w dyskurs na temat redefinicji bezpieczeństwa energetycznego Polski w dobie rywalizacji poniżej progu wojny.

Słowa kluczowe

morskie farmy wiatrowe, infrastruktura krytyczna, zagrożenia hybrydowe, bezpieczeństwo energetyczne, Morze Bałtyckie, ochrona infrastruktury

Abstract

Offshore wind farms (OWFs) are becoming a key component of Poland's energy security. Due to location and nature, they are vulnerable to hybrid threats. The author of the article discussed OWFs as a new component of critical infrastructure in the context of incidents in the Baltic Sea since 2022 and analysed the degree of OWF resilience in the context of hybrid threats. The author described legal and organisational gaps in the Polish infrastructure protection system, pointed out best practices used around the world, and made recommendations for the administration and operators in Poland. She drew attention to the need to test the resilience of OWFs using digital twin simulations and red teaming exercises. The author advocates a complex approach to OWF security, integrating legislative, technological and organisational measures. The article contributes to the discourse on redefining Poland's energy security in an era of competition below the threshold of war.

Keywords

offshore wind farms, critical infrastructure, hybrid threats, energy security, Baltic Sea, infrastructure protection

Wprowadzenie

Transformacja energetyczna w kierunku niskoemisyjnych źródeł energii czyni morskie farmy wiatrowe (offshore wind farms, OWFs[1]) jednym z najważniejszych elementów nowoczesnego systemu bezpieczeństwa energetycznego Polski. Ich rozwój wpisuje się w cele polityki klimatyczno-energetycznej Unii Europejskiej, w tym w osiągnięcie neutralności klimatycznej do 2050 r. oraz we wzrost udziału odnawialnych źródeł energii (OZE) w miksie energetycznym państw członkowskich[2]. Morskie farmy wiatrowe budowane przez Polskę na Morzu Bałtyckim docelowo mają dostarczać do 2040 r. do 11 GW mocy zainstalowanej, co czyni je największym projektem infrastrukturalnym w historii polskiego sektora OZE[3]. W skali europejskiej prognozuje się wzrost mocy zainstalowanej morskiej energetyki wiatrowej

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

[2] Komisja Europejska, *Plan REPowerEU*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [dostęp: 20 VI 2025].

[3] Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r. (PEP2040)*, Warszawa 2021.

z ok. 90 GW w połowie dekady do ok. 170 GW do 2030 r. To oznacza niemal dwukrotne zwiększenie potencjału tego sektora[4].

Rosnące znaczenie OWFs jako zasobu energetycznego stwarza nowe wyzwania w obszarze bezpieczeństwa. Infrastruktura ta, zlokalizowana na otwartym morzu, poza strefą wód terytorialnych i rozproszona przestrzennie, jest narażona na zagrożenia hybrydowe. Obejmują one działania poniżej progu wojny takie jak sabotaż, cyberataki, zakłócenia nawigacyjne czy operacje dezinformacyjne oraz inne opisane w literaturze przedmiotu[5]. Działania te mają na celu nie tylko testowanie odporności infrastruktury krytycznej (IK), lecz także wywieranie presji strategicznej i geopolitycznej poniżej progu konfliktu zbrojnego, generowanie kosztów ekonomicznych, osłabianie zdolności reagowania państwa oraz podważanie jego wiarygodności jako podmiotu zdolnego do kontroli i ochrony przestrzeni morskiej.

Na poziomie UE kwestia bezpieczeństwa OWFs została uregulowana w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych (Critical Entities Resilience, dalej: dyrektywa CER), która zastąpiła wcześniejszą dyrektywę o europejskiej IK[6]. Nowe przepisy zobowiązują państwa członkowskie do identyfikacji i ochrony podmiotów krytycznych w 12 sektorach, w tym w sektorze energetycznym, bez rozróżnienia na infrastrukturę lądową i morską. Morskie farmy wiatrowe, jako element sieci produkcji i przesyłu energii elektrycznej, w oczywisty sposób wpisują się w ten zakres, a operatorzy tych instalacji są zobowiązani do wdrażania środków zwiększających ich odporność fizyczną i cybernetyczną.

W najnowszych analizach think tanku Centrum Studiów Strategicznych i Międzynarodowych (Center for Strategic and International Studies) oraz Centrum Eksperckiego NATO ds. Komunikacji Strategicznej (NATO Strategic Communication Centre of Excellence) OWFs są postrzegane jako tzw. soft targets – cele o wysokiej wartości strategicznej i relatywnie niskim poziomie ochrony[7]. Ich położenie z dala od wybrzeży, zależność od zautomatyzowanych systemów sterowania (SCADA/OT;

---

4 *Energy Transition Outlook 2025*, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [dostęp: 20 VI 2025].

5 A. Sari, *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 20 VI 2025]; *Countering hybrid threats*, NATO, 7 V 2024 r., https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [dostęp: 20 VI 2025].

6 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE*, s. 164–186.

7 A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/, s. 5–8 [dostęp: 20 VI 2025].

supervisory control and data acquisition/operational technology), a także skomplikowana struktura własnościowa i regulacyjna – m.in. prawo morza, które przez gwarantowanie swobód żeglugowych ułatwia agresorom kreowanie zagrożeń – czynią je podatnymi na działania przeciwnika w szarej strefie (gray zone). Przykładami tych zagrożeń mogą być rozwijane od lat przez Chiny i Rosję (Główny Zarząd Badań Głębinowych, GUGI) zdolności podwodne czy flota cieni (shadow fleet)[8].

Celem artykułu jest przedstawienie OWFs jako nowego komponentu IK w Polsce oraz przeanalizowanie stopnia ich odporności w obliczu rosnących zagrożeń hybrydowych. Szczególną uwagę poświęcono trzem obszarom: lukom prawnym i organizacyjnym w polskim systemie ochrony IK, dobrym praktykom na poziomach krajowym i międzynarodowym w zakresie ochrony OWFs oraz rekomendacjom dla decydentów i operatorów w Polsce. Artykuł stanowi wkład w dyskusję o konieczności redefinicji bezpieczeństwa energetycznego w kontekście rywalizacji poniżej progu wojny oraz ochrony zasobów energetycznych w przyszłości.

Ewolucja zagrożeń hybrydowych od 2022 roku – opis przypadków

Wraz z rozpoczęciem pełnoskalowej agresji Federacji Rosyjskiej na Ukrainę w lutym 2022 r. zaobserwowano wzrost liczby incydentów o charakterze hybrydowym, skierowanych przeciwko państwom UE i Sojuszu Północnoatlantyckiego. Obiektem tych działań coraz częściej staje się infrastruktura podmorska, w tym systemy energetyczne i komunikacyjne w regionie Morza Bałtyckiego. Działania te cechuje niska wykrywalność, trudność w jednoznacznym przypisaniu odpowiedzialności oraz prowadzenie ich poniżej progu otwartego konfliktu zbrojnego. W tym kontekście OWFs, stanowiące strategiczne źródło energii, jawią się jako nowa przestrzeń rywalizacji w szarej strefie[9].

Punktem zwrotnym w postrzeganiu zagrożeń wobec infrastruktury morskiej był sabotaż gazociągów Nord Stream 1 i Nord Stream 2 we wrześniu 2022 r. Do eksplozji doszło na wodach terytorialnych Szwecji i Danii, a ich skutkiem było trwałe wyłączenie obu nitek przesyłowych. Szwedzkie służby stwierdziły obecność śladów

[8] T. Szubrycht, *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim*, „Bezpieczeństwo Narodowe" 2025, t. 46, nr 1, s. 49–75. https://doi.org/10.59800/bn/207646.

[9] M. Cavcic, *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, Offshore Energy, 11 XII 2024 r., https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [dostęp: 19 VI 2025].

materiałów wybuchowych i uznały zdarzenie za sabotaż[10]. Mimo że sprawca nie został jednoznacznie wskazany, zdarzenie to uświadomiło opinii publicznej, że infrastruktura podmorska może zostać zaatakowana za pomocą środków poniżej progu wojny.

W październiku 2023 r. doszło do poważnego incydentu dotyczącego gazociągu Balticconnector, łączącego Finlandię i Estonię. Śledztwo wykazało, że rurociąg został przecięty przez kotwicę kontenerowca Newnew Polar Bear, która naruszyła również biegnący równolegle kabel telekomunikacyjny[11]. Premier Finlandii Petteri Orpo poinformował opinię publiczną, że uszkodzenie było celowe i można je uznać za działania hybrydowe[12].

W grudniu 2024 r. został naruszony podmorski kabel energetyczno-telekomunikacyjny EstLink 2, który łączy Estonię i Finlandię. Jak podała fińska policja, doszło do tego w wyniku przeciągnięcia kotwicy przez statek Eagle S należący do rosyjskiej floty cieni. Incydent był przedmiotem dochodzenia z udziałem służb wywiadowczych i został zakwalifikowany jako działanie mogące zagrażać bezpieczeństwu IK[13].

Coraz częściej w rejonie Bałtyku obserwuje się również zakłócenia sygnału GPS i AIS (automatic identification system – system automatycznej identyfikacji jednostek), zwłaszcza w okolicach Gotlandii, norweskiego Finnmarku oraz Zatoki Fińskiej[14]. Zakłócenia te, wywoływane najprawdopodobniej przez systemy walki radioelektronicznej, mają bezpośredni wpływ na bezpieczeństwo nawigacji cywilnej i wojskowej.

W literaturze przedmiotu dotyczącej bezpieczeństwa morskiego oraz ochrony morskiej IK do klasyfikacji zagrożeń coraz częściej stosuje się podejście domenowe[15]. Pozwala to na precyzyjniejsze powiązanie charakteru zagrożenia z adekwatnymi środkami detekcji, ochrony i reagowania. W odniesieniu do OWFs zagrożenia

---

[10] J. Henley, *'Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022 r., https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [dostęp: 19 VI 2025].

[11] *Finnish media: Balticconnector pipeline leak 'does not appear to be an accident'*, ERR News, 10 X 2023 r., https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [dostęp: 19 VI 2025].

[12] *Finland blames Chinese ship for Baltic Sea gas pipeline damage*, Euronews, 25 X 2023 r., https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [dostęp: 19 VI 2025].

[13] C. Smith, *Finland investigates Russia's 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024 r., https://www.bbc.com/news/articles/cr56l7prj2mo [dostęp: 19 VI 2025].

[14] *Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni*, Portal Morski, 18 I 2025 r., https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [dostęp: 19 VI 2025].

[15] R. Miętkiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa*, „Sprawy Międzynarodowe" 2019, t. 72, nr 1. https://doi.org/10.35757/SM.2019.72.1.06.

hybrydowe należy analizować nie jako jednorodne „formy", ale jako działania realizowane w odrębnych, lecz przenikających się domenach operacyjnych.

Domeny nawodnej dotyczą zagrożenia o charakterze fizycznym, obejmujące m.in. sabotaż jednostek serwisowych, celowe kolizje statków z elementami infrastruktury OWFs, nieautoryzowaną obecność jednostek w strefach bezpieczeństwa czy działania realizowane z wykorzystaniem floty cieni[16]. Z perspektywy bezpieczeństwa operacyjnego domena ta jest szczególnie istotna w czasie eksploatacji OWFs.

Domena podwodna obejmuje działania skierowane przeciwko infrastrukturze ukrytej pod powierzchnią morza, zwłaszcza kablom eksportowym służącym do przesyłu energii (export cables) i kablom wewnętrznym (array cables) oraz światłowodom telekomunikacyjnym. W literaturze wskazuje się, że działania w tej domenie charakteryzują się wysokim progiem wykrywalności, asymetrią kosztów oraz trudnością z jednoznacznym przypisaniem sprawstwa. Jest to zatem szczególnie użyteczne narzędzie oddziaływań hybrydowych[17].

W domenie cybernetycznej zagrożenia dotyczą przede wszystkim ataków na systemy SCADA/OT, systemy zarządzania energią oraz infrastrukturę IT operatorów OWFs. Cyberataki mogą prowadzić zarówno do zakłóceń operacyjnych, jak i do naruszenia bezpieczeństwa fizycznego farm przez ingerencję w systemy monitoringu, pozycjonowania czy sterowania turbinami wiatrowymi.

Domena informacyjna obejmuje działania dezinformacyjne i operacje wpływu, których celem jest zmniejszenie poziomu społecznej akceptacji dla OWFs, kwestionowanie ich bezpieczeństwa i opłacalności oraz eksponowanie negatywnego wpływu tych farm na środowisko morskie. Działania te mogą pośrednio wpływać na decyzje regulacyjne, inwestycyjne oraz tempo rozwoju sektora morskiej energetyki wiatrowej[18].

W domenie radioelektronicznej są identyfikowane zagrożenia polegające na zakłócaniu sygnałów GNSS (global navigation satellite system), łączności morskiej oraz systemów nawigacyjnych wykorzystywanych przez jednostki serwisowe i systemy autonomiczne[19]. Zakłócenia te mogą stanowić element przygotowania lub wsparcia działań fizycznych i podmorskich.

Domenowe ujęcie zagrożeń, obecne w nowszych analizach dotyczących bezpieczeństwa morskiego i energetycznego, pozwala na odejście od uproszczonego

[16] M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, „Ekspertyzy PTBN" 2023, nr 1.

[17] Tamże.

[18] R. Miętkiewicz, *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych*, „Gospodarka Materiałowa i Logistyka" 2017, nr 12, s. 688–702.

[19] Tamże.

podziału na „formy zagrożeń" na rzecz systemowej analizy wielodomenowej, lepiej odpowiadającej charakterowi zagrożeń hybrydowych wobec OWFs.

Zdaniem wiceadmirała Didiera Maleterre'a z NATO Allied Maritime Command przestrzeń Morza Bałtyckiego stała się nową areną działań destabilizacyjnych, w której celem jest nie tylko sprzęt, lecz także cała zdolność państw do skutecznego reagowania[20]. Skala, częstotliwość i złożoność tych incydentów świadczą o konieczności adaptacji narodowych strategii ochrony infrastruktury do realiów szarej strefy i uwzględnienia OWFs jako potencjalnych celów.

Analiza luk w systemie ochrony infrastruktury krytycznej w Polsce

Polski system ochrony IK, mimo rozwoju legislacyjnego, nie nadąża za specyfiką zagrożeń hybrydowych wobec obiektów offshore, w tym OWFs. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* oraz *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* tworzą ramy formalne dla ochrony IK, ale OWFs nie zostały jednoznacznie sklasyfikowane jako IK o znaczeniu strategicznym. W *Polityce energetycznej Polski do 2040 roku* (PEP2040) wskazano OWFs jako kluczowy element transformacji energetycznej i bezpieczeństwa dostaw, ale dokument nie zawiera opisu procedur i mechanizmów ochrony przeznaczonych dla infrastruktury offshore[21].

Brak precyzyjnych przepisów skutkuje niejasnym podziałem kompetencji międzyresortowych. Nie wskazano wyraźnie, które instytucje odpowiadają za prewencję, monitoring i reagowanie na zagrożenia wobec OWFs. Formalnie zadania z zakresu ochrony IK realizują Agencja Bezpieczeństwa Wewnętrznego, Straż Graniczna, Marynarka Wojenna RP oraz Centrum Operacyjne Ministra Obrony Narodowej, ale nie istnieje zintegrowany mechanizm koordynacji między tymi podmiotami. Sytuację dodatkowo komplikuje brak jednoznacznych wytycznych dla operatorów OWFs co do obowiązków informacyjnych i współpracy z państwowymi centrami zarządzania kryzysowego (Rządowym Centrum Bezpieczeństwa, CERT Polska, CSIRT MON)[22].

---

[20] M. Bryant, *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024 r., https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [dostęp: 19 VI 2025].

[21] Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r…*

[22] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych…*

W raporcie przygotowanym przez Europejskie Centrum Doskonałości ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats) zostały wskazane poważne luki w zakresie testowania odporności infrastruktury offshore na działania hybrydowe. Przepisy krajowe nie przewidują obowiązku prowadzenia regularnych ćwiczeń z udziałem operatorów OWFs, służb porządkowych i struktur wojskowych. Nie stosuje się również narzędzi takich jak red teaming czy realistyczne symulacje digital twin, które pozwoliłyby na ocenę odporności technicznej i organizacyjnej OWFs w warunkach zakłóceń fizycznych, cybernetycznych czy działań dezinformacyjnych[23].

Kolejnym obszarem problemowym jest niewystarczające dostosowanie do warunków morskich przepisów dotyczących fizycznej ochrony IK. Obowiązujące regulacje opierają się na modelu ochrony infrastruktury lądowej, co powoduje trudności we wdrażaniu systemów zabezpieczeń w środowisku morskim (np. patrolowanie akwenów, instalacja detektorów akustycznych, integracja radarowa)[24]. Brakuje również zharmonizowanych procedur ochrony kabli energetycznych i fundamentów obiektów IK. Istnieją jednak zasady tworzenia systemów ochrony stacji transformatorowych i linii kablowych zawarte w *Rozporządzeniu Ministra Klimatu i Środowiska z dnia 25 maja 2022 r. w sprawie szczegółowych wymagań dla elementów zespołu urządzeń służących do wyprowadzenia mocy oraz dla elementów stacji elektroenergetycznych zlokalizowanych na morzu*.

W zakresie cyberbezpieczeństwa brakuje spójności. Według ustaleń Najwyższej Izby Kontroli wiele jednostek samorządowych i operatorów energetycznych nie posiada zaktualizowanych planów reagowania na cyberincydenty ani nie wdraża standardów pokrewnych do tych zawartych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dalej: dyrektywa NIS 2)[25] oraz w normie PN-EN ISO/IEC 27001 dotyczącej Systemu Zarządzania Bezpieczeństwem Informacji[26]. Chociaż niektórzy operatorzy OWFs działający w Polsce (np. Ørsted, Equinor) implementują dobre praktyki zaczerpnięte ze skandynawskich rynków, to nie istnieje narodowy standard cyberbezpieczeństwa przeznaczony dla infrastruktury offshore.

---

[23] A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[24] A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats*…

[25] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)*, s. 80–152.

[26] Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego*, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [dostęp: 20 VI 2025].

Ze strategicznego punktu widzenia główną lukę stanowi brak kompleksowej, międzyresortowej strategii ochrony infrastruktury morskiej jako całości. Obecne dokumenty strategiczne, w tym *Krajowy Plan Zarządzania Kryzysowego* (KPZK)[27] czy *Doktryna cyberbezpieczeństwa RP*[28], nie uwzględniają specyfiki OWFs jako obiektów o podwójnej wrażliwości – energetycznej i morskiej. Ochrona OWFs wymaga podejścia multidomenowego, obejmującego komponenty militarne (ochrona przed sabotażem), informatyczne (ochrona cyber), instytucjonalne (koordynacja) i inżynieryjne (zaawansowanie techniczne). Należy nadmienić, że w Narodowym Programie Ochrony Infrastruktury Krytycznej 2023 uwzględniono działania techniczne, prowadzone głównie przez Rządowe Centrum Bezpieczeństwa i operatorów IK (w tym przypadku OWFs). Obejmują one: tworzenie grup roboczych i opracowanie standardów bezpieczeństwa IK, identyfikację i weryfikację skuteczności tychże, stworzenie bazy incydentów, do których doszło na obiektach IK, oraz platform szkoleniowych dla operatorów IK i administracji[29].

Istotnym kontekstem dla oceny skuteczności krajowego systemu ochrony OWFs jako IK są zmiany w prawie UE wynikające z dyrektywy CER oraz jej relacji z dyrektywą NIS 2.

Dyrektywa CER wprowadza fundamentalną zmianę w podejściu do ochrony IK polegającą na odejściu od modelu ochrony „obiektów" na rzecz identyfikacji i regulacji podmiotów krytycznych, w tym podmiotów o szczególnym znaczeniu dla Europy. Nakłada ona na te podmioty szereg publicznoprawnych obowiązków, obejmujących m.in.: przeprowadzanie regularnych ocen ryzyka, wdrażanie środków technicznych i organizacyjnych służących zapewnieniu odporności, obowiązek zgłaszania incydentów oraz poddanie się nadzorowi właściwych organów, które są wyposażone w instrumenty sankcyjne.

Dyrektywa NIS 2 przewiduje, że podmioty zidentyfikowane na gruncie dyrektywy CER jako mające charakter krytyczny powinny być uznane za podmioty kluczowe również w rozumieniu przepisów o cyberbezpieczeństwie, co wynika z art. 2 ust. 3 dyrektywy NIS 2.

Mechanizm „automatycznego" objęcia OWFs podwójnym reżimem regulacyjnym rodzi ryzyko kolizji normatywnych oraz rozproszenia odpowiedzialności instytucjonalnej w procesie implementacji obu dyrektyw do polskiego porządku

[27] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*, https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [dostęp: 20 VII 2025].

[28] Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 20 VI 2025].

[29] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, Warszawa 2023.

prawnego. W tym kontekście zasadne wydaje się rozważenie spójnego modelu nadzoru i reagowania, w tym ustanowienia wyspecjalizowanych struktur sektorowych, takich jak CSIRT ENERGY (Computer Security Incident Response Team for the Energy Sector), zdolnych do obsługi specyfiki energetycznej infrastruktury offshore.

Dodatkowym problemem jest czas implementacji przepisów. Termin transpozycji dyrektywy CER upłynął 17 października 2024 r., a nowelizacja ustawy o zarządzaniu kryzysowym oraz wydania aktów wykonawczych nadal jest w toku. Eksploatacja pierwszych OWFs na polskich obszarach Morza Bałtyckiego ma się rozpocząć w 2026 r. W okresie przejściowym infrastruktura ta może zatem funkcjonować w stanie regulacyjnego zawieszenia i być objęta instrumentami ochrony niedostosowanymi do realiów sektora offshore. Uzasadnione jest zatem pytanie, czy projektowane rozwiązania legislacyjne będą stanowiły skuteczny i koherentny instrument budowania odporności na zagrożenia hybrydowe, czy też ujawnią się kolejne luki systemowe w momencie uruchamiania OWFs.

Przykłady dobrych praktyk na poziomach krajowym i międzynarodowym

W odpowiedzi na rosnące zagrożenia hybrydowe wobec infrastruktury morskiej państwa NATO i UE rozwijają wieloaspektowe modele ochrony, łączące działania wojskowe, cywilne i techniczne. Szczególne znaczenie mają doświadczenia państw o rozwiniętym sektorze offshore – Wielkiej Brytanii, Holandii oraz państw nordyckich, które wypracowały nowoczesne instrumenty reagowania i prewencji.

Na poziomie sojuszniczym NATO rozwija koncepcję Baltic Sentry[30] – wspólnego systemu patrolowania i rozpoznania IK na Morzu Bałtyckim. Program ten zakłada integrację działań sił państw nadmorskich oraz współdzielenie danych pomiędzy strukturami NATO, operatorami prywatnymi oraz cywilnymi instytucjami odpowiedzialnymi za ochronę IK. Istotnym elementem Baltic Sentry jest wykorzystanie zaawansowanych narzędzi analitycznych, w tym systemów opartych na sztucznej inteligencji, służących do wykrywania anomalii w ruchu morskim, identyfikacji nietypowych wzorców zachowań jednostek oraz wczesnego ostrzegania przed potencjalnymi działaniami hybrydowymi. Rozwiązania te są rozwijane i wykorzystywane m.in. w ramach struktur NATO Allied Maritime Command (MARCOM) i obejmują swoim zakresem operacyjnym również Morze Bałtyckie.

[30] *NATO launches 'Baltic Sentry' to increase critical infrastructure security*, NATO, 14 I 2025 r., https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [dostęp: 6 I 2026].

W ramach Baltic Sentry są prowadzone wspólne ćwiczenia oraz rozwijane zdolności podwodne i bezzałogowe. Uzupełnieniem tych działań jest uruchomienie wyspecjalizowanego Morskiego Centrum Bezpieczeństwa ds. Krytycznej Infrastruktury Podwodnej (Maritime Centre for Security of Critical Undersea Infrastructure)[31], którego zadaniem jest koordynacja analiz, wymiana informacji oraz wsparcie państw sojuszniczych w zakresie ochrony podmorskiej IK.

Unia Europejska, uzupełniając działania wojskowe, rozwija platformę CISE (Common Information Sharing Environment). System ten umożliwia współdzielenie danych między strażami granicznymi, służbami ochrony środowiska, jednostkami służb ratownictwa morskiego (search and rescue, SAR), a także prywatnymi operatorami infrastruktury morskiej. Docelowo CISE ma zwiększyć tzw. świadomość sytuacyjną na morzu (maritime situational awareness) w czasie pokoju, kryzysu i konfliktu[32].

Dobrą praktyką jest również model partnerstwa publiczno-prywatnego stosowany w Holandii i Norwegii. Operatorzy OWFs współpracują z siłami zbrojnymi i agencjami rządowymi przy tworzeniu wspólnych procedur zarządzania ryzykiem, reagowania na incydenty oraz testowania odporności fizycznej i cybernetycznej farm. Specjaliści z brytyjskiej organizacji non profit Carbon Trust oraz z firmy konsultingowej ABPmer opracowali szereg standardów technicznych i wytycznych dla operatorów, m.in. w zakresie zabezpieczeń kabli, fundamentów i systemów SCADA[33].

Wyróżniającym się podejściem jest również implementacja zasady „defence by design", czyli projektowania infrastruktury offshore z uwzględnieniem odporności na działania hybrydowe. Oznacza to np. instalowanie redundantnych systemów zasilania i transmisji danych, lokalizowanie punktów wrażliwych pod poziomem dna morskiego oraz fizyczne separowanie systemów krytycznych.

Wielka Brytania, jako jedno z pierwszych państw, uruchomiła specjalną jednostkę do ochrony infrastruktury podmorskiej. W 2023 r. Marynarka Królewska wprowadziła do służby w Królewskiej Flocie Pomocniczej (Royal Fleet Auxiliary) okręt Proteus w ramach programu MROSS (Multi-Role Ocean Surveillance Ship). Jednostka ta została wyposażona w systemy sonarowe, podwodne drony oraz

[31] *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure*, MARCOM NATO, 28 V 2024 r., https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [dostęp: 6 I 2026].

[32] *Common information sharing environment (CISE)*, European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 20 VI 2025].

[33] *Industry leaders agree best practice for protecting offshore wind cables*, Carbon Trust, 13 XI 2024 r., https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [dostęp: 20 VI 2025].

centrum analiz danych, które umożliwiają monitorowanie kabli i OWFs w czasie rzeczywistym[34].

Dania wdraża z kolei innowacyjne systemy opierające się na technologii autonomicznej. Testowane są platformy Saildrone Voyager – bezzałogowe jednostki pływające z napędem żaglowym, zdolne do wielotygodniowego monitorowania wybranych obiektów na Bałtyku. Urządzenia te są wyposażone w sensory meteorologiczne, radar, kamery termowizyjne i zestawy do AIS[35].

Z międzynarodowych doświadczeń wynika, że skuteczna ochrona OWFs nie może ograniczać się do zabezpieczeń fizycznych i cyfrowych, ale musi być częścią zintegrowanego, międzysektorowego systemu reagowania. Niektóre państwa nadbałtyckie (Estonia, Finlandia i Szwecja) wdrażają aktualnie modele narodowe, które integrują straż przybrzeżną, służby wywiadowcze, operatorów sieci energetycznej oraz wojsko. Model ten może stanowić inspirację dla Polski, zwłaszcza w kontekście braku klarownych procesów koordynacyjnych.

W wymiarze operacyjnym w Polsce są rozwijane również inicjatywy ukierunkowane na cyfrowe wsparcie monitoringu i ochrony infrastruktury morskiej w regionie Morza Bałtyckiego, w tym programy określane roboczo jako Digital Baltic[36]. Ich celem jest integracja danych pochodzących z systemów nadzoru morskiego, sensorów technicznych oraz źródeł operatorów w celu zwiększenia świadomości sytuacyjnej na morzu. Inicjatywy te wpisują się w szerszy trend wykorzystania narzędzi cyfrowych i analitycznych do wczesnego wykrywania anomalii oraz wspierania procesów decyzyjnych w czasie pokoju i kryzysu[37]. Istotną rolę w systemie ochrony infrastruktury morskiej odgrywa Morski Oddział Straży Granicznej (MOSG)[38], którego zadania obejmują m.in. ochronę polskiej granicy morskiej, zapewnienie bezpieczeństwa żeglugi oraz reagowanie na incydenty w pasie morza terytorialnego, gdzie są zlokalizowane newralgiczne elementy infrastruktury, w tym odcinki linii eksportowych OWFs. Włączenie MOSG w model ochrony OWFs stanowi

[34] *RFA Proteus (K60)*, Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [dostęp: 20 VI 2025].

[35] *Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea*, Saildrone, 16 VI 2025 r., https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [dostęp: 20 VI 2025].

[36] Digital Baltic, https://digitalbaltic.pl [dostęp: 7 I 2026].

[37] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*, „Nautologia" 2024, nr 161, s. 71–76.

[38] *Zadania Morskiego Oddziału Straży Granicznej*, Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012 r., https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [dostęp: 7 I 2026].

kluczowy element pozamilitarnego komponentu bezpieczeństwa, uzupełniającego działania sił zbrojnych i struktur sojuszniczych, zwłaszcza w zakresie bieżącego monitoringu, kontroli ruchu morskiego oraz współpracy z operatorami IK.

Rekomendacje strategiczne, organizacyjne i technologiczne

W Polsce konieczne są zdecydowane działania na poziomie legislacyjnym i operacyjnym, aby zapewnić OWFs skuteczną ochronę. Doświadczenia państw nadmorskich wskazują, że wymaga to współdziałania instytucji publicznych, sektora prywatnego (operatorów) i sił zbrojnych. Proponowane rekomendacje strategiczne, organizacyjne i technologiczne wynikają z takiego zintegrowanego podejścia do bezpieczeństwa IK.

Rekomendacje strategiczne

1. Ustawowe uznanie OWFs za IK – konieczne jest doprecyzowanie statusu OWFs w polskim systemie prawnym przez włączenie ich do wykazu sektorów IK, zgodnie z dyrektywą CER oraz zaktualizowaną PEP2040.
2. Opracowanie narodowej strategii ochrony infrastruktury offshore – strategia ta powinna integrować komponent militarny i pozamilitarny, obejmujący MOSG, Policję (w tym policję wodną), administrację morską oraz operatorów IK. Szczególną rolę w tym systemie należy przypisać operatorom OWFs zlokalizowanym w wyłącznej strefie ekonomicznej (WSE), którzy – ze względu na stałą obecność operacyjną – są pierwszym ogniwem w zakresie monitorowania IK, wczesnego wykrywania anomalii oraz zgłaszania incydentów o charakterze hybrydowym. Rola operatorów IK w WSE powinna polegać przede wszystkim na: a) utrzymywaniu systemów monitoringu technicznego i środowiskowego (SCADA, sensory, systemy pozycjonowania i obserwacji), b) zapewnianiu interoperacyjności danych z systemami państwowymi i sojuszniczymi, c) wdrażaniu procedur reagowania na incydenty zgodnych z KPZK, d) uczestniczeniu w ćwiczeniach i testach odporności prowadzonych z udziałem administracji publicznej i sił zbrojnych. Tak zdefiniowana rola operatorów pozwala na uzupełnienie ograniczonej fizycznej obecności państwa w WSE przez model współodpowiedzialności i partnerstwa publiczno-prywatnego, zgodny z rozwiązaniami przyjmowanymi w państwach nordyckich i w ramach NATO.
3. Włączenie OWFs do cyklicznych ćwiczeń obronnych i z zarządzania kryzysowego – OWFs powinny stać się m.in. integralną częścią ćwiczeń

krajowych takich jak IGNIS[39], w ramach testowania odporności na sabotaż fizyczny i ataki cybernetyczne[40].

Rekomendacje organizacyjne

1. Powołanie międzyresortowego zespołu ds. bezpieczeństwa infrastruktury offshore – w skład zespołu powinni wchodzić przedstawiciele Ministerstwa Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, Ministerstwa Spraw Wewnętrznych i Administracji, administracji morskiej (urzędy morskie), MOSG, Policji (w tym policji wodnej), a także operatorzy OWFs jako podmioty bezpośrednio odpowiedzialne za eksploatację infrastruktury. Rola administracji morskiej powinna polegać w szczególności na koordynacji działań w zakresie zarządzania ruchem morskim, wyznaczaniu i egzekwowaniu stref bezpieczeństwa oraz na integracji informacji o zagrożeniach z systemami służby VTS (vessel traffic service) i krajową świadomością sytuacyjną na morzu. Operatorzy OWFs powinni być włączeni w prace zespołu nie tylko w charakterze interesariuszy, lecz także jako aktywni uczestnicy procesu planowania, testowania i doskonalenia procedur reagowania na incydenty, w tym przez udział w ćwiczeniach międzyinstytucjonalnych oraz przekazywanie danych operacyjnych do właściwych organów państwowych.
2. Zacieśnienie współpracy cywilno-wojskowej – wspólne patrole, interoperacyjne centra dowodzenia i wymiana danych (z wykorzystaniem platform takich jak CISE) pozwolą na szybsze wykrywanie i neutralizację zagrożeń.
3. Obowiązkowa integracja operatorów OWFs z systemem KPZK i krajowym systemem cyberbezpieczeństwa – wymaga to rewizji aktów wykonawczych oraz systemu zgłaszania incydentów.

Rekomendacje technologiczne

1. Inwestowanie w bezzałogowe systemy rozpoznawcze[41] (uncrewed surface vehicle, USV; unmanned aerial systems, UAS; unmanned aerial vehicle,

[39] *Krajowe ćwiczenia ratownicze „IGNIS 2025"*, Serwis Rzeczypospolitej Polskiej, 15 X 2025 r., https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [dostęp: 20 XI 2025].

[40] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*…

[41] R. Miętkiewicz, *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, t. 213, nr 2, s. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

UAV) – do ochrony OWFs należy wykorzystać autonomiczne platformy patrolowe (takie jak Saildrone), które zapewnią całodobowy nadzór obszaru morskiego i wczesne wykrywanie nieautoryzowanej aktywności.
2. Zastosowanie systemów sensorycznych zgodnie z krajowymi zasadami funkcjonowania OWFs – instalacja radarów, sensorów akustycznych, sonarów pasywnych oraz systemów obserwacji elektrooptycznej powinna być realizowana na podstawie prowadzonych w Polsce analiz oddziaływania OWFs na systemy bezpieczeństwa i obronności państwa, stanowiące element procesu planistycznego i uzgodnieniowego dla inwestycji offshore. Potrzeba implementacji wybranych sensorów została rozpoznana i jest stopniowo uwzględniana w ramach krajowych i sojuszniczych systemów monitoringu przestrzeni morskiej, przy zachowaniu interoperacyjności z istniejącymi rozwiązaniami państwowymi.
3. Budowa odporności cybernetycznej zgodnie ze standardami dyrektywy NIS 2 i normy PN-EN ISO/IEC 27001 – operatorzy OWFs powinni być zobowiązani do wdrażania podlegających kontroli procedur zarządzania incydentami oraz regularnych testów penetracyjnych i red teaming, czyli sprawdzania całościowej odporności organizacji na zagrożenie od poziomu technologii po procedury.

Podsumowanie i kierunki dalszych badań

Morskie farmy wiatrowe zyskują status infrastruktury strategicznej nie tylko z punktu widzenia ekologii, ekonomii i gospodarki, lecz także jako potencjalne cele operacji hybrydowych i aktywności w szarej strefie. W obliczu rosnących napięć w regionie Morza Bałtyckiego stają się one nowym polem rywalizacji – obejmującym działania fizyczne, cybernetyczne i informacyjne prowadzone poniżej progu otwartego konfliktu i zacierające granicę pomiędzy stanem wojny a stanem pokoju.

Polska, aspirując do roli regionalnego lidera sektora OZE, znajduje się w bardzo ważnym momencie. Dzięki zastosowaniu zintegrowanego, wielowarstwowego podejścia – obejmującego regulacje prawne, interoperacyjne działania cywilno-wojskowe, cyberodporność, rozpoznanie techniczne oraz współpracę międzynarodową i sektorową – może stać się przykładem skutecznej ochrony infrastruktury morskiej przed zagrożeniami hybrydowymi.

Kierunki dalszych badań powinny obejmować:

1. Modelowanie ryzyka hybrydowego z wykorzystaniem symulacji digital twin[42] – należy je traktować jako narzędzie uzupełniające procesy identyfikacji i szacowania ryzyka realizowane przez operatorów OWFs na etapie planowania, budowy i eksploatacji infrastruktury. Zgodnie z wymogami regulacyjnymi i dobrymi praktykami sektora offshore operatorzy OWFs prowadzą analizy ryzyka obejmujące zagrożenia techniczne, środowiskowe i operacyjne[43]. Zastosowanie digital twin nie zastępuje tych działań, pozwala natomiast na ich pogłębienie oraz analizę zależności pomiędzy różnymi kategoriami zagrożeń, m.in. fizycznych, cybernetycznych i informacyjnych. Stworzenie wirtualnego odpowiednika OWF umożliwia testowanie odporności infrastruktury na złożone, wielodomenowe scenariusze zagrożeń w kontrolowanym środowisku symulacyjnym, bez ingerencji w funkcjonowanie rzeczywistych obiektów. Narzędzie to pozwoli na ocenę skutków skumulowanych oddziaływań, takich jak zakłócenia elektroenergetyczne, ingerencje w systemy SCADA/OT czy działania informacyjne wpływające na procesy decyzyjne. Podejście to znajduje już praktyczne zastosowanie w sektorze offshore, przede wszystkim w państwach nordyckich, jako element wsparcia decyzji operacyjnych i planowania zabezpieczeń infrastruktury morskiej[44].
2. Projektowanie i przeprowadzanie ćwiczeń red teaming – wdrażanie realistycznych scenariuszy ataku (fizycznych, cybernetycznych, socjotechnicznych) umożliwia rzetelną ocenę gotowości operatorów OWFs oraz instytucji państwowych, co jest niezbędne do poprawienia procedur reagowania na naruszenia infrastruktury.
3. Analizę włączenia sektora prywatnego do koordynacji reagowania na zagrożenia – dalsze badania powinny koncentrować się na określeniu miejsca operatorów OWFs w wielopoziomowej architekturze reagowania, w której operator odpowiada za poziomy operacyjny i techniczny (detekcja, wstępna ocena incydentu, zabezpieczenie ciągłości działania), a koordynacja reagowania kryzysowego oraz decyzje o charakterze strategicznym pozostają w gestii właściwych organów państwowych i struktur

[42] G. Faiz, *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [dostęp: 7 I 2026].

[43] *Energy Transition Outlook 2025*…

[44] T. Russell, *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020 r., https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [dostęp: 7 I 2026].

sojuszniczych[45]. Takie przypisanie ról jest spójne z podejściem przyjmowanym w dokumentach NATO i UE oraz z praktyką w sektorze offshore, w ramach której operatorzy pełnią funkcję pierwszej linii monitoringu i raportowania, a nie podmiotów dowodzących reakcją na sytuację kryzysową[46].

4. Rozwój i ocenę krajowych technologii na potrzeby bezpieczeństwa OWFs – należy skupić się na identyfikacji i ocenie potencjału krajowych technologii podwójnego zastosowania (dual-use), które mogą zostać wykorzystane do ochrony OWFs, w szczególności w obszarze systemów sensorowych, bezzałogowych platform morskich i powietrznych, analityki danych oraz cyberbezpieczeństwa infrastruktury offshore[47]. Istotnymi kierunkami badań są: analiza wpływu rozwoju i wdrażania krajowych technologii na zwiększenie odporności systemowej OWFs, ograniczenie zależności technologii od systemów wrażliwych na ataki oraz poprawa kontroli państwa nad kluczowymi elementami systemu bezpieczeństwa[48]. Badania powinny obejmować również ocenę mechanizmów integracji krajowych rozwiązań technologicznych z systemami państwowymi i sojuszniczymi, w tym UE i NATO, a także analizę barier prawnych, organizacyjnych i finansowych ograniczających implementację tych rozwiązań w środowisku offshore[49].

Bibliografia

Mickiewicz P., *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*, „Nautologia" 2024, nr 161, s. 71–76.

Miętkiewicz R., *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa*, „Sprawy Międzynarodowe" 2019, t. 72, nr 1. https://doi.org/10.35757/SM.2019.72.1.06.

Miętkiewicz R., *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych*, „Gospodarka Materiałowa i Logistyka" 2017, nr 12, s. 688–702.

[45] *Energy Transition Outlook 2025*…

[46] *Industry leaders agree best practice*…; A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[47] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*…; P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?*…

[48] Tamże.

[49] *Common information sharing environment (CISE)*…

Miętkiewicz R., *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, t. 213, nr 2, s. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, „Ekspertyzy PTBN" 2023, nr 1.

Szubrycht T., *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim*, „Bezpieczeństwo Narodowe" 2025, t. 46, nr 1, s. 49–75. https://doi.org/10.59800/bn/207646.

Źródła internetowe

Ávila-Zúñiga-Nordfjeld A., *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/ [dostęp: 20 VI 2025].

Bryant M., *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024 r., https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [dostęp: 19 VI 2025].

Cavcic M., *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, Offshore Energy, 11 XII 2024 r., https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [dostęp: 19 VI 2025].

Common information sharing environment (CISE), European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 20 VI 2025].

Countering hybrid threats, NATO, 7 V 2024 r., https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [dostęp: 20 VI 2025].

Digital Baltic, https://digitalbaltic.pl [dostęp: 7 I 2026].

Energy Transition Outlook 2025, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [dostęp: 20 VI 2025].

Faiz G., *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [dostęp: 7 I 2026].

Finland blames Chinese ship for Baltic Sea gas pipeline damage, Euronews, 25 X 2023 r., https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [dostęp: 19 VI 2025].

Finnish media: Balticconnector pipeline leak 'does not appear to be an accident', ERR News, 10 X 2023 r., https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [dostęp: 19 VI 2025].

Henley J., '*Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022 r., https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [dostęp: 19 VI 2025].

Industry leaders agree best practice for protecting offshore wind cables, Carbon Trust, 13 XI 2024 r., https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [dostęp: 20 VI 2025].

Krajowe ćwiczenia ratownicze „IGNIS 2025", Serwis Rzeczypospolitej Polskiej, 15 X 2025 r., https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [dostęp: 20 XI 2025].

NATO launches 'Baltic Sentry' to increase critical infrastructure security, NATO, 14 I 2025 r., https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [dostęp: 6 I 2026].

NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure, MARCOM NATO, 28 V 2024 r., https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [dostęp: 6 I 2026].

RFA Proteus (K60), Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [dostęp: 20 VI 2025].

Russell T., *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020 r., https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [dostęp: 7 I 2026].

Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea, Saildrone, 16 VI 2025 r., https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [dostęp: 20 VI 2025].

Sari A., *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 20 VI 2025].

Smith C., *Finland investigates Russia's 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024 r., https://www.bbc.com/news/articles/cr56l7prj2mo [dostęp: 19 VI 2025].

Zadania Morskiego Oddziału Straży Granicznej, Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012 r., https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [dostęp: 7 I 2026].

Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni, Portal Morski, 18 I 2025 r., https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku--utrzymuja-sie-od-ponad-60-dni [dostęp: 19 VI 2025].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27 XII 2022 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333 z 27 XII 2022 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2026 r. poz. 20).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122, ze zm.).

Rozporządzenie Ministra Klimatu i Środowiska z dnia 25 maja 2022 r. w sprawie szczegółowych wymagań dla elementów zespołu urządzeń służących do wyprowadzenia mocy oraz dla elementów stacji elektroenergetycznych zlokalizowanych na morzu (DzU z 2022 r. poz. 1257).

Inne dokumenty

Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 20 VI 2025].

Komisja Europejska, *Plan REPowerEU*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [dostęp: 20 VI 2025].

Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r. (PEP2040)*, Warszawa 2021.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego*, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [dostęp: 20 VI 2025].

Norma PN-EN ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*, https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [dostęp: 20 VII 2025].

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, Warszawa 2023.

Klaudia Maciata

Specjalistka ds. operacji offshore w sektorze energetyki wiatrowej. Ambasadorka inicjatywy Women Offshore, członkini międzynarodowych projektów z zakresu bezpieczeństwa morskiego i klimatycznego. Ekspertka zajmująca się tematyką ochrony infrastruktury krytycznej przed zagrożeniami hybrydowymi w regionie Morza Bałtyckiego. Autorka publikacji w „NATO Review". Zawodowo związana m.in. z firmą Ørsted, wcześniej pracowała w sektorze usług przemysłowych, technologii bezzałogowych i doradztwa public affairs. Obecnie fundatorka projektu „Baltic Sea Security" i freelancerka.

Kontakt: klaudia.maciata@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 133–145

https://doi.org/10.4467/20801335PBW.26.006.23368

ARTYKUŁ

Rozwój zagrożeń cybernetycznych związany z wykorzystaniem AI

The development of cyber threats related to the use of AI

JAKUB GAJECKI

Autor niezależny

https://orcid.org/0009-0007-3488-0236

Abstrakt

Dynamiczny rozwój sztucznej inteligencji (artificial intelligence, AI) powoduje, że rośnie także jej rola w cyberprzestrzeni, zarówno w kontekście zagrożeń, jak i obrony przed nimi. Wspiera ona automatyzację wykrywania anomalii, analizę danych i reakcję na incydenty, co zwiększa efektywność ochrony. Z kolei cyberprzestępcy wykorzystują rozwiązania oparte na AI do tworzenia inteligentnych narzędzi ataków, takich jak zaawansowane phishingi, deepfaki i trudne do wykrycia malware'y. Autor analizuje rolę AI w generowaniu zagrożeń w cyberprzestrzeni i w tym kontekście ocenia strategie obronne. Wskazuje potrzebę międzynarodowej współpracy i regulacji prawnych w zakresie wykorzystania AI w cyberbezpieczeństwie.

Słowa kluczowe

sztuczna inteligencja, cyberbezpieczeństwo, AI as a service, cyberprzestępczość, kryptografia kwantowa

Abstract

In light of the rapid development of artificial intelligence (AI), its role in cybersecurity is crucial for both defense and emerging threats. AI supports the automation of anomaly detection, data analysis, and incident response, which enhances protection efficiency. However, AI as a service enables cybercriminals to create sophisticated attack tools, such as advanced phishing schemes, deepfakes, and hard-to-detect malware. This work analyzes AI's role in cyber threats and evaluates defensive strategies, highlighting the need for international cooperation and legal regulations. Conclusions point to the necessity of research on AI's resilience against attacks.

Keywords

artificial intelligence, cybersecurity, AI as a service, cybercrime, quantum cryptography

Wprowadzenie

Rozwój technologii informatycznych i sztucznej inteligencji (artificial intelligence, AI[1]) zmienił podejście do cyberbezpieczeństwa oraz zainicjował nową erę cyberzagrożeń. W przeszłości ataki w cyberprzestrzeni, takie jak wirusy komputerowe czy phishing, czyli podszywanie się pod instytucje lub osoby w celu wyłudzenia informacji[2], były stosunkowo proste i ograniczone do działań pojedynczych hakerów lub małych grup. Na przełomie XX i XXI w. największym wyzwaniem było zapobieganie rozprzestrzenianiu się złośliwego oprogramowania (malicious software, malware), w tym typu ransomware, i szybkie reagowanie na jego atak[3]. Zwykle te ataki były ukierunkowane na pojedyncze osoby lub mniejsze organizacje, a ich zakres i skutki – ograniczone możliwościami technologicznymi[4]. Postęp w zakresie AI i uczenia maszynowego przekształcił cyberprzestrzeń i spowodował, że zagrożenia są bardziej złożone, dynamiczne i trudniejsze do wykrycia. Sztuczna inteligencja

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

[2] J. Jancelewicz, *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Trzeci Sektor" 2022, t. 3–4, nr 59–60, s. 80–81. https://doi.org/10.26368/17332265-59/60-3/4-2022-5.

[3] *The Evolution of Cybersecurity*, Codecademy, https://www.codecademy.com/article/evolution-of-cybersecurity [dostęp: 7 X 2024].

[4] B. Dash i in., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review,* „International Journal of Software Engineering & Applications" 2022, t. 13, nr 5, s. 14. https://doi.org/10.5121/ijsea.2022.13502.

wprowadziła nową jakość zarówno pod względem przeprowadzania ataków w cyberprzestrzeni, jak i obrony przed nimi.

Sztuczna inteligencja pozwala m.in.:

- analizować infrastrukturę zabezpieczeń,
- automatyzować wyszukiwanie jej słabych punktów,
- rozwijać inteligentne narzędzia, które potrafią adaptować się do działań obronnych atakowanych systemów w czasie rzeczywistym.

Wykorzystanie AI czyni ataki wyjątkowo trudnymi do neutralizacji.

W artykule przeanalizowano wpływ rozwoju AI, szczególnie jej klasycznych i generatywnych (GenAI) typów, na rozwój zagrożeń w cyberprzestrzeni, w wymiarze zarówno ofensywnym (działania cyberprzestępcze), jak i defensywnym (systemy cyberobrony).

Problem badawczy sformułowano następująco: w jaki sposób wykorzystanie klasycznych i generatywnych AI zmienia charakter, skalę oraz automatyzację zagrożeń w cyberprzestrzeni oraz jakie to ma konsekwencje dla systemów cyberbezpieczeństwa?

Cele szczegółowe badania to:

- identyfikacja klasycznych zastosowań AI w cyberbezpieczeństwie,
- analiza wykorzystania generatywnej AI przez grupy cyberprzestępcze,
- ocena aktualnych systemów obronnych wobec automatyzacji ataków,
- wskazanie kierunków dalszych badań i działań regulacyjnych.

W artykule zastosowano metody badawcze takie jak analiza i synteza oraz indukcja i dedukcja. Autor korzystał z różnych materiałów źródłowych: publikacji zwartych, monografii i artykułów naukowych, raportów, publikacji specjalistycznych oraz opisów studiów przypadków.

Rozwój botnetów i złośliwego oprogramowania

Botnety, czyli grupy zainfekowanych komputerów kontrolowanych bez wiedzy ich właścicieli, zaczęły się rozwijać na początku XXI w. Jednym z pierwszych i najbardziej znanych botnetów był Agobot, który wykorzystywał zainfekowane urządzenia do rozsyłania spamu i przeprowadzania ataków DDoS (distributed denial of service)[5], których celem jest przeciążenie serwerów zaatakowanych podmiotów i uniemożliwienie dostępu do usług. Kolejne botnety takie jak Storm i Conficker

[5] A. Kurniawan, A. Fitriansyah, *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, „International Journal of Computer and Communication Engineering" 2018, t. 7, nr 4, s. 130–131. https://doi.org/10.17706/ijcce.2018.7.4.128-135.

pokazały swoją siłę i skalę działania, przejmując kontrolę nad milionami urządzeń i stając się realnym zagrożeniem dla globalnych systemów komputerowych[6].

Ewolucja złośliwego oprogramowania dotyczy jego wielu form: wirusów, robaków, oprogramowania szpiegującego (spyware), uciążliwych reklam (advertising-supported software, adware), rootkitów, które zapewniają dostęp na poziomie administratora i ransomware'u. Przykładem wczesnego rozwoju malware'ów jest wirus ILOVEYOU, który nie był jeszcze botnetem, ale ze względu na skalę oddziaływania stał się inspiracją do poszukiwania bardziej zaawansowanych form malware'ów. W miarę jak technologia ewoluowała również złośliwe oprogramowanie stawało się coraz bardziej wyspecjalizowane. Zeus i SpyEye to przykłady malware'ów skoncentrowanych na kradzieży danych z bankowości internetowej[7]. Stuxnet natomiast był pierwszym programem zaprojektowanym do fizycznego uszkodzenia urządzeń przemysłowych infrastruktury krytycznej[8]. Botnety stały się głównym narzędziem w atakach DDoS. Przykładami są botnety Mirai i Satori, które przekształciły urządzenia internetu rzeczy (internet of things) w narzędzia ataków na masową skalę. W 2016 r. Mirai zaatakował serwery należące do dostawców DNS (domain name system) i zablokował na całym świecie dostęp do popularnych witryn internetowych[9].

Obecnie złośliwe oprogramowanie i botnety korzystają z rozwiązań opartych na AI, co ułatwia im omijanie systemów detekcji i skuteczniejsze ukrywanie swojej obecności. Sztuczna inteligencja umożliwia botnetom analizę i adaptację w czasie rzeczywistym. Zwiększa to skuteczność ataków i zmniejsza prawdopodobieństwo ich wykrycia. Zautomatyzowane botnety mogą samodzielnie identyfikować nowe cele, a nawet korzystać z technik uczenia maszynowego, aby rozpoznać wzorce zachowań ofiar i odpowiednio dostosowywać swoje działania.

---

[6] J. Yimu, L. Shangdong, *Threats from Botnets*, w: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernández-Caramés (red.), September 2020, https://www.intechopen.com/chapters/69332 [dostęp: 18 X 2024].

[7] N. Etaher, G.R.S. Weir, *Understanding the Threat of Banking Malware*, w: *Proceedings of Cyberforensics 2014*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf, s. 77–79 [dostęp: 18 X 2025].

[8] M. Hagerott, *Stuxnet and the vital role of critical infrastructure operators and engineers*, „International Journal of Critical Infrastructure Protection" 2014, t. 7, nr 4, s. 244–246. https://doi.org/10.1016/j.ijcip.2014.09.001.

[9] H. Griffioen, Ch. Doerr, *Examining Mirai's Battle over the Internet of Things*, https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf, s. 744 [dostęp: 18 X 2025].

Sztuczna inteligencja jako narzędzie cyberprzestępców

Sztuczna inteligencja jest definiowana jako dziedzina informatyki zajmująca się projektowaniem systemów zdolnych do wykonywania zadań wymagających wcześniej ludzkich umiejętności takich jak uczenie się, rozumowanie, planowanie czy podejmowanie decyzji. Klasyczne podejście do AI obejmuje m.in.: systemy regułowe, uczenie maszynowe, sieci neuronowe oraz algorytmy wnioskowania probabilistycznego[10].

Cyberprzestępcy są w stanie automatyzować i usprawniać ataki phishingowe i malware, co sprawia, że mają one większy zasięg i są trudniejsze do wykrycia. Dzięki AI hakerzy mogą w krótkim czasie analizować dużo danych, np. zachowania i profile użytkowników, by tworzyć bardziej przekonujące wiadomości, dostosowane do różnych grup docelowych. Personalizacja zwiększa prawdopodobieństwo, że odbiorca zdecyduje się kliknąć w złośliwy link lub pobrać załącznik. Sztuczna inteligencja może również wspomagać tworzenie i dystrybucję złośliwego oprogramowania. Analizuje mechanizmy ochronne systemów, dostosowując działanie malware'u tak, aby pozostawał niewykrywalny. Przykładem może być złośliwe oprogramowanie, które wykorzystuje uczenie maszynowe do przeprowadzania tzw. ataków polimorficznych. Polegają one na tym, że malware zmienia swoje cechy przy każdej infekcji, co znacznie utrudnia jego identyfikację przez tradycyjne programy antywirusowe[11]. Cyberprzestępcy używają AI również do tworzenia deepfake'ów, czyli fałszywych obrazów, nagrań wideo lub audio, które wykorzystują w różnych scenariuszach przestępczych, takich jak oszustwa finansowe, manipulacja opinią publiczną, a nawet szantaż[12].

Rozwój GenAI, w tym dużych modeli językowych (large language models, LLM) oraz generatywnych modeli opartych na architekturze sieci neuronowych takich jak generative adversarial networks, znacznie zmienił modus operandi grup cyberprzestępczych. Generatywna AI umożliwia automatyczne tworzenie treści phishingowych o wysokim stopniu personalizacji, generowanie kodu malware oraz skalowanie ataków socjotechnicznych. Badania wskazują, że wykorzystanie LLM pozwala na obniżenie bariery wejścia do cyberprzestępczości, umożliwiając prowadzenie zaawansowanych ataków osobom bez specjalistycznej wiedzy[13]. Przykładem

[10] S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, bmw 2021, s. 1–2.

[11] R. Chauhan i in., *Polymorphic Adversarial Cyberattacks Using WGAN*, „Journal of Cybersecurity and Privacy" 2021, nr 1, s. 788–789. https://doi.org/10.3390/jcp1040037.

[12] O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, t. 9, nr 3, s. 20–24. https://doi.org/10.24917/26578549.9.3.2.

[13] Y. Yigit i in., *Review of Generative AI Methods in Cybersecurity*, preprint, arXiv, 13 III 2024 r. https://doi.org/10.48550/arXiv.2403.08701.

może być analiza historii wyszukiwań i odwiedzanych stron w celu dostosowania komunikatów phishingowych, które dla ofiary mogą wyglądać na autentyczne.

Uczenie maszynowe jest wykorzystywane do tworzenia bardziej wyrafinowanego i adaptacyjnego złośliwego oprogramowania. Algorytmy te pozwalają malware'owi na dostosowywanie swojego działania w zależności od wykrytych zabezpieczeń systemu ofiary i przeprowadzenie ataku w najbardziej odpowiednim momencie, np. kiedy użytkownik loguje się do wrażliwych systemów takich jak konta bankowe. Algorytmy uczenia maszynowego umożliwiają generowanie i testowanie w krótkim czasie nowych wariantów złośliwego kodu.

Inną formą cyberprzestępstwa opartą na uczeniu maszynowym są wspomniane ataki polimorficzne. Techniki takie jak polimorfizm i metamorfizm pozwalają na generowanie różnych wariantów tego samego malware'u, dzięki czemu oprogramowanie zabezpieczające, które bazuje na wykrywaniu wzorców, nie jest w stanie rozpoznać zmienionego kodu. Takie techniki są jednymi z najtrudniejszych do wykrycia. Uczenie maszynowe daje także możliwość szybkiego przetwarzania danych i próbowania różnych kombinacji przy atakach brute force, mających na celu odgadnięcie haseł lub kodów zabezpieczeń. Algorytmy te są w stanie przewidywać, jakie hasła mogą być najbardziej prawdopodobne, co znacznie skraca czas potrzebny do złamania zabezpieczeń. Przykładowo, w połączeniu z analizą behawioralną algorytmy mogą generować propozycje haseł zgodne z charakterystycznymi schematami stosowanymi przez użytkownika, takimi jak imiona, daty urodzin lub inne osobiste szczegóły.

Cyberprzestępcy wykorzystują algorytmy uczenia maszynowego do analizowania struktury i konfiguracji systemów bezpieczeństwa. Tego rodzaju oprogramowanie jest w stanie zidentyfikować i przeanalizować specyficzne cechy mechanizmów zabezpieczających takich jak firewalle, systemy detekcji włamań (intrusion detection system) oraz programy antywirusowe. Dzięki tej wiedzy atakujący mogą dostosowywać swoje metody w czasie rzeczywistym, przełamywać kolejne warstwy ochrony i unikać wykrycia. Sztuczna inteligencja może nie tylko generować różne warianty tego samego malware'u (polimorfizm, metamorfizm), lecz także uczyć malware, by rozpoznawał różne systemy zabezpieczeń i do nich dostosowywał swoje działanie, co będzie minimalizować ryzyko detekcji. Zaawansowane ataki z użyciem AI polegają na predykcji zachowań użytkowników opartej na analizie behawioralnej. Analizując duże zbiory danych dotyczących zachowań użytkowników, atakujący mogą przewidzieć momenty, kiedy system będzie najmniej odporny na atak, np. podczas próby logowania w czasie, gdy system zabezpieczeń rejestruje wzmożony ruch i łatwiej ignoruje pewne nieprawidłowości.

Współczesne przypadki cyberataków

Atak na platformę GitHub w 2018 r. był jednym z najpotężniejszych ataków DDoS w historii – uzyskano w nim przepływ danych rzędu 1,35 Tb/s. Cyberprzestępcy wykorzystali botnety sterowane AI do masowego wysyłania żądań, co przeciążyło serwery GitHub. Sztuczna inteligencja pomogła dynamicznie dostosowywać atak i omijać zabezpieczenia w czasie rzeczywistym. Botnety wspomagane przez AI stają się coraz powszechniejsze, co umożliwia przeprowadzanie ataków na duże platformy[14].

W 2020 r. firma Cognizant, globalny dostawca usług IT, padła ofiarą ransomware'u Maze. Jest to przykład oprogramowania wykorzystującego AI i zaawansowane techniki infiltracji sieci. Oprogramowanie to stosuje analizę systemu, aby zidentyfikować najbardziej wrażliwe dane i uniemożliwić do nich dostęp, a także rozsyła je dalej do centrów dowodzenia przestępców. W wyniku ataku firma Cognizant poniosła ogromne straty finansowe i wydała miliony dolarów na naprawę infrastruktury oraz wsparcie dla klientów i dostawców[15]. Przedsiębiorstwo podjęło działania naprawcze obejmujące izolację zainfekowanych systemów, wzmocnienie procedur reagowania na incydenty oraz rozbudowę mechanizmów monitorowania sieci. Przypadek ten pokazuje jednak, że systemy wykrywania zagrożeń oparte głównie na sygnaturach nie zawsze są w stanie odpowiednio wcześnie wykryć zaawansowane kampanie ransomware[16].

W tym samym roku Twitter został zaatakowany przez cyberprzestępców, którzy przejęli konta znanych osób i firm, w tym Billa Gatesa, Elona Muska i Apple'a. Hakerzy wykorzystali technologię przetwarzania języka naturalnego (natural language processing, NLP) do generowania wiadomości wyglądających na osobiste i spersonalizowane, w których zachęcali do przesyłania pieniędzy na podany adres kryptowalutowy[17]. Atak był skuteczny dzięki m.in. wykorzystaniu AI do analizowania sposobu komunikacji ofiar i adaptacji wiadomości. Po wykryciu incydentu platforma zablokowała możliwość publikowania wpisów przez zweryfikowane konta oraz rozpoczęła proces przywracania bezpieczeństwa przejętych profili. Wdrożono

---

[14] L.H. Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018 r., https://www.wired.com/story/github-ddos-memcached/ [dostęp: 26 X 2024].

[15] F. Truță, *Cognizant Expects to Lose up to $70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020 r., https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/ [dostęp: 24 X 2024].

[16] *Cognizant Security Incident Update*, Cognizant, 18 IV 2020 r., https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm [dostęp: 9 III 2026].

[17] N. Statt, *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020 r., https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised [dostęp: 24 X 2025].

również dodatkowe środki kontroli dostępu do narzędzi administracyjnych oraz wzmocniono procedury uwierzytelniania pracowników.

W 2025 r. został wykryty pierwszy udokumentowany przypadek wykorzystania na dużą skalę autonomicznych agentów AI w operacjach cyberwywiadowczych. W połowie września zespół Threat Intelligence firmy Anthropic zidentyfikował i następnie przerwał kampanię cyberszpiegowską, w której narzędzie oparte na modelu językowym Claude Code zostało zmanipulowane przez aktora uznawanego za powiązanego z chińskimi strukturami państwowymi. Celem było przeprowadzenie złożonych operacji wywiadowczych[18].

W tej kampanii AI nie pełniło jedynie funkcji doradczej czy generatywnej, lecz działało jako autonomiczny agent wykonujący większość zadań operacyjnych. System rozkładał wieloetapowe instrukcje na mniejsze zadania, które następnie wykonywał samodzielnie z minimalnym nadzorem człowieka. Claude Code przeprowadził autonomicznie do 80–90% taktycznych operacji, włączając w to:

- rozpoznanie infrastruktury celu i analizę słabych punktów,
- generowanie i wykonanie kodów wykorzystujących luki,
- zbieranie poświadczeń i danych,
- ruch boczny (lateral movement),
- wydobywanie i klasyfikację danych[19].

Taka automatyzacja oznacza, że AI przeprowadzała bez ciągłej interwencji operatora działania, które wcześniej wymagałyby zaangażowania dużych zespołów ekspertów: od skanowania sieci, przez analizy podatności, po eksfiltrację danych. W tym przypadku rola człowieka ograniczała się głównie do inicjalizacji kampanii i podejmowania strategicznych decyzji w kluczowych momentach, np. zatwierdzania przejścia między fazami ataku[20]. Co więcej, mechanizm działania agentów AI opierał się na wykorzystaniu ich zdolności do autonomicznego podejmowania decyzji w sekwencji zadań oraz do adaptacji narracji i strategii względem kolejnych etapów ataku. Znacznie zwiększało to tempo i skalę operacji w porównaniu z tradycyjnym „ręcznym sterowaniem". Maszyna była w stanie wykonać tysiące operacji na sekundę, co dla zespołów cyberprzestępczych niekorzystających z automatyzacji jest niedostępne[21].

[18] *Disrupting the first reported AI-orchestrated cyber espionage campaign*, Anthropic, 13 XI 2025 r., https://www.anthropic.com/news/disrupting-AI-espionage [dostęp: 24 XI 2025].

[19] Tamże.

[20] Tamże.

[21] Tamże.

Sztuczna inteligencja w cybernetycznych systemach obronnych

Rozwój usług typu AI as a service niesie ze sobą korzyści dla biznesu, ale jednocześnie tworzy nowe wektory ataków dla cyberprzestępców. AI as a service oferuje dostęp do zaawansowanych algorytmów AI, które mogą zostać wykorzystane do automatyzacji działań takich jak analiza słabych punktów systemów lub tworzenie zaawansowanych botów phishingowych. Cyberprzestępcy mogą w przyszłości wykorzystywać AI as a service do rozwoju deepfake'ów, przeprowadzania socjotechnicznych ataków na większą skalę, tworzenia trudniejszych do wykrycia malware'ów, projektowania ransomware'ów, które będą automatycznie wybierać najskuteczniejsze metody ataku, zwiększając ich skuteczność.

Aby sprostać tym wyzwaniom, równolegle są rozwijane nowe technologie obronne oparte na AI. Przykładem są adaptacyjne systemy oparte na uczeniu maszynowym, które mogą dynamicznie reagować na zagrożenia i automatycznie dostosowywać swoje funkcje ochronne w zależności od napotkanych ataków. Dodatkowo technologie NLP są stosowane do analizy komunikacji cyberprzestępczej, co pomaga w przewidywaniu i wykrywaniu nowych zagrożeń. Przewiduje się, że w przyszłości systemy obronne oparte na AI będą zdolne do samodzielnej analizy złośliwego oprogramowania oraz do tworzenia dynamicznych, odpornych na zagrożenia środowisk wirtualnych, co zmniejszy ryzyko naruszeń bezpieczeństwa[22].

Warto podkreślić, że zarówno na poziomie krajowym, jak i międzynarodowym obecnie obowiązuje wiele regulacji z zakresu cyberbezpieczeństwa. W Europie istotną rolę odgrywają dyrektywa NIS 2[23] dotycząca bezpieczeństwa sieci i systemów informatycznych, a także rozporządzenie Artificial Intelligence Act[24] regulujące wykorzystanie systemów AI w Unii Europejskiej. Ważnym instrumentem jest również Konwencja Rady Europy o cyberprzestępczości[25], która stanowi podstawę współpracy międzynarodowej w zwalczaniu cyberprzestępczości.

---

[22] R. Keshava i in., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, w: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC 2025), Coimbatore 2025. https://doi.org/10.1109/ICESC65114.2025.11212519.

[23] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).*

[24] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).*

[25] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.*

Należy jednak zauważyć, że większość przepisów powstawała w okresie, gdy technologie AI nie były wykorzystywane na szeroką skalę w działaniach cybernetycznych. W związku z tym obecne regulacje często nie odnoszą się wprost do specyfiki systemów opartych na AI, takich jak autonomiczne systemy detekcji zagrożeń, generatywne modele wykorzystywane do tworzenia phishingu czy zautomatyzowane narzędzia prowadzenia cyberataków.

Rozwój możliwości zastosowania AI w cyberbezpieczeństwie powoduje przede wszystkim konieczność doprecyzowania i rozszerzenia istniejących regulacji, a nie tworzenia ich od podstaw. Dotyczy to szczególnie kwestii odpowiedzialności za decyzje podejmowane przez systemy AI, transparentności algorytmów, standardów bezpieczeństwa oraz zasad międzynarodowej współpracy w zakresie przeciwdziałania cyberzagrożeniom. Jednocześnie skuteczna walka z cyberprzestępczością wymaga pogłębionej współpracy międzynarodowej oraz harmonizacji regulacji prawnych, aby ograniczyć możliwości wykorzystywania przez sprawców przestępstw różnic między systemami prawnymi. Wynika to z charakteru cyberprzestrzeni, która przekracza granice państw. Przyszłe regulacje powinny dotyczyć wykorzystania systemów AI do prowadzenia nielegalnej działalności, w tym cyberprzestępczości, doprecyzować zasady odpowiedzialności za użycie tych systemów oraz ograniczyć stosowanie niektórych technologii wysokiego ryzyka. Organizacje międzynarodowe, takie jak Organizacja Narodów Zjednoczonych i Unia Europejska, odgrywają istotną rolę w tworzeniu polityk przeciwdziałających cyberprzestępczości oraz w promowaniu wspólnych standardów ochrony danych. Takie działania umożliwią szybsze reagowanie na globalne zagrożenia oraz ułatwią wymianę informacji i doświadczeń w zakresie najlepszych praktyk w cyberbezpieczeństwie.

Podsumowanie

Na podstawie rozważań teoretycznych oraz analizy wybranych przypadków sformułowano następujące wnioski końcowe:

1. Sztuczna inteligencja istotnie zwiększa skuteczność i skalowalność cyberataków, w szczególności przez automatyzację phishingu, tworzenie adaptacyjnego złośliwego oprogramowania oraz wykorzystanie technik generatywnych (deepfake), co prowadzi do obniżenia progu wejścia do cyberprzestępczości.
2. Rozwój systemów cyberobrony opartych na AI poprawia zdolności wykrywania i reagowania na zagrożenia. Dochodzi jednak do wyścigu technologicznego pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyfrowe a cyberprzestępcami.

3. Skuteczne przeciwdziałanie zagrożeniom, które są generowane z pomocą AI, wymaga skoordynowanych działań systemowych obejmujących współpracę międzynarodową, rozwój ram regulacyjnych oraz harmonizację standardów prawnych i technicznych w zakresie wykorzystania AI w cyberprzestrzeni. Obecnie na poziomie międzynarodowym podstawę współpracy państw w zwalczaniu cyberprzestępczości stanowi Konwencja o cyberprzestępczości przyjęta przez Radę Europy. Określa ona ramy współpracy w zakresie ścigania przestępstw popełnianych z wykorzystaniem systemów informatycznych. W ramach UE istotną rolę odgrywa również dyrektywa NIS 2, której celem jest podniesienie poziomu bezpieczeństwa sieci i systemów informatycznych w państwach członkowskich, a także rozporządzenie Artificial Intelligence Act wprowadzające ramy prawne dla bezpiecznego i odpowiedzialnego stosowania systemów AI.
4. Dynamiczny rozwój technologii AI stawia przed obowiązującymi systemami prawnymi i technicznymi nowe wyzwania. Nie wydaje się jednak konieczne tworzenie nowych regulacji, a raczej doprecyzowanie oraz dostosowanie obowiązujących przepisów do specyfiki zagrożeń związanych z wykorzystaniem AI w cyberprzestrzeni.

Bibliografia

Chauhan R., Sabeel U., Izaddoost A., Heydari S.S., *Polymorphic Adversarial Cyberattacks Using WGAN*, „Journal of Cybersecurity and Privacy" 2021, nr 1, s. 767–792. https://doi.org/10.3390/jcp1040037.

Dash B., Ansari M.F., Sharma P., Ali A., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review*, „International Journal of Software Engineering & Applications" 2022, t. 13, nr 5, s. 13–21. https://doi.org/10.5121/ijsea.2022.13502.

Hagerott M., *Stuxnet and the vital role of critical infrastructure operators and engineers*, „International Journal of Critical Infrastructure Protection" 2014, t. 7, nr 4, s. 244–246. https://doi.org/10.1016/j.ijcip.2014.09.001.

Jancelewicz J., *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Trzeci Sektor" 2022, t. 3–4, nr 59–60, s. 79–88. https://doi.org/10.26368/17332265-59/60-3/4-2022-5.

Keshava R., Pandurangan S.K., Sakthivanitha M., Parmsivan S., Sunkara G., Maruthi R., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, w: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC 2025), Coimbatore 2025. https://doi.org/10.1109/ICESC65114.2025.11212519.

Kurniawan A., Fitriansyah A., *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, „International Journal of Computer and Communication Engineering" 2018, t. 7, nr 4, s. 128–135. https://doi.org/10.17706/ijcce.2018.7.4.128-135.

Russell S., Norvig P., *Artificial Intelligence. A Modern Approach*, bmw 2021.

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, t. 9, nr 3, s. 19–30. https://doi.org/10.24917/26578549.9.3.2.

Yigit Y., Buchanan W.J., Tehrani M.G., Maglaras L., *Review of Generative AI Methods in Cybersecurity*, preprint, arXiv, 13 III 2024 r. https://doi.org/10.48550/arXiv.2403.08701.

Źródła internetowe

Cognizant Security Incident Update, Cognizant, 18 IV 2020 r., https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm [dostęp: 9 III 2026].

Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 XI 2025 r., https://www.anthropic.com/news/disrupting-AI-espionage [dostęp: 24 XI 2025].

Etaher N., Weir G.R.S., *Understanding the Threat of Banking Malware*, w: *Proceedings of Cyberforensics 2014*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf [dostęp: 18 X 2025].

Griffioen H., Doerr Ch., *Examining Mirai's Battle over the Internet of Things*, https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf [dostęp: 18 X 2025].

Newman L.H., *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018 r., https://www.wired.com/story/github-ddos-memcached/ [dostęp: 26 X 2024].

Statt N., *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020 r., https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised [dostęp: 24 X 2025].

The Evolution of Cybersecurity, Codecademy, https://www.codecademy.com/article/evolution-of-cybersecurity [dostęp: 7 X 2024].

Truță F., *Cognizant Expects to Lose up to $70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020 r., https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/ [dostęp: 24 X 2024].

Yimu J., Shangdong L., *Threats from Botnets*, w: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernández-Caramés (red.), September 2020, s. 52–75, https://www.intechopen.com/chapters/69332 [dostęp: 18 X 2024].

Akty prawne

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (DzU z 2015 r. poz. 728).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27 XII 2022 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) – (Dz. Urz. L 2024/1689 z 12 VII 2024 r.).

Jakub Gajecki

Absolwent Akademii im. Jakuba z Paradyża w Gorzowie Wielkopolskim na kierunku kryminologia stosowana, ze specjalnością zwalczanie cyberprzestępczości. Student studiów II stopnia w Akademii Policji w Szczytnie na kierunku bezpieczeństwo w cyberprzestrzeni. Jego zainteresowania naukowe obejmują cyberbezpieczeństwo oraz bezpieczeństwo państwa. Funkcjonariusz Policji zajmujący się prowadzeniem postępowań przygotowawczych.

Kontakt: gajeckijakub@protonmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 147–171

https://doi.org/10.4467/20801335PBW.26.007.23369

ARTYKUŁ

Ataki hybrydowe przeciwko Rzeczypospolitej Polskiej prowadzone i koordynowane przez Federację Rosyjską i ich związek z wojną w Ukrainie

Hybrid attacks against the Republic of Poland conducted and coordinated by the Russian Federation and their link to the war in Ukraine

AGATA RYTEL

Szkoła Główna Handlowa w Warszawie

https://orcid.org/0009-0008-1506-1822

Abstrakt Celem artykułu jest opis ataków i działań hybrydowych ze strony Federacji Rosyjskiej wymierzonych w Rzeczpospolitą Polską, które zostały przeprowadzone od czerwca 2021 r. do końca 2024 r. Przedstawiono je z rozróżnieniem na ataki godzące w nienaruszalność polskiej granicy z Białorusią, ataki prowadzone w polskiej cyberprzestrzeni oraz ataki dezinformacyjne w polskiej przestrzeni informacyjnej. Teza przyjęta w artykule zakłada, że działania te miały bezpośredni związek z wojną w Ukrainie i były intencjonalną ingerencją Rosji i Białorusi. Przeanalizowano literaturę przedmiotu dotyczącą teorii wojny hybrydowej oraz aktywności Federacji Rosyjskiej i Białorusi postrzeganych jako elementy wojny hybrydowej. Ponadto przeanalizowano informacje na temat wrogich działań przeciwko Rzeczypospolitej Polskiej, udostępnione przez polskie instytucje państwowe i zespoły powołane do reagowania na incydenty komputerowe.

Słowa kluczowe ataki hybrydowe, wojna hybrydowa, nielegalna migracja, cyberprzestrzeń, dezinformacja

Abstract

The aim of this article is to describe attacks and hybrid activities the Russian Federation against the Republic of Poland between June 2021 and the end of 2024. They are presented with a distinction between attacks against the integrity of the Polish border with Belarus, attacks carried out in Polish cyberspace, and disinformation attacks in the Polish information space. The thesis adopted in the article assumes that these actions were directly related to the war in Ukraine and were intentional interference by Russia and Belarus. The literature on the theory of hybrid warfare and the actions carried out by the Russian Federation and Belarus, perceived as part of hybrid warfare, was analysed. Furthermore, information related to hostile actions against the Republic of Poland, made available by Polish state institutions and teams set up to respond to computer incidents, was analysed.

Keywords

hybrid attacks, hybrid warfare, illegal migration, cyberspace, disinformation

Wprowadzenie

Sytuacja geopolityczna w Europie i na świecie w ostatnich latach znacznie się zmieniła, m.in. z powodu coraz bardziej jawnych dążeń imperialistycznych Federacji Rosyjskiej. Obecne wydarzenia (wojna w Ukrainie, ataki hybrydowe skierowane przeciwko Polsce) są związane z dynamicznym rozwojem technologii sieciowych i bezprecedensowym wpływem cyberprzestrzeni na funkcjonowanie państw i społeczeństw. Rozwój narzędzi, jakie oferuje cyberprzestrzeń, sprzyja działaniom hybrydowym. Rosja sukcesywnie rozwija metody prowadzenia wrogich, pozostających poniżej progu wojny działań wobec innych państw. Są to działania nieregularne na terytorium atakowanego państwa oraz działania polegające na atakowaniu jego cyberprzestrzeni i sfery informacyjnej. Cele FR to osłabienie państwa, dezorganizacja, podważenie zaufania do rządu i instytucji publicznych oraz polaryzacja społeczeństwa. Nasilenie ataków hybrydowych na Polskę ze strony rosyjskiej zaobserwowano wraz z wybuchem pełnoskalowej wojny w Ukrainie. Nagły wzrost liczby ataków na polską cyberprzestrzeń oraz infosferę nastąpił wraz z kryzysem migracyjnym na granicy polsko-białoruskiej w 2021 r.

W literaturze przedmiotu niewiele jest publikacji, w których zestawione zostały różne metody ataków hybrydowych przeprowadzanych przez Rosję wobec Polski. Ze względu na tempo rozwoju technologii, a także wpływ cyberprzestrzeni

i infosfery (często wykorzystywanych do ataków hybrydowych) na funkcjonowanie państwa i społeczeństwa budowanie świadomości o przedmiocie badań wydaje się fundamentalne.

Celem artykułu[1] jest opis ataków i działań hybrydowych ze strony FR godzących w bezpieczeństwo narodowe i cyberprzestrzeń Rzeczypospolitej Polskiej, które przeprowadzono od czerwca 2021 r. do grudnia 2024 r. Teza przyjęta w artykule zakłada, że ataki na nienaruszalność granicy Polski przeprowadzone przez FR przy pomocy Białorusi miały związek z wojną w Ukrainie oraz że działania hybrydowe wymierzone w Polskę przed wojną i w jej trakcie były intencjonalną, systemową ingerencją Rosji i Białorusi. Aby zrealizować założenia badawcze, zastosowano takie metody, jak analiza, synteza i wnioskowanie. Przeanalizowano literaturę przedmiotu, raporty opracowane przez polskie instytucje państwowe, a także oficjalne informacje związane z wrogimi działaniami wymierzonymi w RP, udostępnione przez zespoły powołane do reagowania na incydenty komputerowe.

Teoria wojny hybrydowej

Wojna hybrydowa jest połączeniem wojny w rozumieniu klasycznym oraz innych typów działań. Mogą one występować zarówno niezależnie, jak i równolegle czy bezpośrednio po sobie. Taki schemat stwarza atakującemu szerokie możliwości, a co za tym idzie – generuje duży zbiór zagrożeń, z jakimi musi się zmagać atakowany.

Należy zaznaczyć, że definicje pojęć dotyczących wojny hybrydowej są różne w państwach zachodnich i FR. Rosyjska teoria jest stworzona w opozycji do teorii wypracowanej w Stanach Zjednoczonych i Europie Zachodniej. Zabieg przenoszenia terminologii na grunt rosyjski ma podkreślać jej „obronny" charakter[2]. Najczęściej przywoływanym zachodnim teoretykiem wojny hybrydowej jest pochodzący ze Stanów Zjednoczonych Frank G. Hoffman, który zauważa, że wojny tego rodzaju nie są nowe, lecz za każdym razem są inne[3]. Według niego taki rodzaj konfliktu cechuje się (…) *zbieżnością* (…) *fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów* (…), *sił zbrojnych i społeczności, państw i aktorów niepaństwowych,*

[1] Artykuł powstał na podstawie pracy dyplomowej pt. *Ataki hybrydowe prowadzone i koordynowane przez Federację Rosyjską przeciwko Rzeczypospolitej Polskiej w kontekście wojny w Ukrainie*, napisanej pod kierunkiem dr. hab. Jerzego Surmy, profesora Szkoły Głównej Handlowej (SGH) w Warszawie. Praca została obroniona w 2025 r. w ramach studiów podyplomowych w SGH na kierunku zarządzanie cyberbezpieczeństwem (przyp. red.).

[2] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*, Warszawa 2014, s. 11.

[3] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, s. 8.

a także zdolności bojowych, w które są wyposażone[4]. Pojęcie zbieżności w kontekście teorii przedstawionej przez Hoffmana można rozumieć jako jednoczesne występowanie i wzajemne przenikanie się elementów militarnych i niemilitarnych w działaniach charakterystycznych dla wojen hybrydowych.

Olga Wasiuta i Sergiusz Wasiuta prezentują inne cechy wojny hybrydowej wskazywane w amerykańskiej teorii. Są to:

- połączenie wojny konwencjonalnej, działań nieregularnych, wojny informacyjnej i cyberwojny,
- przeprowadzanie ataków przy użyciu różnych metod i narzędzi,
- stosowanie kombinacji broni i działań nieregularnych (wojny partyzanckiej, terroryzmu, przestępczości),
- złożona, dynamiczna i elastyczna przestrzeń pola walki,
- szybka reakcja i adaptacja uczestników do dynamiki konfliktu,
- stosowanie nowoczesnych technologii, działań i metod mobilizacji[5].

Za głównego rosyjskiego badacza teorii wojny hybrydowej uważa się Walerija Gierasimowa. Pomimo że nie używa on w swoich rozważaniach pojęcia wojny hybrydowej, to wskazuje na charakterystyczne dla tego zjawiska elementy, tj. konieczność wykorzystania w nowoczesnych konfliktach rozmaitych instrumentów politycznych, ekonomicznych i humanitarnych oraz połączenia ich z manipulowaniem nastrojami społeczności zamieszkującej teren adwersarza. Działania te mają być wspierane przez środki pozamilitarne takie jak wojna informacyjna i operacje jednostek specjalnych. W późniejszej fazie konfliktu dopuszcza się wykorzystanie oddziałów zbrojnych, jednak pod postacią misji pokojowych czy humanitarnych[6].

Andrzej Krzak opisał również inne definicje wojny hybrydowej obecne w rosyjskiej literaturze przedmiotu. Zgodnie z jedną z przytoczonych przez niego teorii wojna hybrydowa charakteryzuje się mnogością różnego rodzaju działań, prowadzonych w sposób konwencjonalny (klasyczny) i nieregularny, przy wsparciu segmentu pozamilitarnego. W myśl kolejnej rosyjskiej teorii wojna hybrydowa ma charakteryzować się w stosunkach międzynarodowych kompleksowym i metodycznym oddziaływaniem zarówno militarnym, jak i politycznym, ekonomicznym i społecznym. W jeszcze innym rosyjskim ujęciu wojny hybrydowej, tym razem w kontekście wojskowo-politycznym, jest to zastosowanie na terytorium potencjalnego

[4] F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly" 2009, nr 52, s. 34. Tłumaczenia w artykule pochodzą od autorki (dop. red.).

[5] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017, s. 56–57.

[6] A. Krzak, *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 25.

przeciwnika różnorodnej taktyki wojskowej i politycznej, a także działań destabilizacyjnych o charakterze społeczno-ekonomicznym[7].

Federacja Rosyjska swoją doktrynę wojny hybrydowej zamienia w rzeczywiste działania podejmowane wobec innych państw, a w związku z wybuchem wojny w Ukrainie zwłaszcza wobec RP. Rosyjskie działania noszące znamiona wojny hybrydowej wymierzonej przeciwko Polsce można podzielić na trzy kluczowe obszary: kryzys migracyjny, ataki w cyberprzestrzeni oraz kampanie dezinformacyjne. Działania te są skoordynowane w czasie, pod względem wykorzystywanych narzędzi, podmiotów je przeprowadzających oraz celów. Pomimo starań Rosji o odsunięcie od siebie winy i odpowiedzialności za ataki polskie służby i eksperci[8] w wielu przypadkach jednoznacznie przypisali sprawstwo stronie rosyjskiej i białoruskiej oraz ujawnili ich motywacje i wrogie dążenia.

Ataki na nienaruszalność polskiej granicy z Białorusią

Kryzys migracyjny, z którym Polska mierzy się od 2021 r., jest elementem działań hybrydowych prowadzonych przez Rosję przy pomocy Białorusi. Jest on organizowany i zarządzany przez reżim Aleksandra Łukaszenki, wykorzystujący migrantów jako narzędzia politycznego nacisku. Ataki wymierzone w nienaruszalność polskiej granicy, wspierane wrogimi działaniami dezinformacyjnymi, mają na celu destabilizację bezpieczeństwa Polski i Unii Europejskiej, wywarcie presji politycznej, polaryzację i zantagonizowanie społeczeństwa, a także stwarzają możliwość wprowadzenia na teren UE terrorystów i innego rodzaju przestępców[9].

Migranci, będący podmiotem działań hybrydowych, które koordynują reżimy Białorusi i Rosji, codziennie podejmują próby nielegalnego przekraczania polskiej granicy z Białorusią[10]. Granica polsko-białoruska jest jednocześnie częścią wschodniej granicy UE, strefy Schengen oraz NATO. Pierwszym krajem dotkniętym kryzysem migracyjnym wywołanym przez Rosję i Białoruś była Litwa, która musiała zmierzyć się z nim już w lipcu i sierpniu 2021 r. Przytoczone poniżej dane wskazują, że w tym samym czasie, kiedy trwał kryzys migracyjny na granicy

[7] Tamże, s. 18–19.

[8] Zob. szerzej: *Hybrydowa agresja Białorusi na UE*, Serwis Rzeczypospolitej Polskiej, 9 XI 2021 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [dostęp: 3 VI 2025]; M. Marek, *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*, Warszawa 2025.

[9] *Hybrydowy atak na Polskę*, Serwis Rzeczypospolitej Polskiej, 9 VIII 2022 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [dostęp: 30 V 2025].

[10] *Wojna Federacji Rosyjskiej z Zachodem*, M. Banasik (red. nauk.), Warszawa 2022, s. 126.

Polski z Białorusią, Straż Graniczna odnotowała zwiększoną liczbę prób nielegalnego przekroczenia granicy polsko-litewskiej przez obywateli państw trzecich[11].

Jak informował rzecznik koordynatora służb specjalnych, w organizację działań związanych z kolejnym etapem wojny hybrydowej jest zaangażowany niemal cały aparat państwowy białoruskiego reżimu. Schemat organizacyjny szlaku nielegalnej migracji rozpoczyna się od wystawiania migrantom zaproszeń przez specjalne biura podróży oraz wiz „turystycznych" przez Ministerstwo Spraw Zagranicznych Białorusi. Następnie migranci docierają na Białoruś państwowymi białoruskimi liniami lotniczymi, które specjalnie w tym celu utworzyły nowe połączenia. Z lotnisk migranci są przemieszczani na granicę z Polską[12]. Tam białoruskie służby wspierają działania migrantów, którzy podejmują próby siłowego przekraczania granicy, atakują polskich funkcjonariuszy służących przy granicy i niszczą infrastrukturę[13].

Eskalacja agresywnych działań migrantów na granicy polsko-białoruskiej nastąpiła 8 listopada 2021 r. Próbowali oni siłą przedrzeć się na stronę polską, niszczyli ogrodzenie, przy czynnym wsparciu białoruskich służb[14]. Do kolejnej napastliwej próby nielegalnego masowego przekroczenia granicy przez cudzoziemców doszło 16 listopada na terenie przejścia granicznego w Kuźnicy.

Napięcie na granicy dodatkowo zwiększały różnego rodzaju prowokacje stosowane przez funkcjonariuszy białoruskiego reżimu. Dokonywali oni wobec polskich funkcjonariuszy i żołnierzy napaści słownych, rzucali w nich kamieniami, próbowali ogłuszać petardami, oślepiać reflektorami i laserami. Powszechne były prowokacje polegające na oddawaniu przez białoruskie służby strzałów przy granicy, przekraczanie jej przez umundurowane osoby z bronią długą, a nawet celowanie z broni do polskich żołnierzy i funkcjonariuszy pełniących służbę na granicy[15].

W 2021 r. Straż Graniczna odnotowała 2869 cudzoziemców będących obywatelami państw trzecich (spoza UE), którzy zostali zatrzymani za przekroczenie granicy państwowej wbrew przepisom (dalej: pgpwp) lub usiłowanie pgpwp na odcinku jej z Białorusią. Oznacza to wzrost o 1164% w stosunku do 2020 r. (odnotowano 227 cudzoziemców). Wśród zatrzymanych osób największe grupy stanowili obywatele Iraku, Afganistanu, Syrii, Somalii, Rosji oraz Białorusi. W tym samym okresie

[11] *Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa*, W. Śmiałek, Ł. Kominek, O. Balogh (red. nauk.), Poznań 2022, s. 293–294.

[12] *Hybrydowa agresja Białorusi na UE…*

[13] *Bezpieczeństwo i zagrożenia hybrydowe*, M. Banasiak, A. Rogozińska (red. nauk.), Warszawa 2022, s. 22.

[14] *Wielowymiarowość konfliktów kulturowych we współczesnym świecie*, W. Śmiałek (red. nauk.), Poznań 2024, s. 186.

[15] Tamże, s. 187.

na odcinku granicy z Litwą Straż Graniczna zarejestrowała 320 osób będących obywatelami państw trzecich, zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp, co daje wzrost o 158% w stosunku do 2020 r. (odnotowano 124 cudzoziemców). Najwięcej zatrzymanych osób pochodziło z Iraku i Syrii[16].

W 2022 r. Straż Graniczna odnotowała 586 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią. Jest to spadek o 80% w stosunku do 2021 r. Najwięcej zatrzymanych/ujawnionych osób było obywatelami Iraku, Syrii, Iranu, Afganistanu, a także Białorusi. W tym samym okresie na odcinku granicy z Litwą Straż Graniczna zarejestrowała 726 osób będących obywatelami państw trzecich, zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp. Oznacza to wzrost o 127% w stosunku do 2021 r. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Iraku, Afganistanu, Iranu i Syrii[17].

W 2023 r. Straż Graniczna odnotowała 562 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią, co daje spadek o 4% w stosunku do 2022 r. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Afganistanu, Białorusi i Syrii. Na odcinku granicy z Litwą Straż Graniczna odnotowała 727 cudzoziemców będących obywatelami państw trzecich zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp. W stosunku do 2022 r. jest to wzrost o 0,1%. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Syrii, Afganistanu, Iranu i Indii[18].

W 2024 r. Straż Graniczna odnotowała 2582 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią. Oznacza to wzrost o 359% w stosunku do 2023 r. Najwięcej zatrzymanych/ujawnionych osób było obywatelami Etiopii, Erytrei, Somalii, Syrii, Jemenu, Sudanu i Afganistanu. W tym samym okresie na odcinku granicy z Litwą Straż Graniczna zarejestrowała 432 osoby będące obywatelami państw trzecich, które zostały zatrzymane/ujawnione za pgpwp lub usiłowanie pgpwp. W stosunku do 2023 r. jest to spadek o 41%. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Afganistanu, Mołdawii, Białorusi[19].

[16] Statystyki SG – styczeń–grudzień 2021, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[17] Statystyki SG – styczeń–grudzień 2022, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[18] Statystyki SG – styczeń–grudzień 2023, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[19] Statystyki SG – styczeń–grudzień 2024, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Należy zaznaczyć, że przytoczone dane statystyczne odnoszą się do migrantów faktycznie zatrzymanych/ujawnionych. Liczba podejmowanych prób przekroczenia granic polsko-białoruskiej i polsko-litewskiej jest znacznie wyższa. Jak podają Podlaski Oddział Straży Granicznej i Nadbużański Oddział Straży Granicznej, tylko w 2021 r. na granicy z Białorusią odnotowano 39 697 prób nielegalnego przekroczenia granicy poza przejściami granicznymi. To ponad 300 razy więcej prób niż w 2020 r.[20] W 2024 r., jak informuje Podlaski Oddział Straży Granicznej, odnotowano blisko 30 000 prób nielegalnego przekroczenia granicy polsko-białoruskiej. Migranci pochodzili z 52 państw, głównie z Etiopii, Erytrei i Somalii. Zatrzymano również 346 organizatorów nielegalnego przekraczania granicy i pomocników w tym procederze, z czego 316 osób na granicy z Białorusią, a 30 na granicy z Litwą. Wśród zatrzymanych dominowali obywatele Ukrainy, Polski i Białorusi[21].

Kryzys migracyjny na granicy polsko-białoruskiej jest przykładem świadomych i zorganizowanych działań hybrydowych, w których Rosja, przy pomocy białoruskiego reżimu, wykorzystuje migrantów jako narzędzie politycznego szantażu. Aparat państwowy reżimu Łukaszenki nie tylko organizuje i kontroluje szlak migracyjny, lecz także prowadzi skoordynowane działania prowokacyjne i dezinformacyjne, mające na celu obarczenie Polski winą za kryzys i wywołanie podziałów w polskim społeczeństwie oraz na arenie międzynarodowej. Tego typu operacje pokazują, w jaki sposób Rosja wykorzystuje współczesne zagrożenia w swoich działaniach hybrydowych, aby destabilizować bezpieczeństwo i porządek w Polsce i Europie.

Ataki w cyberprzestrzeni

Intensywność rosyjskich cyberataków wymierzonych w Polskę wyraźnie wzrosła tuż przed inwazją Rosji w Ukrainie i po jej rozpoczęciu, co potwierdzają dane statystyczne przedstawione poniżej. Ataki są elementem szerszej strategii hybrydowej Kremla, mającej na celu destabilizację sytuacji w RP, wywieranie presji na polskie władze oraz wywołanie chaosu i niepewności w społeczeństwie. Prorosyjskie grupy hakerskie uderzają zarówno w instytucje państwowe, jak i w sektor prywatny,

[20] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [dostęp: 3 VI 2025].

[21] K. Zdanowicz, *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie*, 21 I 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [dostęp: 3 VI 2025].

media czy obywateli. Wykorzystują zaawansowane metody, takie jak ataki DDoS (ang. *distributed denial of service*), ransomware, phishing czy podszywanie się pod oficjalne strony rządowe. Część tych działań to bezpośrednia odpowiedź na wsparcie udzielane Ukrainie przez Polskę oraz na decyzje polityczne władz RP niekorzystne dla FR. We współczesnych konfliktach cyberprzestrzeń stała się istotnym polem walki, a jej skuteczna ochrona wymaga nieustannego monitoringu i szybkiej reakcji.

Szczególnie niebezpieczne są ataki typu APT (ang. *advanced persistent threats*), przeprowadzane przez grupy określane tym samym mianem. Są to zaawansowane, długotrwałe ataki, charakterystyczne dla tego rodzaju grup cyberprzestępczych, działających na zlecenie rządów. Grupy APT atakują, aby uzyskać strategiczne informacje, prowadzić cyberszpiegostwo, zakłócać funkcjonowanie atakowanego państwa, wpływać na jego politykę i gospodarkę. Wsparcie finansowe uzyskiwane od rządów zapewnia cyberprzestępcom dostęp do zaawansowanych zasobów i technologii, sprzyjających długotrwałym i skomplikowanym cyberatakom[22]. Znaczny segment tego środowiska stanowią grupy prorosyjskie[23].

Zgodnie z informacją podaną przez Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP incydenty w cyberprzestrzeni są typowymi dla Rosji działaniami retorsyjnymi, stanowiącymi odpowiedź na niekorzystne dla FR działania podejmowane przez inne państwa[24]. Grupy hakerskie stosujące m.in. ataki DDoS, ransomware czy phishing, a także wykorzystujące fałszywe strony internetowe podszywające się pod istniejące serwisy są powiązane z Kremlem. Szczególnie zagrożone są podmioty ze strategicznych sektorów, takich jak energetyczny czy zbrojeniowy. Ataki te są zbieżne z założeniami działań hybrydowych, które mają prowadzić do destabilizacji, zastraszenia i chaosu. Każdy cyberatak przynosi określone skutki – polityczne, finansowe, społeczne[25].

Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa powołano w Polsce trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego, tj. CSIRT GOV, CSIRT NASK i CSIRT MON. Ze względu na tematykę raportów o stanie polskiego bezpieczeństwa w cyberprzestrzeni, publikowanych przez te zespoły, autorka artykułu przeanalizowała raporty CSIRT GOV i CERT Polska (działający w strukturze CSIRT NASK) za lata 2021–2024, a także raporty za lata

[22] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025*, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf, s. 6 [dostęp: 10 VI 2025].

[23] Tamże, s. 14.

[24] *Rosyjskie cyberataki*, Serwis Rzeczypospolitej Polskiej, 29 XII 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [dostęp: 5 VI 2025].

[25] Tamże.

2021–2022 sporządzone przez CSIRT KNF, będący zespołem reagowania na incydenty bezpieczeństwa komputerowego w polskim sektorze finansowym[26].

Zespół CSIRT GOV (prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego) od 2010 r. publikuje roczne raporty o stanie bezpieczeństwa cyberprzestrzeni RP[27]. Największy przyrost liczby zgłoszeń dotyczących potencjalnych incydentów, a w konsekwencji wzrost liczby potwierdzonych incydentów, odnotowano w III i IV kwartale 2021 r. Najwięcej zgłoszeń dotyczyło w kolejności: infrastruktury krytycznej, instytucji, urzędów, ministerstw, służb i wojska, pozostałych sektorów[28]. W raporcie za 2021 r. zespół CSIRT GOV poinformował o ponadtrzykrotnym wzroście liczby zgłoszeń potencjalnych incydentów bezpieczeństwa teleinformatycznego w stosunku do roku poprzedniego. Odnotowano także aktywność sponsorowanych grup APT, szczególnie w kontekście infrastruktury krytycznej i administracji publicznej[29]. Z kolei zespół CERT Polska w 2021 r. poinformował o wzroście liczby obsłużonych incydentów o 182% w stosunku do roku poprzedniego[30].

W raporcie poświęconym analizie zagrożeń bezpieczeństwa cyberprzestrzeni dla rynku finansowego w Polsce z 2021 r. CSIRT KNF również odnotował, że największy przyrost liczby zgłoszonych niebezpiecznych stron nastąpił w III i IV kwartale 2021 r.[31]

W serwisie gov.pl, w sekcji dotyczącej cyberbezpieczeństwa, od 2022 r. zaczęło pojawiać się coraz więcej artykułów na temat zagrożeń związanych z oszustwami i dezinformacją, a w 2023 r. zaczęto publikować artykuły mówiące wprost o rosyjskich cyberatakach[32].

W raporcie CSIRT GOV dotyczącym 2022 r. po raz pierwszy poświęcono cały rozdział analizie działalności grup APT, których aktywność w obszarze cyberprzestrzeni RP była związana z wojną w Ukrainie[33]. Zwrócono uwagę na nieodnotowane

---

[26] *Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego*, Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [dostęp: 10 VI 2025].

[27] Raporty o stanie bezpieczeństwa cyberprzestrzeni RP, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 5 VI 2025].

[28] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*, Warszawa 2022, s. 14.

[29] Tamże, s. 64.

[30] CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2022, s. 12.

[31] CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków*, https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [dostęp: 8 VI 2025].

[32] Baza wiedzy – cyberbezpieczeństwo, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [dostęp: 8 VI 2025].

[33] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*, Warszawa 2023, s. 56.

wcześniej na tak szeroką skalę zagrożenia i działania, w tym wzrastającą liczbę kampanii socjotechnicznych i ataków DDoS, które były wymierzone przede wszystkim w usługi publiczne świadczone w internecie. Największą liczbę incydentów z 2022 r. zespół CSIRT GOV sklasyfikował w kategoriach: podatność, socjotechnika i niedostępność. W kategorii podatność odnotowano największą liczbę incydentów ze względu na wprowadzenie w lutym 2022 r. stopnia alarmowego CHARLIE-CRP, co skutkowało wzrostem liczby zidentyfikowanych zdarzeń, które mogły naruszyć bezpieczeństwo infrastruktury teleinformatycznej RP.

Kampanie socjotechniczne odnotowane przez CSIRT GOV w 2022 r. to kampanie phishingowe, podmiany stron internetowych i podszycia (często pod witryny administracji rządowej lub systemów rządowych). Ich intensywność utrzymywała się na wysokim poziomie, a adresatami byli odbiorcy masowi oraz przedstawiciele wybranych podmiotów. Te działania były ukierunkowane przede wszystkim na zdobycie nieuprawnionego dostępu do zasobów, którymi dysponował atakowany podmiot, przez pozyskanie danych uwierzytelniających. Ponadto ataki miały na celu dystrybucję złośliwego oprogramowania oraz uzyskanie dostępu do systemów informatycznych, aby realizować dalsze działania cyberprzestępcze[34].

W kategorii niedostępność odnotowano od lutego 2022 r. znaczny wzrost liczby ataków DDoS (826 incydentów, a w roku poprzednim – 310) wymierzonych w polskie witryny podmiotów administracji publicznej oraz infrastruktury krytycznej. Realizowały je grupy haktywistyczne, m.in. Killnet, NoName057(16), Cyber Armia Ludowa. Zespół CSIRT GOV wskazał, że w 2022 r. komponentem najbardziej narażonym na ataki w cyberprzestrzeni była infrastruktura krytyczna RP[35]. Potwierdził również, że działania Polski na rzecz wsparcia Ukrainy w wojnie z Rosją znacznie podniosły poziom zagrożenia w cyberprzestrzeni RP.

Zespół CERT Polska w raporcie rocznym z działalności w 2022 r. poświęca cały rozdział wpływowi wojny w Ukrainie na polskie cyberbezpieczeństwo. Z perspektywy czasu potwierdzono, że działania wojenne prowadzone przez Rosję są wspierane przez aktywność hakerów i grup haktywistycznych, a także szerzenie dezinformacji. Te nasilone działania w cyberprzestrzeni Rosja prowadziła już w miesiącach poprzedzających wojnę konwencjonalną w Ukrainie. Zdarzenia w polskiej cyberprzestrzeni, jakie CERT Polska łączy bezpośrednio z wojną w Ukrainie, podobnie jak CSIRT GOV, to zmasowane ataki DDoS na strony rządowe i witryny ważnych podmiotów gospodarczych, a także kampanie phishingowe wykorzystujące motyw wojny i pojawiające się głównie w mediach społecznościowych. W raporcie stwierdzono, że ataki mają destabilizować sytuację wewnętrzną w państwach, które wspierają Ukrainę.

[34] Tamże, s. 30.

[35] Tamże, s. 13–17.

Podano przykłady ataków DDoS przeprowadzonych przez rosyjskich haktywistów. Podkreślono ich częstą nieskuteczność oraz wykorzystywanie przede wszystkim do szerzenia propagandy i dezinformacji. Wymieniono również kampanie wykorzystujące wygląd znanych stron internetowych i stron instytucji rządowych, a także motyw wojny. Oszustwa obejmowały m.in. fałszywe panele logowania do Facebooka, fałszywe zbiórki, nigeryjski przekręt, fałszywe inwestycje[36].

W raporcie z 2022 r. CSIRT KNF również poświęcił rozdział zagrożeniom i rekomendacjom odnośnie do ataków DDoS oraz działań haktywistów w kontekście wojny w Ukrainie. Zespół poinformował, że w 2022 r. ataki typu DDoS były najliczniejsze. Miały one pewien wpływ na sektor finansowy w Polsce. Podkreślono dużą dostępność, łatwość wykorzystania, stosunkowo niewielki koszt i skuteczność tego typu metod przestępczych. Wskazano także na możliwość przeprowadzenia (planowanie ataków i kierowanie nimi) czy uczestniczenia (udostępnianie swoich zasobów) w ataku przez niemal każdą osobę. Zespół CSIRT GOV zauważył ponadto zależność celu ataków prorosyjskich grup cyberprzestępców od działań politycznych państw, które w ocenie haktywistów są wrogie wobec Rosji czy sprzyjające Ukrainie[37].

W raporcie CSIRT GOV dotyczącym 2023 r. znalazły się informacje, że w tym roku Polska nadal zmagała się z nasilonymi cyberzagrożeniami związanymi z konfliktem zbrojnym w Ukrainie. Na podstawie oceny aktywności grup APT w 2023 r. stwierdzono, że były to w dużej mierze ataki będące kontynuacją działań odnotowanych w 2022 r. Głównymi celami ataków pozostały instytucje państwowe oraz infrastruktura krytyczna, zwłaszcza w sektorach energetycznym i transportowym. Dominowały dwa typy działań przestępczych: ataki DDoS – wykorzystywane przez prorosyjskie grupy do zakłócania funkcjonowania stron internetowych i usług publicznych, a także kampanie socjotechniczne – mające na celu wyłudzanie danych, infekowanie systemów złośliwym oprogramowaniem, destabilizację procesów politycznych. Intensyfikacja tych działań nastąpiła w związku z wyborami parlamentarnymi w Polsce. Z raportu wynika, że w 2023 r. Polska była kluczowym celem rosyjskich operacji hybrydowych, łączących cyberataki z wojną informacyjną[38].

Zespół CERT Polska w raporcie za 2023 r. przedstawił analizę dotyczącą działań grup APT. Od czasu rozpoczęcia wojny w Ukrainie zauważono znaczne nasilenie ich aktywności, której celem w 2023 r. było przede wszystkim zakłócenie ciągłości

[36] CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2023, s. 93–100.

[37] CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [dostęp: 8 VI 2025].

[38] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, Warszawa 2024, s. 4–6.

działania polskich podmiotów z sektora transportu i logistyki[39]. Zauważono, że te grupy są powiązane z FR i/lub Białorusią[40].

Zespół CSIRT GOV w raporcie z działalności za 2024 r. poinformował, że w Polsce nadal utrzymywał się podwyższony poziom zagrożeń w cyberprzestrzeni, które obejmowały działania socjotechniczne, próby wykorzystywania podatności, ataki typu DDoS, publikacje danych pochodzących z wycieków, dokonywane także przez sponsorowane grupy haktywistyczne. W 2024 r. miały miejsce szczególne wydarzenia z perspektywy bezpieczeństwa, tj. wybory samorządowe, wybory do Europarlamentu, a także XXXIII Letnie Igrzyska Olimpijskie w Paryżu. Incydenty z 2024 r. opisane w raporcie potwierdzały, że w zainteresowaniu cyberprzestępców i aktorów państwowych są wszelkie podmioty, których zaatakowanie będzie godziło również w bezpieczeństwo kraju. W raporcie stwierdzono ponadto, że cyberataki to zagrożenie hybrydowe i element nowoczesnych konfliktów, w których wrogie działania są prowadzone poniżej progu wojny[41]. Szczególną uwagę zwrócono na zagrożenia atakami na łańcuchy dostaw, które zdefiniowano jako ataki wymierzone w zaufanego zewnętrznego dostawcę usług niezbędnego dla tego łańcucha. To poszerzyło potencjalny obszar ataku na kluczowe sektory infrastruktury w Polsce[42]. Potwierdzono, że ataki grup APT, motywowanych ideologicznie, politycznie i finansowo, niezmiennie stanowią największe zagrożenie dla administracji rządowej oraz infrastruktury krytycznej. W 2024 r. grupy te koncentrowały się na kontynuacji działań z lat 2022–2023 i tak jak wcześniej tę aktywność wspierały kampanie propagandowe, mające pokazać skuteczność i potencjał cyberataków. Zauważono, że 2024 r. charakteryzował się wzrostem wolumenu grup cyberprzestępczych, który był spowodowany przyrostem liczby grup motywowanych finansowo oraz zwiększającym się dostępem do wspomagających narzędzi typu AI. Jako głównego aktora wymieniono grupę APT28 (znaną również jako Fancy Bear), a następnie grupy APT29 (inaczej Cozy Bear), UNC1151 (znaną również jako Ghostwriter), APT15, DaVinci[43].

Zespół CERT Polska w raporcie z działalności za 2024 r. przedstawił, podobną do zespołu CSIRT GOV, obserwację dotyczącą aktywności grup APT, powiązanych przede wszystkim z FR i Białorusią. Poinformował, że te grupy miały realizować cele wywiadowcze i propagandowe, a większość ich działań polegała na próbach wyłudzenia danych uwierzytelniających do skrzynek pocztowych, dystrybucji złośliwego oprogramowania oraz atakach na systemy przemysłowe. Zwrócił ponadto

[39] CERT Polska, *Raport roczny z działalności CERT Polska 2023*, Warszawa 2024, s. 34.

[40] Tamże.

[41] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, Warszawa 2025, s. 5–6.

[42] Tamże, s. 113.

[43] Tamże, s. 54–56.

uwagę na proceder atakowania nie tylko instytucji publicznych czy dużych przedsiębiorstw, lecz także mniejszych podmiotów, będących ogniwami łańcuchów dostaw. Zespół CERT Polska jako najaktywniejsze spośród zaobserwowanych grup APT wymienił UNC1151, APT28 oraz APT29[44].

Należy zauważyć, że wszystkie zespoły przedstawiły w swoich analizach podobne wnioski co do trendów, głównych typów zagrożeń oraz sektorów najbardziej narażonych na cyberataki w Polsce. Są to:

- znaczny wzrost od 2021 r. liczby zgłoszeń i potwierdzonych incydentów w sieci w porównaniu z latami poprzednimi, zauważalny na kilka miesięcy przed agresją Rosji na Ukrainę w 2022 r.,
- nasilona i dynamiczna działalność grup cyberprzestępców powiązanych z FR i Białorusią,
- najczęstsze typy ataków to ataki DDoS i kampanie socjotechniczne,
- jedną z intencji ataków było wywołanie szeroko rozumianych zakłóceń w funkcjonowaniu państwa,
- obiektami cyberataków były przede wszystkim administracja rządowa, instytucje publiczne i podmioty infrastruktury krytycznej,
- charakterystycznym działaniem grup APT jest propagowanie swojej działalności w mediach społecznościowych,
- wzrost liczby ataków wymierzonych w mniejsze podmioty, będące ogniwami łańcuchów dostaw.

Amerykański odpowiednik polskich zespołów CSIRT, tj. Cybersecurity and Infrastructure Security Agency, opublikował w maju 2025 r. raport na temat szczególnego zagrożenia, z jakim obecnie mierzą się wschodnioeuropejskie podmioty, w tym polskie, będące ogniwami łańcuchów dostaw. Stwarza je wielokrotnie wymieniana przez polskie zespoły grupa APT28. Jak podkreśliło amerykańskie źródło, jest ona utożsamiana z rosyjskim Głównym Zarządem Wywiadowczym (GRU) i rosyjską jednostką wojskową 26165[45].

Cyberprzestrzeń stała się kluczowym polem działań hybrydowych, obejmujących zarówno ataki techniczne, jak i towarzyszące im kampanie informacyjne, mające na celu destabilizację państwa oraz wywieranie presji społecznej i politycznej. Rosyjskie cyberataki wpisują się w strategię działań hybrydowych, niejednokrotnie są odpowiedzią na działania niekorzystne dla Rosji i stanowią integralną część wojny z Ukrainą.

---

[44] CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2025, s. 33.

[45] *Russian GRU Targeting Western Logistics Entities and Technology Companies*, CISA, 21 V 2025 r., https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [dostęp: 10 VI 2025].

Dezinformacja w polskiej przestrzeni informacyjnej

Działania propagandowe i dezinformacyjne ze strony rosyjskiej są obserwowane przynajmniej od czasów Związku Radzieckiego, jednak rządy prezydenta Władimira Putina uczyniły Rosję jednym z najbardziej aktywnych aktorów w sferze informacyjnej, w tym w cyberprzestrzeni, na międzynarodowej scenie politycznej[46]. Kompleksowe działania prowadzone przez FR są określane mianem wojny informacyjnej i obejmują skoordynowane kampanie propagandowe i dezinformacyjne w cyberprzestrzeni[47]. Wojna informacyjna jest postrzegana jako jeden z najważniejszych elementów strategii rywalizacji międzynarodowej Rosji, mający umożliwić osiąganie celów politycznych tego państwa. Cyberprzestrzeń natomiast umożliwia FR prowadzenie działań w ramach tej wojny[48].

Jerzy Surma podkreśla szczególną rolę, jaką w wojnie informacyjnej odgrywają media społecznościowe. Zwraca uwagę na konsekwencje dla bezpieczeństwa państwa, jakie niesie łatwa i tania możliwość publikowania i wymiany informacji. Te cechy mediów społecznościowych sprawiają, że stają się one jednocześnie miejscem i narzędziem prowadzenia wojen informacyjnych, których celem jest zarządzanie informacją w taki sposób, aby wpływać na zachowania społeczeństwa i kształtować je zgodnie z wolą atakującego.

Wojna informacyjna jest prowadzona w sposób zorganizowany, przy wykorzystaniu zarówno działań jawnych, takich jak propaganda czy manipulowanie informacjami, jak i niejawnych, polegających m.in. na fabrykowaniu informacji w celach dezinformacyjnych. Federacja Rosyjska została przez niego podana jako przykład państwa systemowo prowadzącego w ramach wojen hybrydowych działania, które mają znamiona wojen informacyjnych[49].

Wrogim działaniom tego typu można przypisać następujące cele:

- zachwianie systemu wartości (rozpad więzi społecznych, izolowanie jednostek lub grup, nieufność wobec instytucji publicznych),
- atak na ważne obiekty (infrastrukturę krytyczną, obiekty kultu i symbole międzynarodowe),

[46] *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*, M. Banasik (red. nauk.), Warszawa 2021, s. 7.

[47] Tamże.

[48] Tamże, s. 8.

[49] J. Surma, *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo*, Warszawa 2017, s. 90.

- kreowanie i wykorzystanie liderów opinii (kształtowanie percepcji przez osoby wpływowe i/lub mające zdolność oddziaływania na szerokie grupy odbiorców)[50].

W literaturze przedmiotu podkreśla się wieloaspektowość rosyjskich kampanii realizowanych w sferze informacyjnej, a także ich znaczenie strategiczne. Prowadzona przez nich wojna informacyjna obejmuje procesy, które są ukierunkowane na sferę poznawczą człowieka i kształtowanie postaw ludzi zgodnie z oczekiwaniami atakującego[51].

Od 24 lutego 2022 r. Rosjanie deprecjonowali wizerunek RP zarówno w swojej, jak i zewnętrznej infosferze. Aktywność ta polegała m.in. na rozwijaniu polskojęzycznych kanałów na platformie Telegram (na których grupy haktywistyczne udostępniały w celach propagandowych np. nieprawdziwe informacje o atakach wymierzonych w polskie obiekty[52]), działaniach tzw. kont trollowskich i botowskich oraz zauważalnej aktywności środowisk zaangażowanych w rozpowszechnianie rosyjskiego przekazu. Dezinformacyjne materiały i narracje obecne na rosyjskich kanałach na Telegramie, także tych polskojęzycznych, były następnie udostępniane w innych kanałach polskiego segmentu sieci społecznościowych. W realizację rosyjskich celów informacyjnych wpisywały się również nowo powstałe stowarzyszenie Polski Ruch Antywojenny oraz kampanie o politycznym wydźwięku, takie jak „Stop ukrainizacji Polski" czy „To nie nasza wojna". Ponadto strona białoruska ujawniła polskich obywateli, którzy wyemigrowali do Białorusi i Rosji i rozpoczęli prorosyjską działalność dezinformacyjną. Rozpowszechniali oni w mediach społecznościowych rosyjskie przekazy propagandowe i dezinformacyjne[53].

Platforma Telegram została założona przez rosyjskich obywateli w 2013 r. W 2021 r. nastąpił rozwój jej polskojęzycznego segmentu. Do jej popularyzacji w Polsce przyczyniły się dwa wydarzenia z 2021 r., za które prawdopodobnie odpowiada strona rosyjska.

Pierwszym z nich było opublikowanie na Telegramie danych pozyskanych po ataku na skrzynki mailowe polskich polityków[54]. Jednym z nich był minister Michał Dworczyk. Informacje pochodzące z jego skrzynki mailowej zaczęły pojawiać się na kanale Telegram od 4 czerwca. Eksperci twierdzą, że za te działania jest

[50] *Odporność państwa, społeczeństwa i gospodarki na zagrożenia*, M. Piotrowska-Trybull, K. Górska-Rożej (red. nauk.), Warszawa 2024, s. 331–332.

[51] *Informacja czynnikiem warunkującym bezpieczeństwo*…, s. 50.

[52] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, s. 25–28.

[53] M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, s. 116–117.

[54] Tamże, s. 119.

odpowiedzialna Rosja lub współpracująca z nią Białoruś[55]. Atak wpisuje się w założenia kampanii o nazwie „Ghostwriter", której celem jest pozyskiwanie przez rosyjskie służby specjalne danych i wrażliwych informacji oraz rozprzestrzenianie rosyjskiej dezinformacji[56]. W ramach tej kampanii są atakowane konta poczty internetowej oraz konta w mediach społecznościowych należące do osób publicznych z krajów Europy Środkowo-Wschodniej, głównie z Polski. Przestępcy podejmują próby przejmowania zasobów informacyjnych na potrzeby rosyjskiej dezinformacji[57].

Drugim wydarzeniem był kryzys migracyjny na granicy polsko-białoruskiej w Polsce w 2021 r. Przez Telegram (a dalej inne platformy społecznościowe i media) do polskiej infosfery trafiały nagrania i przekazy propagandowe[58]. Popularyzacja tego narzędzia w Polsce pozwoliła na przekazywanie narracji rosyjsko-białoruskiej[59].

Jak podaje Michał Marek, kierownik Zespołu Analiz Zagrożeń Zewnętrznych NASK, rosyjska dezinformacja skupia się na trzech głównych narracjach: o popychaniu Polski w stronę wojny z Rosją[60], o odpowiedzialności NATO i USA za wybuch wojny w Ukrainie[61], o objęciu Polski tzw. ukrainizacją[62]. Rok po wybuchu wojny w Ukrainie rzecznik prasowy Ministerstwa Spraw Zagranicznych RP zamieścił komentarz, w którym napisał o bezprecedensowym wzroście skali rosyjskiej działalności dezinformacyjnej. Zauważył, że Rosja prowadzi szeroko zakrojoną kampanię dezinformacyjną. Jej celami są podważenie wartości wolnego i demokratycznego świata oraz wywołanie chaosu, nawoływanie do nienawiści i destabilizacja międzynarodowego porządku. Rzecznik wskazał, że pomimo nowych form fałszywych narracji podstawowe metody manipulacji pozostają takie same. Ten sam jest również cel – wzbudzenie napięć i niepokojów w atakowanych społeczeństwach. Przestrzegał przed przekazywaniem odbiorcom sprzecznych informacji, które mają

[55] *Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki*, CyberDefence24, 16 VIII 2024 r., https://cyber-defence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [dostęp: 11 VI 2025].

[56] *Rozwój technik ataku grupy UNC1151/Ghostwriter*, Cert.pl, 19 VII 2022 r., https://cert.pl/posts/2022/07/techniki-unc1151/ [dostęp: 23 VI 2025].

[57] *Rosyjskie cyberataki*…

[58] M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, s. 119.

[59] Tamże, s. 123.

[60] Tamże, s. 131.

[61] Tamże, s. 140.

[62] Tamże, s. 146.

sprawić, że ludzie przestaną odróżniać prawdę od fałszu. To pozwoliłoby na uwiarygodnienie nawet najbardziej absurdalnych wersji wydarzeń[63].

W styczniu 2025 r. został opublikowany raport zespołu ds. dezinformacji z Komisji do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024. Zwrócono w nim uwagę na teorię rosyjskiej strategii walki informacyjnej, która oddaje istotę i charakter działań prowadzonych w polskiej infosferze. Zafałszowane w różnym stopniu treści pojawiają się zarówno w tradycyjnych mediach, jak i mediach społecznościowych oraz na platformach internetowych. Wskazano na rosyjską agencję informacyjną Sputnik, która miała polską wersję strony, a publikowane na niej treści były udostępniane przez spreparowane środowiska informacyjne, a dalej przez konta w mediach społecznościowych[64]. Stwierdzono ponadto, że wraz z wybuchem wojny w Ukrainie w 2022 r. rosyjska propaganda zaczęła prowadzić narrację o bezbronności państw zachodnich (w tym Polski), słabości ich armii i władz. Celem było przekonanie odbiorców, że państwo nie zapewnia im bezpieczeństwa, a w razie zagrożenia nie warto go bronić[65]. Eksperci tworzący ten raport zwrócili uwagę na cele rosyjskiej dezinformacji i propagandy, czyli polaryzację społeczeństwa, erozję zaufania do państwa, a także do nauki, mediów i współobywateli[66].

Skalę rosyjskich działań dezinformacyjnych odzwierciedlają również meldunki sytuacyjne zamieszczone w serwisie gov.pl. W 2023 r. opublikowano 31 meldunków opisujących działania dezinformacyjne prowadzone przez Rosję i Białoruś przeciwko Polsce. Dotyczyły one fałszywych oskarżeń wobec Polski, m.in. o brutalne traktowanie migrantów na granicy oraz plany agresji na Ukrainę. Podkreślono w tych meldunkach, że te działania miały na celu wywołanie społecznych podziałów oraz osłabienie zaufania do polskich władz i instytucji, a także były elementem wojny informacyjnej mającej na celu destabilizację Polski i regionu[67].

---

[63] *O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ*, Serwis Rzeczypospolitej Polskiej, 23 II 2023 r., https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [dostęp: 14 VI 2025].

[64] Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, *Raport Zespołu ds. Dezinformacji*, Warszawa 2025, s. 5.

[65] Tamże, s. 19.

[66] Tamże, s. 20.

[67] Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [dostęp: 14 VI 2025].

Skalę dezinformacji w 2023 r. ukazało również Rządowe Centrum Bezpieczeństwa (RCB). W ramach projektu DisInfo Radar RCB opublikowano 57 infografik przedstawiających tematy, których dotyczyła rosyjska i białoruska dezinformacja. Informowano w nich m.in. o fałszywych liniach rosyjskich perswazji i narracji, nieprawdziwych tezach, manipulacjach, stronach internetowych zaobserwowanych w 2023 r.[68] Przed kampanią dezinformacyjną ostrzegano zwłaszcza w październiku 2023 r., kiedy w Polsce odbywały się wybory parlamentarne. Wymieniono zagrożenia, na jakie narażone było bezpieczeństwo procesu wyborczego, a także poinformowano o trwającej kampanii informacyjnej, sugerującej przygotowywanie w Polsce zamachu stanu i zamiar użycia wojska przeciwko społeczeństwu[69].

Polskie zespoły reagowania na incydenty komputerowe od 2021 r. również zwracały uwagę w swoich rocznych raportach na rosyjskie kampanie dezinformacyjne. Zespół CSIRT GOV w raporcie z działalności za 2021 r. informował o odnotowanych aktywnościach grup APT, którym przypisano szerzenie dezinformacji. Jako jeden z przykładów podano operację „Ghostwriter", której sprawstwo przypisuje się grupie UNC1151[70].

W raporcie z działalności za 2022 r. zespół CSIRT GOV informował o identyfikacji incydentów, które wskazywały na kontekst dezinformacyjny. Jako przykład podano atak z września 2022 r. polegający na umieszczeniu na stronie Urzędu Transportu Kolejowego treści o tematyce antyukraińskiej wraz z propagandowymi grafikami. Zespół CSIRT GOV poinformował ponadto o identyfikacji procederu polegającego na rejestracji witryn podszywających się pod nazwy oficjalnych domen rządowych, co wskazywało na możliwość wykorzystania ich do przeprowadzania ataków socjotechnicznych, w tym do dezinformacji[71]. Zespół CERT Polska w raporcie z działalności w 2022 r. także informował o dezinformacyjnych działaniach prorosyjskich grup cyberprzestępczych. Stwierdzono, że cechą charakterystyczną tych grup jest szerzenie dezinformacji[72].

To zjawisko zostało opisane również w raporcie z działalności CSIRT GOV w 2023 r. Zespół zwrócił uwagę na wybory parlamentarne, które stanowiły bodziec do intensyfikacji działań grup haktywistycznych, prowadzących

[68] Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [dostęp: 14 VI 2025].

[69] Tamże.

[70] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*…, s. 27.

[71] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, s. 31.

[72] CERT Polska, *Raport roczny z działalności CERT Polska 2022*…, s. 93.

ataki dezinformacyjne z wykorzystaniem różnych środków przekazu, w tym wiadomości e-mail i SMS. Sprawstwo przypisał m.in. grupie UNC1151[73].

Podobne obserwacje opisał zespół CERT Polska w raporcie z działalności za 2023 r. Jako najbardziej aktywną grupę APT także wskazał grupę UNC1151 oraz jej powiązanie z rządem Białorusi i rosyjskimi służbami specjalnymi. Atakowane osoby pochodziły głównie ze środowiska polityki i wojskowości, ale były to również osoby mogące mieć pośredni związek z Rosją czy Białorusią, np. prawnicy, tłumacze przysięgli języka rosyjskiego, księża prawosławni, pracownicy organizacji pozarządowych, dziennikarze. Wskazano na motywacje działań, jakimi były kradzież informacji w celach wywiadowczych oraz prowadzenie kampanii dezinformacyjnych. W 2023 r. zespół zaobserwował kampanie dezinformacyjne, które były związane z zagrożeniem terrorystycznym w Polsce, zbieraniem informacji o uchodźcach, rekrutacją do wojska czy brakiem jodku potasu w aptekach. W ocenie CERT Polska kampanie były ukierunkowane na szerzenie niepewności i podziałów w społeczeństwie. Odnotowano, że po wyborach parlamentarnych aktywność grupy UNC1151 znacznie zmalała[74].

W raporcie z działalności w 2024 r. zespół CSIRT GOV ponownie zwrócił uwagę na wybory samorządowe oraz wybory do Parlamentu Europejskiego, które były narażone na wrogie operacje dezinformacyjne prowadzone w cyberprzestrzeni. Kolejnym wydarzeniem, z którym wiązał się incydent dezinformacyjny, były XXXIII Letnie Igrzyska Olimpijskie w Paryżu. W sierpniu 2024 r. działające wspólnie prorosyjskie grupy haktywistyczne Beregini i Zarya wykradły dokumenty z systemów teleinformatycznych Polskiej Agencji Antydopingowej i opublikowały je w zmodyfikowanej formie, aby zdyskredytować polskich sportowców[75]. Zespół, podobnie jak w poprzednich latach, zaobserwował działalność grupy UNC1151, która tym razem prowadziła kampanię wymierzoną w użytkowników poczty najpopularniejszych dostawców – Gmail, Interia, Wirtualna Polska, Onet, o2. Dane ze skrzynek pocztowych przestępcy pozyskiwali przez podszywanie się pod administratorów poczty i nakłanianie użytkowników do logowania się za pomocą fałszywego panelu logowania[76]. Kolejnym poważnym incydentem przypisywanym sponsorowanym grupom cyberprzestępczym był atak na Polską Agencję Prasową w maju 2024 r. Na jej oficjalnej stronie dwukrotnie została zamieszczona fałszywa informacja dotycząca mobilizacji wojskowej w Polsce[77].

[73] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*…, s. 6.

[74] CERT Polska, *Raport roczny z działalności CERT Polska 2023*…, s. 93.

[75] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*…, s. 6.

[76] Tamże, s. 69.

[77] Tamże, s. 78.

Zespół CERT Polska w raporcie z działalności za 2024 r. omówił, podobnie jak zespół CSIRT GOV, kampanię dezinformacyjną wymierzoną w Polską Agencję Antydopingową. Ponadto została opisana kampania dezinformacyjna związana z ćwiczeniami wojskowymi Steadfast Defender 2024 i Dragon-24, dotycząca rzekomo pijanego kierowcy wojskowej ciężarówki. Zespół podkreślił, że treści dezinformacyjne, które pojawiły się w polskiej infosferze w 2024 r., nawiązywały do wielu wydarzeń społeczno-politycznych[78].

Podsumowanie

Przeprowadzona analiza informacji dotyczących kryzysu migracyjnego, ataków w cyberprzestrzeni i sferze informacyjnej Polski pozwala stwierdzić, że przedstawiciele polskich organów rządowych, służb mundurowych, w tym służb specjalnych, a także specjaliści zajmujący się wykrywaniem ataków w cyberprzestrzeni i zapobieganiu im nie mają wątpliwości co do specyfiki i charakteru rosyjskich działań skierowanych przeciwko Polsce. Stwierdzają, że agresywne działania ze strony Rosji są elementem prowadzonej wojny hybrydowej, ściśle związanej z atakiem na Ukrainę. Rosyjską strategię charakteryzuje stopniowe, zaplanowane osłabianie adwersarza przez prowadzenie działań na wielu płaszczyznach funkcjonowania państwa. To właśnie takie działania mają być najbardziej skuteczne.

Analiza danych zawarta w niniejszym artykule dowodzi prawdziwości postawionej tezy. Ataki na integralność RP dokonane przez FR miały bezpośredni związek z wojną w Ukrainie. Badania materiałów źródłowych przeprowadzone metodą analizy, syntezy i wnioskowania pozwalają stwierdzić, że za ataki hybrydowe prowadzone przeciwko Polsce od 2021 r. jest odpowiedzialna Rosja we współpracy z Białorusią.

Rosyjskie działania hybrydowe charakteryzuje zatarcie granicy między obszarami militarnym i cywilnym. Do realizacji swoich celów Rosja wykorzystuje cywili. Rosyjsko-białoruskie ataki hybrydowe są wymierzone w obszary, które mogą być istotne dla bezpieczeństwa Polski. Skoordynowane prowadzenie tych ataków w wielu obszarach jednocześnie ma spotęgować ich dotkliwość. Niezbędne jest zatem prowadzenie ćwiczeń na wypadek sytuacji kryzysowych, obejmujących nie tylko sferę militarną, lecz także cywilną, oraz wspólnych ćwiczeń międzysektorowych.

[78] CERT Polska, *Raport roczny 2024 z działalności CERT Polska*…, s. 35.

Bibliografia

Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa, W. Śmiałek, Ł. Kominek, O. Balogh (red. nauk.), Poznań 2022.

Bezpieczeństwo i zagrożenia hybrydowe, M. Banasik, A. Rogozińska (red. nauk.), Warszawa 2022.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*, Warszawa 2014.

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly" 2009, nr 52, s. 34–39.

Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski, M. Banasik (red. nauk.), Warszawa 2021.

Krzak A., *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 11–39.

Marek M., *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*, Warszawa 2025.

Odporność państwa, społeczeństwa i gospodarki na zagrożenia, M. Piotrowska-Trybull, K. Górska-Rożej (red. nauk.), Warszawa 2024.

Surma J., *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo*, Warszawa 2017.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017.

Wielowymiarowość konfliktów kulturowych we współczesnym świecie, W. Śmiałek (red. nauk.), Poznań 2024.

Wojna Federacji Rosyjskiej z Zachodem, M. Banasik (red. nauk.), Warszawa 2022.

Źródła internetowe

Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki, CyberDefence24, 16 VIII 2024 r., https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [dostęp: 11 VI 2025].

Baza wiedzy – cyberbezpieczeństwo, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [dostęp: 8 VI 2025].

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego, Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [dostęp: 10 VI 2025].

Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [dostęp: 14 VI 2025].

Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [dostęp: 14 VI 2025].

Hybrydowa agresja Białorusi na UE, Serwis Rzeczypospolitej Polskiej, 9 XI 2021 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [dostęp: 3 VI 2025].

Hybrydowy atak na Polskę, Serwis Rzeczypospolitej Polskiej, 9 VIII 2022 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [dostęp: 30 V 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 10 VI 2025].

O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ, Serwis Rzeczypospolitej Polskiej, 23 II 2023 r., https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [dostęp: 14 VI 2025].

Raporty o stanie bezpieczeństwa cyberprzestrzeni RP, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 5 VI 2025].

Rosyjskie cyberataki, Serwis Rzeczypospolitej Polskiej, 29 XII 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [dostęp: 11 VI 2025].

Rozwój technik ataku grupy UNC1151/Ghostwriter, Cert.pl, 19 VII 2022 r., https://cert.pl/posts/2022/07/techniki-unc1151/ [dostęp: 23 VI 2025].

Russian GRU Targeting Western Logistics Entities and Technology Companies, CISA, 21 V 2025 r., https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [dostęp: 10 VI 2025].

Statystyki SG – styczeń–grudzień 2021, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2022, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2023, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2024, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [dostęp: 3 VI 2025].

Zdanowicz K., *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie*, 21 I 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [dostęp: 3 VI 2025].

Akty prawne

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2026 r. poz. 20).

Inne dokumenty

CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2025.

CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2022.

CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2023.

CERT Polska, *Raport roczny z działalności CERT Polska 2023*, Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*, Warszawa 2022.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*, Warszawa 2023.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, Warszawa 2025.

CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [dostęp: 8 VI 2025].

CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków*, https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [dostęp: 8 VI 2025].

Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, *Raport Zespołu ds. Dezinformacji*, Warszawa 2025.

Agata Rytel

Absolwentka studiów podyplomowych na kierunku zarządzanie cyberbezpieczeństwem w Szkole Głównej Handlowej w Warszawie.

Kontakt: agatakalota0@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego

2026, nr 34, s. 173–194

 https://doi.org/10.4467/20801335PBW.26.008.23370

ARTYKUŁ

Wsparcie dla polskich służb mundurowych chroniących granicę polsko-białoruską jako odpowiedź na reperkusje operacji „Śluza" z 2021 roku

Support for Polish uniformed services protecting the Polish-Belarusian border as a response to the repercussions of the operation 'Sluice' in 2021

NORBERT ŁUCARZ

Uniwersytet Jagielloński

https://orcid.org/0009-0005-2615-9727

Abstrakt Celem artykułu jest opisanie wsparcia dla polskich służb mundurowych chroniących granicę polsko-białoruską, które w wyniku operacji „Śluza" z 2021 r. stały się obiektem dyskredytacji, a także celem agresji fizycznej i psychicznej. W artykule omówiono proceder instrumentalizacji migrantów w polityce Białorusi i Rosji, następnie przedstawiono wybrane służby mundurowe zaangażowane w ochronę granicy polsko-białoruskiej. Ukazano również formy agresji wobec polskich służb mundurowych w czasie operacji „Śluza" oraz omówiono ogólnopolską akcję społeczną „Murem za polskim mundurem".

Słowa kluczowe granica polsko-białoruska, kryzys migracyjny, akcja społeczna „Murem za polskim mundurem", instrumentalizacja migrantów

Abstract

The aim of the article is to describe the support for Polish uniformed services protecting the Polish-Belarusian border, which, as a result of the operation 'Sluice' in 2021 have undoubtedly become the object of discredit, as well as the target of physical and psychological aggression. The article discusses the migrants instrumentalisation practice in the policies of Belarus and Russia, then presents selected uniformed services involved in protecting the Polish-Belarusian border. The forms of aggression towards the Polish uniformed services during the operation 'Sluice' and the nationwide social campaign 'United we stand behind the Polish uniform' were also presented.

Keywords

Polish-Belarusian border, migration crisis, social campaign 'United behind the Polish Uniform', instrumentalization of migrants

Wprowadzenie

Kryzys migracyjny na granicach Białorusi z Litwą, Łotwą oraz Polską został starannie przygotowany. Za transport migrantów na tereny przygraniczne odpowiadały mafie przemytnicze, które przekonywały potencjalnych klientów o skuteczności i bezpieczeństwie świadczonych przez nie usług[1]. Migrantami byli przede wszystkim obywatele państw Bliskiego Wschodu i Azji Południowej: Afganistanu, Iraku, Iranu, Pakistanu, Syrii, a także Libii[2]. Za odpowiednią kwotę (liczoną w tysiącach dolarów) migranci otrzymywali transport do Mińska, zakwaterowanie oraz przewóz do granicy państw członkowskich Unii Europejskiej. Proceder był realizowany na wzór podróży turystycznych. Ściśle nadzorowały go władze z Białorusi[3]. Wiele podmiotów zaangażowanych w przerzut migrantów UE objęła sankcjami. W tej grupie znalazły się: białoruska linia lotnicza Belavia, syryjska linia lotnicza Cham Wings Airlines, białoruskie biura podróży CentrKurort i Oskartour,

[1] D. Niedźwiedzki, *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego*, „Politeja" 2024, t. 21, nr 1, s. 58–59. https://doi.org/10.12797/Politeja.21.2024.88.3.04.

[2] Z. Śliwa, A.K. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, „Wiedza Obronna" 2022, t. 278, nr 1, s. 93. https://doi.org/10.34752/2022-d278.

[3] J. Maciejewski, *Wewnętrzny front. Łukaszenki wojna informacyjna i kryzys migracyjny na granicy polsko-białoruskiej*, Warszawa 2022, s. 73.

hotele Mińsk i Planeta oraz turecka firma Vip Grup[4]. Miejsca przemytu migrantów do Europy pokrywają się ze wschodnioeuropejskim szlakiem migracyjnym, który obejmuje ponad 6000 km i przebiega wzdłuż granic państw członkowskich UE – Finlandii, Estonii, Łotwy, Litwy, Polski, Słowacji, Węgier, Rumunii oraz Bułgarii[5]. Wśród białoruskich służb zaangażowanych w wywołanie kryzysu migracyjnego były Komitet Bezpieczeństwa Państwowego Republiki Białorusi (ros. Комитет государственной безопасности Республики Беларусь, KGB), Państwowy Komitet Graniczny Republiki Białorusi (ros. Государственный пограничный комитет Республики Беларусь) oraz Specjalna Służba Aktywnych Działań (ros. Отдельная Служба Активных Мероприятий)[6]. Według białoruskiego opozycjonisty Aliaksandra Azarau operacja przemytu migrantów należała do zakresu działań KGB oraz służby granicznej, a opracował ją szef KGB Iwan Tertel. Operacja otrzymała kryptonim „Śluza"[7]. Należy rozróżnić dwie operacje: pierwszą z 2010 r. oraz drugą z 2021 r. Celem pierwszej było sprawdzenie szczelności granic UE, a także uzyskanie od wspólnoty europejskiej wsparcia finansowego dla Białorusi na wzmocnienie granicy państwowej. W tej operacji została wykorzystana ludność kaukaska wraz z cudzoziemcami przebywającymi na Białorusi. W kolejnej dekadzie zmienił się kierunek pozyskania migrantów oraz cel ich wykorzystania w działalności politycznej[8].

Celem artykułu jest opisanie przejawów solidarności wobec polskich służb mundurowych strzegących granicy polsko-białoruskiej na przykładzie akcji społecznej „Murem za polskim mundurem". Autor sformułował następujące pytania badawcze: jakie były powody rozpoczęcia akcji społecznej „Murem za polskim mundurem"? W jaki sposób przebiegała ta akcja? Postawił tezę: akcja społeczna „Murem za polskim mundurem" była odpowiedzią na dyskredytację polskich służb mundurowych w następstwie operacji „Śluza". W artykule zostały wykorzystane metoda analizy i krytyki piśmiennictwa, synteza oraz metoda deskrypcyjna.

---

[4] *Organizatorzy nielegalnego przerzutu migrantów do Polski objęci zachodnimi sankcjami*, InfoSecurity24, 27 I 2022 r., https://infosecurity24.pl/za-granica/organizatorzy-nielegalnego-przerzutu-migrantow-do-polski-objeci-zachodnimi-sankcjami [dostęp: 4 VII 2025].

[5] J. Werner, *Ochrona granicy wschodniej Rzeczypospolitej Polskiej w kontekście nielegalnej migracji*, „Studia Bezpieczeństwa Narodowego" 2024, t. 31, nr 1, s. 90. https://doi.org/10.37055/sbn/178377.

[6] B. Fraszka, *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, Warsaw Institute, 23 XII 2021 r., https://warsawinstitute.org/pl/sytuacja-na-granicy-polsko-bialoruskiej-przyczyny-aspekt-geopolityczny-narracje/ [dostęp: 14 II 2026].

[7] J. Maciejewski, *Wewnętrzny front*…, s. 73–74.

[8] A. Szachoń-Pszenny, A. Zaręba, *Instrumentalizacja migrantów jako forma destabilizacji bezpieczeństwa na wschodniej granicy zewnętrznej UE w kontekście wojny w Ukrainie*, „Politeja" 2024, t. 21, nr 1, s. 97–98. https://doi.org/10.12797/Politeja.21.2024.88.3.06.

Instrumentalizacja migrantów w polityce Białorusi i Rosji na przykładzie operacji „Śluza"

Instrumentalizacja migrantów przez białoruski reżim wpisuje się w jeden z czterech rodzajów inżynierii migracji opisanych przez Kelly Greenhill[9]. Zaaranżowany kryzys graniczny to odpowiednik tzw. przymusowej inżynierii migracji, charakteryzującej się wykorzystaniem człowieka w celach politycznych[10]. We współczesnych konfliktach między państwami działania militarne nie są jedyną metodą zdobywania przewagi nad przeciwnikiem. Środków i narzędzi wywierania nacisku jest znacznie więcej[11].

Rosyjski wojskowy gen. mjr Aleksander Władimirow, odnosząc się do doświadczeń Europy z masową migracją, wskazał na problemy wynikające z obecności przybyszów, w tym na zanik tożsamości europejskiej oraz możliwy wzrost radykalnych postaw w społeczeństwie przyjmującym migrantów. Zdaniem Władimirowa sterowanie masową migracją to współczesna broń strategiczna, za pomocą której można oddziaływać na sfery polityczną, gospodarczą i kulturową państwa. Zwrócił on również uwagę na pułapkę dylematu moralnego. Dotyczy on tego, czy państwo zachowa postawę humanitarną w sytuacji masowej migracji, czy jednak zdecyduje się zmarginalizować to podejście ze względu na potrzebę zapewnienia sobie bezpieczeństwa[12].

Na kolejny dylemat, powiązany z poprzednim, zwraca uwagę Krzysztof Chochowski. Wskazuje on na dwie formy działania w odpowiedzi na proceder instrumentalizacji migrantów: legalną (tzn. zgodną z prawem, lecz nieproduktywną) oraz efektywną (tzn. produktywną, ale naruszającą normy prawne). W ocenie Chochowskiego wybór któregokolwiek z rozwiązań będzie powodem do destabilizacji wewnętrznej państwa i polaryzacji społeczeństwa, gdyż jak stwierdził (odnosząc się do kryzysu na granicy polsko-białoruskiej): *W tym właśnie wyraża się swego rodzaju pułapka reżimu białoruskiego* (…)[13].

---

[9] A. Szachoń-Pszenny, A. Zaręba, *Etapowość instrumentalizacji migrantów na przykładzie granicy z Białorusią – wyzwania współczesności*, „Przegląd Geopolityczny" 2024, t. 49, s. 55.

[10] Tamże.

[11] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red. nauk.), Warszawa 2011, s. 11.

[12] M. Wojnowski, *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 31–33. https://doi.org/10.4467/20801335PBW.21.034.15694.

[13] K. Chochowski, *Kryzys na granicy polsko-białoruskiej jako przejaw wojny hybrydowej. Aspekty administracyjnoprawne*, „Roczniki Nauk Społecznych" 2021, t. 49, nr 4, s. 94. https://doi.org/10.18290/rns21494.8.

Za impuls do rozpoczęcia operacji „Śluza" można uznać konsekwencje wydarzeń z 23 maja 2021 r. związanych z wymuszonym lądowaniem samolotu linii Ryanair w Mińsku. Znajdował się w nim białoruski opozycjonista Raman Pratasiewicz, który został aresztowany przez funkcjonariuszy białoruskiej KGB. W odpowiedzi na powtarzające się przypadki zwalczania legalnej opozycji przez Aleksandra Łukaszenkę UE podjęła decyzję o nałożeniu sankcji na Białoruś[14]. Ponadto wspólnota europejska nie uznała zwycięstwa Łukaszenki w wyborach prezydenckich z 9 czerwca 2020 r. To pogłębiało izolację Białorusi na arenie międzynarodowej, a dla Łukaszenki stało się kolejnym argumentem potwierdzającym jego przekonanie, że celem UE jest destabilizacja sytuacji wewnętrznej na Białorusi[15]. Operacja „Śluza" miała doprowadzić do zniesienia sankcji nałożonych przez UE, wyjścia Białorusi z izolacji, a także pozyskania wsparcia finansowego potrzebnego do rozwiązania kryzysu[16]. Zdaniem Jerzego Marka Nowakowskiego jednym z powodów wywołania kryzysu migracyjnego mogła być także chęć Łukaszenki, aby społeczność międzynarodowa uznała go za pełnoprawnego prezydenta Białorusi[17]. Operacja „Śluza" nie doprowadziła do osiągnięcia zakładanych celów. Unia Europejska potępiła działania reżimu Łukaszenki i nałożyła na Białoruś kolejny, piąty pakiet sankcji (zostały nim objęte m.in. elity białoruskiego reżimu)[18]. Decyzja o wyborze Polski czy Litwy jako celów ataku wynikała z przynależności tych państw do UE, wspierania przez te państwa białoruskiej opozycji oraz z ich aprobaty dla nałożenia sankcji na reżim Łukaszenki[19].

Operacja „Śluza" była istotna przede wszystkim dla Rosji. Z kilku powodów. Po pierwsze, umożliwiła przetestowanie zdolności państw członkowskich UE oraz Sojuszu Północnoatlantyckiego z zakresu reagowania kryzysowego. Po drugie,

---

[14] G. Baziur, *Operation „Sluice". The so-called migration crisis at the Polish-Belarussian border: an example of hybrid actions taken in the second half of 2021 as documented in the reports of the Polish border guard*, „Bezpieczeństwo. Teoria i Praktyka" 2022, t. 46, nr 1, s. 137. http://dx.doi.org/10.48269/2451-0718-btip-2022-1-008.

[15] J. Szyszka, *Zjawisko state-sponsored human trafficking na przykładzie Białorusi*, w: *Wybrane zagadnienia handlu ludźmi i zagrożonymi gatunkami roślin i zwierząt*, B. Stępień-Załucka, J. Uliasz (red. nauk.), Rzeszów 2023, s. 122–123. http://dx.doi.org/10.15584/978-83-8277-037-7.9.

[16] A. Wawrzusiszyn, *Rosyjsko-białoruskie działania hybrydowe na granicach Unii Europejskiej i NATO*, „Journal of Modern Science" 2025, t. 61, nr 1, s. 19. https://doi.org/10.13166/jms/203108.

[17] J.M. Nowakowski, *O co idzie gra?*, w: *Raport IV. Granica dyktatora. Polska i Białoruś wobec kryzysu granicznego*, J.M. Nowakowski, J. Olędzka, M. Rust (red.), Warszawa 2021, s. 74.

[18] K. Wańczyk, *Relacje Unii Europejskiej z Białorusią po sierpniu 2020 roku. Powrót do przeszłości*, w: *Raport V. Białoruś 500 dni po: od społecznej mobilizacji do neototalitarnej konsolidacji?*, J.M. Nowakowski, J. Olędzka, M. Rust (red.), Warszawa 2022, s. 96–97.

[19] A. Szabaciuk, *Forced migrations in Eastern Europe after 2020*, seria: Prace Instytutu Europy Środkowej, nr 9, B. Surmacz, T. Stępniewski (red.), Lublin 2022, s. 28.

doprowadziła do polaryzacji społeczeństwa w państwie dotkniętym kryzysem migracyjnym, a także utrzymania niepokoju i niepewności co do zasadności działań aparatu państwowego w odpowiedzi na narastające zagrożenie zewnętrzne. Po trzecie, zdestabilizowała granice zaatakowanych państw (ich władze zostały zmuszone m.in. do znacznego zwiększenia wydatków finansowych na potrzeby bezpieczeństwa granic). Po czwarte, kryzys migracyjny na wschodzie Europy odciągnął uwagę od działań Rosji w Ukrainie oraz na Kaukazie[20]. Ponieważ do incydentów granicznych doszło na terytorium Białorusi, Rosja uniknęła bezpośredniej odpowiedzialności za wywołanie kryzysu[21].

Proceder instrumentalizacji migrantów wspierały białoruskie i rosyjskie ośrodki propagandowe: Białoruska Agencja Telegraficzna, Rosyjska Agencja Informacyjna TASS, RIA Novosti, Regnum oraz kanały telewizyjne: Biełarus-1, ONT i CTV, Rossija 1 oraz Pierwyj Kanał. W przypadku Polski zastosowano narrację odnoszącą się do nazizmu, rasizmu, ksenofobii oraz brutalności polskich służb mundurowych[22]. Wykorzystując zniekształcone bądź niezgodne z rzeczywistością informacje, Białoruś podawała w wątpliwość skuteczność działań poszczególnych państw oraz organizacji międzynarodowych. W operacjach informacyjnych szczególny nacisk kładła na podważanie praworządności, legalności władz, ich zdolność do zapewnienia bezpieczeństwa, jak również na godzenie w dobre imię państw Europy Środkowo-Wschodniej, szczególnie Polski, na arenie międzynarodowej. Tak wykreowany obraz rozmywał odpowiedzialność za kryzys migracyjny na wschodzie Europy. Białoruskie ośrodki medialne silnie oddziaływały na emocje odbiorców przez wykorzystywanie m.in. wizerunków dzieci[23]. O zbrodnie oraz naruszenia prawa były posądzane przede wszystkim służby mundurowe. Białoruski aparat państwowy stosował analogię do nazistowskich oddziałów z czasów II wojny światowej i ich metod działania. W obiegu publicznym funkcjonowały zwroty „oprawcy" w odniesieniu do polskich służb mundurowych oraz „obozy koncentracyjne" w odniesieniu do miejsc przebywania migrantów[24].

---

[20] Zob. szerzej: A. Wawrzusiszyn, *Rosyjsko-białoruskie działania*…, s. 19–27.

[21] J. Maciejewski, *Wewnętrzny front*…, s. 64–66.

[22] B. Ociepka, *Dziennikarzom wstęp wzbroniony: kryzys na polsko-białoruskiej granicy w 2021 r. jako wydarzenie (nie)relacjonowane przez media*, „Studia Medioznawcze" 2023, t. 24, nr 2, s. 198–199. https://doi.org/10.33077/uw.24511617.sm.2023.2.715.

[23] K. Kuśmirek, *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*, „Bezpieczeństwo. Teoria i Praktyka" 2022, t. 48, nr 3, s. 312–315. http://dx.doi.org/10.48269/2451-0718-btip-2022-3-023.

[24] A. Szabaciuk, *„Natowskie wojska szczękające gąsienicami czołgów". Polska i granica polsko-białoruska w propagandzie białoruskiej po 2020 roku*, w: *Bezpieczeństwo granic – granice bezpieczeństwa*, D. Karczewski, R. Zenderowski (red.), Warszawa 2023, s. 347–349.

Wzmocnienie ochrony granicy polsko-białoruskiej w odpowiedzi na operację „Śluza"

Według danych Komendy Głównej Straży Granicznej w 2021 r. aż 39 697 osób próbowało w sposób niezgodny z prawem przekroczyć granicę polsko-białoruską. W poprzednich latach takich przypadków odnotowano niewiele: 4 w 2018 r., 20 w 2019 r. oraz 129 w 2020 r. W 2021 r. apogeum kryzysu migracyjnego przypadło na październik (17 447 prób przekroczenia). Najwięcej prób przekroczenia podejmowano na odcinkach należących do obszaru Podlaskiego Oddziału Straży Granicznej. Były to odcinki podlegające placówkom Straży Granicznej (SG): Michałowo, Czeremcha, Białowieża oraz Kuźnica[25].

Do wzmocnienia ochrony granicy polsko-białoruskiej wykorzystano zarówno tradycyjne, jak i nowoczesne środki zabezpieczeń. Do tradycyjnych środków można zaliczyć całodobowe patrole, realizowane pieszo bądź przy użyciu różnego typu pojazdów. Katalog nowoczesnych środków obejmuje natomiast zastosowanie chłodzonych kamer termowizyjnych, fotopułapek oraz dronów. Środki te charakteryzują się odpornością na różnice temperatur, dokładnością identyfikacji zagrożenia i są trudne do wykrycia, dlatego stanowią ważny element ochrony granicy[26].

Decyzją Sejmu Rzeczypospolitej Polskiej została przyjęta *Ustawa z dnia 29 października 2021 r. o budowie zabezpieczenia granicy państwowej*. Na granicy polsko-białoruskiej powstały zabezpieczenia fizyczne i elektroniczne. Zapora fizyczna złożona ze stalowych przęseł mierzących 5,5 m wysokości objęła w sumie 186 km granicy. Została ona wzmocniona drutem żyletkowym. W drugiej kolejności wybudowano zaporę elektroniczną wzdłuż całej granicy z Białorusią. W skład systemu perymetrycznego wchodzą kamery dzienno-nocne, termowizyjne, kable detekcyjne oraz kontenery teletechniczne. Całkowity koszt umocnień granicznych wyniósł 1,6 mld zł[27]. Zabezpieczenia okazały się niewystarczające, dlatego w 2024 r. podjęto decyzję o zamontowaniu poprzecznych belek wraz z dodatkowym zwojem drutu żyletkowego, aby uniemożliwić rozginanie stalowych przęseł. Zapora elektroniczna

[25] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią w 2021 r.*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021r.html [dostęp: 1 IV 2025].

[26] J. Werner, *Ochrona granicy wschodniej*…, s. 95–97.

[27] K. Szwed, *Zakończenie odbioru bariery elektronicznej na granicy polsko-białoruskiej*, Straż Graniczna, 15 VI 2023 r., https://www.strazgraniczna.pl/pl/aktualnosci/11875,Zakonczenie-odbioru-bariery-elektronicznej-na-granicy-polsko-bialoruskiej.html [dostęp: 5 IV 2025].

została wzmocniona większą liczbą kamer i oświetleniem wraz z sensorami[28]. Modernizację ukończono 30 marca 2025 r.[29]

W ochronie granicy polsko-białoruskiej SG wspierały Policja, żołnierze Wojska Polskiego (WP) oraz Państwowa Straż Pożarna (PSP). Policja realizowała swoje zadania w ramach operacji pod kryptonimem „Zapora". Było w nią zaangażowanych 32 759 funkcjonariuszy różnych specjalności, m.in. kontrterroryści, lotnicy, przewodnicy psów służbowych[30]. Umożliwiło to wymianę doświadczeń oraz wzajemne szkolenia służb mundurowych obecnych na granicy polsko-białoruskiej. Policja prowadziła patrole wzdłuż granicy, odpierała zmasowane ataki migrantów oraz zwalczała aktywność siatek przemytniczych. Do identyfikacji zagrożeń wykorzystywała wielozadaniowe śmigłowce typu S70i Black Hawk oraz Bell 407GXi. Operacja „Zapora" zakończyła się 19 grudnia 2024 r.[31]

Żołnierze WP wspomogli działania funkcjonariuszy SG w ramach kilku operacji. Jedna z nich pod kryptonimem „Silne wsparcie" rozpoczęła się 3 września 2021 r.[32] Jednostki Wojsk Obrony Terytorialnej (WOT), w tym 1 Podlaska Brygada Obrony Terytorialnej oraz 2 Lubelska Brygada Obrony Terytorialnej, prowadziły patrole piesze, wodne, konne, a także posługiwały się systemami bezzałogowymi. Efektem tych działań były liczne zatrzymania migrantów i przemytników. Ze względu na wprowadzony stan wyjątkowy w terenach przygranicznych żołnierze WOT udzielali wsparcia również społeczności lokalnej[33]. W operację zostały zaangażowane także Żandarmeria Wojskowa oraz wojska operacyjne, m.in.: 12 Szczecińska Dywizja Zmechanizowana im. Bolesława Krzywoustego, 16 Pomorska Dywizja Zmechanizowana im. Króla Kazimierza Jagiellończyka, 18 Dywizja Zmechanizowana im. gen. broni Tadeusza Buka[34]. Zwiększenie obecności żołnierzy na granicy nastąpiło w wyniku operacji „Gryf". Wzmocniono w ten sposób działania funkcjonariuszy SG i Policji. Operacja

[28] *Szef BBN na granicy polsko-białoruskiej. Wzmacnianie zabezpieczeń to „dowód ciągłości myśli strategicznej państwa"*, Biuro Bezpieczeństwa Narodowego, 11 X 2024 r., https://www.bbn.gov.pl/pl/wydarzenia/10003,Szef-BBN-na-granicy-polsko-bialoruskiej-Wzmacnianie-zabezpieczen-to-quot-dowod-ci.html [dostęp: 5 IV 2025].

[29] *Modernizacja bariery elektronicznej na granicy Polski z Białorusią (WIDEO)*, Telbud S.A., https://telbud.pl/strefa-informacji/modernizacja-bariery-elektronicznej-na-granicy-polski-z-bialorusia-wideo [dostęp: 14 II 2026].

[30] *Zakończenie operacji policyjnej „Zapora"*, „Gazeta Policyjna" 2025, nr 49, s. 24–25.

[31] Tamże.

[32] *3 miesiące operacji #SilneWsparcie*, Wojska Obrony Terytorialnej, 3 XII 2021 r., https://media.terytorialsi.wp.mil.pl/informacje/712389/3-miesiace-operacji-silnewsparcie [dostęp: 6 IV 2025].

[33] Tamże.

[34] E. Moczuk, D. Czekaj, *Kryzys migracyjny jako element wojny hybrydowej. Analiza działania wojska na granicy polsko-białoruskiej*, Rzeszów 2024, s. 224.

„Rengaw" miała charakter szkoleniowo-obronny[35]. Decyzją ministra obrony narodowej powołano wojskowe zgrupowanie zadaniowe, które realizowało na terenie województwa podlaskiego program szkoleń dla żołnierzy. Zwiększenie ich obecności na terenach przygranicznych w ramach działań szkoleniowych miało pełnić również funkcję odstraszającą[36]. Dla zapewnienia pełnej skuteczności prowadzonych działań obie operacje 1 sierpnia 2024 r. zastąpiła operacja „Bezpieczne Podlasie"[37].

W ochronie granicy polsko-białoruskiej istotną rolę odegrali także funkcjonariusze PSP. Podczas masowych prób przekroczenia granicy przez migrantów zapewniali stały dostęp do wody dla policyjnych pojazdów specjalistycznych. Odpowiadali również za bezpieczeństwo i sprawne działanie lotnictwa wojskowego. Wraz z pozostałymi służbami mundurowymi wzmacniali zabezpieczenia graniczne oraz udzielali pomocy potrzebującym migrantom[38].

Formy agresji wobec polskich służb mundurowych

Służby mundurowe były narażone na przemoc zarówno fizyczną, jak i psychiczną ze strony migrantów, a także innych środowisk. Prowokacje białoruskich służb względem polskich żołnierzy i funkcjonariuszy miały na celu przetestowanie ich wytrzymałości psychicznej oraz wyszkolenia. W stronę polskich służb rzucano materiałami pirotechnicznymi, symulowano rzuty granatami, oddawano tzw. puste strzały, a także oślepiano latarkami i pozostawiano podejrzane opakowania[39]. Jak relacjonuje Helsińska Fundacja Praw Człowieka, białoruskie służby wykorzystywały również przemoc fizyczną wobec migrantów, aby w ten sposób wymusić na nich nielegalne przekroczenie granicy oraz wywołać reakcję polskich żołnierzy

[35] J. Dziemiańczuk, *„Bezpieczne Podlasie" zastąpi dwie dotychczasowe operacje*, Wojska Obrony Terytorialnej, 31 VII 2024 r., https://media.terytorialsi.wp.mil.pl/informacje/838336/bezpieczne-podlasie-zastapi-dwie-dotychczasowe-operacje [dostęp: 6 IV 2025].

[36] E. Korsak, *Nowa operacja wojskowa na Podlasiu*, Polska Zbrojna, 12 VIII 2023 r., https://polskazbrojna.pl/home/articleshow/40146?t=Nowa-operacja-wojskowa-na-Podlasiu [dostęp: 7 IV 2025].

[37] *Nowa operacja wojskowa na wschodniej granicy: OP Bezpieczne Podlasie*, Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-07-176-op-bezpieczne-podlasie/ [dostęp: 7 IV 2025].

[38] M. Łozowski, *Państwowa Straż Pożarna w obronie granic RP*, Krajowa Sekcja Pożarnictwa, 7 XII 2021 r., https://kspnszz.org/index.php/2021/12/07/panstwowa-straz-pozarna-w-obronie-granic-rp/ [dostęp: 8 IV 2025].

[39] J. Maciejewski, *Wewnętrzny front*…, s. 248–249.

i funkcjonariuszy[40]. Jednym z przykładów był atak na przejściu granicznym Kuźnica–Bruzgi w listopadzie 2021 r. Został on poprzedzony podprowadzeniem przez białoruskie służby tysiąca migrantów. Przyjęły one postawę obserwatora wydarzeń. Migranci wielokrotnie zaatakowali polskich żołnierzy oraz funkcjonariuszy, wykorzystując różnego rodzaju narzędzia: kamienie, kostki brukowe, butelki, kłody, a także granaty hukowe. Zdrowie i życie funkcjonariuszy polskich służb mundurowych i żołnierzy[41] były narażone na duże niebezpieczeństwo. Potwierdzają to fotografie i relacje z tych zdarzeń.

W atak na polskie służby mundurowe włączyli się również niektórzy polscy politycy i celebryci. Z ich ust padały obraźliwe komentarze pod adresem ludzi strzegących granicy[42].

Uznanie dla polskich służb mundurowych ze strony władz państwowych i społeczeństwa

W związku z wydarzeniami na granicy polsko-białoruskiej oraz negatywnymi narracjami dotyczącymi działań polskich służb mundurowych zarówno władze państwowe, jak i społeczeństwo okazały wsparcie funkcjonariuszom i żołnierzom pełniącym służbę na granicy. Sejm RP podjął dwie uchwały, a minister obrony narodowej ustanowił znak specjalny. Społeczeństwo wyraziło uznanie w ramach

[40] K. Czarnota, M. Górczyńska, *Gdzie prawo nie sięga. Raport Helsińskiej Fundacji Praw Człowieka z monitoringu sytuacji na polsko-białoruskiej granicy*, Helsińska Fundacja Praw Człowieka, Warszawa 2022, s. 39–40.

[41] M. Jurkowska, *Masowy szturm na przejście graniczne w Kuźnicy. Mija rok od ataku cudzoziemców na granicę i funkcjonariuszy SG*, Sokółka Nasze Miasto, 16 XI 2022 r., https://sokolka.naszemiasto.pl/masowy-szturm-na-przejscie-graniczne-w-kuznicy-mija-rok-od/ar/c1-9090195 [dostęp: 11 IV 2025].

[42] M. Kożdoń-Dębecka, *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych*, „Media Biznes Kultura" 2023, t. 14, nr 1, s. 170–171. https://doi.org/10.4467/25442554.MBK.23.010.18033; K. Orzech, *Zagrożenia dla Polski kreowane przez Republikę Białorusi w kontekście sytuacji kryzysowej na granicy polsko-białoruskiej*, „Studia Bezpieczeństwa Narodowego" 2021, t. 22, nr 4, s. 63. https://doi.org/10.37055/sbn/147013; P. Rojek-Socha, K. Żaczkiewicz-Zborska, *SN: Sprawa aktorki oskarżonej o zniesławienie Straży Granicznej do ponownego rozpoznania*, Prawo.pl, 6 XI 2024 r., https://www.prawo.pl/prawnicy-sady/sn-sprawa-aktorki-oskarzonej-o-znieslawienie-strazy-granicznej-do-ponownego-rozpoznania,529890.html [dostęp: 27 II 2026]; *Znany aktor Piotr Z. usłyszał zarzuty zniesławienia i znieważenia rzeczniczki Straży Granicznej*, Polska Agencja Prasowa, 31 III 2022 r., https://www.pap.pl/aktualnosci/news%2C1137489%2Cznany-aktor-piotr-z-uslyszal-zarzuty-znieslawienia-i-zniewazenia [dostęp: 27 II 2026].

ogólnopolskiej akcji pod hasłem „Murem za polskim mundurem", obejmującej różne inicjatywy.

Uchwały Sejmu RP i decyzja ministra obrony narodowej

Sejm RP podjął *Uchwałę z dnia 17 grudnia listopada 2021 r. o solidarności w sprawie ochrony polskich granic*. Wskazano w niej jednoznaczną odpowiedzialność białoruskiego reżimu za destabilizowanie granicy polsko-białoruskiej przez instrumentalizację migrantów. Sejm RP wyraził ponadto wdzięczność wszystkim podmiotom zaangażowanym w ochronę granicy państwowej. Szczególne słowa podziękowania skierowano do funkcjonariuszy SG, Policji i żołnierzy WP. Zgodnie z tekstem uchwały obowiązkiem każdego obywatela Polski jest (…) *wspieranie instytucji państwa i jego służb* oraz stanie (…) *ramię w ramię z funkcjonariuszami Straży Granicznej i Policji, żołnierzami Wojska Polskiego, w tym Wojsk Obrony Terytorialnej, i przedstawicielami innych służb dumnie noszącymi polski mundur i strzegącymi granic państwa oraz suwerenności naszej Ojczyzny*.

Kolejnym wyrazem wsparcia od Sejmu RP była *Uchwała z dnia 24 lipca 2024 r. w sprawie wyrażenia uznania służbie i poświęceniu żołnierzy i funkcjonariuszy strzegących bezpieczeństwa granic Rzeczypospolitej Polskiej*. Sejm ponownie potępił reżimy białoruski oraz rosyjski za działania hybrydowe na granicy polsko-białoruskiej. W uchwale silnie wybrzmiało uznanie dla służb mundurowych, ich ofiarności, oddania ojczyźnie, profesjonalizmu, odwagi oraz odporności na trudy. W uchwale podziękowano również za liczne oddolne akcje społeczne wspierające polskie służby mundurowe.

Jako wyraz wdzięczności żołnierzom za utrzymanie szczelności wschodniej granicy Polski minister obrony narodowej decyzją nr 148 z 17 października 2022 r. wprowadził znak specjalny „Za Ochronę Granicy Rzeczypospolitej Polskiej" jako formę (…) *uhonorowania żołnierzy Sił Zbrojnych Rzeczypospolitej Polskiej, pracowników resortu obrony narodowej, żołnierzy innych państw oraz innych osób, którzy przyczynili się do zapewnienia bezpieczeństwa i nienaruszalności granic Rzeczypospolitej Polskiej*[43]. Oznaczenie to ma trójstopniową hierarchię. Stopień I (złoty) jest nadawany za czyn bohaterski, stopień II (srebrny) za szczególne zasługi, a stopień III (brązowy) za wykonywanie zadań zapewniających bezpieczeństwo i nienaruszalność granicy państwa polskiego[44].

[43] *Decyzja nr 148/MON Ministra Obrony Narodowej z dnia 17 października 2022 r. w sprawie wprowadzenia znaku specjalnego „Za Ochronę Granicy Rzeczypospolitej Polskiej"*, załącznik nr 7: *Regulamin znaku specjalnego „Za Ochronę Granicy Rzeczypospolitej Polskiej"*.

[44] Tamże.

Ogólnopolska akcja społeczna „Murem za polskim mundurem"

Aby bronić dobrego imienia polskich żołnierzy i funkcjonariuszy, internauci zainicjowali działania pod hasłem „Murem za polskim mundurem", które przekształciły się w ogólnopolską akcję społeczną. Stała się ona symbolicznym gestem wsparcia dla polskich służb mundurowych strzegących granicy z Białorusią[45]. W akcję zaangażowali się zarówno polscy obywatele, jak i instytucje samorządowe, rządowe, organizacje pozarządowe, media oraz wiele innych podmiotów.

Jedną z najbardziej rozpoznawalnych inicjatyw była akcja „Kartka dla Obrońców Granic", zapoczątkowana przez Fundację Niepodległości[46]. Do uczestnictwa w niej zachęcano zwłaszcza dzieci i młodzież szkolną. Prace plastyczne miały zostać wykonane w postaci rysunku. Zakres tematyczny nie został ściśle określony. Nagrodami były pomoce dydaktyczne, m.in. w formie komiksu historycznego. Akcji partnerowały Kuratorium Oświaty w Lublinie, 2 Lubelska Brygada Obrony Terytorialnej oraz Radio Lublin[47]. W późniejszym okresie akcja uzyskała także wsparcie Oddziału Regionalnego Agencji Mienia Wojskowego w Lublinie, który dla autorów wybranych prac przygotował kieszonkowe apteczki pierwszej pomocy[48].

W akcję „Murem za polskim mundurem" zaangażowały się polskie władze, m.in. prezydent i premier. Okazali oni solidarność ze służbami mundurowymi broniącymi granicy polsko-białoruskiej, sprzeciwiając się jednocześnie wrogiej propagandzie reżimów białoruskiego i rosyjskiego. Prezydent Andrzej Duda w jednej ze swoich wypowiedzi zadeklarował: *Chylę głowę przed wszystkimi polskimi funkcjonariuszkami i funkcjonariuszami Straży Granicznej i innych służb, polskimi żołnierzami* (…) *za ten niezwykły wysiłek, ofiarność i oddanie sprawom Rzeczypospolitej* (…)[49]. Słowa o podobnej treści wypowiedział premier Mateusz Morawiecki podczas sejmowego wystąpienia na temat sytuacji na granicy polsko-

[45] *Murem za polskim mundurem*, Wojska Obrony Terytorialnej, 21 XI 2021 r., https://media.terytorialsi.wp.mil.pl/informacje/708475/murem-za-polskim-mundurem [dostęp: 3 VIII 2025].

[46] Fundacja Niepodległości z siedzibą w Lublinie zajmuje się przede wszystkim popularyzowaniem polskiej historii w kraju i za granicą. Ponadto prowadzi działania edukacyjne i naukowe w tym obszarze oraz ochrania dziedzictwo narodowe. Organizuje szkolenia, konferencje, debaty publiczne, wydaje czasopisma oraz opracowuje programy edukacyjne. Zob. *Statut fundacji „Fundacja Niepodległości"*, https://www.fundacja-niepodleglosci.pl/images/STATUT_FUNDACJI/Fundacja_Niepodleg%C5%82o%C5%9Bci_Statut_17.11.2021_r.pdf [dostęp: 29 VII 2025].

[47] *Kartka dla obrońców granic*, Fundacja Niepodległości, 10 XI 2021 r., https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2451-kartka-dla-obroncow-granic [dostęp: 30 VI 2025].

[48] *Kartka dla obrońców granic – nasza akcja się rozszerza*, Fundacja Niepodległości, 25 XI 2021 r., https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2456-kartka-dla-obroncow-granic-nasza-akcja-sie-rozszerza [dostęp: 30 VI 2025].

[49] *Murem za polskim mundurem!*, prezydent.pl, 13 X 2023 r., https://t.prezydent.pl/kancelaria/archiwum/andrzej-duda/multimedia/wideo/murem-za-polskim-mundurem,1148,3 [dostęp: 2 VII 2025].

-białoruskiej: (…) *jesteśmy winni podziękowanie za godną służbę, za obronę godności munduru polskiego żołnierza, polskiego funkcjonariusza, wszystkim wspaniałym funkcjonariuszom i funkcjonariuszkom, żołnierzom wojsk operacyjnych, żołnierzom Wojsk Obrony Terytorialnej*[50].

Hasło „Murem za polskim mundurem" wybrzmiało również w akcji przeprowadzonej przez Pocztę Polską (PP). W ramach tej akcji należało napisać list lub przygotować kartkę wyrażającą wsparcie dla polskich służb mundurowych. Wymogiem formalnym było umieszczenie w pracy hasła „Obrońcom granicy" i nieadresowanie jej. Uczestnik akcji mógł jednak wskazać konkretnego odbiorcę (osobę lub jednostkę)[51]. Ponadto PP wyemitowała specjalny znaczek pocztowy wraz z kopertą FDC, z wyrazami wdzięczności dla polskich służb mundurowych za ochronę wschodniej granicy państwa. Oba produkty opatrzono napisem „#♥ZaPolskimMundurem"[52].

Narodowy Bank Polski (NBP) wyemitował srebrną monetę kolekcjonerską „Ochrona polskiej granicy wschodniej" o wartości nominalnej 10 zł. Awers monety ukazuje polski słup graniczny, kamuflaż wojskowy oraz tereny leśne, a rewers – sylwetki funkcjonariuszy SG, Policji oraz żołnierza WP. Nad postaciami umieszczono śmigłowiec. Funkcjonariusz Policji jest przedstawiony w kasku i z tarczą ochronną, żołnierz z bronią długą. W tle widnieją kontury polskiej granicy z wyraźnym zaznaczeniem granicy polsko-białoruskiej[53]. Kilka miesięcy po ukazaniu się srebrnej monety NBP wyemitował banknot kolekcjonerski „Ochrona polskiej granicy wschodniej" o wartości nominalnej 20 zł. Zastosowano w nim podobny układ graficzny jak na monecie kolekcjonerskiej[54].

Obchody rocznicy odzyskania przez Polskę niepodległości, zorganizowane pod hasłem „Dzień szacunku dla munduru", miały w 2021 r. szczególny wymiar.

---

[50] *Wypowiedź premiera Mateusza Morawieckiego w Sejmie nt. sytuacji na granicy polsko-białoruskiej*, https://www.gov.pl/attachment/f93dffbc-f0ea-48c5-990b-7c01608b2213 [dostęp: 2 VII 2025].

[51] *Jesteśmy z Wami – wyślij kartkę mundurowym na granicy*, Poczta Polska, 11 XI 2021 r., https://media.poczta-polska.pl/releases/jestesmy-z-wami-wyslij-kartke-mundurowym-na-granicy#:~:text=Poczta%20Polska%20bezp%C5%82atnie%20przeka%C5%BCe%20takie%20kartki%20s%C5%82u%C5%BCbom,dor%C4%99czane.%20LISTA%20plac%C3%B3wek%20ze%20specjalnymi%20pojemnikami:%20Lp. [dostęp: 30 VI 2025].

[52] *Poczta Polska ze specjalną emisją „#♥ZaPolskimMundurem" poświęconą obrońcom wschodniej granicy*, Poczta Polska, 27 I 2022 r., https://www.poczta-polska.pl/news/poczta-polska-ze-specjalna-emisja-%E2%99%A5zapolskimmundurem-poswiecona-obroncom-wschodniej-granicy/ [dostęp: 1 VII 2025].

[53] *„Ochrona polskiej granicy wschodniej" na srebrnej monecie NBP*, Narodowy Bank Polski, 26 I 2022 r., https://nbp.pl/ochrona-polskiej-granicy-wschodniej-na-srebrnej-monecie-nbp/ [dostęp: 1 VII 2025].

[54] *NBP wprowadza banknot kolekcjonerski „Ochrona polskiej granicy wschodniej"*, Narodowy Bank Polski, 18 VII 2022 r., https://nbp.pl/nbp-wprowadza-banknot-kolekcjonerski-ochrona-polskiej-granicy-wschodniej/ [dostęp: 1 VII 2025].

W 103 jednostkach wojskowych (w związku ze 103. rocznicą odzyskania przez Polskę niepodległości) przeprowadzono prezentacje na temat symboliki munduru. Ponadto dzień przed centralnymi obchodami Święta Niepodległości w Sejmie RP otwarto wystawę „Mundury polskich żołnierzy – szacunek dla munduru"[55].

Na oficjalnej stronie internetowej SG zaprezentowano także stanowiska instytucji i organizacji społecznych, w tym Stowarzyszenia Weteranów Polskich Formacji Granicznych, Rady Miejskiej w Lublińcu, Rady Gminy Spytkowice, Rady Gminy Lubomino, Stowarzyszenia Osób Represjonowanych w Stanie Wojennym oraz Ruchu Kultury Chrześcijańskiej „Odrodzenie", będące wyrazami wdzięczności za służbę na granicy polsko-białoruskiej[56].

Żołnierzom na granicy towarzyszyli kapelani wojskowi, którzy poza posługą sakramentalną służyli wsparciem psychologicznym. Jak wskazał ks. ppor. Artur Janczarek (kapelan 15 Gołdapskiego Pułku Przeciwlotniczego), żołnierze są narażeni na nieustanną agresję ze strony białoruskich służb, co wpływa na ich stan fizyczny oraz psychiczny[57]. Duchowe wsparcie przekazał im Przewodniczący Konferencji Episkopatu Polski abp Stanisław Gądecki w komunikacie dotyczącym eskalacji napięć na granicy polsko-białoruskiej[58]. Z kolei za sprawą Prawosławnego Ordynariatu Wojska Polskiego przy współpracy z Prawosławnym Metropolitalnym Ośrodkiem Miłosierdzia ELEOS do placówek SG dostarczano środki pierwszej potrzeby[59].

W okresie świąt Bożego Narodzenia 2021 r. były podejmowane liczne inicjatywy ze strony instytucji i organów państwowych, aby podziękować służbom mundurowym za ich trud włożony w utrzymanie bezpieczeństwa i porządku publicznego.

---

[55] *Narodowe Święto Niepodległości – „Dzień szacunku dla munduru"*, Wojsko Polskie, https://www.wojsko-polskie.pl/weterani/articles/aktualnosci-r/narodowe-swieto-niepodleglosci-dzien-szacunku-dla-munduru/ [dostęp: 3 VII 2025].

[56] *#MuremZaPolskimMundurem – stanowiska instytucji i organizacji*, Straż Graniczna, 3 XII 2021 r., https://strazgraniczna.pl/pl/pozostale-informacje/muremzapolskimmundurem/muremzapolskimmundurem/9548,MuremZaPolskimMundurem-stanowiska-instytucji-i-organizacji.html [dostęp: 3 VII 2025].

[57] K. Stępkowski, *Ks. ppor. Artur Janczarek: nasza posługa na granicy to realizacja przysięgi wojskowej*, Ordynariat Polowy, 18 XI 2021 r., https://archiwum2023-ordynariat.wp.mil.pl/pl/articles/wiadomosci-listopad-2021/ks-ppor-artur-janczarek-nasza-posluga-na-granicy-realizacja-przysiegi-wojskowej/index.html [dostęp: 19 VIII 2025].

[58] M. Pietraszczyk, *Komunikat Przewodniczącego Konferencji Episkopatu Polski wobec eskalacji napięć na granicy polsko-białoruskiej*, Straż Graniczna, 11 XI 2021 r., https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/rzymskokatolickie/9542,Komunikat-Przewodniczacego-Konferencji-Episkopatu-Polski-wobec-eskalacji-napiec-.html [dostęp: 3 VII 2025].

[59] *Duchowe wsparcie na granicy*, Straż Graniczna, 26 XI 2021 r., https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/prawoslawne/9573,Duchowe-wsparcie-na-granicy.html [dostęp: 3 VII 2025].

Z myślą o żołnierzach i funkcjonariuszach, którzy w okresie świąt pozostają z dala od swoich rodzin, została zorganizowana akcja „#WolneMiejsceDlaMunduru". Formą zaangażowania w nią miało być pozostawienie podczas wieczerzy wigilijnej winietki przy wolnym talerzu[60].

Aktywnością wykazały się również społeczności lokalne. Na przykład, z inicjatywy senator RP Marii Koc oraz starosty powiatu garwolińskiego Mirosława Walickiego przeprowadzono zbiórkę słodyczy dla służb mundurowych. W akcję zaangażowały się m.in. firmy, koła gospodyń wiejskich oraz ochotnicze straże pożarne (OSP)[61]. Hasło „Murem za polskim mundurem" utrwalono w formie muralu na ścianie remizy OSP w Kochcicach. Przedstawia on sylwetki funkcjonariuszy SG, OSP, Policji oraz żołnierza WP[62].

Podsumowanie

Kryzys migracyjny na granicy polsko-białoruskiej pokazał, jak niebezpieczny i problematyczny jest proceder instrumentalizacji migrantów. Człowiek został wykorzystany jako środek walki, w tym jako broń psychologiczna[63]. Zgodnie z wytycznymi białoruskich służb migranci przeprowadzali liczne szturmy z użyciem niebezpiecznych narzędzi. Celami ataku stały się granica i służby mundurowe państwa[64]. Negatywny wpływ na polskie społeczeństwo wywarły propaganda i dezinformacja. Białoruskie ośrodki medialne, przy wsparciu ze strony Rosji, przedstawiały zniekształcony obraz rzeczywistości, zgodny z celami politycznymi tych reżimów. Polskie służby mundurowe reagujące na sztucznie wywołane zjawisko masowej migracji były oskarżane o wyjątkową brutalność i nieludzkie traktowanie migrantów. Taką narrację podtrzymywały także niektóre środowiska w Polsce. Skutkiem tych działań była narastająca polaryzacja polskiego społeczeństwa[65].

---

[60] Ł. Wilczewski, *W tę wigilię zostawmy #WolneMiejsceDlaMunduru*, Wojsko Polskie, https://www.wojsko-polskie.pl/1bot/articles/aktualnosci-w/w-te-wigilie-zostawmy-wolnemiejscedlamunduru/ [dostęp: 19 VIII 2025].

[61] *Powiat Garwoliński wspiera służby mundurowe!*, Starostwo Powiatowe w Garwolinie, https://samorzad.gov.pl/web/powiat-garwolin/zbiorka-slodyczy [dostęp: 3 VII 2025].

[62] P. Ciastek, *Na remizie OSP Kochcice powstał mural z przesłaniem. Są na nim polskie służby mundurowe*, Lubliniec Nasze Miasto, 25 IX 2023 r., https://lubliniec.naszemiasto.pl/na-remizie-osp-kochcice-powstal-mural-z-przeslaniem-sa-na/ar/c1-9464993 [dostęp: 3 VII 2025].

[63] K. Chochowski, *Kryzys na granicy polsko-białoruskiej*…, s. 96.

[64] M. Pieczyński, *Granica propagandy. Łukaszenka i Putin na wojnie hybrydowej z Polską*, Warszawa 2022, s. 10.

[65] K. Orzech, *Zagrożenia dla Polski*…, s. 62–64.

Jednym z wyrazów sprzeciwu wobec tych wydarzeń była ogólnopolska akcja społeczna „Murem za polskim mundurem". Do funkcjonariuszy i żołnierzy spływały słowa wsparcia ze strony przedstawicieli organów państwowych i członków społeczeństwa, kartki wykonane przez dzieci i młodzież, środki pierwszej potrzeby oraz wiele innych. Te działania pokazały, że polskie służby mundurowe mogą liczyć na poparcie rodaków.

Niniejsza publikacja została sfinansowana ze środków Wydziału Studiów Międzynarodowych i Politycznych w ramach Programu Strategicznego Inicjatywa Doskonałości w Uniwersytecie Jagiellońskim.

Bibliografia

Baziur G., *Operation „Sluice". The so-called migration crisis at the Polish-Belarussian border: an example of hybrid actions taken in the second half of 2021 as documented in the reports of the Polish border guard*, „Bezpieczeństwo. Teoria i Praktyka" 2022, t. 46, nr 1, s. 133–150. http://dx.doi.org/10.48269/2451-0718-btip-2022-1-008.

Chochowski K., *Kryzys na granicy polsko-białoruskiej jako przejaw wojny hybrydowej. Aspekty administracyjnoprawne*, „Roczniki Nauk Społecznych" 2021, t. 49, nr 4, s. 81–99. https://doi.org/10.18290/rns21494.8.

Czarnota K., Górczyńska M., *Gdzie prawo nie sięga. Raport Helsińskiej Fundacji Praw Człowieka z monitoringu sytuacji na polsko-białoruskiej granicy*, Helsińska Fundacja Praw Człowieka, Warszawa 2022.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red. nauk.), Warszawa 2011, s. 9–17.

Kuśmirek K., *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*, „Bezpieczeństwo. Teoria i Praktyka" 2022, t. 48, nr 3, s. 311–321. http://dx.doi.org/10.48269/2451-0718-btip-2022-3-023.

Maciejewski J., *Wewnętrzny front. Łukaszenki wojna informacyjna i kryzys migracyjny na granicy polsko-białoruskiej*, Warszawa 2022.

Moczuk E., Czekaj D., *Kryzys migracyjny jako element wojny hybrydowej. Analiza działania wojska na granicy polsko-białoruskiej*, Rzeszów 2024.

Niedźwiedzki D., *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego*, „Politeja" 2024, t. 21, nr 1, s. 57–74. https://doi.org/10.12797/Politeja.20.2024.88.1.01.

Nowakowski J.M., *O co idzie gra?*, w: *Raport IV. Granica dyktatora. Polska i Białoruś wobec kryzysu granicznego*, J.M. Nowakowski, J. Olędzka, M. Rust (red.), Warszawa 2021, s. 73–81.

Ociepka B., *Dziennikarzom wstęp wzbroniony: kryzys na polsko-białoruskiej granicy w 2021 r. jako wydarzenie (nie)relacjonowane przez media*, „Studia Medioznawcze" 2023, t. 24, nr 2, s. 190–203. https://doi.org/10.33077/uw.24511617.sm.2023.2.715.

Orzech K., *Zagrożenia dla Polski kreowane przez Republikę Białorusi w kontekście sytuacji kryzysowej na granicy polsko-białoruskiej*, „Studia Bezpieczeństwa Narodowego" 2021, t. 22, nr 4, s. 55–68. https://doi.org/10.37055/sbn/147013.

Pieczyński M., *Granica propagandy. Łukaszenka i Putin na wojnie hybrydowej z Polską*, Warszawa 2022.

Szabaciuk A., *Forced migrations in Eastern Europe after 2020*, seria: Prace Instytutu Europy Środkowej, nr 9, B. Surmacz, T. Stępniewski (red.), Lublin 2022.

Szabaciuk A., *„Natowskie wojska szczękające gąsienicami czołgów". Polska i granica polsko-białoruska w propagandzie białoruskiej po 2020 roku*, w: *Bezpieczeństwo granic – granice bezpieczeństwa*, D. Karczewski, R. Zenderowski (red.), Warszawa 2023, s. 331–364.

Szachoń-Pszenny A., Zaręba A., *Etapowość instrumentalizacji migrantów na przykładzie granicy z Białorusią – wyzwania współczesności,* „Przegląd Geopolityczny" 2024, t. 49, s. 49–68.

Szachoń-Pszenny A., Zaręba A., *Instrumentalizacja migrantów jako forma destabilizacji bezpieczeństwa na wschodniej granicy zewnętrznej UE w kontekście wojny w Ukrainie*, „Politeja" 2024, t. 21, nr 1, s. 89–104. https://doi.org/10.12797/Politeja.20.2024.88.1.01.

Szyszka J., *Zjawisko state-sponsored human trafficking na przykładzie Białorusi*, w: *Wybrane zagadnienia handlu ludźmi i zagrożonymi gatunkami roślin i zwierząt*, B. Stępień-Załucka, J. Uliasz (red. nauk.), Rzeszów 2023, s. 118–133. http://dx.doi.org/10.15584/978-83-8277-037-7.9.

Śliwa Z., Olech A.K., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, „Wiedza Obronna" 2022, t. 278, nr 1, s. 87–105. https://doi.org/10.34752/2022-d278.

Wańczyk K., *Relacje Unii Europejskiej z Białorusią po sierpniu 2020 roku. Powrót do przeszłości*, w: *Raport V. Białoruś 500 dni po: od społecznej mobilizacji do neototalitarnej konsolidacji?*, J.M. Nowakowski, J. Olędzka, M. Rust (red.), Warszawa 2022, s. 87–109.

Wawrzusiszyn A., *Rosyjsko-białoruskie działania hybrydowe na granicach Unii Europejskiej i NATO*, „Journal of Modern Science" 2025, t. 61, nr 1, s. 10–32. https://doi.org/10.13166/jms/203108.

Werner J., *Ochrona granicy wschodniej Rzeczypospolitej Polskiej w kontekście nielegalnej migracji*, „Studia Bezpieczeństwa Narodowego" 2024, t. 31, nr 1, s. 83–106. https://doi.org/10.37055/sbn/178377.

Wojnowski M., *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 11–49. https://doi.org/10.4467/20801335PBW.21.034.15694.

Zakończenie operacji policyjnej „Zapora", „Gazeta Policyjna" 2025, nr 49, s. 24–25.

Źródła internetowe

3 miesiące operacji #SilneWsparcie, Wojska Obrony Terytorialnej, 3 XII 2021 r., https://media.terytorialsi.wp.mil.pl/informacje/712389/3-miesiace-operacji-silnewsparcie [dostęp: 6 IV 2025].

Ciastek P., *Na remizie OSP Kochcice powstał mural z przesłaniem. Są na nim polskie służby mundurowe*, Lubliniec Nasze Miasto, 25 IX 2023 r., https://lubliniec.naszemiasto.pl/na-remizie-osp-kochcice-powstal-mural-z-przeslaniem-sa-na/ar/c1-9464993 [dostęp: 3 VII 2025].

Duchowe wsparcie na granicy, Straż Graniczna, 26 XI 2021 r., https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/prawoslawne/9573,Duchowe-wsparcie-na-granicy.html [dostęp: 3 VII 2025].

Dziemiańczuk J., *„Bezpieczne Podlasie" zastąpi dwie dotychczasowe operacje*, Wojska Obrony Terytorialnej, 31 VII 2024 r., https://media.terytorialsi.wp.mil.pl/informacje/838336/bezpieczne-podlasie-zastapi-dwie-dotychczasowe-operacje [dostęp: 6 IV 2025].

Fraszka B., *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, Warsaw Institute, 23 XII 2021 r., https://warsawinstitute.org/pl/sytuacja-na-granicy-polsko-bialoruskiej-przyczyny-aspekt-geopolityczny-narracje/ [dostęp: 14 II 2026].

Jesteśmy z Wami – wyślij kartkę mundurowym na granicy, Poczta Polska, 11 XI 2021 r., https://media.poczta-polska.pl/releases/jestesmy-z-wami-wyslij-kartke-mundurowym-na-granicy#:~:text=Poczta%20Polska%20bezp%C5%82atnie%20przeka%C5%BCe%20takie%20kartki%20s%C5%82u%C5%BCbom,dor%C4%99czane.%20LISTA%20plac%C3%B3wek%20ze%20specjalnymi%20pojemnikami:%20Lp. [dostęp: 30 VI 2025].

Jurkowska M., *Masowy szturm na przejście graniczne w Kuźnicy. Mija rok od ataku cudzoziemców na granicę i funkcjonariuszy SG*, Sokółka Nasze Miasto, 16 XI 2022 r., https://sokolka.naszemiasto.pl/masowy-szturm-na-przejscie-graniczne-w-kuznicy-mija-rok-od/ar/c1-9090195 [dostęp: 11 IV 2025].

Kartka dla obrońców granic, Fundacja Niepodległości, 10 XI 2021 r., https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2451-kartka-dla-obroncow-granic [dostęp: 30 VI 2025].

Kartka dla obrońców granic – nasza akcja się rozszerza, Fundacja Niepodległości, 25 XI 2021 r., https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2456-kartka-dla-obroncow-granic-nasza-akcja-sie-rozszerza [dostęp: 30 VI 2025].

Korsak E., *Nowa operacja wojskowa na Podlasiu*, Polska Zbrojna, 12 VIII 2023 r., https://polska-zbrojna.pl/home/articleshow/40146?t=Nowa-operacja-wojskowa-na-Podlasiu [dostęp: 7 IV 2025].

Kożdoń-Dębecka M., *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych*, „Media Biznes Kultura" 2023, t. 14, nr 1, s. 161–174. https://doi.org/10.4467/25442554.MBK.23.010.18033.

Łozowski M., *Państwowa Straż Pożarna w obronie granic RP*, Krajowa Sekcja Pożarnictwa, 7 XII 2021 r., https://kspnszz.org/index.php/2021/12/07/panstwowa-straz-pozarna-w-obronie-granic-rp/ [dostęp: 8 IV 2025].

Modernizacja bariery elektronicznej na granicy Polski z Białorusią (WIDEO), Telbud S.A., https://telbud.pl/strefa-informacji/modernizacja-bariery-elektronicznej-na-granicy-polski-z-bialorusia-wideo [dostęp: 14 II 2026].

Murem za polskim mundurem!, prezydent.pl, 13 X 2023 r., https://www.prezydent.pl/multimedia/wideo/murem-za-polskim-mundurem,1148,33 [dostęp: 2 VII 2025].

#MuremZaPolskimMundurem – stanowiska instytucji i organizacji, Straż Graniczna, 3 XII 2021 r., https://strazgraniczna.pl/pl/pozostale-informacje/muremzapolskimmundurem/muremzapolskimmundurem/9548,MuremZaPolskimMundurem-stanowiska-instytucji-i-organizacji. html [dostęp: 3 VII 2025].

Murem za polskim mundurem, Wojska Obrony Terytorialnej, 21 XI 2021 r., https://media.terytorialsi.wp.mil.pl/informacje/708475/murem-za-polskim-mundurem [dostęp: 3 VIII 2025].

Narodowe Święto Niepodległości – „Dzień szacunku dla munduru", Wojsko Polskie, https://www.wojsko-polskie.pl/weterani/articles/aktualnosci-r/narodowe-swieto-niepodleglosci-dzien-szacunku-dla-munduru/ [dostęp: 3 VII 2025].

NBP wprowadza banknot kolekcjonerski „Ochrona polskiej granicy wschodniej”, Narodowy Bank Polski, 18 VII 2022 r., https://nbp.pl/nbp-wprowadza-banknot-kolekcjonerski-ochrona-polskiej-granicy-wschodniej/ [dostęp: 1 VII 2025].

Nowa operacja wojskowa na wschodniej granicy: OP Bezpieczne Podlasie, Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-07-176-op-bezpieczne-podlasie/ [dostęp: 7 IV 2025].

„Ochrona polskiej granicy wschodniej” na srebrnej monecie NBP, Narodowy Bank Polski, 26 I 2022 r., https://nbp.pl/ochrona-polskiej-granicy-wschodniej-na-srebrnej-monecie-nbp/ [dostęp: 1 VII 2025].

Organizatorzy nielegalnego przerzutu migrantów do Polski objęci zachodnimi sankcjami, InfoSecurity24, 27 I 2022 r., https://infosecurity24.pl/za-granica/organizatorzy-nielegalnego-przerzutu-migrantow-do-polski-objeci-zachodnimi-sankcjami [dostęp: 4 VII 2025].

Pietraszczyk M., *Komunikat Przewodniczącego Konferencji Episkopatu Polski wobec eskalacji napięć na granicy polsko-białoruskiej*, Straż Graniczna, 11 XI 2021 r., https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/rzymskokatolickie/9542,Komunikat-Przewodniczacego-Konferencji-Episkopatu-Polski-wobec-eskalacji-napiec-.html [dostęp: 3 VII 2025].

Poczta Polska ze specjalną emisją „#♥ZaPolskimMundurem” poświęconą obrońcom wschodniej granicy, Poczta Polska, 27 I 2022 r., https://www.poczta-polska.pl/news/poczta-polska-ze-specjalna-emisja-%E2%99%A5zapolskimmundurem-poswiecona-obroncom-wschodniej-granicy/ [dostęp: 1 VII 2025].

Powiat Garwoliński wspiera służby mundurowe!, Starostwo Powiatowe w Garwolinie, https://samorzad.gov.pl/web/powiat-garwolin/zbiorka-slodyczy [dostęp: 3 VII 2025].

Rojek-Socha P., Żaczkiewicz-Zborska K., *SN: Sprawa aktorki oskarżonej o zniesławienie Straży Granicznej do ponownego rozpoznania*, Prawo.pl, 6 XI 2024 r., https://www.prawo.pl/prawnicy-sady/sn-sprawa-aktorki-oskarzonej-o-znieslawienie-strazy-granicznej-do-ponownego-rozpoznania,529890.html [dostęp: 27 II 2026].

Statut fundacji „Fundacja Niepodległości”, https://www.fundacja-niepodleglosci.pl/images/STATUT_FUNDACJI/Fundacja_Niepodleg%C5%82o%C5%9Bci_Statut_17.11.2021_r.pdf [dostęp: 29 VII 2025].

Stępkowski K., *Ks. ppor. Artur Janczarek: nasza posługa na granicy to realizacja przysięgi wojskowej*, Ordynariat Polowy, 18 XI 2021 r., https://archiwum2023-ordynariat.wp.mil.pl/pl/articles/wiadomosci-listopad-2021/ks-ppor-artur-janczarek-nasza-posluga-na-granicy-realizacja-przysiegi-wojskowej/index.html [dostęp: 19 VIII 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią w 2021 r.*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021r.html [dostęp: 1 IV 2025].

Szef BBN na granicy polsko-białoruskiej. Wzmacnianie zabezpieczeń to „dowód ciągłości myśli strategicznej państwa", Biuro Bezpieczeństwa Narodowego, 11 X 2024 r., https://www.bbn.gov.pl/pl/wydarzenia/10003,Szef-BBN-na-granicy-polsko-bialoruskiej-Wzmacnianie-zabezpieczen-to-quotdowod-ci.html [dostęp: 5 IV 2025].

Szwed K., *Zakończenie odbioru bariery elektronicznej na granicy polsko-białoruskiej*, Straż Graniczna, 15 VI 2023 r., https://www.strazgraniczna.pl/pl/aktualnosci/11875,Zakonczenie-odbioru-bariery-elektronicznej-na-granicy-polsko-bialoruskiej.html [dostęp: 5 IV 2025].

Wilczewski Ł., *W tę wigilię zostawmy #WolneMiejsceDlaMunduru*, Wojsko Polskie, https://www.wojsko-polskie.pl/1bot/articles/aktualnosci-w/w-te-wigilie-zostawmywolnemiejscedlamundru/ [dostęp: 19 VIII 2025].

Wypowiedź premiera Mateusza Morawieckiego w Sejmie nt. sytuacji na granicy polsko-białoruskiej, https://www.gov.pl/attachment/f93dffbc-f0ea-48c5-990b-7c01608b2213 [dostęp: 2 VII 2025].

Znany aktor Piotr Z. usłyszał zarzuty zniesławienia i znieważenia rzeczniczki Straży Granicznej, Polska Agencja Prasowa, 31 III 2022 r., https://www.pap.pl/aktualnosci/news%2C1137489%2Cznany-aktor-piotr-z-uslyszal-zarzuty-znieslawienia-i-zniewazenia [dostęp: 27 II 2026].

Akty prawne

Ustawa z dnia 29 października 2021 r. o budowie zabezpieczenia granicy państwowej (t.j. DzU z 2023 r. poz. 1390).

Inne dokumenty

Decyzja nr 148/MON Ministra Obrony Narodowej z dnia 17 października 2022 r. w sprawie wprowadzenia znaku specjalnego „Za Ochronę Granicy Rzeczypospolitej Polskiej", załącznik nr 7: *Regulamin znaku specjalnego „Za Ochronę Granicy Rzeczypospolitej Polskiej"* (Dz. Urz. MON z 2022 r. poz. 173).

Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 24 lipca 2024 r. w sprawie wyrażenia uznania służbie i poświęceniu żołnierzy i funkcjonariuszy strzegących bezpieczeństwa granic Rzeczypospolitej Polskiej (M.P. z 2024 r. poz. 737).

Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 17 listopada 2021 r. o solidarności w sprawie ochrony polskich granic (M.P. z 2021 r. poz. 1129).

Norbert Łucarz

Ukończył z wyróżnieniem studia I stopnia na kierunku bezpieczeństwo narodowe na Wydziale Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego. Obecnie uczęszcza na studia II stopnia na kierunku bezpieczeństwo narodowe na Uniwersytecie Jagiellońskim. Laureat konkursu „Granty dla przyszłości" dla wybitnych studentów Wydziału Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego – wsparcie mobilności (IV edycja). Członek zespołu reprezentacyjnego Uniwersytetu Jagiellońskiego na V edycji International Forum for Peace, Security and Prosperity. Interesuje się zagadnieniami związanymi z zagrożeniami hybrydowymi, edukacją dla bezpieczeństwa, terroryzmem.

Kontakt: norbert.lucarz@student.uj.edu.pl

ARTYKUŁY RECENZYJNE / RECENZJE

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 197–201

https://doi.org/10.4467/20801335PBW.26.009.23371

RECENZJA

Szpiegostwo. Studium kryminologiczne, Piotr Chlebowicz[1]

TOMASZ SAFJAŃSKI

Centrum Badań nad Bezpieczeństwem Transgranicznym,
Akademia WSB w Dąbrowie Górniczej

https://orcid.org/0000-0003-1775-8857

Przegląd literatury dotyczącej szpiegostwa wskazuje, że to zagrożenie stosunkowo rzadko było przedmiotem badań empirycznych. W krajowej i zagranicznej literaturze naukowej dominują prace teoretyczne odnoszące się do historycznych, politologicznych i prawnych aspektów tego zjawiska. Monografia autorstwa Piotra Chlebowicza pt. *Szpiegostwo. Studium kryminologiczne* stanowi pod tym względem opracowanie pionierskie, a jej ukazanie się ma wyjątkowe znaczenie dla rozwoju badań kryminologicznych nad przestępczością przeciwko bezpieczeństwu państwa. Autor – jako pierwszy badacz w Polsce – podjął się całościowej, systematycznej i opartej na źródłach empirycznych analizy kryminologicznej zjawiska szpiegostwa w Polsce w latach 1990–2022. Wypełnił tym samym istotną lukę badawczą.

[1] P. Chlebowicz, *Szpiegostwo. Studium kryminologiczne*, seria: Monografie Prawnicze, Warszawa 2025, C.H. Beck, 227 s.

Temat poruszony przez Chlebowicza ma kluczowe znaczenie dla bezpieczeństwa państwa. Ekspansywna polityka Federacji Rosyjskiej, ukierunkowana na rekonstrukcję stref wpływów z okresu sowieckiego, jest zagrożeniem polskiej racji stanu. W tym kontekście działalność szpiegowska prowadzona przez rosyjskie i białoruskie służby specjalne może być postrzegana jako instrument wojny hybrydowej oraz element potencjalnych przygotowań do konfliktu zbrojnego. Wraz z intensyfikacją działań szpiegowskich o rosyjskiej proweniencji obserwuje się ich ewolucję jakościową. Polega ona na poszerzaniu repertuaru stosowanych metod oraz na rekrutacji osób przypadkowych, w tym przestępców działających w ramach zasady *espionage as a service*. Szpiegostwo poprzedza i wspiera operacje wpływu noszące znamiona dywersji i sabotażu. Operacje te, obejmujące zarówno działania dezinformacyjne, jak i oddziaływanie na opinię publiczną, procesy decyzyjne oraz struktury polityczne państw Zachodu, nabierają coraz większego znaczenia. Równolegle są rozwijane zdolności w zakresie cyberszpiegostwa, których celem jest penetracja systemów teleinformatycznych, pozyskiwanie danych wrażliwych oraz zakłócanie funkcjonowania infrastruktury krytycznej państwa. Skala i charakter działań prowadzonych przez rosyjskie i białoruskie służby specjalne wymagają pogłębionych badań i analiz oraz adekwatnej reakcji ze strony instytucji w Polsce odpowiedzialnych za bezpieczeństwo.

Recenzowana publikacja jest podsumowaniem trwających ponad dziesięć lat badań autora dotyczących szpiegostwa, opartych na badaniach aktowych, archiwalnych, wywiadach swobodnych i literaturze przedmiotu. Autor uzyskał dostęp do akt operacyjnych i sądowych w sprawach o szpiegostwo znajdujących się w zasobach archiwalnych Instytutu Pamięci Narodowej oraz sądów powszechnych i wojskowych. Starannie przeanalizował te dokumenty i zrekonstruował przypadki działalności szpiegowskiej przeciwko Polsce, co stanowi ważny wkład w rozwój badań nad infiltracją szpiegowską oraz funkcjonowaniem służb specjalnych. Triangulacja źródeł – wyjątkowo trudna w badaniach obejmujących w dużej mierze treści niejawne – nadaje pracy wysoki poziom rzetelności naukowej oraz pozwala na wieloaspektową rekonstrukcję mechanizmów działania obcych służb wywiadowczych i identyfikację wzorców taktyk szpiegowskich.

Założenia metodologiczne przyjęte przez autora integrują trzy perspektywy: kryminologiczną, kryminalistyczną oraz nauk o bezpieczeństwie, co pozwala na ujęcie szpiegostwa jako zjawiska wielowymiarowego. Jednocześnie tekst pozostaje uporządkowany i przejrzysty. Zasługuje to na podkreślenie, gdyż przy tak złożonej tematyce łatwo popaść w chaos informacyjny.

Zawarte w monografii analizy przypadków białoruskiego, rosyjskiego i niemieckiego szpiegostwa, zjawiska oferentów, czyli osób samodzielnie zgłaszających gotowość współpracy z obcym wywiadem, oraz procesu kształtowania agenta

wpływu przyczyniają się do rozwinięcia istniejących koncepcji teoretycznych. Autor zgłębia zarówno proces werbunku, jak i działania operacyjne, sposób komunikacji, strukturę prowadzenia agentury oraz stosowane zabezpieczenia. Prace o podobnym poziomie szczegółowości są rzadkie nawet w literaturze anglosaskiej. Chlebowicz analizuje również modus operandi sprawców szpiegostwa, ciemną liczbę tego zjawiska oraz obszary zainteresowania obcych służb wywiadowczych. Celnie identyfikuje zmiany jakościowe w działaniach służb FR i Białorusi po 2014 r. Omawia także instrumenty prawne w zakresie zwalczania szpiegostwa, uwzględniając zagrożenia wywiadowcze, które pojawiły się po aneksji Krymu przez FR.

Struktura monografii odpowiada logice klasycznego wywodu naukowego. Autor prowadzi czytelnika od fundamentów teoretycznych ku analizie empirycznej i praktycznym wnioskom. Książka otwiera się rozdziałem, w którym szpiegostwo jest ujęte jako kategoria kryminologiczna. Chlebowicz wskazuje problemy definicyjne oraz wielowarstwowy charakter tego zjawiska, zwłaszcza jego związki z przestępczością polityczną. Zwraca uwagę na funkcje wywiadu, które wykraczają poza klasyczne gromadzenie danych i obejmują wpływanie na procesy polityczne czy destabilizację państw. Zabieg ten pozwala osadzić dalsze rozważania w szerszym kontekście politycznym oraz pokazać, dlaczego tradycyjne podejścia kryminologiczne są niewystarczające w analizie szpiegostwa.

W rozdziale drugim zostaje omówiona metodologia badań kryminologicznych dotyczących szpiegostwa, a także stan badań w Polsce.

Najobszerniejszy jest rozdział trzeci poświęcony złożonym przyczynom szpiegostwa, zawierający wielowymiarową analizę czynników sprzyjających takiej działalności. Chlebowicz operuje zarówno perspektywą makrostrukturalną, odwołując się do geopolityki i zmian po 2014 r., jak i mikrostrukturalną, w ramach której analizuje motywacje sprawców, ich uwarunkowania psychologiczne oraz indywidualne ścieżki życiowe. Szczególnie wartościowe jest wykorzystanie wyników projektu „Slammer", dotyczącego psychologii zdrady, oraz studium oferentów. Takie podejście wykracza poza klasyczne schematy badań nad szpiegostwem, gdyż uwzględnia rzadko opisywane wewnętrzne dynamiki i modele zachowań sprawców.

W kolejnym rozdziale autor przechodzi do fenomenologii szpiegostwa, przy czym koncentruje się na konkretnych przejawach omawianego zjawiska. Problematyka ciemnej liczby oraz trudności statystyczne związane z opisem przestępstwa zostały przedstawione z zachowaniem wymogów precyzji metodologicznej, co stanowi istotną wartość naukową. Analiza najczęściej występujących obszarów zainteresowania obcych służb, motywacji sprawców oraz stosowanych przez nich technik działania ukazuje praktyczny wymiar ustaleń teoretycznych opisanych we wcześniejszych rozdziałach. Na uwagę zasługuje również włączenie zagadnienia pogranicza lobbingu i działalności wywiadowczej, zobrazowane na przykładzie sprawy

Mateusza Piskorskiego. Pokazuje to trudności, jakie organy państwa napotykają przy rozróżnianiu legalnych działań politycznych i aktywności wywiadowczej.

Rozdział piąty obejmuje studia przypadków – szczegółowe analizy spraw Olgi Sołomenik, Marka Zielińskiego, Ryszarda Tomaszka i Piotra Hoffmanna. Autor rekonstruuje modus operandi sprawców, okoliczności werbunku oraz działania kontrwywiadu, a także wskazuje zależności między poszczególnymi etapami ich aktywności. Materiał aktowy został zaprezentowany w sposób uporządkowany, z wyraźnym oddzieleniem faktów od interpretacji. Rozdział ten stanowi najważniejszy wkład empiryczny, gdyż ukazuje mechanizmy działania sprawców i służb w sposób niedostępny dla opracowań teoretycznych.

Rozdział szósty dotyczy instrumentów zwalczania szpiegostwa i w sposób przekrojowy obejmuje aspekty prawne, operacyjne oraz polityczne. Chlebowicz opisuje w nim właściwości poszczególnych instytucji państwowych, regulacje prawa karnego, obowiązek denuncjacji oraz rolę prawa administracyjnego. Szczególnie istotne jest omówienie działań operacyjno-rozpoznawczych, w tym instytucji tzw. szpiega koronnego oraz procedur analitycznych. Interesującym wątkiem jest pokazanie perspektywy politycznej, zwłaszcza wymian szpiegów i ekspulsji dyplomatów jako narzędzi polityki międzynarodowej, a także współpracy służb specjalnych po 1990 r., z naciskiem na kierunek wschodni. Całość zamyka refleksja nad efektywnością polskiego systemu przeciwdziałania szpiegostwu.

Dzięki takiej strukturze monografia prezentuje zjawisko szpiegostwa w sposób wieloaspektowy: od analiz definicyjnych, przez rzetelnie uzasadnioną metodologię, po ocenę działań państwa. Autor tworzy spójny, osadzony empirycznie model teoretyczno-metodologiczny, pozwalający opisywać i systematyzować zjawisko szpiegostwa, a także wyjaśniać jego mechanizmy, funkcje oraz ewolucję w kontekście współczesnych zagrożeń zewnętrznych bezpieczeństwa państwa.

Na wyróżnienie zasługują rozważania poświęcone teorii szpiegostwa. Autor syntetyzuje istniejące ujęcia, a także rozwija własne propozycje interpretacyjne, sytuując szpiegostwo w kategorii transgranicznej przestępczości politycznej, której dynamika jest powiązana z geopolityką oraz zmianami w środowisku bezpieczeństwa. Przekonująco dowodzi, że szpiegostwo to nie tylko przestępstwo sensu stricto, lecz przede wszystkim zagrożenie bezpieczeństwa państwa ściśle zespolone z geopolityką, strategią bezpieczeństwa państwa i jego interesami.

Wnioski dotyczące przeciwdziałania szpiegostwu mają dużą wartość naukową i aplikacyjną. Chlebowicz kompleksowo omawia rolę instrumentów karnomaterialnych, administracyjnych i operacyjno-rozpoznawczych służących zwalczaniu szpiegostwa, w tym ocenia ich przydatność w kontekście nowych zagrożeń szpiegowskich. Szczególne znaczenie mają analiza wykładni art. 130 Kodeksu karnego

oraz omówienie obowiązku denuncjacji, a także przedstawienie praktycznego wymiaru pracy operacyjnej kontrwywiadu.

Recenzowana monografia spełnia kryteria pracy wybitnej – jest oryginalna, empirycznie ugruntowana, teoretycznie dopracowana i spójna. Stanowi wzór, jak powinny być prowadzone interdyscyplinarne badania nad zjawiskami trudnymi, wrażliwymi i dotychczas zmarginalizowanymi w dyskursie naukowym. Ma zatem potencjał, aby stać się publikacją referencyjną w badaniach nad szpiegostwem i przestępczością polityczną w Polsce oraz punktem odniesienia dla przyszłych opracowań. Z wielu względów warto byłoby ją przetłumaczyć na język angielski.

W dobie nasilenia zagrożeń hybrydowych książka Piotra Chlebowicza powinna stać się lekturą obowiązkową dla kryminologów, karnistów, analityków, a także polityków i innych osób odpowiedzialnych za bezpieczeństwo narodowe.

Dr hab. Tomasz Safjański, prof. AWSB

Doktor habilitowany nauk o bezpieczeństwie, doktor nauk prawnych, specjalista w zakresie taktyki kryminalistycznej i zwalczania przestępczości transgranicznej. Zastępca dyrektora Centrum Badań nad Bezpieczeństwem Transgranicznym Akademii WSB w Dąbrowie Górniczej.

Kontakt: tsafjanski@wsb.edu.pl

PRACE KONKURSOWE

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 205–223

https://doi.org/10.4467/20801335PBW.26.010.23372

ARTYKUŁ

Łączność w ramach administracji państwowej jako fundament odporności państwa na przykładzie Polski[1]

Communications within the state administration as the foundation of a nation's resilience: the case of Poland

DAVID CYBULSKI

Akademia Sztuki Wojennej

https://orcid.org/0009-0003-9195-4407

Abstrakt

Celem artykułu jest przedstawienie roli oraz stanu łączności między organami współczesnej administracji Rzeczypospolitej Polskiej. Zostały omówione aspekty prawne, organizacyjne i techniczne problematyki łączności w ramach tej administracji. Wskazano poważne braki w funkcjonowaniu dotychczasowych systemów łączności w cywilnych strukturach państwa, co może przekładać się na zdolności Polski do sprawnego reagowania na zagrożenia bezpieczeństwa narodowego. Podstawowym problemem jest brak ujednoliconego podejścia państwa do funkcjonowania komunikacji między

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Łączność i komunikacja administracji państwa w sytuacji zagrożenia bezpieczeństwa narodowego: na przykładzie Polski*, obronionej na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Autor wykorzystał fragmenty rozdziałów I, II i IV. Praca została nagrodzona w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

jednostkami administracji publicznej, w szczególności organami bezpieczeństwa, służbami ratunkowymi. Konieczne jest tym samym pilne dokonanie modernizacji podsystemu łączności państwowej do celów zarządzania kryzysowego w kontekście współczesnych wyzwań.

Słowa kluczowe komunikacja elektroniczna, łączność, łączność awaryjna, zarządzanie kryzysowe, System Bezpiecznej Łączności Państwowej

Abstract The purpose of this article is to present the role and current state of communications among the agencies of the modern administration of the Republic of Poland. The article addresses legal, organisational, and technical aspects of communication within the state administration. It highlights serious systemic deficiencies related to the functioning of existing communication systems in the civilian structures of the state, which may affect Poland's ability to respond effectively to emerging threats to national security. The fundamental problem here is the lack of a unified state perspective on the establishment and operation of communication between its various components, namely security agencies, emergency services, and public administration. It is therefore necessary to urgently modernise the state communications subsystem for crisis management purposes in the context of contemporary challenges.

Keywords electronic communication, telecommunications, emergency communications, crisis management

Wprowadzenie

Współczesne środowisko bezpieczeństwa narodowego charakteryzuje się ewoluującymi zagrożeniami, w tym cyberatakami, terroryzmem, a także działaniami o charakterze hybrydowym. W takich warunkach klasyczne, liniowe modele zarządzania kryzysowego okazują się niewystarczające, a zdolność państwa do skutecznego reagowania jest w coraz większym stopniu uzależniona od jakości przepływu informacji między kluczowymi uczestnikami systemu bezpieczeństwa. Szczególne znaczenie w tym kontekście zyskuje podsystem łączności, który nie tylko stanowi techniczne zaplecze dla działań administracji publicznej, służb ratowniczych i podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej, lecz także odpowiada za sprawne działanie całego systemu zarządzania kryzysowego.

Cyfryzacja administracji oraz rosnąca złożoność środowiska zagrożeń sprawiają, że skuteczna i bezpieczna wymiana informacji staje się warunkiem sine qua non przeciwdziałania incydentom mającym wpływ na funkcjonowanie państwa, zarówno o charakterze fizycznym, jak i cyfrowym. Jednocześnie wiele dokumentów, np. informacje pokontrolne NIK, wskazuje, że obecne systemy łączności w administracji publicznej często nie są w pełni dostosowane do jej współczesnych realiów operacyjnych i technologicznych. Przejawia się to m.in. w rozdrobnieniu rozwiązań telekomunikacyjnych, braku jednolitej architektury wymiany informacji, niedostatkach interoperacyjności, a także w znacznej podatności na błędy projektowe czy błędy popełnione przez człowieka.

Problem badawczy to pytanie: w jakim stopniu obecny podsystem łączności administracji państwowej jest odporny na aktualne zagrożenia dla bezpieczeństwa narodowego oraz jakie kierunki zmian mogą zwiększyć jego efektywność? Odpowiedź na to pytanie wymaga potraktowania łączności jako złożonego systemu społeczno-technicznego, w którym ramy prawne, rozwiązania organizacyjne, technologie i kompetencje użytkowników wzajemnie się warunkują. Hipoteza przyjęta w artykule zakłada, że istniejący system łączności administracji państwowej – budowany przez lata w sposób resortowy (jedynie pod zapotrzebowanie danego resortu) i fragmentaryczny – nie zapewnia w wystarczającym stopniu spójności i odporności na współczesne zagrożenia oraz że możliwe jest wskazanie realistycznych kierunków jego optymalizacji.

W artykule dokonano przeglądu ram normatywnych funkcjonowania łączności na potrzeby bezpieczeństwa narodowego, obejmujących zarówno ustawy, jak i rozporządzenia wykonawcze oraz wybrane dokumenty strategiczne. Ponadto zidentyfikowano i sklasyfikowano główne kategorie ryzyka – od błędów planistycznych i projektowych, przez problemy eksploatacyjne i ograniczenie suwerenności technologicznej, aż po zagrożenia cyberbezpieczeństwa. Następnie zaproponowano kierunki modernizacji, obejmujące zarówno integrację funkcjonujących systemów, jak i potencjał nowych technologii oraz koncepcję zintegrowanego podsystemu łączności państwa.

Zastosowano takie metody, jak: analiza aktów prawnych, przegląd literatury z zakresu bezpieczeństwa narodowego i telekomunikacji oraz analiza dokumentacji technicznej wybranych systemów. Wskazano także przykłady rozwiązań wdrożonych we Francji i Australii. Wykorzystano również analizę systemową, pozwalającą potraktować podsystem łączności jako element większej całości – narodowego systemu bezpieczeństwa – oraz ocenić jego funkcjonowanie w kategoriach spójności, redundancji i odporności. Zakres analizy celowo został ograniczony do rozwiązań komunikacyjnych w administracji państwowej, z wyłączeniem komunikacji

masowej między obywatelami oraz wojskowej, co umożliwia pogłębione ujęcie problematyki z perspektywy instytucji państwa.

Artykuł wpisuje się w szerszy nurt badań nad modernizacją systemów bezpieczeństwa państwa w warunkach transformacji cyfrowej i nasilających się napięć geopolitycznych. Wskazuje, że problematyka łączności – często postrzegana jako domena techniczna – powinna być traktowana jako strategiczny element bezpieczeństwa narodowego, wymagający spójnej polityki publicznej oraz świadomych decyzji inwestycyjnych. Proponowane wnioski i rekomendacje mogą stanowić punkt wyjścia zarówno do dalszych badań naukowych, jak i do prac koncepcyjnych związanych z aktualizacją krajowego podsystemu łączności administracji państwowej na potrzeby zarządzania kryzysowego.

Ramy prawne

Zapewnienie ciągłej i niezawodnej wymiany informacji uznano w Polsce za jeden z filarów bezpieczeństwa narodowego i sprawnego działania administracji publicznej, zwłaszcza w sytuacjach kryzysowych, nadzwyczajnych czy zagrożenia konfliktem zbrojnym. W efekcie stworzono rozbudowany system aktów prawnych, które regulują budowę, funkcjonowanie i ochronę systemów wchodzących w skład podsystemu łączności państwa, obejmujących zarówno systemy rządowe, jak i ogólnodostępne systemy komercyjne, mogące pełnić funkcję łączności zapasowej dla organów państwa.

W *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* wybrane systemy łączności i sieci teleinformatyczne zaliczono do infrastruktury krytycznej (art. 3 pkt 2 lit. b i c). Ustawa nakłada obowiązek opracowania i aktualizowania planów zarządzania kryzysowego, które muszą uwzględniać również kwestie teleinformatyczne i łączności (art. 6 ust. 5b), oraz ustanawiania zasady obiegu informacji w krajowym systemie zarządzania kryzysowego (art. 11 ust. 2 pkt 8). Ustawa wyraźnie wskazuje, że systemy łączności będące częścią infrastruktury krytycznej – zarówno rządowe, jak i część systemów komercyjnych – podlegają szczególnej ochronie przed zagrożeniami.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych reguluje ochronę infrastruktury teleinformatycznej przed zdarzeniami o charakterze terrorystycznym oraz zasady wymiany informacji między organami administracji publicznej i służbami w razie wystąpienia takich zagrożeń. Przewiduje ona m.in. możliwość czasowego dostosowywania i montażu przewodowych i bezprzewodowych instalacji łączności na potrzeby zabezpieczenia wydarzenia o podwyższonym ryzyku, z pewnymi odstępstwami od prawa budowlanego, tak aby zapewnić łączność

właściwym służbom (art. 13). Ustawa wprowadza również system stopni alarmowych i stopni alarmowych CRP (dotyczących cyberprzestrzeni RP), ogłaszanych zarządzeniem Prezesa Rady Ministrów. Dla podsystemu łączności istotne z punktu widzenia powyższych stopni są takie zadania, jak m.in.: informowanie podległego personelu, weryfikacja działania środków łączności, wzmożone monitorowanie systemów teleinformatycznych i integralności komunikacji elektronicznej, zapewnienie dyżurów administratorów i osób decyzyjnych, przegląd zapasowej infrastruktury teleinformatycznej oraz realizacja planów postincydentalnych przy najwyższych stopniach zagrożenia terrorystycznego[2].

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny kompleksowo opisuje zadania państwa w zakresie bezpieczeństwa militarnego, w tym kwestie organizacji łączności na potrzeby obronności. Jednym z centralnych elementów ustawy jest wojskowy system telekomunikacyjny (art. 17), który łączy Siły Zbrojne RP i resort obrony z innymi organami administracji publicznej oraz – w razie potrzeby – z organizacjami społecznymi służącymi obronności[3]. Ma on zapewniać funkcjonowanie systemu kierowania bezpieczeństwem narodowym oraz sprawne działanie państwa w czasie wojny, zagrożenia zewnętrznego i poważnych kryzysów, co wymaga od systemów łączności m.in. skalowalności i wysokiej żywotności, czyli zachowania integralności i dostępności w skrajnych warunkach. Ustawa przewiduje także możliwość militaryzacji wybranych podmiotów o kluczowym znaczeniu dla obronności, w tym przedsiębiorców telekomunikacyjnych. W praktyce oznacza to, że np. operator telefonii komórkowej może zostać objęty reżimem wojskowym, aby w razie zagrożenia zapewnić dostępność jego sieci na potrzeby administracji państwowej i sił zbrojnych.

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej porządkuje zasady funkcjonowania rynku telekomunikacyjnego i komunikacji elektronicznej. Nakłada jednocześnie obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Zobowiązuje przedsiębiorców telekomunikacyjnych do opracowania planów działania w sytuacjach szczególnych zagrożeń i utrzymywania ciągłości świadczenia usług, a Prezesowi Urzędu Komunikacji Elektronicznej (UKE) przyznaje uprawnienia do nakładania na nich określonych obowiązków, np. w zakresie utrzymania działania sieci. Istotny z punktu widzenia podsystemu łączności państwa jest nałożony na przedsiębiorców obowiązek świadczenia usług na rzecz organów państwowych w razie szczególnego zagrożenia

[2] *Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP.*

[3] *Rozporządzenie Ministra Obrony Narodowej z dnia 20 kwietnia 2022 r. w sprawie działania wojskowego systemu telekomunikacyjnego.*

bezpieczeństwa, stanów nadzwyczajnych czy wojny. Ustawa zobowiązuje także operatorów do przekazywania Prezesowi UKE informacji o posiadanej infrastrukturze telekomunikacyjnej potrzebnej do przygotowania systemów łączności służących obronności i bezpieczeństwu, co umożliwia władzom państwowym planowanie wykorzystania potencjału sieci publicznych jako elementu systemu bezpieczeństwa.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz *Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (art. 21 pkt 6) przyznają władzom państwowym prawo do czasowego ograniczania praw i wolności obywatelskich, w tym swobody korzystania z systemów łączności. Pozwala to na redukowanie lub wyłączanie części usług dla ogółu użytkowników, aby zapewnić administracji państwowej, wojsku i służbom priorytetowy dostęp do łączności. Dzięki tym regulacjom możliwe jest również sięgnięcie po komercyjne systemy łączności jako łącza zapasowe, z jednoczesnym ograniczeniem ich publicznego obciążenia w taki sposób, aby w krytycznym momencie nie doszło do przeciążenia infrastruktury.

Obowiązująca od 2025 r. *Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej* wypełnia dotychczasową lukę regulacyjną w obszarze obrony cywilnej i porządkuje system ochrony ludności w sytuacjach pokoju, kryzysu i wojny. Określa ona m.in. infrastrukturę niezbędną do realizacji zadań ochrony ludności, w tym infrastrukturę łączności i systemy teleinformatyczne jako podstawowy warunek efektywnej koordynacji działań różnych szczebli administracji. Na podstawie art. 71 wyodrębniono katalog narzędzi komunikacyjnych tworzących system komunikacji administracji państwowej: syreny alarmowe i urządzenia nagłaśniające, systemy ostrzegania (w tym Regionalny System Ostrzegania), dzienniki lokalne i ogólnopolskie, radio i telewizję, system ALERT RCB, ostrzeżenia wysyłane w ramach technologii cyfrowych oraz oficjalne serwisy informacyjne administracji.

Jednym z centralnych projektów przewidzianych w ustawie o ochronie ludności i obronie cywilnej jest System Bezpiecznej Łączności Państwowej (SBŁP), nadzorowany przez ministra właściwego do spraw wewnętrznych (art. 15 ust. 1 pkt 24). System ma stanowić zintegrowaną, bezpieczną i o wysokiej dostępności platformę łączności dla najważniejszych organów państwa, służb ratowniczych, podmiotów ochrony ludności i sił zbrojnych, łącząc różne dotychczasowe systemy resortowe przez odpowiednie interfejsy i standardy. W ustawie wyróżniono kilka funkcjonalnych wariantów SBŁP: system jawny (SBŁP-J), system wielopunktowej wideokonferencji (SBŁP-V), radiowy system mobilny (SBŁP-M), system radiowej łączności trankingowej (SBŁP-T) oraz system łączności satelitarnej (SBŁP-S). Wszystkie te moduły mają zapewniać szyfrowanie end-to-end oraz spełniać określone przez

Radę Ministrów minimalne wymagania bezpieczeństwa teleinformatycznego, adekwatne do poziomu zagrożeń (art. 78 pkt 2).

Dodatkowo *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* reguluje zasady przetwarzania informacji klauzulowanych w systemach teleinformatycznych. Dla podsystemu łączności oznacza to konieczność projektowania oddzielnych, akredytowanych systemów dla komunikacji niejawnej, takich jak systemy niejawnej łączności stacjonarnej (SBŁP-N), a częściowo również SBŁP-M i SBŁP-S. Przetwarzanie informacji niejawnych jest dopuszczalne wyłącznie w systemach do tego dostosowanych, w tym specjalnie akredytowanych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego. To powoduje, że dystrybucja danych, np. wywiadowczych czy informacji operacyjnych, staje się logistycznie trudniejsza, równocześnie jednak zwiększa ochronę przed ich przechwyceniem. Wymusza też tworzenie wyspecjalizowanych sieci i urządzeń końcowych dla uprawnionych użytkowników.

Analiza zagrożeń dla podsystemu łączności

Podsystem łączności administracji państwowej stanowi jeden z filarów zarządzania kryzysowego oraz szeroko rozumianego systemu bezpieczeństwa narodowego. Jest kluczem do efektywnego zarządzania siłami i środkami zarówno w wymiarze prewencyjnym, jak i na etapie reagowania na sytuacje kryzysowe, w których przekaz informacji za pomocą technicznych środków łączności pozostaje podstawowym kryterium zintegrowanego zarządzania zasobami[4]. Jednocześnie brakuje alternatyw dla współczesnych systemów teleinformatycznych, co sprawia, że konieczność priorytetyzacji przez państwo rozwoju, utrzymania i zabezpieczenia tych systemów jest bezdyskusyjna. Bez odpowiednich rozwiązań technologicznych nawet najlepiej przygotowana i wyspecjalizowana administracja nie będzie zdolna do skutecznego wykonywania swoich zadań, ponieważ nie będzie miała narzędzi do sprawnej koordynacji działań na poziomach taktycznym, operacyjnym i strategicznym, co grozi pogłębieniem kryzysu.

Znaczenie systemów łączności dla bezpieczeństwa narodowego potwierdzają dokumenty strategiczne, w tym Strategia Bezpieczeństwa Narodowego z 2020 r. Wskazano w niej, że sieci łączności satelitarnej i mobilnej stanowią podstawę wymiany informacji i są kluczowym elementem zasobów bezpieczeństwa narodowego

[4] J. Pilżys, *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, t. 8, nr 1, s. 45.

oraz gotowości państwa na wypadek sytuacji kryzysowych[5]. Systemy łączności zostały zaliczone do krajowej infrastruktury krytycznej, a dokument strategiczny akcentuje potrzebę dalszego rozwoju bezpiecznych, nowoczesnych sieci telekomunikacyjnych.

Dotychczasowy rozwój podsystemu łączności w Polsce miał charakter rozproszony i resortowy. Brak całościowego, odgórnego programu budowy jednolitego systemu łączności państwowej sprawił, że poszczególne organy i służby tworzyły własne rozwiązania na miarę bieżących potrzeb i możliwości. W rezultacie funkcjonują systemy, które często nie są ze sobą zintegrowane ani technicznie, ani organizacyjnie[6]. Wymiana informacji między resortami, służbami, a nawet na różnych poziomach administracji publicznej (centralnym, wojewódzkim, powiatowym i gminnym) jest utrudniona. System zarządzania kryzysowego i system kierowania bezpieczeństwem narodowym mają wprawdzie formalnie określoną strukturę hierarchiczną, jednak brak jednolitych środków łączności zarówno w pionie, jak i w poziomie powoduje ryzyko paraliżu decyzyjnego, powielania zadań oraz rozproszenia wysiłków w sytuacji realnego zagrożenia. Wskazuje na to również Najwyższa Izba Kontroli, która w licznych raportach z kontroli zwracała uwagę na problem braku jednolitego cyfrowego systemu łączności radiowej dla służb ratowniczych i struktur zarządzania kryzysowego. Oceniała, że to negatywnie oddziałuje na przepływ informacji i skuteczność działań[7].

Ważnym elementem kształtowania każdego systemu teleinformatycznego jest jego właściwe zaplanowanie i zaprojektowanie. Standardy z obszaru inżynierii systemów i oprogramowania, takie jak norma ISO/IEC/IEEE 24748-1, wyróżniają pełen cykl życia systemu: planowanie, projektowanie, budowę, użytkowanie, doskonalenie i ostatecznie wycofanie z eksploatacji[8]. Każdy z tych etapów jest ze sobą ściśle powiązany, a błędy popełnione w fazie planistycznej mogą się kumulować w kolejnych fazach projektu. W przypadku systemów o znaczeniu państwowym, szczególnie tych o zasięgu krajowym, błędne założenia, niedoszacowanie kosztów i terminów, wybór niewłaściwych partnerów, pominięcie analizy rzeczywistych potrzeb użytkowników czy rezygnacja z wbudowania redundancji mogą doprowadzić do sytuacji, w której system nie będzie spełniał swojej podstawowej funkcji.

---

5 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, s. 8.

6 M. Gawroński, *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego*, „Wiedza Obronna" 2014, nr 2–3, s. 61–63.

7 Najwyższa Izba Kontroli, *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych*, 2017 r., s. 11.

8 ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Przykładem takich zaniedbań jest pożar Mostu Łazienkowskiego w Warszawie w 2015 r. Spowodował zniszczenie kluczowych łączy światłowodowych, co doprowadziło do czasowego odcięcia od sieci części instytucji centralnych, w tym resortu obrony[9]. Z kolei ogólnokrajowe awarie systemów dyspozytorskich Centrów Powiadamiania Ratunkowego w 2021 r. i 2024 r. doprowadziły do sytuacji, w której dyspozytorzy nie byli w stanie przydzielać zadań zespołom ratownictwa medycznego w standardowy sposób, a rozwiązaniem było ręczne zapisywanie zgłoszeń[10]. Zdarzenia te mogły mieć znacznie łagodniejszy przebieg, gdyby już na etapie projektowania przewidziano obowiązek redundancji niezależnych kanałów, alternatywnych tras transmisyjnych oraz procedur przełączenia między nimi.

Równie istotny jest sposób eksploatacji systemów łączności. Etap użytkowania nie kończy cyklu życia systemu – to właśnie w codziennej pracy jest on weryfikowany przez użytkowników końcowych, a równocześnie są gromadzone doświadczenia niezbędne do jego dalszego doskonalenia. Kluczową rolę odgrywa przygotowanie użytkowników. Jeżeli nie zostaną właściwie przeszkoleni, a interfejs systemu okaże się zbyt skomplikowany lub nieintuicyjny, istnieje ryzyko, że w praktyce będą oni obchodzić przewidziane rozwiązania i sięgać po kanały pozasystemowe. Dążenie przez użytkownika do wygody w obszarze łączności może prowadzić np. do wykorzystywania popularnych komunikatorów internetowych, które nie są przystosowane do wymiany informacji niejawnych czy informacji na temat sytuacji kryzysowych. W ostatnich latach odnotowano przykłady wykorzystania komercyjnych aplikacji do przekazywania wrażliwych informacji m.in. w administracjach amerykańskiej oraz w polskiej, w których istotne decyzje były konsultowane z użyciem ogólnodostępnych usług[11]. Takie praktyki podważają poziom bezpieczeństwa informacji i pokazują, że systemy łączności muszą być projektowane z uwzględnieniem nie tylko wymagań technicznych i norm bezpieczeństwa, lecz także ergonomii, łatwości obsługi i nawyków użytkowników.

---

[9] M. Gąsior, *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu*, naTemat, 15 II 2015 r., https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [dostęp: 18 III 2026].

[10] *Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja*, TVN24, 15 V 2021 r., https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [dostęp: 18 III 2026]; *Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112*, Onet, 16 XII 2024 r., https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [dostęp: 18 III 2026].

[11] J. Goldberg, *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025 r., https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [dostęp: 18 III 2026]; Z. Wanat, *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021 r., https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [dostęp: 18 III 2026].

Warunkiem poprawnej eksploatacji są szczegółowe procedury operacyjne oraz regularne ćwiczenia. Procedury powinny precyzyjnie opisywać czynności użytkowników i administratorów, a także zawierać plany awaryjne, tryby postępowania w razie utraty części infrastruktury czy wystąpienia incydentów bezpieczeństwa. Ćwiczenia – zarówno symulacje sytuacji kryzysowych, jak i testy obciążeniowe – pozwalają zweryfikować założenia projektowe, wykryć wąskie gardła oraz utrzymać na odpowiednim poziomie kompetencje personelu. Brak ćwiczeń lub ich pobieżny charakter prowadzi do stopniowej utraty umiejętności korzystania z systemów w sytuacjach niestandardowych. To oznacza, że w chwili realnego kryzysu personel może spontanicznie sięgnąć po nieautoryzowane narzędzia, czym narazi bezpieczeństwo informacji i ciągłość działania instytucji.

W wymiarze organizacyjnym szczególnego znaczenia nabiera zagadnienie suwerenności technologicznej. Korzystanie z rozwiązań sprzętowych i programowych pochodzących z państw trzecich, stwarza ryzyko utraty kontroli nad kluczowymi parametrami bezpieczeństwa informacji: poufnością, integralnością i dostępnością. Przykłady takich zagrożeń obejmują zarówno rekomendacje władz[12], aby w systemach krytycznych nie stosować niektórych zagranicznych produktów bezpieczeństwa, jak i przypadki wykrycia backdoorów (pol. tylnych furtek) w urządzeniach i oprogramowaniach[13] wykorzystywanych do przetwarzania danych wrażliwych. Informacje o możliwości zdalnej ingerencji w zaawansowane systemy wojskowe czy o eksfiltracji danych medycznych z wykorzystaniem luk w urządzeniach monitorujących pokazują, że brak pełnej kontroli nad technologią może zostać wykorzystany do wywierania presji politycznej, destabilizacji systemów ochrony zdrowia czy zakłócenia działania sił zbrojnych. W przypadku Polski istnieje ryzyko braku dostępu do ponadnarodowych źródeł danych, np. NATO i Unii Europejskiej czy własnych systemów rozlokowanych poza terytorium kraju (placówki dyplomatyczne, konstelacje satelitarne). Racjonalnym rozwiązaniem jest budowa nadmiarowych, niezależnych torów łączności oraz rozwój krajowego potencjału w zakresie projektowania i produkcji systemów łączności, co pozwoli w większym stopniu uniezależnić się od zagranicznych dostawców i ograniczy możliwość szantażu technologicznego.

Pod względem technicznym bezpieczeństwo i odporność podsystemu łączności opierają się na zapewnieniu określonych atrybutów bezpieczeństwa informacji. Normy z rodziny ISO/IEC 27000 i pokrewnych wyróżniają w tym zakresie przede wszystkim poufność, integralność i dostępność, a także autentyczność,

[12] *Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r.* (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022 r., s. 1.

[13] *Contec CMS8000 Contains a Backdoor*, CISA 2025, s. 1 i nast.

rozliczalność, aktualność i kompletność danych[14]. W kontekście łączności państwowej oznacza to, że informacje muszą być dostępne dla uprawnionych podmiotów wtedy, kiedy są potrzebne, nie mogą być zmieniane lub niszczone w sposób nieautoryzowany, muszą pochodzić z wiarygodnych źródeł, a każde działanie na nich powinno być możliwe do przypisania do konkretnego użytkownika lub procesu. Dodatkowo informacje wykorzystywane w procesie decyzyjnym muszą być aktualne oraz kompletne, aby umożliwić ich przetworzenie w rzetelną wiedzę operacyjną. Brak któregokolwiek z tych atrybutów może prowadzić do błędnych decyzji, opóźnień lub całkowitego paraliżu działań.

Ponadto poważnym wyzwaniem jest zapewnienie interoperacyjności i kompatybilności stosowanych rozwiązań. Poszczególne służby i instytucje państwowe korzystają z wielu systemów, częstotliwości, protokołów i standardów, które nie zawsze są ze sobą spójne. Brak ogólnokrajowych standardów dla łączności kryzysowej i wspólnej platformy wymiany informacji powoduje, że w sytuacjach wymagających współdziałania mogą pojawić się opóźnienia, nieporozumienia i przerwy w przepływie danych[15]. Rozdrobnienie systemów zwiększa też skalę ataku – utrzymywanie wielu niespójnych rozwiązań utrudnia skuteczne zabezpieczenie i monitoring tych systemów. W obliczu rosnącej liczby cyberataków, w tym ze strony zaawansowanych, sponsorowanych przez państwa grup APT (ang. *advanced persistent threats*), konieczne staje się podejście, w którym bezpieczeństwo łączności postrzegane jest jako element konstytucyjnego obowiązku państwa w zakresie zapewnienia bezpieczeństwa obywateli, a nie jako koszt. Wymaga to stosowania silnego szyfrowania end-to-end, konsekwentnej aktualizacji oprogramowania, segmentacji sieci, stosowania zasady najmniejszych uprawnień (ang. *principle of least privilege*) oraz rozwiązań silnego, najlepiej wieloskładnikowego uwierzytelniania użytkowników.

Wszystkie wskazane zagrożenia prowadzą do jednoznacznego wniosku, że Polska powinna konsekwentnie rozwijać spójny, jednolity podsystem łączności państwa, integrujący istniejące systemy resortowe i zapewniający bezpieczną, odporną i efektywną wymianę informacji na wszystkich poziomach zarządzania i współpracy. Oznacza to odejście od modelu wyspowego na rzecz świadomie zaprojektowanej, skalowalnej i redundantnej architektury, opartej na narodowych kompetencjach technologicznych i wspólnych standardach. Tylko w ten sposób

[14] PN-EN ISO/IEC 27000 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, Polski Komitet Normalizacyjny, Warszawa 2012, s. 14, 17.

[15] M. Bieńkowski, *Funkcjonowanie systemu ochrony ludności w Polsce*, „Kontrola Państwowa" 2019, nr 5, s. 60–62.

można zagwarantować, że w sytuacjach kryzysowych, w tym w warunkach działań hybrydowych czy konfliktów zbrojnych, aparat państwowy będzie w stanie skutecznie realizować swoje zadania i chronić bezpieczeństwo obywateli.

Możliwości rozwiązania impasu komunikacyjnego

Obecnie w Polsce różne instytucje i resorty korzystają z własnych, często dublujących się rozwiązań (np. dwóch systemów mobilnej łączności niejawnej – CATEL i SKR-Z czy kilku środowisk poczty elektronicznej dla tych samych poziomów tajności – CATEL i System Niejawnej Poczty Internetowej OPAL), które nie są kompatybilne. Brak jednolitego systemu i wspólnych standardów powoduje, że wymiana informacji pomiędzy systemami często odbywa się ręcznie, co wydłuża czas reakcji na zdarzenia kryzysowe i zwiększa ryzyko błędu.

Brak jednolitości systemów generuje również koszty i ryzyka na kilku poziomach. Po pierwsze, zwielokrotniają się nakłady inwestycyjne – państwo finansuje wiele równoległych projektów, co obciąża budżet i ogranicza środki na modernizację infrastruktury czy innowacje. Po drugie, rozproszenie systemów poszerza wektor ataku: każdą nową platformę trzeba osobno nadzorować, aktualizować, testować i zabezpieczać, co utrudnia zarządzanie podatnościami w skali całej administracji. Po trzecie, wymusza to utrzymywanie dużej liczby specjalistów w wielu instytucjach – poszczególne jednostki muszą dysponować własnym zespołem utrzymania i bezpieczeństwa, co nie tylko podnosi koszty, lecz także prowadzi do sytuacji, w której wzrost zatrudnienia w danej instytucji następuje kosztem osłabienia innej. W tym kontekście coraz wyraźniej zarysowuje się potrzeba wypracowania nowego, zintegrowanego podejścia, które z jednej strony pozwoli zachować elastyczność i sprostać specyficznym wymaganiom różnych instytucji, z drugiej zaś zapewni spójność i interoperacyjność całego podsystemu łączności państwa.

Jedną z możliwości jest przyjęcie architektury warstwowej, inspirowanej europejskimi ramami interoperacyjności[16]. W takim modelu poszczególne instytucje mogłyby nadal korzystać z właściwych interfejsów i aplikacji (np. różnych komunikatorów, platform wideokonferencyjnych czy systemów telefonii IP), lecz cała wymiana danych odbywałaby się za pośrednictwem wspólnej warstwy transportowej i semantycznej (tabela 1). Funkcje komunikacyjne byłyby odseparowane od używanego medium – ta sama rozmowa czy komunikat przechodziłyby przez sieć komórkową, światłowód, radio lub satelitę, przy zachowaniu jednolitych standardów

[16] *Europejskie Rady Interoperacyjności*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [dostęp: 30 III 2026].

szyfrowania i metadanych. Kluczowe byłoby wdrożenie translatorów protokołów działających w czasie rzeczywistym, które automatycznie konwertowałyby komunikaty między różnymi formatami i protokołami bez utraty informacji o nadawcy, odbiorcy, klauzuli tajności czy priorytecie wiadomości. Uzupełnieniem tego podejścia byłyby inteligentne mechanizmy routingu, wybierające optymalny kanał transmisji w zależności od kontekstu – ważności komunikatu, dostępnych łączy, obciążenia sieci czy rodzaju urządzenia, jakim dysponuje odbiorca.

Tabela 1. Koncepcja rozwoju systemu zintegrowanej łączności państwowej.

Warstwa	Opis	Przykładowe standardy
Aplikacyjna	Narzędzia dostosowane do potrzeb instytucji	Threema OnPrem dla urzędów, Matrix dla organów bezpieczeństwa
Semantyczna	Słowniki, translatory i schematy wymiany danych	XML GovCore, JSON-LD z ontologiami EU Vocab
Transportowa	Uniwersalne protokoły szyfrowanej komunikacji	TLS 1.3, QUIC, SCIP dla głosu
Fizyczna	Neutralna technologicznie infrastruktura sieciowa	SD-WAN, 5G NSA, sieci kampusowe

Źródło: opracowanie własne.

Inspiracji dla takiego podejścia dostarczają rozwiązania wdrożone w innych państwach. Francuski system Tchap, uruchomiony w 2019 r., opiera się na otwartym, zdecentralizowanym protokole Matrix, co pozwala budować federacyjną architekturę komunikacyjną – każdy resort czy agencja może utrzymywać własny serwer, zachowując kontrolę nad danymi, a jednocześnie pozostaje w bezpiecznym kontakcie z innymi jednostkami administracji[17]. Protokół Matrix umożliwia też tworzenie tzw. mostów do innych platform (np. XMPP, IRC, Slack), co ułatwia bezpieczny kontakt z partnerami zewnętrznymi przy zachowaniu standardów bezpieczeństwa i zgodności z regulacjami, takimi jak rozporządzenie eIDAS[18]. System

[17] C. Dussutour, *French government launches in-house developed messaging service, Tchap*, European Commission, 10 XII 2021 r., https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [dostęp: 19 III 2026].

[18] eIDAS (ang. *Electronic IDentification, Authentication and Trust Services*) – jednolity standard identyfikacji elektronicznej i usług zaufania Unii Europejskiej działający na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji*

Tchap oferuje m.in. szyfrowanie end-to-end, integrację z państwowym systemem tożsamości elektronicznej oraz mechanizmy automatycznego usuwania wiadomości. Jego skuteczność została potwierdzona podczas XXXIII Letnich Igrzysk Olimpijskich w Paryżu, kiedy znacznie wzrosła liczba użytkowników, wysyłanych komunikatów i tworzonych pokoi roboczych (chatów wieloosobowych) na potrzeby koordynacji bezpieczeństwa i logistyki[19].

Kolejnym przykładem rozwiązania ukierunkowanego na bezpieczną integrację komunikacyjną rozproszonej struktury rządowej jest australijski GovLINK. System zarządzany przez Department of Finance tworzy szyfrowane środowisko wymiany informacji między agencjami federalnymi, stanowymi oraz wybranymi partnerami publicznymi i prywatnymi[20]. Bazuje na federacyjnej architekturze i wspólnych standardach bezpieczeństwa (np. S/MIME, X.509), co pozwala agencjom zachować własne systemy i równocześnie korzystać z jednolitych mechanizmów uwierzytelniania, szyfrowania i podpisu elektronicznego.

Oba przykłady pokazują, że otwarte protokoły, federacyjna architektura i mocne algorytmy kryptograficzne mogą skutecznie przezwyciężyć problem braku jednolitości systemów przy zachowaniu autonomii poszczególnych instytucji.

W polskich realiach punktem odniesienia dla takiego kierunku zmian jest projekt SBŁP. Ma on stać się wielowarstwowym, zintegrowanym systemem, nadzorowanym przez ministra właściwego do spraw wewnętrznych. System ma połączyć różne kanały komunikacyjne – od sieci stacjonarnych i radiowych, przez komórkowe, aż po satelitarne – w jedno spójne środowisko łączności administracji państwowej. Najważniejszym zadaniem SBŁP ma być zapewnienie ciągłości łączności między organami państwa zarówno w czasie pokoju, jak i w sytuacjach zagrożenia czy wojny oraz umożliwienie interoperacyjności między odrębnymi systemami cywilnymi, służb bezpieczeństwa i struktur wojskowych. Projekt zakłada wyodrębnienie kilku komponentów funkcjonalnych: SBŁP-J, SBŁP-N, SBŁP-V, SBŁP-M, SBŁP-T i SBŁP-S. Wszystkie są oparte na certyfikowanych rozwiązaniach kryptograficznych.

Istotną zaletą koncepcji SBŁP jest możliwość wykorzystania istniejącej infrastruktury, takiej jak sieci OST112 czy GovNet, zarówno dla systemów jawnych, jak i niejawnych. Pozwoliłoby to ograniczyć koszty i przyspieszyć wdrożenie systemu. Integracja z funkcjonującymi już rozwiązaniami (np. wykorzystanie systemu

elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

[19] *Tchap, the French administration federation: past, present and future - Julie Ripa*, YouTube, 29 X 2024 r., https://www.youtube.com/watch?v=m1roliPrNqc [dostęp: 19 III 2026].

[20] GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [dostęp: 19 III 2026].

CATEL w komponencie SBŁP-M) zwiększy redundancję kanałów i umożliwi stopniowe przechodzenie z rozwiązań rozproszonych do bardziej spójnej architektury. Na obecnym etapie nie zostało jednak ujawnione, czy SBŁP będzie całkowicie nowym systemem projektowanym od podstaw, zbiorem zmodyfikowanych istniejących rozwiązań czy połączeniem obu podejść. Wiele wskazuje na to, że ze względów ekonomicznych i organizacyjnych może dominować podejście ewolucyjne, polegające na stopniowej integracji i unifikacji.

Planowanie i realizacja takiej transformacji wymaga podejścia etapowego. W fazie pilotażowej można zbudować fundament nowego systemu, oparty na otwartych protokołach (jak Matrix) i zintegrować z nim ograniczoną liczbę resortów, testując w praktyce mechanizmy interoperacyjności i bezpieczeństwa. Następny etap to rozszerzanie zasięgu na kolejne instytucje oraz wdrażanie translatorów protokołów dla starszych systemów, tak aby umożliwić im wymianę informacji bez konieczności natychmiastowej wymiany całej infrastruktury (np. z metadanych TETRA na standard JSON-LD lub Matrix do formatu XMPP). Równolegle należałoby prowadzić certyfikację zgodności z przyjętymi standardami bezpieczeństwa (np. ISO 27001) oraz wypracowywać wspólne polityki bezpieczeństwa, które docelowo można częściowo zautomatyzować. W perspektywie długofalowej możliwa byłaby także integracja z systemami komunikacji na poziomie Unii Europejskiej, zgodnie z promowanymi koncepcjami typu GovStack, które zakładają budowę ustandaryzowanych, modułowych komponentów możliwych do łączenia według potrzeb[21].

Korzyści z wdrożenia zintegrowanego, interoperacyjnego systemu łączności są wielowymiarowe. Poza skróceniem czasu reakcji na sytuacje kryzysowe i podniesieniem poziomu bezpieczeństwa informacji można oczekiwać znacznego obniżenia kosztów utrzymania infrastruktury oraz większej odporności na awarie i ataki. Warunkiem osiągnięcia sukcesu pozostaje jednak zachowanie równowagi – system musi być na tyle jednolity, by wszystkie instytucje mogły bezproblemowo współpracować, a jednocześnie na tyle modułowy, by można go było dostosowywać do specyficznych zadań poszczególnych użytkowników i rozwijać wraz ze zmianami technologii oraz zagrożeń. Jeśli SBŁP zostanie zaprojektowany jako otwarta, interoperacyjna platforma, a nie kolejny zamknięty system resortowy o ograniczonym zasięgu, to może stać się fundamentem nowej jakości w łączności państwowej.

[21] GovStack, https://www.govstack.global/about/ [dostęp: 19 III 2026].

Podsumowanie

Podsystem łączności administracji państwowej jest jedną z kluczowych determinant odporności państwa na współczesne zagrożenia, a jego skuteczność wynika z równoczesnego oddziaływania czterech czynników: ram prawnych, jakości procesów planowania i projektowania, dojrzałości technologicznej oraz kompetencji użytkowników. Pomimo istnienia rozbudowanej infrastruktury telekomunikacyjnej obecny system łączności nie jest w pełni zintegrowany, co prowadzi do opóźnień, dysfunkcji i zwiększenia podatności na zakłócenia w sytuacjach kryzysowych. Tym samym potwierdzona została hipoteza o niedostosowaniu obecnego systemu łączności do aktualnych zagrożeń.

W wymiarze aplikacyjnym zaproponowano model optymalizacji podsystemu łączności, w którym zróżnicowane systemy i media transmisji są integrowane przez spójne warstwy planistyczno-organizacyjne i techniczne. Model ten zakłada wykorzystanie istniejących zasobów infrastrukturalnych, ich stopniową integrację oraz nowe funkcjonalności umożliwiające automatyczne kierowanie ruchem informacyjnym różnymi kanałami, w zależności od priorytetu, wrażliwości danych i dostępności łączy. Tak ujęta modernizacja redukuje ryzyko utraty łączności w skrajnych sytuacjach oraz ogranicza koszty przez odejście od dublowania rozwiązań na rzecz świadomej konsolidacji.

W artykule doprecyzowano kryteria oceny odporności systemów łączności w kategoriach czterech komplementarnych wymiarów:

1) prawnego (zgodność i kompletność regulacji),
2) planistycznego (jakość koncepcji funkcjonalnych),
3) redundancji (zapewnienie wielotorowości komunikacji),
4) integracji (rzeczywista zdolność do współdziałania między systemami).

Ujęcie to sprzyja odejściu od uproszczonego, infrastrukturalnego spojrzenia na łączność i pozwala włączyć ją w główny nurt badań nad systemem bezpieczeństwa narodowego.

Ograniczenia badania – w szczególności brak pełnego dostępu do danych operacyjnych oraz do szczegółowych założeń rozwijanego SBŁP – wskazują na potrzebę kontynuacji prac nad empiryczną weryfikacją różnych wariantów integracji istniejących systemów. Za zasadne należy uznać zwłaszcza dalsze badania nad architekturami federacyjnymi, mechanizmami tłumaczenia protokołów i standardami wymiany danych pomiędzy podmiotami bezpieczeństwa do implementacji w systemach łączności państwowej.

Wnioski płynące z przeprowadzonych badań prowadzą do jednoznacznej konkluzji: inwestycje w cyfrową transformację i integrację systemu łączności nie są jedynie kwestią modernizacji technicznej, lecz warunkiem utrzymania realnej

zdolności operacyjnej państwa w XXI w. Implementacja przedstawionych rekomendacji może przełożyć się na skrócenie czasu reakcji administracji, służb bezpieczeństwa i ratownictwa w sytuacjach kryzysowych, co będzie miało bezpośredni wpływ na ciągłość funkcjonowania instytucji publicznych, ochronę ludności oraz zachowanie stabilności państwa w warunkach narastającej niepewności strategicznej.

Bibliografia

Bieńkowski M., *Funkcjonowanie systemu ochrony ludności w Polsce*, „Kontrola Państwowa" 2019, nr 5, s. 52–70.

Contec CMS8000 Contains a Backdoor, CISA, 2025.

Gawroński M., *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego*, „Wiedza Obronna" 2014, nr 2–3, s. 47–86.

Pilżys J., *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, t. 8, nr 1, s. 33–49.

Źródła internetowe

Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja, TVN24, 15 V 2021 r., https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [dostęp: 18 III 2026].

Dussutour C., *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021 r., https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [dostęp: 19 III 2026].

Europejskie Rady Interoperacyjności, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [dostęp: 30 III 2026].

Gąsior M., *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu*, naTemat, 15 II 2015 r., https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [dostęp: 18 III 2026].

Goldberg J., *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025 r., https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [dostęp: 18 III 2026].

GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [dostęp: 19 III 2026].

GovStack, https://www.govstack.global/about/ [dostęp: 19 III 2026].

Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112, Onet, 16 XII 2024 r., https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [dostęp: 18 III 2026].

Tchap, the French administration federation: past, present and future – Julie Ripa, YouTube, 29 X 2024 r., https://www.youtube.com/watch?v=m1roliPrNqc [dostęp: 19 III 2026].

Wanat Z., *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021 r., https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [dostęp: 18 III 2026].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (DzU z 2024 r. poz. 1907, ze zm.).

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (DzU z 2024 r. poz. 1221, ze zm.).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2025 r. poz. 825, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2025 r. poz. 194).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2025 r. poz. 1209).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122, ze zm.).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. DzU z 2025 r. poz. 504).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (DzU z 2017 r. poz. 1928).

Rozporządzenie Ministra Obrony Narodowej z dnia 20 kwietnia 2022 r. w sprawie działania wojskowego systemu telekomunikacyjnego (DzU z 2022 r. poz. 870).

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (t.j. DzU z 2022 r. poz. 2065).

Inne dokumenty

ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych*, 2017 r.

PN-EN ISO/IEC 27000 –Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, Polski Komitet Normalizacyjny.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r. (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022 r.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, Warszawa 2020.

David Cybulski

Specjalista w dziedzinie cyberbezpieczeństwa. Doświadczenie zawodowe zdobywał na rynku prywatnym oraz w administracji państwowej. Pasjonat zagadnień związanych z innowacyjnymi rozwiązaniami z zakresu cyberbezpieczeństwa oraz nowych technik cyberataków grup APT, ze szczególnym uwzględnieniem ataków socjotechnicznych. Jego zainteresowania naukowe obejmują ochronę infrastruktury krytycznej, aktywność wybranych grup APT, tematykę bezpieczeństwa zjawiska Shadow IT oraz działania Cyber Threat Intelligence / Threat Hunting wobec wybranych grup cyberprzestępczych.

Kontakt: dcybulski@proton.me

Kontakt
tel. (+48) 22 58 58 613
e-mail: wydawnictwo@abw.gov.pl

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Polska

Druk
Biuro Logistyki Agencji Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A, 00-993 Warszawa, Polska
tel. (+48) 22 58 57 657

INTERNAL SECURITY REVIEW

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335
e-ISSN 2720-0841

MEiN points: 20

Printed in April 2026

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

Articles express the views of the authors

Declaration of the original version
The printed version of the journal is the original version
The online version of the journal is available at:
https://ejournals.eu/en/journal/przeglad-bezpieczenstwa-wewnetrznego

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

Indexing in databases
"Internal Security Review" can be found in the following databases: Index Copernicus Journal Master List with 100 points, ERIH PLUS, Central European Journal for Social Sciences and Humanities, Polish Scientific Bibliography

Texts submission
Materials submitted to PBW should be made via the editorial panel available at:
https://ojs.ejournals.eu/PBW/about/submissions

Contact
phone (+48) 22 58 58 613
e-mail: wydawnictwo@abw.gov.pl
https://ejournals.eu/en/journal/przeglad-bezpieczenstwa-wewnetrznego

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

TABLE OF CONTENTS

ARTICLES

REVIEW ARTICLES / REVIEWS

AWARDED THESES

Ladies and Gentlemen!

I am pleased to be able to recommend the latest issue of the "Internal Security Review". In this issue, we have devoted a great deal of attention to the activities of various uniformed services in Poland. Our authors write, among other things, about specialist rescue operations in the State Fire Service, issues relating to human resources policy in the Border Guard and the Polish Armed Forces, as well as about difficult experiences of soldiers and officers who were guarding our country's eastern border in 2021 during the Russian-Belarusian operation 'Sluice'.

The geopolitical situation in Central and Eastern Europe, which is heavily influenced by the armed conflict in Ukraine, is creating new demands on threat response systems, including CBRNE (chemical, biological, radiological, nuclear and explosive). CBRN mobile laboratories, with which the State Fire Service has been equipped play an important role in ensuring safety in Poland. Grzegorz Bugaj, PhD Eng., analysed operational effectiveness of these laboratories in accordance with the relevant legislation and the principles of the National Firefighting and Rescue System. He also identified the challenges and limitations associated with their use. One such challenge is recruiting and retaining the highly skilled staff needed to operate such technologically advanced solutions.

Radosław Wiśniewski, PhD and Denis Tomala write about the need to ensure that uniformed services have an optimal number of well-trained personnel, enabling them to carry out their tasks to a sufficiently high standard. They present the results of research into Border Guard officer retention. The researchers sought answers to questions regarding the extent to which individual and organisational factors influence whether officers leave or remain in the service, and what solutions might not only increase interest

in a career in the Border Guard – and in uniformed services in general – but also optimise the conditions for serving for many years. Having experienced staff on the team, among many other benefits, ensures that the staff succession process runs smoothly. The insights gained from the research presented enable us to refine our internal human resources practices and enhance the stability of our formation, as well as state security. It is well worth reading.

The article by Major Mariusz Domżalski, PhD, deals with the issue of human resources policy, but within the Polish Armed Forces. He discusses matters relating to the prohibition on undertaking paid employment and carrying out business activities by a professional soldier. It should be borne in mind that the labour market is becoming increasingly complex and new forms of employment are emerging. As the author rightly points out, this may require a clearer definition of the concept of paid employment and the adoption of implementing regulations concerning occupational restrictions for persons serving in uniformed formations.

Norbert Łucarz describes the operation 'Sluice' and the migrants instrumentalisation practice in the policies of the Russian Federation and the Republic of Belarus. As a result of this operation, Polish uniformed services guarding the Polish-Belarusian border became the target of aggression from migrants and Belarusian officers supporting them. The operation 'Sluice' was accompanied by hostile propaganda and disinformation activities – narratives emerged in which Polish security services were presented in an extremely negative light. The result of these actions was growing polarisation among the Polish society. One expression of opposition to these events was the 'United behind the Polish uniform' campaign. Its aim was to express support for people who, in the course of their duties, had to cope with intense physical and mental strain.

Agata Rytel also writes about attacks on the integrity of the Polish border with Belarus, addressing the issue of hybrid operations carried out by the Russian Federation, which in 2021 – 2024 were directed at the Polish information sphere and cyberspace. The author shows that these events were directly linked to the war in Ukraine and constituted deliberate interference by Russia and Belarus. This is yet another example of the complex nature of modern cyberattacks, in which the attacker combines various types of activities and carries them out across multiple domains.

One of the most common targets of attacks is financial sector. Associate Professor Kamil Mroczka and Paweł Piekutowski write about enhancing the digital resilience of entities in this sector in light of the obligations arising from the DORA (Digital Operational Resilience Act) regulation. They point to TLPT (threat-led penetration testing) tests, as an effective method of strengthening this resilience. The aim of these tests is to replicate real-world attack scenarios as closely as possible, in order to precisely identify vulnerabilities in an organisation's cyber security system and improve its ability to detect cyber threats. The authors believe TLPT tests are essential, as they enable the verification not only of technical measures but also of staff behaviour.

The issue of resilience testing also features in Klaudia Maciata's article on offshore wind farms, which are vital to the country's energy security. Their specific location increases their vulnerability to hybrid threats, including in cyberspace. It is therefore necessary to conduct multi-faceted resilience testing of these farms. In the cyber domain, this will include, among other things, red teaming exercises, i.e. simulated attacks that replicate the tactics and techniques used by cybercriminals. According to the author, legal, technological and organisational measures must be combined in order to improve the safety of wind farms.

The emergence of artificial intelligence has a significant impact on the development of cyber threats. This is discussed in an article by Jakub Gajecki. Advances in AI and machine learning have made threats more complex, dynamic and difficult to detect. In this context, the author analyses and evaluates the existing defence strategies. He points to the role of international cooperation in combating cybercrime and the need to keep regulations up to date. Most of them were developed at a time when AI technologies were not yet being used in cyber operations on such a large scale.

This issue also features a topic of significance for crisis management and defence of the Republic of Poland concerning the safeguarding of the continuity of state functioning.

In the 'Competition entries' section, we present the text by David Cybulski on the government connectivity and communication in the event of a national security threat. The implementation of the System of Secure State Communication supervised by the minister responsible for internal affairs is expected to lead

to a reduction in response times of the administration and security services, as well as to improve rescue in crisis situations.

'Internal Security Review' is a periodical of a counterintelligence-oriented special service, it could hardly omit a reference to issues revolving around Article 130 of the Criminal Code. Tomasz Safjański, PhD, reviewed for us the monograph entitled *Szpiegostwo. Studium kryminologiczne* (Espionage. Cryminology study). Its author, Associate Professor Piotr Chlebowicz, undertook a comprehensive criminological analysis of the phenomenon of espionage in Poland between 1990 and 2022. This publication is a summary of his many years of research based on file and archival research, informal interviews and literature on the subject. According to the reviewer, this is outstanding work and should become required reading for criminologists, criminal lawyers, analysts, as well as politicians and others responsible for national security. I also encourage you to read this unique book!

To conclude, I would like to thank the authors, reviewers, members of the Academic Editorial Board and the editorial team for co-creating the journal I lead. It is both a pleasure and a responsibility for me. I believe that the topics we address are interesting to you, and that our contribution to the popularisation of security issues is both needed and recognised.

Editor-in-Chief
Daria Olender, PhD

ARTICLES

Internal Security Review
2026, no. 34, pp. 237–258

https://doi.org/10.4467/20801335PBW.26.011.23373

ARTICLE

Threat-led penetration testing (TLPT) – a new approach to testing digital resilience of financial entities in Poland in the perspective of requirements under the Digital Operational Resilience Act (DORA)

KAMIL MROCZKA

Faculty of Political Science and International Studies,
University of Warsaw

https://orcid.org/0000-0003-3809-3479

PAWEŁ PIEKUTOWSKI

Cybersecurity Department,
Polish Financial Supervision Authority

https://orcid.org/0009-0001-5861-7367

Abstract

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA) launched a new model for testing the digital resilience of financial services operating in the Polish financial market into the EU and thus into the domestic legal framework. The primary purpose of this article is to discuss and evaluate the Threat-Led Penetration Testing (TLPT) model. TLPT tests can include both technical and sociotechnical components. The hypothesis of the article is that

TLPT testing will have a positive impact on enhancing the digital resilience of financial stakeholders because these tests are designed to simulate real-world cyber attacks, enabling organisations to understand their resilience to threats and initiate relevant countermeasures. The results obtained from the analysis confirm the validity of the proposed research hypothesis. This follows from the fact that the main premise of TLPT testing is to replicate real-world attack scenarios as accurately as possible, thereby enabling a more reliable and detailed assessment of organisation's security level. The authors emphasise that such an approach allows not only for the verification of the effectiveness of information system safeguards, but also for the evaluation of the resilience of operational processes and the level of employee awareness regarding cyber threats.

Keywords TLPT tests, DORA, Polish Financial Supervision Authority, digital resilience, cybersecurity

Introduction

Information and communication technologies (ICT) are present in almost every area of the functioning of states and their economies[1]. They provide real support for complex systems used in everyday activities. These technologies drive the Polish economy and its most important sectors, including the financial sector, and strengthen the functioning of the European Union's internal market. The increasingly dense network of interconnections between financial market stakeholders, financial service providers, and customers, together with the ongoing digitisation of financial systems, increases vulnerability to various types of risk, including those resulting from cyber threats and disruptions to the functioning of ICT. It is therefore essential to take measures to increase the digital resilience of financial entities.

Recital 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial

[1] The article draws on a publication by one of the authors prepared for the purposes of implementing the DORA regulation. See: *Testy TLPT – nowe podejście do testowania cyfrowej odporności Organizacji* (Eng. TLPT testing – a new approach to testing digital resilience of organisation), Komisja Nadzoru Finansowego, 14 VII 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [accessed: 9 II 2026].

sector (hereinafter: DORA Regulation)[2] clearly emphasises that (…) *The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities*. The literature rightly points out that the DORA regulation in force since January 2025 has obliged financial entities and external ICT service providers to apply best practices in the field of cybersecurity. Threat-led penetration testing (TLPT) has been identified as one of the advanced measures leading to increased digital resilience of financial entities. They will be used to assess the cybersecurity status of these entities[3].

Without going into an in-depth analysis of the meaning of the term 'threat-led penetration testing' at this point, it should be emphasised that it is a cybersecurity assessment technique used to simulate realistic cyberattack scenarios targeting an organisation's critical systems and infrastructure. Unlike traditional penetration tests, which may be based on a standard list of vulnerabilities, TLPT method focuses on mimicking specific actors, techniques and tactics that are most likely to occur in an organisation due to its unique risk profile. TLPT tests are conducted to identify weaknesses, verify existing security measures, and enhance the organisation's ability to detect, respond to real cyber threats, and recover data[4].

The main aim of the article is to critically analyse TLPT model as an instrument for assessing the digital resilience of financial entities in Poland in the context of the requirements of the DORA regulation, with particular empahasis on the differences between TLPT tests and classic penetration tests, the role of supervisory authorities and the implications for implementation.

The authors of the article adopted the following hypothesis: TLPT tests should have a positive impact on increasing the digital resilience of financial entities. They are designed to mimic real cyber attacks, which enables organisations to understand their resilience to threats and take appropriate corrective actions.

For the purposes of this study, the comparative law method, institutional analysis and critical analysis of scientific literature were used. Participant observation based on professional experience of the authors was also applied. The methods indicated the role and competences of entitites responsible for financial market cybersecurity, identified differences in approaches to digital resilience testing,

---

[2] *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.*

[3] M.L. Dozsa*, Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, master's thesis, Oslo 2024, p. ii.

[4] B. Riaz, Z. Younas, *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024, p. 26.

assessed the degree of regulatory harmonisation, and highlighted areas where the Polish model of financial market cybersecurity supervision may need to be clarified or further developed.

TLPT testing – definition

When defining TLPT testing, cybersecurity experts empasise that this is (…) *an advanced form of penetration testing that goes beyond the standard approach, simulating real cyber attacks using tactics, techniques and procedures (TTP) employed by real cybercriminals. Unlike traditional penetration testing, TLPT focuses on analysing the specific threats to which an organisation is exposed, tailoring attack simulations to its specific risk profile*[5].

The legal definition of TLPT tests is contained in Article 3 point 17 of the DORA regulation. According to this provision the testing means (…) *a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems*[6].

Penetration testing and TLPT testing – the most important differences

The main objective of the tests is to assess the institution's actual resilience to threats and possible attack scenarios. The penetration test focuses more on identifying technical vulnerabilities and configuration errors in IT systems.

To be more specific, the following differences can be identified:

1) scope of test implementation – penetration tests typically focus on specific elements of the IT infrastructure – individual systems, applications or network components. Their primary goal is to detect technical vulnerabilities in a defined area. This approach allows for an assessment of the security of a specific system, but does not provide a complete picture of how an organisation would cope with a complex cyber attack. TLPT testing takes a much broader approach. It covers not only systems

[5] *Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA* (Eng. TLPT tests – digital resilience of organisations in accordance with the DORA regulation), Bankowe ABC, 2 I 2025, https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [accessed: 19 IV 2025].

[6] See also: J. Kurek-Sobieraj, Komentarz do art. 3 (Eng. Commentary on Article 3), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 85–86.

and technologies, but also operational processes and people. The aim is to examine the organisation's entire cyber defence ecosystem and answer questions like: how does security monitoring work? How does internal communication work? How does the team respond to incidents? What are the escalation paths? TLPT testing allows you to see whether your organisation is prepared for an attack not only in theory but also in practice. This makes it possible to increase the resilience of the entire 'organism' rather than just a single element;

2) attack scenarios – penetration tests are mainly based on known vulnerabilities and focus more on identifying potential threats in a specific IT system. TLPT tests are implemented on the basis of scenarios developed by a special threat intelligence team. It is intended to identify the most realistic cyber threats and attack scenarios that a given organisation may face. These scenarios may be based on reports concerning general analysis of cyber threats (generic threat intelligence) for a given sector. The report published by the Computer Security Incident Response Team of the Polish Financial Supervision Authority (KNF CSIRT) describes the potential types of attacks, categories of adversaries, and trends in cyber attacks[7]. It places great emphasis on the potential development of threats related to the use of techniques and tools based on artificial intelligence, as well as the dangers resulting from attacks on supply chains. Other important aspects include the intensification of ransomware attacks, increasingly carried out in the ransomware as a service model, and the development of hacktivism, which has gained momentum since the outbreak of war in Ukraine;
3) test environment and risk approach – penetration tests are usually carried out in appropriate test environments to avoid disruptions to system operations. TLPT tests place great emphasis on comprehensively examining the actual level of security within an organisation, which is why they are carried out in production environments. This means additional risk associated with the possibility of disrupting the continuity of systems and business processes. Therefore, during TLPT testing, it is necessary to conduct a risk analysis to mitigate any disruptions that may arise during implementation;
4) test procedure and confidentiality – a characteristic feature of TLPT tests is the requirement to keep them secret from most organisations. Only a small

[7] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025* (Eng. The cyber threat landscape in the Polish financial sector 2025), CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 19 I 2026].

group of employees are aware of their implementation. The intention is to verify the organisation's response to cyber threats. Not only is the digital resilience of ICT systems examined, but also the preparedness of security teams and the functioning of relevant processes within the organisation. Maintaining test confidentiality is a major challenge for the organisation due to the complexity of many business processes;

5) results and reporting – an important element of TLPT tests are purple team exercises, which take place after the attack phase. These are exercises in which the team simulating attacks and the team responsible for defence jointly discuss the scenarios carried out, identify weaknesses in the processes and systems as well as develop solutions to increase the organisation's cyber resilience. Then, a corrective action plan is prepared;
6) test frequency – penetration tests can be performed more frequently. TLPT tests are performed much less frequently due to their complexity and costs.

Obligation to test the digital resilience of financial entities in light of Article 26 of the DORA regulation

The DORA regulation obliges financial entities (with certain exceptions specified in Article 16(1), first paragraph of the DORA regulation) to conduct TLPT tests at least every three years. However, based on the risk profile of the financial entity concerned and taking into account the operational circumstances, the competent authority may, if necessary, request that entity to reduce or increase the frequency of TLPT testing. The literature states that this may occur if (…) *the competent authority has reasonable grounds to suspect that there has been improper risk management within the organisation (e.g. due to the appearance of offers to sell the organisation's data on the black market)*[8].

Paragraph 2 of the aforementioned provision is extremely important from the perspective of quality requirements. It states that: *each threat-led penetration test shall cover several critical or important functions of a financial entity or all such functions, and shall be performed on live production systems supporting such functions.* The first step towards conducting reliable TLPT tests is to identify all relevant base systems. Financial entities should then determine all ICT processes

[8] C. Cichocki, *Komentarz do art. 26* (Eng. Commentary on Article 26), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, p. 280.

and technologies that support critical or important functions. The final step is to determine which ICT services, including systems, processes and ICT technologies supporting critical or essential functions and services, have been outsourced to external ICT service providers or are covered by a contract with such providers.

The doctrine rightly emphasises that the professional process of gathering this information and data requires business knowledge about the functioning of the organisation and its translation into technological and technical knowledge. Various ICT tools can be used for such activities, e.g. CMDB systems (computer management database)[9]. In practice, the study may cover all or only selected systems or functionalities. Taking into account the high level of interdependence of systems and ICT tools across financial entities, comprehensive research is recommended. Based on the information and data obtained from the analysis, these entities are required to assess which critical or significant functions should be covered by TLPT tests. This assessment shall be approved by the competent authorities. In the Polish legal order this is the Polish Financial Supervision Authority (KNF), which will be discussed later in the article.

Where the scope of TLPT includes external ICT service providers, the financial entity shall take the necessary measures and safeguards to ensure that they participate in the tests and shall remain fully responsible for ensuring compliance with the DORA regulation at all times. This requirement is critically important in the context of how financial entities operate, as they all use the services of external suppliers.

The EU legislator, aware of the scale of ICT service providers' operations, introduces certain derogations from the general rule of their participation in TLPT tests. In accordance with the wording of Article 26(4) of the DORA regulation:

> (…) where the participation of an ICT third-party service provider in TLPT (…) is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services.
>
> That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT

[9] Ibid.

third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities participating in the pooled testing.

The number of financial entities participating in such testing shall be appropriately adjusted and take into account the complexity and type of services covered. After the tests have been completed, the reports and corrective action plans have been agreed upon, the financial entity and, where applicable, the external testers shall submit to the competent authority a summary of the findings, the corrective action plans and documentation demonstrating that the tests have been carried out in accordance with the requirements of the Regulation. On this basis, the competent authorities issue a certificate to the financial entities confirming that the tests have been carried out in accordance with the requirements set out in documentation. It enables authorities to mutually recognise TLPT tests, but does not exempt financial entities from responsibility for the results of these tests.

Financial entities were required to conclude agreements aimed at carrying out TLPT tests. If financial entity has internal testing teams, the DORA regulation requires that such tests be performed by an external tester every three tests, i.e. at least every nine years. An exception to this rule applies to credit institutions classified as significant in accordance with Article 6(4) of the Council Regulation (EU) No. 1024/2013[10]. These entities are obliged to use only external testers.

The DORA regulation also defines the criteria used by the competent authorities to determine which entities are subject to TLPT testing. The assessment takes into account:

- impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector,
- possible financial stability concerns, including the systemic character of the financial entity at Union or national level,
- specific ICT risk profile, level of ICT maturity of the financial entity or the applied technological solutions.

Synthesising the objective and subjective analysis of Article 26 of the DORA regulation, it should be noted that this provision gives Member States the possibility to designate a single public authority in the financial sector which will be responsible at national level for matters relating to TLPT testing in this sector. This authority is entrusted with all competences and tasks in this area.

[10] *Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions,* p. 63.

Requirements for external and internal testers

Article 27 of the DORA regulation defines the basic requirements for testers conducting TLPT tests. Paragraph 1 of this provision stipulates that financial entities shall only use the services of external testers who:

a) are of the highest suitability and reputability;
b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;
c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;
d) provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and mitigation of the business risks of the financial entity;
e) are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

The doctrine rightly emphasises that (…) *the accuracy and reliability of TLPT tests is considered crucial by the legislator, as individual financial organisations should trust the certificates presented by other entities in the industry. The level of trust in external and internal testers is also important for the competent supervisory authority*[11].

EU law permits the use of internal testers. However, the legislator imposes additional requirements, apart from those mentioned above in relation to external testers. Article 27(2) of the DORA regulation stipulates that financial entities using internal testers shall ensure that the following conditions are met:

a) such use of internal testers has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);
b) the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test; and
c) the threat intelligence provider is external to the financial entity.

Article 27(3) of the DORA regulation draws attention to issues of information and data security arising from TLPT testing. Financial entities are required to ensure that contracts concluded with external testers oblige those testers to (…) *a sound*

[11] C. Cichocki, Komentarz do art. 27 (Eng. Commentary on Article 27), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, p. 284.

management of TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the financial entity.

Cezary Cichocki rightly points out that the data obtained as a result of TLPT tests should be treated as particularly sensitive, given that if it (…) *falls into the wrong hands, it will serve as a kind of guide to vulnerabilities in the financial organisation's systems and make it much easier for a potential intruder to launch an attack. The risk of disclosing this data lies in the fact that there may be a time lag between the disclosure of threats in TLPT tests and their mitigation, which could become a window of opportunity for attack if the test data is disclosed to unauthorised persons*[12].

Testing the digital resilience of financial entities under national law

The DORA regulation created a new regulatory environment for financial entities and the Polish Financial Supervision Authority, as the body responsible for supervising compliance. The provisions of the regulation are applied directly, but some of them require changes to the national legal system, especially with regard to the designation of competent authorities and the imposition of obligations on financial entities[13].

The first draft act implementing the aforementioned EU regulations was submitted by the Minister of Finance in April 2024[14]. The legislative process took over a year, which raises questions in the context of the urgency of introducing this regulation. The tardiness of decision-makers led the European Commission to call on Poland and 12 other EU countries at the end of March 2025 to fully implement the DORA regulation within national legal systems[15]. The government legislative process was completed in April 2025. The draft law amending certain laws in connection with ensuring the operational digital resilience of the financial

[12] Ibid., p. 285.

[13] *Ustawa wdrażająca DORA do prawa polskiego* (Eng. Act implementing DORA into Polish law), "Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [accessed: 12 IV 2025].

[14] *Draft law amending certain laws in connection with ensuring the operational digital resilience of the financial sector and the issuance of European Green Bonds*, print no. UC11, Rządowe Centrum Legislacji, Warszawa 2025.

[15] The list of countries that have not implemented the regulation also includes: Belgium, Bulgaria, Denmark, Greece, Spain, France, Lithuania, Latvia, Malta, Portugal, Romania and Slovenia.

sector has been approved by the Standing Committee of the Council of Ministers. The act implementing the DORA regulation was passed in June 2025[16].

From the perspective of the purpose of this article, the most important changes concern the introduction of Article 18zk to the *Act of 21 July 2006 on financial market supervision*. This provision regulates the tasks of the Polish Financial Supervision Authority concerning the performance of the tests referred to in Article 26 of the DORA regulation and the procedure to be followed by financial entities obliged to perform them. Pursuant to this provision, the supervisory authority became the authority responsible for performing the duties of the competent authority specified in Article 26 and Article 27 of the DORA regulation. In the light of the above, the Polish Financial Supervision Authority has been granted the statutory power to designate, by way of a decision, the financial entity responsible for conducting TLPT tests. Article 18zk replicates the criteria for selecting entities obliged to carry out these tests, taking into account the principle of proportionality (Article 4(2) of the DORA regulation).

Entities to which the Polish Financial Supervision Authority has issued the aforementioned decision are obliged to submit to the supervisory authority, for approval, the result of the assessment carried out in accordance with Article 26(2) paragraph three of the DORA regulation. This result indicates which critical or important functions should be covered by TLPT tests. After conducting them, agreeing on reports and corrective action plans, the financial entity and, where applicable, the external testers shall be required to submit to the Polish Financial Supervision Authority a summary of the findings, corrective action plans and documentation confirming that TLPT tests have been conducted in accordance with the requirements of the DORA regulation. It will be the supervisory authority's responsibility – in the light of Article 18zk(4) – to confirm this compliance. This is to enable mutual recognition of penetration tests by the relevant authorities.

The Polish Financial Supervision Authority has also been granted powers to reduce or increase the frequency of TLPT testing and the authority to approve financial entity's intention to use the services of internal testers. It is also responsible for verifying that internal testers meet the requirements of the DORA regulation. The fulfilment of this obligation – in light of the vague requirements of Article 27 of the DORA regulation – may cause significant problems. However, it can be assumed that it is in the interest of financial entities to ensure the appropriate quality of resources for conducting TLPT tests. The quality of these tests increases

[16] *Act of 25 June 2025 on amendments to certain acts in connection with ensuring the operational digital resilience of the financial sector and the issuance of European green bonds.*

the level of digital resilience and, consequently, the broadly understood security of financial entity.

Regulatory technical standards in the field of TLPT testing

In Article 26(11) of the DORA regulation, the EU legislator decided that the European Supervisory Authorities (ESA), in consultation with the European Central Bank, would develop common draft regulatory technical standards (RTS)[17] in accordance with the European framework for threat intelligence-based ethical red teaming (TIBER-EU). The following elements are to be clarified in the RTS:

- criteria used for the purpose of the application of paragraph 8, second subparagrap of the DORA regulation,
- criteria defining the methods of identification and notification of entities obliged to perform TLPT tests,
- roles and responsibilities of individual teams participating in tests,
- requirements and standards governing the use of internal testers,
- requirements in relation to:
  - scope of TLPT,
  - testing methodology and approach to be followed for each specific phase of the testing process,
  - testing stages relating to results, test closure and corrective measures,
- the type of supervisory cooperation and other relevant cooperation which are needed for the implementation of TLPT tests, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State. This is to enable appropriate level of supervisory involvement and a flexible implementation taking into account specificities of financial sub-sectors or local financial markets.

In July 2024, the ESA presented the RTS consultation final report on TLPT[18].

[17] Regulatory technical standards impose detailed technical requirements for the implementation of regulations. They are more prescriptive and focus on the practical aspects of implementing the DORA regulation. In turn, implementing technical standards (ITS) are responsible for the harmonisation and standardisation of the processes for implementing these provisions in the EU and are more procedural in nature. They focus much more on the appropriate way of reporting to the relevant supervisory authorities.

[18] *Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554*, European Banking Authority, 17 July 2024.

TLPT and TIBER-EU tests

Before discussing the interdependencies between TLPT and TIBER-EU tests[19], it is necessary to briefly characterise the assumptions of this document. The TIBER-EU framework was established in 2018 by the European Central Bank in order to systematise and standardise the approach and implementation of realistic penetration tests in organisations from the financial sector of EU Member States[20]. TIBER-EU defines a model for red team tests/operations preceded by reconnaissance and analysis of data on threats targeting the tested entity. It is the foundation of the requirements for TLPT tests. In the initial stage there were differences between the assumptions of this document and the requirements specified in the DORA regulation. The main one concerned the approach to conducting tests with the participation of internal testers. TIBER-EU did not initially allow for this solution, and in TLPT tests it is acceptable provided that certain criteria are met. The TIBER-EU framework was updated in 2025 and its current version reflects the requirements arising from the DORA regulation[21]. It can therefore be considered that the current TIBER-EU is a textbook for TLPT tests. While the DORA regulation specifies what must be done in TLPT tests, TIBER-EU indicates how it should be done.

The TIBER-EU framework also allows for local implementation to better suit the specific nature of a given country[22]. As of April 2025, among those who decided to implement were: Austria, Belgium, the Netherlands, France, Germany, Denmark, Finland, Sweden and Norway.

---

[19] On the topic of TIBER-EU assumptions, see more: T. Valkeasuo, *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023; M. Bayle de Jessé, *The Eurosystem's cyber resilience strategy for financial market infrastructures*, "Cyber Security: A Peer-Reviewed Journal" 2019, vol. 2, no. 4, pp. 294–302. https://doi.org/10.69554/DFBJ2963; B.F. Scott, *Red teaming financial crime risks in the banking sector*, "Journal of Financial Crime" 2021, vol. 28, no. 1, pp. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

[20] *TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym* (Eng. TIBER-EU and DORA as an opportunity to build real cyber resilience in the financial sector), Z-LABS, 8 VII 2024, https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [accessed: 19 IV 2025].

[21] *TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [accessed: 9 II 2026].

[22] *Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce* (Eng. Implementations of the TIBER-EU framework in Europe and implementation in Poland), Komisja Nadzoru Finansowego, 27 I 2025, https://www.knf.gov.pl/?articleId=91971&p_id=18 [accessed: 19 IV 2025].

TIBER-EU documentation includes numerous studies that may be useful during the implementation of both TLPT and TIBER-EU tests. The most important are:

- *TIBER-EU Guidance for Service Provider Procurement*[23] – a collection of best practices in the implementation of red team and threat intelligence provider service procurement processes,
- *TIBER-EU Purple-Teaming Guidance*[24] – a collection of best practices for conducting purple team exercises that take place after red team testing,
- *TIBER-EU Scope Specification Document Guidance*[25] – guidelines for the appropriate selection of the scope of tests,
- *TIBER-EU Test Summary Report Guidance*[26] – guidelines on preparing a test summary report.

Main principles of TIBER-EU:

- tests based on real threats (threat intelligence) – test scenarios that take into account current threat intelligence,
- simulation of real attacks (red teaming) – a controlled test in which red team simulates the actions of cybercriminals,
- protection of critical functions – verification of resistance to attacks on key business functions,
- cooperation and consent – financial institution voluntarily agrees to participate in the tests,
- standardisation and possibility of implementation in various EU countries – a framework model adapted at the national level,
- learning and improvement – the analysis and learning (lessons learned) phase as an important TIBER-EU element.

[23] *TIBER-EU Guidance for Service Provider Procurement*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [accessed: 19 IV 2025].

[24] *TIBER-EU Purple Teaming Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [accessed: 19 IV 2025].

[25] *TIBER-EU Scope Specification Document Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [accessed: 19 IV 2025].

[26] *TIBER-EU Test Summary Report Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [accessed: 19 IV 2025].

TLPT teams

As already mentioned, TLPT tests are highly complex. They require various competencies and skills from team members. It is very important to precisely define the roles, responsibilities, and duties of the people and teams involved. This increases the chance that every aspect of the test will be well managed and that subsequent activities will be carried out according to the agreed schedule. Precise definition and assignment of roles means better coordination of activities, minimisation of the risk of errors, as well as quick identification and appropriate addressing of any problem.

The basic model of division of roles, responsibilities and duties assumes the existence of the following teams:

- TLPT cyber team (TCT),
- control team (CT) also known as white team,
- blue team (BT),
- threat intelligence provider (TIP),
- red team (RT),
- purple team (PT).

TLPT cyber team – is appointed by the authorised test supervisory authority. The team is responsible for monitoring and assessing the correctness of the tests, as well as their reliable and secure execution. The team should also ensure that all aspects of the test are carried out according to plan, minimising the risk of errors and irregularities.

Control team (white team) – plays a key role as it is responsible for coordinating the implementation of tests on the financial entity's side – planning, monitoring and managing all aspects of them. Senior managers and experts with knowledge of the organisation's infrastructure and operational processes participate in CT's work. The team is also responsible for protecting the integrity and stability of production systems during testing. It is the only team that has information about the details of the tests, which allows it to objectively assess the organisation's employees' responses to simulated threats.

Blue team – is responsible for managing internal cybersecurity of the organisation and ensuring its appropriate level. The main task of the team is to monitor and respond to potential threats in real time, as well as to maintain the protection of systems and data against cyber attacks. This team is is not kept informed of the details of ongoing testing, allowing simulations to be conducted in conditions as close to real-world conditions as possible. This allows to assess organisation's response to threats and test the effectiveness of existing procedures and defence mechanisms, thereby gaining a better understanding of the organisation's actual level of preparedness for incidents related to ICT.

Threat intelligence provider – is responsible for gathering information about threats to the organisation, using methods such as OSINT (open source intelligence). It collects intelligence data, analyses available public sources and other sources of information to create a comprehensive picture of the threats that may affect the organisation. TIP team is tasked with providing accurate and up-to-date information to help develop realistic scenarios for attacks carried out by RT. This ensures that the tests are better aligned with the threats that the organisation may face.

Red team – performs security tests in accordance with accepted and approved scenarios, using information, materials and data provided by TIP. The main task of RT is to simulate real attacks on organisation's systems in order to assess how effectively they can detect and respond to threats. Both technical and organisational security measures are tested. A holistic approach should enable the identification of potential weaknesses and gaps in the organisation's security. Red team uses various techniques and methods of attacks to make the tests as realistic and effective as possible. The reliability of the test results depends on the quality of the RT work. The higher the quality, the greater the chance of eliminating potential threats, mitigating identified risks and strengthening the level of security in the context of the functioning of the organisation.

Purple team – consists of members of RT and BT teams. The task of PT is to analyse the results obtained from the tests, identify areas for improvement and formulate recommendations that will help strengthen the organisation's security. Due to the cooperation of both teams, it is possible to more accurately assess the effectiveness of existing defence mechanisms and propose specific actions to improve both technical and procedural aspects of security.

TLPT implementation stages

Due to the complex and multifaceted nature of TLPT tests, they are carried out in three consecutive stages: preparation for testing, testing and summary. This approach increases the chances of conducting a reliable and in-depth assessment of the organisation's resilience to various types of threats.

In the first stage, i.e. the preparatory stage, the following activities are carried out:

- preliminary meetings between the entity conducting the tests and the supervisory authority and the TCT team to discuss and agree on the details of the tests, including the objectives, methodology and assessment criteria;

- defining the scope of the tests, i.e. the areas to be tested and potential threats to be considered. This step also involves setting the test objectives and expected results;
- procurement processes to select the appropriate RT and TIP teams. The selection of these teams is crucial to ensuring high-quality testing and realistic attack scenarios;
- preparing documentation specifying all aspects of the tests, including the schedule, communication rules, and safety procedures. This documentation provides the basis for subsequent testing stages and confirms that all parties agree on expectations and responsibilities.

The second stage during which the main testing activities are carried out includes:

- preparation of TTI (targeted threat intelligence) report and attack scenarios – TIP team provides a report regarding targeted TTI threats and preliminary attack scenarios. This report contains detailed information on potential threats and attack vectors that may affect organisation. On this basis TIP team creates realistic attack scenarios that will be used in further testing;
- RT conducts tests based on scenarios developed by TIP team, which allows for a thorough assessment of the resilience of the organisation's systems and procedures. Red team uses various techniques and methods of attacks to test how effectively the organisation deals with threats.

The third stage involves summarising and analysing the test results obtained, as well as developing recommendations. It consists of:

- preparation of reports by RT and BT teams. They include analyses of results, description of attack scenarios carried out, as well as assessment of the effectiveness of responses and defences. These documents are the basis for further analysis and conclusions regarding the organisation's security;
- conducting purple teaming workshops, during which RT and BT teams discuss past attack scenarios in order to exchange information and experiences. This allows for a better understanding of the effectiveness of the tests and identification of areas for improvement, as well as helping to develop practical recommendations and improvement plans;
- preparation of final report on the implementation of TLPT based on the reports from RT and BT teams as well as workshop results. It includes a summary of all activities carried out, conclusions from the tests, and recommendations for improving security. This document is submitted to the organisation and forms the basis for implementing security changes.

Summary and conclusions

As shown in the article, the basic premise of TLPT tests is to replicate real attacks as accurately as possible. This makes it possible to check not only the effectiveness of IT system security measures, but also the security level of operational processes and employee awareness of cyber threats, which increases the accuracy of assessing the resilience of organisation's systems and procedures. However, due to the complexity and diversity of TLPT tests, their implementation may pose a challenge for organisation. They require careful preparation and appropriate procedures to ensure both the effectiveness of the tests and the safety of the organisation during their implementation.

The analysis conducted for the purposes of this article leads to the conclusion that the implementation of TLPT tests as a standard for financial entities was a step in the right direction. There is no doubt that in a complex digital environment, it is necessary to develop effective risk management mechanisms based on real factors and challenges, and not only those defined for the purposes of building appropriate models. The authors share the position of the European Central Bank, which emphasises that TLPT tests allow for the verification not only of technical means, but also of personnel and processes. This bank rightly points out that (…) *the results of these tests can significantly increase the security awareness of the senior management within the entities being tested*[27]. Wojciech Dworakowski is also right when he points out that TLPT is an investment in security that pays off, because it is better to be proactive than to repair the damage caused by a cyberattack[28].

In the coming years, it will be crucial to ensure consistent and proportionate application of TLPT tests across the EU financial sector. Financial supervision should take advantage of this opportunity to support entities in preparing for these tests and in developing their capabilities to defend themselves against cyber attacks. Verifying the organisation's resistance using realistic attack scenarios should significantly contribute to improving the cyber resilience of the entire financial market.

---

[27] *Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (CON/2021/20)*, p. 1.

[28] W. Dworakowski, *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?* (Eng. Threat-Led Penetration Testing (TLPT) – How to be DORA compliant in 2025?), Securing, 28 II 2025, https://www.securing.pl/en/threat-led-penetration-testing-tlpt-how-to-be-dora-compliant-in-2025/ [accessed: 18 IV 2025].

Bibliography

Bayle de Jessé M., *The Eurosystem's cyber resilience strategy for financial market infrastructures*, "Cyber Security: A Peer-Reviewed Journal" 2019, vol. 2, no. 4, pp. 294–302. https://doi.org/10.69554/DFBJ2963.

Cichocki C., Komentarz do art. 26 (Eng. Commentary on Article 26), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 276–282.

Cichocki C., Komentarz do art. 27 (Eng. Commentary on Article 27), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 283–286.

Dozsa M.L., *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, master's thesis, Oslo 2024.

Kurek-Sobieraj J., Komentarz do art. 3 (Eng. Commentary on Article 3), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 69–106.

Riaz B., Younas Z., *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024.

Scott B.F., *Red teaming financial crime risks in the banking sector*, "Journal of Financial Crime" 2021, vol. 28, no. 1, pp. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

Valkeasuo T., *TIBER-EU Preparation Phase Framework Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023.

Internet sources

Dworakowski W., *Threat-Led Penetration Testing (TLPT) – How to be DORA compliant in 2025?*, Securing, 28 II 2025, https://www.securing.pl/en/threat-led-penetration-testing-tlpt-how-to-be-dora-compliant-in-2025/ [accessed: 18 IV 2025].

Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce (Eng. Implementations of the TIBER-EU framework in Europe and implementation in Poland), Komisja Nadzoru Finansowego, 27 I 2025, https://www.knf.gov.pl/?articleId=91971&p_id=18 [accessed: 19 IV 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025 (Eng. The cyber threat landscape in the Polish financial sector 2025), CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 19 I 2026].

Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA (Eng. TLPT tests – digital resilience of organisations in accordance with the DORA regulation), Bankowe ABC, 2 I 2025, https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [accessed: 19 IV 2025].

Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji (Eng. TLPT tests – a new approach to testing the digital resilience of organisation), Komisja Nadzoru Finansowego, 14 VII 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [accessed: 9 II 2026].

TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [accessed: 9 II 2026].

TIBER-EU Guidance for Service Provider Procurement, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [accessed: 19 IV 2025].

TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym (Eng. TIBER-EU and DORA as an opportunity to build real cyber resilience in the financial sector), Z-LABS, 8 VII 2024, https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [accessed: 19 IV 2025].

TIBER-EU Purple Teaming Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [accessed: 19 IV 2025].

TIBER-EU Scope Specification Document Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [accessed: 19 IV 2025].

TIBER-EU Test Summary Report Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [accessed: 19 IV 2025].

Ustawa wdrażająca DORA do prawa polskiego (Eng. Act implementing DORA into Polish law), "Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [accessed: 12 IV 2025].

Legal acts

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Official Journal of the EU L 333 of 2022, as amended).

Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (Official Journal of the EU L 287 of 2013).

Act of 25 June 2025 on amendments to certain acts in connection with ensuring the operational digital resilience of the financial sector and the issuance of European green bonds (Journal of Laws of 2025, item 1069).

Act of 21 July 2006 on financial market supervision (consolidated text, Journal of Laws of 2025, item 640, as amended).

Other documents

Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554, European Banking Authority, 17 July 2024.

Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (CON/2021/20) – (Official Journal of the EU C 343/1 of 2021).

Draft law amending certain laws in connection with ensuring the operational digital resilience of the financial sector and the issuance of European Green Bonds, print no. UC11, Rządowe Centrum Legislacji, Warszawa 2025.

Assoc. Prof. Kamil Mroczka

Post-doctoral degree in social sciences in the field of political science and administration, assistant professor in the Department of State and Public Administration at the Faculty of Political Science and International Studies of the University of Warsaw, graduate of the Executive MBA programme. He has many years of experience in managerial positions in public administration and in the private sector. He is currently employed as Chief Compliance Officer at Santander Bank Poland.

Contact: ks.mroczka@uw.edu.pl

Paweł Piekutowski

Graduate of the Military University of Technology in Warsaw. He has many years of professional experience in the field of cybersecurity, particularly in the area of penetration testing. He currently serves as Deputy Director of the Cybersecurity Department at the Polish Financial Supervision Authority (UKNF).

Contact: pawel.piekutowski@gmail.com

Internal Security Review
2026, no. 34, pp. 259–277

https://doi.org/10.4467/20801335PBW.26.012.23374

ARTICLE

Legal aspect of prohibition on taking up gainful employment and conducting business activities by a professional soldier

MARIUSZ DOMŻALSKI

Headquarters of the 18th Mechanised Division
named after General Tadeusz Buk

https://orcid.org/0000-0002-7749-2598

Abstract

The employment relationship of a professional soldier distinguishes him from persons working under an employment contract not only by numerous rights, but also by numerous restrictions. Professional military service requires availability and is characterised, among other things, by subordination in the service. One of the restrictions is also refraining from taking up additional gainful employment outside of service without the permission of the commander of the military unit in which the soldier serves. This article aims to analyse the regulations related to taking up paid employment and conducting business activity by professional soldiers. This institution is defined in Article 335 of the *Act of 11 March 2022 on the defence of the Homeland* and in the *Regulation of the Minister of National Defence of 13 June 2023 on the performance of paid employment or conducting business activity by professional soldiers*. The author compared the applicable regulations in this regard with the *Act of 11 September 2003 on the military service of professional soldiers*. He then answered the research question whether the Act on the defence of the Homeland and related implementing regulations adequately regulate the discussed issues? In the analysis of legal

acts, the author used a formal-dogmatic method supplemented by a theoretical-legal method. In summary, he pointed out provisions which, in his opinion, require clarification of supplementation.

Keywords Armed Forces, employment relationship, additional gainful employment

Introduction

The possibility of performing additional paid work and conducting business activity by a professional soldier should be treated as an exception to the principle of complete dedication to professional military service, which stems from the function of the armed forces in the state. This is reflected in Article 65(1) in conjunction with Article 31(3) of the *Constitution of the Republic of Poland of 2 April 1997*. According to these provisions, everyone is guaranteed the freedom to choose and pursue a profession and to choose their place of work, and (…) *any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect of the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights*. It is therefore acceptable that there are certain categories of employees who are subject to greater restrictions due to the nature of their duties[1]. These individuals include professional soldiers. In their case, restrictions on the exercise of constitutional freedoms result from the nature of their service and the specific characteristics of the army as an employer, which is based on hierarchical subordination, command and control, and single-person command[2]. The ban on additional work is a consequence of conditions such as availability, political neutrality and the prestige of the service.

Pursuant to Article 335(1) of the *Act of 11 March 2022 on the defence of the Homeland* (hereinafter: the Act on the defence of the Homeland), professional

[1] P. Pakuła-Gawarecka, *Zakres przedmiotowy i podmiotowy zakazu podejmowania dodatkowych zajęć przez funkcjonariuszy Policji* (Eng. The scope and subject matter of the prohibition on police officers taking on additional work), "Roczniki Administracji i Prawa" 2015, no. 15(2), p. 282.

[2] M. Domżalski, *Neutralność polityczna sił zbrojnych w wymiarze prawnokonstytucyjnym* (Eng. Political neutrality of the armed forces in legal and constitutional terms), "Wrocławskie Studia Politologiczne" 2023, no. 32, p. 13. https://doi.org/10.19195/1643-0328.32.1.

soldiers are prohibited from taking up gainful employment and conducting business activities. A similar provision was contained in the previously applicable *Act of 11 September 2003 on the military service of professional soldiers* (hereinafter: the Military Service Act).

Gainful employment of a professional soldier

Work in the sense of providing services or producing goods does not directly lead to the accounting recognition of assets in the balance sheet of the entity providing the work, e.g. an employee. From their perspective, it is usually an exchange of time and skills for income (wages), which may or may not be converted into fixed or current assets. Only the wages received become current assets, i.e. cash or funds in a bank account. The moment when the assets arise is delayed in relation to the act of work itself (from the performance of the service to the receipt of payment). At the same time, it should be emphasised that not every action of a soldier that results in the receipt of income is treated as gainful employment.

For example, income-generating work does not include gains resulting from the disposal of one's assets, such as opening savings accounts and other forms provided for by banking law, which are aimed at achieving financial benefits. Although the main purpose of such activities is to generate income, they should be treated as a form of investment of cash assets. In other words, the income in this case is not related to the soldier's activities, but arises from entrusting a certain amount of money to a financial institution in exchange for receiving income.

The definition of the term 'employment' appears in Article 2 point 51 of the *Act of 20 March 2025 on the labour market and employment services*. It states that this is (…) *the performance of work on the basis of an employment relationship, a service relationship or a contract for outwork*. In case law the term 'gainful employment' is understood as all forms of employment connected with earning income, i.e. economic activity, an employment relationship, a service relationship and any type of civil law contract, as well as membership in the statutory bodies of any institution, if this is connected with earning regular or periodic monetary income. Gainful employment also includes performing work for remuneration without signing a contract that would specify the terms and conditions of the activity performed[3].

[3] Ruling of the Provincial Administrative Court in Szczecin of 7 V 2008, ref. no. II SA/Sz 99/08, LEX No. 515274; ruling of the Provincial Administrative Court in Szczecin of 25 I 2017, ref. no. II SA/Sz 1395/16, LEX No. 2237739; ruling of the Provincial Administrative Court in Poznań of 8 X 2015, ref. no. IV SA/Po 467/15, LEX No. 1933084.

An essential element in classifying the activities performed by a soldier as gainful employment is that he receives remuneration or cash benefits for the work performed. The guarantees resulting from the employee's right to fair remuneration are the norm in this regard. This concept appears in international legal acts, including: the Universal Declaration of Human Rights of 1948 (Article 23)[4], the International Covenant on Economic, Social and Cultural Rights of 1966 (Article 7)[5], the European Social Charter of 1961 (Article 4)[6] and the conventions of the International Labour Organisation[7]. As a rule, in the case of an employment relationship, the employer has the right to use the work performed by the employee in exchange for which they are obliged to pay them remuneration (Article 22 § 1 of the *Act of 26 June 1974 – Labour Code*). Remuneration for work includes all benefits, both monetary and non-monetary, received by the employee from the employer on account of being in an employment relationship. The Labour Code stipulates that an employment relationship is remunerated, which distinguishes it from civil law relationships[8], e.g. contracts for specific work or contracts of mandate. Benefits in this respect are civil law benefits and are therefore not subject to the rigours and protection provided for by labour law[9].

Business activity of a professional soldier

Pursuant to Article 3 of the *Act of 6 March 2018 – Entrepreneurs' Law* (hereinafter: Entrepreneurs' Law Act), economic activity is defined as organised gainful activity performed on one's own behalf and on a continuous basis. The Supreme Court stated in one of its resolutions that (…) *economic activity is an activity of a professional,*

[4] *Universal Declaration of Human Rights*, Paris, 10 XII 1948, https://libr.sejm.gov.pl/tek01/txt/onz/1948.html [accessed: 1 VII 2025].

[5] *International Covenant on Economic, Social and Cultural Rights, opened for signature in New York on 19 December 1966.*

[6] *European Social Charter drawn up in Turin on 18 October 1961.*

[7] K. Prokop, *Konstytucyjne prawo do godziwego wynagrodzenia za pracę* (Eng. The constitutional right to fair remuneration for work), "Białostockie Studia Prawnicze" 2021, vol. 26, no. 2, p. 120. https://doi.org/10.15290/bsp.2021.26.02.08.

[8] M. Liskowski, *Pojęcie wynagrodzenia za pracę w Kodeksie pracy* (Eng. The concept of remuneration for work in the Labour Code), "Pracownik i Pracodawca" 2016, no. 2, p. 35. https://doi.org/10.12775/PiP.2016.012; see also: E. Beck-Krala, *Wynagrodzenie pracowników w organizacji. Teoria i praktyka* (Eng. Employee remuneration in an organisation. Theory and practice), Kraków 2013.

[9] A. Górnicz-Mulcahy, *„Własność" wynagrodzenia za pracę* (Eng. 'Ownership' of remuneration for work), in: *Własność w prawie i gospodarce*, U. Kalina-Prasznic (ed.), Wrocław 2017, p. 162.

and therefore permanent, nature, subject to the rules of profitability and profit or the principle of rational management, acting on one's own account and participating in economic turnover[10].

The organised nature of economic activity means that the chosen type of activity is incorporated into a formal organisational framework, which (…) *means, for example, establishing a specific legal form, setting up a registered office, organising an office or other premises for conducting business, employing staff and establishing internal legal regulations*[11]. The view has become established in case law that, when assessing whether a business activity is being conducted, characteristics such as continuity and organisation should be taken into account, regardless of whether the entity is actually registered. These characteristics of the activity are an objective category, independent of how the entity performing the activity assesses it[12].

Another feature that distinguishes economic activity from other activities is its profit-making nature. *An activity is considered to be profit-making if it is conducted for the purpose of generating income (profit) understood as the surplus of revenue over costs incurred. Activities that do not have this aspect are considered to be charitable, social, cultural or other activities (referred to as non-profit activities)*[13].

Economic activity is to be carried out on one's own behalf, i.e. independently, at one's own risk and on one's own responsibility. A natural person who conducts business activity independently and separately from other entities may be considered a separate economic entity[14].

The last condition for classifying an activity as economic activity is its continuity. *Therefore, only those who perform repetitive activities in such a way that they form a coherent whole, rather than isolated services or specific goods or services, will be considered entrepreneurs. If such activities are of an economic or professional nature, there are grounds for considering the entity undertaking them to be an entrepreneur*[15]. Occasional activity is not a business activity[16]. The line between sporadic activities and planned (organised) but intermittent business activities in Poland is based

[10] Resolution of the Supreme Court of 23 II 2005, ref. no. III CZP 88/04, LEX No. 143136, pp. 5–6.

[11] Ruling of the Supreme Court of 6 IV 2017, ref. no. II UK 98/16, LEX No. 2307127.

[12] Ruling of the Provincial Administrative Court in Opole of 7 V 2008, ref. no. I SA/Op 18/08, LEX No. 484040.

[13] Ruling of the Supreme Administrative Court of 26 IX 2008, ref. no. II FSK 789/07, LEX No. 495147. Cf. Ruling of the Provincial Administrative Court in Warsaw of 8 X 2004, ref. no. II SA 3673/03, LEX No. 159913.

[14] Ruling of the Supreme Administrative Court of 1 X 1997, ref. no. II SA 1811/96, LEX No. 33310.

[15] Decision of the Court of Appeal in Szczecin of 7 VIII 2006, ref. no. I ACz 441/06, LEX No. 279953.

[16] Ruling of the Supreme Administrative Court of 17 IX 1997, ref. no. II SA 1089/96, LEX No. 31312.

on the definition of business activity (continuity, organisation, profit motive) and income limits for unregistered activities. To maintain continuity, it is sufficient that the overall circumstances indicate an intention to repeat a specific set of activities in order to earn income. This should be a permanent, planned (purposeful) activity, regardless of whether the plan covers a longer or shorter period. However, it is not required to conduct the activity without interruption[17].

In order for a specific activity to be considered a business activity, the specified conditions (organised, continuous activity conducted on one's own behalf and for profit) must be met cumulatively. The absence of any one of these conditions means that the activity in question cannot be classified as a business activity.

Other forms of gainful employment for professional soldiers

In the context of the issue under analysis, the question of unregistered activity regulated in Article 5 of the Entrepreneurs' Law Act is interesting. Unregistered activity is defined by three conditions:

1) subjective, which refers to the fact that the activity is performed by a natural person;
2) income-based, based on the proviso that the income due from this activity does not exceed 225% of the minimum wage referred to in the *Act of 10 October 2002 on the minimum wage*;
3) formal, i.e. demonstrating that the entity performing such activity has not performed any economic activity in the last 60 months.

Unregistered activity is not formally considered economic activity, but it is gainful activity, performed personally, and may violate the conditions specified in Article 335(3) of the Act on the defence of the Homeland, e.g. interfere with the performance of official duties or violate the prestige of a professional soldier. Therefore, even in the case of unregistered activity, although the regulations do not require the commander's consent, the soldier must take into account the restrictions resulting from the aforementioned article. At the same time, it should be remembered that, pursuant to Article 5(3) of the Entrepreneurs' Law Act, if in a given quarter the income exceeds 225% of the minimum wage, unregistered activity becomes, by law, economic activity from the date on which this amount was exceeded. In such a situation, a professional soldier must obtain the consent of the commander of the military unit. Failure to do so constitutes a violation

[17] Ruling of the Provincial Administrative Court in Wrocław of 27 IV 2005, ref. no. I SA/Wr 3237/03, LEX No. 496830.

of Article 335(1) of the Act on the defence of the Homeland, which may result in disciplinary proceedings or the withdrawal of consent for other forms of activity, if previously granted. If a soldier obtains consent to conduct economic activity, he or she may continue to perform activities that they have previously performed as unregistered activity.

Additional income of a professional soldier *de jure*

The legislator has provided for the possibility for a professional soldier to take up additional gainful employment and conduct business activity, provided that he submits a request for permission to do so to the commander of his military unit. According to the definition contained in the Article 2 of the Act on the defence of the Homeland, the commander of a military unit is a person who manages or commands a military unit in which a soldier holds a position or to which he has been assigned as part of his professional military service.

Detailed conditions and procedures for granting professional soldiers permits to perform gainful employment or conduct business activity, as well as the information to be included in a soldier's application for a permit to work or conduct business activity, are specified in the *Regulation of the Minister of National defence of 13 June 2023 on the performance of gainful employment or business activity by professional soldiers* (hereinafter: the Regulation on the performance of work). On the basis of the delegation contained in Article 56 of the Military Service Act, the *Regulation of the Minister of National Defence of 7 October 2009 on the performance of gainful employment or business activity by professional soldiers* was issued.

A professional soldier submits a written application for permission to perform gainful employment or conduct business activity exclusively on his own behalf through official channels. This means that this action cannot be taken by a representative appointed by the soldier, nor can it be carried out on behalf of or in the interest of a third party. The official channel means that the application is reviewed by each of the applicant soldier's superiors, so that the immediate superior, who has the most comprehensive knowledge of the soldier, can determine whether the subordinate's additional activity will interfere with his or her official duties[18].

[18] P. Gacek, *Dodatkowe zajęcie zarobkowe poza służbą (art. 62 ust. 1 ustawy o Policji) – wybrane zagadnienia proceduralne* (Eng. Additional gainful employment outside of service (Article 62(1) of the Police Act) – selected procedural issues), "Ius et Administratio" 2017, no. 1, p. 6.

It is worth noting that there is no legal basis for a military unit commander to decide on a professional soldier's request for permission to perform gainful employment by way of an administrative decision, i.e. under the provisions of the *Act of 14 June 1960 – Code of Administrative Procedure*. This matter is an internal matter arising from the chain of command and should be dealt with through official channels, rather than by means of an administrative decision. The decision of the commander of the military unit is not subject to appeal to a higher authority and, consequently, cannot be reviewed by way of a complaint lodged with an administrative court[19]. The decision concerning the settlement of a matter relating to the employment relationship of a professional soldier must be based on the applicable provision, and not on the Code of Administrative Procedures[20]. The regulation on performance of work does not specify a deadline by which the procedure for granting or refusing permission to perform gainful employment or conduct business activity must be completed. However, it should be recognised that the commander of the military unit should make a decision before the date indicated by the soldier in the application as the date of commencement of work/business activity, with the proviso that the application must be submitted sufficiently in advance.

In § 3(2) point 1of the regulation on the performance of work it was stated that in the case of gainful employment, the application shall include:

a) the rank, first name and surname of the soldier,
b) the name of the entity for which the gainful employment will be performed and the address of its registered office, or the first name and surname of the person for whom the gainful employment will be performed and that person's place of residence,
c) the basis for the work performed (under an employment contract or on another basis),
d) the place of work,
e) the period for which the entity referred to in point b) intends to conclude an employment contract or a contract on another basis,
f) the working time,
g) the weekly duty schedule, including the determination of official duties within 40 hours in a 5-day working week,

[19] Ruling of the Provincial Administrative Court in Bydgoszcz of 22 I 2013, ref. no. II SA/Bd 1012/12, LEX No. 1351366.

[20] Decision of the Supreme Administrative Court of 23 VIII 2012, ref. no. I OSK 1649/12, LEX No. 1331525; decision of the Supreme Administrative Court of 26 IV 2006, ref. no. I OSK 303/06, LEX No. 203585; decision of the Provincial Administrative Court in Poznań of 15 I 2010, ref. no. II SA/Po 882/09, LEX No. 635705; decision of the Provincial Administrative Court in Białystok of 19 III 2013, ref. no. II SA/Bk 171/13, LEX No. 1301609.

h) the nature of the work performed,
i) the start date of work.

In accordance with § 3(2) point 2 of the regulation on the performance of work, an application for consent to conduct business activity shall include:

a) rank, first name and surname of the soldier,
b) specification of the subject of the business activity, in accordance with the Polish Classification of Activities, and the address of the registered office or place of residence of the entity conducting the business activity,
c) the address at which the business activity will be carried out,
d) the legal form of the business activity,
e) the amount of time necessary to carry out the business activity,
f) the date of commencement of the business activity.

In accordance with § 3(2) point 3 of the regulation on the performance of work, together with the application, the soldier shall submit a mandatory statement that (…) *the business activity or activity of the entity for which the work will be performed does not concern products referred to in the provisions on the classification of defence products and supplies, construction works and services intended for military units*. Detailed rules for the codification of defence products are set out in *Decision No. 115/MON of the Minister of National Defence of 18 September 2024 on the Defence Products Codification System*. This regulation is subsequent to the Act. Neither the Military Service Act nor the Act on the defence of the Homeland provide for the possibility of conducting gainful activity related to defence products and supplies, construction works and services intended for military units. Nor was the soldeir required to submit a declaration on this matter.

In Article 56(3) of the Military Service Act and in Article 335(3) of the Act on the defence of the Homeland, the legislator indicated that the commander of a military unit may allow a soldier to perform gainful employment or conduct business activity if:

1) it does not interfere with the soldier's performance of his official duties,
2) it contributes to improving their qualifications,
3) it does not undermine the prestige of a professional soldier,
4) the business activity or activity of the entity for which the work will be performed does not concern products referred to in the regulations on the classification of defence products and supplies, construction works and services intended for military units.

A soldier's additional work must therefore not adversely affect his availability, but should improve his qualifications. This is provided, for instance, by working as a lecturer or paramedic.

In one of the rulings of administrative courts based on the Military Service Act, a negative premise in the form of a violation of professional soldier's prestige was indicated:

> The military service of a professional soldier, as the name suggests, is not a professional job [,] but a service characterised by discipline, loyalty and dedication. Professional soldiers are soldiers in active military service. Their length of service is determined by official duties that are difficult to predict and plan. They are sent to the most difficult areas to secure the independence of their homeland, but also to ensure the safety of citizens, with a readiness to sacrifice their lives. Their basic duties are defined by the Constitution of the Republic of Poland and the Act on the military service of professional soldiers. Therefore, it is not possible to agree with the complainant that his business activity does not interfere with his military service and that the status of a salesperson in a computer shop has the same prestige as that of a professional soldier[21].

Pursuant to § 3(4) of the Regulation on the performance of work, the commander of a military unit may request the future employer of a soldier to provide (…) *information on the nature of the work to be performed by the soldier, the working time schedule applied and the possibility of performing official duties outside the permanent place of work, including outside the country, at the employer's request*.

When making a decision, the commander of a military unit must consider all the circumstances determining whether to grant consent, both positive and negative for the applicant. At the same time, he must remember that the most important thing is to secure the current activities of the military unit he commands[22]. The decision as to whether the type of gainful activity performed by a soldier conflicts with the performance of his official duties rests solely with the commander of the military unit[23].

---

[21] Ruling of the Provincial Administrative Court in Gorzów Wielkopolski of 25 XI 2009, ref. no. II SA/Go 676/09, LEX No. 589116.

[22] P. Palka, *Dodatkowa praca zarobkowa żołnierzy zawodowych (uwagi de lege lata)* (Eng. Additional gainful employment of professional soldiers (comments de lege lata)), "Wojskowy Przegląd Prawniczy" 2006, no. 2, p. 35; M. Czechowski, *Prawny charakter zatrudnienia żołnierzy zawodowych* (Eng. The legal nature of the employment of professional soldiers), Toruń 2016, pp. 224–227.

[23] Ruling of the Supreme Administrative Court of 9 II 2001, ref. no. II SA 3072/00, LEX No. 53672.

In the event of a breach of the conditions for obtaining consent, the commander of the military unit shall immediately revoke the permit to perform gainful employment or conduct business activity, ensuring a soldier the time necessary to terminate the employment contract or other contract on the basis of which the soldier performs gainful employment[24], or to terminate the business activity (§ 10 of the Regulation on the performance of work). This regulation specifies the conditions for refusing or revoking a permit to perform gainful employment or conduct business activity. The difference between the current regulation and the previous regulations is that the commander revokes the permit immediately, i.e. it is mandatory. The previous regulations indicated that the commander may revoke the permit, so it was a discretionary power.

In the case of gainful employment undertaken by a soldier under an employment contract or running a business, the commander of the military unit must give his consent regardless of the period for which the employment contract is concluded or the expected period of running the business. In the case of other types of contracts, e.g. a contract of mandate or a contract for specific work, the obligation to obtain consent will apply to contracts concluded for a period longer than one month.

Previous regulations did not require informing the commander of the military unit in which a soldier holds a position about the name of the entity for which the soldier performed paid work for a period not exceeding one month, within one month from the date of commencement of such work. Currently, it is not necessary to provide information about the type of work, remuneration and working hours – it is only mandatory to indicate the entity for which the soldier performed work.

It is worth noting that gainful employment cannot be performed by a professional soldier in another military unit, unless the soldier obtains the consent of the Minister of National Defence to take up such employment, with the exception of the employment at a military university as a lecturer conducting classes. In accordance with the definition included in Article 2 of the Act on the defence of the Homeland, a military unit should be understood as (…) *an organisational unit of the Armed Forces operating on the basis of a position assigned by the Minister of National Defence and using an official seal with the emblem of the Republic of Poland and the name (number) of the unit*. A professional soldier may not perform additional paid work in the military unit in which he or she serves.

In a situation where the gainful employment undertaken by a soldier is to be performed in another military unit, in accordance with § 4 of the Regulation on the performance of work, the soldier must submit an application (…) *to the Minister*

[24] Ruling of the Provincial Administrative Court in Warsaw of 14 IV 2008, ref. no. II SA/Wa 1842/07, LEX No. 480072.

of National Defence through the commander of the military unit in which he holds a position or to which he has been assigned as part of his professional military service. The commander shall forward the application, together with his opinion on it, to the Minister of National Defence via the head of the organisational unit of the Ministry of National Defence responsible for human resources. The minister's decision to grant or refuse consent is also communicated to the soldier by the commander. In addition, once the soldier has obtained permission to perform gainful employment or conduct business activity, the commander of the military unit may require him (…) *to produce for inspection the employment contract or other contract on the basis of which the soldier performs gainful employment, or printouts from the register of entrepreneurs of the National Court Register or from the Central Register and Information on Economic Activity* (§ 5 of the Regulation on the performance of work).

In the Military Service Act, additional gainful employment of a soldier in a military unit was regulated differently. In accordance with Article 56(3a) and (3b) of the aforementioned act, such work could not be performed by a professional soldier in the military unit in which he served or in a military unit directly subordinate to it, except where the work was undertaken in an entity that is not a budgetary entity, on a basis other than an employment contract. In the author's opinion, the current regulations in this matter are more transparent – the application must be submitted to the Minister of National Defence, whereas previously the decision to grant consent for additional work could be made by an authority which could also be the soldier's additional employer.

In accordance with § 9(1) of the Regulation on the performance of work:

> In the event that a soldier who has been granted permission to perform gainful employment or conduct business activity is assigned to a position in another military unit or is transferred to another military unit as part of his professional military service, the soldier interested in continuing to perform gainful employment or conduct business activity shall submit a request to the commander of that military unit within 14 days from the date of assuming duties in the official position or the date of reporting to the military unit as part of performing professional military service at the disposal of the commander. Until the commander of the military unit or the Minister of National Defence issues a decision on this matter, the soldier shall perform work or conduct business activity on the basis of the existing permit.

As in the case of revocation of a permit to perform gainful employment or conduct business activity, the commander of the military unit shall ensure a soldier sufficient time to terminate the employment contract or other contract

on the basis of which the soldier performs gainful employment, or to terminate the business activity (§10(3) of the Regulation on the performance of work). The Military Service Act and the *Regulation of the Minister of National Defence of 7 October 2009 on the performance of gainful employment or business activity by professional soldiers* lacked regulations in this area. Undoubtedly, this change has a positive impact on the financial stability of soldiers. It is worth noting here that personnel movements in the Polish Armed Forces are very frequent, which is why this regulation takes on a particular practical dimension.

In accordance with § 6 of the Regulation on the performance of work:

> 1. A soldier who has obtained permission to perform gainful employment or conduct business activity shall immediately notify the commander of the military unit in writing of:
>   1) not taking up gainful employment;
>   2) interruption of gainful employment;
>   3) termination of gainful employment;
>   4) not taking up business activity;
>   5) termination of business activity;
>   6) suspension of business activity;
>   7) resumption of business activity.
> 2. In the cases referred to in points 1–5, the commander of the military unit shall declare the expiry of the permit to perform gainful employment or conduct business activity.

The legislator has regulated the performance of paid work by professional soldiers for a period shorter than one month differently. In such a case, a professional soldier is obliged to provide the commander of the military unit in which he holds a position with information about the name of the entity for which he performed the work, within one month of the date of commencement of the work. Despite the formal lack of a requirement to obtain consent from the commander of the military unit, a professional soldier is not allowed to perform paid work for periods shorter than one month if it would interfere with the performance of their official duties, violate the prestige of the service, or if the work concerned products referred to in the regulations on the classification of defence products and supplies, construction works and services intended for military units.

It should be noted that, pursuant to Article 547 of the Act on the defence of the Homeland, in the event of mobilisation, martial law or war, Article 335 concerning the possibility of professional soldiers taking up additional paid work does not apply to them. This reflects the priority of the state's interests over the individual interests of soldiers, especially in times of emergency.

Pursuant to Article 353(1) of the Act on the defence of the Homeland: (…) *a breach of military discipline is an act committed by a soldier which damages the reputation or interests of the Armed Forces, culpable exceeding of powers or failure to perform duties arising from legal provisions, including orders and instructions issued by superiors authorised under those provisions*. On the other hand, Article 353(2) point 2 of the aforementioned Act stipulates that a violation of military discipline is, in particular: (…) *a failure to fulfil the duties of a soldier arising from the military oath taken, as well as from legal provisions, military regulations and the principles of military ethics*. In view of these regulations, it should be considered that taking up additional paid work or conducting business activity without the consent of the commander of a military unit is a disciplinary offence. It is worth quoting here the judgment of the Provincial Administrative Court in Lublin, which was issued on the basis of the Police Act, but the ruling will also apply to professional soldiers:

> (…) pursuant to Article 62(1) of the Police Act, a police officer may not engage in gainful employment outside of service without the written consent of their superior, nor may they perform activities or tasks that are contrary to their duties under the Act or that undermine trust in the Police. Pursuant to Article 132(1) and (2) of the Police Act, a police officer is subject to disciplinary action for committing a disciplinary offence consisting in a breach of professional discipline or failure to comply with the rules of professional ethics. A breach of professional discipline is an act by a police officer consisting in the culpable exceeding of powers or failure to perform duties arising from legal provisions or orders and instructions issued by superiors authorised on the basis of these provisions[25].

The disciplinary standard is part of a broader set of regulations concerning the official status of professional soldiers and is a typical example of restrictions also known in other uniformed services, such as the Police, the Internal Security Agency or the Border Guard. Its purpose is, among other things, to eliminate conflicts of interest, minimise the risk of corruption and safeguard the operational capabilities of the armed forces.

Summary

When joining the professional military service, soldiers must be aware that they are giving up certain rights that they had as a civilian. This is due to the need for

[25] Ruling of the Provincial Administrative Court in Lublin of 25 X 2007, ref. no. III SA/Lu 422/07, LEX No. 492288.

high availability and the hierarchical structure of the army. One such restriction is the obligation for professional soldiers to refrain from taking up gainful employment outside of service without the written consent of the commander of the military unit. The legislator has provided for the possibility of obtaining such consent under certain conditions. The soldier must submit an official application containing the information listed in the Regulation on the performance of work. The legislator has also provided for the possibility of revoking consent, but only in cases specified in the Act on the defence of the Homeland. It is important to note that the provisions on administrative procedure will not apply to the procedure for granting, refusing or revoking consent.

The previous law on the military service also prohibited professional soldiers from taking up gainful employment or conducting business activities. The definition of gainful employment is the same in both acts, with the exception that the Act on the defence of the Homeland stipulates the need to inform the commander of the military unit about performing paid work for periods shorter than one month. As before, at the soldier's request, the unit commander may grant them permission to take up employment or conduct business activity if the conditions of no conflict with service, improvement of qualifications, no damage to prestige and no activity in the defence sector are met. The procedure for obtaining permission is identical in both regulations. Both the Act on the defence of the Homeland and the Military Service Act specify the application procedure and the assessment of the grounds for granting consent. Article 335 of the Act on the defence of the Homeland extends – in comparison with Article 56 of the Military Service Act – the control and restrictions on soldiers' gainful employment in other military units – it is not permitted unless the soldier obtains the consent of the Minister of National Defence. An exception is made for work as a lecturer at a military university. Undoubtedly, this exception is a form of strengthening the educational potential of the armed forces. In the author's opinion, there is no possibility of working in the military unit in which the soldier serves.

It should be noted that the provisions of the pragmatics and the executive act thereto in this matter are regulated in a fairly unambiguous manner and give priority to the service over the individual interests of the soldier. Most of the existing provisions prohibiting professional soldiers from taking on additional paid work have not changed. However, Article 335 of the Act on the defence of the Homeland introduces greater precision and new conditions, e.g. those concerning paid work in another military unit. This may limit the practice of employing soldiers on additional contracts within the armed forces. It is also important that in the event of a violation of the rules on additional work, the commander of the military unit is obliged to revoke the permit to perform gainful employment or conduct business activity. In the author's opinion, the regulations introduced in the Act on the Defence

of the Homeland have brought about beneficial changes compared to the Military Service Act, which affect the transparency and clarity of granting permits for additional work. However, there is still room for improvement in this regard. The commander has considerable discretion when it comes to granting consent. The provision does not define the method of assessing conflicts between work and official duties, which may lead to differences in practice among commanders of different units. The assessment of a soldier's prestige in the context of their work may also pose interpretation problems. This is a general clause that requires interpretative guidelines. The provision allows for work at military universities, but does not explicitly refer to civilian universities, which leads to the need for approvals and increased official supervision. It is worth noting that the realities of the labour market are becoming increasingly complex and new, flexible forms of employment are emerging, such as freelancing, platform work and the gig economy, which may in the future require clarification of the concept of gainful employment or the issuance of implementing regulations.

In summary, Article 335 of the Act on the defence of the Homeland is an important element stabilising the structure of professional service, protecting national security and counteracting abuse in the service. From a scientific point of view, this provision meets constitutional requirements and complies with standards concerning professional restrictions for members of uniformed services.

Bibliography

Beck-Krala E., *Wynagrodzenie pracowników w organizacji. Teoria i praktyka* (Eng. Employee remuneration in an organisation. Theory and practice), Kraków 2013.

Czechowski M., *Prawny charakter zatrudnienia żołnierzy zawodowych* (Eng. The legal nature of the employment of professional soldiers), Toruń 2016.

Domżalski M., *Neutralność polityczna sił zbrojnych w wymiarze prawnokonstytucyjnym* (Eng. Political neutrality of the armed forces in legal and constitutional terms), "Wrocławskie Studia Politologiczne" 2023, no. 32, pp. 7–20. https://doi.org/10.19195/1643-0328.32.1.

Gacek P., *Dodatkowe zajęcie zarobkowe poza służbą (art. 62 ust. 1 ustawy o Policji) – wybrane zagadnienia proceduralne* (Eng. Additional gainful employment outside of service (Article 62(1) of the Police Act) – selected procedural issues), "Ius et Administratio" 2017, no. 1, pp. 1–25.

Górnicz-Mulcahy A., *„Własność" wynagrodzenia za pracę* (Eng. 'Ownership' of remuneration for work), in: *Własność w prawie i gospodarce,* U. Kalina-Prasznic (ed.), Wrocław 2017, pp. 161–173.

Liskowski M., *Pojęcie wynagrodzenia za pracę w Kodeksie pracy* (Eng. The concept of remuneration for work in the Labour Code), "Pracownik i Pracodawca" 2016, no. 2, pp. 32–42. https://doi.org/10.12775/PiP.2016.012.

Pakuła-Gawarecka P., *Zakres przedmiotowy i podmiotowy zakazu podejmowania dodatkowych zajęć przez funkcjonariuszy Policji* (Eng. The scope and subject matter of the prohibition on police officers taking on additional work), "Roczniki Administracji i Prawa" 2015, no. 15(2), pp. 281–298.

Palka P., *Dodatkowa praca zarobkowa żołnierzy zawodowych (uwagi de lege lata)* (Eng. Additional gainful employment of professional soldiers (comments de lege lata)), "Wojskowy Przegląd Prawniczy" 2006, no. 2, pp. 31–43.

Prokop K., *Konstytucyjne prawo do godziwego wynagrodzenia za pracę* (Eng. The constitutional right to fair remuneration for work), "Białostockie Studia Prawnicze" 2021, vol. 26, no. 2, pp. 119–135. https://doi.org/10.15290/bsp.2021.26.02.08.

Legal acts

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

International Covenant on Economic, Social and Cultural Rights, opened for signature in New York on 19 December 1966 (Journal of Laws of 1977, no. 38, item 169).

European Social Charter drawn up in Turin on 18 October 1961 (Journal of Laws of 1999, no. 8, item 67).

Universal Declaration of Human Rights, Paris, 10 X 1948, https://libr.sejm.gov.pl/tek01/txt/onz/1948.html [accessed: 1 VII 2025].

Act of 20 March 2025 on the labour market and employment services (Journal of Laws of 2025, item 620, as amended).

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

Act of 6 March 2018 – Entrepreneurs' Law (consolidated text, Journal of Laws of 2025, item 1480, as amended).

Act of 11 September 2003 on the military service of professional soldiers (consolidated text, Journal of Laws of 2022, item 536).

Act of 10 October 2002 on the minimum wage (consolidated text, Journal of Laws of 2024, item 1773).

Act of 26 June 1974 – Labour Code (consolidated text, Journal of Laws of 2025, item 277, as amended).

Act of 14 June 1960 – Code of Administrative Procedure (consolidated text, Journal of Laws of 2025, item 1691).

Regulation of the Minister of National Defence of 13 June 2023 on the performance of gainful employment or business activity by professional soldiers (Journal of Laws of 2023, item 1217).

Regulation of the Minister of National Defence of 7 October 2009 on the performance of gainful employment or business activity by professional soldiers (Journal of Laws of 2009, no. 176, item 1366).

Decision No. 115/MON of the Minister of National Defence of 18 September 2024 on the Defence Products Codification System (Journal of Laws of the Ministry of National Defence of 2024, item 145).

Case law

Resolution of the Supreme Court of 23 II 2005, ref. no. III CZP 88/04, LEX No. 143136.

Ruling of the Supreme Court of 6 IV 2017, ref. no. II UK 98/16, LEX No. 2307127.

Decision of the Court of Appeal in Szczecin of 7 VIII 2006, ref. no. I ACz 441/06, LEX No. 279953.

Ruling of the Supreme Administrative Court of 26 IX 2008, ref. no. II FSK 789/07, LEX No. 495147.

Ruling of the Supreme Administrative Court of 9 II 2001, ref. no. II SA 3072/00, LEX No. 53672.

Ruling of the Supreme Administrative Court of 1 X 1997, ref. no. II SA 1811/96, LEX No. 33310.

Ruling of the Supreme Administrative Court of 17 IX 1997, ref. no. II SA 1089/96, LEX No. 31312.

Decision of the Supreme Administrative Court of 23 VIII 2012, ref. no. I OSK 1649/12, LEX No. 1331525.

Decision of the Supreme Administrative Court of 26 IV 2006, ref. no. I OSK 303/06, LEX No. 203585.

Ruling of the Provincial Administrative Court in Bydgoszcz of 22 I 2013, ref. no. II SA/Bd 1012/12, LEX No. 1351366.

Ruling of the Provincial Administrative Court in Gorzów Wielkopolski of 25 XI 2009, ref. no. II SA/Go 676/09, LEX No. 589116.

Ruling of the Provincial Administrative Court in Lublin of 25 X 2007, ref. no. III SA/Lu 422/07, LEX No. 492288.

Ruling of the Provincial Administrative Court in Opole of 7 V 2008, ref. no. I SA/Op 18/08, LEX No. 484040.

Ruling of the Provincial Administrative Court in Poznań of 8 X 2015, ref. no. IV SA/Po 467/15, LEX No. 1933084.

Ruling of the Provincial Administrative Court in Szczecin of 25 I 2017, ref. no. II SA/Sz 1395/16, LEX No. 2237739.

Ruling of the Provincial Administrative Court in Szczecin of 7 V 2008, ref. no. II SA/Sz 99/08, LEX No. 515274.

Ruling of the Provincial Administrative Court in Warsaw of 14 IV 2008, ref. no. II SA/Wa 1842/07, LEX No. 480072.

Ruling of the Provincial Administrative Court in Warsaw of 8 X 2004, ref. no. II SA 3673/03, LEX No. 159913.

Ruling of the Provincial Administrative Court in Wrocław of 27 IV 2005, ref. no. I SA/Wr 3237/03, LEX No. 496830.

Decision of the Provincial Administrative Court in Białystok of 19 III 2013, ref. no. II SA/Bk 171/13, LEX No. 1301609.

Decision of the Provincial Administrative Court in Poznań of 15 I 2010, ref. no. II SA/Po 882/09, LEX No. 635705.

Major Mariusz Domżalski, PhD

Legal advisor at the Headquarters of the 18th Mechanised Division named after General Tadeusz Buk.

Contact: mariuszdomzalski89@gmail.com

Internal Security Review
2026, no. 34, pp. 279–298

https://doi.org/10.4467/20801335PBW.26.013.23375

ARTICLE

Functionality of the mobile CBRNE laboratory of the State Fire Service in the context of legal regulations and operational assumptions of the National Firefighting and Rescue System

GRZEGORZ BUGAJ

Association of CBRNE Security Specialists

https://orcid.org/0000-0003-1650-023X

Abstract

The article analyses the functionality of the mobile CBRNE laboratory of the State Fire Service in the context of applicable legal regulations and operational assumptions of the National Firefighting and Rescue System. This laboratory, designed as the highest (L) level of operational readiness in the chemical and ecological rescue structure, significantly strengthens the analytical capabilities of the State Fire Service to respond to chemical, biological, radiological, nuclear and explosive threats. The paper presents a technical characteristics of the laboratory, including its modular construction, advanced filtration and decontamination systems, and analytical equipment compliant with NATO standards. Operational scenarios for the laboratory's use are discussed, with particular emphasis on the identification of dangerous shipments, assessment of environmental contamination, and response to radiological threats. The article also analyses challenges related to the operation of mobile laboratories, including formal issues regarding BSL-3 classification, staffing requirements, and logistical aspects. The strategic importance of mobile CBRNE laboratories for Poland's security as a border state of the EU and NATO is emphasised,

especially in light of experiences from the conflict in Ukraine, indicating the real risk of releasing toxic substances as a result of warfare.

Keywords mobile CBRNE laboratory, State Fire Service, CBRNE security, chemical rescue, radiological threats

Introduction

Chemical, biological, radiological, nuclear and explosive (CBRNE) threats are among the most serious challenges facing modern public safety systems. There has been a systematic increase in interest in this issue in the literature on the subject, as evidenced by the growing number of scientific publications[1].

Mobile CBRNE laboratories became the subject of detailed research at the beginning of the 21st century. Examples include Italian mobile laboratory designs[2] and concepts such as Deployable Mobile CBRN Laboratory[3], developed thanks to intensified investment after terrorist attacks in the US and Japan. A mobile diagnostic laboratory enabling field analyses has been developed in Finland. Its usefulness

[1] Cf. e.g.: *CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapons*, A. Richardt et al. (eds.), Weinheim 2013; M. Gawlik-Kobylińska, M. Urban, G. Gudzbeler, *The EU-SENSE System as a Tool to Support Airport Security*, in: *Reliability and Statistics in Transportation and Communication: Human Sustainability and Resilience in the Digital Age*, I. Kabashkin, I. Yatskiv, O. Prentkovskis (eds.), pp. 597–605, series: Lecture Notes in Networks and Systems, vol. 1337, Cham 2025. https://doi.org/10.1007/978-3-031-87532-8_53; M. Urban, *Protection of Airports against the Threat of CBRNE*, "Studia Bezpieczeństwa Narodowego" 2023, vol. 29, no. 3, pp. 7–34. https://doi.org/10.37055/sbn/171016; *Przeciwdziałanie zagrożeniom CBRNE – aspekty teoretyczne i praktyczne* (Eng. Counteracting CBRNE threats – theoretical and practical aspects), Ł. Jureńczyk, A. Pieczywok, M. Urban (eds.), Bydgoszcz 2024; A. Rabajczyk et al., *Monitoring of Selected CBRN Threats in the Air in Industrial Areas with the Use of Unmanned Aerial Vehicles*, "Atmosphere" 2020, no. 11, 1373. https://doi.org/10.3390/atmos11121373.

[2] G. Mari et al., *CBRN mobile laboratories in Italy*, "Proceedings SPIE 7304, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing X", vol. 7304. https://doi.org/10.1117/12.819445.

[3] C. Toader et al., *Mobile Deployable Laboratory – Chemical Module*, "International Conference KNOWLEDGE-BASED ORGANIZATION" 2016, vol. 22, no. 3, pp. 677–680. https://doi.org/10.1515/kbo-2016-0116.

has been assessed by NATO[4]. These solutions are part of a global trend towards increasing mobile analytical capabilities, which has been intensified since 2001. With regard to the equipment used in mobile laboratories, international research focuses on miniaturising analytical devices and increasing their effectiveness[5]. Analyses are also being conducted on the use of mobile laboratories as tools to support rescue operations. Research indicates that mobile analytical capabilities are crucial for reducing response times and improving the quality of operational decisions. This is confirmed both by experiences gained from the use of mobile laboratories during the Ebola epidemic in Africa[6] and by the results of the project MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU), funded by the European Union. The aim of this project was to develop the ability to assess CBRN threats directly at the site where they occur[7].

Mobile CBRN laboratories are the subject of systematic research conducted not only within the framework of EU programmes, but also NATO initiatives. Projects such as PRACTICE (Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment) and EU-SENSE (European Sensor System for CBRN Applications) serve to develop new concepts for mobile analytical systems[8].

The geopolitical situation in Central and Eastern Europe, which is particularly affected by the conflict in Ukraine, generates new requirements for CBRNE threat response systems. Not all issues were fully taken into account in studies.

---

[4] P.M. Kinnunen et al., *Mobile Diagnostic CBRN Field Laboratory: NATO evaluated Finnish Design*, Challenge – Medical CBRN Defence International" 2012, no. 1.

[5] Cf. e.g.: D. Di Giovanni et al., *Design of Miniaturized Sensors for a Mission-Oriented UAV Application: A New Pathway for Early Warning*, "International Journal of Safety and Security Engineering" 2021, vol. 11, no. 4, pp. 435–444. https://doi.org/10.18280/ijsse.110417; M. Gawlik-Kobylińska et al., *The EU-SENSE System for Chemical Hazards Detection, Identification, and Monitoring*, "Applied Sciences" 2021, vol. 11, no. 21. https://doi.org/10.3390/app112110308; Ł. Szklarski, *Diagnoza potrzeb w zakresie usprawnienia technologii i sprzętu służącego reagowaniu na incydenty o charakterze CBRN. Zarys problemu z perspektywy europejskich straży pożarnych* (Eng. A diagnosis of needs for improvements of technology and hardware used by units responding to CBRN-related incidents. An outline of the problem from the perspective of European fire services), "Zeszyty Naukowe SGSP" 2021, vol. 2, no. 80, pp. 142–160. https://doi.org/10.5604/01.3001.0015.6474.

[6] A. Parsons et al., *Examining the utility and readiness of mobile and field transportable laboratories for biodefence and global health security-related purposes*, "Global Security: Health, Science and Policy" 2018, vol. 3, no. 1, pp. 1–13. https://doi.org/10.1080/23779497.2018.1480403.

[7] *Final Report Summary – MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU)*, CORDIS – EU research results, 9 II 2016, https://cordis.europa.eu/project/id/312885/reporting [accessed: 25 IX 2025].

[8] Ł. Szklarski, *CBRN threats, EU-SENSE system: Paving the way for future national security systems – an assessment of the suitability of the concept for the future of national security*, "Zeszyty Naukowe SGSP" 2024, vol. 2, no. 89, pp. 139–156. https://doi.org/10.5604/01.3001.0054.3833.

The literature on the subject does not contain in-depth analyses of the integration of mobile laboratories with rescue systems in Poland and their compliance with national legal regulations and technical standards. There is also a lack of studies analysing the actual operational barriers to these laboratories. The capabilities of analytical devices are described in detail in technical literature, but there are no studies dedicated to the human resource, procedural, logistical and organisational challenges that can have a significant impact on the effectiveness of using these technologically advanced solutions in practice[9]. The focus is primarily on general issues related to chemical safety and specialist rescue operations. There are not enough detailed analysis concerning modern technical solutions implemented within the structures of the State Fire Service (SFS).

The research problem addressed by the author of the article was the question of the actual operational effectiveness of the SFS's mobile CBRNE laboratories, understood as their real potential for use in rescue operations, in the context of discrepancies between formal technical and legal requirements and human resource, procedural, logistical and organisational conditions. These discrepancies can significantly limit the ability to respond effectively to CBRNE incidents. The aim of the research was to conduct a comprehensive analysis of the functionality of the SFS's mobile CBRNE laboratories by answering the following research questions:

1. To what extent do SFS's mobile CBRNE laboratories meet legal and regulatory requirements?
2. What are the real operational capabilities of the SFS's mobile CBRNE laboratories in the context of the objectives of the National Firefighting and Rescue System (hereinafter: NFRS)?
3. What are the main challenges and limitations in the functioning of the SFS's mobile CBRNE laboratories?

The author adopted the hypothesis that technological advancement of CBRNE mobile laboratories can generate organisational and operational challenges that require the implementation of adequate systemic solutions to overcome. The article is of a contributory nature, constituting a study of functionality of the SFS's mobile CBRNE laboratories, opening the way for further empirical research on optimising the use of these laboratories in the state security system.

[9] R. Jankowski, P. Wereski, *CBRNE lab*, Przegląd Pożarniczy, https://www.ppoz.pl/czytelnia/ratownictwo-i-ochrona-ludnosci/CBRNE-lab/idn:2828 [accessed: 25 IX 2025].

Research methods

The study was based on a qualitative analysis of legal documents, technical standards and technical documentation of the SFS's mobile CBRNE laboratories. Content analysis and comparative analysis were used to assess the compliance of technical solutions with normative requirements.

The following data sources were used in the study:

- legal acts: the Act on the State Fire Service and implementing regulations concerning the organisation and functioning of the NFRS,
- operational documents: *Principles of chemical and environmental rescue organisation in the national firefighting and rescue system*,
- technical standards,
- technical documentation from the laboratory manufacturer,
- audiovisual materials presenting the functionality of laboratories.

The functionality of the SFS's CBRNE laboratories was assessed according to the following criteria:

- compliance with national legislation,
- compliance with technical standards,
- operational capabilities in the context of the tasks of the NFRS,
- interoperability with national and international systems,
- technical and organisational limitations.

The study was based mainly on document analysis and did not include empirical research on the operation of laboratories in real-life conditions. Access to some operational documents was limited due to their classified nature. This resulted in methodological limitations.

Legal and regulatory framework for the operation of the SFS's mobile CBRNE laboratories in Poland

Operation of the CBRNE mobile laboratory of the State Fire Service is embedded in a complex system of legal regulations, including both national regulations and international standards. The legal basis is provided by the Act on the State Fire Service[10], which defines the organisation and scope of its activities, including the performance of tasks in the field of chemical and ecological rescue. The implementing provisions for this Act, primarily the regulation on the detailed organisation of the NFRS, define CBRNE threats as: (…) *hazards caused by chemical,*

[10] *Act of 24 August 1991 on the State Fire Service.*

biological, radioactive, nuclear and explosive agents which, due to their properties, have been used or could be used deliberately to cause a threat to the life and health of humans, animals and the natural environment[11].

Equally important are the *Principles of chemical and environmental rescue organisation in the national firefighting and rescue system*[12] that define the organisational structure and tasks of specialised chemical and ecological rescue groups (SGRChem-Eko) at various levels of operational readiness. This document introduces a division into five levels of readiness:

1) level A – chemical protection,
2) level B – chemical reconnaissance,
3) level C – special reconnaissance,
4) level D – decontamination,
5) level L – laboratory analysis.

The implemented SFS's mobile CBRNE laboratories meet the highest level of readiness (L). Laboratory analysis includes activities requiring the use of advanced analytical methods and means, exceeding the capabilities of chemical reconnaissance and special reconnaissance levels. SGRChem-Eko, with its L readiness level and qualified staff, provides expert support in interpreting incident data and analysis results obtained by the NFRS[13] entities.

The scope of the laboratory's tasks includes:

– direct participation in activities at the scene of the incident,
– analysis of samples provided by units involved in the NFRS,
– remote interpretation of transmitted chemical analysis results.

The SFS's CBRNE laboratories were designed in accordance with national regulations and international standards, including:

– standards concerning laboratory infrastructure and equipment (PN-EN 13150:2004[14], PN-EN 14175[15], PN-EN 14727:2006[16]),

[11] *Regulation of the Minister of the Interior and Administration of 17 September 2021 on the detailed organisation of the national firefighting and rescue system*.

[12] *Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym* (Eng. Principles of chemical and environmental rescue organisation in the national firefighting and rescue system), Warszawa 2025.

[13] Ibid., point 3.2L, p. 14.

[14] PN-EN 13150:2004 – Workbenches for laboratories – Dimensions, safety requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 2004.

[15] PN-EN 14175 (parts 1–6) – Fume cupboards, Polski Komitet Normalizacyjny, Warszawa.

[16] PN-EN 14727:2006 – Laboratory furniture – Storage units for laboratories – Requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 2006.

– standards for water, clean rooms and decontamination (PN-EN ISO 3696:1999[17], PN-EN ISO 14644[18]),
– biotechnology and biosafety standards (PN-EN 12128:2000[19], PN-EN 12740:2002[20], PN-EN 12469:2002[21]),
– standard concerning power and automation systems (PN-EN 62040[22]),
– performance standards for tanks and auxiliary equipment (PN-EN 13311-1:2004[23], PN-EN 12347:2002[24]),
– international and specialised standards (DIN 16892:2000-07[25], DIN 19541:2004-09[26]).

According to the manufacturer's declaration[27], the SFS's mobile CBRNE laboratories also comply with NATO standards, including:

– STANAG 4632[28] – Deployable NBC Analytical Laboratory,

[17] PN-EN ISO 3696:1999/Ap1:2004 – Water quality in analytical laboratories – Requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 1999/2004.

[18] PN-EN ISO 14644 – Cleanrooms and associated controlled environments, Polski Komitet Normalizacyjny, Warszawa.

[19] PN-EN 12128:2000/Ap1:2001 – Biotechnology – Laboratories for research, development and analysis – Degrees of airtightness of microbiology laboratories, risk zones and requirements regarding location and physical security, Polski Komitet Normalizacyjny, Warszawa 2000/2001.

[20] PN-EN 12740:2002 – Biotechnology – Laboratories for research, development and analysis – Guidance for handling, inactivating and testing of waste, Polski Komitet Normalizacyjny, Warszawa 2002.

[21] PN-EN 12469:2002 – Biotechnology – Performance criteria for microbiological safety cabinets, Polski Komitet Normalizacyjny, Warszawa 2002.

[22] PN-EN 62040 – Uninterruptible power systems (UPS), Polski Komitet Normalizacyjny, Warszawa.

[23] PN-EN 13311-1:2004 – Biotechnology – Performance criteria for vessels – Part 1: General performance criteria; PN-EN 13311-5:2004 – Biotechnology – Performance criteria for vessels – Part 5: Kill tanks, Polski Komitet Normalizacyjny, Warszawa 2004.

[24] PN-EN 12347:2002 – Biotechnology – Performance criteria for steam sterilizers and autoclaves, Polski Komitet Normalizacyjny, Warszawa 2002.

[25] DIN 16892:2000-07 – Kunststoff-Rohrleitungssysteme aus vernetztem Polyethylen (PE-X) – Allgemeine Güteanforderungen, Prüfungen, Deutsches Institut für Normung, Berlin 2000.

[26] DIN 19541:2004-09 – Abscheideranlagen für Leichtflüssigkeiten, Deutsches Institut für Normung, Berlin 2004.

[27] *PEX DEFENCE POLSKA – Prezentacja produktu Laboratorium CBRNE* (Eng. PEX DEFENCE POLSKA – Product presentation: CBRNE Laboratory), YouTube, https://www.youtube.com/watch?app=desktop&v=ClJ9FZuZGQM [accessed: 18 V 2025].

[28] STANAG 4632 (Edition 1) – *Deployable NBC Analytical Laboratory*, NATO Standardization Agency, Brussels 2005.

– AEP-66[29] – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA),
– DD/3.8(B)[30] – Defence against weapons of mass destruction in joint operations,
– DD 4.10(A)[31] – Medical support of the Polish Armed Forces.

Technical characteristics of the SFS's mobile CBRNE laboratories

The laboratory was designed as a complete, self-sufficient analytical system, capable of performing the entire research process in field conditions. The key design assumption was to reduce the time between sample collection and obtaining reliable analysis results, which is crucial in emergency situations. The system was divided into five key functional areas.

1. Time required for deployment and achieving operational readiness – the construction allows for achieving the required climatic conditions and analytical readiness in no more than 45 minutes from the moment of deployment (does not apply to devices requiring a longer stabilisation period).
2. Comprehensive analysis capabilities – the equipment enables detection and identification of chemical, biological, radiation and radioactive substances using advanced analytical devices (GC-MS, FTIR, Raman, PCR, XRF, IMS, HPGe, FPD)[32].
3. Autonomy and logistics – provided by 80 kW power generator and UPS, decontamination and wastewater management systems, allowing for long-term operation without access to external infrastructure.

[29] AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA), NATO Standardization Agency, Brussels 2015.

[30] DD/3.8(B) – Obrona przed bronią masowego rażenia w operacjach połączonych (Eng. Defence against weapons of mass destruction in joint operations), Ministerstwo Obrony Narodowej, Sztab Generalny Wojska Polskiego, Warszawa 2013.

[31] DD 4.10(A) – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej (Eng. Medical support of the Polish Armed Forces), Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2015.

[32] GC-MS – gas chromatography-mass spectrometry; FTIR – Fourier transform infrared spectroscopy; Raman – Raman spectroscopy; PCR – polymerase chain reaction; XRF – X-ray fluorescence; IMS – ion mobility spectrometry; HPGe – high-purity germanium gamma radiation detector, used in spectrometry; FPD – flame photometric detector, selective, among others, for sulphur and phosphorus compounds, commonly used in the analysis of warfare agents and toxic organic compounds.

4. Operator and environmental safety – meeting BSL-3 (biosafety level 3) class requirements applicable to work with high-risk airborne microorganisms. This was achieved through the use of hermetic personnel airlocks, Class III glove boxes, ventilation systems with HEPA H14 filters, and redundant safeguards.
5. Interoperability and integration with other services – compliance with NATO requirements for CBRNE reconnaissance, ability to work based on SIBCRA procedures (sampling and identification of biological, chemical and radiological agents) and operating in CBRN Reachback mode (remote exchange of data, expertise and consultations between field units and analytical and expert centres in the field of CBRN threats).

Structure and functional division

The laboratory was built on a three-axle semi-trailer with air suspension, enabling the safe transport of sensitive analytical devices. The semi-trailer is equipped with hydraulic stabilising supports, allowing it to operate in a stationary mode without needing a prime mover.

The functional layout of the laboratory consists of four main compartments.

1. Operational compartment (A) – extendable segment of the semi-trailer designed for managing onboard systems, serving as a supervision centre and climatic buffer. Once the vehicle is deployed, the extendable structure increases the working space.
2. Biological compartment (B) – laboratory meets BSL-3 containment conditions, it is equipped with a Class III glove box, fume hood, autoclave, decontamination system, HVAC system (heating, ventilation, air conditioning), as well as pass-through and personnel airlocks.
3. Chemical compartment (C) – the central part of the laboratory, dedicated to physicochemical analysis, equipped with chromatographs, spectrometers, an explosion-proof fume hood, and a laboratory sink with a drainage system to waste tanks.
4. Technical zones – contain supporting installations (filtration, ventilation, power supply systems).

The laboratory's technical infrastructure includes advanced power supply, ICT and environmental monitoring systems.

Filtration, ventilation and decontamination systems

The laboratory has advanced filtration and airflow control systems, which ensure safe operation with hazardous materials. The ventilation system was integrated with the filter-ventilation unit and generates a precisely controlled pressure cascade. Airflow is in accordance with zoning principles. This eliminates the possibility of cross-contamination. The air supplied to the laboratory space passes through a multi-stage purification system. It consists of pre-filters and high-efficiency HEPA H14 carbon filters, which meet the requirements of PN 1822:2009 standard[33]. The filter housings comply with PN-EN ISO 14644-3:2020 standard[34], which ensures leakage control and tightness of installation. The design allows for decontamination of filter housings using hydrogen peroxide.

The central ventilation unit handles an airflow of 1500 m^3/h, using only external air. The system maintains a precise pressure cascade – the personnel airlock operates at a reference pressure of 0 Pa, while the biological compartment operates under negative pressure at -30 Pa.

The biological compartment is equipped with advanced gaseous decontamination system which uses hydrogen peroxide. This enables complete sterilisation of the compartment, glove box and filtration system components. Personnel decontamination is ensured by a special personnel airlock with a water shower and protective clothing. Interlock system prevents the simultaneous opening of doors to the contaminated and clean zones.

Analytical equipment

The SFS's mobile CBRNE laboratory is equipped with advanced analytical equipment enabling the identification of a wide range of chemical, biological and radiological hazards. The equipment was selected based on its ability to quickly and accurately identify hazardous substances in various environmental matrices.

[33] PN-EN 1822-1:2009 – High efficiency air filters (EPA, HEPA and ULPA) – Part 1: Classification, performance testing, marking, Polski Komitet Normalizacyjny, Warszawa 2009.

[34] PN-EN ISO 14644-3:2020 – Cleanrooms and associated controlled environments – Part 3: Test methods, Polski Komitet Normalizacyjny, Warszawa 2020. The standard specifies methods for verifying the tightness, integrity of installation and leakage control in ventilation and filtration systems, including testing of HEPA/ULPA filter housings, air flows and pressure differences.

Chemistry module is equipped with:

- Gas Chromatograph-Mass Spectrometer GC-MS with FPD and FTIR detectors for detecting and identifying chemical warfare agents, pesticides, aromatic compounds, and halogenated derivatives,
- FTIR/ATR spectrometer[35] equipped with attachments for analysis of gas and liquid,
- UV-VIS spectrophotometer for determining pollutants in water and soil,
- Ion Chromatograph (IC) for quantitative determination of anions and cations in water samples, sewage,
- microscope and handheld RAMAN spectrometers for analysing solid substances and explosives,
- PID and IMS/AP4C kits for rapid detection of hazardous substances in the air,
- XRF spectrometers for elemental composition analysis.

Biological module is equipped with:

- PCR detection device – an advanced system that isolates genetic material (DNA or RNA[36]) and analyses it for pathogens. It allows for the simultaneous identification of at least ten different biological agents (recognised as biological weapons). The device is designed for safe operation inside a glove box under vacuum conditions,
- disposable colorimetric tests for rapid preliminary assessment of samples, intended mainly for the analysis of powders and loose substances, enabling the detection of proteins, bacterial spores and determination of Ph,
- bioluminometer for detecting ATP[37] on surfaces and in liquid samples, enabling rapid assessment of the degree of biological contamination,
- mechanical homogeniser for preparing biological samples in hermetically sealed, disposable tubes, which reduces the risk of infectious material being released during processing,
- sample preparation systems, including laboratory centrifuges, shakers for mixing small volumes, and a set of automatic pipettes with filters suitable for autoclave sterilisation.

[35] FTIR/ATR (Fourier transform infrared spectroscopy with attenuated total reflectance) – infrared spectroscopy technique enabling direct analysis of sample surfaces without preparation.

[36] DNA (deoxyribonucleic acid) and RNA (ribonucleic acid) – they constitute the genetic material of organisms and viruses. It is used in molecular diagnostics to identify biological agents.

[37] ATP (adenosine triphosphate) is a universal energy carrier found in living cells. Its detection by bioluminescence is a non-specific, rapid indicator of the presence of active biological material on surfaces and in liquid samples. It is used in screening analyses for biological contamination.

The following are used to identify radiation and nuclear hazards:

– Polimaster radiation spectrometer (detection of alpha, beta, gamma radiation and neutrons),
– portable HPGe gamma radiation spectrometer based on an HPGe semiconductor detector, which identifies over 400 different isotopes.

Spectrometric measurements are conducted according to standard operating procedures of IAEA (International Atomic Energy Agency) and NATO, with acquisition times ranging from 1–5 minutes (rapid scanning) to 15–60 minutes (accurate quantitative analyses). These devices are fully compatible with SIBCRA procedures and CBRN Reachback data exchange systems.

Operational scenarios and areas of application for CBRNE mobile laboratories of the SFS

The SFS's mobile CBRNE laboratory is intended for use in the following operational scenarios:

1) identification of hazardous shipments and unknown substances – carried out in accordance with procedures of the National Headquarters of the SFS, including a full protocol for securing the material, its transport and analysis[38],
2) contamination assessment – conducting analysis of soil, air and water, including determining the presence of volatile organic compounds and heavy metals,
3) security for mass events and high-risk occurrences – proactive environmental monitoring and control for the presence of hazardous substances,
4) support for law enforcement agencies – identification of explosives, narcotics, designer drugs and other substances.

According to the *Principles of chemical and environmental rescue organisation in the national firefighting and rescue system*, when dispatching SGRChem-Eko teams with readiness level L for direct rescue operations, SGRChem-Eko teams with readiness level B are also dispatched each time. This is to ensure a comprehensive

[38] *Regulation of the Minister of the Interior and Administration of 17 September 2021…*, § 16; *Principles of chemical and environmental rescue organisation…*, appendix no. B.2: *Rules of conduct for the State Fire Service in the event of a threat involving an unidentified parcel and organisation of transport of biological materials to laboratory.*

approach to hazard identification – the chemical reconnaissance group (B) supports the analytical activities of the laboratory (L).

A specific area of application for the mobile CBRNE laboratory is the identification of radiation hazards, which involves:

- verifying reports of hazards at the scene of the incident,
- performing radiometric measurements to determine the level of exposure,
- designating an area where the ionising radiation dose exceeds 100 μSv/h and/or radioactive contamination is present,
- identification of radioactive isotopes,
- cooperation with other services involved in the operations.

The radiation equipment of the SFS's mobile CBRNE laboratory, including radiation spectrometers and HPGe detectors, enables precise identification of radioactive isotopes, which is crucial for determining the nature of the threat and selecting the appropriate neutralisation methods.

Challenges and limitations associated with the SFS's mobile CBRNE laboratories

Despite advanced technical solutions and a high level of compliance with standards, the use of the SFS's mobile CBRNE laboratories involves certain challenges and limitations that need to be taken into account in operational planning. One of the most limitations stems from the fact that, despite being designed in accordance with the safety requirements for BSL-3 laboratories, the mobile laboratory cannot be formally classified as a fully-fledged laboratory of this class. According to normative definitions, laboratories of this type must be permanent, immovable structures. The laboratory semi-trailer does not meet this requirement. There is also no validation certification in accordance with PN-EN ISO 14644-3:2020 standard. Furthermore, the SFS's CBRNE laboratory was designed for short-term activities (rescue operations, security measures) rather than for long-term breeding, pathogen research or work with high-risk strains. However, its functional layout and the technologies used enable the effective analysis of high-risk samples in field conditions, in accordance with best biosafety practices.

A significant challenge is ensuring that there are sufficient specialists to operate the laboratory. According to the *Principles of chemical and environmental rescue organisation in the national firefighting and rescue system*, designated chemical rescue workers from SGRChem-Eko with readiness level L should additionally have a university degree in chemistry, physics or biology. Recruiting and retaining such highly qualified personnel within the SFS structures may pose an organisational

and financial challenge. SGRChem-Eko at readiness level L should consist of at least 12 firefighters or rescuers, including at least:

1) 12 chemical rescuers,
2) 12 chemical rescuers authorised to operate the specialist equipment constituting the L-level group's equipment,
3) 6 chemical rescuers authorised to operate motor vehicles,
4) 9 chemical rescuers with higher education in chemistry, physics or biology (…)[39].

Ensuring the continuity of the group's operations with such high competency requirements necessitates long-term career planning for officers and a systematic approach to their professional development.

Although designed as an autonomous unit, the SFS's mobile CBRNE laboratory requires adequate logistical support. In the event of contamination caused by warfare or a terrorist attack, the laboratory must be able to operate under conditions of limited access to resources such as water or fuel. This requires detailed operational planning and logistical security. Performing analytical tasks in conditions of limited resources is a major challenge, especially in the context of potential chemical hazards, e.g. in or near a war zone. In the event of more serious incidents involving hazardous materials, it may be necessary to deploy more specialists and use additional analytical resources. The undertaking of direct rescue operations by SGRChem-Eko at readiness level L is conditional, as already mentioned, on the presence of SGRChem-Eko at readiness level B at the scene of the incident. This approach ensures the complementarity of operations, but requires coordination between different levels of operational readiness and different SFS units. Joint exercises and training for these units are essential. Failure to provide them may lead to communication problems, unfamiliarity with operational procedures, and inefficient use of advanced analytical equipment during real-life CBRNE incidents. As a result, the potential of the mobile laboratory may not be fully exploited, and the response time to a threat may be prolonged. Regular exercises integrating various levels of SGRChem-Eko preparedness are a key element in building a coherent and effective response system for incidents involving hazardous materials.

[39] *Principles of chemical and environmental rescue organisation*…, point 3.4.L, p. 19.

Prospects for the development of mobile CBRNE laboratories in the Polish security system

The implementation of the SFS's mobile CBRNE laboratories is an important step in the development of analytical capabilities, as it enables rapid and accurate identification of threats directly at the scene of an incident. The development of these capabilities should be based on both national experience and international trends in the area of responding to CBRNE incidents. The priority for the coming years seems to be to deepen the integration of mobile laboratories with the multi-level crisis management system. Thanks to their compliance with key NATO standards (STANAG 4632, AEP-66) and their ability to interoperate within the EU Civil Protection Mechanism, SFS laboratories can function effectively within the European crisis response network. Such integration not only provides the possibility of receiving international support in the event of large-scale incidents, but also allows for the provision of specialist assistance to other EU Member States. The ability to operate within CBRNE Reachback system is particularly valuable in the context of geographically dispersed analytical resources. In order to fully exploit this potential, dedicated ICT infrastructure should be developed and analytical data exchange protocols should be standardised. Development of mobile CBRNE laboratories should therefore take into account the exploration of new applications and integration with existing infrastructure, which could significantly increase the effectiveness of rescue operations in the event of incidents involving CBRNE materials. It is relevant to modernise analytical equipment in parallel with the development of system integration. The evolution of CBRNE threats, including new substances and methods of their use, requires continuous adaptation of detection capabilities. Development directions should take into account advanced measurement techniques, solutions using artificial intelligence to interpret complex data, and systems that integrate information from various types of detectors and sensors.

Due to Poland's location, mobile CBRNE laboratories are gaining additional strategic importance. The experiences of the war in Ukraine highlight the importance of mobile analytical capabilities. Cases of industrial infrastructure destruction, especially in urbanised regions, demonstrate the reality of the risk of large-scale release of toxic chemicals. The ability to quickly detect and identify these substances can be crucial for protecting the civilian population. As a border state of both the EU and NATO, Poland can play a special role in building a regional CBRNE response system. Advanced analytical capabilities can be part of cross-border cooperation. In this context, mobile laboratories are not only part of the national security system,

but also a component of potential international support, strengthening collective resilience to asymmetric threats in Central and Eastern Europe.

Conclusions

The analyses showed that the SFS's mobile laboratories meet key regulatory requirements and have high operational potential. Technical solutions used in these laboratories comply with applicable laws, technical standards and NATO standards, which strengthens the national and international interoperability of the SFS. The integration of advanced filtration systems, airtight working compartments and specialised analytical equipment enables operations to be carried out in a variety of conditions.

According to the author, the research results confirm the hypothesis that the high level of technological advancement of mobile CBRNE laboratories poses organisational and operational challenges, which require the implementation of adequate system solutions to overcome. These include the need to ensure highly qualified personnel, the development of procedures integrating various levels of SGRChem-Eco, stable equipment maintenance mechanisms, and systematic exercises to improve interoperability.

In the face of the dynamics of asymmetric threats, mobile laboratories should be seen not only as a technological breakthrough, but above all as a strategic investment in national security and civil protection. Development of laboratory capabilities should include the modernisation of equipment, the implementation of artificial intelligence solutions and deepening of international cooperation, which will allow their potential to be fully exploited in the crisis response system.

Bibliography

CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapons, A. Richardt, B. Hülseweh, B. Niemeyer, F. Sabath (eds.), Weinheim 2013.

Di Giovanni D., Fumian F., Chierici A., Bianchelli M., Martellucci L., Carminati G., Malizia A., d'Errico F., Gaudio P., *Design of Miniaturized Sensors for a Mission-Oriented UAV Application: A New Pathway for Early Warning*, "International Journal of Safety and Security Engineering" 2021, vol. 11, no. 4, pp. 435–444. https://doi.org/10.18280/ijsse.110417.

Gawlik-Kobylińska M., Gudzbeler G., Szklarski Ł., Kopp N., Koch-Eschweiler H., Urban M., *The EU-SENSE System for Chemical Hazards Detection, Identification, and Monitoring*, "Applied Sciences" 2021, vol. 11, no. 21, 10308. https://doi.org/10.3390/app112110308.

Gawlik-Kobylińska M., Urban M., Gudzbeler G., *The EU-SENSE System as a Tool to Support Airport Security*, in: *Reliability and Statistics in Transportation and Communication: Human Sustainability and Resilience in the Digital Age*, I. Kabashkin, I. Yatskiv, O. Prentkovskis (eds.), pp. 597–605, series: Lecture Notes in Networks and Systems, vol. 1337, Cham 2025. https://doi.org/10.1007/978-3-031-87532-8_53.

Kinnunen P.M., Haataja T., Hemmila H., Maatela P., Teho K., Elo M., Raijas T., Nikkari S., *Mobile Diagnostic CBRN Field Laboratory: NATO evaluated Finnish Design*, "Challenge – Medical CBRN Defence International" 2012, no. 1.

Mari G., Giraudi G., Bellino M., Pazienza M., Garibaldi C., Lancia C., *CBRN mobile laboratories in Italy*, "Proceedings SPIE 7304, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing X", vol. 7304. https://doi.org/10.1117/12.819445.

Parsons A., Matero P., Adams M., Yeh K., *Examining the utility and readiness of mobile and field transportable laboratories for biodefence and global health security-related purposes*, "Global Security: Health, Science and Policy" 2018, vol. 3, no. 1, pp. 1–13. https://doi.org/10.1080/23779497.2018.1480403.

Przeciwdziałanie zagrożeniom CBRNE – aspekty teoretyczne i praktyczne (Eng. Counteracting CBRNE threats – theoretical and practical aspects), Ł. Jureńczyk, A. Pieczywok, M. Urban (eds.), Bydgoszcz 2024.

Rabajczyk A., Zboina J., Zielecka M., Fellner R., *Monitoring of Selected CBRN Threats in the Air in Industrial Areas with the Use of Unmanned Aerial Vehicles*, "Atmosphere" 2020, no. 11, 1373. https://doi.org/10.3390/atmos11121373.

Szklarski Ł., *CBRN threats, EU-SENSE system: Paving the way for future national security systems – an assessment of the suitability of the concept for the future of national security*, "Zeszyty Naukowe SGSP" 2024, vol. 2, no. 89, pp. 139–156. https://doi.org/10.5604/01.3001.0054.3833.

Szklarski Ł., *Diagnoza potrzeb w zakresie usprawnienia technologii i sprzętu służącego reagowaniu na incydenty o charakterze CBRN. Zarys problemu z perspektywy europejskich straży pożarnych* (Eng. A diagnosis of needs for improvements of technology and hardware used by units responding to CBRN-related incidents. An outline of the problem from the perspective of European fire services), "Zeszyty Naukowe SGSP" 2021, vol. 2, no. 80, pp. 142–160. https://doi.org/10.5604/01.3001.0015.6474.

Toader C., Epure G., Mosteanu D., Epure C., Iorga O., Florin I., *Mobile Deployable Laboratory – Chemical Module*, "International Conference KNOWLEDGE-BASED ORGANIZATION" 2016, vol. 22, no. 3, pp. 677–680. https://doi.org/10.1515/kbo-2016-0116.

Urban M., *Protection of Airports against the Threat of CBRNE*, "Studia Bezpieczeństwa Narodowego" 2023, vol. 29, no. 3, pp. 7–34. https://doi.org/10.37055/sbn/171016.

Internet sources

Final Report Summary – MIRACLE (Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU), CORDIS - EU research results, 9 II 2016, https://cordis.europa.eu/project/id/312885/reporting [accessed: 25 IX 2025].

Jankowski R., Wereski P., *CBRNE lab*, Przegląd Pożarniczy, https://www.ppoz.pl/czytelnia/ratownictwo-i-ochrona-ludnosci/CBRNE-lab/idn:2828 [accessed: 25 IX 2025].

PEX DEFENCE POLSKA – Prezentacja produktu Laboratorium CBRNE (Eng. PEX DEFENCE POLSKA – Product presentation: CBRNE Laboratory), YouTube, https://www.youtube.com/watch?app=desktop&v=ClJ9FZuZGQM [accessed: 18 V 2025].

Legal acts

Act of 24 August 1991 on the State Fire Service (consolidated text, Journal of Laws of 2025, item 1312, as amended).

Regulation of the Minister of the Interior and Administration of 17 September 2021 on the detailed organisation of the national firefighting and rescue system (Journal of Laws of 2021, item 1737).

Other documents

AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA), NATO Standardization Agency, Brussels 2015.

DD/3.8(B) – Obrona przed bronią masowego rażenia w operacjach połączonych (Eng. Defence against weapons of mass destruction in joint operations), Ministerstwo Obrony Narodowej, Sztab Generalny Wojska Polskiego, Warszawa 2013.

DD 4.10(A) – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej (Eng. Medical support of the Polish Armed Forces), Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2015.

STANAG 4632 (Edition 1) – Deployable NBC Analytical Laboratory, NATO Standardization Agency, Brussels 2005.

Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym (Eng. Principles of chemical and environmental rescue organisation in the national firefighting and rescue system), Warszawa 2025.

Polish standards

PN-EN 12469:2002 – Biotechnology – Performance criteria for microbiological safety cabinets, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 12347:2002 – Biotechnology – Performance criteria for steam sterilizers and autoclaves, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 13311-1:2004 – Biotechnology – Performance criteria for vessels – Part 1: General performance criteria.

PN-EN 13311-5:2004 – Biotechnology – Performance criteria for vessels – Part 5: Kill tanks, Polski Komitet Normalizacyjny, Warszawa 2004.

PN-EN 12740:2002 – Biotechnology – Laboratories for research, development and analysis – Guidance for handling, inactivating and testing of waste, Polski Komitet Normalizacyjny, Warszawa 2002.

PN-EN 12128:2000/Ap1:2001 – Biotechnology – Laboratories for research, development and analysis – Degrees of airtightness of microbiology laboratories, risk zones and requirements regarding location and physical security, Polski Komitet Normalizacyjny, Warszawa 2000/2001.

PN-EN 14727:2006 – Laboratory furniture – Storage units for laboratories – Requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 2006.

PN-EN ISO 14644 – Cleanrooms and associated controlled environments, Polski Komitet Normalizacyjny, Warszawa.

PN-EN 13150:2004 – Workbenches for laboratories – Dimensions, safety requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 2004.

PN-EN 62040 – Uninterruptible power systems (UPS), Polski Komitet Normalizacyjny, Warszawa.

PN-EN ISO 3696:1999/Ap1:2004 – Water quality in analytical laboratories – Requirements and test methods, Polski Komitet Normalizacyjny, Warszawa 1999/2004.

PN-EN 14175 (parts 1–6) – Fume cupboards, Polski Komitet Normalizacyjny, Warszawa.

PN-EN 1822-1:2009 – High efficiency air filters (EPA, HEPA and ULPA) – Part 1: Classification, performance testing, marking, Polski Komitet Normalizacyjny, Warszawa 2009.

German standards

DIN 19541:2004-09 – Abscheideranlagen für Leichtflüssigkeiten, Deutsches Institut für Normung, Berlin 2004.

DIN 16892:2000-07 – Kunststoff-Rohrleitungssysteme aus vernetztem Polyethylen (PE-X) – Allgemeine Güteanforderungen, Prüfungen, Deutsches Institut für Normung, Berlin 2000.

Senior Brig. (Ret.) Grzegorz Bugaj, PhD

Former Vice-Rector – Deputy Commandant of the Main School of Fire Service (currently the Fire University). For many years he served as the Commander of the Specialized Chemical Rescue Group and Fire and Rescue Unit No. 6 in Warsaw, as well as the Commander of the "CBRN Det. Mazowsze" module within the EU Civil Protection Mechanism. He has over 30 years of operational experience in the State Fire Service, primarily within the Warsaw metropolitan area. He is a graduate of the Main School of Fire Service and the Fire Service Academy, as well as the University of Łódź (Faculty of Biology and Environmental Protection), Poznań Medical Academy, and the Central Institute for Labour Protection. He currently provides expert and training services.

Contact: g.bugaj@cbrne.org.pl

Internal Security Review
2026, no. 34, pp. 299–329

https://doi.org/10.4467/20801335PBW.26.014.23376

ARTICLE

Study on the retention of Border Guard officers in the context of staff level security within the formation

RADOSŁAW WIŚNIEWSKI

The Border Guard Higher School

https://orcid.org/0009-0005-0751-9002

DENIS TOMALA

The Border Guard Higher School

https://orcid.org/0009-0008-0169-1612

Abstract

The aim of the study was to determine the extent to which individual and organisational factors influence the retention of Border Guard officers. The impact of job satisfaction, organisational commitment, and perseverance on the intention to remain in service and the intention to leave service was analysed. The study was conducted among 184 Border Guard officers using a questionnaire survey. Partial least squares structural equation modeling (PLS-SEM) was used, which enabled the simultaneous analysis of multiple relationships. The developed model is characterised by a good fit and high explanatory power – the variables included in the model explain over 50% of the variance in the intention to leave the service. It was found that job satisfaction, organisational commitment, and perseverance significantly increase the intention to remain in the force, which should be taken into account in solutions to counteract the departure of officers.

Keywords

retention, organisational commitment, satisfaction, perseverance, PLS-SEM, Border Guard

Introduction

Demographic changes in Poland related to population decline and ageing are reducing the pool of people of working age. These changes are resulting in competition for job and service candidates as well as creating solutions to improve staff retention (Latin: retentio). Ensuring that there are sufficient numbers of properly trained personnel to carry out the statutory tasks of individual uniformed services is therefore a challenge in terms of personnel security, which is a prerequisite for national security. The issue of staff retention is universal and affects both domestic and foreign uniformed services, which struggle with premature departures from service and staff vacancies. This situation prompts a search for solutions that not only increase interest in serving in uniformed services, but also optimise conditions for long-term service. These intentions are reflected, among other things, in the content of the command issued by the U.S. Army Chief of Staff[1] and in the order of the Secretary of State of the Ministry of the Interior and Administration of the Republic of Poland[2], relating to the problem of the staff retention. The need to ensure personnel security has led to various initiatives and research projects being taken in the uniformed services. The US Army is conducting retention studies involving several million soldiers[3], aimed at determining the reasons for leaving the service. On the other hand, factors influencing graduation or dropping out were identified among the cadets at the elite West Point Academy[4]. Furthermore, NATO task force worked to fully investigate the mechanisms influencing recruitment and retention outcomes[5].

---

1 W.J. Strickland, *A Longitudinal Examination of First Term Attrition and Reenlistment Among FY1999 Enlisted Accessions*, https://apps.dtic.mil/sti/tr/pdf/ADA448564.pdf, p. V [accessed: 10 I 2025].

2 Najwyższa Izba Kontroli (Eng. The Supreme Audit Office), *Informacja o wynikach kontroli pt. Realizacja programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2017–2020* (Eng. Information on the results of the audit entitled Implementation of the modernisation programme of the Police, the Border Guard, the State Fire Service, the State Protection Service in 2017–2020), https://www.nik.gov.pl/plik/id,21396,vp,24037.pdf [accessed: 12 II 2025].

3 J.V. Marrone, *Predicting 36-Month Attrition in the U.S. Military. A Comparison Across Service Branches*, Santa Monica 2020, p. 11. https://doi.org/10.7249/RR4258.

4 D.R. Kelly, M.D. Matthews, P.T. Bartone, *Grit and Hardiness as Predictors of Performance Among West Point Cadets*, "Military Psychology" 2014, vol. 26, no. 4, pp. 327–342. https://doi.org/10.1037/mil0000050.

5 North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel. Final Report of Research Task Group HFM-107*, https://apps.dtic.mil/sti/tr/pdf/ADA476488.pdf [accessed: 11 I 2025].

There is a lack of similar studies in Polish uniformed services, which is why addressing this issue seems highly justified in relation to the security of the personnel of the formation and the state, as well as the expenditure of significant budgetary resources for this purpose. The article describes research conducted at the Border Guard Higher School among 184 officers, taking into account their opinions, assessments and intentions related to continuing or terminating their service. The research problem is the question: what individual and organisational factors influence the intention to remain in service and the intention to leave service? The aim of the study was to identify and measure the variables that influence the intention to remain in service and the intention to leave it. The objective was achieved by using a partially structured questionnaire survey method and partial least squares structural equation modeling (PLS-SEM).

Literature review

A review of the literature on staff retention in the civil service and civilian entities allowed for the selection of an appropriate methodology and variables. The analysis showed that a two-way approach is used in staff retention studies, in which factors influencing the willingness to remain in the organisation are identified, and factors influencing the willingness to leave it are revealed[6]. This approach to the issue is based on the assumptions of a theory of planned behaviour[7] that links behavioural intentions with actual behaviour – which has been empirically confirmed[8]. The research is conducted among people currently working in the institution or performing service, who are asked about their intentions to remain in or leave the organisation and about the factors influencing this. This solution was adopted due to experience indicating that individuals who have resigned from an organisation are reluctant to discuss the reasons for their decision.

---

[6] See for example: M.C. Lytell, F. Drasgow, *"Timely" Methods: Examining Turnover Rates in the U.S. Military*, "Military Psychology" 2009, vol. 21, no. 3, pp. 334–350. https://doi.org/10.1080/08995600902914693; T.W. Lee, T.R. Mitchell, *The unfolding effects of organizational commitment and anticipated job satisfaction on voluntary employee turnover*, "Motivation and Emotion" 1991, vol. 15, no. 1, pp. 99–121. https://doi.org/10.1007/BF00991478.

[7] I. Ajzen, *From Intentions to Actions: A Theory of Planned Behawior*, in: *Action Control: From Cognition to Behavior*, J. Kuhl, J. Beckmann (eds.), Berlin 1985, pp. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2.

[8] B.H. Sheppard, J. Hartwick, P.R. Warshaw, *The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research,* "Journal of Consumer Research" 1988, vol. 15, no. 3, pp. 325–343. https://doi.org/10.1086/209170.

Staff retention is therefore determined on the basis of declared intention to stay, understood – according to Robert P. Tett and John P. Meyer – as the conscious and deliberate desire of employees to remain in the organisation[9], and intention to leave, defined by William H. Mobley, Stanley O. Horner, Abner T. Hollingsworth as the conscious and deliberate desire to leave the organisation in the near future[10]. Intention to leave is considered a direct predictor of actual turnover in retention models[11], which has also been empirically confirmed[12].

The best-researched and statistically confirmed variables influencing the intention to stay or leave (both in the military and civilian entities) are job satisfaction and organisational commitment[13]. There is no single generally accepted definition of these concepts in the literature, and their meanings vary. Paul E. Spector defines job satisfaction as a feeling about work and its various

---

[9] R.P. Tett, J.P. Meyer, *Job satisfaction, organizational commitment, turnover intention, and turnover: Path analyses based on meta-analytic findings*, "Personnel Psychology" 1993, vol. 46, no. 2, pp. 259––293. https://doi.org/10.1111/j.1744-6570.1993.tb00874.x.

[10] W.H. Mobley, S.O. Horner, A.T. Hollingsworth, *An evaluation of precursors of hospital employee turnover*, "Journal of Applied Psychology" 1978, vol. 63, no. 4, pp. 408–414. https://doi.org/10.1037/0021-9010.63.4.408.

[11] D. Pitts, J. Marvel, S. Fernandez, *So Hard to Say Goodbye? Turnover Intention among U.S. Federal Employees*, "Public Administration Review" 2011, vol. 71, no. 5, pp. 751–760. https://doi.org/10.1111/j.1540-6210.2011.02414.x; R.W. Griffeth, P.W. Hom, S. Gaertner, *A Meta-Analysis of Antecedents and Correlates of Employee Turnover: Update, Moderator Tests, and Research Implications for the Next Millennium*, "Journal of Management" 2000, vol. 26, no. 3, pp. 463–488. https://doi.org/10.1177/014920630002600305.

[12] Y.J. Cho, G.B. Lewis, *Turnover Intention and Turnover Behavior: Implications for Retaining Federal Employees*, "Review of Public Personnel Administration" 2011, vol. 32, no. 1, pp. 4–23. https://doi.org/10.1177/0734371X11408701; A.H. Huffman et al., *The Impact of Operations Tempo on Turnover Intentions of Army Personnel*, "Military Psychology" 2005, vol. 17, no. 3, pp. 175–202. https://doi.org/10.1207/s15327876mp1703_4.

[13] See for example: North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel…*, p. 329; H.M. Weiss et al., *Retention in the Armed Forces: Past Approaches and New Research Directions*, https://www.mfri.purdue.edu/wp-content/uploads/2018/03/Retention-in-the-Armed-Forces.pdf [accessed: 17 I 2025]; W.J. Strickland, *A Longitudinal Examination…*, p. 9; R.W. Griffeth, P.W. Hom, S. Gaertner, *A Meta-Analysis of Antecedents…*; D.B Currivan, *The Causal Order of Job Satisfaction and Organizational Commitment in Models of Employee Turnover*, "Human Resource Management Review" 1999, vol. 9, no. 4, pp. 495–524. https://doi.org/10.1016/S1053-4822(99)00031-5; T.W. Lee, T.R. Mitchell, *The unfolding effects of organizational commitment…*; S. Gaertner, *Structural Determinants of Job Satisfaction and Organizational Commitment in Turnover Models*, "Human Resource Management Review" 1999, vol. 9, no. 4, pp. 479–493. https://doi.org/10.1016/S1053-4822(99)00030-3; P.W. Hom et al., *A meta-analytical structural equations analysis of a model of employee turnover*, "Journal of Applied Psychology" 1992, vol. 77, no. 6, pp. 890–909. https://doi.org/10.1037/0021-9010.77.6.890.

aspects[14], which, according to Edwin A. Locke, depends on whether the work allows the emploee to satisfy their important needs[15]. Job satisfaction studies often refer to Frederick Herzberg's motivation-hygiene theory that points to the influence of motivating factors (motivators) on the level of satisfaction and hygiene factors (demotivators) on dissatisfaction, which together influence staff retention[16]. John P. Meyer and Natalie J. Allen define organisational commitment as a psychological state that characterises the employee's relationship with the organisation and influences the decision to continue or terminate membership in the organisation[17]. It consists of three dimensions: affective, continuance, and normative. The affective component refers to the employee's emotional attachment to the organisation, identification with it, and commitment to its activities. The continuance (calculative) component concerns attachment based on the costs that the employee associates with leaving the organisation, while the normative component is related to the sense of duty to remain in the organisation[18]. Furthermore, Richard T. Mowday, Richard M. Steers and Lyman W. Porter pointed out that organisational commitment includes a willingness to make an effort for the organisation, belief in its values and acceptance of its goals[19].

In addition to the factors traditionally considered in staff retention studies, such as job satisfaction and organisational commitment, new factors have emerged that are being investigated both in the services and in civilian entities. One of them is perseverance. This construct was defined as the pursuit of long-term goals with

---

[14] P.E. Spector, *The Nature of Job Satisfaction*, in: idem, *Job Satisfaction: Application, Assessment, Causes, and Consequences*, London 1997, p. 2. https://doi.org/10.4135/9781452231549.n1.

[15] E.A. Locke, *The Nature and Causes of Job Satisfaction*, College Park 1976, https://www.researchgate.net/publication/238742406_The_Nature_and_Causes_of_Job_Satisfaction, p. 1307 [accessed: 13 I 2025].

[16] F. Herzberg, B. Mausner, B.B. Snyderman, *The Motivation to Work*, New York 1959, https://api.pageplace.de/preview/DT0400.9781351504430_A30546568/preview-9781351504430_A30546568.pdf [accessed: 18 I 2025]; H. Dogonyaro, F. Nwosu, *Exploring Employee Retention in the Hospitality Industry Through Herzberg's Two-Factor Motivation Theory*, preprint. https://doi.org/10.13140/RG.2.2.34721.93287; L.C. Chiat, S.A. Panatik, *Perceptions of Employee Turnover Intention by Herzberg's Motivation-Hygiene Theory: A Systematic Literature Review*, "Journal of Research in Psychology" 2019, vol. 1, no. 2, pp. 10–15. https://doi.org/10.31580/jrp.v1i2.949.

[17] J.P. Meyer, N.J. Allen, *A three-component conceptualization of organizational commitment*, "Human Resource Management Review" 1991, vol. 1, no. 1, pp. 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z.

[18] N.J. Allen, J.P. Meyer, *The measurement and antecedents of affective, continuance and normative commitment to the organization*, "Journal of Occupational Psychology" 1990, vol. 63, no. 1, pp. 1–18. https://doi.org/10.1111/j.2044-8325.1990.tb00506.x.

[19] R.T. Mowday, R.M. Steers, L.W. Porter, *The measurement of organizational commitment*, "Journal of Vocational Behavior" 1979, vol. 14, no. 2, pp. 224–247. https://doi.org/10.1016/0001-8791(79)90072-1.

perseverance and passion[20], and the results of the study showed that individuals with higher levels of perseverance were significantly less likely to voluntarily drop out of the demanding 24-day Army Special Operations Forces (ARSOF) course[21] than individuals with lower levels of perseverance[22]. A study conducted among 1558 cadets at the West Point Academy also confirmed that perseverance was a reliable predictor of resignation – a higher level of perseverance significantly increased the chance of completing the four-year training program at the academy[23]. Perseverance is therefore identified as a promising predictor of retention that could be used in the uniformed services, although further research is needed for full confirmation[24].

The variables characterised were also adopted in a research project carried out in the Border Guard Higher School and compiled in Table 1.

Table 1. Definitions of the variables used in the study.

Variable name	Definition	Sources
Job satisfaction	Feeling about work and its various aspects. Depends on whether the work allows the emploee to satisfy their important needs	P.E. Spector (1997) E.A. Locke (1976) F. Herzberg (1959)
Organisational commitment	Psychological state that characterises the employee's relationship with the organisation and influences the decision to continue or terminate membership in the organisation. Readiness to make an effort for the organisation and belief in its values and acceptance of its goals	J.P. Meyer, N.J. Allen (1991) R.T. Mowday, R.M. Steers, L.W. Porter (1979)
Perseverance	Pursuit of long-term goals with perseverance and passion	A.L. Duckworth, C. Peterson, M.D. Matthews, D.R. Kelly (2007)

[20] A.L. Duckworth et al., *Grit: Perseverance and passion for long-term goals*, "Journal of Personality and Social Psychology" 2007, vol. 92, no. 6, pp. 1087–1101. https://doi.org/10.1037/0022-3514.92.6.1087.

[21] ARSOF training focuses on intensive physical and mental fitness tests, leadership, problem solving, and cultural adaptation in order to select candidates who are ready for the unique demands of special forces. Its essence is rigorous selection and identification of individuals capable of mastering irregular warfare, unconventional tactics, and operating globally.

[22] L. Eskreis-Winkler et al., *The grit effect: predicting retention in the military, the workplace, school and marriage*, "Frontiers in Psychology" 2014, vol. 5, no. 36. https://doi.org/10.3389/fpsyg.2014.00036.

[23] D.R. Kelly, M.D. Matthews, P.T. Bartone, *Grit and Hardiness…*

[24] K.N. Roach, *Leveraging Grit in Military Research: A Comprehensive Review*, https://apps.dtic.mil/sti/trecms/pdf/AD1211251.pdf [accessed: 20 I 2025].

Variable name	Definition	Sources
Intention to stay in organisation	Intention relating to conscious and deliberate desire of employees to remain in the organisation	R.P. Tett, J.P. Meyer (1993)
Intention to leave the organisaton	Conscious and deliberate desire of employees to leave the organisation	W.H. Mobley, S.O. Horner, A.T. Hollingsworth (1978)

Source: own elaboration based on the literature on the subject.

Research methodology

The methodology and organisation of the research were inspired by the project A Longitudinal Examination of First Term Attrition and Reenlistment among FY1999 Enlisted Accessions implemented in the U.S. Army by the United States Army Research Institute for the Behavioral and Social Sciences. The project described the research approach and tools, as well as the most important results of staff retention management. The research project, formally approved by the Border Guard Higher School, covered permanent officers training at the university. The criterion for selection for the research sample was availability, and the ethical conditions of the study were voluntary participation and anonymity of respondents. The final research sample included 184 officers with at least three years' service, a diverse in terms of gender, age, length of service, as well as units and posts they represent. The research data was collected between February and September 2024.

The review of the literature on the subject, ongoing projects and professional needs in the area of staff retention made it possible to set the main objective of the study: to identify and measure variables influencing the intention to remain in service and the intention to leave it.

The directions of the research were reflected in the following hypotheses and the presented conceptual model (Figure 1):

H1: Satisfaction, organisational commitment, perseverance will have a significant and positive impact on the intention to remain in service.

H2: Satisfaction, organisational commitment, perseverance will have a significant and negative impact on the intention to leave service.

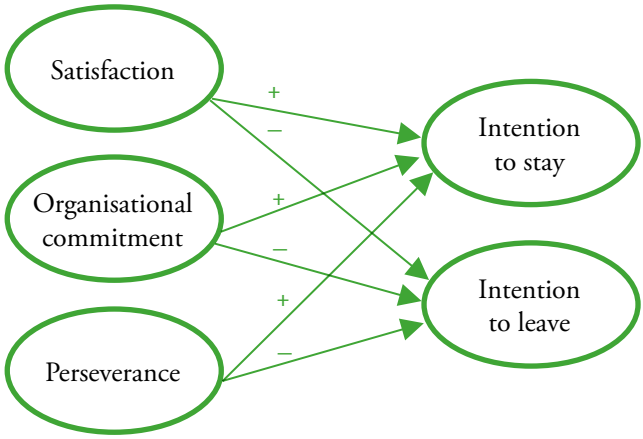


Figure 1. Basic conceptual model for studying Border Guard officer retention.

Source: own elaboration based on the literature review.

The research utilised a partially structured questionnaire survey method and partial least squares structural equation modeling (PLS-SEM).

The survey questionnaire included the following variables with the original number of questions associated with them: job satisfaction (45 items), organisational commitment (18 items), perseverance (12 items), intention to stay in organisation (3 items), intention to leave the organisation (3 items). In addition, the survey questionnaire included a semi-open catalogue of 45 potential reasons for resigning from service, with the option to enter other reasons not listed and for respondents to express themselves freely.

All questions were rated on a 5-point Likert-type scale, where 1 meant an extremely negative opinion or complete disagreement with the statement, 3 meant a neutral attitude, and 5 meant an extremely positive opinion or complete agreement with the statement. The content of the research tool was consulted with psychologists affiliated with the service in terms of comprehensibility, completeness and correctness of the wording used.

The target study was preceded by a pilot questionnaire among 50 officers studying at the Border Guard Higher School who were not included in the final research sample. Respondents confirmed that the questions and statements contained in the survey were understandable, which was reflected in the high consistency of responses with a repeat test conducted two weeks later (Table 2), demonstrating the good stability of a tool[25].

[25] K.S. Jankowski, M. Zajenkowski, *Metody szacowania rzetelności pomiaru testem* (Eng. Methods for estimating measurement reliability using a test), in: *Psychometria – podstawowe zagadnienia*, K. Fronczyk (ed.), Warszawa 2009, pp. 84–110.

Table 2. Test-retest correlation results for the components of the research tool.

Construct name	Test-retest (pilot study) n = 50
Job satisfaction	0.83
Affective commitment	0.65
Normative commitment	0.84
Continuance commitment	0.96
Perseverance	0.65
Intention to stay in organisation	0.77
Intention to leave organisation	0.68

Source: own elaboration based on a statistical test.

Guided by the principle of research economy, the number of questions in the survey was reduced without compromising its cognitive value and statistical parameters, which made it possible to shorten the time needed to complete the survey and reduced the amount of work involved. First, the Kaiser–Meyer–Olkin (KMO) coefficient was calculated. Its high value (> 0,8) confirmed the validity of the exploratory factor analysis (EFA), on the basis of which six factors were identified for the variable job satisfaction: S1 – interpersonal relations, S2 – remuneration, S3 – job stability, S4 – promotion opportunities, S5 – self-fulfilment, S6 – sense of security. The number of questions related to this variable was reduced from 45 to the 18 most relevant items. Similarly, the number of questions concerning organisational commitment was reduced from 18 to 9, and three factors of this commitment were identified: affective commitment, normative commitment, continuance commitment. A similar approach was taken in the case of perseverance, for which the number of questions was reduced from 12 to 5 most important ones. The dimensions for individual variables were selected using factor analysis that yielded satisfactory parameters – all factor loadings exceeded 0.5, and the cumulative explained variance exceeded 60%. Due to the one-dimensional nature of the intention to stay and the intention to leave, and the small number of questions concerning them, their number was not reduced. In the catalogue of potential reasons for leaving the service, no factors were identified and the number of questions was not reduced due to the diversity of open-ended responses obtained in this area.

The intention to build a structural model of officer retention, distributions that deviate from the normal, and the need to analyse multiple relationships simultaneously led to the use of PLS-SEM in the study. The application of PLS-SEM to study staff behaviour is currently recommended by leading

European management journals (e.g. *Journal of Business Research*, *European Management Journal*)[26]. The structural equation model allows us to illustrate and measure the impact of variables such as satisfaction, organisational commitment and perseverance on the intention to stay or the intention to leave the service – which can be used to explain and predict the behaviour of officers in relation to staying with or leaving the Border Guard. All calculations were performed in the R environment[27], and the higher-order construct was reflective-reflective in nature and was estimated using a disjoint two-stage approach. Unlike many other statistical techniques, PLS-SEM remains relatively resistant to violations of the assumption of normality of distributions and works well with moderate sample sizes, which made it a suitable tool for these analyses.

Research results

Satisfaction with individual motivational factors

An analysis of the results obtained for individual motivators indicates that the most satisfying factor for officers is job stability, while the least satisfying factor is remuneration, which scored 3.11 (Table 3). The overall level of satisfaction with all 18 motivators surveyed is 3.51 on a five-point scale, which means that respondents generally had a positive opinion of the incentive system consisting of the analysed elements. Against this background, the level of satisfaction with remuneration may suggest a potential risk to staff retention and be a basis for considering improvements.

Table 3. Level of satisfaction with individual motivational factors (n = 184).

Satisfaction factors	Arithmetic mean	Standard deviation
Job stability (3 motivators)	3.88	0.99
Self-fulfilment (3 motivators)	3.74	0.88
Interpersonal relations (3 motivators)	3.60	1.02

[26] See: M. Ratzmann, S.P. Gudergan, R. Bouncken, *Capturing heterogeneity and PLS-SEM prediction ability: Alliance governance and innovation*, "Journal of Business Research" 2016, vol. 69, no. 10, pp. 4593–4603. https://doi.org/10.1016/j.jbusres.2016.03.051; N.F. Richter et al., *European management research using partial least squares structural equation modeling (PLS-SEM)*, "European Management Journal" 2016, vol. 34, no. 6, pp. 589–597. https://doi.org/10.1016/j.emj.2016.08.001.

[27] R – interpreted programming language and environment for statistical computing and data visualisation. Version 4.5.1 and the SEMinR package version 2.3.4 were used.

Satisfaction factors	Arithmetic mean	Standard deviation
Sense of security (3 motivators)	3.56	1.05
Promotion opportunities (3 motivators)	3.19	1.16
Remuneration (3 motivators)	3.11	1.12
Overall satisfaction level with all 18 motivators surveyed	3.51	1.04

Source: own elaboration based on the research conducted.

Organisational commitment and perseverance

The level of organisational commitment among the officers surveyed was moderate – it achieved an average of 2.93, which is close to the neutral value of 3.00 (Table 4). This result suggests that respondents' overall sense of connection to the organisation was neither clearly positive nor clearly negative. Within the individual dimensions of organisational commitment, the highest level was recorded for affective commitment – average 3.41. This dimension – measured, among other things, by statements such as: *The Border Guard is very important to me personally, I feel a strong sense of belonging to the Border Guard, I feel an emotional connection to the Border Guard* – indicates that respondents have a fairly strong emotional connection to the organisation and identify with its values. In turn, continuance commitment and normative commitment achieved significantly lower averages, respectively: 2.72 and 2.67. This result may indicate a relatively weak sense of loyalty to the organisation (normative dimension) and attachment resulting from the costs of leaving (continuance dimension).

The average declared level of perseverance in action was 4.05, which means that the respondents assessed themselves as people striving to achieve long-term goals with slightly above-average passion and determination. This is a moderately high level of perseverance, which may bode well in terms of continuing service in the Border Guard and a lack of desire to leave it – more persevering individuals are generally less likely to be discouraged from pursuing their chosen career path.

Table 4. Level of organisational commitment and perseverance (n = 184).

Construct name	Arithmetic mean	Standard deviation
Total organisational commitment	2.93	1.12
Affective commitment	3.41	1.01
Continuance commitment	2.72	1.21

Construct name	Arithmetic mean	Standard deviation
Normative commitment	2.67	1.13
Perseverance	4.05	0.83

Source: own elaboration based on the research conducted.

The results presented indicate critical areas for the Border Guard officers surveyed, which should be monitored and taken into account in management activities to avoid undesirable high staff turnover. On the one hand, the relatively low level of organisational commitment (of normative and continuance type) suggests the need to strengthen the sense of loyalty and attachment of officers to the formation by various means. On the other hand, relatively high perseverance of the respondents is a positive sign – it may encourage them to remain in service despite possible difficulties.

Potential reasons for leaving the service

According to the officers surveyed, the most significant potential reason for resigning from the service (the so-called demotivator) in the Border Guard is an unfavourable change in the regulations concerning salaries, benefits or the pension system (Table 5). Three of the top ten reasons for resignation were related to the remuneration system (the aforementioned unfavourable change in pay regulations; too low remuneration; infrequent and low pay rises). Two reasons belong to the category related to work-life balance: lack of time for private life (due to an excessive number of work tasks) and difficulties in reconciling work responsibilities with family life (constant tension when trying to balance these spheres). Two further reasons can be linked to relationships with superiors: unfair punishment and unequal treatment. Furthermore, one interpersonal reason was indicated: lack of respect from superiors and colleagues, as well as one related to job stability: transfers between the Border Guard organisational units/departments (forced relocations). The list is completed by one market factor – a better job offer from another employer.

Table 5. The ten most important potential reasons for officers resigning from service in the Border Guard (n = 184).

No.	Potential reason for leaving the Border Guard	Arithmetic mean	Standard deviation
1.	Unfavourable changes to regulations concerning salaries/ benefits/pensions, etc.	4.29	1.00

No.	Potential reason for leaving the Border Guard	Arithmetic mean	Standard deviation
2.	Transfers between Border Guard organisational units/departments	4.06	1.07
3.	Unfair punishment	4.06	1.13
4.	No time for a private life due to an excessive number of tasks	4.05	1.05
5.	Stress related to balancing family relationships and work demands	4.02	1.02
6.	Unequal treatment	3.96	1.11
7.	Insufficient remuneration	3.95	1.07
8.	Infrequent and low pay rises	3.91	1.20
9.	A better job offer from another employer	3.91	1.04
10.	Lack of respect towards me from my superior and colleagues	3.91	1.05

Source: own elaboration based on the research conducted.

The results concerning the reasons for leaving indicate problem areas that the Border Guard, as an employer, should focus on in order to reduce the risk of losing officers. The issue of remuneration and benefits is particularly prominent – as many as three of the ten most important reasons relate to financial matters. The remuneration system and the predictability of career paths (problem of transfers) as well as relations with superiors require attention from decision-makers. Identifying these factors creates an opportunity to take targeted management actions to prevent staff turnover.

Intention to stay and intention to leave

The desire to remain in service or leave it was surveyed by examining officers' declarations in this regard, which made it possible to measure both the potential level of retention and staff turnover, which were not treated as complementary to each other. In accordance with the five-point scale used in the research tool, the neutral threshold separating the responses was value 3.00 (Table 6). Intention to stay (level of retention) was at a good level – the average declaration was 3.89, which is clearly above the threshold of 3.00. Of the 184 people surveyed, 38 had intention to stay below the neutral level, which translates into a percentage of 21% and determines retention at 79%.

The levels of intention to leave and turnover were low, because the average value for intention to leave was 2.00. Only 25 out of 184 people had intention to leave above the neutral level, which sets turnover at a level of 14%.

Table 6. The level of intention to stay/to leave and retention/turnover of the Border Guard officers.

Specification of measures	Intention to stay	Intention to leave
Arithmetic mean	3.89	2.00
Retention level in %	79	-
Turnover level in %	-	14
Standard deviation	1.08	1.06

Source: own elaboration based on the research conducted.

The presented results indicate that the Border Guard has a high capacity to retain officers, as the vast majority plan to remain in service, with few individuals considering leaving.

Results of PLS-SEM structural model

The most important research objective was to apply PLS-SEM structural modeling to the study of staff retention in Polish uniformed services and to develop a model (Figure 2).

The elliptical shapes in the model represent latent variables: satisfaction, organisational commitment, perseverance, intention to stay, intention to leave, and R^2 values entered in the intention indicate the percentage to which they are explained by variables that affect them. The direction of this influence is indicated by the arrows, while positive or negative β values correspond to the strength of the influence.

The rectangular shapes in yellow represent individual dimensions identified in the structure of a given variable. For instance, organisational commitment variable is reflected in three dimensions, of which normative commitment dimension has the largest share ($\lambda = 0.846$) in organisational commitment level compared to affective commitment ($\lambda = 0.833$) and continuance commitment ($\lambda = 0.723$). In turn, the dimensions of self-fulfilment ($\lambda = 0.785$) and sense of security ($\lambda = 0.783$) have the greatest impact on the overall level of job satisfaction.

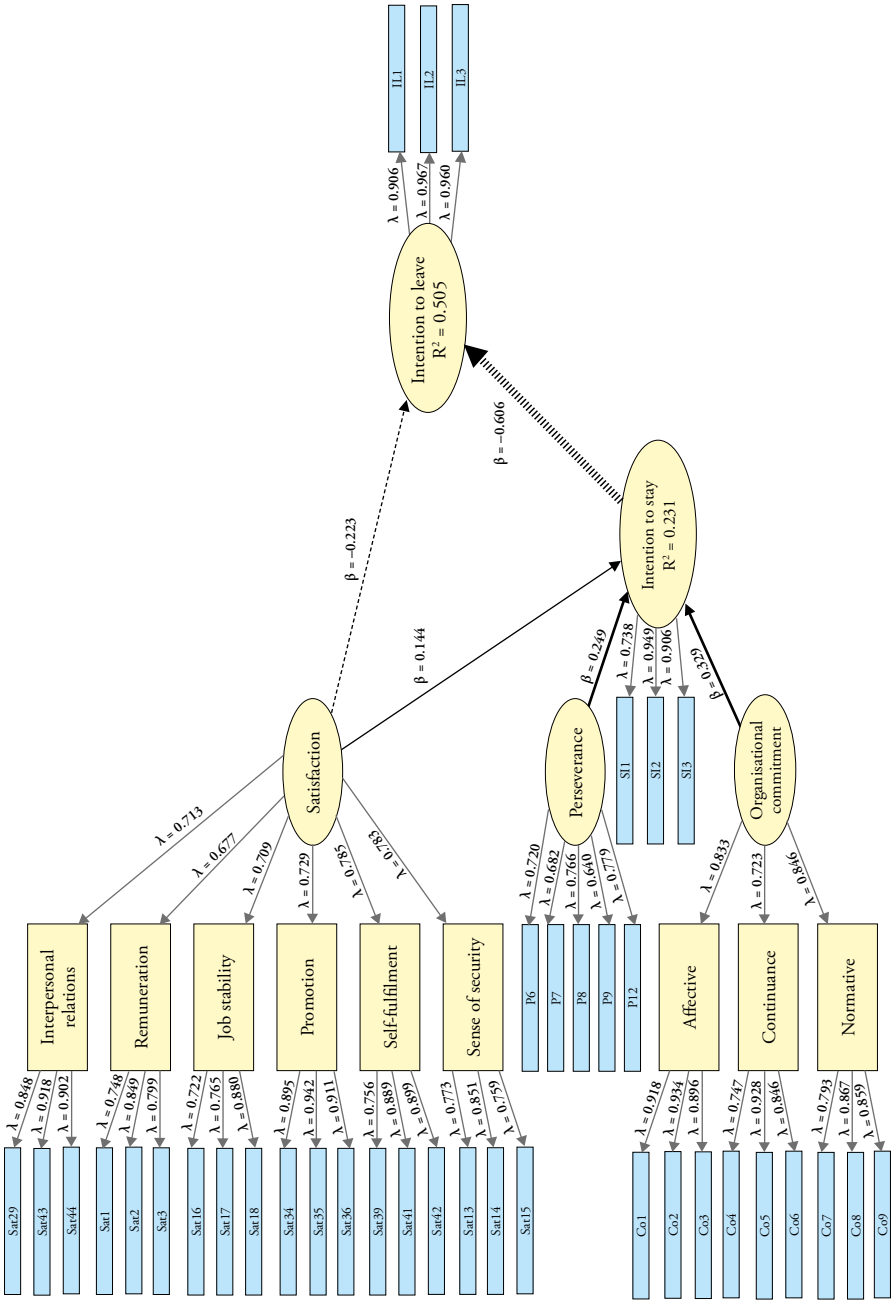


Figure 2. The PLS-SEM structural model of retention of Border Guard officers.

Source: own elaboration based on the research conducted.

The results obtained in the retention model of the Border Guard officers are satisfactory, as all R^2 determination coefficients exceeded the threshold of 0.20[28], and the examined key variable – the intention to leave – was explained in over 50% ($R^2 = 0.505$) by the variables: intention to stay and job satisfaction as well as indirectly by organisational commitment and perseverance. This means that more than half of the variation in the propensity to leave in this group can be explained by the measured variables, which confirms the validity of their selection and significance.

The results of the study indicated a very strong negative influence of intention to stay on intention to leave, because an increase of intention to stay by 1 standard deviation translates into a decrease in intention to leave by 0.606 standard deviations. This confirms the logic that fostering a desire to stay in the Border Guard among officers directly reduces the risk of them leaving. It also turned out that intention to leave is determined by both intention to stay and job satisfaction level ($\beta = -0.223$), with intention to stay having a stronger effect on intention to leave than satisfaction. This can be interpreted as follows: the more someone is dissatisfied with the conditions, the more they think about leaving, but even more important is the general attitude – the very intention to stay in service. People who, despite certain dissatisfactions, want to stay, e.g., out of loyalty or a sense of mission, are less likely to think about leaving. High satisfaction, on the other hand, can deter those who intended to leave. Intention to stay in this model is explained by more than 23% ($R^2 = 0.231$) by the following variables: organisational commitment ($\beta = 0.329$), perseverance ($\beta = 0.249$) and job satisfaction ($\beta = 0.144$), of which organisational commitment has the strongest effect. This is a significant, albeit moderate effect, suggesting that for officers, building identification with the organisation and loyalty is a factor that has a stronger influence on actual plans to remain in service than perseverance and job satisfaction. To sum up this part of the study, it can be concluded that the structural model for officers confirmed the important role of organisational commitment and satisfaction in staff retention. It also indicated that the strongest factor preventing people from leaving the service is their strong desire to remain attached to it. Therefore, measures that strengthen identification of the Border Guard

[28] A. Kacprzak, *Modelowanie strukturalne w analizie zachowań konsumentów: porównanie metod opartych na analizie kowariancji (CB-SEM) i częściowych najmniejszych kwadratów (PLS-SEM)* (Eng. Structural equation modeling in the consumer behaviour analysis: the comparison of covariance-based (CB-SEM) and partial least square (PLS-SEM) methods), "Handel Wewnętrzny" 2018, vol. 1, no. 6, p. 255; R.F. Frank, N.B. Miller, *A Primer for Soft Modeling*, Ohio 1992; J.F. Hair et al., *An assessment of the use of partial least squares structural equation modeling in marketing research*, "Journal of the Academy of Marketing Science" 2012, vol. 40, pp. 414–433. https://doi.org/10.1007/s11747-011-0261-6; J.F. Hair Jr. et al., *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*, series: Classroom Companion: Business, Cham 2021, pp. 76–78. https://doi.org/10.1007/978-3-030-80519-7.

officers (sense of mission, pride, bonds) and ensure their satisfaction in various aspects can reduce the phenomenon of leaving the service.

Evaluation of statistical parameters of the PLS-SEM structural model

Testing the reliability and measurement accuracy of the PLS-SEM structural model used confirmed that it has good psychometric parameters, as shown in the Table 7. The reliability measures – both Cronbach's Alpha, the rho_A index and composite reliability (CR) – for most constructs were in the range of 0.70–0.95[29]. The exception was the construct of intention to leave, for which the CR value was 0.961. Such a high result may suggest redundancy of indicators, i.e. their excessive similarity in content. However, considering that intention to leave is a homogeneous construct measured using three indicators, and the value of rho_A remains at an acceptable level, this result can be considered justified and unobjectionable. In addition, average variance extracted (AVE) for each construct was above 0.50[30], which indicates a high degree of convergence between the indicators contained therein.

Table 7. Validity and reliability of the PLS-SEM structural model measures – indicators for latent constructs.

Specification of measures	Cronbach's Alpha	rho_A	CR	AVE
Intention to leave	0.939	0.944	0.961	0.892
Intention to stay	0.837	0.888	0.902	0.756
Satisfaction	0.829	0.834	0.875	0.538
Perseverance	0.771	0.790	0.842	0.517
Organisational commitment	0.723	0.732	0.844	0.644

Source: own elaboration based on the research conducted.

In order to verify the discriminant validity of the constructs, heterotrait-monotrait (heterotrait-monotrait ratio of correlations, HTMT) coefficients were also calculated for each pair of latent variables. The Table 8 presents HTMT values – in all cases, they are clearly below the accepted criterion of 0.85[31], which indicates

[29] J.F. Hair Jr. et al., *Partial Least Squares*…, pp. 77–78, 80.

[30] Ibid., p. 78, 80.

[31] J. Henseler, Ch.M. Ringle, M. Sarstedt, *A new criterion for assessing discriminant validity in variance-based structural equation modeling*, "Journal of the Academy of Marketing Science" 2015, vol. 43, pp. 115–135. https://doi.org/10.1007/s11747-014-0403-8.

good separability of individual constructs – none of them measure the same phenomenon. In other words, the latent variables used in the model are mutually discrete and there is no undesirable overlap in their meanings.

Table 8. HTMT coefficient matrix – discriminant validity of the PLS-SEM structural model constructs.

Construct name	Organisational commitment	Satisfaction	Perseverance	Intention to stay	Intention to leave	Interpersonal relations	Remuneration	Job stability	Promotion	Self-fulfilment	Sense of security	Affective commitment	Continuance commitment
Satisfaction	0.59												
Perseverance	0.27	0.18											
Intention to stay	0.44	0.37	0.28										
Intention to leave	0.46	0.47	0.20	0.76									
Interpersonal relations	0.38	*	0.13	0.20	0.34								
Remuneration	0.55	*	0.12	0.35	0.30	0.43							
Job stability	0.40	*	0.24	0.31	0.41	0.46	0.54						
Promotion	0.37	*	0.06	0.22	0.31	0.52	0.57	0.41					
Self-fulfilment	0.46	*	0.15	0.27	0.32	0.72	0.62	0.50	0.68				
Sense of security	0.55	*	0.20	0.34	0.46	0.57	0.51	0.81	0.57	0.65			
Affective commitment	*	0.47	0.20	0.36	0.30	0.29	0.43	0.30	0.24	0.42	0.49		
Continuance commitment	*	0.30	0.33	0.32	0.38	0.17	0.36	0.21	0.23	0.17	0.26	0.34	
Normative commitment	*	0.53	0.14	0.28	0.31	0.37	0.43	0.38	0.35	0.45	0.44	0.74	0.57

* We do not assess the differential validity between satisfaction and organisational commitment and their lower-order component, because a violation of differential validity between these constructs is expected.

Source: own elaboration based on the research conducted.

All values of the variance inflation factor (VIF) for the internal model[32] (Table 9) are well below generally accepted thresholds[33], indicating that there is no significant collinearity between constructs in the PLS-SEM structural model. Low VIF values for the internal model suggest that the constructs are relatively independent of each other, which allows for a more reliable interpretation of the path coefficients.

Table 9. VIF values – assessment of the collinearity of the internal model.

Specification of measures	VIF
Intention to stay → intention to leave	1.12
Satisfaction → intention to leave	1.12
Satisfaction → intention to stay	1.31
Perseverance → intention to stay	1.04
Organisational commitment → intention to stay	1.30

Source: own elaboration based on the research conducted.

In the PLS-SEM structural model, using bootstrapping (10 000 iterations), a 95% confidence interval (CI) was estimated for all paths, whose values are presented in Table 10. The interpretation of these intervals confirms the significance of most of the links in the model. For each path, if the entire confidence interval is above or below zero, this indicates a statistically significant effect (when $p < 0.05$). In the analysed model, all main paths proved to be important.

Table 10. Path coefficients, significance level, confidence interval of the PLS-SEM structural model.

Path	Original sample	Average of samples	Standard deviation	Stat. t	2.5% CI	97.5% CI
Organisational commitment → intention to stay	0.329	0.342	0.079	4.184	0.196	0.494

[32] The presented PLS-SEM structural model consists of an external and internal model. The external model includes lower-order constructs that influence higher-order constructs. The internal model includes higher-order constructs: satisfaction, commitment, perseverance, intention to leave, intention to stay.

[33] J-M. Becker et al., *How collinearity affects mixture regression results*, "Marketing Letters" 2015, vol. 26, no. 4, pp. 643–659. https://doi.org/10.1007/s11002-014-9299-9.

Path	Original sample	Average of samples	Standard deviation	Stat. t	2.5% CI	97.5% CI
Satisfaction → intention to stay	0.144	0.151	0.073	1.962	0.007	0.293
Satisfaction → intention to leave	–0.223	–0.228	0.075	–2.972	–0.375	–0.082
Perseverance → intention to stay	0.249	0.259	0.083	2.994	0.110	0.407
Intention to stay → intention to leave	–0.606	–0.605	0.077	–7.867	–0.751	–0.450

Source: own elaboration based on the research conducted.

In addition to the direct effects included in the model, the indirect effects (mediations) of key predictive variables on outcome variables were also analysed. The results of this analysis are presented in Table 11. The data shows that job satisfaction has a significant indirect effect on both intention to leave and intention to stay. The indirect effect of satisfaction on intention to leave is –0.087, which means that satisfaction reduces the propensity to leave through its impact on intention to stay.

Organisational commitment and perseverance also show negative indirect effects on intention to leave, –0.199 and –0.151 respectively, which indicates that these factors reduce the propensity to leave service indirectly, by reinforcing the intention to stay.

Table 11. Indirect effects of selected variables in the PLS-SEM structural model.

Path	Indirect effect
Organisational commitment → intention to leave	–0.199
Satisfaction → intention to leave	–0.087
Perseverance → intention to leave	–0.151

Source: own elaboration based on the research conducted.

According to the data presented in Table 12, the greatest overall impact on the intention to leave is exerted by, in order: intention to stay (–0.606), satisfaction (–0.310), organisational commitment (–0.199) and perseverance (–0.151).

Table 12. Total effects of selected variables in the PLS-SEM structural model (bootstrapping – 10 000 iterations, $p < 0.05$).

Path	Original sample	Sample mean	Standard deviation	T statistics	2.5% CI	97.5% CI
Organisational commitment → intention to stay	0.329	0.342	0.079	4.18	0.196	0.494
Organisational commitment → intention to leave	–0.199	–0.210	0.065	–3.05	–0.347	–0.097
Satisfaction → intention to stay	0.144	0.151	0.073	1.96	0.007	0.293
Satisfaction → intention to leave	–0.310	–0.320	0.076	–4.07	–0.465	–0.166
Perseverance → intention to stay	0.249	0.259	0.083	2.99	0.110	0.407
Perseverance → intention to leave	–0.151	–0.157	0.056	–2.71	–0.266	–0.061
Intention to stay → intention to leave	–0.606	–0.605	0.077	–7.87	–0.751	–0.450

Source: own elaboration based on the research conducted.

The f^2-index measures how much the R^2 of the dependent variable increases when we include or remove a specific predictor. All f^2 values reached the threshold value of 0.02 indicated by Jacob Cohen[34], which proves their practical significance (Table 13).

Table 13. Strength of f^2 effects for relations in the PLS-SEM structural model.

Construct name	Intention to stay	Intention to leave
Organisational commitment	0.111	-
Satisfaction	0.020	0.089

[34] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, New York 1988, p. 413. https://doi.org/10.4324/9780203771587.

Construct name	Intention to stay	Intention to leave
Perseverance	0.077	-
Intention to stay	-	0.663

Source: own elaboration based on the research conducted.

These results confirm the need to include intention to stay, satisfaction, organisational commitment and perseverance in the model as predictors that directly or indirectly influence on intention to leave.

Using the PLSpredict function – direct antecedents approach, 10-fold cross-validation was performed. The obtained prediction error values RMSE (root mean square error) and MAE (mean absolute error) for the PLS-SEM structural model were lower than in the linear regression model, which indicates high predictive power[35]. The results are presented in Table 14.

Table 14. Results of cross-validation performed using the PLSpredict function.

PLS prediction quality measures for out-of-sample data						
	IP1	IP2	IP3	IO1	IO2	IO3
RMSE	1.067	0.980	0.966	0.969	0.688	0.717
MAE	0.774	0.734	0.767	0.718	0.502	0.521
Measures of prediction quality for linear regression model (LM) for out-of-sample data						
	IP1	IP2	IP3	IO1	IO2	IO3
RMSE	1.096	1.001	0.974	1.004	0.714	0.728
MAE	0.815	0.757	0.767	0.759	0.522	0.532

Source: own elaboration based on the research conducted.

[35] G. Shmueli et al., *Predictive model assessment in PLS-SEM: guidelines for using PLSpredict*, "European Journal of Marketing" 2019, vol. 53, no. 11, pp. 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189.

Comparison of the PLS-SEM structural model results with other studies

The correlation of higher-order constructs was calculated and a comparative analysis was performed to assess the strength and direction of the relationship between variables (Table 15) in order to relate the results of this study to studies conducted in foreign uniformed services.

Table 15. Higher-order construct correlation matrix.

Construct name	Organisational commitment	Satisfaction	Perseverance	Intention to stay	Intention to leave
Organisational commitment	1.000	-	-	-	-
Satisfaction	0.463	1.000	-	-	-
Perseverance	–0.075	0.118	1.000	-	-
Intention to stay	0.377	0.325	0.241	1.000	-
Intention to leave	–0.378	–0.420	–0.180	–0.679	1.000

Source: own elaboration based on the research conducted.

Analysis of the correlation of data from Table 15 indicates that the specific directions of dependence are consistent with the directions adopted in the research hypotheses. The results indicate that intention to leave – the key construct of the study – is most strongly correlated negatively with intention to stay (–0.679), followed by satisfaction (–0.420) and organisational commitment (–0.378) and perseverance (–0.180). This means that as any of the constructs increase – intention to stay, satisfaction, organisational commitment or perseverance – intention to leave will decrease significantly or moderately. This finding provides statistical evidence of the possibility of reducing the number of unwanted departures of officers from service by optimisation of the conditions of service that affect these constructs.

Due to the lack of information on national research in this area, the project results could only be compared with the results of foreign projects. A study of 400 New Zealand police officers showed a significant correlation between job

satisfaction and intention to leave, which was r = –0.43[36], a result very similar to that obtained in this project, r = –0.42. In turn, in a study involving 3580 Dutch soldiers, the correlation of organisational commitment and intention to leave was r = –0.34[37], which is also a result similar to the result of the present study, r = –0.38.

In a study of 450 Canadian soldiers, the multiple regression coefficient between satisfaction and intention to leave was β = –0.28[38], while in this model the path coefficient was β = –0.22 and the total effect was –0.31. These results confirm the negative direction of the relationship and the similar order of magnitude of the effect obtained in this study.

Based on a comparison of the results, it can be assumed that satisfaction and organisational commitment significantly influence the intention to leave in the entire population of people working in the uniformed services, and the directions and magnitude of the impact of key variables on each other will be similar.

Summary and conclusions

The results of the PLS-SEM structural modeling positively verify hypotheses H1 and H2. Job satisfaction, organisational commitment and perseverance significantly encourage remaining in service – they have a positive impact on the intention to remain and counteract departure – they have a negative impact (directly or indirectly) on the intention to leave. Furthermore, the model highlights the key role of the intention to stay as a factor that directly reduces the intention to leave.

In view of the results of the survey conducted among the Border Guard officers, the following practical solutions may be considered:

1. Increasing staff retention by focusing on solutions addressing the most important potential reasons for leaving the service, as well as ensuring the stability of regulations governing salaries/benefits/pensions and the indexation of their amounts. This is achieved by applying objective and

[36] P. Brough, R. Frame, *Predicting Police Job Satisfaction and Turnover Intentions: The role of social support and police organisational variables*, "New Zealand Journal of Psychology" 2004, vol. 33, no. 1, https://www.psychology.org.nz/journal-archive/NZJP-Vol331-2004-2-Brough.pdf, pp. 8–16 [accessed: 5 V 2025].

[37] M.W. van Eetveldt et al., *The Importance of Career Insecurity for Turnover Intentions in the Dutch Military*, "Military Psychology" 2013, vol. 25, no. 5, pp. 489–501. https://psycnet.apa.org/doi/10.1037/mil0000016.

[38] K.E. Duprè, A.L. Day, *The effects of supportive management and job quality on the turnover intentions and health of military personnel*, "Human Resource Management" 2007, vol. 46, no. 2, pp. 185–201. https://doi.org/10.1002/hrm.20156.

fair criteria for transfers, taking into account the situation of the officer before the transfer decision is made, as well as training for managers and an assessment by their subordinates of their soft skills. Work planning should take into account the needs of officers including their recovery.

2. Proposing to Border Guard organisational units and other Polish uniformed services that they adopt the presented methodology and research tool for conducting cyclical surveys concerning job satisfaction, organisational commitment, perseverance, and intentions to stay or leave among officers and soldiers in permanent service. Regular monitoring of these indicators will allow for quick identification of problems and optimisation of management solutions related to retention, which will have a positive impact on personnel and state security.
3. Emphasising the importance of organisational commitment (and its individual components) in training intended for management as a variable that can have a measurable impact on the willingness to continue service. The competences of management staff should be developed in the area of shaping and strengthening the organisational commitment of subordinates – especially in the affective dimension – through appropriate leadership style and communication as well as building identification with the mission of the formation.
4. Inclusion of elements assessing the perseverance of candidates for service in recruitment and selection procedures, e.g. development of behavioural questions or tests to assess the level of perseverance of candidates already at the recruitment stage. Perseverance is a predictor of remaining in service, and people with high perseverance are better able to endure the hardships of service and are less likely to resign prematurely.
5. Analysing factors influencing the intention to leave and the intention to stay in individual Border Guard units. Border Guard organisational units could periodically analyse which factors (e.g. identified in this study) have the strongest impact on their officers' plans to leave and which encourage them to stay. This will allow them to adapt and improve internal HR solutions (e.g. motivation programmes, trainings, psychological support).
6. Consider changes to the remuneration system for Border Guard officers. The results clearly indicate that pay issues are a significant weak point affecting officer dissatisfaction and their propensity to leave. Adjusting the remuneration system – so that they feel that their pay is fair and that they receive a real increase in remuneration in line with their seniority and achievements – can significantly improve retention rates.

Retention staff research is a challenge. It is worth taking it on, as the results obtained can help to increase personnel security and the achievement of goals within a given formation. National security therefore requires the implementation of research projects that use statistical methods to monitor variables that influence whether staff remain in service or resign.

Achieving the research objective of identifying and measuring variables influencing the intention to remain in service and the intention to leave service made it possible to identify the following significant variables: satisfaction, organisational commitment, perseverance and link them to the reasons for the decisions and suggest initiatives to support management actions.

The methodology, the structural model constructed and the recommended solutions presented in the article can serve as guidelines for Polish uniformed services in overcoming current challenges and minimising future ones concerning staff retention. The implementation of the proposed initiatives, such as systematic monitoring of satisfaction, organisational commitment and perseverance, improvement of service conditions and development of leadership skills among staff – should translate into improved retention of the Border Guard officers and, consequently, strengthen the capacity of this formation to ensure security of the state.

The described research could be implemented in all Polish uniformed services, taking into account their specific characteristics, which on national scale would allow for synergies to be achieved in the area of security.

Bibliography

Ajzen I., *From Intentions to Actions: A Theory of Planned Behawior*, in: *Action Control: From Cognition to Behavior*, J. Kuhl, J. Beckmann (eds.), Berlin 1985, pp. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2.

Allen N.J., Meyer J.P., *The measurement and antecedents of affective, continuance and normative commitment to the organization*, "Journal of Occupational Psychology" 1990, vol. 63, no. 1, pp. 1–18. https://doi.org/10.1111/j.2044-8325.1990.tb00506.x.

Becker J-M., Ringle Ch.M., Sarstedt M., Völckner F., *How collinearity affects mixture regression results*, "Marketing Letters" 2015, vol. 26, no. 4, pp. 643–659. https://doi.org/10.1007/s11002-014-9299-9.

Chiat L.C., Panatik S.A., *Perceptions of Employee Turnover Intention by Herzberg's Motivation-Hygiene Theory: A Systematic Literature Review*, "Journal of Research in Psychology" 2019, vol. 1, no. 2, pp. 10–15. https://doi.org/10.31580/jrp.v1i2.949.

Cho Y.J., Lewis G.B., *Turnover Intention and Turnover Behavior: Implications for Retaining Federal Employees*, "Review of Public Personnel Administration" 2011, vol. 32, no. 1, pp. 4–23. https://doi.org/10.1177/0734371X11408701.

Cohen J., *Statistical Power Analysis for the Behavioral Sciences*, New York 1988. https://doi.org/10.4324/9780203771587.

Currivan D.B., *The Causal Order of Job Satisfaction and Organizational Commitment in Models of Employee Turnover*, "Human Resource Management Review" 1999, vol. 9, no. 4, pp. 495–524. https://doi.org/10.1016/S1053-4822(99)00031-5.

Hair J.F. Jr., Hult G.T.M., Ringle Ch.M., Sarstedt M., Danks N.P., Ray S., *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*, series: Classroom Companion: Business, Cham 2021. https://doi.org/10.1007/978-3-030-80519-7.

Dogonyaro H., Nwosu F., *Exploring Employee Retention in the Hospitality Industry Through Herzberg's Two-Factor Motivation Theory*, preprint. https://doi.org/10.13140/RG.2.2.34721.93287.

Duckworth A.L., Peterson C., Matthews M.D., Kelly D.R., *Grit: Perseverance and passion for long-term goals*, "Journal of Personality and Social Psychology" 2007, vol. 92, no. 6, pp. 1087–1101. https://doi.org/10.1037/0022-3514.92.6.1087.

Dupré K.E., Day A.L., *The effects of supportive management and job quality on the turnover intentions and health of military personnel*, "Human Resource Management" 2007, vol. 46, no. 2, pp. 185–201. https://doi.org/10.1002/hrm.20156.

Eetveldt M.W. van, Ven N. van de, Tooren M. van den, Versteeg R.C., *The Importance of Career Insecurity for Turnover Intentions in the Dutch Military*, "Military Psychology" 2013, vol. 25, no. 5, pp. 489–501. https://psycnet.apa.org/doi/10.1037/mil0000016.

Eskreis-Winkler L., Shulman E.P., Beal S.A., Duckworth A.L., *The grit effect: predicting retention in the military, the workplace, school and marriage*, "Frontiers in Psychology" 2014, vol. 5, no. 36. https://doi.org/10.3389/fpsyg.2014.00036.

Falk R.F., Miller N.B., *A Primer for Soft Modeling*, Ohio 1992.

Gaertner S., *Structural Determinants of Job Satisfaction and Organizational Commitment in Turnover Models*, "Human Resource Management Review" 1999, vol. 9, no. 4, pp. 479–493. https://doi.org/10.1016/S1053-4822(99)00030-3.

Griffeth R.W., Hom P.W., Gaertner S., *A Meta-Analysis of Antecedents and Correlates of Employee Turnover: Update, Moderator Tests, and Research Implications for the Next Millennium*, "Journal of Management" 2000, vol. 26, no. 3, pp. 463–488. https://doi.org/10.1177/014920630002600305.

Hair J.F., Sarstedt M., Ringle Ch.M., Mena J.A., *An assessment of the use of partial least squares structural equation modeling in marketing research*, "Journal of the Academy of Marketing Science" 2012, vol. 40, pp. 414–433. https://doi.org/10.1007/s11747-011-0261-6.

Henseler J., Ringle Ch.M., Sarstedt M., *A new criterion for assessing discriminant validity in variance-based structural equation modeling*, "Journal of the Academy of Marketing Science" 2015, vol. 43, pp. 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hom P.W., Caranikas-Walker F., Prussia G.E., Griffeth R.W., *A meta-analytical structural equations analysis of a model of employee turnover*, "Journal of Applied Psychology" 1992, vol. 77, no. 6, pp. 890–909. https://doi.org/10.1037/0021-9010.77.6.890.

Huffman A.H., Adler A.B., Dolan C.A., Castro C.A., *The Impact of Operations Tempo on Turnover Intentions of Army Personnel*, "Military Psychology" 2005, vol. 17, no. 3, pp. 175–202. https://doi.org/10.1207/ s15327876mp1703_4.

Jankowski K.S., Zajenkowski M., *Metody szacowania rzetelności pomiaru testem* (Eng. Methods for estimating measurement reliability using a test), in: *Psychometria – podstawowe zagadnienia*, K. Fronczyk (ed.), Warszawa 2009, pp. 84–110.

Kacprzak A., *Modelowanie strukturalne w analizie zachowań konsumentów: porównanie metod opartych na analizie kowariancji (CB-SEM) i częściowych najmniejszych kwadratów (PLS-SEM)* (Eng. Structural equation modeling in the consumer behaviour analysis: the comparison of covariance-based (CB-SEM) and partial least square (PLS-SEM) methods), "Handel Wewnętrzny" 2018, vol. 1, no. 6, pp. 247–261.

Kelly D.R., Matthews M.D., Bartone P.T., *Grit and Hardiness as Predictors of Performance Among West Point Cadets*, "Military Psychology" 2014, vol. 26, no. 4, pp. 327–342. https://doi.org/10.1037/mil0000050.

Lee T.W., Mitchell T.R., *The unfolding effects of organizational commitment and anticipated job satisfaction on voluntary employee turnover*, "Motivation and Emotion" 1999, vol. 15, no. 1, pp. 99–121. https://doi.org/10.1007/BF00991478.

Lytell M.C., Drasgow F., *"Timely" Methods: Examining Turnover Rates in the U.S. Military,* "Military Psychology" 2009, vol. 21, no. 3, pp. 334–350. https://doi.org/10.1080/08995600902914693.

Marrone J.V., *Predicting 36-Month Attrition in the U.S. Military: A Comparison Across Service Branches*, Santa Monica 2020. https://doi.org/10.7249/RR4258.

Meyer J.P., Allen N.J., *A three-component conceptualization of organizational commitment*, "Human Resource Management Review" 1991, vol. 1, no. 1, pp. 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z.

Mobley W.H., Horner S.O., Hollingsworth A.T., *An evaluation of precursors of hospital employee turnover*, "Journal of Applied Psychology" 1978, vol. 63, no. 4, pp. 408–414. https://doi.org/10.1037/0021-9010.63.4.408.

Mowday R.T., Steers R.M., Porter L.W., *The measurement of organizational commitment*, "Journal of Vocational Behavior" 1979, vol. 14, no. 2, pp. 224–247. https://doi.org/10.1016/0001-8791(79)90072-1.

Pitts D., Marvel J., Fernandez S., *So Hard to Say Goodbye? Turnover Intention among U.S. Federal Employees*, "Public Administration Review" 2011, vol. 71, no. 5, pp. 751–760. https://doi.org/10.1111/j.1540-6210.2011.02414.x.

Ratzmann M., Gudergan S.P., Bouncken R., *Capturing heterogeneity and PLS-SEM prediction ability: Alliance governance and innovation*, "Journal of Business Research" 2016, vol. 69, no. 10, pp. 4593–4603. https://doi.org/10.1016/j.jbusres.2016.03.051.

Richter N.F., Cepeda G., Roldán J.L., Ringle Ch.M., *European management research using partial least squares structural equation modeling (PLS-SEM)*, "European Management Journal" 2016, vol. 34, no. 6, pp. 589–597. https://doi.org/10.1016/j.emj.2016.08.001.

Sheppard B.H., Hartwick J., Warshaw P.R., *The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research*, "Journal of Consumer Research" 1988, vol. 15, no. 3, pp. 325–343. https://doi.org/10.1086/209170.

Shmueli G., Sarstedt M., Hair J.F., Cheah J-H., Ting H., Vaithilingam S., Ringle Ch.M., *Predictive model assessment in PLS-SEM: guidelines for using PLSpredict*, "European Journal of Marketing" 2019, vol. 53, no. 11, pp. 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189.

Spector P.E., *The Nature of Job Satisfaction*, in: idem, *Job Satisfaction: Application, Assessment, Causes, and Consequences*, London 1997. https://doi.org/10.4135/9781452231549.n1.

Tett R.P., Meyer J.P., *Job satisfaction, organizational commitment, turnover intention, and turnover: Path analyses based on meta-analytic findings*, "Personnel Psychology" 1993, vol. 46, no. 2, pp. 259–293. https://doi.org/10.1111/j.1744-6570.1993.tb00874.x.

Internet sources

Brough P., Frame R., *Predicting Police Job Satisfaction and Turnover Intentions: The role of social support and police organisational variables*, "New Zealand Journal of Psychology" 2004, vol. 33, no. 1, https://www.psychology.org.nz/journal-archive/NZJP-Vol331-2004-2-Brough.pdf, pp. 8–16 [accessed: 5 V 2025].

Herzberg F., Mausner B., Snyderman B.B., *The Motivation to Work*, New York 1959, https://api.pageplace.de/preview/DT0400.9781351504430_A30546568/preview-9781351504430_A30546568.pdf [accessed: 18 I 2025].

Locke E.A., *The Nature and Causes of Job Satisfaction*, College Park 1976, https://www.researchgate.net/publication/238742406_The_Nature_and_Causes_of_Job_Satisfaction [accessed: 13 I 2025].

Strickland W.J., *A Longitudinal Examination of First Term Attrition and Reenlistment Among FY1999 Enlisted Accessions*, https://apps.dtic.mil/sti/tr/pdf/ADA448564.pdf [accessed: 10 I 2025].

Other documents

Najwyższa Izba Kontroli (Eng. The Supreme Audit Office), *Informacja o wynikach kontroli pt. Realizacja programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2017–2020* (Eng. Information on the results of the audit entitled Implementation of the modernisation programme of the Police, the Border Guard, the State Fire Service, the State Protection Service in 2017–202), https://www.nik.gov.pl/plik/id,21396,vp,24037.pdf [accessed: 12 II 2025].

North Atlantic Treaty Organisation, Research and Technology Organisation, *Recruiting and Retention of Military Personnel. Final Report of Research Task Group HFM-107*, https://apps.dtic.mil/sti/tr/pdf/ADA476488.pdf [accessed: 11 I 2025].

Roach K.N., *Leveraging Grit in Military Research: A Comprehensive Review*, https://apps.dtic.mil/sti/trecms/pdf/AD1211251.pdf [accessed: 20 I 2025].

Weiss H.M., MacDermid S.M., Strauss R., Kurek K.E., Le B., Robbins D., *Retention in the Armed Forces: Past Approaches and New Research Directions*, https://www.mfri.purdue.edu/wpcontent/uploads/2018/03/Retention-in-the-Armed-Forces.pdf [accessed: 17 I 2025].

Radosław Wiśniewski, PhD

Officer of the Border Guard, he serves at the Border Guard Higher School in Koszalin. Graduate of the University of Szczecin, where he obtained a PhD in economics in the field of management science in 2015. At the Border Guard Higher School, he is a lecturer on human resource management topics and conducts research projects, including:

'Study on the effectiveness and efficiency of the incentive system for Border Guard officers and the incentive preferences of potential candidates for service from the so-called Generation Z', 'Cohort study of Border Guard officer retention'.

Contact: radekwisniewski@poczta.onet.pl

Denis Tomala

Officer serving at the Border Guard Higher School in Koszalin, formerly a Police officer. Graduate of environmental engineering as well as geodesy and cartography at the Faculty of Civil Engineering, Environment and Geodetic Sciences of Koszalin University of Technology. He deals with the use of data analysis and statistical methods to study management and social issues in the field of security.

Contact: denis8908@gmail.com

Internal Security Review
2026, no. 34, pp. 331–350

https://doi.org/10.4467/20801335PBW.26.015.23377

ARTICLE

Offshore wind farms as critical infrastructure in the era of hybrid threats – a new dimension of Poland's energy security

KLAUDIA MACIATA

Gdańsk University of Technology
https://orcid.org/0000-0001-6227-2851

Abstract

Offshore wind farms (OWFs) are becoming a key component of Poland's energy security. Due to location and nature, they are vulnerable to hybrid threats. The author of the article discussed OWFs as a new component of critical infrastructure in the context of incidents in the Baltic Sea since 2022 and analysed the degree of OWF resilience in terms of hybrid threats. She described legal and organisational gaps in the Polish infrastructure protection system, pointed out best practices used around the world, and made recommendations for the administration and operators in Poland. She drew attention to the need to test the resilience of OWFs using digital twin simulations and red teaming exercises. The author advocates a complex approach to OWF security, integrating legislative, technological and organisational measures. The article contributes to the discourse on redefining Poland's energy security in an era of competition below the threshold of war.

Keywords

offshore wind farms, critical infrastructure, hybrid threats, energy security, Baltic Sea, infrastructure protection

Introduction

The energy transition towards low-carbon energy sources makes offshore wind farms (OWFs) one of the most important elements of Poland's modern energy security system. Their development is in line with the European Union's climate and energy policy objectives, including achieving climate neutrality by 2050 and increasing the share of renewable energy sources (RES) in the energy mix of Member States[1]. The offshore wind farms being built by Poland in the Baltic Sea are expected to deliver up to 11 GW of installed capacity by 2040, making them the largest infrastructure project in the history of the Polish RES sector[2]. On a European scale, offshore wind energy capacity is projected to grow from around 90 GW in the middle of the decade to around 170 GW by 2030. This means almost doubling the potential of this sector[3].

The growing importance of OWFs as an energy resource poses new challenges in the area of security. This infrastructure, located on the open sea, outside territorial waters and spatially dispersed, is vulnerable to hybrid threats. They include below-the-threshold warfare activities such as sabotage, cyber attacks, navigation disruptions, disinformation operations and others described in the literature on the subject[4]. These actions are aimed not only at testing the resilience of critical infrastructure (CI), but also at exerting strategic and geopolitical pressure below the threshold of armed conflict, generating economic costs, weakening the state's response capabilities, and undermining its credibility as an entity capable of controlling and protecting maritime space.

At EU level, the issue of OWF safety has been regulated in Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (hereinafter: the CER Directive) that replaced the earlier directive on European CI[5]. The new regulations oblige Member States to identify and protect

---

1 European Commission, *The REPowerEU Plan*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [accessed: 20 VI 2025].

2 Ministerstwo Klimatu i Środowiska (Ministry of Climate and Environment), *Polityka energetyczna Polski do 2040 r. (PEP2040)* (Eng. Poland's energy policy until 2040 (PEP2040)), Warszawa 2021.

3 *Energy Transition Outlook 2025*, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [accessed: 20 VI 2025].

4 A. Sari, *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [accessed: 20 VI 2025]; *Countering hybrid threats*, NATO, 7 V 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [accessed: 20 VI 2025].

5 *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, pp. 164–186.

critical entities in 12 sectors, including in the energy sector, without distinguishing between onshore and offshore infrastructure. The offshore wind farms, as part of the electricity production and transmission network, clearly fall within this scope, and the operators of these installations are required to implement measures to increase their physical and cyber resilience.

In the latest analyses by the Center for Strategic and International Studies think tank and the NATO Strategic Communication Centre of Excellence, OWFs are perceived as so-called soft targets – objectives of high strategic value and relatively low level of protection[6]. Their location far from the coast, dependence on automated control systems (SCADA/OT; supervisory control and data acquisition/operational technology), as well as complex ownership and regulatory structures – including maritime law, which by guaranteeing freedom of navigation facilitates threats by aggressors – make them vulnerable to enemy action in the grey zone. Examples of these threats include the submarine capabilities developed over many years by China and Russia (the Main Directorate of Deep-Sea Research, GUGI) or shadow fleet[7].

The aim of the article is to present OWFs as a new component of CI in Poland and to analyse their resilience in the face of growing hybrid threats. Particular attention is paid to three areas: legal and organisational gaps in the Polish CI protection system, good practices in the protection of OWFs at national and international levels, and recommendations for decision-makers and operators in Poland. The article contributes to the discussion on the need to redefine energy security in the context of competition below the threshold of war as well as the protection of energy resources in the future.

The evolution of hybrid threats since 2022 – case studies

With the start of the Russian Federation's full-scale aggression against Ukraine in February 2022, there has been an increase in the number of hybrid incidents targeting EU and North Atlantic Treaty Organisation countries. Submarine infrastructure, including energy and communication systems in the Baltic Sea region, is increasingly becoming the target of such activities. These activities are

[6] A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/, pp. 5–8 [accessed: 20 VI 2025].

[7] T. Szubrycht, *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim* (Eng. Allied response to threat in the Baltic Sea), "Bezpieczeństwo Narodowe" 2025, vol. 46, no. 1, pp. 49–75. https://doi.org/10.59800/bn/207646.

characterised by low detectability, difficulty in clearly assigning responsibility, and being conducted below the threshold of open armed conflict. In this context, OWFs, which are a strategic source of energy, appear to be a new area of competition in the grey zone[8].

The turning point in the perception of threats to maritime infrastructure was the sabotage of the Nord Stream 1 and Nord Stream 2 gas pipelines in September 2022. The explosions occurred in the territorial waters of Sweden and Denmark, resulting in the permanent shutdown of both pipelines. The Swedish services found traces of explosives and classified the incident as sabotage[9]. Although the perpetrator was not clearly identified, this incident made the public aware that undersea infrastructure could be attacked using means below the threshold of war.

In October 2023, a serious incident occurred involving the Balticconnector gas pipeline connecting Finland and Estonia. The investigation revealed that the pipeline had been cut by the anchor of the Newnew Polar Bear container ship, which also damaged a parallel telecommunications cable[10]. Finnish Prime Minister Petteri Orpo informed the public that the damage was deliberate and could be considered hybrid activities[11].

In December 2024, the EstLink 2 submarine power and telecommunications cable which links Estonia and Finland was damaged. According to the Finnish police, this was caused by the dragging of an anchor by the Eagle S ship belonging to the Russian shadow fleet. The incident was investigated by the intelligence services and classified as an act that could threaten the security of CI[12].

GPS and AIS (automatic identification system) signal interference is also increasingly being observed in the Baltic Sea region, especially around Gotland,

---

8 M. Cavcic, *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, Offshore Energy, 11 XII 2024, https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [accessed: 19 VI 2025].

9 J. Henley, *'Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022, https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [accessed: 19 VI 2025].

10 *Finnish media: Balticconnector pipeline leak 'does not appear to be an accident'*, ERR News, 10 X 2023, https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [accessed: 19 VI 2025].

11 *Finland blames Chinese ship for Baltic Sea gas pipeline damage*, Euronews, 25 X 2023, https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [accessed: 19 VI 2025].

12 C. Smith, *Finland investigates Russia 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024, https://www.bbc.com/news/articles/cr56l7prj2mo [accessed: 19 VI 2025].

Finnmark in Norway and the Gulf of Finland[13]. These disruptions, most likely caused by radio-electronic warfare systems, have a direct impact on the safety of civil and military navigation.

In the literature on maritime security and protection of maritime CI, a domain-based approach is increasingly being used to classify threats[14]. This allows for a more precise correlation between the nature of the threat and the appropriate detection, protection and response measures. With regard to OWFs, hybrid threats should be analysed not as homogeneous 'forms', but as activities carried out in separate but overlapping operational domains.

The surface domain concerns physical threats, including sabotage of service vessels, deliberate collisions of ships with OWF infrastructure elements, unauthorised presence of vessels in safety zones, and activities carried out using shadow fleets[15]. From an operational safety perspective, this domain is particularly important during the operation of the OWFs.

The underwater domain covers activities targeting infrastructure hidden beneath the sea surface, especially export cables used to transmit energy and array cables as well as telecommunications fibre optics. The literature indicates that activities in this domain are characterised by a high threshold of detectability, asymmetry of costs and difficulty in clearly attributing responsibility. It is therefore a particularly useful tool for hybrid operations[16].

In the cyber domain, threats mainly concern attacks on SCADA/OT systems, energy management systems and the IT infrastructure of OWF operators. Cyber attacks can lead to both operational disruptions and breaches of physical security of farms by interfering with monitoring, positioning or wind turbine control systems.

The information domain includes disinformation activities and influence operations aimed at reducing the level of public acceptance of OWFs, questioning their safety and profitability, as well as highlighting their negative impact on the marine environment. These activities may indirectly influence regulatory and

[13] *Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni* (Eng. GPS interference in the Baltic Sea has persisted for over 60 days), Portal Morski, 18 I 2025, https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [accessed: 19 VI 2025].

[14] R. Miętkiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Offshore wind farms, new elements of maritime security), "Sprawy Międzynarodowe" 2019, vol. 72, no. 1. https://doi.org/10.35757/SM.2019.72.1.06.

[15] M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), "Ekspertyzy PTBN" 2023, no. 1.

[16] Ibid.

investment decisions and the pace of development of the offshore wind energy sector[17].

In the radio-electronic domain, threats are identified that involve interference with GNSS (global navigation satellite system) signals, maritime communications and navigation systems used by service units and autonomous systems[18]. Such interference may be part of the preparation for or support of physical and undersea activities.

The domain-based approach to threats, present in more recent analyses of maritime and energy security, allows us to move away from a simplified division into 'forms of threats' in favour of a systemic multi-domain analysis that better reflects the nature of hybrid threats to OWFs.

According to V Adm. Didier Malaterre from NATO Allied Maritime Command, the Baltic Sea region has become a new arena for destabilising activities, targeting not only equipment but also the entire capacity of states to respond effectively[19]. The scale, frequency and complexity of these incidents demonstrate the need to adapt national infrastructure protection strategies to the realities of the grey zone and to consider OWFs as potential targets.

Analysis of vulnerabilities in the critical infrastructure protection system in Poland

Despite legislative developments, the Polish CI protection system is not keeping pace with the specific nature of hybrid threats to offshore facilities, including OWFs. The *Act of 26 April 2007 on crisis management* and the *Act of 5 July 2018 on the national cybersecurity system* establish a formal framework for the protection of CI, but OWFs have not been explicitly classified as CI of strategic importance. The *Poland's energy policy until 2040* (PEP2040) identifies OWFs as a key element of energy transition and security of supply, but the document does not describe the procedures and protection mechanisms intended for offshore infrastructure[20].

[17] R. Miętkiewicz, *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych* (Eng. Offshore wind farms. Security architecture using unmanned technologies), "Gospodarka Materiałowa i Logistyka" 2017, no. 12, pp. 688–702.

[18] Ibid.

[19] M. Bryant, *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024, https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [accessed: 19 VI 2025].

[20] Ministry of Climate and Environment, *Polityka energetyczna Polski do 2040 r…*

The lack of precise regulations results in an unclear division of responsibilities between ministries. It is not clearly indicated which institutions are responsible for prevention, monitoring and responding to threats to OWFs. Formally, tasks related to CI protection are carried out by the Internal Security Agency, the Border Guard, the Polish Navy and the Operational Centre of the Ministry of National Defence, but there is no integrated coordination mechanism between these entities. The situation is further complicated by the lack of clear guidelines for OWF operators regarding their information obligations and cooperation with state crisis management centres (the Government Centre for Security, CERT Polska, CSIRT MON)[21].

The report prepared by the European Centre of Excellence for Countering Hybrid Threats identified serious gaps in testing the resilience of offshore infrastructure to hybrid activities. National regulations do not require regular exercises involving OWF operators, law enforcement agencies and military structures. Tools such as red teaming or realistic digital twin simulations, which would allow for the assessment of the technical and organisational resilience of OWFs in conditions of physical and cyber disruptions or disinformation activities, are also not used[22].

Another problem area is the insufficient adaptation of regulations concerning the physical protection of CI to maritime conditions. The regulations in force are based on the model of land infrastructure protection, which causes difficulties in implementing security systems in the maritime environment (e.g. patrolling of water areas, installation of acoustic detectors, radar integration)[23]. There is also a lack of harmonised procedures for protecting power cables and the foundations of CI facilities. However, there are rules for creating protection systems for transformer stations and cable lines contained in the *Regulation of the Minister of Climate and Environment of 25 May 2022 on specific requirements for components of power transmission equipment and for components of offshore power stations*.

There is a lack of consistency in the area of cybersecurity. According to the findings of the Supreme Audit Office, many local government units and energy operators do not have updated cyber incident response plans in place, nor do they implement standards similar to those contained in Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common

[21] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities...*

[22] A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[23] A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats*…

level of cybersecurity across the Union (hereinafter: NIS 2 Directive)[24] and in PN-EN ISO/IEC 27001 standard concerning Information Security Management System[25]. Although some OWF operators operating in Poland (e.g. Ørsted, Equinor) implement good practices drawn from Scandinavian markets, there is no national cybersecurity standard for offshore infrastructure.

From a strategic point of view, the main gap is the lack of a comprehensive, inter-ministerial strategy for the protection of maritime infrastructure as a whole. Current strategic documents, including the *National Crisis Management Plan*[26] or the *Cybersecurity doctrine of the Republic of Poland*[27], do not take into account the specific nature of OWFs as objects with dual sensitivity – energy and maritime. The protection of OWFs requires a multi-domain approach, including military (sabotage protection), IT (cyber protection), institutional (coordination) and engineering (technical advancement) components. It should be noted that the National Critical Infrastructure Protection Programme 2023 includes technical measures, carried out mainly by the Government Centre for Security and CI operators (in this case – OWFs). These include: establishing working groups and developing CI security standards, identifying and verifying their effectiveness, creating a database of incidents that have occurred at CI facilities, and training platforms for CI operators and administration[28].

The changes in EU law resulting from the CER Directive and its relation with the NIS 2 Directive are an important context for assessing the effectiveness of the national system for protecting OWFs as CI.

---

[24] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, pp. 80–152.

[25] Najwyższa Izba Kontroli (Supreme Audit Office), *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego* (Eng. Information on audit results. Ensuring information security and continuity of IT systems in local government units), https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [accessed: 20 VI 2025].

[26] Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Krajowy Plan Zarządzania Kryzysowego 2025* (Eng. The National Crisis Management Plan 2025), https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [accessed: 20 VII 2025].

[27] Biuro Bezpieczeństwa Narodowego (National Security Bureau), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Eng. The Cybersecurity doctrine of the Republic of Poland), https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 20 VI 2025].

[28] Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity* (Eng. The National Critical Infrastructure Protection Programme 2023 – consolidated text), Warszawa 2023.

The CER Directive introduces a fundamental change in the approach to CI protection, moving away from the model of protecting 'facilities' towards identifying and regulating critical entities, including those of particular importance for Europe. It imposes a number of public law obligations on these entities, including: conducting regular risk assessments, implementing technical and organisational measures to ensure resilience, reporting incidents, and submitting to supervision by competent authorities equipped with sanctioning instruments.

The NIS 2 Directive stipulates that entities identified under the CER Directive as being of critical importance should also be considered key entities within the meaning of cybersecurity regulations, as follows from Article 2(3) of the NIS 2 Directive.

The mechanism of 'automatic' subjection of OWFs to a dual regulatory regime creates a risk of normative conflicts and dispersion of institutional responsibility in the process of implementing both directives into the Polish legal system. In this context, it seems reasonable to consider a coherent model of supervision and response, including the establishment of specialised sectoral structures, such as CSIRT ENERGY (Computer Security Incident Response Team for the Energy Sector), capable of handling the specific nature of offshore energy infrastructure.

An additional problem is the time needed to implement the regulations. The deadline for transposing the CER Directive expired on 17 October 2024, and the amendment to the Act on crisis management and the issuance of implementing acts are still pending. The operation of the first OWFs in Polish areas of the Baltic Sea is to commence in 2026. During the transition period, this infrastructure may therefore operate in a state of regulatory limbo and be subject to protection instruments that are unsuitable to the realities of the offshore sector. It is therefore reasonable to ask whether the proposed legislative solutions will constitute an effective and coherent instrument for building resilience to hybrid threats, or whether further systemic gaps will emerge when OWFs are launched.

Examples of good practices at national and international levels

In response to growing hybrid threats to maritime infrastructure, NATO and EU countries are developing multifaceted protection models that combine military, civil and technical measures. The experiences of countries with developed offshore sectors – the United Kingdom, the Netherlands and the Nordic countries – are particularly important, as they have developed modern response and prevention instruments.

At the NATO alliance level, the Baltic Sentry[29] concept is being developed – a joint system for patrolling and surveying critical infrastructure for the Baltic Sea. This programme involves the integration of coastal states' forces and the sharing of data between NATO structures, private operators and civil institutions responsible for CI protection. An important element of the Baltic Sentry is the use of advanced analytical tools, including AI-based systems, to detect anomalies in maritime traffic, identify unusual patterns of behaviour by vessels, and provide early warning of potential hybrid activities. These solutions are developed and utilised, among others, within the structures of NATO's Allied Maritime Command (MARCOM) and cover also the Baltic Sea in their operational scope. Within the framework of the Baltic Sentry, joint exercises are conducted as well as underwater and unmanned capabilities are developed. These activities are complemented by the launch of a specialised Maritime Centre for Security of Critical Undersea Infrastructure[30], whose task is to coordinate analyses, exchange information and support allied countries in the field of undersea CI protection.

The European Union, complementing military activities, is developing the CISE (Common Information Sharing Environment) platform. This system enables data sharing between border guards, environmental protection services, search and rescue (SAR) units, and private maritime infrastructure operators. Ultimately, CISE aims to increase so-called maritime situational awareness in times of peace, crisis and conflict[31].

The public-private partnership model used in the Netherlands and Norway is a good practice. OWF operators cooperate with the armed forces and government agencies to develop joint procedures for risk management, incident response, and testing the physical and cyber resilience of farms. Specialists from the British non-profit organisation Carbon Trust and the consultancy company ABPmer have developed a series of technical standards and guidelines for operators, including in the area of cable protection, foundations and SCADA systems[32].

---

[29] *NATO launches 'Baltic Sentry' to increase critical infrastructure security*, NATO, 14 I 2025, https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [accessed: 6 I 2026].

[30] *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure*, MARCOM NATO, 28 V 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [accessed: 6 I 2026].

[31] *Common Information Sharing Environment (CISE)*, European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [accessed: 20 VI 2025].

[32] *Industry leaders agree best practice for protecting offshore wind cables*, Carbon Trust, 13 XI 2024, https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [accessed: 20 VI 2025].

Another distinctive approach is the implementation of the *defence by design* principle, i.e. designing offshore infrastructure with resistance to hybrid activities in mind. This means, for example, installing redundant power supply and data transmission systems, locating vulnerable points below sea level and physically separating critical systems.

The United Kingdom was one of the first countries to launch a special unit for the protection of undersea infrastructure. In 2023, the Royal Navy commissioned the Proteus ship into the Royal Fleet Auxiliary as part of the MROSS (Multi-Role Ocean Surveillance Ship) programme. This ship is equipped with sonar systems, underwater drones and a data analysis centre, which enable real-time monitoring of cables and OWFs[33].

Denmark, in turn, is implementing innovative systems based on autonomous technology. The Saildrone Voyager platforms are being tested – unmanned sailing vessels capable of monitoring selected objects in the Baltic Sea for several weeks. These devices are equipped with meteorological sensors, radar, thermal imaging cameras and AIS kits[34].

International experience shows that effective protection of OWFs cannot be limited to physical and digital security measures, but must be part of an integrated, cross-sectoral response system. Some countries of the Baltic region (Estonia, Finland and Sweden) are currently implementing national models that integrate coast guards, intelligence services, energy network operators and the military. This model could serve as inspiration for Poland, especially in the context of a lack of clear coordination processes.

At the operational level, initiatives are also being developed in Poland aimed at providing digital support for the monitoring and protection of maritime infrastructure in the Baltic Sea region, including programmes provisionally referred to as Digital Baltic[35]. Their aim is to integrate data from maritime surveillance systems, technical sensors and operator sources in order to increase situational awareness at sea. These initiatives are part of a broader trend towards the use of digital and analytical tools for early detection of anomalies and to support decision-making processes in times of peace and crisis[36]. An important role in the maritime infrastructure protection

[33] *RFA Proteus (K60)*, Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [accessed: 20 VI 2025].

[34] *Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea*, Saildrone, 16 VI 2025, https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [accessed: 20 VI 2025].

[35] Digital Baltic, https://digitalbaltic.pl [accessed: 7 I 2026].

[36] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*

system is played by the Maritime Border Guard Regional Unit[37] whose tasks include protecting Poland's maritime border, ensuring the safety of navigation and responding to incidents in the territorial sea, where critical infrastructure elements are located, including sections of OWF export lines. The inclusion of the Maritime Border Guard Regional Unit in the OWF protection model is a key element of the non-military security component, complementing the activities of the armed forces and allied structures, especially in the area of ongoing monitoring, control of maritime traffic and cooperation with CI operators.

Strategic, organisational and technological recommendations

In Poland, decisive action is needed at the legislative and operational levels to ensure effective protection for OWFs. The experience of coastal states shows that this requires cooperation between public institutions, the private sector (operators) and the armed forces. The proposed strategic, organisational and technological recommendations are based on such an integrated approach to security of CI.

Strategic recommendations

1. Statutory recognition of OWFs as CI – it is necessary to clarify the status of OWFs in Polish legal system by including them in the list of CI sectors, in accordance with the CER Directive and the updated PEP2040.
2. Development of a national strategy for the protection of offshore infrastructure – this strategy should integrate military and non-military components, including the Maritime Border Guard Regional Unit, Police (including water police), maritime administration and CI operators. A special role in this system should be assigned to OWF operators located in exclusive economic zone (EEZ), who, due to their constant operational presence, are the first link in CI monitoring, early detection of anomalies and reporting of hybrid incidents. The role of the CI operators in EEZ should primarily consist of: a) maintaining technical and environmental monitoring systems (SCADA, sensors, positioning and observation systems), b) ensuring data interoperability with national

(Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), "Nautologia" 2024, no. 161, pp. 71–76.

[37] *Zadania Morskiego Oddziału Straży Granicznej* (Eng. Tasks of the Maritime Border Guard Regional Unit), Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012, https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [accessed: 7 I 2026].

and allied systems, c) implementing incident response procedures in accordance with the National Crisis Management Plan, d) participating in exercises and resilience tests conducted with the involvement of public administration and armed forces. This definition of the role of operators allows the limited physical presence of the state in EEZ to be supplemented by a model of shared responsibility and public-private partnership, in line with solutions adopted in the Nordic countries and within NATO.

3. Inclusion of OWFs in regular defence and crisis management exercises – OWFs should become an integral part of national exercises such as IGNIS[38], as part of testing resilience to physical sabotage and cyber attacks[39].

Organisational recommendations

1. Establishment of an interministerial team for offshore infrastructure safety – the team should include representatives of the Ministry of National Defence, the Internal Security Agency, the Government Centre for Security, the Ministry of the Interior and Administration, the maritime administration (maritime authorities), the Maritime Border Guard Regional Unit, Police (including water police), and OWF operators as entities directly responsible for infrastructure operation. The role of the maritime administration should include, in particular, the coordination of maritime traffic management activities, the designation and enforcement of security zones, and the integration of threat information with VTS (vessel traffic service) service systems and national maritime situational awareness. OWF operators should be involved in the team's work not only as stakeholders, but also as active participants in the process of planning, testing and improving incident response procedures, including through participation in inter-agency exercises and the provision of operational data to the relevant state authorities.
2. Closer civil-military cooperation – joint patrols, interoperable command centres and data exchange (using platforms such as CISE) will enable faster detection and neutralisation of threats.
3. Mandatory integration of OWF operators with the National Crisis Management Plan system and the national cybersecurity system – this requires a review of executive acts and the incident reporting system.

---

[38] *Krajowe ćwiczenia ratownicze "IGNIS 2025"* (Eng. National rescue exercises 'IGNIS 2025'), Serwis Rzeczypospolitej Polskiej, 15 X 2025, https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [accessed: 20 XI 2025].

[39] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*…

Technological recommendations

1. Investing in unmanned reconnaissance systems[40] (uncrewed surface vehicle, USV; unmanned aerial systems, UAS; unmanned aerial vehicle, UAV) – autonomous patrol platforms (such as Saildrone) should be used to protect OWFs, ensuring round-the-clock surveillance of the maritime area and early detection of unauthorised activity.
2. The use of sensor systems in accordance with national rules governing the operation of OWFs – the installation of radars, acoustic sensors, passive sonars and electro-optical observation systems should be carried out on the basis of analyses conducted in Poland on the impact of OWFs on national security and defence systems, which are part of the planning and consultation process for offshore investments. The need to implement selected sensors has been recognised and is gradually being taken into account in national and allied maritime monitoring systems, while maintaining interoperability with existing state solutions.
3. Building cyber resilience in accordance with the standards of the NIS 2 Directive and PN-EN ISO/IEC 27001 standard – OWF operators should be required to implement auditable incident management procedures as well as regular penetration testing and red teaming, i.e. testing the overall resilience of the organisation to threats, from the level of technology to procedures.

Summary and directions for further research

Offshore wind farms are gaining the status of strategic infrastructure not only from an ecological, economic and business perspective, but also as potential targets for hybrid operations and activities in grey zone. In the face of growing tensions in the Baltic Sea region, they are becoming a new arena for rivalry – involving physical, cyber and information activities conducted below the threshold of open conflict and blurring the line between war and peace.

Poland, aspiring to become a regional leader in the RES sector, is at a very important moment. By adopting an integrated, multi-layered approach – encompassing legal regulations, interoperable civil-military activities, cyber resilience, technical reconnaissance, as well as international and sectoral

[40] R. Miętkiewicz, *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, vol. 213, no. 2, pp. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

cooperation – Poland can become a model for the effective protection of maritime infrastructure against hybrid threats.

Directions for further research should include:

1. Hybrid risk modelling using digital twin simulation[41] – this should be treated as a tool supplementing the risk identification and assessment processes carried out by OWF operators at the infrastructure planning, construction and operation stages. In accordance with regulatory requirements and good practices in the offshore sector, OWF operators conduct risk analyses covering technical, environmental and operational risks[42]. The use of digital twin does not replace these activities, but allows for their deepening and analysis of the relationships between different categories of threats, including physical, cyber and information threats. The creation of a virtual equivalent of OWF enables testing the resilience of infrastructure to complex, multi-domain threat scenarios in a controlled simulation environment, without interfering with the functioning of real facilities. This tool will allow for the assessment of the effects of cumulative impacts, such as power disruptions, SCADA/OT system interference, or information activities affecting decision-making processes. This approach is already being put to practical use in the offshore sector, primarily in the Nordic countries, as part of operational decision support and maritime infrastructure security planning[43].
2. Designing and conducting red teaming exercises – implementing realistic attack scenarios (physical, cybernetic, social engineering) enables a reliable assessment of the readiness of OWF operators and state institutions, which is necessary to improve procedures for responding to infrastructure violations.
3. Analysis of private sector involvement in coordinating responses to threats – further research should focus on determining the place of OWF operators in a multi-level response architecture, in which the operator is responsible for the operational and technical levels (detection, initial assessment of the incident, securing business continuity), while crisis response coordination and strategic decisions remain the responsibility

[41] G. Faiz, *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [accessed: 7 I 2026].

[42] *Energy Transition Outlook 2025*…

[43] T. Russell, *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020, https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [accessed: 7 I 2026].

of the relevant state authorities and allied structures[44]. This allocation of roles is consistent with the approach adopted in NATO and EU documents and with practice in the offshore sector, where operators perform a front-line monitoring and reporting function rather than commanding the response to a crisis situation[45].

4. Development and evaluation of national technologies for OWF security – focus should be placed on identifying and evaluating the potential of national dual-use technologies that can be used to protect OWFs, particularly in the areas of sensor systems, unmanned maritime and aerial platforms, data analytics, and offshore infrastructure cybersecurity[46]. Important areas of research include the analysis of the impact of the development and implementation of national technologies on increasing the systemic resilience of OWFs, reducing the dependence of technologies on attack-sensitive systems, and improving state control over the key elements of security system[47]. The research should also include an assessment of the mechanisms for integrating national technological solutions with state and allied systems, including the EU and NATO, as well as an analysis of the legal, organisational and financial barriers limiting implementation of these solutions in offshore environment[48].

Bibliography

Mickiewicz P., *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku* (Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), "Nautologia" 2024, no. 161, s. 71–76.

Miętkiewicz R., *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Offshore wind farms, new elements of maritime security), "Sprawy Międzynarodowe" 2019, vol. 72, no. 1. https://doi.org/10.35757/SM.2019.72.1.06.

[44] *Energy Transition Outlook 2025*…

[45] *Industry leaders agree best practice*…; A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[46] Rządowe Centrum Bezpieczeństwa, *Krajowy plan zarządzania kryzysowego 2025*…; P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie*…

[47] Ibid.

[48] *Common information sharing environment (CISE)*…

Miętkiewicz R., *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych* (Eng. Offshore wind farms. Security architecture using unmanned technologies), "Gospodarka Materiałowa i Logistyka" 2017, no. 12, pp. 688–702.

Miętkiewicz R., *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, vol. 213, no. 2, pp. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), "Ekspertyzy PTBN" 2023, no. 1.

Szubrycht T., *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim* (Eng. Allied response to threat in the Baltic Sea), "Bezpieczeństwo Narodowe" 2025, vol. 46, no. 1, pp. 49–75. https://doi.org/10.59800/bn/207646.

Internet sources

Ávila-Zúñiga-Nordfjeld A., *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/ [accessed: 20 VI 2025].

Bryant M., *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024, https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [accessed: 19 VI 2025].

Cavcic M., *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, OffshoreEnergy, 11 XII 2024, https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [accessed: 19 VI 2025].

Common information sharing environment (CISE), European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [accessed: 20 VI 2025].

Countering hybrid threats, NATO, 7 V 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [accessed: 20 VI 2025].

Digital Baltic, https://digitalbaltic.pl [accessed: 7 I 2026].

Energy Transition Outlook 2025, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [accessed: 20 VI 2025].

Faiz G., *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [accessed: 7 I 2026].

Finland blames Chinese ship for Baltic Sea gas pipeline damage, Euronews, 25 X 2023, https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [accessed: 19 VI 2025].

Finnish media: Balticconnector pipeline leak 'does not appear to be an accident', ERR News, 10 X 2023, https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [accessed: 19 VI 2025].

Henley J., *'Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022, https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [accessed: 19 VI 2025].

Industry leaders agree best practice for protecting offshore wind cables, Carbon Trust, 13 XI 2024, https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [accessed: 20 VI 2025].

Krajowe ćwiczenia ratownicze "IGNIS 2025" (Eng. National rescue exercises 'IGNIS 2025'), Serwis Rzeczypospolitej Polskiej, 15 X 2025, https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [accessed: 20 XI 2025].

NATO launches 'Baltic Sentry' to increase critical infrastructure security, NATO, 14 I 2025, https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [accessed: 6 I 2026].

NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure, MARCOM NATO, 28 V 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [accessed: 6 I 2026].

RFA Proteus (K60), Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [accessed: 20 VI 2025].

Russell T., *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020, https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [accessed: 7 I 2026].

Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea, Saildrone, 16 VI 2025, https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [accessed: 20 VI 2025].

Sari A., *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [accessed: 20 VI 2025].

Smith C., *Finland investigates Russia 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024, https://www.bbc.com/news/articles/cr56l7prj2mo [accessed: 19 VI 2025].

Zadania Morskiego Oddziału Straży Granicznej (Eng. Tasks of the Maritime Border Guard Regional Unit), Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012, https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [accessed: 7 I 2026].

Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni (Eng. GPS interference in the Baltic Sea has persisted for over 60 days), Portal Morski, 18 I 2025, https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [accessed: 19 VI 2025].

Legal acts

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC – (Official Journal of the EU L 333 of 27 XII 2022).

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

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws of 2026, item 20).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

Regulation of the Minister of Climate and Environment of 25 May 2022 on specific requirements for components of power transmission equipment and for components of offshore power stations (Journal of Laws of 2022, item 1257).

Other documents

Biuro Bezpieczeństwa Narodowego (National Security Bureau), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Eng. The cybersecurity doctrine of the Republic of Poland), https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 20 VI 2025].

European Commission, *The REPowerEU Plan*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [accessed: 20 VI 2025].

Ministerstwo Klimatu i Środowiska (Ministry of Climate and Environment), *Polityka energetyczna Polski do 2040 r. (PEP2040)* (Eng. Poland's energy policy until 2040 (PEP2040)), Warszawa 2021.

Najwyższa Izba Kontroli (Supreme Audit Office), *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego* (Eng. Information on audit results. Ensuring information security and continuity of IT systems in local government units), https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [accessed: 20 VI 2025].

PN-EN ISO/IEC 27001 standard – Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Krajowy Plan Zarządzania Kryzysowego 2025* (Eng. The National Crisis Management Plan 2025), https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [accessed: 20 VII 2025].

Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity* (Eng. The National Critical Infrastructure Protection Programme 2023 – consolidated text), Warszawa 2023.

Klaudia Maciata

Offshore operations specialist in the wind energy sector. Ambassador for the Women Offshore initiative, member of international projects in the field of maritime and climate security. Expert on the protection of critical infrastructure against hybrid threats in the Baltic Sea region. Author of publications in "NATO Review". Professionally associated with, among others, Ørsted, she previously worked in the industrial services, unmanned technology and public affairs consulting sectors. Currently she is a founder of the "Baltic Sea Security" project and a freelancer.

Contact: klaudia.maciata@gmail.com

Internal Security Review
2026, no. 34, pp. 351–362

https://doi.org/10.4467/20801335PBW.26.016.23378

ARTICLE

The development of cyber threats related to the use of AI

JAKUB GAJECKI

Independent author

https://orcid.org/0009-0007-3488-0236

Abstract

The rapid development of artificial intelligence (AI) means that its role in cyberspace is also growing, both in terms of threats and defence against them. AI supports the automation of anomaly detection, data analysis, and incident response, which enhances protection efficiency. However, cybercriminals use AI-based solutions to create sophisticated attack tools, such as advanced phishing schemes, deepfakes, and hard-to-detect malware. The author analyses the role of AI in generating cyber threats and evaluates defensive strategies in this context. He highlights the need for international cooperation and legal regulation regarding the use of AI in cybersecurity.

Keywords

artificial intelligence, cybersecurity, AI as a service, cybercrime, quantum cryptography

Introduction

The development of information technology and artificial intelligence (AI) has changed the approach to cybersecurity and ushered in a new era of cyber threats. In the past, cyber attacks such as computer viruses and phishing, i.e. impersonating institutions or individuals in order to obtain information[1], were relatively simple and limited to activities carried out by individual hackers or small groups. At the turn of the 20th and 21st centuries, the biggest challenge was to prevent the spread of malicious software (malware), including ransomware type, and to respond quickly to it[2]. These attacks were usually targeted at individuals or smaller organisations, and their scope and impact were limited by technological capabilities[3]. Advances in AI and machine learning have transformed cyberspace and made threats more complex, dynamic, and difficult to detect. AI has introduced a new quality in both conducting attacks in cyberspace and defending against them.

AI allows makes it possible to:

- analyse security infrastructure,
- automate the search for its vulnerabilities,
- develop intelligent tools that can adapt to the defensive actions of attacked systems in real time.

AI makes such attacks extremely difficult to neutralise.

The article analyses the impact of the development of AI, particularly its classical and generative (GenAI) types, on the development of threats in cyberspace, both offensively (cybercrime activities) and defensively (cyber defence systems).

The research problem was formulated in the following way: How does the use of classical and generative AI methods change the nature, scale and automation of threats in cyberspace, and what are the consequences for cybersecurity systems?

The specific objectives of the study are:

- identification of classic AI applications in cybersecurity,
- analysis of the use of generative AI by cybercriminal groups,
- assessment of current defence systems against automated attacks,

---

1 J. Jancelewicz, *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych* (Eng. Phishing and related social engineering attacks as a threat to non-governmental organisations), "Trzeci Sektor" 2022, vol. 3–4, no. 59–60, pp. 80–81. https://doi.org/10.26368/17332265-59/60-3/4-2022-5.

2 *The Evolution of Cybersecurity*, Codecademy, https://www.codecademy.com/article/evolution-of-cybersecurity [accessed: 7 X 2024].

3 B. Dash et. al., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review,* "International Journal of Software Engineering & Applications" 2022, vol. 13, no. 5, p. 14. https://doi.org/10.5121/ijsea.2022.13502.

- identification of directions for further research and regulatory action.

The article employs research methods such as analysis and synthesis as well as induction and deduction. The author used various source materials: compact publications, monographs and scientific articles, reports, specialist publications and case study descriptions.

Development of botnets and malware

Botnets, i.e. groups of infected computers controlled without their owners' knowledge, began to develop at the beginning of the 21st century. One of the first and most well-known botnets was Agobot, which used infected devices to send spam and carry out DDoS (Distributed Denial of Service) attacks[4], the aim of which is to overload the servers of attacked entities and prevent access to their services. Subsequent botnets such as Storm and Conficker demonstrated their power and scale of operation, taking control of millions of devices and becoming a real threat to global computer systems[5].

The evolution of malware encompasses its many forms: viruses, worms, spyware, advertising-supported software (adware), rootkits which provide administrator-level access and ransomware. An example of early malware development is ILOVEYOU virus, which was not yet a botnet, but due to the scale of its impact, it became an inspiration for the search for more advanced forms of malware. As technology evolved, malware also became increasingly specialised. Zeus and SpyEye are examples of malwares focused on stealing data from online banking[6]. In turn, Stuxnet was the first programme designed to physically damage industrial critical infrastructure devices[7]. Botnets have become the main tools in DDoS attacks. The examples are Mirai and Satori botnets, which transformed IoT (Internet of Things) devices into tools for large-scale attacks. In 2016, Mirai attacked

[4] A. Kurniawan, A. Fitriansyah, *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, "International Journal of Computer and Communication Engineering" 2018, vol. 7, no. 4, pp. 130–131. https://doi.org/ 10.17706/ijcce.2018.7.4.128-135.

[5] J. Yimu, L. Shangdong, *Threats from Botnets*, in: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernandez-Carames (eds.), September 2020, https://www.intechopen.com/chapters/69332 [accessed: 18 X 2024].

[6] N. Etaher, G.R.S. Weir, *Understanding the Threat of Banking Malware*, in: *Proceedings of Cyber-forensics*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf, pp. 77–79 [accessed: 18 X 2025].

[7] M. Hagerott, *Stuxnet and the vital role of critical infrastructure operators and engineers,* "International Journal of Critical Infrastructure Protection" 2014, vol. 7, no. 4, pp. 244–246. https://doi.org/10.1016/j.ijcip.2014.09.001.

servers belonging to DNS (Domain Name System) providers, blocking access to popular websites around the world[8].

Malware and botnets currently use AI-based solutions, which allow them to bypass detection systems and conceal their presence more effectively. AI enables botnets to analyse and adapt in real time. This increases the effectiveness of attacks and reduces the likelihood of detection. Automated botnets can independently identify new targets and even use machine learning techniques to recognise patterns of victim behaviour and adapt their actions accordingly.

Artificial intelligence as a tool for cybercriminals

Artificial intelligence is defined as a field of computer science concerned with designing systems capable of performing tasks that previously required skills such as learning, reasoning, perception, or decision-making. The classical approach to AI includes, among others, rule-based systems, machine learning, neural networks, and probabilistic inference algorithms[9].

Cybercriminals are able to automate and streamline phishing and malware attacks, making them more widespread and difficult to detect. Thanks to AI, hackers can quickly analyse large amounts of data, e.g. user behaviour and profiles, to create more convincing messages tailored to different target groups. Personalisation increases the likelihood that the recipient will decide to click on a malicious link or download an attachment. Artificial intelligence can also facilitate the creation and distribution of malicious software. AI analyses system protection mechanisms, adapting malware behaviour so that it remains undetectable. An example of this is malware that uses machine learning to carry out so-called polymorphic attacks. They involve the malware changing its characteristics with each infection, making it much more difficult for traditional antivirus programmes to identify[10]. Cybercriminals also use AI to create deepfakes, i.e. fake images, video or audio recordings, which they use in various criminal scenarios, such as financial fraud, manipulation of public opinion, and even blackmail[11].

---

[8] H. Griffioen, Ch. Doerr, *Examining Mirai's Battle over the Internet of Things*, https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf, p. 744 [accessed: 18 X 2025].

[9] S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, n.p. 2021, pp. 1–2.

[10] R. Chauhan et. al., *Polymorphic Adversarial Cyberattacks Using WGAN*, "Journal of Cybersecurity and Privacy" 2021, no. 1, pp. 788–789. https://doi.org/10.3390/jcp1040037.

[11] O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość* (Eng. Deepfake as a complicated and deeply false reality), "Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, vol. 9, no. 3, pp. 20–24. https://doi.org/10.24917/26578549.9.3.2.

The development of GenAI, including large language models (LLM) and generative models based on neural network architecture such as generative adversarial networks, has significantly changed the modus operandi of cybercriminal groups. Generative AI enables the automatic creation of highly personalised phishing content, the generation of malware code, and the scaling of social engineering attacks. Research indicates that the use of LLM lowers the barrier to entry into cybercrime, enabling individuals without specialist knowledge to carry out sophisticated attacks[12]. An example of this is analysing search histories and visited websites in order to tailor phishing messages that appear authentic to the victim.

Machine learning is used to create more sophisticated and adaptive malware. These algorithms enable the malware to adapt its activities depending on the security measures detected on the victim's system and to carry out an attack at the most appropriate moment, e.g. identifying moments when the user logs into sensitive systems such as bank accounts. Machine learning algorithms enable new variants of malicious code to be generated and tested in a short period of time.

Another form of cybercrime based on machine learning are the aforementioned polymorphic attacks. Techniques such as polymorphism and metamorphism allow different variants of the same malware to be generated, making it impossible for pattern-based security software to recognise the modified code. Such techniques are among the most difficult to detect. Machine learning also enables for rapid data processing and trying different combinations in brute force attacks aimed at guessing passwords or security codes. These algorithms are able to predict which passwords are most likely to be used, which significantly reduces the time needed to break security measures. For example, when combined with behavioural analysis, algorithms can generate password suggestions that match the characteristic patterns applied by the user, such as names, birth dates or other personal details.

Cybercriminals use machine learning algorithms to analyse the structure and configuration of security systems. This type of software is capable of identifying and analysing specific features of security mechanisms such as firewalls, intrusion detection systems (IDS) and antivirus software. With this knowledge, attackers can adapt their methods in real time, break through successive layers of protection, and avoid detection. Artificial intelligence can not only generate different variants of the same malware (polymorphism, metamorphism), but also teach malware to recognise different security systems and adapt its behaviour to them, minimising the risk of detection. Advanced attacks using AI rely on predicting user behaviour based on behavioural analysis. By analysing large data sets of user behaviour,

[12] Y. Yigit et. al., *Review of Generative AI Methods in Cybersecurity*, arXiv, 13 III 2024. https://doi.org/10.48550/arXiv.2403.08701.

attackers can predict when a system will be least resilient to attack, for example, when attempting to log in while the security system is recording increased traffic and is more likely certain to ignore some irregularities.

Contemporary cases of cyberattacks

The attack on GitHub platform in 2018 was one of the most powerful DDoS attacks in history, reaching a data flow of 1.35 Tb/s. Cybercriminals used AI-controlled botnets, sending mass requests, which overloaded GitHub's servers. Artificial intelligence helped dynamically adapt the attack and bypass security measures in real time. AI assisted botnets are becoming more and more common, enabling attacks on large platforms[13].

In 2020, Cognizant company, global IT services provider, became a victim of Maze ransomware. This is an example of software using AI and advanced network infiltration techniques. This software uses system analysis to identify the most sensitive data and prevent access to it, and also distributes it further to criminal command centres. As a result of the attack, Cognizant experienced massive financial losses and spent millions of dollars on infrastructure repairs and support for customers and suppliers[14]. The company took corrective actions, including isolating infected systems, strengthening incident response procedures and expanding network monitoring mechanisms. However, this case shows that threat detection systems based primarily on signatures are not always able to detect advanced ransomware campaigns early enough[15].

In the same year, Twitter was attacked by cybercriminals who took over the accounts of famous people and companies, including Bill Gates, Elon Musk and Apple. Hackers used natural language processing (NLP) technology to generate messages that appeared personal and personalised, encouraging people to send money to a provided cryptocurrency address[16]. The attack was successful thanks

[13] L.H. Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018, https://www.wired.com/story/github-ddos-memcached/ [accessed: 26 X 2024].

[14] F. Truță, *Cognizant Expects to Lose up to $70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020, https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/ [accessed: 24 X 2024].

[15] *Cognizant Security Incident Update*, Cognizant, 18 IV 2020, https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm [accessed: 9 III 2026].

[16] N. Statt, *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020, https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised [accessed: 24 X 2025].

to, among other things, the use of AI to analyse the victims' communication patterns and adapt the messages. After detecting the incident, the platform blocked the ability of verified accounts to post and began the process of restoring the security of the compromised profiles. Additional measures controlling access to administrative tools were implemented, and employee authentication procedures were strengthened.

In 2025, the first documented case of large-scale use of autonomous AI agents in cyber intelligence operations was detected. In mid-September, Anthropic's Threat Intelligence team identified and subsequently disrupted a cyber espionage campaign in which a tool based on Claude Code language model was manipulated by an actor believed to have links to Chinese state bodies. The aim was to carry out complex intelligence operations[17].

In this campaign, AI did not play a merely advisory or generative role, but acted as an autonomous agent performing most of the operational tasks. The system broke down multi-step instructions into smaller tasks, which it then performed independently with minimal human supervision. Claude Code performed autonomously up to 80–90% of tactical operations, including:

- recognition of target infrastructure and analysis of vulnerabilities,
- generating and executing code that exploits vulnerabilities,
- collecting certificates and data,
- lateral movement,
- data extraction and classification[18].

This automation means that AI performed tasks that would previously have required the involvement of large teams of experts without constant operator intervention: from network scanning and vulnerability analysis to data exfiltration. In this case, the human's role was limited mainly to launching the campaigns and making strategic decisions at key moments, e.g. approving the transition between attack phases[19]. Furthermore, the AI agents' operating mechanism relied on their ability to make autonomous decisions within a sequence of tasks and to adapt their narrative and strategy to the subsequent stages of the attack. This significantly increased the speed and scale of operations compared to traditional 'manual control'. The machine was capable of performing thousands of operations per second – a feat beyond the reach of cybercriminal groups without automation[20].

---

[17] *Disrupting the first reported AI-orchestrated cyber espionage campaign*, Anthropic, 13 XI 2025, https://www.anthropic.com/news/disrupting-AI-espionage [accessed: 24 XI 2025].

[18] Ibid.

[19] Ibid.

[20] Ibid.

Artificial intelligence in cyber defence systems

The growth of AI as a service offerings brings benefits to business, but at the same time creates new attack vectors for cybercriminals. AI as a service provides access to advanced AI algorithms that can be used to automate tasks such as analysing system vulnerabilities or creating advanced phishing bots. In the future, cybercriminals may use AI as a service to develop deepfakes, carry out social engineering attacks on a larger scale, create malware that is harder to detect, and design ransomware that automatically selects the most effective attack methods, thereby increasing its efficiency.

To meet these challenges, new defence technologies based on AI are being developed. For example, adaptive systems based on machine learning can dynamically respond to threats and automatically adjust their protective functions depending on the attacks they encounter. In addition, NLP technologies are used to analyse cybercriminal communications, which helps in predicting and detecting new threats. In the future, it is expected that AI-based systems will be capable of independently analysing malware and creating dynamic, threat-resistant virtual environments, which will reduce the risk of security breaches[21].

It is worth emphasising that many cybersecurity regulations are currently in force both at the national and international levels. In Europe, the NIS2 Directive[22] on the security of networks and information systems plays a significant role, as does the Artificial Intelligence Act[23] governing the use of AI systems in the European Union. The Convention of the Council of Europe on Cybercrime[24], which forms the basis for international cooperation in combating cybercrime, is also an important tool.

However, it should be noted, that most of these regulations were drafted at a time when AI technologies were not yet widely used in cyber operations. Consequently, current regulations often do not explicitly address the specific

[21] R. Keshava et al., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, in: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore 2025. https://doi.org/10.1109/ICESC65114.2025.11212519.

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

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

[24] *Convention of the Council of Europe on Cybercrime, drawn up in Budapest on 23 November 2001.*

characteristics of AI-based systems, such as autonomous threat detection systems, generative models used to create phishing attacks, or automated tools for carrying out cyberattacks.

Development of AI application possibilities in cybersecurity primarily necessitates the clarification and extension of existing regulations, rather than creating them from scratch. This applies in particular to issues such as accountability for decisions made by AI systems, algorithm transparency, security standards and international cooperation arrangements for combating cyber threats. At the same time, effectively combating cybercrime requires closer international cooperation and the harmonisation of legal regulations in order to limit the opportunities for criminals to exploit differences between legal systems. This stems from the nature of cyberspace, which transcends national borders. Future regulations should address the use of AI systems for illegal activities, including cybercrime, clarify the rules on liability for the use of such systems, and restrict the use of certain high-risk technologies. International organisations, such as the United Nations and the European Union, play a key role in developing policies to combat cybercrime and in promoting common data protection standards. Such activities will enable a faster response to global threats and facilitate the exchange of information and experience regarding best practices in cybersecurity.

Summary

Based on theoretical considerations and an analysis of selected cases, the following conclusions have been drawn:

1. Artificial intelligence significantly increases the effectiveness and scalability of cyberattacks, particularly through the automation of phishing, the development of adaptive malware and the use of generative techniques (deepfakes), which lowers the barrier to entry into cybercrime.
2. Development of AI-based cyber defence systems improve the ability to detect and respond to threats. However, there is a technological race between the entities responsible for digital security and cybercriminals.
3. Effectively addressing the risks generated by AI requires coordinated systemic action, including international cooperation, the development of regulatory frameworks, and the harmonisation of legal and technical standards regarding the use of AI in cyberspace. Currently, at international level, the basis for cooperation between states in combating cybercrime is the Convention on cybercrime adopted by the Council of Europe. It sets out the framework for cooperation in the prosecution of crimes committed

using computer systems. Within the EU, the NIS2 Directive also plays a significant role, as it aims to enhance the security of networks and information systems, as does Artificial Intelligence Act, which establishes a legal framework for the secure and responsible use of AI systems.

4. Dynamic development of AI technology poses challenges to existing legal and technical systems. However, it does not seem necessary to introduce new regulations, rather, the existing provisions should be clarified and adapted to the specific nature of the risks associated with the use of AI in cyberspace.

Bibliography

Chauhan R., Sabeel U., Izaddoost A., Heydari S.S., *Polymorphic Adversarial Cyberattacks Using WGAN*, "Journal of Cybersecurity and Privacy" 2021, no. 1, pp. 767–792. https://doi.org/10.3390/jcp1040037.

Dash B., Ansari M.F., Sharma P., Ali A., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review,* "International Journal of Software Engineering & Applications" 2022, vol. 13, no. 5, pp. 13–21. https://doi.org/10.5121/ijsea.2022.13502.

Hagerott M., *Stuxnet and the vital role of critical infrastructure operators and engineers,* "International Journal of Critical Infrastructure Protection" 2014, vol. 7, no. 4, pp. 244–246. https://doi.org/10.1016/j.ijcip.2014.09.001.

Jancelewicz J., *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych* (Eng. Phishing and related social engineering attacks as a threat to non-governmental organisations), "Trzeci Sektor" 2022, vol. 3–4, no. 59–60, pp. 79–88. https://doi.org/10.26368/17332265-59/60-3/4-2022-5.

Keshava R., Pandurangan S.K., Sakthivanitha M., Parmsivan S., Sunkara G., Maruthi R., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, in: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore 2025. https://doi.org/10.1109/ICESC65114.2025.11212519.

Kurniawan A., Fitriansyah A., *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, "International Journal of Computer and Communication Engineering" 2018, vol. 7, no. 4, pp.128–135. https://doi.org/10.17706/ijcce.2018.7.4.128-135.

Russell S., Norvig P, *Artificial Intelligence. A Modern Approach*, n.p. 2021.

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość* (Eng. Deepfake as a complicated and deeply false reality), "Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, vol. 9, no. 3, pp. 19–30. https://doi.org/10.24917/26578549.9.3.2.

Yigit Y., Buchanan W.J., Tehrani M.G., Maglaras L., *Review of Generative AI Methods in Cybersecurity*, arXiv, 13 III 2024. https://doi.org/10.48550/arXiv.2403.08701.

Internet sources

Cognizant Security Incident Update, Cognizant, 18 IV 2020, https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm [accessed: 9 III 2026].

Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 XI 2025, https://www.anthropic.com/news/disrupting-AI-espionage [accessed: 24 XI 2025].

Etaher N., Weir G.R.S., *Understanding the Threat of Banking Malware*, in: *Proceedings of Cyberforensics 2014*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf [accessed: 18 X 2025].

Griffioen H., Doerr Ch., *Examining Mirai's Battle over the Internet of Things*, https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf [accessed: 18 X 2025].

Newman L.H., *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018, https://www.wired.com/story/github-ddos-memcached/ [accessed: 26 X 2024].

Statt N., *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020, https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised [accessed: 24 X 2025].

The Evolution of Cybersecurity, Codecademy, https://www.codecademy.com/article/evolution-of-cybersecurity [accessed: 7 X 2024].

Truță F., *Cognizant Expects to Lose up to $70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020, https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/ [accessed: 24 X 2024].

Yimu J., Shangdong L., *Threats from Botnets*, in: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernandez-Carames (eds.), September 2020, pp. 52–75, https://www.intechopen.com/chapters/69332 [accessed: 18 X 2024].

Legal acts

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

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

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) – (Official Journal of the EU L 2024/1689 of 12 VII 2024).

Jakub Gajecki

Graduate of the Jacob of Paradies University in Gorzów Wielkopolski in applied criminology, specialising in combating cybercrime. Second-cycle student at the Police Academy in Szczytno in the field of cybersecurity. His academic interests include cybersecurity and state security. He is a Police officer responsible for conducting preliminary proceedings.

Contact: gajeckijakub@protonmail.com

Internal Security Review
2026, no. 34, pp. 363–387

https://doi.org/10.4467/20801335PBW.26.017.23379

ARTICLE

Hybrid attacks against the Republic of Poland conducted and coordinated by the Russian Federation and their link to the war in Ukraine

AGATA RYTEL

Warsaw School of Economics

https://orcid.org/0009-0008-1506-1822

Abstract

The aim of this article is to describe attacks and hybrid activities from the Russian Federation against the Republic of Poland from June 2021 to the end of 2024. They are presented with a distinction between attacks against the integrity of the Polish border with Belarus, attacks carried out in Polish cyberspace, and disinformation attacks in the Polish information space. The thesis adopted in the article assumes that these actions were directly related to the war in Ukraine and were intentional interference by Russia and Belarus. The literature on the theory of hybrid warfare and the actions carried out by the Russian Federation and Belarus, perceived as part of hybrid warfare, was analysed. Furthermore, information related to hostile actions against the Republic of Poland, made available by Polish state institutions and teams set up to respond to computer incidents, was analysed.

Keywords

hybrid attacks, hybrid warfare, illegal migration, cyberspace, disinformation

Introduction

The geopolitical situation in Europe and worldwide has changed significantly in recent years, partly due to the increasingly overt imperialist ambitions of the Russian Federation. Current events (the war in Ukraine, hybrid attacks against Poland) are linked to the dynamic development of network technologies and the unprecedented impact of cyberspace on the functioning of states and societies. The development of tools offered by cyberspace is conducive to hybrid activities. Russia is gradually developing methods of conducting hostile activities against other states that remain below the threshold of war. These include irregular activities on the territory of the attacked state and activities involving attacks on its cyberspace and information sphere. The RF's goals are to weaken the state, cause disorganisation, undermine trust in the government and public institutions, and polarise society. An intensification of Russian hybrid attacks on Poland was observed with the outbreak of full-scale war in Ukraine. A sudden increase in the number of attacks on Polish cyberspace and the infosphere occurred with the migration crisis on the Polish-Belarusian border in 2021.

There are few publications in the literature on subject that compare various methods of hybrid attacks carried out by Russia against Poland. Given the pace of technological development and the impact of cyberspace and the infosphere (often used for hybrid attacks) on the functioning of the state and society, raising awareness of the subject of research seems fundamental.

The aim of this article[1] is to describe hybrid attacks and activities carried out by the RF between June 2021 and December 2024, which threatened the national security and cyberspace of the Republic of Poland. The thesis adopted in the article assumes that the attacks on the integrity of Poland's border carried out by the RF with the help of Belarus were related to the war in Ukraine and that the hybrid activities targeting Poland before and during the war were intentional, systematic interference by Russia and Belarus. In order to achieve the research objectives, methods such as analysis, synthesis and inference were used. The literature on the subject, reports prepared by Polish state institutions, as well as official information related to hostile actions against the Republic of Poland, made available by teams set up to respond to computer incidents, were analysed.

[1] The article is based on a thesis entitled *Hybrid attacks conducted and coordinated by the Russian Federation against the Republic of Poland in the context of the war in Ukraine*, written under the supervision of Jerzy Surma, Associate Professor at the Warsaw School of Economics (SGH). The thesis was defended in 2025 as part of postgraduate studies at SGH in Warsaw in cybersecurity management.

The theory of hybrid warfare

Hybrid warfare is a combination of warfare in the classical sense and other types of activities. These can occur independently, in parallel, or in quick succession. This pattern creates a wide range of possibilities for the attacker and, consequently, generates a large set of threats that the attacked party must contend with.

It should be noted that definitions of hybrid warfare differ between Western countries and the RF. The Russian theory was developed in opposition to the theory developed in the United States and Western Europe. The transfer of terminology to Russian soil is intended to emphasise its 'defensive' nature[2]. The most frequently cited Western theorist of hybrid warfare is Frank G. Hoffman from the United States, who notes that wars of this kind are not new, but are different each time[3]. According to him, this type of conflict is characterised by (…) *convergence* (…) *physical and psychological, the kinetic and nonkinetic, and combatants and noncombatants* (…), *military force and the interagency community, of states and nonstate actors, and of the capabilities they are armed with*[4]. The concept of convergence in the context of Hoffman's theory can be understood as the simultaneous occurrence and interpenetration of military and non-military elements in actions characteristic of hybrid warfare.

Olga Wasiuta and Sergiusz Wasiuta present other characteristics of hybrid warfare identified in American theory. These are:

- a combination of conventional warfare, irregular warfare, information warfare and cyber warfare,
- carrying out attacks using various methods and tools,
- using a combination of weapons and irregular warfare (guerrilla warfare, terrorism, crime),
- a complex, dynamic and flexible battlefield,
- rapid response and adaptation of participants to the dynamics of the conflict,
- use of modern technologies, actions and methods of mobilisation[5].

Valery Gerasimov is considered to be the leading Russian researcher of hybrid warfare theory. Although he does not use the term hybrid warfare in his deliberations,

---

[2] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku* (Eng. The anatomy of Russian information warfare. Operation Crimea – a case study), Warszawa 2014, p. 11.

[3] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, p. 8.

[4] F.G. Hoffman, *Hybrid Warfare and Challenges*, "Joint Force Quarterly" 2009, no. 52, p. 34.

[5] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie* (Eng. Russia's hybrid war against Ukraine), Kraków 2017, pp. 56–57.

he points to elements characteristic of this phenomenon, i.e. the need to use various political, economic and humanitarian instruments in modern conflicts as well as to combine them with the manipulation of the sentiments of the community inhabiting the adversary's territory. These actions are to be supported by non-military means such as information warfare and special forces operations. In the later stages of the conflict, the use of armed forces is permitted, but in the form of peacekeeping or humanitarian missions[6].

Andrzej Krzak also described other definitions of hybrid warfare found in Russian literature on the subject. According to one of the theories he cited, hybrid warfare is characterised by a multitude of different types of activities, conducted in a conventional (classical) and irregular manner, with the support of non-military segments. According to another Russian theory, hybrid warfare is characterised in international relations by comprehensive and methodical military, political, economic and social influence. In yet another Russian approach to hybrid warfare, this time in a military-political context, it is the use of various military and political tactics, as well as socio-economic destabilisation activities, on the territory of a potential adversary[7].

The RF is turning its hybrid warfare doctrine into real actions against other countries, and in connection with the outbreak of war in Ukraine, especially against Poland. Russian actions bearing the hallmarks of hybrid warfare against Poland can be divided into three key areas: the migration crisis, cyber attacks and disinformation campaigns. These actions are coordinated in terms of timing, the tools used, the entities carrying them out and their objectives. Despite Russia's efforts to shift the blame and responsibility for the attacks away from itself, Polish services and experts[8] have in many cases unequivocally attributed responsibility to Russia and Belarus as well as revealed their motivations and hostile intentions.

---

[6] A. Krzak, *Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict*, "Przegląd Bezpieczeństwa Wewnętrznego" 2018, no. 18, pp. 233–234.

[7] Ibid.

[8] See in more detail: *Hybrydowa agresja Białorusi na UE* (Eng. Belarus' hybrid aggression against the EU), Serwis Rzeczypospolitej Polskiej, 9 XI 2021, https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [accessed: 3 VI 2025]; M. Marek, *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO* (Eng. The Russian Federation's information war against Ukraine, Poland and NATO), Warszawa 2025.

Attacks on the integrity of the Polish border with Belarus

The migration crisis that Poland has been facing since 2021 is part of hybrid activities carried out by Russia with the help of Belarus. It is organised and managed by Alexander Lukashenka's regime, which uses migrants as a tool of political pressure. Attacks targeting the integrity of the Polish border, supported by hostile disinformation activities, are aimed at destabilising the security of Poland and the European Union, exerting political pressure, polarising and antagonising society, and creating opportunities for terrorists and other criminals to enter the EU[9].

Migrants, who are the subject of hybrid activities coordinated by the regimes of Belarus and Russia, attempt to cross the Polish border from Belarus illegally on a daily basis[10]. The Polish-Belarusian border is also part of the eastern border of the EU, the Schengen area and NATO. Lithuania was the first country affected by the migration crisis caused by Russia and Belarus, having to deal with it as early as July and August 2021. The data cited below indicate that at the same time as the migration crisis on the Polish-Belarusian border, the Border Guard recorded an increased number of attempts by third-country nationals to cross the Polish-Lithuanian border illegally[11].

According to the spokesperson for the special services coordinator, almost the entire state apparatus of the Belarusian regime is involved in organising activities related to the next stage of the hybrid war. The organisational scheme of the illegal migration route begins with special travel agencies issuing invitations to migrants and the Belarusian Ministry of Foreign Affairs issuing 'tourist' visas. The migrants then arrive in Belarus on Belarusian state airlines, which have created new connections specifically for this purpose. From the airports, migrants are transported to the border with Poland[12]. There, Belarusian services support the actions of migrants who attempt to cross the border by force, attack Polish border guards and destroy infrastructure[13].

---

[9] *Hybrydowy atak na Polskę* (Eng. Hybrid attack on Poland), Serwis Rzeczypospolitej Polskiej, 9 VIII 2022, https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [accessed: 30 V 2025].

[10] *Wojna Federacji Rosyjskiej z Zachodem* (Eng. The Russian Federation's war with the West), M. Banasik (sci. ed.), Warszawa 2022, p. 126.

[11] *Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa* (Eng. Security in Central and Eastern Europe. National and international perspectives), W. Śmiałek, Ł. Kominek, O. Balogh (sci. eds.), Poznań 2022, pp. 293–294.

[12] *Hybrydowa agresja Białorusi na UE…*

[13] *Bezpieczeństwo i zagrożenia hybrydowe* (Eng. Security and hybrid threats), M. Banasiak, A. Rogozińska (sci. eds.), Warszawa 2022, p. 22.

The escalation of aggressive actions by migrants on the Polish-Belarusian border took place on 8 November 2021. They attempted to force their way onto the Polish side, destroying the fence with the active support of the Belarusian services[14]. Another aggressive attempt at illegal mass border crossing by foreigners took place on 16 November at the border crossing in Kuźnica.

The tension at the border was further heightened by various provocations used by officers of the Belarusian regime. They verbally assaulted Polish officers and soldiers, threw stones at them, tried to stun them with firecrackers, and blind them with spotlights and lasers. Provocations involving Belarusian services firing shots at the border, uniformed persons with long weapons crossing it, and even aiming weapons at Polish soldiers and officers on duty at the border were commonplace[15].

In 2021, the Border Guard recorded 2869 foreigners – the citizens of third countries (from outside the EU) who were detained for crossing the state border in violation of regulations (hereinafter: pgpwp) or attempting pgpwp on the border with Belarus. This represents an increase of 1164% compared to 2020 (227 foreigners were recorded). Among those detained, the largest groups were citizens of Iraq, Afghanistan, Syria, Somalia, Russia and Belarus. During the same period, the Border Guard registered 320 third-country nationals apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. This represents an increase of 158% compared to 2020 (124 foreigners were recorded). Most of the apprehended persons came from Iraq and Syria[16].

In 2022, the Border Guard recorded 586 third-country nationals detained for pgpwp or attempted pgpwp on the section of the border with Belarus. This is a decrease of 80% compared to 2021. Most of the apprehended/detected persons were citizens of Iraq, Syria, Iran, Afghanistan and Belarus. During the same period, the Border Guard recorded 726 third-country nationals apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. This represents an increase of 127% compared to 2021. The largest number of persons apprehended/detected came from Iraq, Afghanistan, Iran and Syria[17].

In 2023, the Border Guard recorded 562 third-country nationals detained for pgpwp or attempted pgpwp on the border with Belarus, which represents

[14] *Wielowymiarowość konfliktów kulturowych we współczesnym świecie* (Eng. The multidimensionality of cultural conflicts in the modern world), W. Śmiałek (sci. ed.), Poznań 2024, p. 186.

[15] Ibid., p. 187.

[16] Statystyki SG – styczeń–grudzień 2021 (Eng. SG statistics – January–December 2021), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[17] Statystyki SG – styczeń–grudzień 2022 (Eng. SG statistics – January–December 2022), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

a 4% decrease compared to 2022. Most of the apprehended/detected persons came from Afghanistan, Belarus and Syria. On the border with Lithuania, the Border Guard recorded 727 third-country nationals apprehended/detected for pgpwp or attempted pgpwp. This represents an increase of 0.1% compared to 2022. The largest number of persons apprehended/detected came from Syria, Afghanistan, Iran and India[18].

In 2024, the Border Guard recorded 2582 third-country nationals detained for pgpwp or attempted pgpwp on the border with Belarus. This represents an increase of 359% compared to 2023. Most of the apprehended/detected persons were citizens of Ethiopia, Eritrea, Somalia, Syria, Yemen, Sudan and Afghanistan. During the same period, the Border Guard registered 432 third-country nationals who were apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. Compared to 2023, this is a decrease of 41%. The largest number of persons apprehended/detected came from Afghanistan, Moldova and Belarus[19].

It should be noted that the statistics cited refer to migrants who were actually apprehended/detected. The number of attempts to cross the Polish-Belarusian and Polish-Lithuanian borders is significantly higher. According to the Podlaski Border Guard Regional Unit and the Nadbużański Border Guard Regional Unit, in 2021 alone, 39 697 attempts to cross the border illegally outside border crossings were recorded on the border with Belarus. This is over 300 times more attempts than in 2020[20]. In 2024, according to the Podlaski Border Guard Regional Unit, nearly 30 000 attempts to illegally cross the Polish-Belarusian border were recorded. The migrants came from 52 countries, mainly Ethiopia, Eritrea and Somalia. A total of 346 organisers of illegal border crossings and their accomplices were also detained, including 316 people on the border with Belarus and 30 on the border with Lithuania. The majority of those detained were citizens of Ukraine, Poland and Belarus[21].

---

[18] Statystyki SG – styczeń–grudzień 2023 (Eng. SG statistics – January–December 2023), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[19] Statystyki SG – styczeń–grudzień 2024 (Eng. SG statistics – January–December 2024), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[20] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią* (Eng. Illegal border crossings from Belarus), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [accessed: 3 VI 2025].

[21] K. Zdanowicz, *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie* (Eng. Illegal migration in the Podlaski Border Guard Regional Unit – summary), 21 I 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [accessed: 3 VI 2025].

The migration crisis on the Polish-Belarusian border is an example of deliberate and organised hybrid actions in which Russia, with the help of the Belarusian regime, is using migrants as a tool for political blackmail. The state apparatus of Lukashenka's regime not only organises and controls the migration route, but also conducts coordinated provocative and disinformation activities aimed at blaming Poland for the crisis and causing divisions within Polish society and on the international stage. Such operations demonstrate how Russia exploits contemporary threats in its hybrid activities to destabilise security and order in Poland and Europe.

Attacks in cyberspace

The intensity of Russian cyberattacks targeting Poland increased significantly just before and after Russia's invasion of Ukraine, as confirmed by the statistics presented below. The attacks are part of a broader hybrid strategy by the Kremlin aimed at destabilising the situation in Poland, putting pressure on the Polish authorities and causing chaos and uncertainty among the population. Pro-Russian hacker groups target state institutions as well as the private sector, the media and citizens. They use advanced methods such as distributed denial of service (DDoS) attacks, ransomware, phishing and impersonating official government websites. Some of these activities are a direct response to Poland's support for Ukraine and to political decisions by the Polish authorities that are unfavourable to the RF. In modern conflicts, cyberspace has become an important battlefield, and its effective protection requires constant monitoring and rapid response.

APT (advanced persistent threats) attacks carried out by groups of the same name are particularly dangerous. These are advanced, long-term attacks characteristic of this type of cybercriminal groups operating on behalf of governments. APT groups attack to obtain strategic information, conduct cyber espionage, disrupt the functioning of the attacked country, and influence its politics and economy. Financial support from governments provides cybercriminals with access to advanced resources and technologies that facilitate long-term and complex cyberattacks[22]. Pro-Russian groups constitute a significant segment of this environment[23].

[22] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025* (Eng. The cyber threat landscape in the Polish financial sector in 2025), https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf, p. 6 [accessed: 10 VI 2025].

[23] Ibid., p. 14.

According to information provided by the Government Plenipotentiary for the Security of Information Space of the Republic of Poland, incidents in cyberspace are typical retaliatory actions by Russia in response to actions taken by other countries that are unfavourable to the RF[24]. Hacker groups using DDoS attacks, ransomware, phishing, and fake websites impersonating existing services are linked to the Kremlin. Entities in strategic sectors, such as energy and defence, are particularly at risk. The attacks are consistent with the objectives of hybrid operations, which are designed to cause destabilisation, intimidation and chaos. Every cyberattack has specific consequences – political, financial and social[25].

The *Act of 5 July 2018 on the national cybersecurity system* established three computer security incident response teams in Poland, namely CSIRT GOV, CSIRT NASK and CSIRT MON. Due to the subject matter of the reports on the state of Polish cybersecurity published by these teams, the author of the article analysed the reports of CSIRT GOV and CERT Polska (operating within the structure of CSIRT NASK) for the years 2021–2024 as well as the reports for the years 2021–2022 prepared by the CSIRT KNF, which is a computer security incident response team in the Polish financial sector, were also analysed[26].

Since 2010, the CSIRT GOV team (led by the Head of the Internal Security Agency) has been publishing annual reports on the state of cyber security in Poland[27]. The largest increase in the number of reports of potential incidents, and consequently the increase in the number of confirmed incidents, was recorded in the third and fourth quarters of 2021. The largest number of reports concerned, in order: critical infrastructure, institutions, offices, ministries, services and the military, and other sectors[28]. In its 2021 report, the CSIRT GOV team reported a more than threefold increase in the number of reports of potential ICT security incidents compared to the previous year. The activity of sponsored APT groups was also noted, particularly in the context of critical infrastructure and public

[24] *Rosyjskie cyberataki* (Eng. Russian cyberattacks), Serwis Rzeczypospolitej Polskiej, 29 XII 2022, https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [accessed: 5 VI 2025].

[25] Ibid.

[26] *Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego* (Eng. Education Centre for Financial Market Security), Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [accessed: 10 VI 2025].

[27] Raporty o stanie bezpieczeństwa cyberprzestrzeni RP (Eng. Reports on the state of cybersecurity in Poland), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [accessed: 5 VI 2025].

[28] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* (Eng. Report on the state of cyberspace security in Poland in 2021), Warszawa 2022, p. 14.

administration[29]. In turn, the CERT Polska team reported an 182% increase in the number of incidents handled in 2021 compared to the previous year[30].

In its 2021 report analysing cyber security threats to the financial market in Poland, CSIRT KNF also noted that the largest increase in the number of reported dangerous websites occurred in the third and fourth quarters of 2021[31].

On the gov.pl website, in the section on cybersecurity, from 2022 onwards, more and more articles began to appear on the threats posed by fraud and disinformation, and in 2023, articles began to be published that explicitly mentioned Russian cyberattacks[32].

The CSIRT GOV report for 2022 devoted an entire chapter for the first time to analysing the activities of APT groups whose activity in Polish cyberspace was related to the war in Ukraine[33]. It highlighted previously unreported threats and activities on such a large scale, including an increasing number of social engineering campaigns and DDoS attacks, which were primarily targeted at public services provided on the internet. The CSIRT GOV team classified the largest number of incidents in 2022 in the following categories: vulnerability, social engineering and unavailability. The vulnerability category recorded the highest number of incidents due to the introduction of the CHARLIE-CRP alert level in February 2022, which resulted in an increase in the number of identified events that could have compromised the security of Poland's ICT infrastructure.

The social engineering campaigns recorded by CSIRT GOV in 2022 included phishing campaigns, website spoofing and impersonation (often of government administration websites or government systems). Their intensity remained high, and the targets were mass recipients and representatives of selected entities. These activities were primarily aimed at gaining unauthorised access to the resources of the attacked entity by obtaining authentication data. In addition, the attacks were

[29] Ibid., p. 64.

[30] CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2021. The security landscape of the Polish internet), Warszawa 2022, p. 12.

[31] CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków* (Eng. Summary of the Year at CSIRT KNF 2021. Description of selected attacks), https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [accessed: 8 VI 2025].

[32] Baza wiedzy – cyberbezpieczeństwo (Eng. Knowledge base – cybersecurity), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [accessed: 8 VI 2025].

[33] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku* (Eng. Report on the state of cyberspace security in Poland in 2022), Warszawa 2023, p. 56.

aimed at distributing malware and gaining access to IT systems in order to carry out further cybercriminal activities[34].

In the category of unavailability, a significant increase in the number of DDoS attacks (826 incidents, compared to 310 in the previous year) targeting Polish public administration websites and critical infrastructure has been recorded since February 2022. These attacks were carried out by hacktivist groups, including Killnet, NoName057(16), the People's Cyber Army. The CSIRT GOV team indicated that in 2022, the component most vulnerable to attacks in cyberspace was Poland's critical infrastructure[35]. It also confirmed that Poland's actions on behalf of Ukraine in the war with Russia have significantly increased the level of threat in Polish cyberspace.

In its annual report on activities in 2022, the CERT Polska team devotes an entire chapter to the impact of the war in Ukraine on Polish cybersecurity. In retrospect, it has been confirmed that Russia's military operations are supported by the activities of hackers and hacktivist groups, as well as the spread of disinformation. Russia had already been conducting these intensified activities in cyberspace in the months preceding the conventional war in Ukraine. The events in Polish cyberspace that CERT Polska, like CSIRT GOV, directly links to the war in Ukraine include massive DDoS attacks on government websites and the websites of important economic entities, as well as phishing campaigns using the war theme and appearing mainly on social media. The report states that the attacks are intended to destabilise the internal situation in countries that support Ukraine. Examples of DDoS attacks carried out by Russian hacktivists are given. Their frequent ineffectiveness and use primarily to spread propaganda and disinformation are highlighted. It also lists campaigns that use the appearance of well-known websites and government websites, as well as the theme of war. The frauds included, among others, fake Facebook login panels, fake fundraisers, Nigerian scams, and fake investments[36].

In its 2022 report, CSIRT KNF also devoted a chapter to threats and recommendations regarding DDoS attacks and hacktivist activities in the context of the war in Ukraine. The team reported that DDoS attacks were the most numerous in 2022. They had a certain impact on the financial sector in Poland. The high availability, ease of use, relatively low cost and effectiveness of this type of criminal method were emphasised. The possibility of almost anyone carrying

[34] Ibid., p. 30.

[35] Ibid., pp. 13–17.

[36] CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2022. The security landscape of the Polish internet), Warszawa 2023, pp. 93–100.

out (planning and directing attacks) or participating (sharing their resources) in an attack was also indicated. The CSIRT GOV team also noted that the targets of pro-Russian cybercriminal groups depend on the political actions of countries which, in the opinion of hacktivists, are hostile to Russia or favourable to Ukraine[37].

The CSIRT GOV report for 2023 includes information that Poland continued to face heightened cyber threats related to the armed conflict in Ukraine this year. Based on an assessment of APT group activity in 2023, it was concluded that these attacks were largely a continuation of those recorded in 2022. The main targets of the attacks remained state institutions and critical infrastructure, especially in the energy and transport sectors. Two types of criminal activity dominated: DDoS attacks – used by pro-Russian groups to disrupt websites and public services, as well as social engineering campaigns – aimed at phishing for data, infecting systems with malware and destabilising political processes. These activities were intensified in connection with parliamentary elections in Poland. The report shows that in 2023, Poland was a key target of Russian hybrid operations combining cyberattacks with information warfare[38].

In its 2023 report, the CERT Polska team presented an analysis of APT group activities. Since the start of the war in Ukraine, there has been a significant increase in their activity, which in 2023 was primarily aimed at disrupting the continuity of operations of Polish entities in the transport and logistics sector[39]. It has been noted that these groups are linked to the RF and/or Belarus[40].

In its 2024 activity report, the CSIRT GOV team reported that Poland continued to experience an elevated level of cyber threats, including social engineering, attempts to exploit vulnerabilities, DDoS attacks, and the publication of leaked data, also carried out by sponsored hacktivist groups. In 2024, there were events of particular importance from a security perspective, namely local elections, European Parliament elections, and the 33rd Summer Olympic Games in Paris. The incidents of 2024 described in the report confirmed that cybercriminals and state actors are interested in any entities whose attack would also affect national security. The report also stated that cyberattacks are a hybrid threat and an element of modern conflicts in which hostile actions are conducted below the threshold

[37] CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022* (Eng. Cyber threats in the financial sector 2022), https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [accessed: 8 VI 2025].

[38] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku* (Eng. Report on the state of cyberspace security in Poland in 2023), Warszawa 2024, pp. 4–6.

[39] CERT Polska, *Raport roczny z działalności CERT Polska 2023* (Eng. Annual report on the activities of CERT Polska 2023), Warszawa 2024, p. 34.

[40] Ibid.

of war[41]. Particular attention was paid to the threat of attacks on supply chains, which were defined as attacks targeting a trusted external service provider essential to that chain. This has broadened the potential area of attack on key infrastructure sectors in Poland[42]. It has been confirmed that attacks by APT groups, motivated by ideology, politics and finance, continue to pose the greatest threat to government administration and critical infrastructure. In 2024, these groups focused on continuing their activities from 2022–2023, and as before, this activity was supported by propaganda campaigns designed to demonstrate the effectiveness and potential of cyberattacks. It was noted that 2024 was characterised by an increase in the volume of cybercriminal groups, which was caused by a growth in the number of financially motivated groups and increasing access to AI-assisted tools. The main actors mentioned were APT28 group (also known as Fancy Bear), followed by groups APT29 (also known as Cozy Bear), UNC1151 (also known as Ghostwriter), APT15, and DaVinci[43].

In its 2024 activity report, the CERT Polska team presented an observation similar to that of the CSIRT GOV team regarding the activity of APT groups, mainly associated with the RF and Belarus. It reported that these groups were pursuing intelligence and propaganda objectives, and that most of these activities consisted of attempts to obtain authentication data for e-mail accounts, distribution of malware, and attacks on industrial systems. It also drew attention to the practice of attacking not only public institutions and large enterprises, but also smaller entities that are links in supply chains. The CERT Polska team identified UNC1151, APT28 and APT29 as the most active of the observed APT groups[44].

It should be noted that all teams presented similar conclusions in their analyses regarding trends, main types of threats and sectors most vulnerable to cyber attacks in Poland. These are:

- a significant increase in the number of reports and confirmed incidents on the network since 2021 compared to previous years, noticeable several months before Russia's aggression against Ukraine in 2022,
- intensified and dynamic activity of cybercriminal groups linked to the RF and Belarus,

[41] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku* (Eng. Report on the state of cyberspace security in Poland in 2024), Warszawa 2025, pp. 5–6.

[42] Ibid., p. 113.

[43] Ibid., pp. 54–56.

[44] CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual Report on the activities of CERT Polska 2024. The security landscape of the Polish internet), Warszawa 2025, p. 33.

- the most common types of attacks were DDoS attacks and social engineering campaigns,
- one of the intentions of the attacks was to cause widespread disruption to the functioning of the state,
- the targets of cyberattacks were primarily government administration, public institutions and critical infrastructure entities,
- a characteristic activity of APT groups is the promotion of their activities on social media,
- an increase in the number of attacks targeting smaller entities that are links in supply chains.

In May 2025, the American equivalent of Polish CSIRT teams, i.e. the Cybersecurity and Infrastructure Security Agency, published a report on the specific threat currently faced by Eastern European entities, including Polish ones, which are links in supply chains. This threat is posed by the APT28 group, which has been mentioned repeatedly by Polish teams. As emphasised by the American source, it is identified with the Russian Main Intelligence Directorate (GRU) and the Russian military unit 26165[45].

Cyberspace has become a key arena for hybrid activities, including both technical attacks and accompanying information campaigns aimed at destabilising the state and exerting social and political pressure. Russian cyberattacks are part of a hybrid strategy, often responding to actions unfavourable to Russia and forming an integral part of the war with Ukraine.

Disinformation in the Polish information space

Propaganda and disinformation activities on the part of Russia have been observed since at least the days of the Soviet Union, but President Vladimir Putin's rule has made Russia one of the most active actors in the information sphere, including cyberspace, on the international political scene[46]. The comprehensive activities carried out by the RF are referred to as information warfare and include coordinated propaganda and disinformation campaigns in cyberspace[47]. Information warfare is seen as one of the most important elements of Russia's international competition strategy,

[45] *Russian GRU Targeting Western Logistics Entities and Technology Companies*, CISA, 21 V 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [accessed: 10 VI 2025].

[46] *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski* (Eng. Information as a factor determining security. The Russian context), M. Banasik (sci. ed.), Warszawa 2021, p. 7.

[47] Ibid.

enabling it to achieve its political goals. Cyberspace, on the other hand, enables the RF to conduct activities within the framework of this information warfare[48].

Jerzy Surma emphasises the special role played by social media in information warfare. He draws attention to the consequences for national security of the easy and cheap possibility of publishing and exchanging information. These features of social media make them both a place and a tool for waging information wars, the aim of which is to manage information in such a way as to influence the behaviour of society and shape it according to the will of the attacker.

Information warfare is conducted in an organised manner, using both overt activities, such as propaganda and manipulation of information, and covert activities, including the fabrication of information for the purpose of disinformation. He cited the RF as an example of a state that systematically conducts activities that bear the hallmarks of information warfare as part of hybrid warfare[49].

The following objectives can be attributed to hostile actions of this type:

- disruption of the value system (breakdown of social bonds, isolation of individuals or groups, distrust of public institutions),
- attacks on important facilities (critical infrastructure, places of worship and international symbols),
- creation and exploitation of opinion leaders (shaping perceptions by influential individuals and/or those with the ability to influence large audiences)[50].

The literature on the subject emphasises the multifaceted nature of Russian campaigns in the information sphere, as well as their strategic importance. The information war they wage involves processes that target the cognitive sphere of human beings and shape people's attitudes in line with the attacker's expectations[51].

Since 24 February 2022, Russians have been undermining the image of the Republic of Poland both in their own and external infosphere. This activity included, among other things, developing Polish-language channels on the Telegram platform (where hacktivist groups shared, for example, false information about attacks on Polish facilities for propaganda purposes[52]), the activities of so-called

---

48 Ibid., p. 8.

49 J. Surma, *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo* (Eng. The digitisation of life in the era of Big Data. People. Business. The State), Warszawa 2017, p. 90.

50 *Odporność państwa, społeczeństwa i gospodarki na zagrożenia* (Eng. Resilience of the state, society and economy to threats), M. Piotrowska-Trybull, K. Górska-Rożej (sci. eds.), Warszawa 2024, pp. 331–332.

51 *Informacja czynnikiem warunkującym bezpieczeństwo*…, p. 50.

52 CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, pp. 25–28.

troll and bot accounts, and the noticeable activity of groups involved in spreading Russian narrative. Disinformation materials and narratives present on Russian channels on Telegram, including Polish-language ones, were then shared on other channels in the Polish segment of social networks. The newly formed Polish Anti-War Movement and campaigns with political overtones, such as 'Stop the Ukrainisation of Poland' and 'This is not our war', also contributed to the achievement of Russian information objectives. In addition, the Belarusian side exposed Polish citizens who had emigrated to Belarus and Russia and started pro-Russian disinformation activities. They spread Russian propaganda and disinformation on social media[53].

The Telegram platform was founded by Russian citizens in 2013. In 2021, its Polish-language segment expanded. Two events in 2021, for which Russia is likely responsible, contributed to its popularity in Poland.

The first was the publication on Telegram of data obtained after an attack on the e-mail accounts of Polish politicians[54]. One of them was Minister Michał Dworczyk. Information from his e-mail account began appearing on the Telegram channel on 4 June. Experts say that Russia or Belarus, which cooperates with it, is responsible for these actions[55]. The attack is part of a campaign called 'Ghostwriter,' which aims to obtain data and sensitive information for Russian special services and spread Russian disinformation[56]. As part of this campaign, webmail accounts and social media accounts belonging to public figures from Central and Eastern European countries, mainly Poland, are being attacked. Criminals are attempting to take over information resources for the purposes of Russian disinformation[57].

The second event was the migration crisis on the Polish-Belarusian border in Poland in 2021. Recordings and propaganda messages were disseminated to the Polish infosphere via Telegram (and then other social media platforms and the media)[58]. The popularisation of this tool in Poland allowed the Russian-Belarusian narrative to be disseminated[59].

---

53 M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, pp. 116–117.

54 Ibid., p. 119.

55 *Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki* (Eng. Email scandal. The prosecutor's office has brought charges, but these are just pawns), CyberDefence24, 16 VIII 2024, https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [accessed: 11 VI 2025].

56 *Rozwój technik ataku grupy UNC1151/Ghostwriter* (Eng. Development of attack techniques by the UNC1151/Ghostwriter group), Cert.pl, 19 VII 2022, https://cert.pl/posts/2022/07/techniki-unc1151/ [accessed: 23 VI 2025].

57 *Rosyjskie cyberataki*…

58 M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, p. 119.

59 Ibid., p. 123.

According to Michał Marek, the head of the External Threat Analysis Team at NASK, Russian disinformation focuses on three main narratives: pushing Poland towards war with Russia[60], NATO and the US being responsible for the outbreak of war in Ukraine[61], and Poland being subjected to so-called Ukrainisation[62]. A year after the outbreak of war in Ukraine, the spokesperson for the Polish Ministry of Foreign Affairs posted a comment in which he wrote about an unprecedented increase in the scale of Russian disinformation activity. He noted that Russia was conducting a large-scale disinformation campaign. Its goals were to undermine the values of a free and democratic world, cause chaos, incite hatred, and destabilise the international order. The spokesman pointed out that despite new forms of false narratives, the basic methods of manipulation remain the same. The goal is also the same – to stir up tensions and unrest in the societies under attack. He warned against providing audiences with contradictory information designed to make people unable to distinguish between truth and falsehood. This would allow even the most absurd versions of events to be believed[63].

In January 2025, a report was published by the disinformation team of the Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024. It drew attention to the theory of the Russian information warfare strategy, which captures the essence and nature of activities carried out in the Polish infosphere. Content falsified to varying degrees appears in traditional media, social media and online platforms. The report pointed to the Russian news agency Sputnik, which had a Polish version of its website, and the content published on it was shared by fabricated information environments and then by social media accounts[64]. It was also found that with the outbreak of war in Ukraine in 2022, Russian propaganda began to promote a narrative about the defencelessness of Western countries (including Poland) and the weakness of their armies and authorities. The aim was

[60] Ibid., p. 131.

[61] Ibid., p. 140.

[62] Ibid., p. 146.

[63] *O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ* (Eng. On Russian disinformation: one year since the full-scale invasion of Ukraine – commentary by the Spokesperson for the Ministry of Foreign Affairs), Serwis Rzeczypospolitej Polskiej, 23 II 2023, https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [accessed: 14 VI 2025].

[64] Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024 (Eng. The Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024), *Raport Zespołu ds. Dezinformacji*, Warszawa 2025, p. 5.

to convince the audience that the state did not provide them with security and that it was not worth defending in the event of a threat[65]. The experts who compiled this report drew attention to the objectives of Russian disinformation and propaganda, namely the polarisation of society and the erosion of trust in the state, as well as in science, the media and fellow citizens[66].

The scale of Russian disinformation activities is also reflected in the situation reports published on the gov.pl website. In 2023, 31 reports were published describing disinformation activities carried out by Russia and Belarus against Poland. They concerned false accusations against Poland, including brutal treatment of migrants at the border and plans for aggression against Ukraine. These reports emphasised that these activities were aimed at causing social divisions and undermining trust in Polish authorities and institutions, and were also part of an information war aimed at destabilising Poland and the region[67].

The scale of disinformation in 2023 was also revealed by the Government Centre for Security (RCB). As part of the DisInfo Radar project, the RCB published 57 infographics presenting topics covered by Russian and Belarusian disinformation. They included information on false Russian persuasion and narratives, untrue theses, manipulations, and websites observed in 2023[68]. Warnings about the disinformation campaign were issued in particular in October 2023, when parliamentary elections were held in Poland. The threats to the security of the electoral process were listed, and information was provided about an ongoing information campaign suggesting that a coup d'état was being prepared in Poland and that the army would be used against the population[69].

Polish computer incident response teams have also highlighted Russian disinformation campaigns in their annual reports since 2021. In its 2021 activity report, the CSIRT GOV team reported on the activities of APT groups that were attributed with spreading disinformation. One example given was operation 'Ghostwriter', which is attributed to the UNC1151 group[70].

---

65 Ibid., p. 19.

66 Ibid., p. 20.

67 Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne (Eng. Disinformation against Poland, situation reports, Special services), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [accessed: 14 VI 2025].

68 Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [accessed: 14 VI 2025].

69 Ibid.

70 CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*…, p. 27.

In its 2022 activity report, the CSIRT GOV team reported on the identification of incidents that indicated a context of disinformation. An example given was an attack in September 2022 involving the posting of anti-Ukrainian content and propaganda graphics on the website of the Office of Rail Transport. The CSIRT GOV team also reported the identification of a practice involving the registration of websites impersonating official government domains, which indicated the possibility of their use for social engineering attacks, including disinformation[71]. In its report on activities in 2022, the CERT Polska team reported on the disinformation activities of pro-Russian cybercriminal groups. It was found that a characteristic feature of these groups is the spread of disinformation[72].

This phenomenon was also described in the CSIRT GOV activity report for 2023. The team drew attention to the parliamentary elections, which prompted an intensification of activities by hacktivist groups conducting disinformation attacks using various means of communication, including e-mails and text messages. It attributed responsibility for these attacks to, among others, the UNC1151 group[73].

Similar observations were described by the CERT Polska team in its 2023 activity report. It also identified UNC1151 as the most active APT group and pointed to its links with the Belarusian government and Russian special services. The targets were mainly from the political and military circles, but there were also people who could have indirect links to Russia or Belarus, such as lawyers, sworn Russian translators, Orthodox priests, NGO employees and journalists. The motivations for these actions were identified as the theft of information for intelligence purposes and the conduct of disinformation campaigns. In 2023, the team observed disinformation campaigns related to the terrorist threat in Poland, the collection of information about refugees, military recruitment, and the lack of potassium iodide in pharmacies. In the assessment of CERT Polska, the campaigns were aimed at spreading uncertainty and divisions in society. It was noted that after the parliamentary elections, the activity of the UNC1151 group decreased significantly[74].

In its 2024 activity report, the CSIRT GOV team once again drew attention to local government elections and European Parliament elections, which were vulnerable to hostile disinformation operations conducted in cyberspace. Another event associated with a disinformation incident was the 33rd Summer Olympic Games in Paris. In August 2024, the pro-Russian hacktivist groups Beregini and Zarya, acting

[71] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, p. 31.

[72] CERT Polska, *Raport roczny z działalności CERT Polska 2022*…, p. 93.

[73] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*…, p. 6.

[74] CERT Polska, *Raport roczny z działalności CERT Polska 2023*…, p. 93.

in concert, stole documents from the IT systems of the Polish Anti-Doping Agency and published them in a modified form in order to discredit Polish athletes[75]. As in previous years, the team observed the activities of the UNC1151 group, which this time was conducting a campaign targeting users of the most popular email providers – Gmail, Interia, Wirtualna Polska, Onet, and o2. The criminals obtained data from mailboxes by impersonating mail administrators and persuading users to log in using a fake login panel[76]. Another serious incident attributed to sponsored cybercriminal groups was the attack on the Polish Press Agency in May 2024. False information about military mobilisation in Poland was posted twice on its official website[77].

In its 2024 activity report, the CERT Polska team, like the CSIRT GOV team, discussed a disinformation campaign targeting the Polish Anti-Doping Agency. In addition, it described a disinformation campaign related to the Steadfast Defender 2024 and Dragon-24 military exercises, concerning an allegedly drunk driver of a military truck. The team emphasised that the disinformation content that appeared in the Polish infosphere in 2024 referred to many socio-political events[78].

Summary

An analysis of information concerning the migration crisis and attacks in cyberspace and the information sphere in Poland allows us to conclude that representatives of Polish government bodies, uniformed services, including special services, as well as specialists involved in detecting and preventing cyber attacks, have no doubt about the specific nature and character of Russian actions directed against Poland. They conclude that Russia's aggressive actions are part of a hybrid war closely linked to the attack on Ukraine. The Russian strategy is characterised by the gradual, planned weakening of its adversary by conducting activities on many levels of the state's functioning. It is precisely such activities that are supposed to be most effective.

The data analysis contained in this article proves the validity of the thesis. The attacks on the integrity of the Republic of Poland carried out by the RF were directly related to the war in Ukraine. Research of source materials conducted using analysis, synthesis and inference allows us to conclude that Russia, in cooperation with Belarus, is responsible for the hybrid attacks carried out against Poland since 2021.

---

[75] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*…, p. 6.

[76] Ibid., p. 69.

[77] Ibid., p. 78.

[78] CERT Polska, *Raport roczny 2024 z działalności CERT Polska*…, p. 35.

Russian hybrid activities are characterised by the blurring of the line between military and civilian areas. Russia uses civilians to achieve its goals. Russian-Belarusian hybrid attacks target areas that may be important for Poland's security. Coordinated attacks in multiple areas simultaneously are intended to increase their severity. It is therefore essential to conduct crisis response exercises covering not only the military sphere but also the civilian sphere, as well as joint cross-sectoral exercises.

Bibliography

Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa (Eng. Security in Central and Eastern Europe. National and international perspectives), W. Śmiałek, Ł. Kominek, O. Balogh (sci. eds.), Poznań 2022.

Bezpieczeństwo i zagrożenia hybrydowe (Eng. Security and hybrid threats), M. Banasik, A. Rogozińska (sci. eds.), Warszawa 2022.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku* (Eng. The anatomy of Russian information warfare. Operation Crimea – a case study), Warszawa 2014.

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid Warfare and Challenges*, "Joint Force Quarterly" 2009, no. 52, pp. 34–39.

Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski (Eng. Information as a factor determining security. The Russian context), M. Banasik (sci. ed.), Warszawa 2021.

Krzak A., *Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict*, "Przegląd Bezpieczeństwa Wewnętrznego" 2018, no. 18, pp. 221–243.

Marek M., *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO* (Eng. The Russian Federation's information war against Ukraine, Poland and NATO), Warszawa 2025.

Odporność państwa, społeczeństwa i gospodarki na zagrożenia (Eng. Resilience of the state, society and economy to threats), M. Piotrowska-Trybull, K. Górska-Rożej (sci. eds.), Warszawa 2024.

Surma J., *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo* (Eng. The digitisation of life in the era of Big Data. People. Business. The State), Warszawa 2017.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie* (Eng. Russia's hybrid war against Ukraine), Kraków 2017.

Wielowymiarowość konfliktów kulturowych we współczesnym świecie (Eng. The multidimensionality of cultural conflicts in the contemporary world), W. Śmiałek (sci. ed.), Poznań 2024.

Wojna Federacji Rosyjskiej z Zachodem (Eng. The Russian Federation's war with the West), M. Banasik (sci. ed.), Warszawa 2022.

Internet sources

Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki (Eng. Email scandal. The prosecutor's office has brought charges, but these are just pawns), CyberDefence24, 16 VIII 2024, https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [accessed: 11 VI 2025].

Baza wiedzy – cyberbezpieczeństwo (Eng. Knowledge base – cybersecurity), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [accessed: 8 VI 2025].

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (Eng. Education Centre for Financial Market Security), Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [accessed: 10 VI 2025].

Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne (Eng. Disinformation against Poland, situation reports, Special services), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [accessed: 14 VI 2025].

Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [accessed: 14 VI 2025].

Hybrydowa agresja Białorusi na UE (Eng. Belarus' hybrid aggression against the EU), Serwis Rzeczypospolitej Polskiej, 9 XI 2021, https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [accessed: 3 VI 2025].

Hybrydowy atak na Polskę (Eng. Hybrid attack on Poland), Serwis Rzeczypospolitej Polskiej, 9 VIII 2022, https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [accessed: 30 V 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025 (Eng. The cyber threat landscape in the Polish financial sector in 2025), https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 10 VI 2025].

O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ (Eng. On Russian disinformation: one year since the full-scale invasion of Ukraine – commentary by the Spokesperson for the Ministry of Foreign Affairs), Serwis Rzeczypospolitej Polskiej, 23 II 2023, https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [accessed: 14 VI 2025].

Raporty o stanie bezpieczeństwa cyberprzestrzeni RP (Eng. Reports on the state of cybersecurity in Poland), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [accessed: 5 VI 2025].

Rosyjskie cyberataki (Eng. Russian cyberattacks), Serwis Rzeczypospolitej Polskiej, 29 XII 2022, https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [accessed: 11 VI 2025].

Rozwój technik ataku grupy UNC1151/Ghostwriter (Eng. Development of attack techniques by the UNC1151/Ghostwriter group), Cert.pl, 19 VII 2022, https://cert.pl/posts/2022/07/techniki-unc1151/ [accessed: 23 VI 2025].

Russian GRU Targeting Western Logistics Entities and Technology Companies, CISA, 21 V 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [accessed: 10 VI 2025].

Statystyki SG – styczeń–grudzień 2021 (Eng. SG statistics – January–December 2021), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2022 (Eng. SG statistics – January–December 2022), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2023 (Eng. SG statistics – January–December 2023), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2024 (Eng. SG statistics – January–December 2024), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią* (Eng. Illegal border crossings from Belarus), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,-Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [accessed: 3 VI 2025].

Zdanowicz K., *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie* (Eng. Illegal migration in the Podlaski Border Guard Regional Unit – summary), 21 I 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [accessed: 3 VI 2025].

Legal acts

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws of 2026, item 20).

Other documents

CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual Report on the activities of CERT Polska 2024. The security landscape of the Polish internet), Warszawa 2025.

CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2021. The security landscape of the Polish internet), Warszawa 2022.

CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2022. The security landscape of the Polish internet), Warszawa 2023.

CERT Polska, *Raport roczny z działalności CERT Polska 2023* (Eng. Annual report on the activities of CERT Polska 2023), Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* (Eng. Report on the state of cyberspace security in Poland in 2021), Warszawa 2022.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku* (Eng. Report on the state of cyberspace security in Poland in 2022), Warszawa 2023.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku* (Eng. Report on the state of cyberspace security in Poland in 2023), Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku* (Eng. Report on the state of cyberspace security in Poland in 2024), Warszawa 2025.

CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022* (Eng. Cyber threats in the financial sector 2022), https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [accessed: 8 VI 2025].

CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków* (Eng. Summary of the Year at CSIRT KNF 2021. Description of selected attacks), https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [accessed: 8 VI 2025].

Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024 (Eng. The Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024), *Raport Zespołu ds. Dezinformacji*, Warszawa 2025.

Agata Rytel

Graduate of postgraduate studies in cybersecurity management at the Warsaw School of Economics.

Contact: agatakalota0@gmail.com

Internal Security Review
2026, no. 34, pp. 389–412

https://doi.org/10.4467/20801335PBW.26.018.23380

ARTICLE

Support for Polish uniformed services protecting the Polish-Belarusian border as a response to the repercussions of the operation 'Sluice' in 2021

NORBERT ŁUCARZ

Jagiellonian University

https://orcid.org/0009-0005-2615-9727

Abstract

The aim of the article is to describe the support for Polish uniformed services protecting the Polish-Belarusian border, which, as a result of the operation 'Sluice' in 2021 have undoubtedly become the object of discredit, as well as the target of physical and psychological aggression. The article discusses the migrants instrumentalisation practice in the policies of Belarus and Russia, then presents selected uniformed services involved in protecting the Polish-Belarusian border. The forms of aggression towards the Polish uniformed services during the operation 'Sluice' and the nationwide social campaign 'United behind the Polish uniform' were also presented.

Keywords

Polish-Belarusian border, migration crisis, social campaign 'United behind the Polish uniform', instrumentalisation of migrants

Introduction

The migration crisis on the borders of Belarus with Lithuania, Latvia and Poland was carefully planned. Smuggling mafias were responsible for transporting migrants to the border areas, convincing potential customers of the effectiveness and safety of their services[1]. The migrants were mainly citizens of Middle Eastern and South Asian countries: Afghanistan, Iraq, Iran, Pakistan, Syria and Libya[2]. For a certain amount (calculated in thousands of dollars), migrants were transported to Minsk, provided with accommodation, and transported to the border of European Union Member States. The practice was carried out in the same way as tourist trips. It was closely monitored by the authorities from Belarus[3]. The EU has imposed sanctions on many entities involved in migrant smuggling. This group includes: Belarusian Belavia Airlines, Syrian Cham Wings Airlines, Belarusian travel agencies – CentrKurort and Oskartour, Minsk and Planeta hotels as well as the Turkish company Vip Grup[4]. The locations where migrants are smuggled into Europe coincide with the Eastern European migration route, which covers over 6000 km and runs along the borders of EU Member States – Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania and Bulgaria[5]. Among the Belarusian services involved in triggering the migration crisis were the State Security Committee of the Republic of Belarus (Russian: Комитет государственной безопасности Республики Беларусь, KGB), the State Border Committee of the Republic of Belarus (Russian: Государственный пограничный комитет Республики Беларусь) as well as the Special Service for Active Operations (Russian: Отдельная

[1] D. Niedźwiedzki, *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego* (Eng. Humanitarian crisis on the Polish-Belarusian border. Analysis of the phenomenon from the perspective of social order), "Politeja" 2024, vol. 21, no. 1, pp. 58–59. https://doi.org/10.12797/Politeja.21.2024.88.3.04.

[2] Z. Śliwa, A.K. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej* (Eng. Challenges in the context of migration and the crisis on the Polish-Belarusian border), "Wiedza Obronna" 2022, vol. 278, no. 1, p. 93. https://doi.org/10.34752/2022-d278.

[3] J. Maciejewski, *Wewnętrzny front. Łukaszenki wojna informacyjna i kryzys migracyjny na granicy polsko-białoruskiej* (Eng. The internal front. Lukashenka's information war and the migration crisis on the Polish-Belarusian border), Warszawa 2022, p. 73.

[4] *Organizatorzy nielegalnego przerzutu migrantów do Polski objęci zachodnimi sankcjami* (Eng. Organisers of illegal migrant smuggling to Poland subject to Western sanctions), InfoSecurity24, 27 I 2022, https://infosecurity24.pl/za-granica/organizatorzy-nielegalnego-przerzutu-migrantow-do-polski-objeci-zachodnimi-sankcjami [accessed: 4 VII 2025].

[5] J. Werner, *Ochrona granicy wschodniej Rzeczypospolitej Polskiej w kontekście nielegalnej migracji* (Eng. Protection of the eastern border of the Republic of Poland in the context of illegal migration), "Studia Bezpieczeństwa Narodowego" 2024, vol. 31, no. 1, p. 90. https://doi.org/10.37055/sbn/178377.

Служба Активных Мероприятий)[6]. According to Belarusian oppositionist Aliaksandr Azarau, the migrant smuggling operation was part of the KGB and the Border Guard activities and was developed by the Chairman of the KGB – Ivan Tertel. The operation was given the code name 'Sluice'[7]. A distinction should be made between two operations: the first in 2010 and the second in 2021. The aim of the first was to check the tightness of the EU's borders as well as to obtain financial support from the European Community for Belarus to strengthen the state border. The Caucasian people and foreigners residing in Belarus were used in this operation. In the following decade, the direction of migrant recruitment changed, as did the purpose of their use in political activities[8].

The aim of the article is to describe manifestations of solidarity with Polish uniformed services guarding the Polish-Belarusian border, using the example of a social campaign 'United behind the Polish uniform'. The author formulated the following questions: what were the reasons for starting the social campaign 'United behind the Polish uniform'? What was the course of the action? He put forward the thesis: the social campaign 'United behind the Polish uniform' was a response to the discrediting of Polish uniformed services following the operation 'Sluice'. The article employs the method of analysis and criticism of literature, synthesis as well as descriptive method.

Instrumentalisation of migrants in Belarusian and Russian politics, as exemplified by the operation 'Sluice'

The instrumentalisation of migrants by the Belarusian regime fits into one of the four types of migration engineering described by Kelly Greenhill[9]. A staged border crisis is equivalent to so-called forced migration engineering, characterised

[6] B. Fraszka, *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje* (Eng. The situation on the Poland-Belarus Border: Background, Geopolitics, Narratives), Warsaw Institute, 23 XII 2021, https://warsawinstitute.org/situation-poland-belarus-border-background-geopolitics-narratives/ [accessed: 14 II 2026].

[7] J. Maciejewski, *Wewnętrzny front*…, pp. 73–74.

[8] A. Szachoń-Pszenny, A. Zaręba, *Instrumentalizacja migrantów jako forma destabilizacji bezpieczeństwa na wschodniej granicy zewnętrznej UE w kontekście wojny w Ukrainie* (Eng. Instrumentalisation of migrants as a form of security destabilisation in the context of the war in Ukraine), "Politeja" 2024, vol. 21, no. 1, pp. 97–98. https://doi.org/10.12797/Politeja.21.2024.88.3.06.

[9] A. Szachoń-Pszenny, A. Zaręba, *Etapowość instrumentalizacji migrantów na przykładzie granicy z Białorusią – wyzwania współczesności* (Eng. Stages of migrants instrumentalisation on the Polish-Belarusian border example – contemporary challenges), "Przegląd Geopolityczny" 2024, vol. 49, p. 55.

by the exploitation of people for political purposes[10]. In modern conflicts between states, military action is not the only way to gain an advantage over the enemy. There are many more means and tools available to exert pressure[11].

Referring to Europe's experience with mass migration, Russian Major General Alexander Vladimirov, highlighted the problems arising from the presence of newcomers, including the loss of European identity and the possible rise of radical attitudes in the host society. According to Vladimirov, controlling mass migration is a modern strategic weapon that can be used to influence the political, economic and cultural spheres of a country. He also drew attention to the trap of moral dilemma. It concerns whether the state will maintain a humanitarian stance in the face of mass migration, or whether it will decide to marginalise this approach due to the need to ensure national security[12].

Krzysztof Chochowski draws attention to another dilemma related to the previous one. He points to two forms of action in response to the instrumentalisation of migrants: legal (i.e. lawful but unproductive) and effective (i.e. productive but violating legal norms). In Chochowski's opinion, choosing any of the options will cause internal destabilisation of the state and polarisation of society, because, as he stated (referring to the crisis on the Polish-Belarusian border): *This is precisely where the trap of the Belarusian regime lies* (…)[13].

The consequences of the events of 23 May 2021, related to the forced landing of a Ryanair airline plane in Minsk, can be considered the impetus for the start of the operation 'Sluice'. The plane was carrying Belarusian oppositionist Raman Pratasevich, who was arrested by Belarusian KGB officers. In response to repeated incidents of Alexander Lukashenka's suppression of the legal opposition, the EU decided to impose sanctions on Belarus[14]. Furthermore, the European Community

[10] Ibid.

[11] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. The hybrid nature of modern warfare – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (sci. eds.), Warszawa 2011, p. 11.

[12] M. Wojnowski, *The genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*, "Przegląd Bezpieczeństwa Wewnętrznego" 2022, no. 26, pp. 263–300. https://doi.org/10.4467/20801335PBW.21.042.15702.

[13] K. Chochowski, *Kryzys na granicy polsko-białoruskiej jako przejaw wojny hybrydowej. Aspekty administracyjnoprawne* (Eng. The crisis on the Polish-Belarusian border as a manifestation of hybrid warfare. Administrative and legal aspects), "Roczniki Nauk Społecznych" 2021, vol. 49, no. 4, p. 94. https://doi.org/10.18290/rns21494.8.

[14] G. Baziur, *Operation "Sluice". The so-called migration crisis at the Polish-Belarussian border: an example of hybrid actions taken in the second half of 2021 as documented in the reports of the Polish border guard*, "Bezpieczeństwo. Teoria i Praktyka" 2022, vol. 46, no. 1, p. 137. http://dx.doi.org/10.48269/2451-0718-btip-2022-1-008.

did not acknowledge Lukashenka's victory in the presidential elections on 9 June 2020. This deepened the isolation of Belarus on the international stage and, for Lukashenka, became yet another argument confirming his belief that the EU's goal was to destabilise the internal situation in Belarus[15]. Operation 'Sluice' was intended to lead to the lifting of EU sanctions, Belarus's emergence from isolation, and the acquisition of the financial support needed to resolve the crisis[16]. According to Jerzy Marek Nowakowski, one of the reasons for the migration crisis could also have been Lukashenka's desire for the international community to recognise him as a fully-fledged president of Belarus[17]. However, operation 'Sluice' did not lead to the achievement of the intended goals. The European Union condemned the actions of Lukashenka's regime and imposed another, fifth package of sanctions on Belarus (including, among others, the elites of the Belarusian regime)[18]. The decision to choose Poland or Lithuania as targets of attack was based on these countries' membership of the EU, their support for the Belarusian opposition and their approval of sanctions against the regime of Lukashenka[19].

Operation 'Sluice' was important for several reasons, primarily for the Russian Federation (RF). Firstly, Russia enabled the testing of the crisis response capabilities of EU Member States and the North Atlantic Alliance. Secondly, the RF led to the polarisation of society in a country affected by migration crisis, as well as maintaining constant anxiety and uncertainty about the legitimacy of the state apparatus's actions in response to the growing external threat. Thirdly, it destabilised the borders of the attacked countries (their authorities were forced, among other things, to significantly increase financial expenditure on border security). Fourthly, the migration crisis in Eastern Europe diverted attention from Russia's actions

[15] J. Szyszka, *Zjawisko state-sponsored human trafficking na przykładzie Białorusi* (Eng. The phenomenon of state-sponsored human trafficking as exemplified by Belarus), in: *Wybrane zagadnienia handlu ludźmi i zagrożonymi gatunkami roślin i zwierząt*, B. Stępień-Załucka, J. Uliasz (sci. eds.), Rzeszów 2023, pp. 122–123. http://dx.doi.org/10.15584/978-83-8277-037-7.9.

[16] A. Wawrzusiszyn, *Rosyjsko-białoruskie działania hybrydowe na granicach Unii Europejskieji NATO* (Eng. Russian-Belarusian hybrid activities on the borders of the European Union and NATO), "Journal of Modern Science" 2025, vol. 61, no. 1, p. 19. https://doi.org/10.13166/jms/203108.

[17] J.M. Nowakowski, *O co idzie gra?* (Eng. What is the game about?), in: *Raport IV. Granica dyktatora. Polska i Białoruś wobec kryzysu granicznego*, J. M. Nowakowski, J. Olędzka, M. Rust (eds.), Warszawa 2021, p. 74.

[18] K. Wańczyk, *Relacje Unii Europejskiej z Białorusią po sierpniu 2020 roku. Powrót do przeszłości* (Eng. The European Union's relations with Belarus after August 2020. A return to the past), in: *Raport V. Białoruś 500 dni po: od społecznej mobilizacji do neototalitarnej konsolidacji?*, J.M. Nowakowski, J. Olędzka, M. Rust (eds.), Warszawa 2022, pp. 96–97.

[19] A. Szabaciuk, *Forced migrations in Eastern Europe after 2020*, series: Prace Instytutu Europy Środkowej, no. 9, B. Surmacz, T. Stępniewski (eds.), Lublin 2022, p. 28.

in Ukraine and the Caucasus[20]. As the border incidents took place on Belarusian territory, Russia avoided direct responsibility for triggering the crisis[21].

The practice of instrumentalisation of migrants was supported by Belarusian and Russian propaganda centres: the Belarusian Telegraph Agency, the Russian News Agency TASS, RIA Novosti, Regnum and TV channels: Belarus-1, ONT and CTV, Rossiya 1 as well as Pervyj Kanal. In the case of Poland, a narrative referring to Nazism, racism, xenophobia and brutality of Polish uniformed services was used[22]. Using distorted or inaccurate information, Belarus questioned the effectiveness of the actions taken by individual countries and international organisations. In its information operations, it placed particular emphasis on undermining the rule of law, the legitimacy of the authorities, their ability to ensure security, as well as compromising the reputation of Central and Eastern European countries, particularly Poland, on the international stage. This image blurred responsibility for the migration crisis in Eastern Europe. Belarusian media centres strongly influenced viewers' emotions by using images of children, among other things[23]. The uniformed services were primarily accused of crimes and violations of the law. Belarusian state apparatus used analogies to Nazi troops from World War II and their methods of operation. Terms such as 'tormentors' in reference to Polish uniformed services and 'concentration camps' in reference to places where migrants were held were used in public discourse[24].

---

[20] See in more detail: A. Wawrzusiszyn, *Rosyjsko-białoruskie działania*…, pp. 19–27.

[21] J. Maciejewski, *Wewnętrzny front*…, pp. 64–66.

[22] B. Ociepka, *Dziennikarzom wstęp wzbroniony: kryzys na polsko-białoruskiej granicy w 2021 r. jako wydarzenie (nie)relacjonowane przez media* (Eng. Journalists barred: the 2021 crisis on the Polish-Belarusian border as an event (not) covered by the media), "Studia Medioznawcze" 2023, vol. 24, no. 2, pp. 198–199. https://doi.org/10.33077/uw.24511617.sm.2023.2.715.

[23] K. Kuśmirek, *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*, "Bezpieczeństwo. Teoria i Praktyka" 2022, vol. 48, no. 3, pp. 312–315. http://dx.doi.org/10.48269/2451-0718-btip-2022-3-023.

[24] A. Szabaciuk, *"Natowskie wojska szczękające gąsienicami czołgów". Polska i granica polsko-białoruska w propagandzie białoruskiej po 2020 roku* (Eng. 'NATO troops chattering with tank tracks'. Poland and the Polish-Belarusian border in post-2020 Belarusian propaganda), in: *Bezpieczeństwo granic – granice bezpieczeństwa*, D. Karczewski, R. Zenderowski (eds.), Warszawa 2023, pp. 347–349.

Strengthening security along the Polish-Belarusian border in response to the operation 'Sluice'

According to the data of the Headquarters of the Border Guard, in 2021 as many as 39 697 people attempted to cross the Polish-Belarusian border illegally. In previous years, few such cases were reported: 4 in 2018, 20 in 2019 and 129 in 2020. In 2021, the migration crisis peaked in October (17 447 attempts to cross the border). Most attempts to cross the border were made on sections belonging to the area of Podlaski Border Guard Regional Unit. These were sections under the jurisdiction of the following Border Guard institutions: Michałowo, Czeremcha, Białowieża and Kuźnica[25].

Both traditional and modern security measures were used to strengthen the Polish-Belarusian border protection. Traditional measures include round-the-clock patrols, carried out on foot or using various types of vehicles. The catalogue of modern measures includes the use of cooled thermal imaging cameras, camera traps and drones. These measures are characterised by resistance to temperature differences, accuracy in identifying threats, and are also difficult to detect, which is why they are important part of border protection[26].

The *Act of 29 October 2021 on the construction of state border security* was passed by a decision of the Sejm of the Republic of Poland. Both physical and electronic security measures were put in place along the Polish-Belarusian border. A physical barrier consisting of steel spans measuring 5.5 metres in height covered a total of 186 km of the border. Secondly, an electronic barrier was built along the entire border with Belarus. The perimeter system consists of day/night cameras, thermal imaging cameras, detection cables and telecommunications containers. The total cost of the border fortifications amounted to PLN 1.6 billion[27]. The security measures proved insufficient, so in 2024, a decision was made to install cross beams with an additional coil of razor wire to prevent the steel spans from being bent. In addition,

[25] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią w 2021 r.* (Eng. Illegal border crossings with Belarus in 2021), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021r.html [accessed: 1 IV 2025].

[26] J. Werner, *Ochrona granicy wschodniej*…, pp. 95–97.

[27] K. Szwed, *Zakończenie odbioru bariery elektronicznej na granicy polsko-białoruskiej* (Eng. Completion of the acceptance of the electronic barrier on the Polish-Belarusian border), Straż Graniczna, 15 VI 2023, https://www.strazgraniczna.pl/pl/aktualnosci/11875,Zakonczenie-odbioru-bariery-elektronicznej-na-granicy-polsko-bialoruskiej.html [accessed: 5 IV 2025].

the electronic barrier was reinforced with more cameras and lighting, along with sensors[28]. The modernisation of the barrier was completed on 30 March 2025[29].

The Border Guard was supported in protecting the Polish-Belarusian border by the Police, soldiers of the Polish Army and the State Fire Service. The Police carried out its tasks as part of an operation codenamed 'Barrier' (Pol. Zapora). A total of 32 759 officers from various fields were involved, including counter-terrorism officers, pilots, and service dog handlers[30]. This enabled the exchange of experiences and mutual training of uniformed services present at the Polish-Belarusian border. The Police conducted patrols along the border, repelled mass attacks by migrants and combated the activities of smuggling networks. It used multi-purpose type S70i Black Hawk and Bell 407GXi helicopters to identify threats. Operation 'Barrier' came to an end on 19 December 2024[31].

Soldiers of the Polish Army assisted Border Guard officers in several operations. One of them, codenamed 'Strong support', began on 3 September 2021[32]. Military units of the Territorial Defence Forces (WOT), including the 1st Podlasie Territorial Defence Brigade and the 2nd Lublin Territorial Defence Brigade, conducted foot, water and horse patrols, and also used unmanned systems. These activities resulted in numerous arrests of migrants and smugglers. Due to the state of emergency introduced in the border areas, WOT soldiers provided support also to the local community[33]. The Military Police and operational troops were also involved in the operation, for instance: the 12th Szczecin Mechanised Division named after Bolesław Krzywousty, the 16th Pomeranian Mechanised Division named after King Casimir IV Jagiellonczyk, 18th Mechanised Division named after Lieutenant General

---

[28] *Szef BBN na granicy polsko–białoruskiej. Wzmacnianie zabezpieczeń to „dowód ciągłości myśli strategicznej państwa*" (Eng. The Head of the National Security Bureau on the Polish-Belarusian border. Strengthening security measures is 'proof of the continuity of the state's strategic thinking), Biuro Bezpieczeństwa Narodowego, 11 X 2024, https://www.bbn.gov.pl/pl/wydarzenia/10003,Szef-BBN-na-granicy-polsko-bialoruskiej-Wzmacnianie-zabezpieczen-to-quotdowod-ci.html [accessed: 5 IV 2025].

[29] *Modernizacja bariery elektronicznej na granicy Polski z Białorusią (WIDEO)* (Eng. Modernisation of the electronic barrier on the Polish-Belarusian border (VIDEO)), Telbud S.A., https://telbud.pl/strefa-informacji/modernizacja-bariery-elektronicznej-na-granicy-polski-z-bialorusia-wideo [accessed: 14 II 2026].

[30] *Zakończenie operacji policyjnej „Zapora*" (Eng. End of the police operation 'Barrier'), "Gazeta Policyjna" 2025, no. 49, pp. 24–25.

[31] Ibid.

[32] *3 miesiące operacji #SilneWsparcie* (Eng. 3 months of the operation *#SilneWsparcie*), Wojska Obrony Terytorialnej, 3 XII 2021, https://media.terytorialsi.wp.mil.pl/informacje/712389/3-miesiace-operacji-silnewsparcie [accessed: 6 IV 2025].

[33] Ibid.

Tadeusz Buk[34]. The increase in the number of soldiers at the border was the result of an operation 'Griffin'. It strengthened the actions of the officers of the Border Guard and the Police. Operation 'Rengaw' was of a training and defence nature[35]. By decision of the Minister of National Defence, a military task force was established to carry out a training programme for soldiers in the Podlaskie Province. Increasing their presence in border areas as part of training activities was also intended to serve as a deterrent[36]. To ensure the full effectiveness of the measures taken, both operations were replaced on 1 August 2024 by a single operation 'Safe Podlasie'[37].

Officers of the State Fire Service also played an important role in protecting the Polish-Belarusian border. During mass attempts by migrants to cross the border, they ensured constant access to water for specialised police vehicles equipped with water cannons. They were also responsible for the safety and efficient operation of military aviation. Together with other uniformed services, they strengthened border security and provided assistance to migrants in need[38].

Forms of aggression towards Polish uniformed services

The uniformed services were exposed to both physical and psychological violence from migrants and other groups. Provocations by the Belarusian services towards Polish soldiers and officers were intended to test their mental resilience and training. Pyrotechnic materials were thrown at Polish services, grenade throws were simulated, so-called blank shots were fired, people were blinded with torches,

[34] E. Moczuk, D. Czekaj, *Kryzys migracyjny jako element wojny hybrydowej. Analiza działania wojska na granicy polsko-białoruskiej* (Eng. Migration crisis as part of hybrid warfare. Analysis of military operations on the Polish-Belarusian border), Rzeszów 2024, p. 224.

[35] J. Dziemiańczuk, *"Bezpieczne Podlasie" zastąpi dwie dotychczasowe operacje* (Eng. 'Safe Podlasie' will replace two existing operations), Wojska Obrony Terytorialnej, 31 VII 2024, https://media.terytorialsi.wp.mil.pl/informacje/838336/bezpieczne-podlasie-zastapi-dwie-dotychczasowe-operacje [accessed: 6 IV 2025].

[36] E. Korsak, *Nowa operacja wojskowa na Podlasiu* (Eng. A new military operation in Podlasie), Polska Zbrojna, 12 VIII 2023, https://polska-zbrojna.pl/home/articleshow/40146?t=Nowa-operacja-wojskowa-na-Podlasiu [accessed: 7 IV 2025].

[37] *Nowa operacja wojskowa na wschodniej granicy: OP Bezpieczne Podlasie* (Eng. A new military operation on the eastern border: OP Safe Podlasie), Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-07-176-op-bezpieczne-podlasie/ [accessed: 7 IV 2025].

[38] M. Łozowski, *Państwowa Straż Pożarna w obronie granic RP* (Eng. The State Fire Service in defence of the borders of the Republic of Poland), Krajowa Sekcja Pożarnictwa, 7 XII 2021, https://kspnszz.org/index.php/2021/12/07/panstwowa-straz-pozarna-w-obronie-granic-rp/ [accessed: 8 IV 2025].

and suspicious packages were left behind[39]. According to the Helsinki Foundation for Human Rights, Belarusian services also used physical violence against migrants to force them to cross the border illegally and provoke reaction from Polish soldiers and officers[40]. One example was the attack on the Kuźnica–Bruzgi border crossing in November 2021. This was preceded by the Belarusian authorities bringing in a thousand migrants. They took on the role of observer of the events. Migrants repeatedly attacked Polish soldiers and officers using various tools: stones, paving stones, bottles, logs, and stun grenades. The health and lives of officers of the Polish uniformed services and soldiers were exposed to great danger. This is confirmed by photographs and reports from these events[41].

Some Polish politicians and celebrities also joined in the attacks on Poland's uniformed services. They made derogatory remarks about the people guarding the border[42].

---

[39] J. Maciejewski, *Wewnętrzny front*…, pp. 248–249.

[40] K. Czarnota, M. Gorczyńska, *Gdzie prawo nie sięga. Raport Helsińskiej Fundacji Praw Człowieka z monitoringu sytuacji na polsko-białoruskiej granicy* (Eng. Where the law does not reach. Report by the Helsinki Foundation for Human Rights on monitoring the situation on the Polish-Belarusian border), Helsińska Fundacja Praw Człowieka, Warszawa 2022, pp. 39–40.

[41] M. Jurkowska, *Masowy szturm na przejście graniczne w Kuźnicy. Mija rok od ataku cudzoziemców na granicę i funkcjonariuszy SG* (Eng. Massive assault on the border crossing in Kuźnica. A year has passed since the attack by foreigners on the border and Border Guard officers), Sokółka Nasze Miasto, 16 XI 2022, https://sokolka.naszemiasto.pl/masowy-szturm-na-przejscie-graniczne-w-kuznicy-mija-rok-od/ar/c1-9090195 [accessed: 11 IV 2025].

[42] M. Kożdoń-Dębecka, *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych* (Eng. Media polarisation on the example of the migration crisis taking place on the Polish-Belarusian border in the summer of 2021 in the reports of three Polish television news services), "Media Biznes Kultura" 2023, vol. 14, no. 1, pp. 170–171. https://doi.org/10.4467/25442554.MBK.23.010.18033; K. Orzech, *Zagrożenia dla Polski kreowane przez Republikę Białorusi w kontekście sytuacji kryzysowej na granicy polsko-białoruskiej* (Eng. The threats to Poland posed by the Republic of Belarus in the context of the crisis situation on the Polish-Belarusian border), "Studia Bezpieczeństwa Narodowego" 2021, vol. 22, no. 4, p. 63. https://doi.org/10.37055/sbn/147013; P. Rojek-Socha, K. Żaczkiewicz-Zborska, *SN: Sprawa aktorki oskarżonej o zniesławienie Straży Granicznej do ponownego rozpoznania* (Eng. Supreme Court: Case of actress accused of defaming the Border Guard to be re-examined), Prawo.pl, 6 XI 2024, https://www.prawo.pl/prawnicy-sady/sn-sprawa-aktorki-oskarzonej-o-znieslawienie-strazy-granicznej-do-ponownego-rozpoznania,529890.html [accessed: 27 II 2026]; *Znany aktor Piotr Z. usłyszał zarzuty zniesławienia i znieważenia rzeczniczki Straży Granicznej* (Eng. Well-known actor Piotr Z. has been charged with defamation and insulting a spokesperson for the Border Guard), Polska Agencja Prasowa, 31 III 2022, https://www.pap.pl/aktualnosci/news%2C1137489%2Cznany-aktor-piotr-z-uslyszal-zarzuty-znieslawienia-i-zniewazenia [accessed: 27 II 2026].

Recognition of the Polish uniformed services from state authorities and society

In connection with the events at the Polish-Belarusian border and negative narratives concerning the activities of the Polish uniformed services, both the state authorities and the society expressed their support for the officers and soldiers serving at the border. The Sejm of the Republic of Poland passed two resolutions, and the Minister of National Defence established a special badge. The public expressed its appreciation as part of a nationwide campaign under the slogan 'United behind the Polish uniform', which consisted of various initiatives.

Resolutions of the Sejm of the Republic of Poland and Decision of the Minister of National Defence

The Sejm of the Republic of Poland passed the *Resolution of 17 November 2021 on solidarity in the protection of Polish borders*. It clearly pointed to the Belarusian regime's responsibility for destabilisation of the Polish-Belarusian border by instrumentalisation of migrants. The Sejm of the Republic of Poland also expressed its gratitude to all those involved in protecting the national border. Special thanks were extended to Border Guard officers, Police officers and Polish Army soldiers. According to the text of the resolution, it is the duty of every Polish citizen to (…) *support state institutions and services and to stand* (…) *side by side with Border Guard and Police officers, Polish Army soldiers, including Territorial Defence Forces, and representatives of other services who proudly wear the Polish uniform and guard the borders of the state and the sovereignty of our Homeland*.

Another expression of support from the Sejm of the Republic of Poland was the *Resolution of 24 July 2024 on expressing appreciation for the service and dedication of soldiers and officers guarding border security of the Republic of Poland*. The Sejm again condemned the Belarusian regime as well as Russian regime for hybrid actions on the Polish-Belarusian border. The resolution strongly emphasised appreciation for the uniformed services, their dedication, devotion to the homeland, professionalism, courage and resilience in the face of hardship. The resolution also expressed gratitude for numerous grassroots social campaigns supporting Polish uniformed services.

As expression of gratitude to the soldiers for maintaining the security of Poland's eastern border, the Minister of National Defence, by Decision no. 148 of 17 October 2022 introduced a special badge 'For the Protection of the Border of the Republic of Poland' as a form of (…) *honouring soldiers of the Armed Forces of the Republic*

of Poland, employees of the Ministry of National Defence, soldiers of other countries and other persons who contributed to ensuring the security and inviolability of the borders of the Republic of Poland[43]. The decoration has a three-tier hierarchy. Tier I (gold) is awarded for heroic deeds, tier II (silver) for special merits, and tier III (bronze) for performing tasks ensuring security and integrity of the Polish border[44].

Nationwide social campaign 'United behind the Polish uniform'

In defence of Polish soldiers and officers, internet users took action under the slogan 'United behind the Polish uniform', which transformed into a nationwide social campaign. It became a symbolic gesture of support for the Polish uniformed services guarding the border with Belarus[45]. Polish citizens, local government institutions, government agencies, non-governmental organisations, the media and many other entities were involved in the campaign.

One of the most recognisable initiatives was the 'Card for Border Defenders' campaign, initiated by the Independence Foundation[46]. Children and schoolchildren in particular were encouraged to participate in it. The artwork was to be in the form of a drawing. The subject matter was not strictly defined. The prizes were teaching aids, including a historical comic book. The campaign was supported by the Board of Education in Lublin, the 2nd Lublin Territorial Defence Brigade and the Radio Lublin[47]. Later on, the campaign gained the support of the Military

[43] *Decision No. 148/MON of the Minister of National Defence of 17 October 2022 on the introduction of a special badge named 'For the Protection of the Border of the Republic of Poland'*, Appendix no. 7: *Special badge regulations 'For the Protection of the Border of the Republic of Poland'*.

[44] Ibid.

[45] *Murem za polskim mundurem* (Eng. United behind the Polish uniform), Wojska Obrony Terytorialnej, 21 XI 2021, https://media.terytorialsi.wp.mil.pl/informacje/708475/murem-za-polskim-mundurem [accessed: 3 VIII 2025].

[46] The Independence Foundation, based in Lublin, is primarily concerned with promoting Polish history both at home and abroad. It also conducts educational and scientific activities in this field and protects national heritage. It organises training courses, conferences and public debates, publishes magazines and develops educational programmes. See: *Statut fundacji „Fundacja Niepodległości"* (Eng. Statute of the 'Independence foundation'), https://www.fundacja-niepodleglosci.pl/images/STATUT_FUNDACJI/Fundacja_Niepodleg%C5%82o%C5%9Bci_Statut_17.11.2021_r.pdf [accessed: 29 VII 2025].

[47] *Kartka dla obrońców granic* (Eng. A card for border defenders), Fundacja Niepodległości, 10 XI 2021, https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2451-kartka-dla-obroncow-granic [accessed: 30 VI 2025].

Property Agency – Regional Office in Lublin, which provided pocket first aid kits for the authors of selected works[48].

The Polish authorities, including the President and Prime Minister, were involved in the 'United behind the Polish uniform' campaign. They showed solidarity with the uniformed services defending the Polish-Belarusian border, opposing the hostile propaganda of the Belarusian and Russian regimes. In one of his statements, President Andrzej Duda declared: *I bow my head to all Polish officers of the Border Guard and other services, Polish soldiers* (…) *for their extraordinary effort, sacrifice and dedication to the Republic of Poland* (…)[49]. Prime Minister Mateusz Morawiecki made similar remarks during his speech in the Sejm regarding the situation at the Polish-Belarusian border: (…) *we owe our gratitude for their honourable service, for defending the dignity of the Polish soldier's uniform, the Polish officer, to all the wonderful officers, soldiers of the operational forces, soldiers of the Territorial Defence Forces*[50].

The slogan 'United behind the Polish uniform' was also used in a campaign carried out by the Polish Post Office. The campaign involved writing a letter or preparing a card expressing support for the Polish uniformed services. The formal requirement was to include the phrase 'To the defenders of the border' in the work and not to address it. However, participants in the campaign could specify the recipient (a person or unit)[51]. Furthermore, the Polish Post Office issued a special postage stamp together with an FDC envelope, expressing gratitude to the Polish uniformed services for protecting the eastern border of the country. Both

---

[48] *Kartka dla obrońców granic – nasza akcja się rozszerza* (Eng. A card for a border defenders – our action is expanding), Fundacja Niepodległości, 25 XI 2021, https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2456-kartka-dla-obroncow-granic-nasza-akcja-sie-rozszerza [accessed: 30 VI 2025].

[49] *Murem za polskim mundurem!* (Eng. United behind the Polish Uniform!), prezydent.pl, 13 X 2023, https://www.prezydent.pl/multimedia/wideo/murem-za-polskim-mundurem,1148,33 [accessed: 2 VII 2025].

[50] *Wypowiedź premiera Mateusza Morawieckiego w Sejmie nt. sytuacji na granicy polsko-białoruskiej* (Eng. The statement of the Prime Minister Mateusz Morawiecki in the Sejm on the situation on the Polish--Belarusian border), https://www.gov.pl/attachment/f93dffbc-f0ea-48c5-990b-7c01608b2213 [accessed: 2 VII 2025].

[51] *Jesteśmy z Wami – wyślij kartkę mundurowym na granicy* (Eng. We are with you, send a card to the border guards), Poczta Polska, 11 XI 2021, https://media.poczta-polska.pl/releases/jestesmy-z-wami-wyslij-kartke-mundurowym-na-granicy#:~:text=Poczta%20Polska%20bezp%C5%82atnie%20przeka%C5%BCe%20takie%20kartki%20s%C5%82u%C5%BCbom,dor%C4%99czane.%20LISTA%20plac%C3%B3wek%20ze%20specjalnymi%20pojemnikami:%20Lp. [accessed: 30 VI 2025].

products bear the '#♥ZaPolskimMundurem' (We stand behind the Polish uniform) logo[52].

The National Bank of Poland (NBP) issued a silver collector coin entitled 'Protection of the Polish Eastern Border' with a face value of PLN 10. The obverse of the coin depicts a Polish border post, military camouflage and forest areas, while the reverse shows silhouettes of officers of the Border Guard, the Police and a soldier of the Armed Forces. A helicopter is positioned above the figures. The Police officer is depicted wearing a helmet and carrying a protective shield, while the soldier is armed with a long weapon. The outline of the Polish border is visible in the background, with the Polish-Belarusian border clearly marked[53]. A few months after the release of the silver coin, the NBP bank issued a collector's banknote entitled 'Protection of the Polish Eastern Border' with a face value of PLN 20. It featured a similar graphic design to that of the collector's coin[54].

The celebrations of the anniversary of Poland regaining independence, organised under the slogan 'Day of Respect for the Uniform', had a special significance in 2021. In 103 military units (in connection with the 103rd anniversary of Poland regaining independence), presentations on the symbolism of the uniform were held. Furthermore, on the day before the central celebrations of the Independence Day, an exhibition entitled 'Uniforms of Polish Soldiers – Respect for the Uniform' was opened in the Sejm of the Republic of Poland[55].

The official website of the Border Guard also presents the positions of institutions and social organisations, including the Association of Veterans of Polish Border Formations, Lubliniec City Council, Spytkowice Municipal Council, Lubomino Municipal Council, the Association of Persons Repressed

---

[52] *Poczta Polska ze specjalną emisją „#♥ZaPolskimMundurem" poświęconą obrońcom wschodniej granicy* (Eng. The Polish Post Office with a special mission 'We stand behind the Polish Uniform' devoted to defenders of the eastern border), Poczta Polska, 27 I 2022, https://www.poczta-polska.pl/news/poczta-polska-ze-specjalna-emisja-%E2%99%A5zapolskimmundurem-poswiecona-obroncom-wschodniej-granicy/ [accessed: 1 VII 2025].

[53] *"Ochrona polskiej granicy wschodniej" na srebrnej monecie NBP* (Eng. 'Protection of Poland's eastern border' on a silver coin issued by the National Bank of Poland), Narodowy Bank Polski, 26 I 2022, https://nbp.pl/ochrona-polskiej-granicy-wschodniej-na-srebrnej-monecie-nbp/ [accessed: 1 VII 2025].

[54] *NBP wprowadza banknot kolekcjonerski "Ochrona polskiej granicy wschodniej"* (Eng. The National Bank of Poland introduces a collector's banknote entitled 'Protection of the Polish eastern border'), Narodowy Bank Polski, 18 VII 2022, https://nbp.pl/nbp-wprowadza-banknot-kolekcjonerski-ochrona-polskiej-granicy-wschodniej/ [accessed: 1 VII 2025].

[55] *Narodowe Święto Niepodległości – „Dzień szacunku dla munduru"* (Eng. National Independence Day – 'Day of respect for the uniform'), Wojsko Polskie, https://www.wojsko-polskie.pl/weterani/articles/aktualnosci-r/narodowe-swieto-niepodleglosci-dzien-szacunku-dla-munduru/ [accessed: 3 VII 2025].

during Martial Law, the Christian Culture Movement 'Rebirth', expressing gratitude for service on the Polish-Belarusian border[56].

Soldiers on the border were accompanied by military chaplains who, in addition to sacramental ministry, provided psychological support. As pointed out by Priest, Second Lieutenant Artur Janczarek (chaplain of the 15th Gołdap Anti-Aircraft Regiment), soldiers are exposed to constant aggression from the Belarusian services, which affects their physical and mental condition[57]. Spiritual support was offered to them by the President of the Polish Episcopal Conference, Archbishop Stanisław Gądecki, in a statement concerning the escalation of tensions at the Polish-Belarusian border[58]. In turn, due to the Orthodox Ordinariate of the Polish Army, in cooperation with the Orthodox Christian Charity ELEOS, essential supplies were delivered to the Border Guard facilities[59].

During the Christmas season of 2021, numerous initiatives were undertaken by state institutions and authorities to thank uniformed services for their efforts in maintaining security and public order. The '#WolneMiejsceDlaMunduru' (Save a seat for the uniform) campaign was organised with soldiers and officers in mind who are away from their families during the Christmas season. The form of involvement in this campaign was to leave a place card next to an empty plate during Christmas Eve dinner[60].

---

[56] *#MuremZaPolskimMundurem – stanowiska instytucji i organizacji* (Eng. United behind the Polish Uniform – positions of the institutions and organisations), Straż Graniczna, 3 XII 2021, https://strazgraniczna.pl/pl/pozostale-informacje/muremzapolskimmundurem/muremzapolskimmundurem/9548,MuremZaPolskimMundurem-stanowiska-instytucji-i-organizacji.html [accessed: 3 VII 2025].

[57] K. Stępkowski, *Ks. ppor. Artur Janczarek: nasza posługa na granicy to realizacja przysięgi Wojskowej* (Eng. Priest, second lieutenant Artur Janczarek: our service at the border is the fulfilment of military oath), Ordynariat Polowy, 18 XI 2021, https://archiwum2023-ordynariat.wp.mil.pl/pl/articles/wiadomosci-listopad-2021/ks-ppor-artur-janczarek-nasza-posluga-na-granicy-realizacja-przysiegi-wojskowej/index.html [accessed: 19 VIII 2025].

[58] M. Pietraszczyk, *Komunikat Przewodniczącego Konferencji Episkopatu Polski wobec eskalacji napięć na granicy polsko-białoruskiej* (Eng. Statement by the President of the Polish Episcopal Conference on the escalation of tensions on the Polish-Belarusian border), Straż Graniczna, 11 XI 2021, https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/rzymskokatolickie/9542,Komunikat-Przewodniczacego-Konferencji-Episkopatu-Polski-wobec-eskalacji-napiec-.html [accessed: 3 VII 2025].

[59] *Duchowe wsparcie na granicy* (Eng. Spiritual support on the border), Straż Graniczna, 26 XI 2021, https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/prawoslawne/9573,Duchowe-wsparcie-na-granicy.html [accessed: 3 VII 2025].

[60] Ł. Wilczewski, *W tę wigilię zostawmy #WolneMiejsceDlaMunduru* (Eng. On this Christmas Eve, save a seat for the uniform), Wojsko Polskie, https://www.wojsko-polskie.pl/1bot/articles/aktualnosci-w/w-te-wigilie-zostawmywolnemiejscedlamundru/ [accessed: 19 VIII 2025].

Local communities were also active. For instance, on the initiative of Polish Senator Maria Koc and the Head of Garwolin District Mirosław Walicki, a collection of sweets was organised for uniformed services. Among others, companies, rural housewive's clubs and volunteer fire brigades (OSP) joined the campaign[61]. The slogan 'United behind the Polish uniform' was preserved in the form of a mural on the wall of the OSP Kochcice fire station. It presents profiles of Border Guard, OSP, Police officers and the Polish Army soldier[62].

Summary

The migration crisis at the Polish-Belarusian border has demonstrated how dangerous and problematic migrants instrumentalisation practice is. People were used as means of combat, including as psychological weapons[63]. In accordance with the guidelines of the Belarusian services, migrants carried out numerous assaults using dangerous tools. The border and state uniformed services were the targets of the attack[64]. Propaganda and disinformation had a negative impact on the Polish society. Belarusian media centres, with Russia's support, presented a distorted picture of reality, consistent with the political goals of those regimes. Polish uniformed services responding to the artificially induced phenomenon of mass migration were accused of exceptional brutality and inhumane treatment of migrants. This narrative was also perpetuated by certain circles in Poland. The result of these actions was growing polarisation of the Polish society[65].

One expression of opposition to these events was the nationwide social campaign 'United behind the Polish uniform'. Officers and soldiers received words of support from representatives of state authorities and members of the public, cards made by children and young people, basic necessities and much more. These

[61] *Powiat Garwoliński wspiera służby mundurowe!* (Eng. Garwoliński District supports uniformed services!), Starostwo Powiatowe w Garwolinie, https://samorzad.gov.pl/web/powiat-garwolin/zbiorka-slodyczy [accessed: 3 VII 2025].

[62] P. Ciastek, *Na remizie OSP Kochcice powstał mural z przesłaniem. Są na nim polskie służby Mundurowe* (Eng. A mural with a message was created at the OSP Kochcice fire station. It depicts Polish uniformed services), Lubliniec Nasze Miasto, 25 IX 2023, https://lubliniec.naszemiasto.pl/na-remizie-osp-kochcice-powstal-mural-z-przeslaniem-sa-na/ar/c1-9464993 [accessed: 3 VII 2025].

[63] K. Chochowski, *Kryzys na granicy polsko-białoruskiej*…, p. 96.

[64] M. Pieczyński, *Granica propagandy. Łukaszenka i Putin na wojnie hybrydowej z Polską* (Eng. The limits of propaganda. Lukashenka and Putin in a hybrid war with Poland), Warszawa 2022.

[65] K. Orzech, *Zagrożenia dla Polski*…, pp. 62–64.

actions showed that Polish uniformed services could count on the support of their compatriots.

This publication was financed by the Faculty of International and Political Studies as part of the Strategic Program Excellence Initiative at the Jagiellonian University.

Bibliography

Baziur G., *Operation "Sluice". The so-called migration crisis at the Polish-Belarussian border: an example of hybrid actions taken in the second half of 2021 as documented in the reports of the Polish border guard*, "Bezpieczeństwo. Teoria i Praktyka" 2022, vol. 46, no. 1, pp. 133–150. http://dx.doi.org/10.48269/2451-0718-btip-2022-1-008.

Chochowski K., *Kryzys na granicy polsko-białoruskiej jako przejaw wojny hybrydowej. Aspekty administracyjnoprawne* (Eng. The crisis on the Polish-Belarusian border as a manifestation of hybrid warfare. Administrative and legal aspects), "Roczniki Nauk Społecznych" 2021, vol. 49, no. 4, pp. 81–99. https://doi.org/10.18290/rns21494.8.

Czarnota K., Górczyńska M., *Gdzie prawo nie sięga. Raport Helsińskiej Fundacji Praw Człowieka z monitoringu sytuacji na polsko-białoruskiej granicy* (Eng. Where the law does not reach. Report by the Helsinki Foundation for Human Rights on monitoring the situation on the Polish-Belarusian border), Helsińska Fundacja Praw Człowieka, Warszawa 2022.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. The hybrid nature of modern warfare – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (sci. eds.), Warszawa 2011, pp. 9–17.

Kuśmirek K., *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*, "Bezpieczeństwo. Teoria i Praktyka" 2022, vol. 48, no. 3, pp. 311–321. http://dx.doi.org/10.48269/2451-0718-btip-2022-3-023.

Maciejewski J., *Wewnętrzny front. Łukaszenki wojna informacyjna i kryzys migracyjny na granicy polsko-białoruskiej* (Eng. The internal front. Lukashenka's information war and the migration crisis on the Polish-Belarusian border), Warszawa 2022.

Moczuk E., Czekaj D., *Kryzys migracyjny jako element wojny hybrydowej. Analiza działania wojska na granicy polsko-białoruskiej* (Eng. Migration crisis as part of hybrid warfare. Analysis of military operations on the Polish-Belarusian border), Rzeszów 2024.

Niedźwiedzki D., *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego* (Eng. Humanitarian crisis on the Polish-Belarusian border. Analysis of the phenomenon from the perspective of social order), "Politeja" 2024, vol. 21, no. 1, pp. 57–74. https://doi.org/10.12797/Politeja.20.2024.88.1.01.

Nowakowski J.M., *O co idzie gra?* (Eng. What is the game about?), in: *Raport IV. Granica dyktatora. Polska i Białoruś wobec kryzysu granicznego*, J. M. Nowakowski, J. Olędzka, M. Rust (eds.), Warszawa 2021, pp. 73–81.

Ociepka B., *Dziennikarzom wstęp wzbroniony: kryzys na polsko-białoruskiej granicy w 2021 r. jako wydarzenie (nie)relacjonowane przez media* (Eng. Journalists barred: the 2021 crisis on the Polish-Belarusian border as an event (not) covered by the media), "Studia Medioznawcze" 2023, vol. 24, no. 2, pp. 190–203. https://doi.org/10.33077/uw.24511617.sm.2023.2.715.

Orzech K., *Zagrożenia dla Polski kreowane przez Republikę Białorusi w kontekście sytuacji kryzysowej na granicy polsko-białoruskiej* (Eng. The threats to Poland posed by the Republic of Belarus in the context of the crisis situation on the Polish-Belarusian border), "Studia Bezpieczeństwa Narodowego" 2021, vol. 22, no. 4, pp. 55–68. https://doi.org/10.37055/sbn/147013.

Pieczyński M., *Granica propagandy. Łukaszenka i Putin na wojnie hybrydowej z Polską* (Eng. The limits of propaganda. Lukashenka and Putin in a hybrid war with Poland), Warszawa 2022.

Szabaciuk A., *Forced migrations in Eastern Europe after 2020*, series: Prace Instytutu Europy Środkowej, no. 9, B. Surmacz, T. Stępniewski (eds.), Lublin 2022.

Szabaciuk A., *"Natowskie wojska szczękające gąsienicami czołgów". Polska i granica polsko-białoruska w propagandzie białoruskiej po 2020 roku* (Eng. 'NATO troops chattering with tank tracks'. Poland and the Polish-Belarusian border in post-2020 Belarusian propaganda), in: *Bezpieczeństwo granic – granice bezpieczeństwa*, D. Karczewski, R. Zenderowski (eds.), Warszawa 2023, pp. 331–364.

Szachoń-Pszenny A., Zaręba A., *Etapowość instrumentalizacji migrantów na przykładzie granicy z Białorusią – wyzwania współczesności* (Eng. Stages of migrants instrumentalisation on the Polish-Belarusian border example – contemporary challenges), "Przegląd Geopolityczny" 2024, vol. 49, pp. 49–68.

Szachoń-Pszenny A., Zaręba A., *Instrumentalizacja migrantów jako forma destabilizacji bezpieczeństwa na wschodniej granicy zewnętrznej UE w kontekście wojny w Ukrainie* (Eng. Instrumentalisation of migrants as a form of security destabilisation in the context of the war in Ukraine), "Politeja" 2024, vol. 21, no. 1, pp. 89–104. https://doi.org/10.12797/Politeja.20.2024.88.1.01.

Szyszka J., *Zjawisko state-sponsored human trafficking na przykładzie Białorusi* (Eng. The phenomenon of state-sponsored human trafficking as exemplified by Belarus), in: *Wybrane zagadnienia handlu ludźmi i zagrożonymi gatunkami roślin i zwierząt*, B. Stępień-Załucka, J. Uliasz (sci. eds.), Rzeszów 2023, pp. 118–133. http://dx.doi.org/10.15584/978-83-8277-037-7.9.

Śliwa Z., Olech A.K., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej* (Eng. The challenges in the context of migration and the crisis on the Polish-Belarusian border), "Wiedza Obronna" 2022, vol. 278, no. 1, pp. 87–105. https://doi.org/10.34752/2022-d278.

Wańczyk K., *Relacje Unii Europejskiej z Białorusią po sierpniu 2020 roku. Powrót do przeszłości* (Eng. The European Union's relations with Belarus after August 2020. A return to the past), in: *Raport V. Białoruś 500 dni po: od społecznej mobilizacji do neototalitarnej konsolidacji?*, J.M. Nowakowski, J. Olędzka, M. Rust (eds.), Warszawa 2022, pp. 87–109.

Wawrzusiszyn A., *Rosyjsko-białoruskie działania hybrydowe na granicach Unii Europejskiej i NATO* (Eng. Russian-Belarusian hybrid activities on the borders of the European Union and NATO), "Journal of Modern Science" 2025, vol. 61, no. 1, pp. 10–32. https://doi.org/10.13166/jms/203108.

Werner J., *Ochrona granicy wschodniej Rzeczypospolitej Polskiej w kontekście nielegalnej Migracji* (Eng. Protection of the eastern border of the Republic of Poland in the context of illegal migration), "Studia Bezpieczeństwa Narodowego" 2024, vol. 31, no. 1, pp. 83–106. https://doi.org/10.37055/sbn/178377.

Wojnowski M., *The genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*, "Przegląd Bezpieczeństwa Wewnętrznego" 2022, no. 26, pp. 263–300. https://doi.org/10.4467/20801335PBW.21.042.15702.

Zakończenie operacji policyjnej „Zapora" (Eng. End of the police operation 'Barrier'), "Gazeta Policyjna" 2025, no. 49, pp. 24–25.

Internet sources

3 miesiące operacji #SilneWsparcie (Eng. 3 months of the operation *#SilneWsparcie*), Wojska Obrony Terytorialnej, 3 XII 2021, https://media.terytorialsi.wp.mil.pl/informacje/712389/3-miesiace-operacji-silnewsparcie [accessed: 6 IV 2025].

Ciastek P., *Na remizie OSP Kochcice powstał mural z przesłaniem. Są na nim polskie służby Mundurowe* (Eng. A mural with a message was created at the OSP Kochcice fire station. It depicts Polish uniformed services), Lubliniec Nasze Miasto, 25 IX 2023, https://lubliniec.naszemiasto.pl/na-remizie-osp-kochcice-powstal-mural-z-przeslaniem-sa-na/ar/c1-9464993 [accessed: 3 VII 2025].

Duchowe wsparcie na granicy (Eng. Spiritual support on the border), Straż Graniczna, 26 XI 2021, https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/prawoslawne/9573,Duchowe-wsparcie-na-granicy.html [accessed: 3 VII 2025].

Dziemiańczuk J., *"Bezpieczne Podlasie" zastąpi dwie dotychczasowe operacje* (Eng. 'Safe Podlasie' will replace two existing operations), Wojska Obrony Terytorialnej, 31 VII 2024, https://media.terytorialsi.wp.mil.pl/informacje/838336/bezpieczne-podlasie-zastapi-dwie-dotychczasowe-operacje [accessed: 6 IV 2025].

Fraszka B., *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje* (Eng. The situation on the Poland-Belarus Border: Background, Geopolitics, Narratives), Warsaw Institute, 23 XII 2021, https://warsawinstitute.org/situation-poland-belarus-border-background-geopolitics-narratives/ [accessed: 14 II 2026].

Jesteśmy z Wami – wyślij kartkę mundurowym na granicy (Eng. We are with you, send a card to the border guards), Poczta Polska, 11 XI 2021, https://media.poczta-polska.pl/releases/jestesmy-z-wami-wyslij-kartke-mundu-rowym-na-granicy#:~:text=Poczta%20Polska%20bezp%C5%82atnie%20przeka%C5%BCe%20takie%20kartki%20s%C5%82u%C5%BCbom,dor%C4%99czane.%20LISTA%20plac%C3%B3wek%20ze%20specjalnymi%20pojemnikami:%20Lp. [accessed: 30 VI 2025].

Jurkowska M., *Masowy szturm na przejście graniczne w Kuźnicy. Mija rok od ataku cudzoziemców na granicę i funkcjonariuszy SG* (Eng. Massive assault on the border crossing in Kuźnica. A year has passed since the attack by foreigners on the border and Border Guard officers), Sokółka Nasze Miasto, 16 XI 2022, https://sokolka.naszemiasto.pl/masowy-szturm-na-przejscie-graniczne-w-kuznicy-mija-rok-od/ar/c1-9090195 [accessed: 11 IV 2025].

Kartka dla obrońców granic (Eng. A card for border defenders), Fundacja Niepodległości, 10 XI 2021, https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2451-kartka-dla-obroncow-granic [accessed: 30 VI 2025].

Kartka dla obrońców granic – nasza akcja się rozszerza (Eng. A card for a border defenders – our action is expanding), Fundacja Niepodległości, 25 XI 2021, https://www.fundacja-niepodleglosci.pl/9-dziaalno/aktualnoci/2456-kartka-dla-obroncow-granic-nasza-akcja-sie-rozszerza [accessed: 30 VI 2025].

Korsak E., *Nowa operacja wojskowa na Podlasiu* (Eng. A new military operation in Podlasie), Polska Zbrojna, 12 VIII 2023, https://polska-zbrojna.pl/home/articleshow/40146?t=Nowa-operacja-wojskowa-na-Podlasiu [accessed: 7 IV 2025].

Kożdoń-Dębecka M., *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych* (Eng. Media polarisation on the example of the migration crisis taking

place on the Polish-Belarusian border in the summer of 2021 in the reports of three Polish television news services), "Media Biznes Kultura" 2023, vol. 14, no. 1, pp. 161–174. https://doi.org/10.4467/25442554.MBK.23.010.18033.

Łozowski M., *Państwowa Straż Pożarna w obronie granic RP* (Eng. The State Fire Service in defence of the borders of the Republic of Poland), Krajowa Sekcja Pożarnictwa, 7 XII 2021, https://kspnszz.org/index.php/2021/12/07/panstwowa-straz-pozarna-w-obronie-granic-rp/ [accessed: 8 IV 2025].

Modernizacja bariery elektronicznej na granicy Polski z Białorusią (WIDEO) (Eng. Modernisation of the electronic barrier on the Polish-Belarusian border (VIDEO)), Telbud S.A., https://telbud.pl/strefa-informacji/modernizacja-bariery-elektronicznej-na-granicy-polski-z-bialorusia-wideo [accessed: 14 II 2026].

Murem za polskim mundurem! (Eng. United behind the Polish Uniform!), prezydent.pl, 13 X 2023, https://www.prezydent.pl/multimedia/wideo/murem-za-polskim-mundurem,1148,33 [accessed: 2 VII 2025].

#MuremZaPolskimMundurem – stanowiska instytucji i organizacji (Eng. United behind the Polish Uniform – positions of the institutions and organisations), Straż Graniczna, 3 XII 2021, https://strazgraniczna.pl/pl/pozostale-informacje/muremzapolskimmundurem/muremzapolskimmundurem/9548,MuremZaPolskimMundurem-stanowiska-instytucji-i-organizacji.html [accessed: 3 VII 2025].

Murem za polskim mundurem (Eng. United behind the Polish uniform), Wojska Obrony Terytorialnej, 21 XI 2021, https://media.terytorialsi.wp.mil.pl/informacje/708475/murem-za-polskim-mundurem [accessed: 3 VIII 2025].

Narodowe Święto Niepodległości – „Dzień szacunku dla munduru" (Eng. National Independence Day – 'Day of respect for the uniform'), Wojsko Polskie, https://www.wojsko-polskie.pl/weterani/articles/aktualnosci-r/narodowe-swieto-niepodleglosci-dzien-szacunku-dla-munduru/ [accessed: 3 VII 2025].

NBP wprowadza banknot kolekcjonerski "Ochrona polskiej granicy wschodniej" (Eng. The National Bank of Poland introduces a collector's banknote entitled 'Protection of the Polish eastern border'), Narodowy Bank Polski, 18 VII 2022, https://nbp.pl/nbp-wprowadza-banknot-kolekcjonerski-ochrona-polskiej-granicy-wschodniej/ [accessed: 1 VII 2025].

Nowa operacja wojskowa na wschodniej granicy: OP Bezpieczne Podlasie (Eng. A new military operation on the eastern border: OP Safe Podlasie), Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-07-176-op-bezpieczne-podlasie/ [accessed: 7 IV 2025].

"Ochrona polskiej granicy wschodniej" na srebrnej monecie NBP (Eng. 'Protection of Poland's eastern border' on a silver coin issued by the National Bank of Poland), Narodowy Bank Polski, 26 I 2022, https://nbp.pl/ochrona-polskiej-granicy-wschodniej-na-srebrnej-monecie-nbp/ [accessed: 1 VII 2025].

Organizatorzy nielegalnego przerzutu migrantów do Polski objęci zachodnimi sankcjami (Eng. Organisers of illegal migrant smuggling to Poland subject to Western sanctions), InfoSecurity24, 27 I 2022, https://infosecurity24.pl/za-granica/organizatorzy-nielegalnego-przerzutu-migrantow-do-polski-objeci-zachodnimi-sankcjami [accessed: 4 VII 2025].

Pietraszczyk M., *Komunikat Przewodniczącego Konferencji Episkopatu Polski wobec eskalacji napięć na granicy polsko-białoruskiej* (Eng. Statement by the President of the Polish Episcopal Conference on the escalation of tensions on the Polish-Belarusian border), Straż Graniczna, 11 XI 2021, https://www.strazgraniczna.pl/pl/pozostale-informacje/duszpasterstwo/rzymskokatolickie/9542,Komunikat-Przewodniczacego-Konferencji-Episkopatu-Polski-wobec-eskalacji-napiec-.html [accessed: 3 VII 2025].

Poczta Polska ze specjalną emisją „#♥ZaPolskimMundurem" poświęconą obrońcom wschodniej granicy (Eng. The Polish Post Office with a special mission 'Behind the Polish uniform' devoted to defenders of the eastern border), Poczta Polska, 27 I 2022, https://www.poczta-polska.pl/news/poczta-polska-ze-specjalna-emisja-%E2%99%A5zapolskimmundurem-poswiecona-obroncom-wschodniej-granicy/ [accessed: 1 VII 2025].

Powiat Garwoliński wspiera służby mundurowe! (Eng. Garwoliński District supports uniformed services!), Starostwo Powiatowe w Garwolinie, https://samorzad.gov.pl/web/powiat-garwolin/zbiorka-slodyczy [accessed: 3 VII 2025].

Rojek-Socha P., Żaczkiewicz-Zborska K., *SN: Sprawa aktorki oskarżonej o zniesławienie Straży Granicznej do ponownego rozpoznania* (Eng. Supreme Court: Case of actress accused of defaming the Border Guard to be re-examined), Prawo.pl, 6 XI 2024, https://www.prawo.pl/prawnicy-sady/sn-sprawa-aktorki-oskarzonej-o-znieslawienie-straz-y-granicznej-do-ponownego-rozpoznania,529890.html [accessed: 27 II 2026].

Statut fundacji „Fundacja Niepodległości" (Eng. Statute of the 'Independence Foundation'), https://www.fundacja-niepodleglosci.pl/images/STATUT_FUNDACJI/Fundacja_Niepodleg%C5%82o%C5%9Bci_Statut_17.11.2021_r.pdf [accessed: 29 VII 2025].

Stępkowski K., *Ks. ppor. Artur Janczarek: nasza posługa na granicy to realizacja przysięgi Wojskowej* (Eng. Priest, second lieutenant Artur Janczarek: our service at the border is the fulfilment of military oath), Ordynariat Polowy, 18 XI 2021, https://archiwum2023-ordynariat.wp.mil.pl/pl/articles/wiadomosci-listopad-2021/ks-ppor-artur-janczarek-nasza-posluga-na-granicy-realizacja-przysiegi-wojskowej/index.html [accessed: 19 VIII 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią w 2021 r.* (Eng. Illegal border crossings with Belarus in 2021), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021r.html [accessed: 1 IV 2025].

Szef BBN na granicy polsko-białoruskiej. Wzmacnianie zabezpieczeń to „dowód ciągłości myśli strategicznej państwa" (Eng. The Head of the National Security Bureau on the Polish-Belarusian border. Strengthening security measures is 'proof of the continuity of the state's strategic thinking), Biuro Bezpieczeństwa Narodowego, 11 X 2024, https://www.bbn.gov.pl/pl/wydarzenia/10003,Szef-BBN-na-granicy-polsko-bialoruskiej-Wzmacnianie-zabezpieczen-to-quotdowod-ci.html [accessed: 5 IV 2025].

Szwed K., *Zakończenie odbioru bariery elektronicznej na granicy polsko-białoruskiej* (Eng. Completion of the acceptance of the electronic barrier on the Polish-Belarusian border), Straż Graniczna, 15 VI 2023, https://www.strazgraniczna.pl/pl/aktualnosci/11875,Zakonczenie-odbioru-bariery-elektronicznej-na-granicy-polsko-bialoruskiej.html [accessed: 5 IV 2025].

Wilczewski Ł., *W tę wigilię zostawmy #WolneMiejsceDlaMunduru* (Eng. On this Christmas Eve, save a seat for the uniform), Wojsko Polskie, https://www.wojsko-polskie.pl/1bot/articles/aktualnosci-w/w-te-wigilie-zostawmywolnemiejscedlamundru/ [accessed: 19 VIII 2025].

Wypowiedź premiera Mateusza Morawieckiego w Sejmie nt. sytuacji na granicy polsko-białoruskiej (Eng. The statement of the Prime Minister Mateusz Morawiecki in the Sejm on the situation on the Polish-Belarusian border), https://www.gov.pl/attachment/f93dffbc-f0ea-48c5-990b-7c01608b2213 [accessed: 2 VII 2025].

Znany aktor Piotr Z. usłyszał zarzuty zniesławienia i znieważenia rzeczniczki Straży Granicznej (Eng. Well-known actor Piotr Z. has been charged with defamation and insulting a spokesperson for the Border Guard), Polska Agencja Prasowa, 31 III 2022, https://www.pap.pl/aktualnosci/news%2C1137489%2Cznany-aktor-piotr-z-uslyszal-zarzuty-znieslawienia-i-zniewazenia [accessed: 27 II 2026].

Legal acts

Act of 29 October 2021 on the construction of state border security (consolidated text, Journal of Laws of 2023, item 1390).

Other documents

Decision No. 148/MON of the Minister of National Defence of 17 October 2022 on the introduction of a special badge named 'For the Protection of the Border of the Republic of Poland', Appendix no. 7: *Special badge regulations 'For the Protection of the Border of the Republic of Poland'* (Journal of Laws of MON of 2022, item 173).

Resolution of the Sejm of the Republic of Poland of 24 July 2024 on expressing appreciation for the service and dedication of soldiers and officers guarding border security of the Republic of Poland (M.P. of 2024, item 737).

Resolution of the Sejm of the Republic of Poland of 17 November 2021 on solidarity in the protection of Polish borders (M.P. of 2021, item 1129).

Norbert Łucarz

Graduated with honours from a first-cycle degree programme in national security at the Faculty of International and Political Studies of the Jagiellonian University. He is currently attending second-cycle studies in the Department of National Security at the Jagiellonian University. Winner of the 'Grants for the Future' competition for distinguished students of the Faculty of International and Political Studies of the Jagiellonian University – support for mobility (4th edition). Member of the representative team of the Jagiellonian University at the fifth edition of the International Forum for Peace, Security and Prosperity. His research interests are hybrid threats, education for security, terrorism.

Contact: norbert.lucarz@student.uj.edu.pl

REVIEW ARTICLES / REVIEWS

Internal Security Review
2026, no. 34, pp. 415–419

https://doi.org/10.4467/20801335PBW.26.019.23381

REVIEW

Szpiegostwo. Studium kryminologiczne, Piotr Chlebowicz[1]

TOMASZ SAFJAŃSKI

Centre for Research on Cross-Border Security
WSB University in Dąbrowa Górnicza

https://orcid.org/0000-0003-1775-8857

A review of the literature on espionage indicates that this threat has been the subject of empirical research relatively rarely. Domestic and foreign academic literature is dominated by theoretical works referring to the historical, political science and legal aspects of this phenomenon. The monograph written by Piotr Chlebowicz entitled *Szpiegostwo. Studium kryminologiczne* (Espionage. Cryminology study) is a pioneering work in this respect, and its publication is of exceptional importance for the development of criminological research on crimes against state security. The author – as the first researcher in Poland – undertook a comprehensive, systematic and empirically based criminological analysis of espionage in the years 1990–2022. He thus filled an important research gap.

[1] P. Chlebowicz, *Szpiegostwo. Studium kryminologiczne* (Eng. Espionage. Criminology study), series: Monografie Prawnicze Warszawa 2025, C.H. Beck, 227 p. The book is available only in Polish.

The issue raised by Chlebowicz is of key importance for national security. The Russian Federation's expansionist policy, aimed at reconstructing the spheres of influence from the Soviet period, is a threat to Poland's raison d'état. In this context, the espionage activities carried out by Russian and Belarusian special services can be seen as an instrument of hybrid warfare and part of potential preparations for armed conflict. Along with the intensification of espionage activities of Russian origin, a qualitative evolution can be observed. It involves expanding the repertoire of methods used and recruiting random individuals, including criminals operating under *espionage as a service* principle. Espionage precedes and supports influence operations bearing the hallmarks of diversion and sabotage. These operations involving both disinformation activities and influencing public opinion, decision-making processes and political structures in Western countries are becoming increasingly important. At the same time, cyber espionage capabilities are being developed with the aim of penetrating ICT systems, obtaining sensitive data and disrupting the functioning of national critical infrastructure. The scale and nature of the activities carried out by the Russian and Belarusian special services require in-depth research and analysis, as well as an adequate response from Polish institutions responsible for security.

The reviewed publication is a summary of the author's more than ten years of research on espionage, based on file and archival research, informal interviews and literature on the subject. The author gained access to operational and court files in espionage cases held in the archives of the Institute of National Remembrance as well as common and military courts. He carefully analysed these documents and reconstructed cases of espionage against Poland, which constitutes an important contribution to the development of research on espionage infiltration and the functioning of the special services. Triangulation of sources – extremely difficult in research involving largely classified content – gives the work a high level of scientific reliability and allows for a multifaceted reconstruction of the operating mechanisms of foreign intelligence services and the identification of patterns of espionage tactics.

The methodological assumptions adopted by the author integrate three perspectives: criminological, forensic and security sciences, which allows espionage to be approached as a multidimensional phenomenon. At the same time, the text remains well-organised and clear. This deserves to be emphasised, as with such a complex subject matter, it is easy to fall into informational chaos.

The monograph's case studies of Belarusian, Russian and German espionage, the phenomenon of walk-in agents, i.e. persons who independently declare their willingness to cooperate with foreign intelligence services, and the process of shaping an agent of influence contribute to the development of existing theoretical

concepts. The author explores both the recruitment process and operational activities, methods of communication, the structure of agency sourcehunting and the security measures used. Works of a similar level of detail are rare even in Anglo-Saxon literature. Chlebowicz also analyses the *modus operandi* of espionage perpetrators, the dark figure of this phenomenon, and areas of interest to foreign intelligence services. He accurately identifies qualitative changes in the activities of the RF and Belarus services after 2014. He discusses legal instruments in the field of combating espionage, taking into account the threats that have emerged following the annexation of Crimea by the RF.

The structure of the monograph follows the logic of a classical scientific argument. The author guides the reader from theoretical foundations to empirical analysis and practical conclusions. The book begins with a chapter in which espionage is treated as a criminological category. Chlebowicz points to definitional problems and the multi-layered nature of this phenomenon, especially its links to political crime. He draws attention to the functions of intelligence that go beyond classical data collection and include influencing political processes or destabilising states. This approach allows further considerations to be placed in a broader political context and shows why traditional criminological approaches are insufficient in the analysis of espionage.

The second chapter discusses the methodology of criminological research on espionage, as well as the state of research in Poland.

The most comprehensive chapter is the third chapter, devoted to the complex causes of espionage, containing a multidimensional analysis of the factors conducive to such activity. Chlebowicz operates both from a macrostructural perspective, referring to geopolitics and changes after 2014, and from a microstructural perspective, analysing the motivations of perpetrators, their psychological conditions and individual life paths. Particularly valuable is the use of the results of 'Slammer' project, concerning the psychology of betrayal, and the study of offerors. This approach goes beyond the classic patterns of espionage research, as it takes into account the rarely described interior dynamics and behaviour patterns of perpetrators.

In the next chapter, the author moves on to the phenomenology of espionage, focusing on specific manifestations of the discussed phenomenon. The issue of the dark figure and the statistical difficulties associated with describing crime have been presented with methodological precision, which is of significant scientific value. The analysis of the most common areas of interest to foreign services, the motivations of perpetrators, and the techniques they use reveal the practical dimension of the theoretical findings described in previous chapters. Also noteworthy is the inclusion of the issue of the borderline between lobbying and

intelligence activities, illustrated by the example of the Mateusz Piskorski case. This shows the difficulties encountered by state authorities in distinguishing between legal political activities and intelligence activities.

The fifth chapter includes case studies – detailed analyses of the cases of Olga Sołomenik, Marek Zieliński, Ryszard Tomaszek and Piotr Hoffmann. The author reconstructs the *modus operandi* of the perpetrators, the circumstances of recruitment, and the activities of counterintelligence, and also indicates the relationships between the individual stages of their activity. The case file material was presented in an orderly manner, with a clear separation between facts and interpretations. This chapter is the most important empirical contribution, as it reveals mechanisms of actions of perpetrators and service in a way that is not possible in theoretical studies.

The sixth chapter concerns instruments for combating espionage and covers legal, operational and political aspects in a comprehensive manner. Chlebowicz describes the properties of individual state institutions, criminal law regulations, obligation to report and the role of the administrative law. It is particularly important to discuss operational and reconnaissance activities, including the institution of the so-called crown spy and analytical procedures. An interesting theme is the presentation of political perspective, especially spy exchanges and the expulsion of diplomats as tools of international policy, as well as cooperation between special services after 1990, with an emphasis on the eastern direction. The whole thing concludes with a reflection on the effectiveness of the Polish anti-espionage system.

Thanks to this structure, the monograph presents the phenomenon of espionage in a multifaceted manner: from definitional analyses, through soundly justified methodology, to the evaluation of the state's activities. The author creates a coherent, empirically grounded theoretical and methodological model that allows for the description and systematisation of the phenomenon of espionage, as well as an explanation of its mechanisms, functions and evolution in the context of contemporary external threats to national security.

The reflections on the theory of espionage deserve special mention. The author synthesises existing approaches and develops his own interpretative proposals, placing espionage in the category of cross-border political crime, the dynamics of which are linked to geopolitics and changes in the security environment. He convincingly argues that espionage is not only a crime in the strict sense of the word, but above all a threat to national security closely linked to geopolitics, the state's security strategy and interests.

The conclusions concerning counter-espionage have great scientific and practical value. Chlebowicz comprehensively discusses the role of criminal law, administrative as well as operational and reconnaissance instruments used to

combat espionage, including an assessment of their usefulness in the context of new espionage threats. Of particular importance are the analysis of the interpretation of Article 130 of the Criminal Code and the discussion of the obligation to report, as well as the presentation of the practical dimension of counterintelligence operational work.

The reviewed monograph meets the criteria for an outstanding work – it is original, empirically grounded, theoretically refined and coherent. It serves as a model for how interdisciplinary research on difficult, sensitive and hitherto marginalised phenomena should be conducted in scientific discourse. It therefore has the potential to become a reference publication in research on espionage and political crime in Poland as well as a point of reference for future studies. For many reasons, it would be worthwhile to translate it into English.

In an era of intensification of hybrid threats, the book by Piotr Chlebowicz should become required reading for criminologists, criminal lawyers, analysts, as well as politicians and others responsible for national security.

Assoc. Prof. Tomasz Safjański,
Professor at the WSB University

Associate Professor in security sciences, doctor of law, specialist in forensic tactics and combating cross-border crime. Deputy director of the Centre for Research Cross-Border Security at the WSB University in Dąbrowa Górnicza.

Contact: tsafjanski@wsb.edu.pl

AWARDED THESES

Internal Security Review
2026, no. 34, pp. 423–441

https://doi.org/10.4467/20801335PBW.26.020.23382

ARTICLE

Communications within the state administration as the foundation of a nation's resilience: the case of Poland[1]

DAVID CYBULSKI

War Studies University

https://orcid.org/0009-0003-9195-4407

Abstract

The purpose of this article is to present the role and current state of communications among the agencies of the modern administration of the Republic of Poland. The article addresses legal, organisational, and technical aspects of communication within the state administration. It highlights serious systemic deficiencies related to the functioning of existing communication systems in the civilian structures of the state, which may affect Poland's ability to respond effectively to emerging threats to national security. The fundamental problem here is the lack of a unified state perspective on the establishment and operation of communication between its various components, namely security agencies,

[1] The article is based on the master's thesis entitled *Łączność i komunikacja administracji państwa w sytuacji zagrożenia bezpieczeństwa narodowego: na przykładzie Polski* (Eng. Communications and connectivity of public administration in situations of national security threat: the case of Poland), which was defended at the Faculty of Political Science and International Studies of the Warsaw University. The author used excerpts from chapters I, II and IV. The thesis was awarded in the 15th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

emergency services, and public administration. It is therefore necessary to urgently modernise the state communications subsystem for crisis management purposes in the context of contemporary challenges.

Keywords electronic communication, telecommunications, emergency communications, crisis management

Introduction

The contemporary national security environment is characterised by evolving threats, including cyber attacks, terrorism as well as hybrid activities. In such circumstances, traditional, linear crisis management models prove inadequate, and the state's ability to respond effectively depends increasingly on the quality of information flow between key actors in the security system. In this context, the communications subsystem takes on particular importance, as it not only provides the technical infrastructure for the operations of the public administration, emergency services and entities responsible for critical infrastructure protection, but is also responsible for the smooth functioning of the entire crisis management system.

The digitalisation of administration and the growing complexity of the threat landscape mean that the effective and secure exchange of information has become essential to countering incidents that affect the functioning of the state, whether physical or digital in nature. At the same time, numerous documents, such as post-audit reports of the Supreme Audit Office, indicate that the current communications systems within the public administration are often not fully adapted to its modern operational and technological realities. This is evident, among other things, in the fragmentation of telecommunications solutions, the lack of a unified information exchange architecture, shortcomings in interoperability, as well as significant susceptibility to design errors or human errors.

The research question is: to what extent is the current public administration communications subsystem resilient to current threats to national security, and what changes could enhance its effectiveness? Answering this question requires treating communications as a complex socio-technical system in which the legal framework, organisational solutions, technologies and user competencies are mutually interdependent. The hypothesis put forward in the article assumes that the existing public administration communications system – developed over the years on a departamental basis (to meet the needs of individual departments

only) and in a piecemeal fashion – does not provide sufficient coherence or resilience against contemporary threats, and that it is possible to identify realistic ways to optimise it.

The article reviews the regulatory framework governing communications for national security purposes, covering both legislation and implementing regulations, as well as selected strategic documents. Furthermore, the main categories of risk were identified and classified – ranging from planning and design errors, through operational issues and restrictions on technological sovereignty, to cybersecurity threats. Subsequently, proposals were put forward for modernisation, covering both the integration of existing systems and the potential of new technologies, as well as the concept of an integrated national communications subsystem.

The following methods were employed: analysis of legal acts, review of the literature on national security and telecommunications, as well as analysis of the technical documentation for selected systems. Examples of solutions implemented in France and Australia were also highlighted. System analysis was also employed to treat the communications subsystem as part of a larger whole – the national security system – and to assess its functioning in terms of coherence, redundancy and resilience. The scope of the analysis has been deliberately limited to communication solutions within the public administration, excluding mass communication between citizens and military communication, which allows for an in-depth examination of the issue from the perspective of state institution.

The article forms part of a broader body of research into the modernisation of national security systems in the context of digital transformation and escalating geopolitical tensions. It argues that the issue of communications – often perceived as a technical domain – should be treated as a strategic element of national security, requiring a coherent public policy and conscious investment decisions. The proposed conclusions and recommendations may serve as a starting point both for further research and for conceptual work relating to the modernisation of the national communications subsystem of the public administration for the purposes of crisis management.

Legal framework

Ensuring the continuous and reliable exchange of information has been recognised in Poland as one of the cornerstones of national security and the efficient functioning of public administration, particularly in crisis situations, emergencies or the threat of armed conflict. As a result, an extensive system of legal acts has been created to regulate the structure, operation and protection of the systems comprising the state's

communications subsystem, covering both government systems and publicly available commercial systems capable of serving as backup communications for state authorities.

Under the *Act of 26 April 2007 on crisis management*, certain communications systems and ICT networks were classified as critical infrastructure (Article 3 point 2(b) and (c)). The Act imposes an obligation to draw up and update crisis management plans, which must also take into account ICT and communications issues (Article 6(5b)), and to establish rules governing the flow of information within the national crisis management system (Article 11(2) point 8). The Act clearly states that communications systems forming part of the critical infrastructure – both government systems and certain commercial systems – are subject to special protection against threats.

The *Act of 10 June 2016 on anti-terrorist activities* regulates the protection of ICT infrastructure against terrorist incidents and the rules governing the exchange of information between public administration bodies and services in the event of such threats. It provides, among other things, for the possibility of temporarily adapting and installing wired and wireless communications systems for the purpose of securing high-risk events, with certain exemptions from building regulations, in order to ensure communications for the relevant services (Article 13). The Act also introduces a system of alert levels and CRP alert levels (relating to Poland's cyberspace), which are declared by order of the Prime Minister. For the communications subsystem, the following tasks are particularly important in relation to the above levels: informing subordinate personnel, verifying the operation of communication systems, intensified monitoring of ICT systems and electronic communications integrity, ensuring that administrators and decision-makers are on duty, reviewing backup ICT infrastructure, as well as implementing post-incident plans at the highest terrorist threat levels[2].

The *Act of 11 March 2022 on the defence of the Homeland* provides a comprehensive description of the state's responsibilities in the field of military security, including matters relating to the organisation of communications for defence purposes. One of the central elements of the Act is the military telecommunications system (Article 17), which connects the Polish Armed Forces and the Ministry of Defence with other public administration bodies and – if necessary – with civil society organisations serving the interests of defence[3]. It is

[2] *Regulation of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels.*

[3] *Regulation of the Minister of National Defence of 20 April 2022 on the operation of the military telecommunications system.*

designed to ensure the functioning of the national security management system and the smooth operation of the state in times of war, external threats and major crises, which requires communications systems to be, among other things, scalable and highly resilient – that is, to maintain their integrity and availability under extreme conditions. The Act also provides for the possibility of placing certain entities of key importance to national defence under military control, including telecommunications operators. In practice, this means that, for example, a mobile phone operator may be placed under military control so that, in the event of a threat, its network remains available for use by the state administration and the armed forces.

The *Act of 12 July 2024 The Electronic Communications Law* sets out the rules governing the operation of the telecommunications and electronic communications market. It also imposes obligations relating to national defence, national security, as well as public safety and order. It requires telecommunications operators to draw up action plans for situations involving specific risks and to ensure the continuity of service provision, and grants the President of the Office of Electronic Communications (UKE) the power to impose specific obligations on them, for example regarding the maintenance of network operations. A key aspect of the state's communications subsystem is the obligation imposed on entrepreneurs to provide services to state authorities in the event of a specific security threat, a state of emergency or war. The Act also requires operators to provide the President of the UKE with information on the telecommunications infrastructure they possess, which is necessary for the development of communications systems for defence and security purposes. This enables the state authorities to plan the use of public networks as part of the security system.

The *Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland* (Article 21 point 6) grants the state authorities the right to temporarily restrict civil rights and freedoms, including the freedom to use communications systems. This allows certain services to be reduced or suspended for the general public in order to ensure that the public administration bodies, the military and the emergency services have priority access to communications. These regulations also make it possible to utilise commercial communications systems as backup links, while limiting public usage of these systems in such a way that the infrastructure does not become overloaded at a critical moment.

The *Act of 5 December 2024 on civil protection and civil defence* which has been in force since 2025, fills the existing regulatory gap in the area of civil defence and streamlines the civil protection system in times of peace, crisis and war. Among other things, it defines the infrastructure necessary for the performance of civil

protection tasks, including communications infrastructure and ICT systems, as a fundamental prerequisite for the effective coordination of activities across different levels of administration. Pursuant to Article 71, a list of communication tools comprising the state administration's communication system has been drawn up: alarm sirens and public address systems, warning systems (including the Regional Warning System), local and national newspapers, radio and television, the ALERT RCB system, warnings sent via digital technologies, as well as the administration's official information services.

One of the key projects provided for in the Act on civil protection and civil defence is National Secure Communications System (hereinafter: SBŁP), which is overseen by the Minister responsible for home affairs (Article 15(1) point 24). The system is intended to serve as an integrated, secure and highly available communications platform for key government bodies, emergency services, civil protection agencies and the armed forces, linking various existing departmental systems via appropriate interfaces and standards. The Act identifies several functional variants of the SBŁP: open system (SBŁP-J), multipoint video conferencing system (SBŁP-V), mobile radio system (SBŁP-M), trunked radio system (SBŁP-T) and satellite communications system (SBŁP-S). All these modules are intended to provide end-to-end encryption and meet the minimum ICT security requirements set by the Council of Ministers, commensurate with the level of threat (Article 78 point 2).

In addition, the *Act of 5 August 2010 on the protection of classified information* sets out the rules governing the processing of classified information in ICT systems. For the communications subsystem, this means that it is necessary to design separate, accredited systems for classified communications, such as classified fixed-line communications systems (SBŁP-N), and, to some extent, SBŁP-M and SBŁP-S. The processing of classified information is permitted only in systems designed for that purpose, including those specifically accredited by the Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW). This makes the distribution of data – such as intelligence or operational information – logistically more challenging, while at the same time enhancing protection against interception. It also necessitates the creation of specialised networks as well as end devices for authorised users.

Risk analysis for the communications subsystem

The communications subsystem of the public administration is one of the cornerstones of crisis management and the national security system in the broadest sense.

It is key to the effective management of personnel and resources, both in terms of prevention and during the response to crisis situations, where the transmission of information via technical means of communication remains a fundamental criterion for integrated resource management[4]. At the same time, there are no alternatives to modern ICT systems, which means that the need for the state to prioritise the development, maintenance and security of these systems is beyond dispute. Without appropriate technological solutions, even the best-prepared and highly specialised administration will not be capable of effectively carrying out its tasks, as it will lack the tools for efficient coordination of activities at the tactical, operational, and strategic levels, which risks deepening the crisis.

The importance of communications systems for national security is confirmed by strategic documents, including the National Security Strategy of 2020. It states that satellite and mobile communications networks form the basis for the exchange of information and are a key component of national security capabilities and the state's preparedness for emergencies[5]. Communications systems have been designated as part of the national critical infrastructure, and the strategic document emphasises the need for the further development of secure, modern telecommunications networks.

The development of communications subsystem in Poland to date has been fragmented and sector-specific. The lack of a comprehensive, top-down programme for building a unified national communications system has meant that individual agencies and services have created their own solutions tailored to current needs and capabilities. As a result, there are systems in place that are often not integrated with one another, either technically or organisationally[6]. The exchange of information between ministries, services and even across different levels of public administration (central, provincial, district and municipal), is hindered. The crisis management system and the national security management system do formally have a defined hierarchical structure, however, the lack of uniform communication both vertical and horizontal creates a risk of decision-making paralysis, duplication of tasks and fragmentation of efforts in the event of a real threat. This is also indicated by the Supreme Audit Office, which in its numerous audit reports pointed to the problem of the lack of a unified digital radio communication system for emergency services

[4] J. Pilżys, *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych* (Eng. Management of communications and data transmission systems in emergency situations), "Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, vol. 8, no. 1, p. 45.

[5] *National Security Strategy of the Republic of Poland 2020*, Warszawa 2020, p. 8.

[6] M. Gawroński, *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego* (Eng. ICT systems supporting the management of the national security system), "Wiedza Obronna" 2014, no. 2–3, pp. 61–63.

and crisis management structures. It assessed that this negatively affects information flow and the effectiveness of operations[7].

An important aspect of developing any ICT system is its proper planning and design. Standards in the field of systems and software engineering, such as ISO/IEC/IEEE 24748-1 standard, cover the entire system life cycle: concept, development, production, utilisation, support and, ultimately, retirement[8]. Each of these stages is closely interrelated, and errors made during the planning phase may accumulate in subsequent phases of the project. In the case of systems of national importance, particularly those with a nationwide scope, incorrect assumptions, underestimation of costs and timelines, the selection of unsuitable partners, failure to analyse users' actual needs, or the decision not to incorporate redundancy may lead to a situation in which the system fails to fulfil its basic function.

One example of such negligence is the fire on the Łazienkowski Bridge in Warsaw in 2015. It caused damage to key fibre optic links, which led to a temporary disconnection from the network for some central government departments, including the Ministry of Defence[9]. In turn, nationwide failures of the Emergency Call Centres dispatch systems in 2021 and 2024 led to a situation in which dispatchers were unable to assign tasks to emergency medical teams in the usual way, and the solution was to record requests manually[10]. These incidents could have had a much milder impact if, at the design stage, provisions had been made for the redundancy of independent channels, alternative transmission routes and procedures for switching between them.

Equally important is how the communications systems are operated. The utilisation phase does not mark the end of the system's life cycle – it is during

---

[7] Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych* (Eng. Report on the results of the inspection: Organisation and preparation for rescue operations on motorways and expressways), 2017, p. 11.

[8] ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

[9] M. Gąsior, *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu* (Eng. Communications systems of the Ministry of National Defence were destroyed in the bridge fire. A few institutions without internet access), naTemat, 15 II 2015, https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [accessed: 18 III 2026].

[10] *Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja* (Eng. The second day of the emergency medical system failure. The Ministry is reassuring the public), TVN24, 15 V 2021, https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [accessed: 18 III 2026]; *Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112* (Eng. Nationwide outage of the 112 Emergency Call Centre), Onet, 16 XII 2024, https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [accessed: 18 III 2026].

day-to-day use that it is put to the test by end-users, while at the same time the experience necessary for its further improvement is gathered. The key role is played by user preparation. If users are not properly trained, and the system interface turns out to be too complex or unintuitive, there is a risk that in practice they will bypass the intended solutions and resort to out-of-system channels. A user's pursuit of convenience in the area of communication can lead, for example, to the use of popular instant messaging applications that are not designed for the exchange of classified information or information regarding crisis situations. In recent years, there have been examples of commercial applications being used to transmit sensitive information, including in the US and Polish administrations, where important decisions were consulted using publicly available services[11]. Such practices undermine information security level and demonstrate that communications systems must be designed taking into account not only technical requirements and security standards but also ergonomics, ease of use and user habits.

Proper operation requires detailed operational procedures and regular exer-cises. The procedures should precisely describe the actions of users and administrators, as well as include contingency plans, modes of operation in the event of partial infrastructure loss, or the occurrence of security incidents. Exercises – including both crisis simulations and stress tests – enable us to verify design assumptions, identify bottlenecks and maintain staff competence at the required level. The lack of exercises, or their cursory nature, leads to a gradual loss of the ability to use systems in non-standard situations. This means that in a real crisis, personnel may spontaneously resort to unauthorised tools, thereby compromising information security and the continuity of the institution's operations.

In the organisational dimension, the issue of technological sovereignty takes on particular significance. The use of hardware and software solutions from third countries poses a risk of losing control over key information security parameters: confidentiality, integrity and availability. Examples of such threats include both government recommendations[12] to avoid using certain foreign security products in critical systems and cases of backdoors being discovered in devices and

[11] J. Goldberg, *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025, https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [accessed: 18 III 2026]; Z. Wanat, *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021, https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [accessed: 18 III 2026].

[12] *Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r.* (Eng. Recommendation from the Government Representative for Cybersecurity of 30 May 2022) (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022, p. 1.

software[13] used for processing sensitive data. Reports of the possibility of remotely compromising advanced military systems or exfiltrating medical data by exploiting vulnerabilities in monitoring devices show that a lack of full control over technology can be exploited to exert political pressure, destabilise healthcare systems or disrupt the operations of the armed forces. In the case of Poland, there is a risk of losing access to transnational data sources, such as NATO and the European Union or its own systems located outside the country (diplomatic missions, satellite constellations). A rational solution is to build redundant, independent communication channels and to develop national capabilities in communications system design and production, which would allow greater independence from foreign suppliers and reduce the risk of technological blackmail.

From a technical perspective, the security and resilience of communications subsystem are based on ensuring specific information security attributes. Standards from the ISO/IEC 27000 family and related standards primarily highlight in this regard confidentiality, integrity, and availability, as well as authenticity, accountability, validity and completeness of data[14]. In the context of state communications, this means that information must be available to authorised entities when needed, cannot be altered or destroyed in an unauthorised manner, must come from reliable sources, and any actions taken on it should be attributable to a specific user or process. In addition, information used in the decision-making process must be up-to-date and complete in order to be processed into reliable operational knowledge. The absence of any of these attributes may lead to incorrect decisions, delays or a complete paralysis of activities.

Furthermore, a major challenge is ensuring interoperability and compatibility of the solutions used. Individual services and state institutions use a variety of systems, frequencies, protocols and standards that are not always consistent with one another. The lack of national standards for emergency communications and a common platform for information exchange means that, in situations requiring cooperation, delays, misunderstandings and interruptions in the flow of data may occur[15]. System fragmentation also increases the scale of an attack – maintaining multiple incompatible solutions makes it difficult to effectively secure and monitor these systems. In the face of a growing number of cyberattacks, including those

[13] *Contec CMS8000 Contains a Backdoor*, CISA 2025, p. 1 et seq.

[14] PN-EN ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, Polski Komitet Normalizacyjny, Warszawa 2012, p. 14, 17.

[15] M. Bieńkowski, *Funkcjonowanie systemu ochrony ludności w Polsce* (Eng. The operation of the civil protection system in Poland), "Kontrola Państwowa" 2019, no. 5, pp. 60–62.

from advanced, state-sponsored APT (advanced persistent threats) groups, an approach is needed in which communications security is viewed as part of the state's constitutional duty to ensure the safety of its citizens, rather than as a cost. This requires the use of strong end-to-end encryption, consistent software updates, network segmentation, the application of the principle of least privilege and solutions for strong, preferably multi-factor, user authentication.

All the risks identified lead to the clear conclusion that Poland should consistently develop a coherent, unified national communications subsystem that integrates existing departmental systems and ensures the secure, resilient and effective exchange of information at all levels of governance as well as cooperation. This marks a shift away from the island model towards a deliberately designed, scalable and redundant architecture, based on national technological capabilities and shared standards. Only in this way can it be guaranteed that, in crisis situations, including hybrid operations or armed conflicts, the state apparatus will be able to effectively carry out its tasks and protect the safety of citizens.

Possibilities for resolving the communication impasse

Currently in Poland, various institutions and ministries use their own solutions, often duplicating each other (e.g. two secure mobile communications systems – CATEL and SKR-Z or several email environments for the same classification levels – CATEL and Classified Email System OPAL) that are not compatible. The lack of unified system and common standards means that information is often exchanged between systems manually, which slows down the response time to emergencies and increases the risk of error.

The lack of uniformity in systems also generates costs and risks at several levels. Firstly, investment outlays multiply – the state finances many parallel projects, which strains the budget and limits funds for infrastructure modernisation or innovations. Secondly, dispersion of systems expands the attack vector: each new platform must be individually monitored, updated, tested and secured, which complicates vulnerability management across the entire administration. Thirdly, this necessitates maintaining a large number of specialists across multiple institutions – individual units must have their own maintenance and security teams, which not only increases costs but also creates situations where staff growth in one institution comes at the expense of weakening another. In this context, the need for a new, integrated approach is becoming increasingly evident – one that, on the one hand, allows for flexibility and meets the specific requirements of different institutions,

and on the other hand, ensures the coherence and interoperability of the entire state communications subsystem.

One possibility is to adopt a layered architecture, inspired by the *European Interoperability Framework*[16]. In such a model, individual institutions could still use their respective interfaces and applications (e.g. different messaging apps, video conferencing platforms or IP telephony systems), but all data exchange would take place through a shared transport and semantic layer (Table 1). Communication functions would be separated from the medium used – the same conversation or message could pass through a cellular network, fibre optic cable, radio or satellite, while maintaining uniform encryption standards and metadata. It would be crucial to implement real-time protocol translators that would automatically convert messages between different formats and protocols without losing information about the sender, recipient, confidentiality level or message priority. This approach would be complemented by intelligent routing mechanisms that select the optimal transmission channel depending on the context – such as the importance of the message, available links, network load or the type of device the recipient has.

Table 1. Concept for the development of an integrated national communications system.

Layer	Description	Examples of standards
Application	Tools tailored to the institution's needs	Threema OnPrem for public authorities, Matrix for security agencies
Semantic	Dictionaries, translators and data exchange schemes	XML GovCore, JSON-LD with EU Vocab ontologies
Transport	Universal protocols for encrypted communication	TLS 1.3, QUIC, SCIP for voice
Physical	Technology-neutral network infrastructure	SD-WAN, 5G NSA, campus networks

Source: own elaboration.

Inspiration for this approach comes from solutions implemented in other countries. The French Tchap system, launched in 2019, is based on open, decentralised Matrix protocol, which allows for building a federated communication

[16] *Europejskie Ramy Interoperacyjności* (Eng. European Interoperability Framework), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [accessed: 30 III 2026].

architecture – each ministry or agency can maintain its own server, retaining control over its data, while at the same time remaining in secure contact with other administrative units[17]. The Matrix protocol also enables the creation of so-called bridges to other platforms (e.g. XMPP, IRC, Slack), which facilitates secure contact with external partners while maintaining security standards and compliance with regulations, such as the eIDAS Regulation[18]. The Tchap system offers, among others, end-to-end encryption, integration with the national electronic identity system and mechanisms for the automatic deletion of messages. Its effectiveness was confirmed during the 33rd Summer Olympic Games in Paris, when there was a significant increase in the number of users, messages sent and chat rooms created for the purpose of coordinating security and logistics[19].

Another example of a solution aimed at secure communication integration of a distributed government structure is Australian GovLINK. The system managed by the Department of Finance creates an encrypted environment for the exchange of information between federal and state agencies as well as selected public and private sector partners[20]. It is based on a federated architecture and common security standards (e.g. S/MIME, X.509), which allows agencies to retain their own systems while utilising uniform mechanisms for authentication, encryption and digital signatures.

Both examples show that open protocols, a federated architecture and robust cryptographic algorithms can effectively overcome the problem of a lack of uniformity across systems while preserving the autonomy of individual institutions.

In the Polish context, the benchmark for this direction of change is the SBŁP project. It is intended to become a multi-layered, integrated system, overseen by the Minister responsible for home affairs. The system is designed to combine various communication channels – from fixed-line and radio networks, through mobile networks, to satellite networks – into a single, coherent communications

---

[17] C. Dussutour, *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [accessed: 19 III 2026].

[18] eIDAS (*Electronic IDentification, Authentication and Trust Services*) – unified standard for electronic identification and trust services of the European Union, operating on the basis of *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

[19] *Tchap, the French administration federation: past, present and future - Julie Ripa*, YouTube, 29 X 2024, https://www.youtube.com/watch?v=m1roliPrNqc [accessed: 19 III 2026].

[20] GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [accessed: 19 III 2026].

environment for the public administration. The most important task of the SBŁP is to ensure the continuity of communications between state authorities both in peacetime and in times of crisis or war, as well as to facilitate interoperability between separate systems within the civil sector, security services and military structures. The project involves identifying several functional components: SBŁP-J, SBŁP-N, SBŁP-V, SBŁP-M, SBŁP-T and SBŁP-S. All of them are based on certified cryptographic solutions.

A key advantage of the SBŁP concept is the ability to utilise existing infrastructure, such as OST112 and GovNet networks, both for open and classified systems. This would help to reduce costs and speed up the implementation of the system. Integration with existing solutions (e.g. the use of CATEL system in the SBŁP-M component) will increase channel redundancy and enable a gradual transition from distributed solutions to a more cohesive architecture. At this stage, however, it has not been revealed whether the SBŁP will be an entirely new system designed from scratch, a collection of modified existing solutions, or a combination of both approaches. There are strong indications that, for economic and organisational reasons, the evolutionary approach may prevail, involving a gradual integration and unification.

Planning and implementing such a transformation requires a phased approach. In the pilot phase, the foundation of a new system can be built based on open protocols (such as Matrix), and a limited number of ministries can be integrated with it, practically testing the interoperability and security mechanisms. The next phase involves expanding the scope to additional institutions and implementing protocol translators for legacy systems, enabling them to exchange information without the need to immediately replace the entire infrastructure (e.g. from TETRA metadata to JSON-LD standard or Matrix to XMPP format). At the same time, it would be advisable to carry out certification of compliance with established security standards (e.g. ISO 27001) and develop common security policies, which could eventually be partially automated. In the long term, integration with communication systems at the European Union level would also be possible, in line with promoted concepts such as GovStack, which envisage building standardised, modular components that can be combined as needed[21].

The benefits of implementing an integrated, interoperable communications system are multifaceted. In addition to reducing response times in crisis situations and enhancing information security, a significant reduction in infrastructure maintenance costs and greater resilience to failures and attacks can be expected. However, achieving success still requires maintaining a balance – the system must

[21] GovStack, https://www.govstack.global/about/ [accessed: 19 III 2026].

be uniform enough for all institutions to cooperate seamlessly, yet modular enough to be adapted to the specific tasks of individual users and to evolve with changes in technology and threats. If the SBŁP is designed as an open, interoperable platform rather than yet another closed, limited-scope departmental system, it could become the foundation for a new standard in national communications.

Summary

Communications subsystem of the public administration is one of the key determinants of a state's resilience to contemporary threats, and its effectiveness results from the simultaneous influence of four factors: legal framework, quality of planning and design processes, technological maturity and competencies of users. Despite the existence of extensive telecommunications infrastructure, the current communications system is not fully integrated, which leads to delays, dysfunctions, and increased vulnerability to disruptions in crisis situations. Thus, the hypothesis regarding the inadequacy of the current communications system in relation to contemporary threats has been confirmed.

In practical terms, a model for optimising the communications subsystem has been proposed, in which diverse systems and transmission media are integrated through coherent planning, organisational and technical layers. This model assumes the use of existing infrastructure resources, their gradual integration, and new functionalities enabling the automatic routing of information traffic through various channels, depending on priority, data sensitivity and the availability of links. Such an approach to modernisation reduces the risk of loss of communications in extreme situations and limits costs by moving away from duplicating solutions in favour of deliberate consolidation.

The article clarifies the criteria for assessing the resilience of communications systems in terms of four complementary dimensions:

1) legal (compliance and completeness of regulations),
2) planning (quality of functional concepts),
3) redundancy (ensuring multi-channel communication),
4) integration (the actual ability of systems to interoperate).

This approach encourages a move away from a simplistic, infrastructure-focused view of communications and allows it to be integrated into mainstream research on the national security system.

Limitations of the study – in particular, the lack of full access to operational data and to the detailed specifications of the SBŁP system under development – highlight the need to continue work on the empirical verification of various options

for integrating existing systems. Further research into federated architectures, protocol translation mechanisms and data exchange standards between security entities for implementation in government communications systems should be considered particularly worthwhile.

The findings of the research lead to an unequivocal conclusion: investment in digital transformation and integration of communications system are not merely a matter of technical modernisation, but a prerequisite for maintaining the state's actual operational capability in the 21st century. The implementation of the presented recommendations may lead to shorter response times for the administration, security and emergency services in crisis situations, which will have a direct impact on the continuity of operations of the public institutions, the protection of the population as well as the maintenance of national stability in the context of growing strategic uncertainty.

Bibliography

Bieńkowski M., *Funkcjonowanie systemu ochrony ludności w Polsce* (Eng. The operation of the civil protection system in Poland), "Kontrola Państwowa" 2019, no. 5, pp. 52–70.

Contec CMS8000 Contains a Backdoor, CISA, 2025.

Gawroński M., *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego* (Eng. ICT systems supporting the management of the national security system), "Wiedza Obronna" 2014, no. 2–3, pp. 47–86.

Pilżys J., *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych* (Eng. Management of communications and data transmission systems in emergency situations), "Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, vol. 8, no. 1, pp. 33–49.

Internet sources

Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja (Eng. The second day of the emergency medical system failure. The Ministry is reassuring the public), TVN24, 15 V 2021, https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [accessed: 18 III 2026].

Dussutour C., *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-

-messaging-service-tchap [accessed: 19 III 2026].

Europejskie Rady Interoperacyjności (Eng. European Interoperability Framework), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [accessed: 30 III 2026].

Gąsior M., *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu* (Eng. Communications systems of the Ministry of National Defence were destroyed in the bridge fire. A few institutions without internet access), naTemat, 15 II 2015, https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [accessed: 18 III 2026].

Goldberg J., *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025, https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [accessed: 18 III 2026].

GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [accessed: 19 III 2026].

GovStack, https://www.govstack.global/about/ [accessed: 19 III 2026].

Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112 (Eng. Nationwide outage of the 112 Emergency Call Centre), Onet, 16 XII 2024, https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [accessed: 18 III 2026].

Tchap, the French administration federation: past, present and future - Julie Ripa, YouTube, 29 X 2024, https://www.youtube.com/watch?v=m1roliPrNqc [accessed: 19 III 2026].

Wanat Z., *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021, https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [accessed: 18 III 2026].

Legal acts

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal of the EU L 257 of 28 VIII 2014).

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

Act of 12 July 2024 The Electronic Communications Law (Journal of Laws of 2024, item 1221,

as amended).

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

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

Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws of 2025, item 1209).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

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

Act of 21 June 2002 on the state of emergency (Journal of Laws of 2017, item 1928).

Regulation of the Minister of National Defence of 20 April 2022 on the operation of the military telecommunications system (Journal of Laws of 2022, item 870).

Regulation of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels (consolidated text, Journal of Laws of 2022, item 2065).

Other documents

ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych* (Eng. Report on the results of the inspection: Organisation and preparation for rescue operations on motorways and expressways), 2017.

PN-EN ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, Polski Komitet Normalizacyjny.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r. (Eng. Recommendation from the Government Representative for Cybersecurity of 30 May 2022) (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022.

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

David Cybulski

Specialist in the field of cybersecurity. He gained professional experience in the private sector and in state administration. Passionate about innovative cybersecurity solutions and new techniques used in cyberattacks by APT groups, with particular emphasis on social engineering attacks. His scientific interests include the protection of critical infrastructure, the activity of selected APT groups, the security aspects of Shadow IT and Cyber Threat Intelligence / Threat Hunting activities towards selected cybercriminal groups.

Contact: dcybulski@proton.me

Contact
phone (+48) 22 58 58 613
e-mail: wydawnictwo@abw.gov.pl

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland