Nr 32 2025
ISSN 2080-1335

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335
e-ISSN 2720-0841

Punkty MEiN: 20

Numer zamknięto i oddano do druku w sierpniu 2025 r.

Printed in August 2025

No. 32 2025
ISSN 2080-1335

INTERNAL SECURITY REVIEW

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

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

Artykuły wyrażają poglądy autorów

Articles express the views of the authors

Deklaracja o wersji pierwotnej / Declaration of the original version

Wersja drukowana czasopisma jest jego wersją pierwotną

The printed version of the journal is the original version

Wersja online czasopisma jest dostępna na stronie: www.abw.gov.pl/wyd/

The online version of the journal is available at: www.abw.gov.pl/pub/

Indeksacja w bazach danych / Indexing in databases

„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)

"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 Science and Humanities, Polish Scientific Bibliography

PBW jest dostępny w Portalu Czasopism Naukowych Uniwersytetu Jagiellońskiego pod adresem: https://www.ejournals.eu/PBW/

The journal is available on the Jagiellonian University Scientific Journals Portal at: https://www.ejournals.eu/PBW/

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

Articles should be submitted via the editorial tab available at: https://ojs.ejournals.eu/PBW/about/submissions

SPIS TREŚCI

ARTYKUŁY RECENZYJNE / RECENZJE

PRACE KONKURSOWE

VARIA

ARTICLES

Szanowni Państwo!

Bezpieczeństwo wewnętrzne to szerokie pojęcie, obejmujące wiele elementów funkcjonowania państwa i życia obywateli. Wpisuje się w nie między innymi bezpieczeństwo publiczne, ustrojowe, społeczne, kulturowe, informacyjne, ekonomiczne, ekologiczne, cyberbezpieczeństwo. Zapewnienie bezpieczeństwa wewnętrznego to jedno z najważniejszych zadań, to fundament stabilności Rzeczpospolitej Polskiej, w której jest możliwy niezakłócony rozwój społeczno-gospodarczy i której znaczenie na arenie międzynarodowej rośnie.

Moją intencją jako redaktora naczelnego „Przeglądu Bezpieczeństwa Wewnętrznego" jest zadbanie o to, aby prezentowane treści ukazywały jak najszerszy zakres zagadnień dotyczących przedmiotowego bezpieczeństwa i były zróżnicowane, a poruszana problematyka – ważka i na czasie. Wspólnie z autorami, pod czujnym okiem recenzentów i członków Rady Naukowej, będziemy dokonywali analiz i ocen i na tej podstawie przedkładali rekomendacje. Wiemy, jak ważną rolę w zapewnianiu bezpieczeństwa i przeciwdziałaniu zagrożeniom odgrywa świadome i wyedukowane społeczeństwo, dlatego chcemy dotrzeć z wiedzą do jak najszerszych kręgów. Obok artykułów naukowych w PBW będą się więc ukazywać wywiady z ekspertami i relacje z warsztatów i konferencji naukowych poświęconych interesującym nas tematom. Ponadto chcemy kontynuować zamieszczanie recenzji książek zawierających treści związane z bezpieczeństwem.

O roli edukacji, ale postrzeganej systemowo, pisze w tym numerze dr hab. Ilona Urych. Jej artykuł jest krytyczną refleksją nad programami kształcenia w zakresie bezpieczeństwa na różnych szczeblach edukacji szkolnej i w uczelniach wyższych.

Jesteśmy w ważnym momencie w kontekście wzmacniania odporności państwa i społeczeństwa. Z początkiem stycznia 2025 r. w Polsce weszła w życie długo wyczekiwana ustawa o ochronie

ludności i obronie cywilnej. Zagadnieniom dotyczącym bezpieczeństwa ludności została poświęcona książka pt. *Mechanizmy ochrony ludności w redukcji ryzyka katastrof. Wybrane zagadnienia*, pod redakcją funkcjonariuszy Straży Pożarnej: Pawła Gromka, Mariusza Feltynowskiego i Moniki Wojakowskiej. Znajomość tej publikacji może pomóc w zrozumieniu istoty ochrony ludności cywilnej w Polsce, na co zwraca uwagę w swojej recenzji dr Julia W. Tocicka. Zachęcam do lektury.

Oczekujemy także na nowelizację ustawy o zarządzaniu kryzysowym, która uwzględni nie tylko zapisy wspomnianej wcześniej ustawy, lecz także wprowadzi przepisy dotyczące unijnego mechanizmu ochrony ludności oraz zaimplementuje do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) o odporności podmiotów krytycznych, czyli dyrektywę CER. W PBW nie mogło więc zabraknąć problematyki związanej z polską infrastrukturą krytyczną. Jej ochronie poświęcono w kraju wiele debat publicznych. W styczniu tego roku wzięłam udział w konferencji „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej". O dobrych praktykach i wyzwaniach w tym obszarze mówią w wywiadzie dla PBW Ireneusz Jabłoński i Piotr Grzybowski z Polskiego Instytutu Kontroli Wewnętrznej, który był organizatorem tego spotkania. Z kolei David Cybulski poruszył w swoim artykule problematykę cyberbezpieczeństwa w sektorze energetyki morskiej i okołomorskiej w kontekście planowanych przez Polskę strategicznych projektów energetycznych na Morzu Bałtyckim.

W tym numerze wiele miejsca poświęcamy również nowoczesnym technologiom. W dziale „Prace konkursowe" prezentujemy tekst Marty Grzywacz na temat transformacji energetycznej związanej z przejściem na czystą energię i roli sektora wodorowego w zachowaniu bezpieczeństwa ekonomicznego państwa. O możliwościach wykorzystania nowoczesnych technologii i narzędzi do wsparcia procesu monitorowania zagrożeń napisali dr Jarosław Przyjemczak i Małgorzata Wolbach. Ten wątek zaistniał również w wywiadzie z kmdr. Sebastianem Kalitowskim, z którym rozmawiałam o ochronie polskich obszarów morskich między innymi przed zagrożeniami hybrydowymi ze strony Federacji Rosyjskiej. Motyw szpiegostwa i innych obcych wpływów jest obecny także w artykule dr. Marka Klasy i Michała Klasy, którzy opisują rosyjską „specjalną operację wojskową" jako nieudany *coup de main*, oraz – w kontekście historycznym –

w pracy konkursowej Szymona Główki analizującej system wywiadu i kontrwywiadu w napoleońskiej Francji.

W ostatnich latach wiele uwagi poświęca się bezpieczeństwu naszych granic. Doktor Łukasz Foryś oraz dr Kornelia Stępień przeanalizowali wpływ kontroli ruchu drogowego na zwalczanie przestępczości transgranicznej. Bezpieczeństwo to także przeciwdziałanie zagrożeniom ekstremistycznym. Patryk Król opisał nowe ruchy antypaństwowe w Polsce, inspirowane amerykańskim ruchem sovereign citizen, i przedstawił propozycje działań prewencyjnych, które mogłyby ograniczyć wpływ tych zjawisk na polskie społeczeństwo.

Zapraszam Państwa także do zapoznania się z wywiadem z insp. dr. Robertem Żółkiewskim, który opowiedział o szansach i możliwościach, jakie daje służba w formacji mundurowej. Jego ciekawe doświadczenia zawodowe mogą stanowić zachętę dla młodych ludzi, którzy chcieliby się poświęcić pracy na rzecz wzmacniania bezpieczeństwa wewnętrznego Polski.

Dziękuję autorom za przedstawienie efektów swoich wysiłków badawczych na łamach PBW i recenzentom za wsparcie w ocenie merytorycznej nadsyłanych treści. Słowa podziękowania kieruję również do członków nowo utworzonej Rady Naukowej oraz do zespołu redakcyjnego.

Redaktor naczelny
dr Daria Olender

ARTYKUŁY

Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 15–33

 https://doi.org/10.4467/20801335PBW.25.001.22167

ARTYKUŁ

Bezpieczeństwo jako kategoria edukacyjna. Współczesne tendencje

Security as an educational category. Contemporary trends

ILONA URYCH

Akademia Sztuki Wojennej

https://orcid.org/0000-0003-4868-9460

Abstrakt Celem artykułu jest omówienie współczesnych tendencji w podejściu do bezpieczeństwa jako kategorii edukacyjnej. Scharakteryzowano w nim, na czym polega nauka o bezpieczeństwie w ramach przedmiotu szkolnego „edukacja dla bezpieczeństwa" i programów kształcenia klas wojskowych. Zaprezentowano też ofertę edukacyjną uczelni wyższych dotyczącą problematyki bezpieczeństwa. Ponadto przedstawiono postawy nauczycieli zajmujących się kształceniem w zakresie bezpieczeństwa wobec wyzwań współczesnej edukacji. Zmiany w środowisku bezpieczeństwa generują konieczność prowadzenia badań naukowych dotyczących edukacji o bezpieczeństwie, w tym o charakterze eksploracyjnym i utylitarnym. Zdobyta wiedza powinna stanowić bodziec do weryfikacji treści kształcenia związanych z bezpieczeństwem oraz służyć wypracowaniu nowych procedur na rzecz bezpieczeństwa państwa.

Słowa kluczowe edukacja, bezpieczeństwo, edukacja dla bezpieczeństwa, klasy wojskowe, nauczyciel, nauki o bezpieczeństwie

Abstract

The aim of the article is to discuss contemporary trends in the approach to security as an educational category. The article characterises what security science entails within the framework of the school subject 'education for security' and in the education programmes of military classes. The educational offer of higher education institutions addressing security-related topics was also presented. Moreover, the study discussed the attitudes of teachers involved in education in the field of security in the face of the challenges of modern education. Changes in the security environment generate the need to conduct scientific research on education on security, including exploratory and utilitarian studies. The acquired knowledge should constitute a trigger for evaluation of the content of security-related education and serve to develop new procedures for state security.

Keywords

education, security, education for security, military classes, teacher, security sciences

Wprowadzenie

Od początku inwazji Rosji na Ukrainę powstają prace naukowe oraz ekspertyzy poświęcone potencjałowi obronnemu obu państw, Unii Europejskiej, a także wielowymiarowym aspektom wojny[1]. Warto zauważyć, że ta problematyka badawcza skłania nie tylko do refleksji nad bezpieczeństwem w wymiarze międzynarodowym, narodowym czy personalnym, lecz także nad potrzebami edukacyjnymi w tym zakresie.

Słowo „bezpieczeństwo" pochodzi od łacińskiego słowa *securites*, będącego pochodną wyrażenia *sine cura*, czyli „bez pieczy". Wskazuje ono na pierwotność poczucia zagrożenia względem poczucia bezpieczeństwa[2]. Oznacza to, jak dowodzi

[1] Zob. np. A. Pacholczak, *Analiza krytyczna efektywności unijnych sankcji finansowych zastosowanych wobec Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, nr 30, s. 97–129. https://doi.org/10.4467/20801335PBW.24.004.19606; M. Zadorożna, M. Butuc, *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, „Security and Defence Quarterly" 2024, nr 46(2), s. 47–65. https://doi.org/10.35467/sdq/189686; Z. Wiktor, *Wojna w Ukrainie – przyczyny i skutki po ponad roku trwania*, „Studia Orientalne" 2023, R. 12, nr 3(27), s. 30–59. https://doi.org/10.15804/so2023302; K. Maciejewska-Mieszkowska, *Eskalacja wojny w Ukrainie jako czynnik determinujący poczucie zagrożenia bezpieczeństwa Polski w ocenie społecznej*, „Środkowoeuropejskie Studia Polityczne" 2023, nr 2, s. 217–236. https://doi.org/10.14746/ssp.2023.2.12.

[2] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 15.

Wojciech Multan, że dopóki nie zagraża nam utrata bezpieczeństwa, dopóty nie zdajemy sobie sprawy, czym ono jest[3]. Z kolei Ryszard Zięba podkreśla, że eksplorując istotę bezpieczeństwa, warto mieć na uwadze jego związek ze zjawiskiem zagrożenia[4]. Według badacza bezpieczeństwo to (…) *pewność istnienia i przetrwania, stanu posiadania oraz funkcjonowania i rozwoju podmiotu*[5]. Jednocześnie zaznacza on, że owa pewność jest skutkiem nie tylko braku zagrożeń, lecz także działalności danego podmiotu. Zdaje się więc, że jest ona zmienna w czasie, a zatem ma charakter procesu społecznego[6].

Bezpieczeństwo jako konstrukt społeczny jest wyodrębniane zwłaszcza w ramach podejścia konstruktywistycznego, charakterystycznego dla tzw. szkoły kopenhaskiej i uczonych skupionych wokół Barry'ego Buzana i Olego Wævera w niefunkcjonującym już Kopenhaskim Instytucie Badań nad Pokojem. Buzan po zakończeniu zimnej wojny postulował potrzebę uwzględniania w analizach bezpieczeństwa nie tylko suwerennych państw, lecz także niepaństwowych zbiorowości ludzkich. Wyróżnił on pięć sektorów bezpieczeństwa: wojskowy, polityczny, ekonomiczny, społeczny oraz ekologiczny i propagował wyodrębnianie kolejnych płaszczyzn[7]. Potrzebę zmian w rozumieniu tego pojęcia zauważył również Wæver. Podkreślał znaczenie opartej na dualizmie konceptualizacji bezpieczeństwa, które w przypadku państw dotyczy ochrony suwerenności, a w odniesieniu do grup społecznych – zachowania ich tożsamości[8].

Różne aspekty bezpieczeństwa są analizowane także w polskim środowisku naukowym[9]. Zainteresowanie bezpieczeństwem można zaobserwować również

---

[3] W. Multan, *Bezpieczeństwo międzynarodowe ery nuklearnej*, Warszawa 1991, s. 22.

[4] R. Zięba, *Teoria bezpieczeństwa*, w: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*, R. Zięba, S. Bieleń, J. Zając (red. nauk.), Warszawa 2015, s. 91.

[5] Tamże, s. 87.

[6] J. Kukułka, *Narodziny nowych koncepcji bezpieczeństwa*, Warszawa 1994, s. 40–41.

[7] B. Buzan, *New Patterns of Global Security in the Twenty-First Century*, „International Affairs" 1991, t. 67, nr 3, s. 433.

[8] O. Wæver, *Securization and Desecurization*, w: *On Security*, R.D. Lipschutz (red.), New York 1995.

[9] Zob. np. S. Koziej, *Wstęp do teorii i historii bezpieczeństwa*, https://koziej.pl/wp-content/uploads/2018/12/BM-Cz-I-Podstawy-ewolucja-i-koncepcje.pdf [dostęp: 14 I 2025]; S. Sulowski, *O rozwoju badań i postulacie interdyscyplinarności w naukach o bezpieczeństwie*, w: *Tożsamość nauk o bezpieczeństwie*, S. Sulowski (red.), Toruń 2015, s. 33; *Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje*, J. Pawłowski (red. nauk.), Warszawa 2015; R. Wróblewski, *Wprowadzenie do nauk o bezpieczeństwie*, Siedlce 2017; A. Glen, *Podstawy poznania bezpieczeństwa podmiotu. Aksjologia, ontologia, epistemologia, metodologia*, Siedlce 2021; B. Wiśniewski, *Praktyczne aspekty bezpieczeństwa*, Warszawa 2020; *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, R. Jakubczak, J. Marczak (red.), Warszawa 2011.

w dziedzinie edukacji[10]. Celem artykułu jest omówienie współczesnych tendencji w podejściu do bezpieczeństwa jako kategorii edukacyjnej. W związku z przyjętym celem sformułowano cztery problemy badawcze:

1. Na czym polega nauka o bezpieczeństwie w przedmiocie szkolnym „edukacja dla bezpieczeństwa"?
2. Czym cechuje się nauka o bezpieczeństwie w programach kształcenia klas wojskowych?
3. Czym charakteryzują się treści programowe dotyczące bezpieczeństwa w ofercie edukacyjnej uczelni wyższych?
4. Jaka jest specyfika postawy nauczyciela treści kształcenia związanych z bezpieczeństwem wobec wyzwań współczesnej edukacji?

Zgodnie z celem badań i problemami badawczymi, które są związane z opisem i diagnozą, a nie z badaniami weryfikacyjnymi, zrezygnowano z formułowania hipotez badawczych, które mogłyby wywrzeć wpływ na wynik przeprowadzonych badań[11]. Sytuacja problemowa była rozpatrywana w kategorii poznawczej, dlatego zastosowano następujące metody badań: analizę, syntezę, wnioskowanie i abstrahowanie[12] oraz analizę i krytykę piśmiennictwa[13]. Przeprowadzone badania ulokowano w dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie[14].

Nauka o bezpieczeństwie w ramach przedmiotu szkolnego „edukacja dla bezpieczeństwa"

Nauka o bezpieczeństwie jest realizowana w ramach przedmiotu szkolnego „edukacja dla bezpieczeństwa". Chociaż samo pojęcie edukacji dla bezpieczeństwa pojawiło się już w 1994 r. podczas badań przeprowadzonych w Akademii Obrony Narodowej nad systemem bezpieczeństwa narodowego[15], to dopiero w 2009 r. został

[10] Zob. np. A. Pieczywok, *Przestrzeń edukacji dla bezpieczeństwa człowieka wobec niepewności i zagrożeń jego egzystencji*, Bydgoszcz 2022; D. Kaźmierczak, M. Szumiec, *Człowiek we współczesnym świecie. Bezpieczeństwo, zdrowie, edukacja*, Kraków 2021; I. Urych, A. Orzyłowska, *Wiedza o bezpieczeństwie w procesie dydaktycznym. Kontynuacja i rozwój myśli pedagogicznej*, Warszawa 2020; K. Krakowski, A. Gębczyńska, *Uwarunkowania dydaktyczne przygotowania obronnego państwa*, Warszawa 2018.

[11] M. Łobocki, *Metody i techniki badań pedagogicznych*, Kraków 2016.

[12] M. Pelc, *Elementy metodologii badań naukowych*, Warszawa 2012, s. 55–78.

[13] J. Pieter, *Zarys metodologii pracy naukowej*, Warszawa 1975, s. 103.

[14] A. Misiuk, *O tożsamości nauk o bezpieczeństwie*, „Historia i Polityka" 2018, nr 23(30), s. 9–19. https://doi.org/10.12775/HiP.2018.001.

[15] J. Świniarski, *Edukacja dla bezpieczeństwa jako najnowsza koncepcja wychowania metawojskowego i metaobronnego czasów globalizacji*, w: *Współczesne trendy w edukacji dla bezpieczeństwa. Kształcenie – wychowanie – motywowanie*, T. Szczurek (red.), Warszawa 2011, s. 21.

wprowadzony przedmiot szkolny pod tą nazwą[16]. Zastąpił on przysposobienie obronne. Było to podyktowane zmianą charakteru zagrożeń z militarnych na niemilitarne. Istotą nowego przedmiotu było kompleksowe ujęcie zagadnień bezpieczeństwa z koncentracją działań edukacyjnych na problematyce zagrożeń w czasie pokoju, a także sposobach zachowań w sytuacjach kryzysowych, zwłaszcza w środowisku lokalnym.

Sposób realizacji przedmiotu „edukacja dla bezpieczeństwa" w wymiarze 30 godzin w szkole ponadpodstawowej określało od 1 września 2009 r. rozporządzenie Ministra Edukacji Narodowej[17]. Po kolejnej reformie edukacji, zgodnie z którą zniesiono szkoły gimnazjalne, a wydłużono czas edukacji w szkołach: podstawowej i ponadpodstawowej[18], od 1 września 2017 r. przedmiot „edukacja dla bezpieczeństwa" stał się obowiązkowy także w klasie VIII szkoły podstawowej w wymiarze jednej godziny tygodniowo. Treści kształcenia dotyczyły bezpieczeństwa państwa, organizacji działań ratowniczych, edukacji zdrowotnej i zasad udzielania pierwszej pomocy[19].

Kolejna zmiana w nauczaniu o bezpieczeństwie w ramach przedmiotu „edukacja dla bezpieczeństwa" zaczęła obowiązywać od roku szkolnego 2022/2023. Powód zmian podstawy programowej kształcenia ogólnego dla szkoły podstawowej i szkół ponadpodstawowych w zakresie edukacji dla bezpieczeństwa został określony następująco: *Wzrastające zagrożenie bezpieczeństwa państwa wymaga uzupełniania celów kształcenia i treści nauczania przedmiotu edukacja dla bezpieczeństwa o kwestie związane z obronnością państwa, nabyciem umiejętności strzelectwa oraz przygotowaniem uczniów do radzenia sobie z zagrożeniami wywołanymi działaniami wojennymi oraz podstawami ratownictwa taktycznego*[20]. Tym samym zrezygnowano z działu dotyczącego edukacji zdrowotnej ujętego w poprzedniej podstawie programowej dla przedmiotu „edukacja dla bezpieczeństwa"

---

[16] *Rozporządzenie Ministra Edukacji Narodowej z dnia 28 sierpnia 2009 r. w sprawie sposobu realizacji edukacji dla bezpieczeństwa*.

[17] Tamże.

[18] *Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej*.

[19] *Rozporządzenie Ministra Edukacji Narodowej z dnia 14 czerwca 2017 r. zmieniające rozporządzenie w sprawie sposobu realizacji edukacji dla bezpieczeństwa*.

[20] *Uzasadnienie do rozporządzenia w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia*, s. 3. Tekst uzasadnienia jest dostępny na stronie: https://www.gov.pl/web/nauka/edukacja-dla-bezpieczenstwa--rozporzadzenia-podpisane [dostęp: 4 I 2025].

na rzecz nowego działu. W szkole podstawowej wprowadzono „kształtowanie postaw obronnych", a w szkole ponadpodstawowej – „edukację obronną", realizowaną w celu opanowania m.in. umiejętności strzeleckich[21]. Są to zmiany, dzięki którym przedmiot „edukacja dla bezpieczeństwa" będzie zawierać elementy budowania sprawności obronnych społeczeństwa.

W roku szkolnym 2024/2025 kontynuowano idee wprowadzone do nauki bezpieczeństwa. Od tego roku już od pierwszych klas odbywają się systematyczne szkolenia z pierwszej pomocy. Przekazywana na nich wiedza ma być pogłębiana na kolejnych etapach edukacji. W podstawie programowej dla klas I–III szkoły podstawowej zagadnienia z udzielania pierwszej pomocy są częścią wymagań z obszaru pod nazwą „osiągnięcia w zakresie funkcji życiowych człowieka, ochrony zdrowia, bezpieczeństwa i odpoczynku". Na dalszych etapach kształcenia nauka pierwszej pomocy ma być realizowana podczas zajęć z wychowawcą, który – co ciekawe – ma podejmować decyzję o tematyce i liczbie godzin przeznaczonych na to zagadnienie. Wiedza na temat pierwszej pomocy ma być przekazywana systematycznie, dzięki czemu będzie mogła być lepiej przyswajana i utrwalana. Zajęcia mają mieć charakter praktyczny, a przy tym kształcić takie postawy, jak odpowiedzialność za innych i gotowość do niesienia pomocy oraz podnosić świadomość znaczenia szybkiej reakcji w sytuacjach zagrożenia życia[22].

Nauka o bezpieczeństwie w programach kształcenia klas wojskowych

Treści dotyczące bezpieczeństwa zawierają się też w programach kształcenia klas wojskowych[23]. Tym mianem określa się dzisiaj w Polsce klasy w szkołach średnich,

[21] Szkoły, które na terenie danego powiatu miały dostęp do broni kulowej, pneumatycznej, replik broni strzeleckiej (ang. *air soft gun*, ASG), strzelnic wirtualnych albo laserowych, miały obowiązek kształcenia umiejętności strzeleckich od roku szkolnego 2022/2023. Szkoły na terenie powiatu, które takiego dostępu nie miały, realizowały ten wymóg w miarę możliwości w latach szkolnych 2022/2023 i 2023/2024.

[22] *Rozporządzenie Ministra Edukacji z dnia 20 maja 2024 r. w sprawie ramowych planów nauczania dla publicznych szkół.*

[23] Treści dotyczące bezpieczeństwa znajdują się też w programach kształcenia innych klas mundurowych, np.: policyjnych, pożarniczych, Straży Granicznej, Służby Więziennej czy Służby Celnej. Niemniej jednak żaden z typów tych klas nie ma instytucjonalnie określonego i spójnego programu edukacyjnego, co oznacza, że te klasy funkcjonują w ramach innowacji pedagogicznych specyficznych dla danych szkół. Tylko klasy wojskowe, występujące wcześniej w formule certyfikowanych wojskowych klas mundurowych, a obecnie oddziałów przygotowania wojskowego, mają spójny dla wszystkich program kształcenia, dlatego w tym artykule właśnie ich program został uwzględniony.

które oprócz programu kształcenia przyjętego w danej szkole realizują program edukacji dla bezpieczeństwa, wzbogacony o tematykę związaną z obronnością kraju, historią oręża polskiego oraz kształtowaniem postaw patriotycznych młodzieży. Atrakcyjne programy kształcenia sprzyjają osiąganiu ambitnych celów dydaktycznych i wychowawczych w obszarze bezpieczeństwa[24].

Współcześnie klasy wojskowe mogą funkcjonować w formułach[25]: innowacji pedagogicznych z zakresu kształcenia obronnego (od 2002 r.)[26], certyfikowanych wojskowych klas mundurowych (od 2017 r.)[27] oraz oddziałów przygotowania wojskowego (od 2020 r.)[28]. Wielość tych form kształcenia może powodować pewne trudności w rozeznaniu się w nich. W celu wskazania współczesnych tendencji kształcenia z obszaru bezpieczeństwa krótko scharakteryzowano oddziały przygotowania wojskowego jako efekt ostatniej reorganizacji klas wojskowych[29].

Oddziały przygotowania wojskowego zaczęły funkcjonować w szkołach ponadpodstawowych od 1 września 2020 r.[30] Był to rezultat prac nad wprowadzeniem rozwiązania systemowego dotyczącego funkcjonowania klas wojskowych. Rozwiązanie to było oparte na wnioskach i doświadczeniach płynących z kolejnych edycji pilotażowego programu realizowanego w wojskowych certyfikowanych klasach mundurowych. Składały się na niego: 185 godzin lekcyjnych na zajęciach teoretycznych i praktycznych oraz pięciodniowy obóz w warunkach poligonowych w ramach przedmiotu „edukacja wojskowa".

---

[24] Na temat celów i programów edukacji w klasach wojskowych zob. szerzej: I. Urych, *Military Innovations in Secondary Schools in Poland as a Manifestation of Strengthening National Security within the Meaning of Articles 5 and 26 of the Polish Constitution,* „Przegląd Prawa Konstytucyjnego" 2020, nr 6(58), s. 461–474. https://doi.org/10.15804/ppk.2020.06.37; L. Kanarski i in., *Wstępna diagnoza funkcjonowania klas mundurowych – wyniki badań pilotażowych*, w: *Klasy mundurowe. Od teorii do dobrych praktyk*, A. Skrabacz, I. Urych, L. Kanarski (red.), Warszawa 2016, s. 71–82.

[25] Zob. szerzej: I. Urych, *Współczesne paradygmaty kształcenia obronnego młodzieży*, „Bellona" 2022, nr 3(210), s. 113–126.

[26] Innowacje pedagogiczne – nowatorskie rozwiązania programowe, organizacyjne lub metodyczne, które mają na celu poprawę jakości pracy szkoły. Zob. § 1 pkt 1 *Rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 9 kwietnia 2002 r. w sprawie warunków prowadzenia działalności innowacyjnej i eksperymentalnej przez publiczne szkoły i placówki*.

[27] Zob. *Pilotażowy program wspierania szkół ponadgimnazjalnych prowadzących piony Certyfikowanych Wojskowych Klas Mundurowych*, Ministerstwo Obrony Narodowej.

[28] Zob. Program szkolenia w oddziałach przysposobienia wojskowego, załącznik do *Rozporządzenia Ministra Obrony Narodowej z dnia 21 maja 2020 r. w sprawie szkolenia w oddziale przygotowania wojskowego*.

[29] *Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Prawo oświatowe oraz ustawy o finansowaniu zadań oświatowych*.

[30] Tamże.

Program nauczania w oddziałach przygotowania wojskowego zgodnie z rozporządzeniem Ministra Obrony Narodowej obejmuje szkolenie w formie 180 godzin obowiązkowych zajęć edukacyjnych. Część teoretyczna to 70 godzin lekcyjnych w szkole, a część praktyczna – 60 jednostek lekcyjnych prowadzonych w patronackiej jednostce wojskowej. Szkolenie kończy 50-godzinny obóz szkoleniowy odbywany na początku ostatniego roku nauki. Zezwolenie na prowadzenie oddziału przygotowania wojskowego wydaje minister obrony narodowej na wniosek organu prowadzącego szkołę[31]. Po wyrażeniu zgody minister udziela wsparcia finansowego w postaci dotacji celowych. Zakres udzielanej pomocy jest ściśle określony i obejmuje: ubiór uczniów (został opracowany jego wzór), doposażenie w sprzęt niezbędny do prowadzenia zajęć, prowadzenie oddziału (np. dowóz uczniów na zajęcia do jednostek wojskowych), inwestycję infrastrukturalną w szkole (np. strzelnica pneumatyczna lub tor sprawności fizycznej)[32]. Warunkiem uzyskania dotacji jest minimum 22 uczniów w oddziale. Udziela się jej w roku otwarcia pierwszego oddziału, a zakupione mienie ma służyć placówce w następnych latach. O kolejną dotację szkoła może ubiegać się po czterech latach od otrzymania pierwszego finansowania.

Uczniowie kształcący się w oddziałach przygotowania wojskowego oprócz zdobycia wiedzy i umiejętności odpowiednich do pierwszego etapu szkolenia żołnierza Sił Zbrojnych RP mają możliwość odbycia skróconej służby przygotowawczej, a w konsekwencji – pozostania żołnierzem rezerw osobowych Sił Zbrojnych RP, lub wstąpienia do czynnej służby wojskowej. Dodatkowo absolwent takiego oddziału może odbyć 12-dniowe szkolenie podstawowe, po którym może otrzymać dodatkowe punkty w rekrutacji do uczelni wojskowych.

Warto przytoczyć uzasadnienie tworzenia takich oddziałów:

> Możliwość tworzenia w szkołach oddziałów przygotowania wojskowego, jako rozwiązanie systemowe, stanowi wyjście naprzeciw oczekiwaniom i potrzebom społecznym, oraz zwiększenie upowszechniania edukacji w zakresie obronności, do czego resort obrony narodowej przykłada szczególną wagę. Rezultatami, jakie Ministerstwo Obrony Narodowej chce osiągnąć, jest zasilenie rezerw osobowych Sił Zbrojnych, Wojsk Obrony Terytorialnej ochotnikami, w dalszej perspektywie czasowej zwiększenie liczebności Sił Zbrojnych, a także wzmocnienie edukacji obronnej w społeczeństwie[33].

[31] Tamże, art. 28a ust. 6.

[32] *Rozporządzenie Ministra Obrony Narodowej z dnia 7 sierpnia 2020 r. w sprawie wsparcia dla organu prowadzącego oddział przygotowania wojskowego*.

[33] *Oddziały przygotowania wojskowego*, Wojsko Polskie, https://www.wojsko-polskie.pl/zostan-zolnierzem/odzialy-przygotowania-wojskowego/ [dostęp: 5 I 2025].

Treści programowe z zakresu bezpieczeństwa w ofercie edukacyjnej uczelni wyższych

Treści programowe związane z bezpieczeństwem występują także w szkolnictwie wyższym. Utworzono nowe kierunki studiów, m.in.: bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, bezpieczeństwo międzynarodowe, bezpieczeństwo informacyjne. Są to również treści przekazywane w ramach wielu studiów podyplomowych (edukacja dorosłych). Można tu wymienić takie kierunki, jak: edukacja dla bezpieczeństwa, międzynarodowe stosunki wojskowe, służby specjalne czy doskonalenie zawodowe w zakresie realizacji szkolenia w oddziałach przygotowania wojskowego[34].

Treści dotyczące bezpieczeństwa, które są przekazywane na studiach licencjackich i magisterskich, zarówno w trybie stacjonarnym, jak i niestacjonarnym, obejmują szeroki zakres elementów teoretycznych oraz praktycznych współczesnego bezpieczeństwa, rozumienia jego zagrożeń oraz prewencji w tym zakresie. Absolwenci takich studiów powinni dysponować zasobem wiedzy i umiejętności z szeroko pojętego bezpieczeństwa, potrzebnym do zrozumienia zasad funkcjonowania państwa, jego systemów bezpieczeństwa, roli instytucji i organów odpowiedzialnych za zapewnienie bezpieczeństwa narodowego, wewnętrznego, międzynarodowego czy cyberbezpieczeństwa. Ponadto zdobywają kompetencje w zakresie planowania i organizacji oraz kierowania ludźmi, które są niezbędne w stanach zagrożenia. Absolwenci mogą być zatrudniani w administracji rządowej i samorządowej, gdzie są realizowane zadania dotyczące przygotowań obronnych, utrzymania gotowości obronnej i ciągłości funkcjonowania państwa, analizowania i prognozowania zagrożeń bezpieczeństwa narodowego lub międzynarodowego, a także przeciwdziałania innego rodzaju zagrożeniom[35]. Absolwenci kierunków studiów związanych z bezpieczeństwem to także przyszli pracownicy np.: Ministerstwa Obrony Narodowej, Ministerstwa Spraw Zagranicznych, służb specjalnych, Policji, Straży Granicznej, Straży Miejskiej, Żandarmerii Wojskowej, Rządowego Centrum Bezpieczeństwa, Wojsk Obrony Terytorialnych, Polskiego Instytutu Spraw Międzynarodowych i innych podmiotów naukowo-analitycznych czy instytucji UE.

Treści programowe związane z bezpieczeństwem są również przekazywane na kursach specjalistycznych (doskonalenie zawodowe i edukacja ustawiczna)

[34] *Oferta studiów podyplomowych (rok akademicki 2024/2025)*, Akademia Sztuki Wojennej, https://www.wojsko-polskie.pl/aszwoj/studia-podyplomowe/ [dostęp: 5 I 2025].

[35] *Bezpieczeństwo narodowe i obrona powszechna*, Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/bezpieczenstwo-narodowe-licencjackie/ [dostęp: 7 I 2025].

będących w ofercie edukacyjnej uczelni wyższych, w których kładzie się nacisk na tę problematykę. Dla przykładu, w Akademii Sztuki Wojennej są prowadzone kursy obronne przeznaczone dla osób kierujących wykonywaniem zadań obronnych i realizujących te zadania w administracji publicznej bądź u przedsiębiorców, na których nałożono obowiązek realizacji zadań obronnych. Głównym celem takich kursów jest (…) *zapoznanie uczestników z zasadami dotyczącymi bezpieczeństwa i obronności, elementami polityki bezpieczeństwa oraz organizacją i zasadami funkcjonowania systemu obronnego państwa pod kątem roli poszczególnych uczestników w systemie obronnym RP*[36].

W ofercie uczelni wyższych treści programowe związane z bezpieczeństwem są przekazywane również na studiach doktoranckich w dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie. Warto przypomnieć, że zgodnie z obowiązującymi uwarunkowaniami prawnymi kształcenie doktorantów może odbywać się wyłącznie w szkołach doktorskich[37].

Nowy model edukacji zawierający treści programowe związane z bezpieczeństwem w ofercie edukacyjnej uczelni wyższych wymaga zmiany sposobu kształcenia i oparcia go na „nowej kulturze uczenia się"[38]. Zgodnie z paradygmatami nowoczesnej edukacji jego istotą powinien być proces samodzielnego zdobywania wiedzy w wyniku podjętej aktywności badawczej. Nowoczesna uczelnia wyższa powinna wykorzystywać potencjał intelektualny zarówno nauczycieli akademickich, jak i studentów, umożliwiać im efektywne uczenie się, poznawanie oraz zrozumienie współczesnej rzeczywistości. Warto zwrócić uwagę, że obecnie kształcone umiejętności, przekazywana wiedza i wartości mogą się różnić od potrzeb, które wystąpią w przyszłości. Dlatego edukacja wyższa w poszczególnych dziedzinach bezpieczeństwa powinna w jak największym stopniu temu zapobiec, antycypować oczekiwania przyszłości, przygotowywać studentów i kursantów na różne zagrożenia, jakie mogą przynieść dynamicznie zmieniające się realia. To sprawia, że lista obszarów bezpieczeństwa jest otwarta i wymaga dalszych poszukiwań poznawczych i badawczych, a nauczyciel akademicki to osoba nie tylko ucząca innych, lecz także edukująca się sama.

---

[36] *Szkoła Administracji Obronnej*, Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/szkola-administracji-obronnej/ [dostęp: 7 I 2025].

[37] *Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce*, art. 198 ust. 1–5.

[38] J. Szymaniak, *Pojęcie kultury i wspólnotowości szkolnej. „Nowa kultura uczenia się"*, „Studia Gdańskie. Wizje i rzeczywistość" 2014, t. 11, s. 28–42.

Nauczyciel zajmujący się kształceniem na temat bezpieczeństwa wobec wyzwań współczesnej edukacji

W rozważaniach na temat bezpieczeństwa jako kategorii edukacyjnej trudno nie odnieść się bezpośrednio do roli nauczycieli odpowiedzialnych za proces dydaktyczno-wychowawczy w szkołach podstawowych i średnich oraz do nauczycieli akademickich. Od ich doświadczenia, wiedzy i umiejętności w znacznym stopniu zależy efektywność edukacji. Trafnie sformułował tę myśl Ryszard Stępień: *Wiodącą rolę w tak pojętej edukacji powinni pełnić odpowiednio przygotowani nauczyciele, których zadaniem jest przekazanie uczniom takiego zasobu wiedzy i umiejętności, który umożliwi im podejmowanie skutecznych działań i trafnych decyzji* (…). *Dzięki temu młodzież po ukończeniu szkoły wejdzie w dorosłe życie dobrze przygotowana nie tylko do wypełniania obowiązków zawodowych, ale i do zapewnienia bezpieczeństwa sobie i innym*[39].

Przy analizie literatury przedmiotu[40] pod kątem postawy nauczyciela przekazującego treści związane z bezpieczeństwem wobec wyzwań współczesnej edukacji warto zwrócić uwagę na opinię ekspertów w tym zakresie[41]. Podkreślają oni, że wyzwaniem współczesnej edukacji są predyspozycje kandydatów do zawodu nauczyciela edukacji dla bezpieczeństwa, klas wojskowych czy wykładowców na studiach wyższych bądź kursach związanych z bezpieczeństwem. Podstawowa wydaje się tu pasja do nauczanego przedmiotu. Ponadto w tej roli najbardziej pożądani byliby praktycy, którzy dobrze znają teorię i zasady prowadzenia tego typu zajęć, lub nauczyciele po przeszkoleniu wojskowym. Istotne są również ich morale oraz reprezentowanie przez nich wartości proobywatelskich i prospołecznych, a także inne cechy dobrego nauczyciela, jak: silna motywacja wewnętrzna, życzliwość i wysoka kultura osobista.

---

[39] R. Stępień, *Teoretyczne zagadnienia edukacji dla bezpieczeństwa*, w: *Materiały z konferencji: edukacja dla bezpieczeństwa dzieci i młodzieży*, R. Stępień (red.), Warszawa 1999, s. 15.

[40] Zob. np. I. Urych, A. Orzyłowska, *Wiedza o bezpieczeństwie*…; *Nauczyciel szkoły wyższej w procesie dydaktyczno-wychowawczym. Implikacje teoretyczne i praktyczne*, I. Urych (red. nauk.), Warszawa 2019; I. Urych, *Potencjał obronny klas wojskowych. Teoretyczno-empiryczne aspekty kształcenia obronnego*, Warszawa 2019; I. Urych, A. Orzyłowska, *Nauczyciel klas mundurowych. Wyzwania i oczekiwania podmiotów publicznych wobec pedagogów*, w: *Edukacja jutra. Formy wzbogacania wychowania i zmniejszania zagrożeń społecznych*, A. Kamińska, P. Oleśniewicz (red. nauk.), Warszawa 2019, s. 119–131.

[41] Analiza jakościowa materiału empirycznego stanowiącego fragment większych badań dotyczących diagnozowania szeroko pojętego potencjału klas mundurowych o profilu wojskowym. Wśród ekspertów byli przedstawiciele wojskowego środowiska akademickiego, urzędnicy Ministerstwa Obrony Narodowej nadzorujący merytorycznie proces edukacji w klasach wojskowych, dyrektorzy szkół, w których działają klasy mundurowe, oraz nauczyciele tych klas. Badania przeprowadzono wśród 12 ekspertów, wykorzystano w nich metodę sondażu diagnostycznego i technikę wywiadu.

Reprezentanci wojskowego środowiska naukowego uważają, że istotnym uzupełnieniem przygotowania do zawodu nauczyciela, który edukuje w zakresie omawianych treści, jest opanowanie wojskowej metodyki nauczania w ramach kursów organizowanych w centrach i ośrodkach szkolenia Ministerstwa Obrony Narodowej lub ukończenie podstawowego szkolenia wojskowego. Cenne byłoby przygotowanie formalne w postaci kursów i studiów podyplomowych z szeroko rozumianej edukacji dla bezpieczeństwa i edukacji obronnej, a także zapewniających przygotowanie pedagogiczne, psychologiczne i metodyczne.

Eksperci krytycznie odnoszą się natomiast do przygotowania nauczycieli na podstawie wiedzy internetowej, z pominięciem zasadnych doktryn, regulaminów i instrukcji. Pojawiają się opinie, że proces przygotowania do zawodu nauczycieli przekazujących treści związane z bezpieczeństwem powinien być analogiczny do edukacji nauczycieli przedmiotów zawodowych. Ponadto stałe dokształcanie się nauczycieli powinno być wspomagane przez platformy e-learningowe, na których znalazłyby się wszystkie potrzebne i systematycznie aktualizowane wiadomości na temat kształcenia zwłaszcza klas wojskowych. Innymi słowy, wyzwaniem współczesnej edukacji jest zapewnienie nauczycielom dostępu do odpowiedniej wiedzy teoretycznej i praktycznej niezbędnej w ich pracy dydaktycznej.

Na temat przygotowania nauczycieli przekazujących treści związane z bezpieczeństwem nasuwają się dwa rozwiązania kładące nacisk na różne etapy ich kształcenia. Pierwsze z nich, łatwiejsze do zrealizowania, podkreśla potrzebę zorganizowania dalszego, stałego edukowania nauczycieli, i przygotowania dla nich bogatej oferty kursów, szkoleń, studiów podyplomowych, również w formie zdalnej. Drugie ma nowatorski charakter i zakłada utworzenie rozbudowanego programu kształcenia nauczycieli zapewniającego rzetelne przygotowanie pedagogiczne oraz wiedzę z ogólnie pojmowanego bezpieczeństwa i obronności. Takie studia mogłyby być prowadzone wspólnie przez kilka uczelni i tym samym wzbogacać proces przygotowania przyszłych nauczycieli o przedsięwzięcia badawcze, specjalizacje i wzajemne staże, które podniosłyby potencjał twórczy (efekt synergii), a także sprzyjałyby modernizacji i optymalizacji systemu kształcenia nauczycieli przekazujących treści związane z bezpieczeństwem.

Kolejne wyzwanie współczesnej edukacji dotyczy samoświadomości kadr dydaktycznych. Nauczyciele edukacji dla bezpieczeństwa, klas wojskowych czy na studiach wyższych bądź kursach związanych z bezpieczeństwem swoimi postawami wobec zawodu uwidaczniają brak zrozumienia dla powinności swojej profesji, czyli przekazywania wiedzy, umiejętności i wzorów zachowania, żeby podmioty edukowane, a także różne grupy społeczne, do których należą te podmioty, mogły się rozwijać. Innymi słowy, przed kadrą dydaktyczną stoi wyzwanie nabycia lub zwiększenia samoświadomości co do oczekiwań, jakie mają wobec niej państwo

i społeczeństwo. Zauważalny jest przy tym brak szerszego spojrzenia na role społeczne odgrywane przez nauczycieli, które mają wpływ na kształtowanie postaw i światopoglądu uczniów, co w szerszej perspektywie wpływa m.in. na politykę obronną państwa, zaangażowanie społeczne czy budowanie społeczeństwa obywatelskiego. Ponadto należy wspomnieć o niskim poziomie kompetencji społecznych osób wykonujących ten zawód i ich przywiązaniu do tradycyjnego encyklopedyzmu.

Współczesny nauczyciel zmaga się również z wieloma ogólnymi problemami. W 2019 r. Centrum Badania Opinii Społecznej przeprowadziło badanie, w którym respondenci wskazywali najbardziej poważane przez nich zawody. Największym uznaniem wśród polskiego społeczeństwa cieszy się strażak (94% badanych Polaków wskazało ten zawód jako cieszący się dużym poważaniem społecznym). Na drugim miejscu znajduje się pielęgniarka (89% wskazań dużego poważania)[42]. Oba te zawody cechują się wysoką użytecznością społeczną, gdyż niesienie pomocy innym jest wpisane w ich istotę. Ciekawe jest to, że te cechy można przypisać również nauczycielowi, tymczasem jego zawód nie znajduje się na szczycie rankingu – zajął siódme miejsce (77% wskazań dużego poważania). Warto dodać, że w stosunku do lat 80. XX w. można zaobserwować spadek dużego poważania społecznego dla profesora akademickiego (o 7 punktów procentowych) i nauczyciela w ogóle (o 4 punkty procentowe). Największe spadki uznania odnotowano w latach 90. XX w. Optymizmem napawa to, że w ostatnich latach odnotowano niewielki, ale jednak wzrost uznania dla pracy nauczyciela[43]. Wydaje się, że prestiż poszczególnych zawodów w pewnej mierze jest kształtowany przez sytuację na rynku pracy, a ta – w przypadku zawodu nauczyciela – nie jest satysfakcjonująca.

Wnioski

Refleksja nad zagadnieniem podjętym w artykule wynika z obserwacji dotyczącej rozważań nad bezpieczeństwem z perspektywy edukacyjnej zarówno w dyskursie publicznym, jak i w debacie naukowej. Celem artykułu było omówienie współczesnych tendencji związanych z rozpatrywaniem bezpieczeństwa jako kategorii edukacyjnej. Przeprowadzona analiza umożliwiła udzielenie odpowiedzi na postawione problemy badawcze oraz sformułowanie następujących wniosków:

1. Pierwotna potrzeba bycia bezpiecznym, a więc dążenie do przetrwania i rozwoju, implikuje działania edukacyjne, których celem jest wspieranie wychowanków w kształtowaniu jakości życia adekwatnie do ideałów

[42] M. Omyła-Rudzka, *Które zawody poważamy*, „Komunikat z badań CBOS" 2019, nr 157.

[43] Tamże, s. 7.

dydaktyczno-wychowawczych przyjętych w danym społeczeństwie. Edukacja jako zamierzony proces zmian rozwojowych podmiotów edukowanych obejmuje procesy wychowania i kształcenia, a zatem działania sprzyjające rozwojowi jednostek, osiąganiu przez nie pożądanej wiedzy i umiejętności, a także kształtowaniu postaw oraz aktywności na rzecz dobra wspólnego, czyli bezpieczeństwa w wymiarze: indywidualnym i zbiorowym, lokalnym i państwowym, przestrzennym i proceduralnym.

2. Różnorodność oczekiwań wobec nauki o bezpieczeństwie w przedmiocie szkolnym „edukacja dla bezpieczeństwa", klasach wojskowych, na studiach wyższych bądź kursach związanych z bezpieczeństwem może stanowić przesłankę do przygotowania programów kształcenia dla kandydatów na nauczyciela specjalizującego się nie tylko w danym przedmiocie lub etapie edukacyjnym, lecz szerzej – w dyscyplinie nauki o bezpieczeństwie.
3. Nauczyciel zajmujący się kształceniem na temat bezpieczeństwa wobec wyzwań współczesnej edukacji przyjmuje różne postawy – od tych mających na celu stałe podnoszenie swoich kompetencji i wypracowywanie coraz skuteczniejszych metod pracy po bierność, brak rozwoju i przekazywanie wyuczonej wiedzy opartej na encyklopedyzmie. Druga wymieniona postawa może świadczyć o tym, że kadra dydaktyczna zarówno edukacji etapu podstawowego, średniego, jak i wyższego skupia się jedynie na czerpaniu korzyści finansowych i innych profitów z wykonywanej pracy. W takiej sytuacji zostaje zatracona fundamentalna powinność edukacji o bezpieczeństwie, dla bezpieczeństwa i w bezpieczeństwie jako wkładu do wieloaspektowego wysiłku społeczeństw do trwania i rozwoju.
4. Zarysowana złożoność problematyki bezpieczeństwa jako kategorii edukacyjnej jest przesłanką do prowadzenia permanentnych badań naukowych w tym obszarze. Powinny one mieć przy tym cel nie tylko eksploracyjny, lecz także utylitarny – zdobyta wiedza teoretyczna może stanowić imperatywy zmian treści kształcenia związanych z bezpieczeństwem. Wydaje się, że konieczne jest również nadanie tej wiedzy charakteru operacyjnego, niezbędnego do zastosowania w formie powszechnie obowiązujących procedur. Będą one efektywnymi wzorcami zachowania w sytuacjach kryzysowych dla wyedukowanych już obywateli, ale także dla instytucji o charakterze pomocowym, służb, administracji rządowej i samorządowej, a szerzej – różnych podmiotów działających na rzecz bezpieczeństwa. Tym samym staną się wyznacznikiem ich działalności statutowej. Wobec tego jest pożądane, żeby wyniki badań w dyscyplinie nauki o bezpieczeństwie służyły wypracowaniu procedur, które eliminowałyby relacje społeczno-polityczne oparte na podziałach i dyskryminacji,

wskazujących na warstwy podporządkowujących i podporządkowanych, czyli służyły ustanowieniu takich samych praw i obowiązków każdego obywatela na rzecz bezpieczeństwa państwa.

Prezentowane w artykule treści nie wyczerpują złożonej problematyki bezpieczeństwa jako kategorii edukacyjnej, ale naświetlają pewne tendencje we współczesnych uwarunkowaniach tej sfery *praxis* i *doctrina*. Tym samym – w zamyśle autorki – mogą zainspirować praktyków do refleksji na temat złożoności procesów edukacyjnych dotyczących bezpieczeństwa, a teoretyków – do dalszych badań. Poruszone kwestie stanowią wyzwanie, zwłaszcza dla edukatorów, których badania i praktyka dydaktyczna dotyczą bezpieczeństwa. Sprostanie wyzwaniom często nie jest łatwe, ale zgodne z ideą bezpieczeństwa jako naczelnej potrzeby, wartości i celu każdego realnego bytu. Poczucie bezpieczeństwa jest potrzebne do przetrwania tego bytu, jego funkcjonowania, rozwoju i realizacji interesów, zarówno indywidualnych, jak i kolegialnych[44].

Bibliografia

Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie, R. Jakubczak, J. Marczak (red.), Warszawa 2011.

Buzan B., *New Patterns of Global Security in the Twenty-First Century*, „International Affairs" 1991, t. 67, nr 3, s. 431–451. https://doi.org/10.2307/2621945.

Glen A., *Podstawy poznania bezpieczeństwa podmiotu. Aksjologia, ontologia, epistemologia, metodologia*, Siedlce 2021.

Kanarski L., Koter M., Loranty K., Urych I., *Wstępna diagnoza funkcjonowania klas mundurowych – wyniki badań pilotażowych*, w: *Klasy mundurowe. Od teorii do dobrych praktyk*, A. Skrabacz, I. Urych, L. Kanarski (red.), Warszawa 2016, s. 71–82.

Kaźmierczak D., Szumiec M., *Człowiek we współczesnym świecie. Bezpieczeństwo, zdrowie, edukacja*, Kraków 2021.

Krakowski K., Gębczyńska A., *Uwarunkowania dydaktyczne przygotowania obronnego państwa*, Warszawa 2018.

Kukułka J., *Narodziny nowych koncepcji bezpieczeństwa*, Warszawa 1994.

[44] *Bezpieczeństwo*, w: *Słownik terminów z zakresu bezpieczeństwa*, J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (red. nauk.), Toruń 2020, s. 20–21.

Łobocki M., *Metody i techniki badań pedagogicznych*, Kraków 2016.

Maciejewska-Mieszkowska K., *Eskalacja wojny w Ukrainie jako czynnik determinujący poczucie zagrożenia bezpieczeństwa Polski w ocenie społecznej*, „Środkowoeuropejskie Studia Polityczne" 2023, nr 2, s. 217–236. https://doi.org/10.14746/ssp.2023.2.12.

Misiuk A., *O tożsamości nauk o bezpieczeństwie*, „Historia i Polityka" 2018, nr 23(30), s. 9–19. https://doi.org/10.12775/HiP.2018.001.

Multan W., *Bezpieczeństwo międzynarodowe ery nuklearnej*, Warszawa 1991.

Nauczyciel szkoły wyższej w procesie dydaktyczno-wychowawczym. Implikacje teoretyczne i praktyczne, I. Urych (red. nauk.), Warszawa 2019.

Omyła-Rudzka M., *Które zawody poważamy*, „Komunikat z badań CBOS" 2019, nr 157.

Pacholczak A., *Analiza krytyczna efektywności unijnych sankcji finansowych zastosowanych wobec Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, nr 30, s. 97–129. https://doi.org/10.4467/20801335PBW.24.004.19606.

Pelc M., *Elementy metodologii badań naukowych*, Warszawa 2012.

Pieczywok A., *Przestrzeń edukacji dla bezpieczeństwa człowieka wobec niepewności i zagrożeń jego egzystencji*, Bydgoszcz 2022.

Pieter J., *Zarys metodologii pracy naukowej*, Warszawa 1975.

Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje, J. Pawłowski (red. nauk.), Warszawa 2015.

Słownik terminów z zakresu bezpieczeństwa, J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (red. nauk.), Toruń 2020.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

Stępień R., *Teoretyczne zagadnienia edukacji dla bezpieczeństwa*, w: *Materiały z konferencji: edukacja dla bezpieczeństwa dzieci i młodzieży*, R. Stępień (red.), Warszawa 1999.

Sulowski S., *O rozwoju badań i postulacie interdyscyplinarności w naukach o bezpieczeństwie*, w: *Tożsamość nauk o bezpieczeństwie*, S. Sulowski (red.), Toruń 2015.

Szymaniak J., *Pojęcie kultury i wspólnotowości szkolnej. „Nowa kultura uczenia się"*, „Studia Gdańskie. Wizje i rzeczywistość" 2014, t. 11, s. 28–42.

Świniarski J., *Edukacja dla bezpieczeństwa jako najnowsza koncepcja wychowania metawojskowego i metaobronnego czasów globalizacji*, w: *Współczesne trendy w edukacji dla bezpieczeństwa. Kształcenie – wychowanie – motywowanie*, T. Szczurek (red.), Warszawa 2011, s. 7–43.

Urych I., *Military Innovations in Secondary Schools in Poland as a Manifestation of Strengthening National Security within the Meaning of Articles 5 and 26 of the Polish Constitution*, „Przegląd Prawa Konstytucyjnego" 2020, nr 6(58), s. 461–474. https://doi.org/10.15804/ppk.2020.06.37.

Urych I., *Potencjał obronny klas wojskowych. Teoretyczno-empiryczne aspekty kształcenia obronnego*, Warszawa 2019.

Urych I., *Współczesne paradygmaty kształcenia obronnego młodzieży*, „Bellona" 2022, nr 3(210), s. 113–126. https://doi.org/10.5604/01.3001.0016.1952.

Urych I., Orzyłowska A., *Nauczyciel klas mundurowych. Wyzwania i oczekiwania podmiotów publicznych wobec pedagogów*, w: *Edukacja jutra. Formy wzbogacania wychowania i zmniejszania zagrożeń społecznych*, A. Kamińska, P. Oleśniewicz (red. nauk.), Warszawa 2019, s. 119–131.

Urych I., Orzyłowska A., *Wiedza o bezpieczeństwie w procesie dydaktycznym. Kontynuacja i rozwój myśli pedagogicznej*, Warszawa 2020.

Wæver O., *Securization and Desecurization*, w: *On Security*, R.D. Lipschutz (red.), New York 1995.

Wiktor Z., *Wojna w Ukrainie – przyczyny i skutki po ponad roku trwania*, „Studia Orientalne" 2023, R. 12, nr 3(27), s. 30–59. https://doi.org/10.34862/rmb.2023.2.5.

Wiśniewski B., *Praktyczne aspekty bezpieczeństwa*, Warszawa 2020.

Wróblewski R., *Wprowadzenie do nauk o bezpieczeństwie*, Siedlce 2017.

Zadorożna M., Butuc M., *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, „Security and Defence Quarterly" 2024, nr 46(2), s. 47–65. https://doi.org/10.35467/sdq/189686.

Zięba R., *Teoria bezpieczeństwa*, w: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*, R. Zięba, S. Bieleń, J. Zając (red. nauk.), Warszawa 2015.

Źródła internetowe

Bezpieczeństwo narodowe i obrona powszechna, Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/bezpieczenstwo-narodowe-licencjackie/ [dostęp: 7 I 2025].

Koziej S., *Wstęp do teorii i historii bezpieczeństwa*, https://koziej.pl/wp-content/uploads/2018/12/BM-Cz-I-Podstawy-ewolucja-i-koncepcje.pdf [dostęp: 14 I 2025].

Oddziały przygotowania wojskowego, Wojsko Polskie, https://www.wojsko-polskie.pl/zostanzolnierzem/odzialy-przygotowania-wojskowego/ [dostęp: 5 I 2025].

Oferta studiów podyplomowych (rok akademicki 2024/2025), Akademia Sztuki Wojennej, https://www.wojsko-polskie.pl/aszwoj/studia-podyplomowe/ [dostęp: 5 I 2025].

Szkoła Administracji Obronnej, Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/szkola-administracji-obronnej/ [dostęp: 7 I 2025].

Akty prawne

Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Prawo oświatowe oraz ustawy o finansowaniu zadań oświatowych (t.j. DzU z 2019 r. poz. 1681, 2248).

Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (t.j. DzU z 2024 r. poz. 1571, ze zm.).

Rozporządzenie Ministra Edukacji z dnia 20 maja 2024 r. w sprawie ramowych planów nauczania dla publicznych szkół (DzU z 2024 r. poz. 781).

Rozporządzenie Ministra Obrony Narodowej z dnia 7 sierpnia 2020 r. w sprawie wsparcia dla organu prowadzącego oddział przygotowania wojskowego (DzU z 2020 r. poz. 1390).

Rozporządzenie Ministra Obrony Narodowej z dnia 21 maja 2020 r. w sprawie szkolenia w oddziale przygotowania wojskowego (DzU z 2020 r. poz. 977).

Rozporządzenie Ministra Edukacji Narodowej z dnia 14 czerwca 2017 r. zmieniające rozporządzenie w sprawie sposobu realizacji edukacji dla bezpieczeństwa (DzU z 2017 r. poz. 1239).

Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (DzU z 2017 r. poz. 356).

Rozporządzenie Ministra Edukacji Narodowej z dnia 28 sierpnia 2009 r. w sprawie sposobu realizacji edukacji dla bezpieczeństwa (DzU z 2009 r. nr 139 poz. 1131).

Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 9 kwietnia 2002 r. w sprawie warunków prowadzenia działalności innowacyjnej i eksperymentalnej przez publiczne szkoły i placówki (DzU z 2002 r. nr 56 poz. 506).

Inne dokumenty

Pilotażowy program wspierania szkół ponadgimnazjalnych prowadzących piony Certyfikowanych Wojskowych Klas Mundurowych, Ministerstwo Obrony Narodowej.

Uzasadnienie do rozporządzenia w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, https://www.gov.pl/web/nauka/edukacja-dla-bezpieczenstwa--rozporzadzenia-podpisane [dostęp: 4 I 2025].

Dr hab. Ilona Urych, prof. ASzWoj

Doktor habilitowany nauk o bezpieczeństwie, prodziekan ds. studenckich Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej. Prowadzi szkolenia dla kadry cywilnej i wojskowej na temat doskonalenia pedagogicznego oraz przywództwa i kompetencji społecznych. Przedmiotami jej zainteresowań są: edukacja wojskowa, edukacja dla bezpieczeństwa, bezpieczeństwo społeczne, bezpieczeństwo zdrowotne, przywództwo, psychologia bezpieczeństwa, interdyscyplinarność nauk o bezpieczeństwie.

Kontakt: i.urych@akademia.mil.pl

Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 35–51

 https://doi.org/10.4467/20801335PBW.25.002.22168

ARTYKUŁ

Kontrola ruchu drogowego a zwalczanie przestępczości transgranicznej

Traffic control and the fight against cross-border crime

ŁUKASZ FORYŚ

Akademia Policji w Szczytnie

https://orcid.org/0000-0003-1241-8722

KORNELIA STĘPIEŃ

Akademia Policji w Szczytnie

https://orcid.org/0000-0002-8804-0765

Abstrakt

Przestępczość transgraniczna, pomimo licznych działań podejmowanych przez podmioty odpowiedzialne za zapewnienie bezpieczeństwa, stanowi poważne wyzwanie dla służb. Celem artykułu jest omówienie przestępczości transgranicznej z perspektywy funkcjonariusza pełniącego służbę na drodze oraz wskazanie – na podstawie przeglądu literatury i danych statystycznych – znaczenia kontroli ruchu drogowego w zwalczaniu tej przestępczości. Autorzy wskazują, jaki wpływ na tę przestępczość ma swobodny przepływ w strefie Schengen i Unii Europejskiej.

Słowa kluczowe

bezpieczeństwo, przestępczość transgraniczna, kontrola, ruch drogowy, strefa Schengen, Unia Europejska

Abstract

Cross-border crime, despite numerous actions taken by entities responsible for ensuring security, poses a serious challenge for law enforcement agencies. The aim of this article is to analyse cross-border crime from the perspective of an officer serving on the road and to indicate – based on a review of literature and statistical data – the importance of traffic control in combating this crime. The authors point out the impact of free movement within the Schengen area and the European Union on this type of crime.

Keywords

security, cross-border crime, control, traffic, Schengen area, European Union

Wprowadzenie

Unijna polityka dotycząca transportu wspiera budowanie nowoczesnej sieci infrastruktury, która zapewnia zarówno bezpieczniejsze, jak i szybsze podróżowanie. Promuje przy tym wdrażanie cyfrowych rozwiązań, które z jednej strony wpływają na usprawnienie łańcuchów transportowych i łatwiejsze przemieszczanie się z wykorzystaniem różnych środków transportu, lecz z drugiej – umożliwiają popełnianie przestępstw.

Transport jest niezbędnym elementem życia każdego człowieka. Z informacji publikowanych przez Komisję Europejską (KE) wynika, że w latach 2011–2019 udział samochodów osobowych w transporcie pasażerskim w UE spadł z 73,1% do 69,8%. W 2020 r. udział ten wzrósł do 81,9%, a w 2021 r. nieznacznie spadł do 79,7%. Udział statków powietrznych w tym transporcie wzrósł z 10,9% w 2011 r. do 15% w 2019 r., ale spadł do 5,7% w 2020 r., a w 2021 r. wyniósł 7,3%. W przypadku pozostałych rodzajów transportu odnotowano podobne wzorce – gwałtowny spadek w 2020 r., a następnie częściowe ożywienie w 2021 r.[1] Zmiany w 2020 r. były następstwem kryzysu związanego z pandemią COVID-19. Wpłynął on na ogólne wykorzystanie transportu oraz spowodował, że chętniej wybierano samochody prywatne niż środki transportu publicznego. Podobną zależność można zauważyć w związku z wojną w Ukrainie. Ludzie, którzy masowo uciekali z terenów zagrożonych, decydowali się głównie na transport drogowy. Jest to najpopularniejszy rodzaj transportu zarówno wśród osób prywatnych, jak i w przedsiębiorstwach. Wpływa na to

[1] *Statistics Explained*, Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=456757 [dostęp: 10 XII 2024].

rozbudowana sieć dróg, łatwy dostęp do pojazdów samochodowych i możliwość sprawnego przewożenia dużych ilości ładunków w jednym czasie. Pojazdy od lat są wykorzystywane także do działalności przestępczej, np. do przemytu narkotyków, ludzi, towarów, dzieł sztuki, egzotycznych zwierząt itp., a także do zamachów terrorystycznych, co w ostatnich latach jest szczególnie widoczne[2]. Sporadyczne kontrole ruchu drogowego są czynnikiem, który zachęca grupy przestępcze do korzystania właśnie z tej gałęzi transportu z uwagi na niskie ryzyko ujawnienia ich działań.

Transport odgrywa ponadto ważną rolę w europejskiej gospodarce. Stanowi ponad 9% wartości dodanej brutto w Unii Europejskiej, a w usługach transportowych jest zatrudnionych blisko 11 mln ludzi[3]. Polityka UE, wraz ze wzrostem mobilności społeczeństw, wspiera systemy transportu w rozwiązywaniu ich głównych problemów, dotyczących m.in. infrastruktury, kongestii, bezpieczeństwa, zanieczyszczeń. W celu ich eliminowania KE podejmowała liczne działania, w tym utworzenie w ciągu ostatniej dekady jednolitego europejskiego obszaru transportu. Miało temu służyć zniesienie barier między rodzajami transportu i systemami krajowymi, usprawnienie integracji czy ułatwienie procesu powstawania międzynarodowych i multimodalnych operatorów[4].

Stale zwiększa się liczba podmiotów świadczących usługi w branży transportowej na skalę światową, między którymi powstaje coraz więcej zależności. Na system globalnej gospodarki mają wpływ zmiany zarówno w samej gospodarce, jak i w innych dziedzinach, co doprowadziło do zauważalnego zwiększenia roli państw azjatyckich, zwłaszcza Chin i Indii, w gospodarce światowej, włączenia się gospodarek Europy Środkowo-Wschodniej w światowy obieg gospodarczy, znacznego spadku kosztów transportu, wielostronnej liberalizacji handlu, deregulacji rynków telekomunikacyjnych, szybkiego postępu we wdrażaniu osiągnięć technik informacyjnych i telekomunikacyjnych[5]. W obliczu zmieniającej się rzeczywistości podmioty odpowiedzialne za zapewnienie bezpieczeństwa muszą analizować podejmowane działania, doskonalić obowiązujące procedury, umiejętności oraz wprowadzać nowe technologie, które pozwolą na przeciwdziałanie przestępczości.

Kontrola ruchu drogowego najczęściej jest kojarzona z działaniami podejmowanymi przez uprawnione organy, np. policję, w celu zapewnienia bezpieczeństwa

---

[2] Na przykład od 14 VII 2016 r. do 1 XI 2017 r. doszło do co najmniej siedmiu dżihadystycznych ataków z wykorzystaniem pojazdu (14 VII 2016 r. – Nicea, 19 XII 2016 r. – Berlin, 22 III i 3 VI 2017 r. – Londyn, 7 IV 2017 r. – Sztokholm, 17 VIII 2017 r. – Barcelona, 31 X 2017 r. – Nowy Jork).

[3] *Bezpieczny, zrównoważony i połączony transport*, Unia Europejska, https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_pl [dostęp: 10 XII 2024].

[4] Ł. Foryś, R. Gwardyński, M. Żuber, *Wybrane aspekty bezpieczeństwa dotyczące mobilności człowieka*, Szczytno 2024, s. 61.

[5] Tamże, s. 62.

i porządku na drogach. Obejmuje ona m.in. sprawdzanie dokumentów, stanu technicznego pojazdów, przestrzegania przepisów ruchu drogowego przez kierowców oraz badanie ich trzeźwości. Zdaniem autorów możliwości wykorzystania kontroli ruchu drogowego w zapewnieniu bezpieczeństwa są jednak dużo szersze. W trakcie przeprowadzania takiej kontroli policjanci mogą sprawdzić osoby i rzeczy w policyjnych systemach teleinformatycznych oraz ładunek, bagaż i ich zgodność z posiadanymi dokumentami (w przypadku gdy są wymagane).

Celem artykułu jest omówienie przestępczości transgranicznej z perspektywy funkcjonariusza pełniącego służbę na drodze oraz wskazanie – na podstawie przeglądu literatury i danych statystycznych – znaczenia kontroli ruchu drogowego w zwalczaniu tej przestępczości.

Pojęcie przestępczości transgranicznej

Zgodnie z *Dyrektywą Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej*:

> (1) Głównym motywem transgranicznej przestępczości zorganizowanej, w tym organizacji przestępczych typu mafijnego, jest uzyskiwanie korzyści finansowych. W związku z tym właściwe organy powinny dysponować środkami pozwalającymi na wykrywanie, zabezpieczanie i konfiskatę korzyści pochodzących z przestępstwa, jak i na zarządzanie tymi korzyściami. Skuteczne zapobieganie przestępczości zorganizowanej i zwalczanie jej powinno jednak polegać na neutralizacji korzyści pochodzących z przestępstwa i powinno zostać rozszerzone, w niektórych przypadkach, na wszelkie mienie pochodzące z działalności przestępczej.
> (2) Zorganizowane grupy przestępcze działają niezależnie od istnienia granic i coraz częściej uzyskują mienie w państwach członkowskich innych niż te, w których głównie działają, oraz w państwach trzecich. Coraz potrzebniejsza staje się skuteczna współpraca międzynarodowa w zakresie odzyskiwania mienia i wzajemnej pomocy prawnej.
> (3) Do najskuteczniejszych metod walki z przestępczością zorganizowaną należy wprowadzenie surowych konsekwencji prawnych popełniania takiego rodzaju przestępstw, jak również skuteczne wykrywanie oraz zabezpieczanie i konfiskata narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa.
> (4) Mimo że danych statystycznych dotyczących tej kwestii jest niewiele, wydaje się, że kwoty odzyskiwane z korzyści pochodzących z przestępstw w Unii nie są wystarczające w porównaniu z szacunkową wysokością takich korzyści.

> Z przeprowadzonych analiz wynika, że mimo iż procedury konfiskaty są uregulowane przepisami unijnymi i krajowymi, to są one wykorzystywane w zbyt ograniczonym zakresie[6].

Według Piotra Kozłowskiego definicja Andrzeja Wawrzusiszyna dotycząca przestępczości transgranicznej wskazuje, że:

> (…) przestępczość transgraniczna jest jedną z form przestępczości zorganizowanej. Jest zjawiskiem dynamicznym, które w zależności od obszaru oraz metod działania jak również od kategorii przemycanych towarów ulega stałym zmianom i modyfikacjom. Przestępczość transgraniczna potrafi się błyskawicznie dostosować do lokalnych potrzeb, a także wypełnić zapotrzebowanie na usługi i towary deficytowe, przynosząc krociowe zyski dla organizatorów procederu. Istniejący ruch graniczny oraz międzynarodową wymianę towarów próbuje do swoich celów wykorzystać przestępczość transgraniczna[7].

Przestępczość transgraniczną określa się jako działania przestępcze, które są prowadzone na terenie różnych państw lub naruszają ich granice. Często jest związana z międzynarodową przestępczością zorganizowaną, która przyjmuje strukturę sieciową. Ten rodzaj przestępczości stanowi poważne zagrożenie systemu bezpieczeństwa państwa z uwagi na: (…) *długofalowe skutki aktywności transgranicznej przestępczości zorganizowanej, których źródeł należy upatrywać w tzw. wtórnym oddziaływaniu grup przestępczych. Biorąc pod uwagę to, iż w wyniku nielegalnej działalności zorganizowane grupy przestępcze osiągają określone korzyści materialne, trzeba założyć także, że zdobyte przez nie zasoby mogą i są wykorzystywane do wpływania na sytuację poszczególnych krajów, ich gospodarek, a w konsekwencji także na ich bezpieczeństwo*[8]. Przestępczość transgraniczna obejmuje m.in. przemyt towarów, narkotyków, broni, odpadów, dzieł sztuki, materiałów jądrowych i promieniotwórczych, a także terroryzm. Sposób, formy oraz zakres aktywności transgranicznej przestępczości zorganizowanej w poszczególnych państwach są bardzo zróżnicowane i zależą od wielu czynników, np. warunków społeczno-ekonomicznych, polityki

---

[6] *Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej*.

[7] P. Kozłowski, *Przestępczość transgraniczna w latach 2015–2017 zagrożeniem dla bezpieczeństwa wewnętrznego państwa w świetle danych statystycznych Bieszczadzkiego Oddziału Straży Granicznej w Przemyślu*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1(16), s. 86. https://doi.org/10.52934/wpz.86.

[8] P. Kuzior, *Transgraniczna przestępczość zorganizowana – asymetryczne zagrożenie*, „Prawo Europejskie w Praktyce" 2008, nr 12(54), s. 29–30.

i stabilności rządu, systemu prawnego i egzekwowania prawa. Bardzo trudno jest ocenić skalę zjawiska oraz jego oddziaływania na bezpieczeństwo państw i systemu międzynarodowego. Jak zauważa Paweł Lubiewski:

> Współczesne uwarunkowania społeczno-polityczne generują szereg problemów, z którymi musi sobie radzić administracja państwowa, a radzenia z dotąd nieznanymi jak najszybciej się nauczyć. Bez wątpienia granica państwowa jest tą płaszczyzną aktywności administracji państwa. (…) W odniesieniu do problemu ochrony granic współczesnego państwa wyraźnie dostrzegalny jest dualizm charakteru ochrony granicy przejawiający się z jednej strony w konieczności ochrony nienaruszalności granicy, a z drugiej w konieczności ochrony przed przenikaniem przez nią w głąb państwa wielu poważnych zagrożeń[9].

Jest to jedna z głównych przyczyn, dla których współcześnie do ochrony granic nie wystarczy jedna instytucja. W polskich realiach ten obowiązek w niejednakowym zakresie został powierzony kilku instytucjom realizującym zadania w różnych obszarach działalności państwa.

Działania zmierzające do zapewnienia bezpieczeństwa muszą mieć kompleksowy i interdyscyplinarny charakter. Według Andrzeja Czopa determinanty, które powodują szczególne zagrożenie dla granicy państwa, to: (…) *terroryzm, zwłaszcza islamski, niekontrolowane ruchy migracyjne, przestępczość zorganizowana, skażenia sanitarne i epidemiologiczne. Wskazano też na konieczność ochrony granic przed zorganizowanym przemytem, zwłaszcza: środków odurzających i psychotropowych, materiałów radioaktywnych, niebezpiecznych odpadów, broni, amunicji i innych środków walki, kradzionych samochodów, alkoholu, papierosów i dzieł sztuki*[10].

Strefa Schengen – europejska strefa bez granic wewnętrznych

Zasady obowiązujące od 1995 r.[11] w strefie Schengen:

> (…) znoszą kontrole na jej wewnętrznych granicach, jednocześnie harmonizując i wzmacniając bezpieczeństwo jej zewnętrznych granic. Ogólna zasada stanowi, że gdy ktoś dostanie się do strefy Schengen, może podróżować

[9] P. Lubiewski, *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, „Przegląd Policyjny" 2019, numer specjalny, s. 66. https://doi.org/10.5604/01.3001.0013.6700.

[10] A. Czop, *Służby specjalne w systemie ochrony granic Rzeczypospolitej Polskiej*, „Przegląd Policyjny" 2019, numer specjalny, s. 129. https://doi.org/10.5604/01.3001.0013.6698.

[11] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice.*

> z jednego kraju członkowskiego do drugiego bez kontroli na granicach. Jednak uprawnione do tego organy krajowe mogą przeprowadzać kontrole pewnych osób na wewnętrznych granicach lub w ich pobliżu, jeśli informacje uzyskane od policji i praktyka uzasadniają tymczasowe zwiększenie nadzoru. Strefa Schengen oznacza również wspólną politykę wizową dla krótkich pobytów obywateli krajów spoza UE. Państwa w strefie Schengen łączą również siły w walce z przestępczością poprzez współpracę policyjną i sądowniczą[12].

System informacyjny Schengen jest usprawniany z myślą o zapewnieniu Europejczykom większego bezpieczeństwa. Strefa Schengen to jeden z filarów integracji europejskiej. Swobodny przepływ daje mieszkańcom UE prawo do życia, nauki, pracy i świadczeń (medycznych, emerytalnych) na terytorium całej wspólnoty. Do strefy Schengen należą wszystkie kraje stowarzyszone w Unii, oprócz Irlandii, która utrzymuje w mocy klauzulę opt-out, i Cypru, który planuje przystąpić do strefy Schengen. Kraje UE zgodziły się znieść od 31 marca 2024 r.[13] kontrole graniczne na granicach powietrznych i morskich dla osób podróżujących z i do Bułgarii i Rumunii. Ponadto do strefy Schengen należą cztery kraje spoza UE: Islandia, Norwegia, Szwajcaria i Liechtenstein (rysunek 1).

Jak podają statystyki, w 2015 r. zewnętrzne granice UE przekroczono nielegalnie 1,83 mln razy. W 2023 r. udało się ograniczyć tę liczbę do 355 300[14]. Nadal jednak zarządzanie migracją i bezpieczeństwem granic zewnętrznych stanowi wyzwanie dla Europy.

Działania podejmowane przez PE przyczyniają się do wzmocnienia wspólnej polityki azylowej, rozwijają legalną migrację zgodnie z potrzebami państw członkowskich, wspierają integrację obywateli państw trzecich oraz powstrzymują nielegalną migrację. Celem Funduszu Bezpieczeństwa Wewnętrznego jest zwalczanie zagrożeń transgranicznych, takich jak terroryzm, przestępczość zorganizowana i cyberprzestępczość. Te wyzwania zapoczątkowały znaczące zmiany w tworzeniu narzędzi i agencji, takich jak: System Informacyjny Schengen, System Informacji Wizowej, Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) oraz system

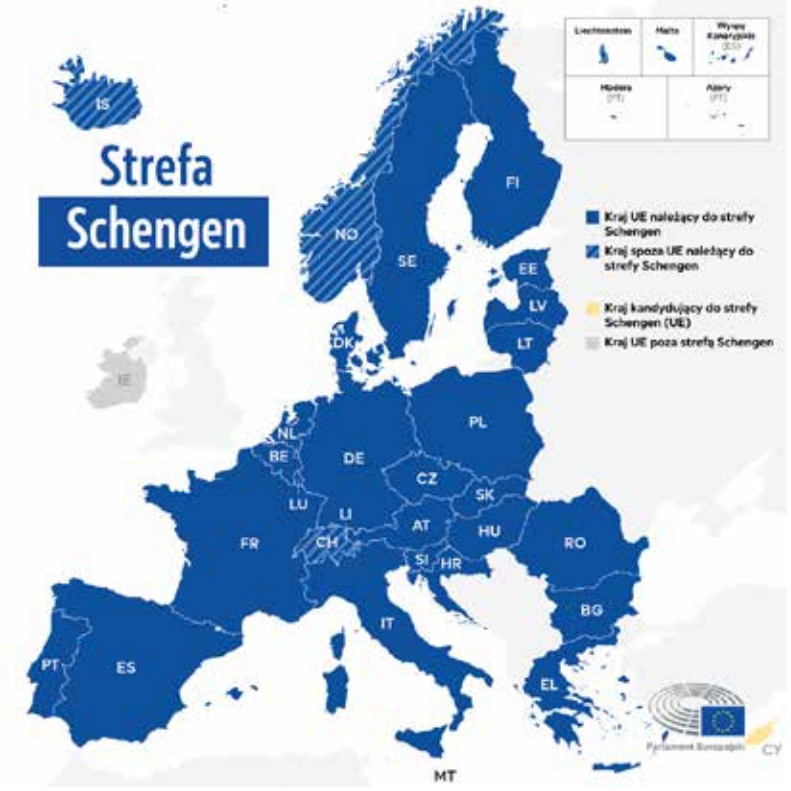
---

[12] *Strefa Schengen: wszystko, co musisz wiedzieć o europejskiej strefie bez granic wewnętrznych*, Parlament Europejski, 18 VI 2019 r., https://www.europarl.europa.eu/topics/pl/article/20190612STO54307/strefa-schengen-wszystko-co-musisz-wiedziec-o-europejskiej-strefie-bez-granic [dostęp: 13 VI 2025].

[13] *Schengen: co wpływa na europejską strefę bez granic wewnętrznych?*, Parlament Europejski, 29 V 2018 r., https://www.europarl.europa.eu/topics/pl/article/20180525STO04311/schengen-co-wplywa-na-europejska-strefe-bez-granic-wewnetrznych [dostęp: 11 XII 2024].

[14] *Irregular border crossings into EU so far this year highest since 2016*, Frontex, 11 XII 2023 r., https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-so-far-this-year-highest-since-2016-hZ9xWZ [dostęp: 11 XII 2024].

wjazdu/wyjazdu (Entry Exit System, EES)[15] na zewnętrznych granicach strefy Schengen. Ich zadaniem jest wykrywanie przestępców, terrorystów lub innych osób stanowiących zagrożenie. Podróżujący, którzy nie potrzebują wizy, będą w przyszłości sprawdzani przed przybyciem do UE za pomocą Europejskiego Systemu Informacji o Podróży oraz Zezwoleń na Podróż (European Travel Information and Authorisation System, ETIAS)[16]. Zacznie on działać w ostatnim kwartale 2026 r.[17]



Rysunek 1. Państwa strefy Schengen.

Źródło: *Strefa Schengen: wszystko, co musisz wiedzieć o europejskiej strefie bez granic wewnętrznych*, Parlament Europejski, 18 VI 2019 r., https://www.europarl.europa.eu/topics/pl/article/20190612STO54307/strefa-schengen-wszystko-co-musisz-wiedziec-o-europejskiej-strefie-bez-granic [dostęp: 13 VI 2025].

[15] System EES nie został jeszcze uruchomiony. Zob. *Entry/Exit System (EES)*, https://travel-europe.europa.eu/en/ees [dostęp: 11 XII 2024].

[16] *Zarządzanie granicami zewnętrznymi*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/zarzadzanie-granicami-zewnetrznymi#:~:text=SIS%20%E2%80%93%20System%20Informacyjny [dostęp: 11 XII 2024].

[17] *ETIAS*, https://travel-europe.europa.eu/en/etias [dostęp: 11 IV 2025].

W strefie Schengen najczęściej wybierany jest transport drogowy, zwłaszcza samochodowy. Wynika to z łatwości przemieszczania się bez kontroli granicznych, co jest szczególnie korzystne dla przewozów towarowych i pasażerskich.

Strefa Schengen – kontrola na granicach

Zgodnie z informacjami podanymi na stronach PE: *Zwiększony napływ obywateli państw trzecich do strefy Schengen, który ma jeszcze wzrosnąć w przyszłości (do roku 2025 około 300 mln obywateli państw trzecich legalnie przekroczy granice strefy Schengen w celu odbycia krótkoterminowej wizyty) oraz obawy związane z bezpieczeństwem zewnętrznych granic UE spowodowały potrzebę opracowania nowych zasad dotyczących zarządzania granicami obszaru Schengen*[18]. Według danych KE:

> (…) w strefie Schengen każdego roku odbywa się ponad 1,25 miliarda podróży. Chociaż w strefie Schengen zniesiono kontrole na granicach wewnętrznych, państwa zachowały prawo do przywrócenia tymczasowych kontroli w przypadku poważnych zagrożeń dla porządku publicznego lub bezpieczeństwa wewnętrznego. Od 2015 r., w związku z kryzysem migracyjnym, a także wzrostem zagrożeń terrorystycznych, szereg państw strefy Schengen przywróciło takie kontrole (…). Podczas pandemii COVID-19 wiele krajów UE przywróciło kontrole graniczne, aby powstrzymać rozprzestrzenianie się wirusa. W grudniu 2021 r. Komisja Europejska zaproponowała aktualizację przepisów regulujących strefę Schengen, aby zapewnić, że przywrócenie kontroli na granicach wewnętrznych jest stosowane jako środek ostateczny. Nowe przepisy mają też wspierać stosowanie alternatywnych środków, takich jak ukierunkowane kontrole policyjne i wzmocniona współpraca policyjna. Posłowie i posłanki do PE kilkakrotnie sprzeciwiali się częstemu przywracaniu kontroli, ponieważ utrudnia to swobodny przepływ osób w UE[19].

W kwietniu 2024 r. Parlament Europejski zatwierdził aktualizację przepisów strefy Schengen. Ustanowiono limity czasowe dla kontroli na granicach wewnętrznych. Rada UE zatwierdziła aktualizację w maju 2024 r. Kodeks graniczny Schengen daje państwom członkowskim możliwość tymczasowego przywrócenia kontroli granicznej na granicach wewnętrznych w przypadku poważnego zagrożenia porządku publicznego lub bezpieczeństwa wewnętrznego. Mogą one z tego prawa

[18] *Strefa Schengen: Wspólny elektroniczny system wzmocni bezpieczeństwo granic*, Parlament Europejski, 25 X 2017 r., https://www.europarl.europa.eu/topics/pl/article/20171023STO86604/strefa-schengen--wspolny-elektroniczny-system-wzmocni-bezpieczenstwo-granic [dostęp: 11 XII 2024].

[19] *Strefa Schengen: rozszerzanie europejskiego obszaru bez granic*, Parlament Europejski, 23 II 2018 r., https://www.europarl.europa.eu/topics/pl/article/20180216STO98008/strefa-schengen-rozszerzenie-europejskiego-obszaru-bez-granic [dostęp: 11 XII 2024].

korzystać w ostateczności, w wyjątkowych sytuacjach, i musi to odbywać się z poszanowaniem zasady proporcjonalności[20].

W lutym 2024 r. parlamentarna Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zatwierdziła porozumienie osiągnięte z rządami krajowymi modyfikujące przepisy dotyczące kontroli osób na zewnętrznych granicach UE[21]. *Przepisy te będą dotyczyły osób niespełniających warunków wjazdu na teren kraju UE, które zostaną zatrzymane podczas nielegalnego przekraczania granicy lub misji ratunkowej na morzu, oraz osób, które aplikują o ochronę międzynarodową na przejściu granicznym granicy zewnętrznej*[22]. Kontroli mogą być poddane osoby znalezione na terenie UE, które uniknęły kontroli granicznej i nie mają odpowiedniego zezwolenia. Kontrole mają obejmować: (…) *identyfikację, pobieranie odcisków palców, kontrole bezpieczeństwa, wstępną ocenę stanu zdrowia i podatności na zagrożenia*[23]. Zgodnie z przepisami procedura ta powinna trwać do siedmiu dni. System monitorowania działań w tym zakresie obowiązuje: (…) *w każdym kraju UE w celu zabezpieczenia fundamentalnych praw człowieka dla osób, które są poddawane kontroli*[24]. Z kolei: (…) *jako alternatywę dla kontroli na granicach wewnętrznych, nowe przepisy wspierają współpracę Policji w regionach przygranicznych w celu przeciwdziałania nielegalnemu przemieszczaniu się w strefie Schengen. Zatrzymane osoby spoza UE o nieuregulowanym statusie często przybywają z innego kraju UE, więc jeśli oba kraje organizują wspólne patrole, te osoby mogą zostać przeniesione z powrotem do pierwszego kraju UE*[25]. Parlament Europejski chce wykluczyć z tego kilka kategorii osób, w tym małoletnich.

Stan bezpieczeństwa w Polsce w latach 2019–2020

Jak wynika z danych dotyczących 2020 r. opublikowanych przez Policję[26], w Polsce popełniono 786 302 przestępstwa, tj. o 36 475 mniej niż w 2019 r., a ich

[20] *Przeciwdziałanie nielegalnej migracji: lepsze zarządzanie granicami UE*, Parlament Europejski, 17 VII 2017 r., https://www.europarl.europa.eu/topics/pl/article/20170627STO78419/przeciwdzialanie-nielegalnej-migracji-lepsze-zarzadzanie-granicami-ue [dostęp: 13 XII 2024].

[21] *Asylum and migration: Civil Liberties committee endorses a new legal framework*, European Parliament, 14 II 2024 r., https://www.europarl.europa.eu/news/en/press-room/20240212IPR17628/asylum-and-migration-civil-liberties-committee-endorses-the-agreements [dostęp: 13 XII 2024].

[22] *Przeciwdziałanie nielegalnej migracji: lepsze zarządzanie granicami UE*…

[23] Tamże.

[24] Tamże.

[25] Tamże.

[26] Ostatnie informacje na temat bezpieczeństwa opublikowane przez Policję pochodzą z początku 2021 r.

wykrywalność wzrosła i wyniosła 73,9%[27]. W 2020 r. skradziono 9121 aut, tj. o 3% więcej w porównaniu z 2019 r. (8856 aut), a wykrywalność tego typu przestępstw wzrosła o 1,9%. W 2020 r. w Polsce doszło do 656 zabójstw, tj. do 125 więcej niż w 2019 r. Odnotowano ponadto 199 020 przestępstw gospodarczych – o 9427 więcej niż w 2019 r. W tym samym roku policjanci zabezpieczyli majątek przestępców o łącznej wartości 867 049 023 zł, a w 2020 r. – mienie o wartości 930 118 572 zł. Funkcjonariusze Centralnego Biura Śledczego Policji (CBŚP), których głównymi zadaniami są identyfikowanie i neutralizacja grup przestępczych, często przy współpracy z polskimi i zagranicznymi instytucjami, zebrali materiał procesowy i przedstawili zarzuty ponad 3200 osobom (w 2019 r. – prawie 3800). W 2019 r. 1836 podejrzanym postawiono zarzuty kierowania zorganizowaną grupą przestępczą lub udziału w niej (w 2020 r. – ponad 2000). Udało się również zlikwidować zaplecze finansowe grup przestępczych i zabezpieczyć majątki podejrzanych na poczet przyszłych kar. W 2020 r. zabezpieczono mienie w wysokości ponad 700 mln zł, a na czarny rynek nie trafiło ponad 10 t narkotyków, z czego ponad 4 t przejęto poza granicami Polski. Zabezpieczono też środki odurzające, psychotropowe, a także duże ilości prekursorów, co wstrzymało produkcję kolejnych narkotyków. Zlikwidowano 31 laboratoriów narkotyków syntetycznych i 75 plantacji konopi indyjskich.

W 2020 r. prowadzono także działania mające na celu zwalczanie przestępczości tytoniowej. Zlikwidowano 20 fabryk papierosów (tyle samo co w 2019 r.). Zabezpieczono ponad 190 mln szt. papierosów (w 2019 r. – ok. 212 mln szt.) i ponad 306 t tytoniu (w 2019 r. – ponad 324 t). Ponadto służby krajów UE, dzięki informacjom przekazanym przez funkcjonariuszy CBŚP, identyfikowały działalność grup przestępczych na swoim terytorium. Zlikwidowano cztery działające fabryki papierosów, a także zabezpieczono ok. 48 mln szt. papierosów i ponad 123 t krajanki tytoniowej. Co istotne: (…) *osiągnięte wyniki CBŚP oraz przeprowadzone akcje były możliwe także dzięki współpracy z prokuraturą, policjantami Komend Wojewódzkich Policji, Strażą Graniczną, Centralnym Biurem Antykorupcyjnym, Agencją Bezpieczeństwa Wewnętrznego, Krajową Administracją Skarbową, Głównym Inspektoratem Sanitarnym, Generalnym Inspektorem Informacji Finansowej i innymi polskimi instytucjami*[28]. Ponadto funkcjonariusze CBŚP, często przy wsparciu Europolu i Eurojustu, współpracowali ze służbami i instytucjami wielu krajów. Poddane analizie działania przestępcze są powiązane również z przestępczością zorganizowaną,

[27] Wszystkie dane w części artykułu *Stan bezpieczeństwa w Polsce w latach 2019–2020* pochodzą z: *Podsumowujemy 2020 rok w Policji*, https://statystyka.policja.pl/st/raporty/roczne-raporty-statyst/226911,Podsumowujemy-2020-rok-w-Policji.html [dostęp: 10 XII 2024].

[28] Tamże.

przybierającą często formę przestępczości transgranicznej. Grupy przestępcze korzystają ze środków transportu (szczególnie drogowego), które pozwalają na sprawne przemieszczanie osób i towarów.

Kontrola ruchu drogowego a zapewnianie bezpieczeństwa

Kontrola ruchu drogowego to działania podejmowane przez organy ścigania w celu zapewnienia bezpieczeństwa na drogach. Obejmuje monitorowanie i egzekwowanie przepisów ruchu drogowego, m.in. ograniczenia prędkości, zakazy parkowania, jazda pod wpływem alkoholu czy narkotyków, oraz innych przepisów mających na celu ochronę uczestników ruchu drogowego. Kontrole mogą być rutynowe lub wynikać z konkretnych incydentów, np. wypadków drogowych. W Polsce do kontroli ruchu drogowego są uprawnione: Policja[29], Straż Graniczna (SG), Inspekcja Transportu Drogowego i Straż Miejska. Funkcjonariusze na podstawie obowiązujących przepisów mają określone uprawnienia dotyczące kontroli ruchu drogowego. Realizacja zadań przez wymienione podmioty najczęściej jest kojarzona z zapewnieniem bezpieczeństwa ruchu drogowego. Z uwagi na zmieniającą się sytuację geopolityczną na świecie oraz położenie geograficzne Polski konieczna jest zmiana podejścia do kontroli ruchu drogowego, m.in. w związku z rozwijającą się przestępczością transgraniczną.

Odnotowuje się coraz więcej nieletnich migrantów bez opieki. W Polsce jest sześć strzeżonych ośrodków dla cudzoziemców (SOC), w których łącznie są 962 miejsca. W 2023 r. przyjęto do nich 1903 cudzoziemców, w tym 32 małoletnich bez opieki. W związku z dużą liczbą nieletnich samotnych migrantów, którzy pojawili się w Polsce od początku kwietnia 2024 r., placówki opiekuńcze są przepełnione. Nieletni pozostają w SOC i placówkach SG, ponieważ nie ma gdzie ich kierować[30].

Z relacji rzecznika Komendy Głównej Straży Granicznej wynika, że w pierwszej połowie 2024 r. SG zatrzymała 243 osoby małoletnie (56 dziewcząt i 187 chłopców), którzy nielegalnie przekroczyli granicę Polski[31]. Straż Graniczna po zatrzymaniu osoby małoletniej, która nielegalnie przekroczyła granicę i jest bez opieki,

[29] Ł. Foryś, *Zapewnienie bezpieczeństwa w związku z kontrolą ruchu drogowego*, w: *Bezpieczeństwo w perspektywie transdyscyplinarnej*, A.W. Filipek (red.), Siedlce 2022, s. 88–102.

[30] A. Rodowicz, *Nieletni migranci. Gdy nie uda się ich wypchnąć za druty, trafiają w tryby niewydolnego systemu*, OKO.press, 3 VIII 2024 r., https://oko.press/maloletni-migranci-polska-granica-ani-prawa-ani-opieki [dostęp: 18 XII 2024].

[31] Tamże.

musi wystąpić do sądu z wnioskiem o umieszczenie jej w placówce opiekuńczo-wychowawczej lub w SOC[32]. Agnieszka Matejczuk, prawniczka ze Stowarzyszenia Interwencji Prawnej, zwraca uwagę, że: (…) *gdy zatrzymany małoletni ma mniej niż 15 lat, musi być zawieziony do placówki interwencyjnej. Jeśli ma powyżej 15 roku życia, ale złoży wolę wnioskowania o ochronę, to również powinien być skierowany do takiej placówki. Osoby między 15–18 rokiem życia można umieścić w SOC-u na czas tzw. procedury powrotowej, czyli zmierzającej do deportacji*[33].

Niewątpliwie problematyka małoletnich nielegalnych migrantów wymaga odrębnych regulacji, zapewniających im odpowiednią opiekę i ochronę, a jednocześnie zgodnych z obowiązującymi standardami w zakresie kontroli granicznej.

Wprowadzenie kontroli na granicach wewnętrznych będzie możliwe – zgodnie z Kodeksem granicznym Schengen – w uzasadnionych przypadkach dotyczących np. zidentyfikowanego i bezpośredniego zagrożenia terroryzmem początkowo na okres do 6 miesięcy, z możliwością przedłużenia do 18 miesięcy, a w wyjątkowych przypadkach jeszcze dłużej za zgodą Rady UE. Jeżeli zagrożenie będzie się utrzymywać, decyzją Rady UE będzie można zezwolić na dalsze kontrole graniczne, zwłaszcza kiedy wiąże się to z poważnym zagrożeniem dla wielu krajów jednocześnie[34]. Warto również wspomnieć, że w Polsce od wielu lat istnieje ścisła współpraca między krajowymi służbami granicznymi, policyjnymi i sądowymi, a ich odpowiednikami w państwach członkowskich, co pomaga w utrzymaniu bezpieczeństwa i porządku publicznego.

Kontrole ruchu drogowego mają znaczenie w zwalczaniu przestępczości transgranicznej z kilku powodów. Mogą przyczynić się do zwiększenia wykrywalności nielegalnego przewozu towarów, takich jak narkotyki, broń czy towary objęte akcyzą. Funkcjonariusze Policji pełniący służbę na drodze mogą współpracować z policjantami z innych państw oraz ze SG czy Służbą Celno-Skarbową, aby skuteczniej zwalczać przemyt. Jeśli podczas kontroli drogowej funkcjonariusze natrafią na osoby, które nielegalnie przekroczyły granicę, to wówczas kluczowa jest współpraca z organami odpowiedzialnymi za kontrolę graniczną. Bardzo często przestępczość transgraniczna ma charakter przestępczości zorganizowanej. Kontrole drogowe mogą pomóc w identyfikacji i zatrzymaniu grup przestępczych, które wykorzystują sieci transportowe do prowadzenia swojej działalności.

---

[32] *Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach.*

[33] A. Rodowicz, *Nieletni migranci…*

[34] *Przeciwdziałanie nielegalnej migracji: lepsze zarządzanie granicami UE…*

Podsumowanie

Zarówno kontrola ruchu drogowego, jak i zwalczanie przestępczości transgranicznej to złożone procesy podejmowane przez liczne podmioty, również w ramach współpracy międzynarodowej. Zmiany geopolityczne zachodzące we współczesnym świecie stanowią duże wyzwanie dla podmiotów odpowiedzialnych za zapewnianie bezpieczeństwa. Działania podejmowane w ramach kontroli ruchu drogowego skupiają się przede wszystkim na poprawianiu stanu bezpieczeństwa polegającym na ograniczaniu liczby osób rannych i zabitych w wypadkach drogowych.

Konflikty zbrojne czy kryzysy humanitarne mogą prowadzić do zwiększonego ruchu migracyjnego. Może to powodować wzrost liczby pojazdów na drogach i wymagać skuteczniejszych mechanizmów kontroli i zarządzania ruchem. W odpowiedzi na nowe zagrożenia kraje mogą wprowadzać zmiany w przepisach ruchu drogowego, co może mieć wpływ na współpracę międzypaństwową oraz obowiązujące procedury.

W strefie Schengen zniesiono kontrole na granicach wewnętrznych, co wymaga skuteczniejszego zarządzania granicami zewnętrznymi. To oznacza konieczność stosowania zaawansowanych narzędzi, systemów informacyjnych i lepszej koordynacji między krajami. Nowe technologie, takie jak systemy monitorowania ruchu, systemy rozpoznawania tablic rejestracyjnych czy drony mogą przyczynić się do lepszego zarządzania ruchem na drogach i monitorowania granic, sprawniejszego ujawniania sprawców przestępstw, skuteczniejszego poszukiwania osób i przeciwdziałania zagrożeniom, np. zamachom terrorystycznym. Ich wdrożenie wymaga jednak inwestycji i przeszkolenia personelu, a także odpowiednich przepisów oraz procedur.

Kontrole ruchu drogowego na granicach i w punktach strategicznych mogą skutecznie utrudniać przemyt osób i nielegalnych towarów, który jest jednym z głównych elementów przestępczości transgranicznej. Wspólne operacje i wymiana informacji między krajami mogą zwiększyć skuteczność kontroli drogowych, a tym samym zwalczania przestępczości, gdyż uderzą w zorganizowane grupy przestępcze. Kolejnym istotnym elementem jest zauważalna obecność służb kontrolnych na drogach, co może działać odstraszająco na potencjalnych przestępców i ograniczać podejmowanie nielegalnych działań związanych np. z przemytem.

Zmiany geopolityczne stawiają przed państwami wiele wyzwań, w tym dotyczących potrzeby wprowadzenia innowacyjnych rozwiązań poprawy bezpieczeństwa, zarówno w ruchu drogowym, jak i w innych jego obszarach. Należy przy tym pamiętać, że przestępczość transgraniczna to złożone zjawisko, które wymaga współpracy, również międzynarodowej, oraz skutecznych narzędzi do jego zwalczania. Jednym z nich jest kontrola ruchu drogowego. Szersze spojrzenie na czynności podejmowane przez funkcjonariuszy wobec uczestników ruchu drogowego

daje możliwość stworzenia skuteczniejszych narzędzi do poprawy bezpieczeństwa na drodze, zapewnienia bezpieczeństwa i porządku publicznego, a tym samym przeciwdziałania i zwalczania przestępczości, również transgranicznej. Autorzy wskazali czynniki warunkujące procedurę kontroli ruchu drogowego oraz przestępczość transgraniczną, której sprzyja swobodny przepływ w strefie Schengen. Należy zwrócić uwagę na systemowy charakter omawianego zagadnienia, co wymaga skoordynowanych działań różnych instytucji. Rozważania poczynione w artykule stanowią punkt wyjścia do głębszego poznania oraz wskazują potrzebę podejścia interdyscyplinarnego do badań związanych z tą problematyką.

Bibliografia

Czop A., *Służby specjalne w systemie ochrony granic Rzeczypospolitej Polskiej*, „Przegląd Policyjny" 2019, numer specjalny, s. 98–130. https://doi.org/10.5604/01.3001.0013.6698.

Foryś Ł., *Zapewnienie bezpieczeństwa w związku z kontrolą ruchu drogowego*, w: *Bezpieczeństwo w perspektywie transdyscyplinarnej*, A.W. Filipek (red.), Siedlce 2022, s. 88–102.

Foryś Ł., Gwardyński R., Żuber M., *Wybrane aspekty bezpieczeństwa dotyczące mobilności człowieka*, Szczytno 2024.

Kozłowski P., *Przestępczość transgraniczna w latach 2015–2017 zagrożeniem dla bezpieczeństwa wewnętrznego państwa w świetle danych statystycznych Bieszczadzkiego Oddziału Straży Granicznej w Przemyślu*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1(16), s. 83–95. https://doi.org/10.52934/wpz.86.

Kuzior P., *Transgraniczna przestępczość zorganizowana – asymetryczne zagrożenie*, „Prawo Europejskie w Praktyce" 2008, nr 12(54).

Lubiewski P., *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, „Przegląd Policyjny" 2019, numer specjalny, s. 49–66. https://doi.org/10.5604/01.3001.0013.6700.

Źródła internetowe

Asylum and migration: Civil Liberties committee endorses a new legal framework, European Parliament, 14 II 2024 r., https://www.europarl.europa.eu/news/en/press-room/20240212IPR17628/asylum-and-migration-civil-liberties-committee-endorses-the--agreements [dostęp: 13 XII 2024].

Bezpieczny, zrównoważony i połączony transport, Unia Europejska, https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_pl [dostęp: 10 XII 2024].

Entry/Exit System (EES), https://travel-europe.europa.eu/en/ees [dostęp: 11 XII 2024].

ETIAS, https://travel-europe.europa.eu/en/etias [dostęp: 11 IV 2025].

Irregular border crossings into EU so far this year highest since 2016, Frontex, 11 XII 2023 r., https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-so-far-this-year-highest-since-2016-hZ9xWZ [dostęp: 11 XII 2024].

Podsumowujemy 2020 rok w Policji, https://statystyka.policja.pl/st/raporty/roczne-raporty-statyst/226911,Podsumowujemy-2020-rok-w-Policji.html [dostęp: 10 XII 2024].

Przeciwdziałanie nielegalnej migracji: lepsze zarządzanie granicami UE, Parlament Europejski, 17 VII 2017 r., https://www.europarl.europa.eu/topics/pl/article/20170627STO78419/przeciwdzialanie-nielegalnej-migracji-lepsze-zarzadzanie-granicami-ue [dostęp: 13 XII 2024].

Rodowicz A., *Nieletni migranci. Gdy nie uda się ich wypchnąć za druty, trafiają w tryby niewydolnego systemu*, OKO.press, 3 VIII 2024 r., https://oko.press/maloletni-migranci-polska-granica-ani-prawa-ani-opieki [dostęp: 18 XII 2024].

Schengen: co wpływa na europejską strefę bez granic wewnętrznych?, Parlament Europejski, 29 V 2018 r., https://www.europarl.europa.eu/topics/pl/article/20180525STO04311/schengen-co-wplywa-na-europejska-strefe-bez-granic-wewnetrznych [dostęp: 11 XII 2024].

Statistics Explained, Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=456757 [dostęp: 10 XII 2024].

Strefa Schengen: rozszerzanie europejskiego obszaru bez granic, Parlament Europejski, 23 II 2018 r., https://www.europarl.europa.eu/topics/pl/article/20180216STO98008/strefa-schengen-rozszerzenie-europejskiego-obszaru-bez-granic [dostęp: 11 XII 2024].

Strefa Schengen: Wspólny elektroniczny system wzmocni bezpieczeństwo granic, Parlament Europejski, 25 X 2017 r., https://www.europarl.europa.eu/topics/pl/article/20171023STO86604/strefa-schengen-wspolny-elektroniczny-system-wzmocni-bezpieczenstwo-granic [dostęp: 11 XII 2024].

Strefa Schengen: wszystko, co musisz wiedzieć o europejskiej strefie bez granic wewnętrznych, Parlament Europejski, 18 VI 2019 r., https://www.europarl.europa.eu/topics/pl/article/20190612STO54307/strefa-schengen-wszystko-co-musisz-wiedziec-o-europejskiej-strefie-bez-granic [dostęp: 13 VI 2025].

Zarządzanie granicami zewnętrznymi, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/zarzadzanie-granicami-zewnetrznymi#:~:text=SIS%20%E2%80%93%20System%20Informacyjny [dostęp: 11 XII 2024].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (Dz. Urz. UE L 77/1 z 23 III 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127/39 z 29 IV 2014 r.).

Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach (t.j. DzU z 2024 r. poz. 769, ze zm.).

Dr Łukasz Foryś

Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Jego aktywność naukowa skupia się wokół problematyki bezpieczeństwa wewnętrznego, ze szczególnym uwzględnieniem bezpieczeństwa i porządku publicznego, bezpieczeństwa transportu oraz bezpieczeństwa ruchu drogowego. Autor opracowań naukowych poświęconych tej problematyce. Współorganizator oraz uczestnik krajowych i międzynarodowych konferencji naukowych.

Kontakt: l.forys@apol.edu.pl

Dr Kornelia Stępień

Doktor nauk prawnych w zakresie prawa, kryminologii, adiunkt Instytutu Nauk Prawnych Wydziału Bezpieczeństwa i Nauk Prawnych Akademii Policji w Szczytnie. Autorka artykułów naukowych opublikowanych w prasie specjalistycznej oraz pracach zbiorowych dotyczących kryminologii, przestępczości nieletnich i wiktymologii. Zainteresowania naukowo-badawcze autorki koncentrują się wokół problematyki patologii społecznych, a także determinant demoralizacji i przestępczości nieletnich i zapobiegania tym zjawiskom. Interesuje się również fenomenologią współczesnych ujemnych zjawisk społecznych, problematyką ekskluzji społecznej oraz resocjalizacji.

Kontakt: k.stepien@apol.edu.pl

Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 53–84

 https://doi.org/10.4467/20801335PBW.25.003.22169

ARTYKUŁ

Rosyjska „specjalna operacja wojskowa" jako nieudany coup de main. Perspektywa analizy wywiadowczej

Russian 'special military operation' as a failed coup de main. An intelligence analysis perspective

MAREK KLASA

Akademia Sztuki Wojennej

https://orcid.org/0000-0003-0863-5601

MICHAŁ KLASA

Autor niezależny

https://orcid.org/0009-0001-1412-0383

Abstrakt

Autorzy dokonują analizy inwazji i działań wywiadowczych jako operacji typu *coup de main*, rozumianych nie jako ścisłe uskutecznianie sztuki wojennej, lecz jako zamach stanu (fr. *coup d'état*) realizowany siłami zewnętrznymi na terytorium atakowanego państwa. *Coup de main* jako skuteczny atak z zaskoczenia wymaga zastosowania infiltracji kontrwywiadu ofensywnego i pacyfikacji oponenta siłami typu policyjnego. W artykule mechanizmy te są analizowane na przykładzie aneksji Krymu dokonanej przez Federację Rosyjską w 2014 r. oraz rosyjskiej inwazji na Ukrainę w 2022 r., którą autorzy przyrównują do inwazji wojsk Układu Warszawskiego

w Czechosłowacji w 1968 r. Zrozumienie takiego modelu agresji wymaga prezentacji instrumentów analizy funkcjonowania państwa autorytarnego.

Słowa kluczowe *coup de main*, zamach stanu, Ukraina, infiltracja, analizy wywiadowcze, logika sytuacyjna

Abstract The authors analyse the invasions and accompanying intelligence activities as *coup de main* operations, understood not as strict execution of the art of war, but rather as a *coup d'état* carried out by external forces on the territory of the attacked state. *Coup de main* as an effective surprise attack requires the use of offensive counterintelligence infiltration and the pacification of the opponent with police-type forces. In the article, these mechanisms are analysed using the example of Soviet actions in countries perceived by Moscow as its sphere of influence, the annexation of Crimea by the Russian Federation in 2014 and the Russian invasion of Ukraine in 2022 historical experience from the Russian invasion of Ukraine in 2022 which the authors compare to the invasion of Czechoslovakia by Warsaw Pact troops in 1968. Understanding this model of aggression requires presenting instruments for analysing how the authoritarian state operates.

Keywords *coup de main*, *coup d'état*, Ukraine, infiltration, intelligence analysis, situational logic

Wprowadzenie

Przedmiotem badań opisanych w artykule jest specyficzny rodzaj działań skierowanych przeciw władzom państwowym i ich aparatowi przymusu, określony terminem *coup de main* (pol. 'cios ręką'). Pojęcie to, zaczerpnięte z literatury anglojęzycznej, przede wszystkim z myśli Edwarda Luttwaka, zostanie opisane szerzej w dalszej części tekstu.

Celem artykułu jest analiza działań Federacji Rosyjskiej (FR) podejmowanych w ramach dwóch aktów agresji na Ukrainę: w 2014 r. i 2022 r. jako operacji *coup de main* w myśl przyjętej definicji operacyjnej. Realizacja celu badań może przyczynić się zarówno do wzrostu świadomości zagrożenia tego typu działaniami, jak i zwiększenia odporności na nie.

Autorzy przyjęli następujące założenia badawcze: instytucje totalne[1], do których można zaliczyć zarówno siły zbrojne, jak i aparat administracyjny w państwach autorytarnych, mają ukryty program, określany w socjologii mianem drugiego życia instytucji totalnej[2]. Odnosząc tę koncepcję do praktyki działania państw autorytarnych, można dostrzec znaczne rozbieżności między formalną doktryną użycia sił zbrojnych a ich faktycznym wykorzystaniem. Jest to dostrzegalne w działaniach Armii Radzieckiej, m.in. w: interwencjach w państwach będących formalnymi sojusznikami ZSRS, działaniach przeciwpartyzanckich i ekspedycyjnych[3]. Federacja Rosyjska przejęła tę spuściznę, a prowadzone przez nią działania wojskowe (w Czeczenii w latach 1994–1996 i 1999–2000, w Gruzji w 2008 r., w Syrii w latach 2015–2024[4] i w Ukrainie od 2014 r.) były odległe od założeń wojny między aktorami państwowymi zbliżonymi do siebie pod względem potencjału. Wynika stąd drugie założenie przyjęte przez autorów – doświadczenia użycia siły militarnej w operacjach po II wojnie światowej zaważyły na funkcjonowaniu Sił Zbrojnych FR w czasie pokoju (czasie „P") i ich sposobie działania podczas inwazji na Ukrainę w 2022 r.

Przyjętym ograniczeniem badawczym jest zawężenie bazy badawczej do studium przypadku dwóch rosyjskich operacji przeciw Ukrainie – aneksji Krymu w 2014 r. i pełnoskalowej inwazji na początku 2022 r. oraz zestawienie tej ostatniej z założeniami interwencji wojsk Układu Warszawskiego w Czechosłowacji w 1968 r. analizowanej na podstawie dokumentacji operacji „Dunaj".

Obszerne badanie interwencji w Czechosłowacji w 1968 r., zarówno pod względem samego sposobu użycia siły, jak i wpływu na inne państwa, przede wszystkim tzw. bloku wschodniego, przeprowadzili: Kent DeBenedictis, Jacques Rupnik, Alexander Stykalin, Slavomír Michálek, Ljubodrag Dimić, Miklós Mitrovits, Mirosław Szumiło, Mihail Gruev, Michal Štefanský i Jakub Drábik oraz Kieran

---

[1] Według Ervinga Goffmanna: „Instytucja totalna to organizacja społeczna, w obrębie której żyje zamknięta, formalnie kontrolowana przez jej personel grupa osób". W oryginale: „A 'total institution' is 'a place of residence and work where a large number of like-situated individuals, cut off from the wider society for an appreciable period of time, together lead an enclosed, formally administered round of life'". Cyt. za: *The Characteristics of Total Institutions*, w: *A Sociological Reader on Complex Organizations*, A. Etzioni (red. nauk.), New York 1961, s. xiii. (Tłumaczenia w tekście pochodzą od autorów – dop. red.).

[2] Tamże, s. 312–338.

[3] Por. В. Триандафиллов, *Характер операций совеременных армий*, Москва 1929 (W. Triandafiłłow, *Charaktier opieracyj sowriemiennych armij*, Moskwa 1929); H. Hermann, *Operacyjny wymiar walki zbrojnej*, Toruń 2004, s. 129–131; M. Depczyński, L. Elak, *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020, s. 233–244, 282–294.

[4] Rosyjska interwencja w Syrii trwała jeszcze po rozpoczęciu pełnoskalowej wojny z Ukrainą.

Williams. Istotny wkład do badanych zagadnień wnieśli Alex Hughes, Marek Świerczek oraz Edward Luttwak[5].

Autorzy niniejszego artykułu wykorzystali badania jakościowe, heurystyczne i teoretyczne, które uzupełnili ustrukturyzowanymi technikami analitycznymi zgodnie z klasyfikacją Randolpha H. Phersona i Richardsa J. Heuera.

Coup de main – definicja operacyjna

Pojęciem *coup de main* posłużono się dla określenia sposobu użycia siły zbrojnej przez agresora[6], który chcąc dokonać zmiany władzy politycznej[7] w zaatakowanym państwie[8], wkracza swoimi siłami (wojskami) na jego terytorium, najczęściej

[5] Zob. szerzej: K. DeBenedictis, *Russian „Hybrid Warfare" and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*, London 2022; *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (red.), Stuttgart 2021 (autorzy rozdziałów: J. Rupnik, A. Stykalin, S. Michálek, L. Dimić, M. Mitrovits, M. Szumiło, M. Gruev, M. Štefanský, J. Drábik); K. Williams, *The Prague Spring and its aftermath: Czechoslovak Politics, 1968–1970*, Cambridge 1997, s. 112–143; A. Hughes, *Plan Z. Reassessing Security-Based Accounts of Russia's Invasion of Ukraine*, „Journal of Advanced Military Studies" 2023, t. 14, nr 2, s. 174–208. https://doi.org/10.21140/mcuj.20231402009; M. Świerczek, *Model infiltracji Jeżowa a zajęcie Krymu przez Federację Rosyjską*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, nr 30, s. 131–157. https://doi.org/10.4467/20801335PBW.24.005.19607; M. Świerczek, *Szturm na siedzibę Służby Bezpieczeństwa Ukrainy w Ługańsku w 2014 r. jako przykład operacji służb specjalnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 28, s. 52–86. https://doi.org/10.4467/20801335PBW.23.002.17652; E.N. Luttwak, *Zamach stanu. Podręcznik*, Warszawa 2017.

[6] Agresorem może być aktor zarówno państwowy, jak i niepaństwowy.

[7] Zmiana ta może zostać dokonana przy zachowaniu formalnej niepodległości zaatakowanego państwa, np. przez obsadzenie rządu marionetkowego kontrolowanego przez agresora.

[8] We wszystkich badanych przez autorów przypadkach *coup de main* został przeprowadzony przeciwko władzom państwowym, co jednak nie stanowi *per se* dowodu na to, że można o nim mówić wyłącznie w odniesieniu do podmiotów państwowych. Autorzy chcą to podkreślić z uwagi na popularną w latach 2001–2022 argumentację dotyczącą „wyjątkowości" (podmioty niepaństwowe miały być wyjątkiem względem zasad strategii) podmiotów państwowych i niemożliwości stosowania dotyczącej ich wiedzy (zwłaszcza dorobku klasyków strategii) do podmiotów niepaństwowych. Por. słowa Christophera Bassforda: „W oszołamiającym pokazie historycznego roztargnienia nasze środowisko bezpieczeństwa narodowego wydaje się […] oszołomione odkryciem, że wojnę mogą prowadzić grupy inne niż weberowskie państwa. […] W obliczu tego, co ewidentnie wielu autorom wydaje się zupełnie nowym rodzajem wojny, prowadzonym przez organizacje takie jak, powiedzmy, Al-Kaida, skłonni są oni używać terminów, które mają na celu uchwycenie ducha tej przełomowej innowacji przez nadanie jej nazwy. Przykładowo: «wojna niepaństwowa», «wojna czwartej (lub piątej) generacji» lub […] «nowe wojny» […]. Być może najbardziej mylący ze wszystkich jest termin «wojna nietrynitarna» ukuty przez Martina van Crevelda […] by podsumować jego rzekomo nowe i «nieclausewitzowskie» podejście do rozważań na temat wojny". Zob. Ch. Bassford, *Na palcach wokół trójcy Clausewitza*, „Kwartalnik Bellona" 2017, t. 688, nr 1, s. 73.

w ugrupowaniu marszowym. Zakłada, że dzięki wywołanemu efektowi szoku nie napotka skutecznego oporu. Preferowaną formą obezwładnienia przeciwnika jest oddziaływanie psychologiczne – w jego wyniku ofiara agresji nie podejmie walki (zbrojnej) i tym samym nie stanie się obrońcą[9]. Rażenie ogniem stosowane jest taktycznie, w sytuacji gdy ofiara agresji stawi opór (stając się obrońcą) lub dla wzmocnienia efektu szoku wobec niestawiającej oporu ofiary (np. bombardowanie niestawiających oporu instalacji wojskowych lub bombardowania terrorystyczne ludności cywilnej). Logika użycia siły w takich działaniach różni się od tej stosowanej w otwartym konflikcie zbrojnym, w którym potencjały stron są zbliżone (ang. *near-peer conflict*).

Na potrzeby badania opisanego w niniejszym artykule sformułowano cztery hipotezy szczegółowe:

1. Działania określone definicją operacyjną *coup de main* mają własną strategię, odmienną niż klasyczna logika konfliktu zbrojnego, a zbliżoną do logiki zamachu stanu (*coup d'état*). Jako sposób weryfikacji tej hipotezy przyjęto metody teoretyczne, w tym opracowanie definicji operacyjnej *coup de main* i zastosowanie jej do wybranych przypadków ujętych w bazie badawczej.
2. Decyzji o przeprowadzeniu „specjalnej operacji wojskowej" jako *coup de main* nie należy wyjaśniać wyłącznie jako błędu racjonalnego aktora lub portretu psychologicznego przywódcy, lecz raczej jako modelowanie zachowań organizacji rzutujące na proces planistyczny. Do weryfikacji tej hipotezy zostały zastosowane ustrukturyzowane techniki analityczne (tabela 1). Wyniki poszczególnych metod przedstawiono w tabelach 3 i 4.
3. Zajęcie Krymu i pierwsza faza rosyjskiej inwazji na Ukrainę na kierunkach: kijowskim, charkowskim i chersońskim były operacjami typu *coup de main*, podobnymi w swych założeniach do interwencji w Czechosłowacji w 1968 r. Do jej weryfikacji zastosowano analogie historyczne, wnioskowanie i abstrahowanie, których wyniki zostały ujęte w tabeli 5.
4. Warunkiem koniecznym dla skutecznego przeprowadzenia operacji typu *coup de main* jest infiltracja wywiadowcza. Jej skala przesądziła o powodzeniu operacji w 2014 r. i niepowodzeniu w 2022 r. Do jej weryfikacji zastosowano te same metody jak do hipotezy trzeciej.

[9] Por. słowa Carla von Clausewitza: „Wojna toczy się raczej dla obrońcy niż dla zdobywcy, gdyż dopiero najazd wywołał obronę, a wraz z nią i wojnę. Zdobywca zawsze jest sposobiony pokojowo (jak to zresztą twierdził stale o sobie Bonaparte), chętnie wkroczyłby do naszego państwa jak najspokojniej. Aby nie mógł tego zrobić, musimy sami pragnąć wojny, a więc ją też przygotować, czyli innymi słowy: sztuka wojenna wymaga aby właśnie słabi, skazani na obronę byli zawsze uzbrojeni, aby nie ulec napadowi". Zob. C. von Clausewitz, *O wojnie*, Lublin 1995, s. 441.

Coup de main jako praktyka działania Federacji Rosyjskiej

Analiza okoliczności, celów i skutków operacji typu *coup de main* wymaga odpowiedniej metodologii. Badania opierające się na obu rozpatrywanych modelach: podejmowania decyzji polityczno-wojskowych oraz funkcjonowania państwa autorytarnego, jakim jest FR, wykorzystują analizę związków przyczynowo-skutkowych[10]. W artykule za punkt wyjścia przyjęto ustrukturyzowane techniki analityczne zgodnie z klasyfikacją Phersona i Heuera, opisane w tabeli 1 wraz z ich zastosowaniem.

Tabela 1. Ustrukturyzowane techniki analityczne określające związki przyczynowo-skutkowe i zastosowanie tych technik w artykule.

Nazwa techniki analitycznej	Opis	Zastosowanie w artykule
Logika sytuacyjna *red hat*	Opinia ekspercka mająca na celu przyjmowanie toku rozumowania rozpracowywanego podmiotu	Elementy metodologii *red hat* stanowią podstawę analizy. Na potrzeby artykułu są syntezowane opinie: • Hieronima Grali i Witolda Jurasza[11], • Andrija Charuka i Mychajły Żyrochowa[12],

[10] R.H. Pherson, R.J. Heuer, *Structured Analytic Techniques for Intelligence Analysis*, [bmw] 2020, s. 361–387.

[11] Hieronim Grala i Witold Jurasz zostali wybrani do analizy *red hat* jako źródła polskie, eksperckie o doświadczeniu praktycznym w dyplomacji na terytorium Rosji. Poddano analizie wywiady: *Czy Jurij Andropow był twórcą pierestrojki? – cykl Oblicza historii*, YouTube, 14 V 2024 r., https://www.youtube.com/watch?v=vbbcuNYaxkU [dostęp: 30 VI 2024]; *ROSYJSKI KRĄG WŁADZY – cykl Kulisy historii odc. 120*, YouTube, 1 VII 2023 r., https://www.youtube.com/watch?v=szr-pwtxV0U [dostęp: 30 VI 2024]; *Rosja Putina – obsesja neoimperialnej potęgi | Czwartki w DeBeKa #1*, YouTube, 29 II 2024 r., https://www.youtube.com/watch?v=rUAgEnRAllw [dostęp: 30 VI 2024]; *Nie będzie końca wojny bez końca Putina: prof. Hieronim Grala – didaskalia #6*, YouTube, 16 IV 2023 r., https://www.youtube.com/watch?v=uTlrecy9m80 [dostęp: 30 VI 2024]; *Debata „Co dalej z Rosją?" – Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J.M. Nowakowski*, YouTube, 4 XII 2023 r., https://www.youtube.com/watch?v=Gk45gw7ECHY [dostęp: 30 VI 2024]; *Elity Zachodu tęsknią za przewidywalną Rosją | Prof. Hieronim Grala*, YouTube, 10 VI 2023 r., https://www.youtube.com/watch?v=K-aU41GKpNmY [dostęp: 30 VI 2024].

[12] Andrij Charuk i Mychajło Żyrochow zostali wybrani do analizy *red hat* jako źródła ukraińskie, eksperckie, mające dostęp do wielu informacji od żołnierzy uczestniczących w walkach stosunkowo niedawno. Źródła wykorzystane na potrzeby analizy *red hat*: А. Харук, М. Жирохов, *Бойова хроніка 2022 року*, Київ 2024 (A. Charuk, M. Żyrochow, *Bojowa chronika 2022 roku*, Kyjiw 2024), s. 49–203; М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (M. Żyrochow, *Newidbutyj blickryh: oborona aerodromiw Hostomela ta Wasylkowa, lutyj 2022 roku*, Czernihiw 2022), s. 4–69; tenże, *Війна танків. Україна, лютий-серпень 2022*, Чернігів 2023 (*Wijna tankiw. Ukrajina, lutyj-serpeń 2022*, Czernihiw 2023), s. 4–88.

Nazwa techniki analitycznej	Opis	Zastosowanie w artykule
Logika sytuacyjna *red hat*	Opinia ekspercka mająca na celu przyjmowanie toku rozumowania rozpracowywanego podmiotu	• Kamila Galiejewa[13], • Williama Spaniela[14] i Marka Galeottiego[15]. Ekspertów dobrano na podstawie metodyki określonej przez Józefa Kozłowskiego[16]
Stosowanie teorii	Zastosowanie teorii i modeli w celu uściślenia okoliczności i warunków występowania określonych zjawisk	W artykule wykorzystano: • model zamachów stanu Edwarda Luttwaka dotyczący rozbieżności między nominalnym[17] a rzeczywistym łańcuchem dowodzenia,

[13] Kamil Galiejew został wskazany do analizy *red hat* jako antyrządowe (opozycyjne) źródło rosyjskie, którego wiarygodność jest trudna do oceny, ale często potwierdzają ją inne analizowane źródła. Galiejewa należy określić bardziej jako autora raportów OSINT niż naukowca, jednak jego obserwacje stanowią cenne uzupełnienie dla prób zrozumienia logiki sytuacyjnej w omawianym przypadku. Zob. K. Galeev (@kamilkazani), wpis na portalu X, 28 II 2022 r., https://x.com/kamilkazani/status/1498377757536968711?lang=en [dostęp: 30 IX 2024]. Pozostałe opozycyjne źródła rosyjskie, takie jak Maksim Kac i Michaił Zygar nie były przyjmowane do tworzenia tez logiki sytuacyjnej w ramach techniki *red hat*.

[14] Wiliam Spaniel został wskazany do analizy *red hat* jako ekspert anglojęzyczny. Jest profesorem nadzwyczajnym (Associate Professor) na Uniwersytecie w Pittsburgu, specjalizuje się w problematyce teorii gier i jej zastosowaniu na potrzeby analiz strategii i polityki. Źródła wykorzystane na potrzeby analizy *red hat*: W. Spaniel, *What Caused the Russia-Ukraine War (And How Will It End?)*, e-book; tenże, *How Ukraine Survived: Inside the Strategy to Stop Russia's Invasion*, e-book; tenże, *Why Russia Miscalculated in Ukraine: A Self-Inflicted Disaster in Three Acts*, YouTube, 24 I 2023 r., https://www.youtube.com/watch?v=8YkGrKQXZxE [dostęp: 25 I 2023]; tenże, *The Hidden Battle that Saved Ukraine*, YouTube, 3 I 2023 r., https://www.youtube.com/watch?v=hh9xT9d6SJU [dostęp: 25 I 2023]; tenże, *The "Battle" of Crimea: Inside Russia's Playbook to Capture the Peninsula*, YouTube, 15 III 2023 r., https://www.youtube.com/watch?v=Ijmoz2VfjrQ [dostęp: 25 IX 2024].

[15] Mark Galeotti został wybrany do analizy *red hat* jako drugi ekspert anglojęzyczny. Pracuje jako senior researcher i koordynator w Centre for European Security, Institute of International Relations Prague (Centrum Bezpieczeństwa Europejskiego Instytutu Stosunków Międzynarodowych w Pradze). Źródła wykorzystane na potrzeby analizy *red hat*: M. Galeotti, *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [bmw] 2023; tenże, *Putin's wars. From Chechnya to Ukraine*, Oxford 2022; tenże, *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022 r., https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins-security-council-meeting-a76522 [dostęp: 1 IX 2024].

[16] J. Kozłowski, *Praktyczny wymiar zagadnień związanych z oceną pewności źródeł oraz wiarygodności danych i informacji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 29, s. 95–130. https://doi.org/10.4467/20801335PBW.23.021.18763.

[17] E.N. Luttwak, *Zamach stanu. Podręcznik*…, s. 59.

Nazwa techniki analitycznej	Opis	Zastosowanie w artykule
Stosowanie teorii	Zastosowanie teorii i modeli w celu uściślenia okoliczności i warunków występowania określonych zjawisk	wiedzę psychologiczną na temat mechanizmu walki lub ucieczki albo też niestawiania czynnego oporu (ang. *fight or flight*), • modele podejmowania decyzji przez państwo w ujęciu Grahama Allisona[18]
Analogie historyczne	Próba zrozumienia zachodzących procesów przez porównanie z historycznymi odpowiednikami	Analiza wskazuje na podobieństwa z innymi operacjami tego typu: inwazją wojsk Układu Warszawskiego na Czechosłowację w 1968 r., opanowaniem Krymu w 2014 r. jako operacją typu *coup de main*, a także rosyjską inwazją na Ukrainę w 2022 r. W przypadku niedoboru informacji nt. Sowietów autorzy artykułu będą rozumować per analogiam względem struktur PRL lub innych państw socjalistycznych w okresie zimnej wojny

Źródło: opracowanie własne na podstawie: R.H. Pherson, R.J. Heuer, *Structured Analytic Techniques for Intelligence Analysis*, [bmw] 2020, s. 361–387.

W ramach metody *red hat*, opisanej w tabeli 1, sformułowano trzy tezy logiki sytuacyjnej na podstawie opinii eksperckich:

1. Zamiast analizy Rosji jako racjonalnego aktora i analiz psychologicznych Władimira Putina jako jedynego przywódcy, należy analizować „kolektywnego Putina" – modele organizacyjne i pałacowe struktury władzy.
2. Pomimo że Rosja eksponuje swoje siły zbrojne i prezentuje się przede wszystkim jako potęga militarna, rola armii w polityce jest bardzo niewielka. Czynnikiem mającym wpływ na państwo (m.in. na myślenie

[18] G. Allison, P. Zelikow, *Essence of Decision. Explaining the Cuban Missile Crisis*, Addison-Wesley Educational Publishers Inc., 1999, s. 18–25. Do tego typu analizy można zastosować również inne techniki, które w tym artykule zostaną pominięte. Stanowią one jednak użyteczne instrumentarium dla bardziej rozbudowanych opracowań poświęconych np. koncepcji diady wywiadowczej czy stopniom zaangażowania wojska w politykę państwa wg Samuela Edwarda Finera.

przywódców) jest Federalna Służba Bezpieczeństwa (FSB) i to ona jest najważniejszym resortem siłowym.

3. Rosyjskie wojska działają w praktyce jako siły pacyfikacyjne. Oficjalna doktryna nie znajduje wielkiego przełożenia w konfliktach zbrojnych ostatnich kilkudziesięciu lat. Rok 2022 był pierwszym od zakończenia II wojny światowej, w którym rosyjskie wojska musiały zmierzyć się na polu walki z regularną armią dobrze uzbrojonego wroga.

Następnie w odniesieniu do FR zastosowano modele podejmowania decyzji opisane przez Grahama Allisona: państwo jako racjonalny aktor, model zachowań organizacji oraz model polityki rządu (tabela 2).

Tabela 2. Modele decyzyjne według Grahama Allisona w odniesieniu do Federacji Rosyjskiej.

Model	**Opis w kontekście Federacji Rosyjskiej**
Państwo jako racjonalny aktor (ang. *rational actor model*) – w którym zachowanie państwa w przestrzeni międzynarodowej jest porównywane do działań świadomej jednostki (osoby)	Do tego modelu można przyporządkować działania Rosji w ścisłym ujęciu polityki międzynarodowej jako podmiotu dążącego m.in. do: • podporządkowania sobie Ukrainy jako państwa satelickiego, dokonania aneksji części lub całości jej terytorium w zależności od rezultatu inwazji, • wzmocnienia swojej pozycji względem USA i NATO przez zademonstrowanie sprawczości w Europie Wschodniej, co zwiększy szansę na akceptację ultimatów względem wschodniej flanki Sojuszu
Model zachowań organizacji (ang. *organizational behavior model*) – działania państwa jako wynikowa struktur, procedur i utartych sposobów działania służb i instytucji	Model zachowań organizacyjnych może wskazywać na kilka podmiotów organizacyjnych wewnątrz Rosji, które miały wpływ na planowanie i przebieg wojny, m.in.: FSB, Główny Zarząd Wywiadowczy Sztabu Generalnego FR (GRU), Główny Zarząd Operacyjny Sztabu Generalnego FR, Dowództwo Sił Operacji Specjalnych. W kontekście aneksji Krymu w 2014 r. kluczową rolę planistyczną odgrywał Główny Zarząd Operacyjny, którego szef jest zwyczajowo pierwszym zastępcą Szefa Sztabu Generalnego. Organ ten najprawdopodobniej posiadał część planów przygotowywanych jeszcze w latach 90. XX w. Pomimo okazjonalnych sporów z Ministerstwem Obrony Główny Zarząd Operacyjny Sił Zbrojnych Federacji Rosyjskiej otrzymał zadanie zaplanowania szczegółów aneksji Krymu, co zakończyło się sukcesem m.in. dzięki rozpoczęciu prac planistycznych już w styczniu, jeszcze przed zapadnięciem decyzji politycznych na najwyższym szczeblu. Znaczący udział w końcowym etapie przygotowań miały również FSB i GRU

Model	Opis w kontekście Federacji Rosyjskiej
Model zachowań organizacji (ang. *organizational behavior model*) – działania państwa jako wynikowa struktur, procedur i utartych sposobów działania służb i instytucji	W 2011 r. utworzono Dowództwo Sił Operacji Specjalnych, które miało kierować specjalnymi operacjami wojskowymi. Jego rola wzrastała systematycznie od udanej aneksji Krymu i interwencji w Syrii, aczkolwiek jego prestiż przekładający się na zwiększoną rolę w kontekście inwazji na Ukrainę w 2022 r. można uznać za błąd w podejściu do stosowania sił specjalnych jako doborowych jednostek do ataku frontowego[19]. W związku z powiązaniami z modelem polityki rządu kluczowy wpływ na rozpatrywane w artykule decyzje podjęte przez FR mają przede wszystkim służby specjalne z FSB jako czynnikiem o największym wpływie na władzę, z rolą sił zbrojnych jako efektora o ograniczonym wpływie na decyzje szczebla centralnego. Należy zwrócić uwagę, że w organizacji rosyjskiego wywiadu za obszar posowiecki odpowiada FSB, co świadczy o tym, że państwa tzw. bliskiej zagranicy nie są traktowane jako „pełnoprawna zagranica"
Model polityki rządu (ang. *governmental politics model*) – model pałacowy, dworski, analizujący zależności wynikające z cech osobowości i wzajemnych powiązań, najbliższego otoczenia liderów itd.	Zgodnie z tezą 1 logiki sytuacyjnej należy przeanalizować decyzje kolektywu o największym wpływie na politykę państwa

Źródło: opracowanie własne na podstawie: M. Galeotti, *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [bmw] 2023, s. 22–23.

Zajęcie Krymu w 2014 r. jako udany coup de main

Preludium do inwazji z 24 lutego 2022 r. było podjęcie osiem lat wcześniej decyzji o rozpoczęciu aneksji Krymu[20] przez Radę Bezpieczeństwa Federacji Rosyjskiej, RBFR (ros. Совет Безопасности Российской Федерации). Jej realizacja doprowadziła do aneksji przez FR Autonomicznej Republiki Krymu, będącej częścią Ukrainy. Złożona natura tego typu operacji wymaga, by poddać badaniu dwa aspekty: twardej

[19] A. Liflyandchick, D. Jones, S. Fabian, *The Fall from Grace of Russian SOF: The Danger of Forgetting Lessons Learned*, Irregular Warfare Center: Insights, t. 1, nr 8, September 2023.

[20] William Spaniel przypuszcza, że decyzja ta mogła zostać podjęta jeszcze wcześniej. Na przykład rosyjski medal „Za odzyskanie Krymu" wskazuje czas operacji od 20 II do 18 III. Aczkolwiek 20 II doszło do incydentu w Czerkasach, wykorzystywanego przez Rosję propagandowo. Zob. W. Spaniel, *The "Battle" of Crimea: Inside Russia's Playbook*…

siły (ang. *hard power*) i polityczny. Analiza posiedzeń RBFR jest o tyle istotna, że obie decyzje zostały przyjęte na posiedzeniach w bardzo podobnym składzie osobowym[21].

Pierwszą kwestią w aspekcie twardej siły jest stosunek liczebny ukraińskich i rosyjskich sił na Półwyspie Krymskim w 2014 r., które – według szacunków opublikowanych przez Defence Express – początkowo były wyrównane. Rosja dysponowała ok. 18 300 wojskowymi, w tym 11 000 marynarzami Floty Czarnomorskiej, 2000 żołnierzy piechoty morskiej i 5300 Specnazu. Kolejne 15 000 żołnierzy oczekiwało nad Cieśniną Kerczeńską od strony Kraju Krasnodarskiego[22]. Ukraina miała początkowo dysponować 14 600 żołnierzami i marynarzami[23]. Stosunek sił szybko zmieniał się jednak na korzyść Rosji, która przeniosła na Krym dodatkowych 6000 żołnierzy.

Drugą kwestią w aspekcie twardej siły jest tempo zajmowania terytorium. Od 27 lutego do 4 marca Rosji udało się przejąć kontrolę nad głównymi miastami, w tym stolicą Autonomicznej Republiki Krymu – Symferopolem, jak również nad Przesmykiem Perekopskim, łączącym Półwysep Krymski z resztą Ukrainy. Siły zbrojne FR zablokowały ukraińskie jednostki w Bałakławie, Sewastopolu, Belbeku, Saki, Eupatorii, Nowoozernym, Czornomorskiem, Teodozji, Kerczu, Weselu i Dżankoju. Rosyjskie działania w powietrzu, m.in. loty transportowe Ił-76 na lotniska w Sewastopolu i Gwardiejsku czy loty śmigłowcowe w innych częściach półwyspu, nie były w żadnym stopniu zakłócane. Rosyjskie oddziały prowadziły też rozpoznanie na 3 km poza granice Krymu, do obwodu chersońskiego.

Specyfiką aneksji Krymu okazało się to, że rosyjskie wojska były już obecne na półwyspie wskutek umów z Ukrainą, a miejsca ich stałej dyslokacji znajdowały się bardzo blisko ukraińskiej infrastruktury wojskowej. Rosyjskie jednostki, zarówno te opuszczające bazy wojskowe Floty Czarnomorskiej, jak i dyslokowane

---

[21] W posiedzeniu uczestniczyli: Dmitrij Miedwiediew, Walentina Matwiejenko, Siergiej Naryszkin, Siergiej Iwanow, Nikołaj Patruszew, Raszyd Nurgalijew, Siergiej Ławrow, Władimir Kołokolcew, Siergiej Szojgu, Aleksander Bortnikow, Michaił Fradkow i Borys Gryzłow. Niestety, Kreml nie opublikował transkryptu ani nagrania z tego spotkania, co uniemożliwia porównanie przebiegu posiedzeń przed aneksją Krymu 27 II 2014 r. i pełnoskalową inwazją 24 II 2022 r. wg źródeł otwartych. Zob. *Meeting with permanent members of the Security Council*, Kremlin.ru, 21 II 2014 r., http://en.kremlin.ru/events/president/news/20301 [dostęp: 24 IX 2024]. Galeotti twierdzi, że faktycznie uczestniczyli w tym posiedzeniu wyłącznie przedstawiciele resortów siłowych (tzw. siłowików), ale tylko szef resortu obrony Szojgu zajmował raczej ostrożne stanowisko, z obawy przed międzynarodowymi reperkusjami. Zob. M. Galeotti, *Putin's wars. From Chechnya to Ukraine*…, s. 170.

[22] *Standoff: A chronicle of Russian invasion of Crimea*, Defense Express, 4 III 2014 r., https://web.archive.org/web/20230226183728/https://issuu.com/ukrainian_defense_review/docs/chronicles-of-russian--aggression-cr [dostęp: 13 VII 2025].

[23] A. Wilk, *Rosyjska interwencja wojskowa na Krymie*, Ośrodek Studiów Wschodnich, 5 III 2014 r., https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [dostęp: 29 IX 2024].

na półwysep z terytorium Rosji, mogły szybko przemieszczać się po Krymie, bez konieczności przekraczania chronionej granicy państwowej.

„Specjalna operacja wojskowa" – uwarunkowania planistyczne, model zachowań organizacji

W lipcu 2021 r. Rosja utworzyła komórkę (na bazie 5. Służby FSB[24]) odpowiedzialną za planowanie inwazji. Jej zadaniem było zbadanie podatności Ukrainy na interwencję, a za jej podstawowy wyznacznik przyjęto postawę ukraińskiego społeczeństwa, zobrazowaną przez badania opinii publicznej. Wzięte pod uwagę wyniki badań ukraińskiej opinii publicznej wskazywały na niskie zaufanie do rządzących, zobojętnienie względem sytuacji politycznej i koncentrację na problemach gospodarczych, przy równoczesnym określeniu pełnoskalowego konfliktu zbrojnego między Rosją a Ukrainą jako mało prawdopodobnego. Zgodnie z analizami kluczowe znaczenie dla opinii publicznej miały: energetyka, ciepłownictwo oraz finanse[25]. Z perspektywy czasu można uznać za nadinterpretację przez stronę rosyjską wyników badań opinii publicznej – sporządzonych na bazie problemów życia codziennego omawianych w ankietach – w których nie wzięto pod uwagę radykalnej mobilizacji społeczeństwa do stawienia oporu w obliczu agresji zbrojnej[26]. Tymczasem to m.in. właśnie kwestie kryzysu socjoekonomicznego na Ukrainie, emigracji zarobkowej i rachunków za prąd czy gaz były istotnym elementem przemówienia

[24] Federalna Służba Bezpieczeństwa Federacji Rosyjskiej dzieli się na „służby" wyróżnione numerami, podobnie jak oddziały Sztabu Generalnego. Numer 5 to Służba Informacji Operacyjnej i Kontaktów Zagranicznych (ros. Служба оперативной информации и международных связей, SOIMS). Odpowiada ona za kontakty ze służbami zagranicznymi, w tym SBU. Należy zauważyć, że szef 5. Służby, generał-pułkownik Siergiej Biesieda w latach 2003–2004 kierował Zarządem Koordynacji Informacji Operacyjnej Departamentu Analiz, Prognoz i Planowania Strategicznego FSB FR, jednostki prowadzącej wywiad na terytorium krajów Wspólnoty Niepodległych Państw, po latach braku pionu wywiadu zagranicznego w strukturze FSB. Przebywał w Kijowie podczas Euromajdanu, a przed inwazją 2022 r. odpowiadał zarówno za tworzenie piątej kolumny na terytorium Ukrainy, jak i za prace analityczne przygotowań do inwazji. Zob. A. Soldatov, *The True Role of the FSB in the Ukrainian Crisis*, The Moscow Times, 15 IV 2014 r., https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985 [dostęp: 28 IX 2024]; M. Minkina, *FSB. Gwardia Kremla*, Warszawa 2016, s. 93, 175.

[25] M. Zabrodskyi i in., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022 r., s. 7.

[26] Jeżeli informacje podane przez Royal United Services Institute są prawdziwe, to należy to uznać za poważny błąd analizy wywiadowczej. O ile nie jest możliwe jego dokładne skategoryzowanie bez dostępu do treści tych raportów, o tyle można przypuszczać, że była to forma np. błędu ewaluacji w postaci braku krytycznej oceny doboru i oceny badań opinii publicznej. Por. J. Kozłowski, *Metody, techniki i narzędzia analityczne*, cz. III, Warszawa 2024.

Putina z 21 lutego 2022 r.[27] Wydaje się to właściwą poszlaką do dalszych badań opierających się na przyjętych modelach decyzyjnych (opisanych w tabeli 2), biorąc pod uwagę, że większość opracowań z tego zakresu wskazuje na błąd Rosjan w ocenie sytuacji jedynie w zakresie przecenienia przez FSB swojej siatki agentów na terytorium Ukrainy[28] lub też przeszacowania zdolności sił własnych i niedoszacowania ich u przeciwnika[29].

Niewystarczająca według rosyjskich władz była też skuteczność wojsk użytych w działaniach przeciwko Gruzji w 2008 r., dlatego podjęto się reform i inwestycji w SZFR. Po ich wprowadzeniu aneksja Krymu w marcu 2014 r. i działania nieregularne prowadzone w obwodach ługańskim i donieckim przebiegły pomyślnie, podobnie jak rosyjska interwencja podczas wojny domowej w Syrii we wrześniu 2015 r. W czasie wizyty w Moskwie w listopadzie 2021 r. szef CIA William Burns ocenił, że Rosjanie są przekonani o swojej gotowości do zajęcia Ukrainy, a ich demonstracje siły nie mają być wyłącznie próbą zastraszenia[30]. Ocena ta była wyolbrzymiona wskutek rozwijania się w autorytarnych systemach władzy tendencji do ograniczania krytyki, uwypuklonej przez kulturę *wranjo*[31], która uniemożliwiała likwidację problemu korupcji w wojsku. Plan „specjalnej operacji wojskowej" przewidywał, że od dziesiątego dnia inwazji wiodąca rola wojsk lądowych zostanie zastąpiona przejęciem kontroli nad operacją przez rosyjskie służby specjalne oraz siły Rosgwardii, których zadaniem byłaby pacyfikacja ewentualnego niezadowolenia społecznego i ustanowienie administracji okupacyjnej. W ramach przygotowań do inwazji FSB trenowała z Wojskami Powietrznodesantowymi Federacji Rosyjskiej (WDW) realizację zadań określanych w anglojęzycznej terminologii wojskowej jako *kill-or-capture*[32]. Następnie plan zakładał akcję przeszukiwania mieszkań i ustanowienie obozów filtracyjnych w celu stworzenia kartotek materiałów do wykorzystania przez

---

[27] „Od 2014 roku rachunki za wodę wzrosły o jedną trzecią, a rachunki za energię wzrosły kilkukrotnie, tak samo kilkukrotnie wzrosły opłaty za gaz. Wielu ludzi po prostu nie ma pieniędzy do opłacenia rachunków. Oni dosłownie walczą o przetrwanie". Cyt. za: *Обращение Президента Российской Федерации*, Президент России (*Obraszczenije priezidienta Rossijskoj Fiedieracyi*, Priezidient Rossii), 21 II 2022 r., http://kremlin.ru/events/president/news/67828 [dostęp: 27 IX 2024].

[28] A.S. Bowen, *Russia's War in Ukraine: Military and Intelligence Aspects*, Congressional Research Service Report, Washington 2023, s. 6.

[29] M. Minkina, *Rosyjskie instrumentarium wpływu, nękania i prowokacji*, Siedlce 2023, s. 186–188.

[30] W. Spaniel, *How Ukraine Survived*…

[31] *Standoff: A chronicle of Russian invasion of Crimea*…

[32] W języku polskim tłumaczone jako 'zabić lub pojmać/zniszczyć lub przechwycić' – w zależności od kontekstu. Por. B. Jagodziński, *Działania i rozwój jednostek specjalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, t. 12, nr 22, s. 169; Ł. Kułaga, *Używanie dronów w celu zwalczania międzynarodowego terroryzmu w świetle „ius in bello"*, „Zeszyty Prawnicze" 2017, t. 17, nr 1, s. 109. https://doi.org/10.21697/zp.2017.17.1.05.

ofensywny kontrwywiad, jak również zastraszenia i wytypowania Ukraińców, którzy mieli zostać wysiedleni do Rosji. Planowano sprowadzenie nauczycieli i urzędników z Rosji na terytoria okupowane w celu reedukacji Ukraińców. Po wyeliminowaniu ukraińskiego rządu i parlamentu do władzy wyniesiono by prorosyjski „Ruch Pokojowy". Istotnym elementem planowania było zajęcie ukraińskich elektrowni atomowych i ustanowienia w nich baz wojskowych i magazynów uzbrojenia, w celu szantażu energetycznego podbitej ludności oraz szantażu politycznego wobec państw europejskich zagrożeniem skażenia radioaktywnego[33]. Przygotowania do inwazji zostały przeprowadzone pod pozorem ćwiczeń „Zachód-2021" (ros. Запад-2021) oraz „Sojusznicze zdecydowanie-2022" (ros. Союзная решимость-2022), pod pretekstem którego przeprowadzono koncentrację i rozwinięcie wojsk.

Kręgi decyzyjne Federacji Rosyjskiej – model polityki rządu

Przedmiotem analizy na potrzeby uproszczonego modelu polityki rządowej mogą być wypowiedzi z posiedzenia RBFR z 21 lutego 2022 r. (opublikowane dzień później), stanowiące preludium do wojny. Spotkanie to można określić jako próbę sił przy „kolektywnym Putinie", biorąc pod uwagę zasłonięte kamery na sali obrad, jak również wypowiedź Putina, stwierdzającego, że przebiegiem tych rozmów testuje swoich doradców[34]. Mark Galeotti analizuje to posiedzenie jako wskaźnik podziału na grupy poszczególnych uczestników (tabela 3). W konkluzji swojego artykułu Galeotti podkreślił również zauważalny podział na zaufanych ludzi prezydenta i pracowników instytucjonalnych zasiadających w RBFR[35]. Rola pozostałych uczestników nie została poddana analizie.

Tabela 3. Model polityki rosyjskiego rządu – podział na frakcje w Radzie Bezpieczeństwa Federacji Rosyjskiej.

Określenie frakcji	Członkowie
wojowniczy	Aleksander Bortnikow, Nikołaj Patruszew, Siergiej Szojgu
spolegliwi	Walentina Matwijenko, Dmitrij Miedwiediew, Władimir Kołokolcew

[33] M. Zabrodskyi i in., *Preliminary Lessons in Conventional Warfighting*…, s. 10–11.

[34] *Заседание Совета Безопасности* (*Zasiedanije Sowieta Biezopasnosti*), YouTube, 22 II 2022 r., https://www.youtube.com/watch?v=_YRUlb_7T9o [dostęp: 28 IX 2024].

[35] M. Galeotti, *The Personal Politics of Putin's Security Council Meeting*…

Określenie frakcji	Członkowie
sceptycy	Siergiej Ławrow, Michaił Miszustin, Dmitrij Kozak
oporni	Siergiej Naryszkin

Źródło: opracowanie własne na podstawie: M. Galeotti, *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022 r., https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins-security-council-meeting-a76522 [dostęp: 1 IX 2024].

W tabeli 4 przedstawiono opis wystąpień 15 uczestników posiedzenia RBFR w dniu 21 lutego 2022 r.

Tabela 4. Model polityki rosyjskiego rządu – opis uczestników posiedzenia Rady Bezpieczeństwa Federacji Rosyjskiej z 21 lutego 2022 r. według kolejności wystąpień.

Imię i nazwisko	Stanowisko	Komentarz
Władimir Putin	prezydent	Skupił się na zagrożeniu dla zaanektowanego Krymu z powodu ewentualnego akcesu Ukrainy do NATO
Siergiej Ławrow[36]	minister spraw zagranicznych	Wskazywał na możliwość dalszych rozmów z USA
Dmitrij Kozak[37]	zastępca szefa kancelarii Prezydenta Federacji Rosyjskiej, przedstawiciel w rozmowach mińskich	Stwierdził brak perspektyw dla dalszych negocjacji i zapytał o możliwość rozważenia aneksji tzw. Donieckiej Republiki Ludowej (DNR) i Ługańskiej Republiki Ludowej (ŁNR). Putin w dość lekceważący sposób zbył pytanie Kozaka i zamiast tego wspomniał o konieczności uznania suwerenności tych republik

[36] O ile pozycja polityczna Ławrowa była silna w czasie prezydentury Miedwiediewa, o tyle zarówno w kontekście decyzji z 2014 r., jak i 2022 r. Ławrow wydawał się znajdować poza wewnętrznym kręgiem decyzyjnym. Pytaniem otwartym jest, czy został od niego odsunięty, czy też odsunął się od niego z własnej woli.

[37] Urodzony i wychowany w Ukrainie. Specjalista ds. operacji sterowanego separatyzmu w tzw. bliskiej zagranicy, w szczególności w Naddniestrzu w Mołdawii. Jego pozycja w kręgach władzy była słaba i ograniczona do zaufania dla jego kompetencji merytorycznych u prezydenta (Galeotti w otoczeniu Putina rozróżnia urzędników zawdzięczających swoją pozycję kompetencjom merytorycznym przydatnym w rządzeniu państwem (merytokracja), oraz zaufanych prezydenta, których wpływy wynikają z bliskich relacji z nim (koterii)). Zob. O. Sukhov, *From Olympics to Crimea, Putin Loyalist Kozak Entrusted With Kremlin Mega-Projects*, The Moscow Times, 28 III 2014 r., https://www.themoscowtimes.com/archive/from-olympics-to-crimea-putin-loyalist-kozak-entrusted-with-kremlin-mega-projects [dostęp: 1 IX 2024].

Imię i nazwisko	Stanowisko	Komentarz
Aleksander Bortnikow[38]	szef Federalnej Służby Bezpieczeństwa	Mówił przede wszystkim na temat bezpieczeństwa granicy w obwodach sąsiadujących z Ukrainą i napływu uchodźców z terytoriów separatystycznych republik
Siergiej Szojgu[39]	minister obrony	Przekazywał propagandowe informacje o rzekomym ostrzale Ługańska i Doniecka przez Ukrainę, katastrofie humanitarnej w separatystycznych republikach, gotowości Ukrainy do inwazji na te terytoria, prowadzenia działań terrorystycznych i prób uzyskania broni jądrowej przez Ukrainę
Dmitrij Miedwiediew	wiceprzewodniczący Rady Bezpieczeństwa	Powołał się na doświadczenia z wojny z Gruzją w 2008 r. i stwierdził, że USA nieustannie prowadzą operacje specjalne na całym świecie, a potem mocarstwa i tak wracają do rozmów ze sobą, z pominięciem państw, które są przedmiotami, a nie podmiotami polityki mocarstwowej
Wiaczesław Wołodin	przewodniczący Dumy Państwowej	W imieniu Dumy Państwowej wnosił o uznanie DNR i ŁNR
Walentina Matwijenko	przewodnicząca Rady Federacji	Argumentowała, że zachodnią broń mogą przejąć „nacjonaliści i banderowcy". Może to wskazywać na nieświadomość argumentu „denazyfikacji" (za Maksimem Kacem z Fundacji Walki z Korupcją Aleksieja Nawalnego – rozbieżności w retoryce stosowanej przez poszczególnych uczestników posiedzenia świadczyły o tym, kto był wtajemniczony w plan przeprowadzenia inwazji w momencie, kiedy odbywało się posiedzenie), który zostanie użyty jako jeden z pretekstów do inwazji

Kozak utrzymywał kontakt z Andrijem Jermakiem, szefem administracji prezydenta Ukrainy Wołodymyra Zełenskiego. Zob. K. Skorkin, *Why President Zelensky Is Purging His Inner Circle*, Carnegie, 15 IV 2024 r., https://carnegieendowment.org/russia-eurasia/politika/2024/04/why-president-zelensky-is-purging-his-inner-circle?lang=en [dostęp: 28 IX 2024].

[38] Wywodzący się z Departamentu Bezpieczeństwa Ekonomicznego (4. Departament) wraz Patruszewem może być uznany za najbliższy krąg prezydenta.

[39] Wywodzący się z mniejszości etnicznej, nie utworzył skutecznej frakcji oligarchicznej z pozostałymi osobami z wewnętrznego kręgu władzy. Nieprzerwanie na stanowiskach ministerialnych od 1994 r. Można go scharakteryzować jako lojalnego wykonawcę o ograniczonych kompetencjach własnych, który nie narusza status quo. Przeniesiony do armii ze struktur Ministerstwa ds. Sytuacji Nadzwyczajnych, nie kontynuował reform Anatolija Serdiukowa i skupił się na działaniach o charakterze fasadowym. Zob. W. Jurasz, H. Grala, *Wataha Putina*, Warszawa 2023, s. 74.

Imię i nazwisko	Stanowisko	Komentarz
Igor Krasnow	Prokurator Generalny	Wystąpienie wycięto z oficjalnego zapisu
Nikołaj Patruszew[40]	sekretarz Rady Bezpieczeństwa	Skoncentrował się na bezzasadności dalszych rozmów, zwłaszcza z podmiotami innymi niż USA
Michaił Miszustin	premier	Ocenił zdolność gospodarki Rosji do działania w wypadku zachodnich sankcji
Siergiej Naryszkin	szef Służby Wywiadu Zagranicznego	Wnosił o „danie jeszcze jednej szansy zachodnim partnerom na wywarcie wpływu na Ukrainę", jakoby w zgodzie z Nikołajem Patruszewem, ale na tyle odmiennym sposobem argumentacji, że należy interpretować to stanowisko jako zalecenie wstrzymywania się od inwazji. Ponadto pomieszał kwestie uznania suwerenności i aneksji separatystycznych republik. Podczas posiedzenia Putin potraktował go w sposób upokarzający[41]
Władimir Kołokolcew	minister spraw wewnętrznych	Ograniczył się do inwektyw pod adresem Ukrainy i państw Zachodu
Igor Szczygolew	przedstawiciel prezydenta w Centralnym Okręgu Federalnym	Ograniczył się do inwektyw pod adresem Ukrainy i państw Zachodu
Wiktor Zołotow	dowódca Rosgwardii	Ograniczył się do inwektyw pod adresem Ukrainy i państw Zachodu

Źródło: opracowanie własne na podstawie: *Заседание Совета Безопасности* (*Zasiedanije Sowieta Biezopasnosti*), YouTube, 22 II 2022 r., https://www.youtube.com/watch?v=_YRUlb_7T9o [dostęp: 28 IX 2024].

Po niepowodzeniach inwazji stanowisko utracił Siergiej Szojgu, a jego zastępca Timur Iwanow został aresztowany w związku z zarzutami korupcyjnymi[42].

[40] Patruszew to były szef FSB, którego ze względu na zażyłe relacje z Putinem jeszcze z lat 90. XX w. należy uważać za część wewnętrznego kręgu władzy. Zainteresowany ciągłością wpływów powierzył swoim synom ważne stanowiska. Grala przypisuje mu krytyczną ocenę jedności rosyjskich elit w przededniu inwazji, która nie pojawiła się w nagraniu z posiedzenia RBFR. Tamże, s. 65.

[41] Relacje Naryszkina z kręgiem Putina i FSB można określić jako skomplikowane ze względu na konflikt organizacyjny między FSB a SWZ i „nadworną" rolę bezpieki w systemie władzy.

[42] М. Кац, *Арестован замминистра обороны Иванов* (M. Kac, *Ariestowan zamministra oborony Iwanow*), YouTube, 24 IV 2024 r., https://www.youtube.com/watch?v=5p4S7AKBPOg [dostęp: 28 IX 2024].

Ministrem obrony został, wywodzący się ze środowisk naukowo-przemysłowych[43], Andriej Biełousow. Stanowisko sekretarza Rady utracił Nikołaj Patruszew, który jednak później wrócił do niej w charakterze doradcy[44]. W stały skład gremium powrócił zaś Siergiej Iwanow (na mało znaczące stanowisko, ale według opinii eksperckich skład osobowy gremium jest w tym ujęciu ważniejszy od formalnych stanowisk). Warto dodać, że po niepowodzeniach planu inwazji z 2022 r. rola tego gremium istotnie zmalała[45].

Hughes wskazał na brak dogłębnych analiz dotyczących wpływu decyzji polityczno-frakcyjnych i podkreślił, że w literaturze przeważają proste czy wręcz trywialne wnioski (pomyłka, niedocenienie przeciwnika)[46]. Autorzy pragną zwrócić uwagę, że modele służbowo-organizacyjne (model zachowań organizacji) i rządowo-urzędowe (model polityki rządu), choć przedstawione w sposób oględny, mogą pozwolić na przełamanie tego impasu.

Inwazja Rosji na Ukrainę w 2022 r. jako nieudany coup de main

Rosyjska inwazja na Ukrainę rozpoczęta 24 lutego 2022 r. spotkała się z rozbieżnymi reakcjami opinii publicznej oraz ośrodków decyzyjnych w świecie zachodnim. Wypowiedzi polityków i ewakuacje personelu dyplomatycznego sugerowały, że Ukraina nie wytrzyma naporu rosyjskich wojsk[47]. Skuteczny opór Ukrainy był dla wielu zaskoczeniem. Skuteczność tego oporu diametralnie zmieniła ocenę potęgi

[43] Połączenie organizacyjne instytucji naukowych i zakładów przemysłowych, charakterystyczne dla rosyjskiego przemysłu obronnego i zaawansowanych technologii podwójnego przeznaczenia. Zob. И.В. Устинович, *Научно-промышленный комплекс как одна из форм взаимодействия организаций*, „Труды БГТУ" 2023 (I.W. Ustinowicz, *Nauczno-promyszlennyj kompleks kak odna iz form wzaimodiejstwija organizacyj*, „Trudy BGTU" 2023), t. 5, nr 2, s. 72–77.

[44] *Putin to keep demoted ally Patrushev on Russia's Security Council*, Reuters, 12 VII 2024 r., https://www.reuters.com/world/europe/putin-keep-demoted-ally-patrushev-russias-security-council-2024-06-11/ [dostęp: 28 IX 2024]; *Security Council structure*, President of Russia, http://www.en.kremlin.ru/structure/security-council/members [dostęp: 28 IX 2024].

[45] G. Kuczyński, *Zmiany w Radzie Bezpieczeństwa Federacji Rosyjskiej*, Warsaw Institute, 14 II 2023 r., https://warsawinstitute.org/pl/zmiany-w-radzie-bezpieczenstwa-federacji-rosyjskiej/ [dostęp: 28 IX 2024].

[46] A. Hughes, *Plan Z. Reassessing Security-Based…*, s. 174–208.

[47] Zob. np. S. Westfall, *These countries are withdrawing embassy staffers from Ukraine amid growing fears of an invasion by Russia*, The Washington Post, 14 II 2022 r., https://www.washingtonpost.com/world/2022/01/25/ukraine-embassy-evacuations/ [dostęp: 21 IX 2024]; S. Walker, *'It is past time to leave Ukraine': western diplomats flee Kyiv*, The Guardian, 13 II 2022 r., https://www.theguardian.com/world/2022/feb/13/it-is-past-time-to-leave-ukraine-western-diplomats-flee-kyiv [dostęp: 21 IX 2024].

wojskowej FR. Decyzję rosyjskich władz o rozpoczęciu inwazji siłami niewystarczającymi (w rozumieniu sztuki wojennej[48]) dla opanowania tak wielkiego terytorium postrzegano jako działanie nieracjonalne[49]. Biorąc pod uwagę logikę sytuacyjną, jest to realizacja scenariusza zaobserwowanego wcześniej na Węgrzech (1956 r.), w Czechosłowacji (1968 r.) czy Afganistanie (1979 r.). Posługiwanie się przez Rosję określeniem „specjalna operacja wojskowa" jest postrzegane jako zabieg czysto propagandowy, mający tłumić prawdę o wojnie[50]. Przeprowadzona analiza pozwala określić, dlaczego w rozumieniu rosyjskich przywódców nieudana próba opanowania Ukrainy w lutym 2022 r. miała dokonać się jako „specjalna operacja wojskowa", a nie wojna konwencjonalna. W związku z mieszanym charakterem działań, w których wykorzystano struktury siłowe Ministerstwa Obrony i Spraw Wewnętrznych oraz struktury wywiadowcze, powstaje chaos pojęciowy.

O ile na wschodzie Ukrainy rosyjskie wojska działały metodycznie, najprawdopodobniej na podstawie dużo wcześniej przygotowanych planów, o tyle na północy SZFR zakładały szybkie przemieszczanie się kolumnami w ugrupowaniu marszowym, aby osiągnąć cel strategiczny, czyli Kijów. Priorytetowym komponentem *coup de main* na tym obszarze był desant wojsk aeromobilnych na Port Lotniczy Hostomel, mający umożliwić przerzut drogą powietrzną znacznych sił WDW, do których miały dołączyć jeszcze siły przebywające na terytorium Białorusi. Atak na Kijów z kierunku północnego na prawym brzegu Dniepru (dla strony ukraińskiej – Poleski Rejon Operacyjny) mógł wydawać się rosyjskim planistom szczególnie obiecujący ze względu na najkrótszy dystans do pokonania, brak konieczności forsowania Dniepru i brak stałej dyslokacji dużych jednostek Sił Zbrojnych Ukrainy, SZU (ukr. Збройні сили України) na tym odcinku. Rejon planowanych działań był zabezpieczony wyłącznie przez jednostki Państwowej Straży Granicznej Ukrainy (ukr. Державна прикордонна служба України), Gwardii Narodowej Ukrainy (ukr. Національна гвардія України) i 200 strażników Czarnobylskiej Elektrowni Atomowej[51] (ukr. Чорнобильська атомна електростанція, CzAES). Ponadto strefa wykluczenia wokół nieczynnej elektrowni atomowej stanowiła znaczny, praktycznie niezamieszkały obszar (100–150 osób na 2600 km^2), który

---

[48] Przykładowe obliczenia zob. C.A. Lawrence, *The Battle for Kyiv. The fight for Ukraine's capital*, [bmw] 2023, s. 50–64.

[49] T. Cooper i in., *War in Ukraine. Volume 2: Russian Invasion, February 2022*, Warwick 2023, s. 33.

[50] Por. *Dylematy rosyjskiej propagandy. „Specjalna operacja wojskowa straciłaby sens"*, Onet, 27 XII 2022 r., https://wiadomosci.onet.pl/swiat/dylematy-rosyjskiej-propagandy-specjalna-operacja-wojskowa-stracilaby-sens/2f1tlb0 [dostęp: 21 IX 2024]; M. Hess, *Vladimir Putin finally calls Russia's 'special military operation' a war*, UnHerd, 21 II 2023 r., https://unherd.com/newsroom/vladimir-putin-finally-calls-russias-special-military-operation-a-war/ [dostęp: 21 IX 2024].

[51] М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю*…, s. 11.

można łatwo kontrolować. Zagrożenie radiacyjne z wojskowego punktu widzenia zostało uznane za nieistotne[52]. Ważne dla rosyjskich planistów było natomiast to, że główne ćwiczenia obronne Ukrainy „Zamieć-2022" (ukr. Заметіль-2022) nie zakładały istotnych walk na tym odcinku. Zgodnie z wynikami przeprowadzonej analizy rejonu operacyjnego Rosjanie dokonali tam koncentracji wojsk pod pretekstem ćwiczeń „Sojusznicze zdecydowanie-2022" trwających od 10 do 20 lutego 2022 r. Znaczne siły zostały dyslokowane na prawy brzeg Dniepru po stronie białoruskiej.

Początkowe sukcesy w Poleskim Rejonie Operacyjnym Rosjanie zawdzięczali przede wszystkim prawidłowo zrealizowanym elementom operacji typu *coup de main*, czyli atakiem z zaskoczenia z terytorium Białorusi, której minister obrony, Wiktor Chrenin, deklarował w rozmowach z kierownictwem politycznym Ukrainy, że wyklucza atak rosyjskich wojsk z tego terytorium[53]. Udało się zaskoczyć ukraińskie jednostki pograniczne i Gwardii Narodowej, które nie zdążyły wysadzić mostów drogowego i kolejowego w tym rejonie. Przejęte pojazdy tych jednostek zostały z kolei wykorzystane do prowokacji rosyjskich grup dywersyjno-rozpoznawczych. Grupy te dotarły do Kijowa i działały na sprzęcie z ukraińskimi oznaczeniami, przez co wprowadzały chaos na pozycjach obrońców, dopóki grupy rozpoznawczo-dywersyjne (ros. Диверсионно-разведывательная группа, ДРГ) nie zostały zlikwidowane[54]. W związku z tym, że 167 żołnierzy 1 samodzielnego batalionu ochrony szczególnie ważnych obiektów Gwardii Narodowej Ukrainy nie było przeszkolonych z zakresu walki z pojazdami opancerzonymi ani nie posiadało stosownego uzbrojenia, poddali się, kiedy rosyjskie czołgi i transportery wjechały na teren CzAES. Na niekorzyść obrońców działała ponadto działalność szpiegowska zwerbowanego przez Rosjan oficera SBU, Andrija Naumowa, który przekazał nieprzyjacielowi plany obrony rejonu, jak również miał kontakty w formacjach ochraniających strefę wykluczenia. Zaskoczenie wywołane desantem na Hostomel wiąże się z kolei z kontrowersyjną rolą podwójnego agenta Denysa Kiriejewa, który – mimo że ostrzegł władze w Kijowie o możliwym ataku – został zlikwidowany przez SBU[55]. O ile w źródłach zachodnich nie doceniono obrońców lotniska i stwierdzono, że pozycje obronne Hostomelu były wskazywane przez rosyjskiego

[52] А. Харук, М. Жирохов, *Бойова хроніка*…, s. 50.

[53] М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю*…, s. 4–9.

[54] Tamże, s. 10–19.

[55] B. Forrest, *Russian Spy or Ukrainian Hero? The Strange Death of Denys Kiryeyev*, The Wall Street Journal, 18 I 2023 r., https://www.wsj.com/articles/russian-spy-or-ukrainian-hero-the-strange-death-of-denys-kiryeyev-11674059395 [dostęp: 29 IX 2024].

agenta ulokowanego w Antonowie[56], o tyle ukraińskie źródła nie potwierdziły tej informacji. Wprost przeciwnie, opór przez jednostkę terytorialnej obrony lotniska stanowił istotną przeszkodę dla desantu i spowodował utratę sprzętu, ludzi i czasu względem planu działania, co potwierdzają dowody z pola bitwy[57]. Pomimo wycofania się z lotniska i budynków koszarowych sił obrony terytorialnej po wyczerpaniu amunicji oraz trudności z pełną likwidacją doborowych rosyjskich formacji przez ukraińskie siły szybkiego reagowania, to zniszczenie lądowiska przez ukraińską artylerię wyeliminowało zagrożenie lądowania na lotnisku samolotów transportowych WDW. Były one zmuszone lądować na terytorium Białorusi. Z kolei akcje dywersyjno-sabotażowe wobec lotniska w Wasylkowie nie zdołały wyłączyć tej bazy z użytkowania[58].

W trakcie ataku rosyjskie kolumny nie prowadziły odpowiednich działań rozpoznawczych, spieszenia piechoty z bojowymi wozami piechoty ani przygotowania artyleryjskiego lub saperskiego, dopóki nie zostały do tego zmuszone przez opór obrońców[59], co jest elementem charakterystycznym operacji typu *coup de main*. Z tego względu rozciągnięte rosyjskie kolumny, które nie zajęły miast w obwodach sumskim i czernichowskim, takich jak: Głuchów, Konotop, Niżyn, Sumy, Romny i Pryłuki, miały coraz większe trudności z zabezpieczeniem logistyki przed atakami SZU. W momencie ataku 9 marca 2022 r. na podkijowskie Browary były to niepoprawnie zabezpieczone linie zaopatrzenia o długości prawie 400 km[60]. Gdyby opór obrońcy udało się przełamać przez infiltrację kontrwywiadu ofensywnego, trudności logistyczne nie byłyby na tyle uciążliwe, by stanowiły decydującą przeszkodę dla kontynuowania operacji. Tymczasem wbrew założeniom planistów „specjalnej operacji wojskowej", wobec oporu i ataków obrońców Ukrainy na kolumny transportowe, doszło do sparaliżowania logistyki najbardziej wysuniętych oddziałów. W związku z tym operacja kijowska jako *coup de main* zakończyła się niepowodzeniem.

Bezpośredni atak na Charków opierał się przede wszystkim na kolumnach Specnazu przypuszczających ataki typu rajd za pomocą lekko opancerzonych pojazdów Tigr. Próba zajęcia z marszu wybranego obiektu administracyjnego nie była możliwa w związku z oporem obrońców i zamiast tego grupa szturmowa

---

[56] W. Spaniel, *How Ukraine Survived*…

[57] *Destination Disaster: Russia's Failure At Hostomel Airport*, Oryx, 13 IV 2022 r., https://www.oryxspioenkop.com/2022/04/destination-disaster-russias-failure-at.html [dostęp: 29 IX 2024].

[58] М. Жирохов, *Невідбутий бліцкриг*…, s. 60–70.

[59] А. Харук, М. Жирохов, *Бойова хроніка*…, s. 35–36.

[60] Dla porównania – najdłuższy „skok" wykonany przez rosyjskie kolumny na Krymie z Kerczu do Armiańska wynosił 288 km w sprzyjających warunkach.

opanowała budynek szkoły. Po długotrwałych walkach została jednak zlikwidowana. Należy zauważyć, że oddziały Specnazu zostały powstrzymane i zlikwidowane w terenie zurbanizowanym przez oddziały ukraińskiej Gwardii Narodowej oraz jednostki improwizowane m.in. ze składu osobowego Charkowskiego Narodowego Uniwersytetu Sił Powietrznych im. Iwana Kożeduba, czy też z czołgów znajdujących się w dyspozycji Charkowskiego Instytutu Wojsk Pancernych[61]. Z kolei kolumna Oddziału Mobilnego Specjalnego Przeznaczenia, OMON (ros. отряд мобильный особого назначения), została zniszczona na podejściu do miasta, niedaleko wsi Wesele, przez ukraińskie czołgi z 92 brygady, wobec których siły przeznaczone do tłumienia demonstracji nie posiadały ani stosownego uzbrojenia, ani nie miały przeszkolenia[62].

Jedyne sukcesy operacyjne Rosjanie odnieśli na kierunku chersońskim, gdzie udało im się przejąć elektrownię wodną w Nowej Kachowce, Most Antonowski i miasta: Chersoń, Mikołajów i Wozniesieńsk (w którym wykorzystano skuteczniej niż w Hostomelu komponent aeromobilny[63]). Część tych osiągnięć można przypisywać również infiltracji wywiadowczej ukraińskich struktur siłowych, zwłaszcza SBU[64].

Operacja na kierunku kijowskim miała więc charakterystyczne cechy *coup de main*, podczas gdy działania na froncie w Donbasie miały charakter klasycznych działań zbrojnych. Nie zakładano w nich przełamania oporu za sprawą nagłości działań i przytłaczającego użycia siły, lecz klasyczne natarcie frontalne z zamiarem wypchnięcia przeciwnika z zajmowanych pozycji, po wcześniejszym przygotowaniu ogniowym (artyleryjskim i lotniczo-rakietowym).

Zgodnie z założeniami przedstawionymi we *Wprowadzeniu* autorzy uznali operację „Dunaj" z 1968 r. za właściwą analogię historyczną dla działań FR w 2022 r. Była to operacja stanowiąca przykład realnych działań Armii Radzieckiej, prowadzonych wraz z sojusznikami, a zarówno przygotowania do niej, jak i jej przebieg mają liczne cechy wspólne, które można zanalizować pod kątem charakterystyki *coup de main* przyjętej na potrzeby artykułu. Porównanie pierwszej fazy rosyjskiej inwazji na Ukrainę z 2022 r. jako nieudanej operacji *coup de main* z inwazją 2 Armii Wojska Polskiego w składzie Połączonych Sił Układu Warszawskiego na Czechosłowację w 1968 r. przedstawia tabela 5.

---

[61] А. Харук, М. Жирохов, *Бойова хроніка*…, s. 111–118.

[62] М. Жирохов, *Війна танків. Україна, лютий-серпень 2022*…, s. 49–54.

[63] А. Харук, М. Жирохов, *Бойова хроніка*…, s. 165–173.

[64] K. Gustafson i in., *Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022*, „Intelligence and National Security" 2024, t. 39, nr 3, s. 405. https://doi.org/10.1080/02684527.2024.2322214.

Tabela 5. Porównanie sposobów działania wojsk Układu Warszawskiego przeciw Czechosłowacji w operacji „Dunaj" w 1968 r. z działaniami wojsk Federacji Rosyjskiej w pierwszej fazie inwazji na Ukrainę na kierunku kijowskim w 2022 r.

Cecha charakterystyczna	Operacja „Dunaj" 1968 r.	Pierwsza faza inwazji na Ukrainę na kierunku kijowskim w 2022 r.
Decepcja	Przygotowania do inwazji zostały przeprowadzone pod pozorem ćwiczeń „Pochmurne Lato 1968"	Przygotowania do inwazji zostały przeprowadzone pod pozorem ćwiczeń „Zachód-2021" oraz „Sojusznicze zdecydowanie-2022"
Ugrupowanie	10 i 11 Dywizje Pancerne zostały pozbawione artylerii rakietowej, ciężkiego sprzętu inżynieryjnego i części komponentu logistycznego. Te same zmiany dotyczyły 4 Dywizji Zmechanizowanej (DZ) w rezerwie 2 Armii. Siły użyte w operacji zostały wzmocnione jednostkami aeromobilnymi i dalekiego rozpoznania	Charakterystyczne było ugrupowanie rosyjskie na frontach północnym i południowym. Duża część sił znajdowała się w ugrupowaniu marszowym i z opóźnieniem przechodziła w bojowe, pomimo napotkania zdecydowanego oporu. Było to szczególnie widoczne na froncie północnym, gdzie siły rosyjskie dysponowały ok. 70 000 żołnierzy, z czego ok. 15 000–30 000 żołnierzy w rozciągniętej w szczytowym momencie na 64 km kolumnie maszerującej na Kijów. Nietypowa była także kompozycja tych sił, gdzie oprócz jednostek Sił Zbrojnych Federacji Rosyjskiej[65] w ich skład wchodziły: 141 Specjalny Pułk Zmotoryzowany (Czeczeński), jednostki Rosgwardii (Specjalnego Oddziału Szybkiego Reagowania – SOBR), OMON i prywatnej firmy wojskowej Reduta
Tempo	Czas na osiągnięcie celów 70–100 km od granicy: 6–12 godzin w kierunku Pragi i Brna. Kolejnych 12 godzin dla 4 DZ na dotarcie do wyznaczonych celów pod Pragą	Dokumenty przejęte pod Chersoniem wiosną 2022 r. wskazują, że np. 1 batalionowa grupa taktyczna z 810 Brygady Piechoty Morskiej miała między 20 lutego a 6 marca 2022 r. osiągnąć cele pomiędzy Odessą a Mikołajowem, 200 km od swoich pozycji początkowych

[65] W skład jednostek Sił Zbrojnych Federacji Rosyjskiej na froncie północnym w okresie 24 II–8 IV 2022 r. wchodziły związki operacyjne: 1 Gwardyjska Armia Pancerna, 35 Armia Ogólnowojskowa, 36 Armia Ogólnowojskowa; związki taktyczne: 90 Gwardyjska Dywizja Pancerna, 11 Gwardyjska Brygada Powietrznodesantowa, 31 Gwardyjska Brygada Powietrznodesantowa.

Cecha charakterystyczna	Operacja „Dunaj" 1968 r.	Pierwsza faza inwazji na Ukrainę na kierunku kijowskim w 2022 r.
Blokady	4 DZ i 27 Pułk Czołgów z 5 Dywizji Pancernej miały za zadanie blokować czechosłowackie garnizony w miastach Mladá Boleslav i Milovice. Wzmocniona czołgami i jednostkami rozpoznania 6 Dywizji Powietrzno-Desantowej z 16 Dywizji Zmechanizowanej miały zaś zablokować garnizony w miejscowościach: Rychów, Kostelec nad Labem, Rokytnice v Orlických horách i Červená Voda	W 2022 r. nie udało się Rosjanom blokować garnizonów tak, jak miało to miejsce na Krymie w 2014 r.
Jednostki pomocnicze	15 Pułk Wojsk Obrony Wewnętrznej miał blokować garnizon w Knowie	Dużą część rosyjskiego ugrupowania stanowiły oddziały Rosgwardii, OMON i SOBR
Stosunek sił obrońcy i agresora	Zakładano, że obrońcy będą dysponować 19 820 żołnierzami przeciwko 14 400 żołnierzom agresora, 456–490 czołgami, 350–405 transporterami opancerzonymi. Zakładany stosunek sił pomiędzy Wojskiem Polskim[66] a Czechosłowacką Armią Ludową wynosił: – ludzi (ogółem): 1:1,4 – czołgów: 1:1,1 – transporterów opanc.: 1,3:1. Z uwzględnieniem gotowości bojowej zakładano, że stosunek sił miałby się wyrównać do 1:1. W związku z tym można zauważyć, że przeprowadzona operacja 2 Armii nie przewidywała stosunku sił właściwego dla ofensywy (agresor nie był dostatecznie liczny względem obrońcy)[67]	Inwazja została zrealizowana przy pomocy ok. 190 000 rosyjskich żołnierzy, co wobec liczebności sił obrońców ok. 196 600 i 102 000 funkcjonariuszy milicji daje stosunek 1:1,57. Dane odnośnie do liczebności ukraińskich sił są zróżnicowane, ale nie ulega wątpliwości, że rosyjskie siły nie dysponowały przewagą liczebną (3:1) właściwą dla prowadzenia ofensywy[68]

[66] Nieoficjalnie: Ludowym Wojskiem Polskim (LWP). Sposób zapisu tej nazwy jest kontrowersyjny. Por. H.Z. Figura, *Ludowe Wojsko Polskie czy Wojsko Polskie?*, „Kwartalnik Bellona" 2015, t. 681, nr 2, s. 215–218.

[67] AIPN, Zbiór dokumentów dotyczących Układu Warszawskiego, *Operacja „Dunaj" dot. interwencji członków Układu Warszawskiego w Czechosłowacji*, t. 1 sygn. BU 02958/1: Sprawy operacyjne Sztabu Generalnego WP, t. 2 sygn. BU 02958/2: Sprawozdania operacyjne Sztabu Generalnego Wojska Polskiego. Sprawozdanie 2 Armii z przebiegu operacji „Dunaj".

[68] *The Military Balance 2022. The annual assessment of global military capabilities and defence economics*, [bmw] 2022.

Cecha charakterystyczna	Operacja „Dunaj" 1968 r.	Pierwsza faza inwazji na Ukrainę na kierunku kijowskim w 2022 r.
Cele z zakresu dowodzenia, kontroli, komunikacji i wywiadu (ang. *command control, communications and intelligence* – C3I)	Szczególną uwagę poświęcono przejęciu ośrodków transmisji telewizyjnej i radiowej w Czechosłowacji, a także lotnisk. Kontrola środków łączności miała kluczowe znaczenie dla umożliwienia wzmożonych działań propagandowych, a lotniska mogły umożliwić siłom inwazyjnym transport lotniczy. Operacja nie powiodła się z powodu niewystarczających badań dotyczących czechosłowackiego systemu łączności, co stworzyło konieczność zajęcia obiektu[69]	Niemożność zniszczenia ukraińskich systemów dowodzenia i łączności spowodowała, że nie osiągnięto celów politycznych „specjalnej operacji wojskowej" zarówno przez zamach stanu (próba osadzenia Wiktora Medwedczuka w Kijowie), jak i *coup de main* w głównych miastach Ukrainy, co ostatecznie zmusiło rosyjskie siły do odwrotu
Interwencja zewnętrzna	Plan uwzględniał możliwość interwencji sił NATO z Republiki Federalnej Niemiec dla wsparcia Czechosłowaków, co stwarzało ryzyko zmiany charakteru operacji z pacyfikacyjnej na bojową	Brak informacji o uwzględnieniu w planach „specjalnej operacji wojskowej" wariantu zagranicznej interwencji zbrojnej
Logistyka	Duża część logistyki opierała się na transporcie kolejowym, gdyż wydolność transportu drogowego była niewystarczająca	„Specjalna operacja wojskowa" była planowana w oderwaniu od wzorców doktrynalnych dotyczących wykorzystania siły zbrojnej w konflikcie konwencjonalnym. Formacje zostały przygotowane na potrzeby krótkiego konfliktu. Wsparcie logistyczne nie nadążało za operacją. Użycie sił rosyjskich nie było zgodne ani z możliwościami logistycznymi, ani ze sposobem organizacji rosyjskiej armii. Logistyka została dostosowana dopiero do działań w Donbasie w 2022 r.[70], które stanowiły już klasyczne działania frontowe, a nie *coup de main*

[69] Na potrzeby badań nad operacjami przerwania łączności, można spekulować, czy ostrożne planowanie operacji „Malwa" przed ogłoszeniem stanu wojennego w 1981 r. przez Sztab Generalny WP było spowodowane niepowodzeniem operacji „Dunaj" w tym zakresie. Zob. AIPN, Ministerstwo Spraw Wewnętrznych w Warszawie [1944] 1954–1990, *Sprawa obiektowa kryptonim „Gotowość" dot. wprowadzenia stanu wojennego. Materiały archiwalne przekazane przez Wydział XII Departamentu II MSW do Archiwum Biura „C" MSW*, sygn. BU 0236/254.

[70] P. Schwartz i in., *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023, s. 68.

Cecha charakterystyczna	Operacja „Dunaj" 1968 r.	Pierwsza faza inwazji na Ukrainę na kierunku kijowskim w 2022 r.
Komponent powietrzny	Jednostki powietrznodesantowe Wojska Polskiego działały jako część komponentu lądowego. W Pradze radzieccy spadochroniarze samolotów cywilnych zdołali przejąć lotnisko przez podszycie się pod samoloty cywilne. Umożliwiło to transport lotniczy wojsk inwazyjnych i materiałów bezpośrednio do stolicy Czechosłowacji	Próba przejęcia przez Rosję lotniska Hostomel w pobliżu Kijowa skorelowana z nadejściem kolumny sił lądowych z Białorusi przez bagna Prypeci była kluczowym założeniem wykonania *coup de main*. Niepowodzenie w zdobyciu lotniska w pobliżu stolicy było jednym z głównych czynników stojących za porażką operacji i początkiem wojny konwencjonalnej na innych obszarach

Źródło: opracowanie własne na podstawie: AIPN, Zbiór dokumentów dotyczących Układu Warszawskiego, *Operacja „Dunaj" dot. interwencji członków Układu Warszawskiego w Czechosłowacji*, t. 1 sygn. BU 02958/1: Sprawy operacyjne Sztabu Generalnego WP, t. 2 sygn. BU 02958/2: Sprawozdania operacyjne Sztabu Generalnego Wojska Polskiego. Sprawozdanie 2 Armii z przebiegu operacji „Dunaj"; А. Харук, М. Жирохов, *Бойова хроніка 2022 року*, Київ 2024 (A. Charuk, M. Żyrochow, *Bojowa chronika 2022 roku*, Kyjiw 2024); М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (M. Żyrochow, *Newidbutyj blickryh: oborona aerodromiw Hostomela ta Wasylkowa, lutyj 2022 roku*, Czernihiw 2022); *The Military Balance 2022. The annual assessment of global military capabilities and defence economics*, [bmw] 2022; M. Zabrodskyi, J. Watling, O.V. Danylyuk, N. Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022 r.; M. Štefanský, *„Operation Danube"*, w: *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (red.), Stuttgart 2021; P. Schwartz, A. Fink, J. Waller, M. Kofman, B. Lennox, M. Chesnut, *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023.

Podsumowanie

W ramach badań autorzy zajęli się problematyką specyficznego sposobu użycia siły, określonego terminem *coup de main* na potrzeby stworzenia definicji operacyjnej, użytej następnie do weryfikacji hipotez roboczych, zgodnie z przyjętymi metodami badawczymi.

Cel badań w postaci analizy działań FR w dwóch aktach agresji na Ukrainę: w 2014 r. i 2022 r., jako operacji *coup de main* został zrealizowany dzięki weryfikacji kolejnych hipotez roboczych z wykorzystaniem wybranych metod badawczych.

Autorzy wysuwają trzy wnioski:

1. Operacje *coup de main* mogą być prowadzone przez Rosję w przyszłości.
2. W odniesieniu do Ukrainy ten model użycia siły, wykorzystany z sukcesami w 2014 r., w 2022 r. się wyczerpał. Może on stanowić realny model dla

ewentualnej interwencji Rosji w Białorusi i Kazachstanie, a także w państwach wschodniej flanki NATO: Litwie, Łotwie i Estonii, w szczególności na tych obszarach, na których występuje duża mniejszość rosyjska.

3. Jak wskazano w części analitycznej artykułu, sukces tego typu operacji wymaga właściwej infiltracji przeciwnika, co w przypadku Polski, która nie była częścią ZSRR, ani nie ma licznej mniejszości rosyjskiej, jest bardzo mało prawdopodobne. Natomiast ze względu na bliskość geograficzną Warszawy do granicy z Białorusią należy rozważać bezpieczeństwo stolicy w sytuacji podjęcia próby śmiałego działania z zaskoczenia w celu pokonania przeciwnika jednym uderzeniem, tj. klasycznie rozumianego *coup de main*.

Można także założyć, że percepcja rosyjskich decydentów ma kluczowe znaczenie przy wyborze metody realizacji celu politycznego przez przeprowadzenie operacji wojskowej. Należy przyjąć, że wewnętrzne uwarunkowania w rosyjskich strukturach decyzyjnych (w tym kwestie frakcyjne) będą miały większe znaczenie niż czynniki intersubiektywne natury geopolitycznej, np. w postaci przynależności danego państwa do organizacji międzynarodowych. Wewnętrzna stabilność danego państwa będącego potencjalnym celem operacji *coup de main* może odgrywać większą rolę niż np. obecność licznej mniejszości rosyjskiej na jego terytorium.

Bibliografia

Allison G., Zelikow P., *Essence of Decision. Explaining the Cuban Missile Crisis*, Addison-Wesley Educational Publishers Inc., 1999.

Bassford Ch., *Na palcach wokół trójcy Clausewitza*, „Kwartalnik Bellona" 2017, t. 688, nr 1, s. 73–100.

Clausewitz C. von, *O wojnie*, Lublin 1995.

Cooper T., Fontanellaz A., Crowther E., Sipos M., *War in Ukraine. Volume 2: Russian Invasion, February 2022*, Warwick 2023.

Depczyński M., Elak L., *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020.

Figura H.Z., *Ludowe Wojsko Polskie czy Wojsko Polskie?*, „Kwartalnik Bellona" 2015, t. 681, nr 2, s. 215–218.

Galeotti M., *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [bmw] 2023.

Galeotti M., *Putin's wars. From Chechnya to Ukraine*, Oxford 2022.

Gustafson K., Lomas D., Wagner S., Shaaban Abdalla N., Davies P.H.J., *Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022*, „Intelligence and National Security" 2024, t. 39, nr 3, s. 400–419. https://doi.org/10.1080/02684527.2024.2322214.

Hermann H., *Operacyjny wymiar walki zbrojnej*, Toruń 2004.

Hughes A., *Plan Z. Reassessing Security-Based Accounts of Russia's Invasion of Ukraine*, „Journal of Advanced Military Studies" 2023, t. 14, nr 2, s. 174–208. https://doi.org/10.21140/mcuj.20231402009.

Jagodziński B., *Działania i rozwój jednostek specjalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, t. 12, nr 22, s. 167–184.

Jurasz W., Grala H., *Wataha Putina*, Warszawa 2023.

Kozłowski J., *Metody, techniki i narzędzia analityczne*, cz. III, Warszawa 2024.

Kozłowski J., *Praktyczny wymiar zagadnień związanych z oceną pewności źródeł oraz wiarygodności danych i informacji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 29, s. 95–130. https://doi.org/10.4467/20801335PBW.23.021.18763.

Kułaga Ł., *Używanie dronów w celu zwalczania międzynarodowego terroryzmu w świetle „ius in bello"*, „Zeszyty Prawnicze" 2017, t. 17, nr 1, s. 107–134. https://doi.org/10.21697/zp.2017.17.1.05.

Lawrence C.A., *The Battle for Kyiv. The fight for Ukraine's capital*, [bmw] 2023.

Liflyandchick A., Jones D., Fabian S., *The Fall from Grace of Russian SOF: The Danger of Forgetting Lessons Learned*, Irregular Warfare Center: Insights, t. 1, nr 8, September 2023.

Luttwak E.N., *Zamach stanu. Podręcznik*, Warszawa 2017.

Minkina M., *FSB. Gwardia Kremla*, Warszawa 2016.

Minkina M., *Rosyjskie instrumentarium wpływu, nękania i prowokacji*, Siedlce 2023.

Pherson R.H., Heuer R.J., *Structured Analytic Techniques for Intelligence Analysis*, [bmw] 2020.

Spaniel W., *How Ukraine Survived: Inside the Strategy to Stop Russia's Invasion*, e-book.

Spaniel W., *What Caused the Russia-Ukraine War (And How Will It End?)*, e-book.

Štefanský M., „*Operation Danube*", w: *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (red.), Stuttgart 2021.

The Characteristics of Total Institutions, w: *A Sociological Reader on Complex Organizations*, A. Etzioni (red. nauk.), New York 1961.

Literatura rosyjska i ukraińska

Харук А., Жирохов М., *Бойова хроніка 2022 року*, Київ 2024 (Charuk A., Żyrochow M., *Bojowa chronika 2022 roku*, Kyjiw 2024).

Триандафиллов В., *Характер операций совеременных армий*, Москва 1929 (Triandafiłłow W., *Charaktier opieracyj sowriemiennych armij*, Moskwa 1929).

Устинович И.В., *Научно-промышленный комплекс как одна из форм взаимодействия организаций*, „Труды БГТУ" 2023 (Ustinowicz I.W., *Nauczno-promyszlennyj kompleks kak odna iz form wzaimodiejstwija organizacyj*, „Trudy BGTU" 2023), t. 5, nr 2, s. 72–77.

Жирохов М., *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (Żyrochow M., *Newidbutyj blickryh: oborona aerodromiw Hostomela ta Wasylkowa, lutyj 2022 roku*, Czernihiw 2022).

Жирохов М., *Війна танків. Україна, лютий-серпень 2022*, Чернігів 2023 (Żyrochow M., *Wijna tankiw. Ukrajina, lutyj-serpeń 2022*, Czernihiw 2023).

Źródła internetowe

Czy Jurij Andropow był twórcą pierestrojki? – cykl Oblicza historii, YouTube, 14 V 2024 r., https://www.youtube.com/watch?v=vbbcuNYaxkU [dostęp: 30 VI 2024].

Debata „Co dalej z Rosją?" - Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J. M. Nowakowski, YouTube, 4 XII 2023 r., https://www.youtube.com/watch?v=Gk45gw7ECHY [dostęp: 30 VI 2024].

Destination Disaster: Russia's Failure At Hostomel Airport, Oryx, 13 IV 2022 r., https://www.oryxspioenkop.com/2022/04/destination-disaster-russias-failure-at.html [dostęp: 29 IX 2024].

Dylematy rosyjskiej propagandy. „Specjalna operacja wojskowa straciłaby sens", Onet, 27 XII 2022 r., https://wiadomosci.onet.pl/swiat/dylematy-rosyjskiej-propagandy-specjalna-operacja-wojskowa-stracilaby-sens/2f1tlb0 [dostęp: 21 IX 2024].

Elity Zachodu tęsknią za przewidywalną Rosją | Prof. Hieronim Grala, YouTube, 10 VI 2023 r., https://www.youtube.com/watch?v=KaU41GKpNmY [dostęp: 30 VI 2024].

Forrest B., *Russian Spy or Ukrainian Hero? The Strange Death of Denys Kiryeyev*, The Wall Street Journal, 18 I 2023 r., https://www.wsj.com/articles/russian-spy-or-ukrainian-hero-the-strange-death-of-denys-kiryeyev-11674059395 [dostęp: 29 IX 2024].

Galeev K. (@kamilkazani), wpis na portalu X, 28 II 2022 r., https://x.com/kamilkazani/status/1498377757536968711?lang=en [dostęp: 30 IX 2024].

Galeotti M., *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022 r., https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins-security-council-meeting-a76522 [dostęp: 1 IX 2024].

Hess M., *Vladimir Putin finally calls Russia's 'special military operation' a war*, UnHerd, 21 II 2023 r., https://unherd.com/newsroom/vladimir-putin-finally-calls-russias-special-military-operation-a-war/ [dostęp: 21 IX 2024].

Kuczyński G., *Zmiany w Radzie Bezpieczeństwa Federacji Rosyjskiej*, Warsaw Institute, 14 II 2023 r., https://warsawinstitute.org/pl/zmiany-w-radzie-bezpieczenstwa-federacji-rosyjskiej/ [dostęp: 28 IX 2024].

Meeting with permanent members of the Security Council, Kremlin.ru, 21 II 2014 r., http://en.kremlin.ru/events/president/news/20301 [dostęp: 24 IX 2024].

Nie będzie końca wojny bez końca Putina: prof. Hieronim Gala – didaskalia #6, YouTube, 16 IV 2023 r., https://www.youtube.com/watch?v=uTlrecy9m80 [dostęp: 30 VI 2024].

Putin to keep demoted ally Patrushev on Russia's Security Council, Reuters, 12 VII 2024 r., https://www.reuters.com/world/europe/putin-keep-demoted-ally-patrushev-russias-security-council-2024-06-11/ [dostęp: 28 IX 2024].

Rosja Putina – obsesja neoimperialnej potęgi | Czwartki w DeBeKa #1, YouTube, 29 II 2024 r., https://www.youtube.com/watch?v=rUAgEnRAllw [dostęp: 30 VI 2024].

ROSYJSKI KRĄG WŁADZY – cykl Kulisy historii odc. 120, YouTube, 1 VII 2023 r., https://www.youtube.com/watch?v=szr-pwtxV0U [dostęp: 30 VI 2024].

Security Council structure, President of Russia, http://www.en.kremlin.ru/structure/security-council/members [dostęp: 28 IX 2024].

Skorkin K., *Why President Zelensky Is Purging His Inner Circle*, Carnegie, 15 IV 2024 r., https://carnegieendowment.org/russia-eurasia/politika/2024/04/why-president-zelensky-is-purging-his-inner-circle?lang=en [dostęp: 28 IX 2024].

Soldatov A., *The True Role of the FSB in the Ukrainian Crisis*, The Moscow Times, 15 IV 2014 r., https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985 [dostęp: 28 IX 2024].

Spaniel W., *The "Battle" of Crimea: Inside Russia's Playbook to Capture the Peninsula*, YouTube, 15 III 2023 r., https://www.youtube.com/watch?v=Ijmoz2VfjrQ [dostęp: 25 IX 2024].

Spaniel W., *The Hidden Battle that Saved Ukraine*, YouTube, 3 I 2023 r., https://www.youtube.com/watch?v=hh9xT9d6SJU [dostęp: 25 I 2023].

Spaniel W., *Why Russia Miscalculated in Ukraine: A Self-Inflicted Disaster in Three Acts*, YouTube, 24 I 2023 r., https://www.youtube.com/watch?v=8YkGrKQXZxE [dostęp: 25 I 2023].

Standoff: A chronicle of Russian invasion of Crimea, Defense Express, 4 III 2014 r., https://web.archive.org/web/20230226183728/https://issuu.com/ukrainian_defense_review/docs/chronicles-of-russian-aggression-cr [dostęp: 13 VII 2025].

Sukhov O., *From Olympics to Crimea, Putin Loyalist Kozak Entrusted With Kremlin Mega-Projects*, The Moscow Times, 28 III 2014 r., https://www.themoscowtimes.com/2014/03/27/from-olympics-to-crimea-putin-loyalist-kozak-entrusted-with-kremlin-mega-projects-a33409 [dostęp: 1 IX 2024].

Walker S., *'It is past time to leave Ukraine': western diplomats flee Kyiv*, The Guardian, 13 II 2022 r., https://www.theguardian.com/world/2022/feb/13/it-is-past-time-to-leave-ukraine-western-diplomats-flee-kyiv [dostęp: 21 IX 2024].

Westfall S., *These countries are withdrawing embassy staffers from Ukraine amid growing fears of an invasion by Russia*, The Washington Post, 14 II 2022 r., https://www.washingtonpost.com/world/2022/01/25/ukraine-embassy-evacuations/ [dostęp: 21 IX 2024].

Wilk A., *Rosyjska interwencja wojskowa na Krymie*, Ośrodek Studiów Wschodnich, 5 III 2014 r., https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [dostęp: 29 IX 2024].

Rosyjskie źródła internetowe

Заседание Совета Безопасности (*Zasiedanije Sowieta Biezopasnosti*), YouTube, 22 II 2022 r., https://www.youtube.com/watch?v=_YRUlb_7T9o [dostęp: 28 IX 2024].

Кац М., *Арестован замминистра обороны Иванов* (Кас М., *Ariestowan zamministra oborony Iwanow*), YouTube, 24 IV 2024 r., https://www.youtube.com/watch?v=5p4S7AKBPOg [dostęp: 28 IX 2024].

Обращение Президента Российской Федерации, Президент России (*Obraszczenijeprieziedienta Rossijskoj Fiedieracyi*, Priezidient Rossii), 21 II 2022 r., http://kremlin.ru/events/president/news/67828 [dostęp: 27 IX 2024].

Inne dokumenty

Bowen A.S., *Russia's War in Ukraine: Military and Intelligence Aspects*, Congressional Research Service Report, Washington 2023.

Schwartz P., Fink A., Waller J., Kofman M., Lennox B., Chesnut M., *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023.

The Military Balance 2022. The annual assessment of global military capabilities and defence economics, [bmw] 2022.

Zabrodskyi M., Watling J., Danylyuk O.V., Reynolds N., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022 r.

Źródła archiwalne

AIPN, Ministerstwo Spraw Wewnętrznych w Warszawie [1944] 1954–1990, sygn. BU 0236/254.

AIPN, Zbiór dokumentów dotyczących Układu Warszawskiego, sygn. BU 02958/1, sygn. BU 02958/2.

Dr Marek Klasa

Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Adiunkt w Wydziale Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

Kontakt: m.klasa@akademia.mil.pl

Michał Klasa

Absolwent studiów podyplomowych na kierunku działania analityczno-informacyjne w obszarze bezpieczeństwa w Instytucie Historii Wojskowej Akademii Sztuki Wojennej.

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 85–96

https://doi.org/10.4467/20801335PBW.25.004.22170

ARTYKUŁ

Projekt Unii Europejskiej SAFE-CITIES. Skuteczniejsze monitorowanie zagrożeń w przestrzeniach publicznych

The European Union project SAFE-CITIES. More effective monitoring of threats in public spaces

MAŁGORZATA WOLBACH

Polska Platforma Bezpieczeństwa Wewnętrznego
https://orcid.org/0009-0005-1837-0389

JAROSŁAW PRZYJEMCZAK

Wydział Prawa i Administracji,
Wyższa Szkoła Administracji i Biznesu w Gdyni
https://orcid.org/0000-0003-3923-8078

Abstrakt

Współcześnie ludzka działalność na wielu polach jest wspierana przez nowoczesne technologie i narzędzia. Dużo takich rozwiązań jest wykorzystywanych w obszarach, które były do tej pory odporne na zmiany, gdyż ich charakter oraz obowiązujące przepisy nie pozwalały na modyfikacje. Zaliczają się do nich przestrzenie publiczne, które z racji swojej roli są ogólnodostępne i przez większość czasu otwarte. W artykule autorzy przedstawili założenia SAFE-CITIES – projektu mającego zapewnić jak najwyższy poziom ochrony przestrzeni publicznych w obliczu rosnącego zagrożenia

terrorystycznego – oraz opisali wybrane technologie w ramach tego projektu, wspierające procesy monitorowania zagrożeń. Omówili także projekty pokrewne podjęte przez Unię Europejską.

Słowa kluczowe Safe-Cities, Unia Europejska, przestrzeń publiczna, służby odpowiedzialne za bezpieczeństwo, nowe technologie, monitorowanie zagrożeń

Abstract Nowadays, human activity is supported by modern technologies and tools. Many of these solutions are used in areas that have so far been resistant to change, as their nature and the applicable regulations did not allow for modifications. Such areas include public spaces which, by virtue of their role, are publicly accessible and open most of the time. In the article, the authors presented the assumptions of the SAFE-CITIES – project aimed at ensuring the highest possible level of protection for public spaces in the face of the growing threat of terrorism – and described selected technologies and tools, created as part of the project, supporting the processes of monitoring threats. They also discussed related projects addressed by the European Union.

Keywords Safe-Cities, European Union, public space, services responsible for safety, new technologies, threat monitoring

Wprowadzenie

W związku z rozrastaniem się dużych miast i aglomeracji miejskich mnożą się trudności związane z ich funkcjonowaniem[1]. Do podstawowych zaliczają się m.in. problemy dotyczące komunikacji, środowiska, administracji, porządku oraz utrzymania właściwego stopnia bezpieczeństwa, szczególnie w otwartych, ogólnodostępnych obiektach czy obszarach. Dlatego istotną cechą istniejących lub dopiero projektowanych systemów bezpieczeństwa jest zdolność do wczesnego ujawnienia zagrożeń, co właściwym podmiotom umożliwia szybką reakcję na incydenty.

[1] Zob. szerzej np.: A. Kaya, M. Koc, *Over-Agglomeration and Its Effects on Sustainable Development: A Case Study on Istanbul*, „Sustainability" 2019, t. 11, nr 1. https://doi.org/10.3390/su11010135.

Z uwagi na liczbę i zróżnicowany charakter zdarzeń, do których może dojść we wskazanych przestrzeniach, nie sposób przygotować się na nie wszystkie. Zarządcy tych miejsc powinni skupić się na określonych scenariuszach.

Zmiany gospodarcze, społeczne i polityczne tworzą warunki sprzyjające szerzeniu się nienawiści, zachowań ekstremistycznych oraz teorii spiskowych, co stwarza ryzyko zwiększenia liczby planowanych i przeprowadzonych ataków terrorystycznych. Z uwagi na stałe zagrożenie terrorystyczne bezpieczeństwo przestrzeni publicznych stanowi jedno z najważniejszych wyzwań dla podmiotów odpowiedzialnych za bezpieczeństwo współczesnych europejskich miast. Jak wskazują dane, liczba zamachów terrorystycznych w Europie utrzymuje się na wysokim poziomie. Zgodnie z informacjami zawartymi w ostatnim raporcie na temat zagrożeń terrorystycznych w Unii Europejskiej opracowanym przez Europol, w 2023 r. w siedmiu państwach członkowskich (Francja, Włochy, Niemcy, Hiszpania, Belgia, Grecja, Luksemburg) odnotowano łącznie 120 ataków terrorystycznych, z czego 98 zostało przeprowadzonych, 9 zakończyło się niepowodzeniem, a 13 udaremniono[2].

Planujący ataki coraz częściej wykorzystują najnowsze osiągnięcia technologiczne nie tylko w celu uprawiania propagandy i werbowania członków, lecz także poszukiwania nowych metod ataku, np. z wykorzystaniem sztucznej inteligencji. Powszechna dostępność materiałów szkoleniowych, m.in. w internecie, sprawia, że takie osoby mogą łatwo zdobywać wiedzę na temat taktyk ataków, metod produkcji broni czy obsługi dronów. Ponadto środowiska wirtualne mogą stanowić przestrzeń do realistycznych symulacji treningowych dla terrorystów, co może ułatwiać im przygotowanie do ataków.

W obliczu tych wyzwań niezwykle istotne staje się wdrażanie oraz stałe doskonalenie nowoczesnych technologii wspierających proces monitorowania i analizy zagrożeń bezpieczeństwa przestrzeni publicznych. Takie rozwiązania pozwalają podmiotom publicznym i niepublicznym odpowiedzialnym za bezpieczeństwo nie tylko na skuteczniejsze zwalczanie zagrożeń, lecz także na przygotowanie się do potencjalnych zamachów. W odpowiedzi na te potrzeby jest podejmowanych wiele działań na różnych poziomach organizacyjnych. Ich celem jest wsparcie instytucji w zapewnieniu bezpieczeństwa obiektom i obszarom ogólnodostępnym.

[2] Europol, *European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, s. 5–11 [dostęp: 13 III 2025].

W dbaniu o bezpieczeństwo należy korzystać z różnych strategii i rozwiązań[3]. Jednym z ważniejszych europejskich projektów jest SAFE-CITIES[4]. Zrealizowanie go pozwoli na skuteczniejszy dozór przestrzeni publicznych. Artykuł ma na celu zaprezentowanie założeń tego projektu oraz przedstawienie wybranych technologii i narzędzi powstałych w ramach tej inicjatywy. Pytanie badawcze brzmiało: jakiego rodzaju inicjatywy na rzecz poprawy bezpieczeństwa w miejscach publicznych podejmuje UE? W ramach badań autorzy korzystali z metod badawczych w postaci analizy, syntezy i wnioskowania. Ze względów formalnych i proceduralnych nie mogli opisać szczegółowo niektórych założeń projektowych oraz wytworzonych technologii i narzędzi. Część z nich została przekazana do dalszych prac mających na celu usprawnienie ich działania i ewentualne wykorzystanie komercyjne. Ponadto jedna z opisanych inicjatyw jest w trakcie realizacji i rezultaty nie są jeszcze znane.

Projekt SAFE-CITIES

Projekt SAFE-CITIES[5] miał na celu zapewnienie jak najwyższego poziomu ochrony przestrzeni publicznych przede wszystkim w obszarach takich jak właściwe zarządzanie ryzykiem oraz wykorzystanie nowoczesnych technologii, które pozwalają na przejście od rozproszonego działania do bardziej kompleksowej i systematycznej oceny bezpieczeństwa i podatności na zagrożenia (ang. *security and vulnerability assessment*, SVA). W ramach projektu m.in. dogłębnie przeanalizowano ryzyko w przestrzeniach publicznych oraz opracowano strategie zapobiegania jego zwiększeniu i łagodzenia skutków potencjalnych zagrożeń terrorystycznych. Działania te mają być wspierane zaawansowaną interaktywną platformą składającą się z różnych, połączonych ze sobą narzędzi. Umożliwią one przeprowadzanie szczegółowych analiz ryzyka oraz pomogą w znalezieniu ewentualnych słabych punktów w badanych lokalizacjach.

Najważniejszymi założeniami projektu SAFE-CITIES, którego realizacja zakończyła się 30 czerwca 2025 r., była ścisła współpraca podmiotów publicznych, i prywatnych, a także zaangażowanie obywateli w proces kształtowania strategii

[3] J. Przyjemczak, *Wstęp*, w: *Zadanie specjalne – człowiek, technologia, instytucja*, cz. 4, J. Przyjemczak (red. nauk.), Gdynia 2024, s. 7.

[4] Projekt SAFE-CITIES Komisji Europejskiej dotyczący perspektywy Horyzont Europa: HORIZON-CL3-2021-FCT-01-07: Zwiększona gotowość na ataki w przestrzeniach publicznych, https://cordis.europa.eu/project/id/101073945 [dostęp: 22 VII 2025].

[5] Zob. *SAFE-CITIES*, https://safe-cities.eu/ [dostęp: 13 III 2025].

bezpieczeństwa przestrzeni miejskich, przy jednoczesnym zachowaniu ich otwartego charakteru. Miało to umożliwić skuteczniejsze prognozowanie zagrożeń, szybsze reagowanie na incydenty oraz lepszą koordynację działań służb odpowiedzialnych za bezpieczeństwo. Kolejną zaletą była możliwość testowania w trakcie trwania projektu innowacyjnych metod minimalizowania skutków ataków. Metody te miały dostosować systemy ochrony do dynamicznie zmieniających się zagrożeń.

Partnerzy projektu SAFE-CITIES

Projekt był realizowany przez konsorcjum składające się z 17 partnerów z ośmiu krajów UE: Włoch, Cypru, Holandii, Grecji, Polski, Belgii, Finlandii, Słowenii i jednego spoza UE, czyli Wielkiej Brytanii. Funkcję koordynatora pełniło prywatne przedsiębiorstwo inżynieryjne STAM[6] z Włoch, specjalizujące się w innowacyjnych rozwiązaniach technologicznych w zakresie bezpieczeństwa, w tym w opracowywaniu narzędzi wspomagających podejmowanie decyzji na podstawie oceny ryzyka i symulacji scenariuszy w sytuacjach kryzysowych dla infrastruktury krytycznej i celów miękkich[7]. Wśród pozostałych partnerów znalazły się:

- firmy technologiczne rozwijające narzędzia analityczne i symulacyjne: IANUS Technologies (Cypr)[8], D-Visor (Holandia)[9], Thridium (Wielka Brytania)[10];
- instytuty badawcze oraz uczelnie wyższe opracowujące metodologie oceny ryzyka i podatności na zagrożenia: Narodowe Centrum Badań Naukowych „Demokritos" (Grecja), Uniwersytet Boloński (Włochy), Międzynarodowy Instytut Socjologiczny w Gorycji (Włochy), Università Verde di Bologna APS w Bolonii (Włochy);
- podmioty reprezentujące użytkowników końcowych oraz interesariuszy kluczowych dla skutecznej implementacji rozwiązań, jak: ministerstwa spraw wewnętrznych Cypru, Finlandii, Słowenii, Komenda Wojewódzka Policji w Gdańsku (Polska), Czerwony Krzyż z Gorycji (Włochy), gmina Nova Gorica (Słowenia), gmina Gorycja (Włochy), Konfederacja

[6] *STAM – Mastering Excellence*, https://www.stamtech.com/ [dostęp: 13 III 2025].

[7] Do celów miękkich, które mogą zostać zaatakowane przez terrorystów, zalicza się obiekty zarówno materialne, jak i osobowe nieobjęte szczególną ochroną prawną, a przez to narażone na atak terrorystyczny ze względu na łatwość jego przeprowadzenia. Zob. szerzej: A. Hołub, *Obiekty ataków terrorystycznych*, „Przegląd Policyjny" 2018, nr 4, s. 18.

[8] *IANUS Technologies*, https://ianus-technologies.com/ [dostęp: 13 III 2025].

[9] *D-Visor*, https://www.d-visor.nl/ [dostęp: 13 III 2025].

[10] *Thridium*, https://thridium.com/t4s/ [dostęp: 13 III 2025].

Europejskich Służb Ochrony (Confederation of European Security Services, Belgia), Polska Platforma Bezpieczeństwa Wewnętrznego (Polska).

Dzięki współdziałaniu wymienionych podmiotów inicjatywa uwzględniała interesy dużego grona odbiorców. Pozwoliło ono ponadto na uzyskanie szerokiego wsparcia technologicznego, praktycznego i merytorycznego w zakresie podjętej problematyki.

Narzędzia SAFE-CITIES

W ramach SAFE-CITIES powstały innowacyjne rozwiązania oparte na wiedzy i narzędziach dostarczonych przez partnerów, dostosowane do aktualnych potrzeb i zmieniających się technologii[11].

SBS

Scenario Builder & Serious Gaming Simulator (SBS) to zaawansowane narzędzie służące do tworzenia i symulacji scenariuszy zagrożeń, a dokładnie do symulacji imprez masowych i innych wydarzeń odbywających się w zatłoczonych przestrzeniach. Pozwala ono na realistyczne odwzorowanie dynamicznych interakcji między ludźmi oraz sposobów reagowania na różne zagrożenia. Dzięki SBS można tworzyć i konfigurować scenariusze zagrożeń w realistycznym środowisku 3D. Symulator wykorzystuje m.in. obiekty wzorcowe (ang. *blueprint objects*) w połączeniu z osią czasu, co umożliwia modelowanie skomplikowanych sekwencji zdarzeń, dostosowywanie zachowań postaci oraz symulowanie reakcji systemów bezpieczeństwa. Użytkownicy na podstawie uzyskanych danych mogą generować i edytować trójwymiarowe przestrzenie przez importowanie modeli CAD, BIM oraz BFX i dokładnie odwzorowywać rzeczywiste miejsca. Narzędzie umożliwia konfigurację elementów zarówno statycznych, takich jak środki bezpieczeństwa czy elementy infrastruktury miejskiej, jak i dynamicznych, w tym zachowanie się poszczególnych osób oraz tłumu, służb porządkowych, a także strategicznych miejsc danej przestrzeni, np. punktów wejść i wyjść, ciągów komunikacyjnych czy węzłów technicznych. Pozwala też na wdrażanie gotowych scenariuszy w trybie wieloosobowym, jako np. realną symulację szkoleniową, tzw. poważną grę (ang. *serious game*), w której uczestnicy mogą się wcielać w różne role. Jest to idealne środowisko szkoleniowe dla wszystkich podmiotów zaangażowanych w zapewnianie porządku publicznego. System oferuje realistyczne symulacje zagrożeń, obejmujące różne, złożone scenariusze, w tym ataki bombowe, podpalenia, ataki nożownika, strzelaniny, ataki dronów z ładunkami wybuchowymi, dzięki czemu można kompleksowo przeanalizować ryzyko i procedury bezpieczeństwa. Jest pomocny również podczas sesji

[11] *SAFE-CITIES Architecture*, https://safe-cities.eu/tools/ [dostęp: 22 VII 2025].

w rzeczywistości wirtualnej (ang. *virtual reality*, VR) zapewnia jeszcze bardziej immersyjne doświadczenia, zwiększa skuteczność szkoleń i pozwala przećwiczyć procedury bezpieczeństwa w warunkach zbliżonych do rzeczywistych. Narzędzie SBS, jako istotny element szkoleniowy, umożliwia bardziej efektywne planowanie zabezpieczeń oraz szybsze i skuteczniejsze reagowanie w sytuacjach kryzysowych, a tym samym zwiększa poziom bezpieczeństwa w przestrzeniach publicznych.

SERVE

SEcuRity Vulnerability assEssment (SERVE) jest interaktywnym narzędziem do oceny ryzyka i podatności przestrzeni publicznych na różne zagrożenia oraz stopnia atrakcyjności dla atakujących celów w dowolnej przestrzeni publicznej. Funkcjonalność systemu pozwala na uproszczenie i usprawnienie analizy bezpieczeństwa i oferuje kompleksowe podejście do tego procesu. Dzięki SERVE użytkownicy mogą bezpośrednio na mapie lub planie obiektu zaznaczać obszary poddane analizie. Narzędzie oferuje również możliwość wyboru zagrożeń z predefiniowanej listy i tym samym personalizację oceny ryzyka w zależności od specyfiki wybranego obszaru. Umożliwia także analizę różnych rodzajów ryzyka, takich jak np. zamachy terrorystyczne, pożary czy zagrożenia chemiczne, a co za tym idzie – precyzyjne dostosowanie strategii bezpieczeństwa do konkretnych scenariuszy czy sytuacji. Analiza obejmuje trzy aspekty: ryzyko, wpływ zagrożenia oraz atrakcyjność danej przestrzeni publicznej dla atakujących. Proces ten jest wspierany przez interaktywny kreator, który prowadzi użytkownika przez zestaw pytań pomagających określić poziom zagrożenia. Każdy z tych trzech wskaźników ma oddzielny, zindywidualizowany zestaw pytań. Narzędzie wyposażono w wiele zaawansowanych opcji, takich jak możliwość importu i eksportu oraz integracji danych czy modyfikacji informacji, takich jak istniejące środki bezpieczeństwa, przeszkody, elementy infrastruktury miejskiej oraz systemów nadzoru. SERVE zapewnia szczegółową analizę podatności terenu w kontekście określonych zagrożeń oraz skuteczniejsze planowanie i wdrażanie środków prewencyjnych. Dzięki intuicyjnemu interfejsowi, zaawansowanym funkcjom analizy oraz szerokiemu zakresowi zastosowań system ten to niezastąpione narzędzie dla ekspertów ds. bezpieczeństwa.

SCoreboard

To inteligentne narzędzie analityczne stworzone do monitorowania i wizualizacji danych. Jego najważniejszą funkcją jest przetwarzanie i prezentowanie wyników z symulacji w czasie rzeczywistym w sposób przejrzysty i użyteczny dla użytkowników. Umożliwia kompleksową ocenę potencjalnych zagrożeń oraz analizę scenariuszy kryzysowych. System wizualizuje kluczowe wskaźniki w intuicyjnej formie, dzięki czemu jest możliwe szybkie interpretowanie wyników i wsparcie działań

operacyjnych. Jego prosty w obsłudze interfejs zapewnia szybki dostęp do wyników symulacji oraz łatwą analizię sytuacyjną w dynamicznie zmieniających się warunkach. Wdrożenie SCoreboard zwiększa skuteczność zarządzania sytuacjami kryzysowymi i poprawia koordynację działań służb. Narzędzie wspiera zarówno fazę planowania operacyjnego, jak i reagowania na zagrożenia, przez dostarczanie danych niezbędnych do podejmowania strategicznych decyzji.

Projekty pokrewne

Przy tworzeniu projektu SAFE-CITIES wzorowano się na europejskich inicjatywach finansowanych przez Komisję Europejską, koncentrujących się na bezpieczeństwie publicznym, zarządzaniu kryzysowym oraz nowych technologiach wspierających ochronę przestrzeni miejskich, aby budować bardziej odporne, inteligentne i bezpieczne środowisko miejskie w Europie.

ENLETS

European Network of Law Enforcement Technology Services (ENLETS) to europejska sieć służb porządku publicznego, której głównym celem jest monitorowanie technologii związanych z bezpieczeństwem, rozpowszechnianie najlepszych praktyk wśród europejskich organów ścigania oraz inicjowanie projektów badawczo-rozwojowych w obszarze zwalczania przestępczości[12]. Sieć działa od 2008 r. i zrzesza przedstawicieli z 27 państw członkowskich UE oraz Wielkiej Brytanii i Norwegii. Wspierają ją krajowe punkty kontaktowe (ang. *national contact points*, NCPs), które pełnią funkcję łączników między poszczególnymi państwami członkowskimi a grupami zarządzającymi ENLETS. Istotnym elementem działalności sieci są tematyczne grupy robocze zajmujące się technologią (ang. *technology interest groups*, TIG), skupiające ekspertów i praktyków w wybranych obszarach technologicznych z różnych europejskich służb. Jedna z grup koncentruje się na zagadnieniach związanych z porządkiem publicznym. ENLETS odgrywa ważną rolę w promowaniu współpracy oraz wymiany wiedzy i doświadczeń między europejskimi służbami porządku publicznego. Współpraca między ENLETS a SAFE-CITIES przyczynia się do lepszego dopasowania technologii do rzeczywistych potrzeb służb odpowiedzialnych za bezpieczeństwo publiczne.

[12] *ENLETS*, https://enlets.eu/ [dostęp: 14 III 2025].

PRECRISIS

Projekt miał na celu rozwój innowacyjnych inteligentnych rozwiązań w zakresie bezpieczeństwa publicznego, wspierających organy ścigania, służby ratownicze, managerów bezpieczeństwa oraz innych interesariuszy[13]. Jego głównymi założeniami były wzmocnienie współpracy publiczno-prywatnej oraz integracja nowoczesnych technologii z najlepszymi praktykami w zakresie zarządzania bezpieczeństwem. W ramach PRECRISIS opracowywano, testowano i wdrażano narzędzia, które pozwalają na skuteczniejsze zabezpieczanie przestrzeni publicznych. Projekt bazował na wiedzy eksperckiej, dobrych praktykach oraz podejściu *privacy-by-design*, zapewniającym zgodność z wymogami ochrony danych i prywatności. Projekty SAFE-CITIES i PRECRISIS łączył wspólny cel, czyli zwiększenie bezpieczeństwa w przestrzeniach publicznych przez zastosowanie innowacyjnych technologii, analizę zagrożeń oraz współpracę między wieloma interesariuszami. Projekt zakończył się 30 kwietnia 2025 r.

SHRINES

Projekt koncentrował się na zwiększeniu bezpieczeństwa i ochrony miejsc kultu religijnego[14]. Jego główne cele to podnoszenie świadomości na temat zagrożeń występujących w miejscach kultu oraz opracowanie innowacyjnych rozwiązań technologicznych i środków prewencyjnych służących ochronie tych miejsc. SHRINES stanowił sieć łączącą różne społeczności religijne, organy ścigania oraz lokalne władze, które razem oceniały czynniki ryzyka, wymieniały się doświadczeniami i identyfikowały możliwości kooperacji w obszarze ochrony obiektów sakralnych. SAFE-CITIES i SHRINES bazowały na współpracy między instytucjami publicznymi, organizacjami społecznymi i sektorem technologicznym, a także promowały innowacyjne podejście do zarządzania ryzykiem i ochrony infrastruktury krytycznej. Projekt zakończył się 31 stycznia 2025 r.

APPRAISE

Inicjatywa miała na celu szybkie rozpoznanie i wdrożenie odpowiednich środków, które uniemożliwiałyby dokonanie ataku lub jego rozprzestrzenienie się bądź pozwoliłyby powstrzymać go. Głównym założeniem było zapewnienie bezpieczeństwa przestrzeni publicznej, bez ograniczania przy tym wolności obywateli, przez zminimalizowanie lub całkowite wyeliminowanie zagrożenia atakami. Powstałe rozwiązania miały zapewnić nowe możliwości przewidywania i identyfikowania aktów przestępczych i terrorystycznych oraz wzmacniać współpracę operacyjną

[13] *PRECRISIS*, https://precrisis-project.eu/ [dostęp: 14 III 2025].

[14] *SHRINES*, https://shrines-project.eu/ [dostęp: 14 III 2025].

przed atakiem, w jego trakcie i po nim służb odpowiedzialnych za bezpieczeństwo. W czasie realizacji projektu dostosowano już istniejące technologie lub stworzono nowe, a także przetestowano wyniki prac w niemal rzeczywistych warunkach. W ramach testów zorganizowano wiele wizyt studyjnych oraz pilotaży, podczas których sprawdzano prawidłowość działania poszczególnych systemów i technologii oraz na bieżąco je udoskonalano. Testy odbyły się w Lubljanie, Bilbao, Gdańsku i Turynie.

Finał tej inicjatywy, który przypadł na początek 2024 r.[15], nie oznaczał zakończenia prac nad powstałymi rozwiązaniami. To dopiero początek budowania zwartego i jednolitego systemu ostrzegawczo-analitycznego, który ma za zadanie dozorować przestrzenie publiczne i alarmować właściwe służby interwencyjne w momencie pojawienia się zagrożenia, a także wykrycia anomalii w zachowaniu się ludzi, tak aby osiągnąć jak najwyższy stopień świadomości sytuacyjnej. Wysiłki osób zaangażowanych w projekt APPRAISE są kontynuowane w ramach innych inicjatyw podejmowanych na rzecz poprawy bezpieczeństwa[16]. SAFE-CITIES przez koncentrowanie się na analizie podatności miast na zagrożenia oraz wdrażaniu narzędzi symulacyjnych uzupełnił działania APPRAISE i dostarczył dodatkowych danych i modeli wykorzystywanych do poprawy skuteczności systemów zarządzania kryzysowego.

Podsumowanie

Współczesne miasta i aglomeracje miejskie mierzą się z coraz większą liczbą wyzwań związanych z zapewnieniem bezpieczeństwa przestrzeni publicznych, zwłaszcza w obliczu narastającego zagrożenia atakami terrorystycznymi. Projekt SAFE-CITIES miał zwiększyć odporność na pojawiające się zagrożenia oraz poprawić bezpieczeństwo przestrzeni publicznych, m.in. przez wykorzystanie nowoczesnych technologii, lepszą koordynację podejmowanych działań oraz efektywniejsze zarządzanie ryzykiem. Systemy wdrożone w ramach tego projektu umożliwiają identyfikację słabych punktów infrastruktury oraz opracowanie, na podstawie uzyskanych danych, skuteczniejszych strategii ochronnych. Dzięki zaawansowanej analizie danych można lepiej prognozować zagrożenia i podejmować trafniejsze decyzje. Interaktywne szkolenia i symulacje zwiększają gotowość służb na realne incydenty, a także usprawniają ich komunikację i koordynację, co przyspiesza reakcję na sytuacje kryzysowe.

[15] *APPRAISE*, https://appraise-h2020.eu/ [dostęp: 14 III 2025].

[16] Zob. szerzej: J. Przyjemczak, N. Czyżewska, *Projekt APPRAISE. Budowanie systemu bezpieczeństwa przestrzeni publicznych*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 195–205. https://doi.org/10.4467/27204383TER.24.007.19395.

Dnia 27 marca 2025 r. w Novej Goricy (Słowenia) zademonstrowano rozwiązania opracowane w ramach projektu. Dla wielu najważniejszych interesariuszy ds. bezpieczeństwa była to unikalna okazja do bezpośredniego zapoznania się z technologiami wspierającymi zapewnienie bezpieczeństwa w miastach. Uczestnicy mogli wziąć udział w specjalnej sesji szkoleniowej opartej na zdefiniowanych scenariuszach, której celem było wypróbowanie opracowanych narzędzi i metodologii. Tego typu projekty przyczyniają się do budowania odporności na zagrożenia i stanowią doskonały materiał do dalszych prac w obszarze szeroko rozumianego bezpieczeństwa.

Bibliografia

Hołub A., *Obiekty ataków terrorystycznych*, „Przegląd Policyjny" 2018, nr 4, s. 18–26.

Kaya A., Koc M., *Over-Agglomeration and Its Effects on Sustainable Development: A Case Study on Istanbul*, „Sustainability" 2019, t. 11, nr 1. https://doi.org/10.3390/su11010135.

Przyjemczak J., *Zadanie specjalne – człowiek, technologia, instytucja*, cz. 4, J. Przyjemczak (red. nauk.), Gdynia 2024.

Przyjemczak J., Czyżewska N., *Projekt APPRAISE. Budowanie systemu bezpieczeństwa przestrzeni publicznych*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 195–205. https://doi.org/10.4467/27204383TER.24.007.19395.

Źródła internetowe

APPRAISE, https://appraise-h2020.eu/ [dostęp: 14 III 2025].

D-Visor, https://www.d-visor.nl/ [dostęp: 13 III 2025].

ENLETS, https://enlets.eu/ [dostęp: 14 III 2025].

Europol, *European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [dostęp: 13 III 2025].

IANUS Technologies, https://ianus-technologies.com/ [dostęp: 13 III 2025].

PRECRISIS, https://precrisis-project.eu/ [dostęp: 14 III 2025].

Projekt SAFE-CITIES Komisji Europejskiej dotyczący perspektywy Horyzont Europa: HORIZON-CL3-2021-FCT-01-07: Zwiększona gotowość na ataki w przestrzeniach publicznych, https://cordis.europa.eu/project/id/101073945 [dostęp: 22 VII 2025].

SAFE-CITIES, https://safe-cities.eu/ [dostęp: 13 III 2025].

SHRINES, https://shrines-project.eu/ [dostęp: 14 III 2025].

STAM – Mastering Excellence, https://www.stamtech.com/ [dostęp: 13 III 2025].

Thridium, https://thridium.com/t4s/ [dostęp: 13 III 2025].

Małgorzata Wolbach

Starsza specjalistka ds. realizacji projektów w Polskiej Platformie Bezpieczeństwa Wewnętrznego (PPBW). Absolwentka studiów magisterskich na kierunku bezpieczeństwo wewnętrzne oraz licencjackich na kierunku kryminologia w Wyższej Szkole Policji w Szczytnie. W PPBW odpowiada za wdrażanie i realizację projektów finansowanych z programów Unii Europejskiej, ze szczególnym uwzględnieniem projektów dotyczących zagrożeń hybrydowych oraz bezpieczeństwa przestrzeni publicznych.

Kontakt: malgorzata.wolbach@ppbw.pl

Dr Jarosław Przyjemczak

Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie, pracownik naukowo-dydaktyczny w Instytucie Bezpieczeństwa i Socjologii Uniwersytetu Pomorskiego w Słupsku. Podinspektor Policji w stanie spoczynku. Uczestnik wielu krajowych i zagranicznych kursów oraz szkoleń policyjnych i pozapolicyjnych związanych z walką z terroryzmem. Ukończył m.in. strategiczny kurs kontrterrorystyczny i zagrożeń terrorystycznych w Bramshill w Wielkiej Brytanii, organizowany przez Kolegium Policyjne CEPOL w ramach Europolu. Członek Polskiego Towarzystwa Bezpieczeństwa Narodowego. Autor licznych prac na temat bezpieczeństwa, policyjnych jednostek specjalnych, ratownictwa medycznego. Redaktor naukowy cyklicznej publikacji *Zadanie specjalne – człowiek, technologia, instytucja.* Pomysłodawca i organizator wydarzenia edukacyjno-szkoleniowego „Paramedyk". Ratownik medyczny, wodny, instruktor nurkowy, strzelectwa i ratownictwa pola walki.

Kontakt: jarek.przyjemczak@wp.pl

Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 97–117

 https://doi.org/10.4467/20801335PBW.25.005.22171

ARTYKUŁ

Cyberbezpieczeństwo w sektorze energetyki morskiej i okołomorskiej Rzeczypospolitej Polskiej

Cybersecurity in the offshore and coastal energy sector of the Republic of Poland

DAVID CYBULSKI

Autor niezależny

https://orcid.org/0009-0003-9195-4407

Abstrakt Celem artykułu jest omówienie poziomu cyberbezpieczeństwa polskiej energetyki morskiej i okołomorskiej w kontekście planowanych strategicznych projektów energetycznych. Autor przedstawił wybrane cyberataki na elementy sektora energetycznego innych państw, a także omówił, m.in. na podstawie *Polityki energetycznej Polski do 2040 r.*, planowane przez Polskę działania związane z infrastrukturą energetyczną w rejonie Morza Bałtyckiego. Wskazał zagrożenia dla polskiego sektora energetyki morskiej i okołomorskiej, do których należy działalność grup APT i grup sponsorowanych przez państwo, rywali biznesowych, haktywistów. Przedstawił stosowane sposoby ochrony tej infrastruktury oraz propozycje zabezpieczenia planowanych inwestycji przed atakami teleinformatycznymi.

Słowa kluczowe cyberbezpieczeństwo, cyberataki, grupy APT, energetyka, sektor energetyczny

Abstract

The purpose of the article is to discuss the level of cybersecurity of Poland's offshore and coastal energy sector in the context of planned strategic energy projects. The author presented selected cyberattacks on elements of other states' energy sector, he also discussed, among other things, on the basis of *Energy Policy of Poland until 2040*, Poland's planned activities related to energy infrastructure in the Baltic Sea region. He identified threats to Poland's offshore and coastal energy sector, which include: the activities of APT groups and state-sponsored groups, business rivals and hacktivists. He presented the methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks.

Keywords

cybersecurity, cyberattacks, APT groups, energetics, energy sector

Wprowadzenie

W związku ze stale rosnącą digitalizacją w społeczeństwie niezbędny jest ciągły rozwój posiadanych mocy wytwarzania energii elektrycznej. Decydenci, świadomi konieczności modernizacji istniejącej infrastruktury energetycznej państwa, dostosowania się do regulacji unijnych[1] oraz spodziewanego wzrostu zapotrzebowania państwa na energię elektryczną, podjęli działania mające określić długofalowe cele strategiczne i projekty dla sektora energetycznego. Stworzono plan rozwoju energetyki państwa polskiego w postaci *Polityki energetycznej Polski do 2040 r.* (dalej: PEP2040).

Działania ofensywne na Morzu Bałtyckim, wymierzone np. w gazociągi Nord Stream 1 i Nord Stream 2[2], kabel telekomunikacyjny C-Lion 1 czy połączenie elektroenergetyczne EstLink 2, ukazują, jak w obecnych czasach jest zagrożone bezpieczeństwo infrastruktury energetycznej[3]. Dążenie do rozwoju narodowych projektów energetycznych na północy Polski oraz w jej wyłącznej strefie ekonomicznej zwiększa stopień informatyzacji zasobów sektora energetycznego. Potęguje

[1] *Polityka energetyczna Polski do 2040 r.*, Ministerstwo Klimatu i Środowiska, Warszawa 2021, s. 3–4.

[2] W. Lorenz, S. Zaręba, *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2*, Polski Instytut Spraw Międzynarodowych, 29 IX 2022 r., https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [dostęp: 16 VII 2025].

[3] K. Buchholz, *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025 r., https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [dostęp: 16 VII 2025].

możliwości oddziaływania przeciwnika na infrastrukturę teleinformatyczną polskiej energetyki. W związku z tym konieczna jest weryfikacja stanu cyberbezpieczeństwa w rozwijającym się polskim sektorze energetyki morskiej i okołomorskiej, jak również odpowiedź na pytanie, w jakim stopniu jest on odporny na zagrożenia.

Jednym ze sposobów prowadzenia polityki wywierania wpływu przez przestępców, w tym terrorystów, oraz podmioty prawa międzynarodowego (państwa) stało się ich oddziaływanie w sposób pośredni lub bezpośredni na sektor energetyczny drugiej strony, będący tzw. celem o wysokiej wartości (ang. *high-value target*). Atak, w tym teleinformatyczny, który doprowadzi do zaprzestania produkcji i dystrybucji określonego zapotrzebowania energetycznego, może spowodować czasową lub trwałą niezdolność do funkcjonowania państwa. W celu mitygacji ryzyka polski ustawodawca zdecydował się, na podstawie art. 3 pkt. 2 lit. a *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, na zaliczenie systemów zaopatrzenia w energię, surowce energetyczne i paliwa do infrastruktury krytycznej (IK). Ustawa o zarządzaniu kryzysowym nakłada na operatorów IK określone obowiązki mające zapewnić jej właściwe zabezpieczenie. Ponadto na podstawie *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[4] operatorzy IK zostali zobligowani do zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w ramach swoich podmiotów, tak aby zminimalizować ryzyko wystąpienia incydentu bezpieczeństwa teleinformatycznego.

Celem artykułu jest omówienie poziomu bezpieczeństwa teleinformatycznego sektora energetyki morskiej i okołomorskiej RP w kontekście planowanych strategicznych projektów energetycznych. Przedstawiono w nim wybrane cyberataki na elementy sektora energetycznego innych państw, a także omówiono, m.in. na podstawie PEP2040, planowane przez Polskę działania związane z infrastrukturą energetyczną w rejonie Morza Bałtyckiego. Wskazano zagrożenia dla polskiego sektora energetyki morskiej i okołomorskiej, do których należy działalność grup APT[5] i grup sponsorowanych przez państwo, rywali biznesowych, haktywistów. Przedstawiono również stosowane sposoby ochrony tej infrastruktury oraz propozycje zabezpieczenia planowanych inwestycji przed atakami teleinformatycznymi.

---

[4] Procedowana jest nowelizacja tej ustawy. Zob. *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, nr UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [dostęp: 16 VII 2025].

[5] Grupa APT (ang. *advanced persistent threat*) – rodzaj zaawansowanej grupy cyberprzestępczej, składającej się z wykwalifikowanych specjalistów od cyberbezpieczeństwa oraz teleinformatyki, którzy są w stanie zrealizować zaawansowane ataki teleinformatyczne na określone podmioty.

Przykłady cyberataków wymierzonych w sektor energetyczny

Infrastruktura energetyczna państw przez dwie pierwsze dekady XXI w. padła ofiarą wielu skutecznych ataków ukierunkowanych m.in. na systemy i sieci teleinformatyczne. Pierwszym z powszechnie znanych działań cyberofensywnych tego typu był atak na infrastrukturę teleinformatyczną ośrodka wzbogacania uranu w miejscowości Natanz w Iranie, dokonany w 2010 r. za pomocą oprogramowania Stuxnet. Zadaniami tej placówki są produkcja energii elektrycznej oraz realizacja strategicznych interesów Iranu dotyczących pozyskania zdolności odstraszania atomowego. Operację pod kryptonimem „Olimpic Games" przeprowadziły we współpracy m.in. Stany Zjednoczone Ameryki oraz Państwo Izrael[6]. Zdecydowano się na cyberatak, gdyż dokonanie ataku i sabotażu drogą kinetyczną nie było możliwe. Opracowano potencjalnie słabe punkty infrastruktury teleinformatycznej placówki, które skutecznie zaatakowane uniemożliwiłyby lub znacznie utrudniły kontynuowanie procesu wzbogacania uranu w Natanz. Za najbardziej destrukcyjną metodę zaszkodzenia irańskiej strategii atomowej uznano zniszczenie wirówek do wzbogacania uranu[7]. W związku z tym, że ośrodek nie miał bezpośredniego dostępu do sieci Internet, atakujący postanowili zainfekować wewnętrzne systemy teleinformatyczne placówki przez podłączenie przenośnej pamięci USB ze złośliwym oprogramowaniem. Zainfekowane wirówki (a dokładnie kontrolujące je programowalne sterowniki logiczne) zaczęły pracować zgodnie z harmonogramem ustalonym przez atakujących. Doszło do uszkodzenia ok. 11–17% wirówek w ośrodku w Natanz[8], co spowodowało spadek produkcji paliwa jądrowego o 15%[9]. Ponadto podejrzewa się, że zostało zainfekowanych ok. 100 000 innych urządzeń, gdy Stuxnet nieplanowanie rozprzestrzenił się na świecie za pomocą sieci Internet[10]. Jest to najprawdopodobniej najbardziej znany przypadek ataku na system teleinformatyczny przeprowadzony przeciwko innemu państwu oraz jego infrastrukturze energetycznej.

---

[6] M. Baezner, P. Robin, *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf, s. 7–8 [dostęp: 16 VII 2025].

[7] Tamże, s. 4.

[8] Tamże, s. 9.

[9] T.M. Chen, *Stuxnet, the Real Start of Cyber Warfare?*, „IEEE Network" 2010, t. 24, nr 6, s. 3. https://doi.org/10.1109/MNET.2010.5634434.

[10] N. Falliere, L.O. Murchu, E. Chien, *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf, s. 5 [dostęp: 16 VII 2025].

Innym przykładem oddziaływania w cyberprzestrzeni na elementy sektora energetycznego państwa był atak w 2012 r. na spółkę Królestwa Arabii Saudyjskiej – Saudi Aramco Oil Company (dalej: Saudi Aramco), największą na świecie firmę z sektora surowcowego. Zgodnie z wyliczeniami Europejskiego Banku Centralnego z 2011 r. – do 2009 r. na Arabię Saudyjską przypadało ok. 12% światowej produkcji ropy naftowej (z czego za większość wydobycia odpowiadała Saudi Aramco)[11]. Atak na Saudi Aramco został przeprowadzony najprawdopodobniej przez grupę cyberprzestępców APT33, powiązaną z Islamską Republiką Iranu. Systemy teleinformatyczne spółki sparaliżowano za pomocą wirusa Shamoon. Zainfekowano ponad 30 000 stacji roboczych[12]. Program ten rozprzestrzeniał się na inne stacje robocze (jest to działanie typowe dla złośliwego oprogramowania klasyfikowanego jako robak, ang. *worm*) i nadpisywał pliki w systemie operacyjnym urządzenia, co wyłączało zainfekowany komputer z użytku[13].

Ofiarą kolejnego poważnego ataku wymierzonego w infrastrukturę energetyczną państwa padła Ukraina. Został on przeprowadzony 23 grudnia 2015 r. wobec trzech regionalnych dystrybutorów energii elektrycznej, tj. Prykarpattyaoblenergo, Kyivoblenergo oraz Chernivtsioblenergo. Byli oni odpowiedzialni za przesył energii elektrycznej odpowiednio na terenach obwodów iwanofrankiwskiego, kijowskiego oraz czerniowieckiego. Według informacji amerykańskiej Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (Cybersecurity and Infrastructure Security Agency) ok. 225 000 osób pozostało bez dostaw prądu na ok. sześć godzin[14]. Ponadto zostały zaatakowane instytucje z sektorów: rządowego, mediów, transportu kolejowego oraz górnictwa[15]. Atak rozpoczął się (po fazie rozpoznania otwartoźródłowego infrastruktury przedsiębiorstw i wstępnych przygotowań do przeprowadzenia operacji) przez dystrybucję kampanii phishingowej do pracowników wymienionych instytucji. Pracownicy przez otwarcie załącznika do wiadomości

---

[11] A. Nakov, G. Nuño, *Saudi Aramco and the Oil Market*, „Working Paper Series" 2011, nr 1354, s. 9.

[12] G. Siboni, S. Kronenfeld, *Iran and Cyberspace Warfare*, „Military and Strategic Affairs" 2012, t. 4, nr 3, s. 90.

[13] Warto dodać, że od listopada 2022 r. spółka z grupy kapitałowej Saudi Aramco (Aramco Overseas Company B.V.) jest właścicielem 30% udziałów w Rafinerii Gdańskiej. Zob. *Saudi Aramco przejmie udziały w gdańskiej rafinerii*, CIRE, 12 I 2022 r., https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [dostęp: 14 XII 2024].

[14] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20 VII 2021 r., https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 28 XI 2024].

[15] J. Styczynski, N. Beach-Westmoreland, *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [bmw] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, s. 5–7, 30–39 [dostęp: 16 VII 2025].

e-mail nieświadomie zainfekowali sieci swoich instytucji złośliwym oprogramowaniem typu trojan[16] o nazwie BlackEnergy 3[17]. Połączyło się ono z serwerami C2[18], po czym cyberprzestępcy zaimplementowali na zainfekowanych stacjach roboczych narzędzia do ekstrakcji danych uwierzytelniających oraz przeprowadzili rozeznanie sieci wewnętrznych zaatakowanych firm. Uzyskali możliwość zalogowania się do tych systemów i sieci oraz dokonania przeglądu widniejącej tam infrastruktury teleinformatycznej. Następnie załadowali kolejne złośliwe oprogramowanie, o nazwie KillDisk, które miało się uruchomić po restarcie systemu operacyjnego. Atakujący wyłączyli zasilacze awaryjne (ang. *uninterrupted power supply*, UPS) dla wybranych serwerów, w tym odpowiedzialnych za usługi telekomunikacyjne, a potem uruchomili wyłączniki prądu. Odłączyli w ten sposób od sieci co najmniej 27 podstacji elektrycznych oraz przerwali dostawy energii elektrycznej dla wspomnianych ok. 225 000 osób[19]. Wgrali następnie własną poprawkę systemu zarządzania przełącznikami, aby powstrzymać ich dalsze zdalne sterowanie, po czym przeprowadzili atak typu DoS[20] na infolinię kijowskiego dystrybutora energii. Uniemożliwiło to klientom zgłoszenie braku dostaw prądu. Ostatnim etapem działań było zaplanowane wcześniej wyłączenie się urządzeń typu UPS, co spowodowało uaktywnienie złośliwego oprogramowania KillDisk przy ponownym uruchomieniu systemów. Miało ono zniszczyć wszelkie dane i logi znajdujące się na urządzeniach, aby znacznie utrudnić późniejszą analizę, która mogłaby ustalić przyczyny zdarzenia i środki zaradcze.

Zakłada się, że za cyberatakiem na ukraińskich dystrybutorów energii stała co najmniej jedna grupa cyberprzestępcza sponsorowana przez państwo (ang. *state-sponsored group*), tj. APT44 powiązana z rosyjskim aparatem państwowym[21]. Przypisuje się jej zależność od Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (Главное управление Генерального штаба

[16] Trojan – typ wirusa komputerowego imitujący rzeczywiste programy i funkcje.

[17] Jest to trojan typu RAT (ang. *remote access trojan*) umożliwiający atakującemu zdalny dostęp do stacji roboczej ofiary.

[18] Serwer C2 (ang. *command & control*) – infrastruktura służąca atakującemu do kontroli i zarządzania systemami i urządzeniami mu podległymi, w tym zaatakowanej infrastruktury.

[19] SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf, s. 11 [dostęp: 6 VIII 2025].

[20] DoS (ang. *denial of service*) – rodzaj ataku mający na celu przerwanie dostępności wybranej usługi.

[21] J. Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016 r., https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [dostęp: 15 XII 2024].

Вооруженных Сил Российской Федерации, GRU)[22]. Grupy tego rodzaju nierzadko stanowią narzędzie polityczne będące do dyspozycji państwa rosyjskiego.

Do następnego ataku w sferze teleinformatycznej na różne sektory ukraińskiego państwa, w tym energetyczny, doszło w 2017 r. Podobnie jak w przypadku ataków z 2015 r. działania te przypisano grupie APT44[23]. Nazwa ataku pochodzi od wykorzystanego w nim złośliwego oprogramowania NotPetya, które charakteryzowało się łatwością w tzw. ruchu lateralnym, szyfrowaniu dysków oraz dużą destruktywnością. Początkowo NotPetya zidentyfikowano jako typ ransomware'u[24], nie przewidywał on jednak kluczy deszyfrujących, mogących sprawić, że zainfekowane urządzenie stałoby się ponownie zdatne do użycia, a pliki na nim zawarte byłyby w nienaruszonym stanie. Takie programy określa się mianem *wiper*. Celem ataku było państwo ukraińskie i szeroko pojęta infrastruktura teleinformatyczna zlokalizowana na jego terytorium. Jednak ze względu na obecność w Ukrainie wielu oddziałów spółek zagranicznej proweniencji oraz specyfikę użytego oprogramowania (jak najszybsza propagacja przez sieć) zasięg ataku szybko przekroczył granice cyfrowe Ukrainy i wirus rozprzestrzenił się po świecie w tempie dotąd niezaobserwowanym[25]. Rząd federalny Stanów Zjednoczonych Ameryki w związku z cyberatakiem pociągnął do odpowiedzialności karnej sześciu obywateli Federacji Rosyjskiej – oficerów GRU[26].

Jak wspomniano, atak miał na celu infekcję jak największej liczby urządzeń teleinformatycznych na terytorium Ukrainy, więc nie został wymierzony bezpośrednio w sektor energetyczny, ten jednak nie uchronił się przed wirusem. Ofiarą ataków padły Kyivenergo oraz Ukrenergo – firmy odpowiedzialne za dystrybucję energii elektrycznej w Ukrainie na szczeblach: lokalnym i krajowym[27]. To zdarzenie pokazuje, że podmioty sektora energetycznego muszą chronić się nie tylko przed zagrożeniami ukierunkowanymi, lecz także przed zagrożeniami ogólnymi, na jakie są narażone inne sektory. Znacznie zwiększa to zakres monitoringu zagrożeń.

---

[22] G. Roncone i in., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024 r., https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, s. 2, 7 [dostęp: 16 VII 2025].

[23] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf, s. 3–4 [dostęp: 16 VII 2025].

[24] Ransomware – typ złośliwego oprogramowania, które blokuje dostęp do danych na komputerze lub w sieci i żąda okupu za ich przywrócenie.

[25] Łatwe infekowanie kolejnych stacji roboczych czy serwerów przez oprogramowanie NotPetya okazało się możliwe przez połączenie dwóch narzędzi, tj. Mimikatz oraz EternalBlue.

[26] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents*…, s. 3–4.

[27] C. Krasznay, *Case Study: The NotPetya Campaign*, w: *Információ- és kiberbiztonság*, B. Török (red.), Budapest 2020, s. 486.

Agencja prasowa Reuters informowała w 2023 r., że po inwazji na Ukrainę Federacja Rosyjska za priorytetowy cel ataków teleinformatycznych obrała sektor energetyczny tego państwa[28]. Zgodnie z doniesieniami tej agencji Służba Bezpieczeństwa Ukrainy (ukr. Служба безпеки України, SBU) ustaliła, że Rosja przeprowadza średnio 10 ataków dziennie, m.in. podejmuje próby wyłączenia części infrastruktury energetycznej Ukrainy. To pokazało, że cyberprzestrzeń działa jak system naczyń połączonych. Przykładem jest atak na ukraińskiego satelitę, który spowodował niedostępność systemu zdalnego nadzorowania pracy ponad 5800 turbin wiatrowych w Niemczech[29].

Od rozpoczęcia rosyjskiej inwazji na Ukrainę są prowadzone działania ofensywne w cyberprzestrzeni wymierzone w infrastrukturę energetyczną innych państw europejskich. Jednym z nich była seria ataków w 2023 r. na duńskich operatorów IK. Opisał je w raporcie SektorCERT – zespół reagowania na incydenty bezpieczeństwa komputerowego odpowiedzialny za ochronę duńskiej IK[30]. Wynika z niego, że był to największy, a zarazem najbardziej kosztowny w historii atak przeprowadzony na tę infrastrukturę. Sprawcy zaatakowali część systemów zarządzania środowiskami automatyki przemysłowej (ang. *industrial control systems*, ICS) w przedsiębiorstwach i uzyskali dostęp do infrastruktury teleinformatycznej 22 podmiotów z sektora energetycznego. Ataków na wszystkie cele dokonano jednocześnie, były one przygotowane starannie i z dużym wyprzedzeniem, a atakujący miał rozeznanie, gdzie należy uderzyć[31]. SektorCERT miał problemem z jednoczesną obsługą 16 zaatakowanych instytucji oraz kolejnych sześciu, które padły ofiarą drugiej fali ataków. Te kolejne ataki SektorCERT przypisał innej, bliżej niezidentyfikowanej grupie cyberprzestępczej, wykorzystującej nowe narzędzia do ataku, w tym liczne podatności typu 0-day[32]. To wskazuje, że sprawca dysponował dużymi umiejętnościami w odkrywaniu tych podatności lub środkami pieniężnymi na zakup od innych grup cyberprzestępczych informacji o lukach bezpieczeństwa[33].

---

[28] N. Buli, N. Chestney, Ch. Steitz, *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023 r., https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [dostęp: 5 XII 2024].

[29] Tamże.

[30] SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 5 XII 2024].

[31] Tamże, s. 10.

[32] Podatność typu 0-day – podatność, która nie została publicznie potwierdzona przez producenta i nie istnieje dla niej oficjalna aktualizacja oprogramowania, która neutralizowałaby tę podatność.

[33] *Behind the Rise of the Million Dollar Zero-Day Market*, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [dostęp: 14 XII 2024].

Przypuszcza się, że za atakami (a przynajmniej częścią z nich) stała grupa APT44[34]. Co warte uwagi, SektorCERT ustalił, że w momencie największego nasilenia ataków źródłami były adresy IP wskazujące swoją geolokalizacją na Polskę i Ukrainę[35].

Identyfikacja zasobów sektora energetyki w obszarze morskim RP

W PEP2040 duży nacisk położono na podsektor energetyki morskiej i okołomorskiej państwa. Świadczą o tym działania wymienione w tym dokumencie:

- utworzenie morskich farm wiatrowych w polskiej wyłącznej strefie ekonomicznej, które do 2040 r. mają osiągnąć zdolność generowania energii elektrycznej o mocy ok. 11 GW,
- stworzenie głównego terminalu instalacyjnego (portu) specjalizującego się w obsłudze łańcucha dostaw dla morskich farm wiatrowych,
- rozbudowa sieci przesyłowej w północnej i północno-zachodniej części Polski w celu przystosowania systemu elektroenergetycznego Polski do odbioru i przesyłu energii wytworzonej m.in. w morskich elektrowniach wiatrowych,
- pozyskiwanie gazu ziemnego gazociągiem Baltic Pipe od 2022 r. Możliwy import 10 mld m^3 gazu ziemnego i eksport – 3 mld m^3,
- zwiększenie zdolności regazyfikacji terminalu LNG w Świnoujściu do 8,3 mld m^3 gazu ziemnego,
- budowa terminalu regazyfikacyjnego gazu ziemnego w Zatoce Gdańskiej (terminal FSRU[36]) o przepustowości nominalnej 4,5 mld m^3 gazu,
- rozbudowa gazociągów w północnej i centralnej części Polski w celu umożliwienia transportu gazu z terminalu FSRU w głąb kraju,
- możliwa rozbudowa Podziemnego Magazynu Gazu Kosakowo w Dębogórzu,
- zwiększenie zdolności przechowywania ropy naftowej w terminalu naftowym oraz bazy PERN w Gdańsku do ok. 1,9 mld m^3,
- budowę drugiej nitki Rurociągu Pomorskiego w celu optymalizacji przesyłu ropy naftowej z Naftoportu w Gdańsku w głąb kraju,
- zwiększenie mocy produkcyjnych Rafinerii Gdańskiej w obszarze petrochemii,

[34] SektorCERT, *The attack against Danish, critical infrastructure*…, s. 14–16.

[35] Tamże, s. 26.

[36] FSRU (ang. *floating storage regasification unit*) – jednostka pływająca służąca do regazyfikacji gazu.

- wydobycie ropy naftowej ze złóż zlokalizowanych na Morzu Bałtyckim oraz norweskim szelfie kontynentalnym,
- identyfikacja nowych złóż ropy naftowej i gazu ziemnego na Morzu Bałtyckim i norweskim szelfie kontynentalnym,
- stworzenie możliwości bunkrowania LNG w czterech największych portach Polski: Gdańsk, Gdynia, Szczecin i Świnoujście,
- ustanowienie podmorskiego połączenia stałoprądowego między Polską a Litwą (i szerzej krajami bałtyckimi) o planowanej mocy 700 MW (220 kV),
- możliwe wykorzystanie potencjału hydroenergetycznego.

Do tej listy można by dopisać istniejącą infrastrukturę energetyczną, która nie została wymieniona w PEP2040, ale poniekąd jest skoncentrowana wokół energetyki morskiej lub okołomorskiej państwa, tj. połączenie podmorskie Szwecji oraz Polski przez linię kablową SwePol Link o mocy 600 MW (450 kV) oraz bazy paliwowe ropy naftowej i paliw ciekłych: Dębogórze, Świnoujście, Trzebież, Szczecin, Koszalin, Ugoszcz, Gdańsk. Prawdopodobnie niemal całość zapotrzebowania Polski na gaz ziemny będzie mogła być pokrywana przez dostawy od strony Morza Bałtyckiego, przede wszystkim przez Baltic Pipe. Morskie farmy wiatrowe mają stanowić jeden z trzech filarów podstawy przyszłego miksu energetycznego RP i zaspokajać ok. 18% zapotrzebowania energetycznego[37]. Ponadto można byłoby uwzględnić energię elektryczną wytwarzaną w planowanej elektrowni jądrowej w województwie pomorskim, ponieważ system elektroenergetyczny (głównie infrastruktura przesyłowa) budowany w północnej części Polski będzie rozbudowywany i modyfikowany w taki sposób, aby współdzielić infrastrukturę przesyłową z tą elektrownią oraz m.in. z morskimi farmami wiatrowymi zlokalizowanymi w co najmniej dwóch ławicach: Ławicy Środkowej i Ławicy Słupskiej. To sprawia, że wszelkie zagrożenia cyberbezpieczeństwa w kontekście dystrybucji energii elektrycznej z planowanych morskich farm wiatrowych oraz elektrowni jądrowej będą w istotny sposób wpływać na oba przedsięwzięcia i tym samym znacznie utrudniać ich funkcjonowanie.

W ramach identyfikacji zasobów sektora energetyki w obszarze morskim RP oraz związanych z tym zagrożeń zostały uwzględnione dodatkowe podmioty mające wpływ na kształt sektora energetycznego RP w kontekście energetyki morskiej i okołomorskiej, w postaci: urzędów morskich w Gdyni i Szczecinie oraz

[37] *Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski*, Polityka, 2023 r., https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [dostęp: 15 XII 2024].

Ministerstwa Klimatu i Środowiska (jako urzędu obsługującego ministra odpowiedzialnego za sektor administracji publicznej „energia")[38].

Rodzaje potencjalnych adwersarzy dla zasobów teleinformatycznych przedsiębiorstw sektora energetycznego RP

Przewiduje się, że inwestycje podjęte w polskim sektorze energetycznym będą przynosić stosunkowo duże zyski, szczególnie dla firm stanowiących trzon tego sektora. Dla cyberprzestępców może to być zachętą do działań ofensywnych wobec tych podmiotów. Nie wszystkie próby ataku muszą być jednak motywowane chęcią zysku. Poważnym zagrożeniem mogą się okazać grupy APT, grupy cyberprzestępców sponsorowane przez podmiot państwowy lub powiązane z nim, rywale biznesowi i haktywiści.

Największe zagrożenie, które należy uwzględniać przy ocenie odporności własnych systemów i sieci teleinformatycznych, stanowią obecnie grupy APT. Celem ich precyzyjnych ataków są zazwyczaj najbardziej krytyczne podmioty i instytucje. Działania te mogą trwać wiele miesięcy czy lat, z uwzględnieniem etapu rozpoznania celu, przygotowania właściwych narzędzi pod zidentyfikowane słabości ofiary, utrzymania uzyskanego dostępu do jej systemów i unikaniem wykrycia.

Zagrożeniem są również grupy cyberprzestępcze sponsorowane przez podmiot państwowy lub powiązane z nim. Funkcjonują one (tak jak grupy APT) nierzadko na zasadzie zleceniowości, w tym sprzedaży swoich usług. Cyberprzestępcy sponsorowani przez państwo niewliczający się do kanonu grup APT prowadzą działania krótkoterminowe i/lub średnioterminowe, które skupiają się np. na utrudnieniu funkcjonowania organizacji lub na propagandzie.

Rywale biznesowi mogą okazać się zagrożeniem w kontekście kradzieży lub innych prób uzyskania informacji o stanie realizowanych projektów i wykonujących je firm. Jest to zjawisko nieuczciwej konkurencji – na podstawie wykradzionych informacji (ang. *data theft*) można próbować zaszkodzić planowanej inwestycji, realizującej ją spółce lub modyfikować własne plany inwestycyjne stosownie do działań adwersarza. Takie szkodliwe działania rywal biznesowy może prowadzić sam, ale znacznie częstszą praktyką jest zlecanie ich podmiotowi zewnętrznemu (grupie cyberprzestępczej), niepowiązanemu ze zleceniodawcą.

Ostatnimi z wymienionych są haktywiści, których działania w cyberprzestrzeni są motywowane względami ideologicznymi. Pobudką do podjęcia akcji są

[38] § 1 ust. 2 pkt. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 19 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Klimatu i Środowiska*.

zazwyczaj wydarzenia polityczne. Haktywiści mogą atakować zarówno instytucje państwowe, m.in. w tzw. afekcie (np. po nieakceptowanej przez nich decyzji władz), jak i przedsiębiorstwa, których polityka biznesowa, ekologiczna, cenowa, wizerunkowa wzbudza ich sprzeciw.

Wymienione podmioty mogą dokonać prób sabotażu, infiltracji czy zniszczenia infrastruktury teleinformatycznej obsługującej projekty energetyczne. Konieczne jest więc, aby podmioty odpowiedzialne ze te projekty oraz decydenci przeprowadzili analizy ryzyka i przygotowali plany zabezpieczeń, tak aby zagrożenie atakiem teleinformatycznym sprowadzić do akceptowalnego poziomu.

Warto zaznaczyć, że obecność na polskim rynku energetycznym spółek z zagranicznym kapitałem może być dla adwersarzy zachętą do podjęcia działań ofensywnych względem ich kapitału ulokowanego w inwestycjach energetycznych w Polsce. Przykładem jest Rafineria Gdańska, w której znaczną część udziałów posiada spółka zależna z grupy kapitałowej Saudi Aramco. Takimi działaniami mogą być zainteresowani zwłaszcza haktywiści i rywale biznesowi.

Zasoby teleinformatyczne przedsiębiorstw sektora energetyki morskiej oraz rodzaje ataków na nie

Aktywa, jakie organizacja z sektora energetycznego, w tym energetyki morskiej, musi chronić, aby uniknąć wystąpienia incydentu bezpieczeństwa teleinformatycznego, można podzielić na dwie grupy tzw. środowisk infrastruktury teleinformatycznej. Są to środowiska: korporacyjne oraz automatyki przemysłowej.

Różne systemy i urządzenia, ze względu na specyfikę spełnianych funkcji, mogą być wykorzystywane do wykonywania czynności biurowych oraz czynności zapewniających funkcjonowanie maszyn przemysłowych niezbędnych do produkcji lub dystrybucji energii elektrycznej. Mimo teoretycznej możliwości zupełnego odseparowania tych dwóch środowisk często są one od siebie zależne. Przykładem może być konieczność podjęcia działań korygujących w środowisku automatyki przemysłowej przez uprawnionego użytkownika z sieci korporacyjnej lub użytkownika z firmy zewnętrznej świadczącej usługi utrzymania maszyn przez zdalny dostęp do środowiska automatyki przemysłowej.

Środowisko korporacyjne w dojrzałej organizacji korzysta z takich systemów i urządzeń, jak: własna domena, kontroler domeny, serwery web, serwery e-mail, serwery bazodanowe, aplikacje biznesowe oraz punkty końcowe (stacje robocze, drukarki) itd. Niezależnie od specyfiki środowiska korporacyjnego powinno być ono odpowiednio chronione ze względu na zagrożenia ciągłości działania przedsiębiorstwa oraz wpływ na środowisko automatyki przemysłowej i zależność od niego.

W środowisku automatyki przemysłowej w dużych przedsiębiorstwach, do których można zaliczyć podmioty zapewniające produkcję oraz dystrybucję energii elektrycznej, powinny występować systemy i urządzenia takie jak: terminale zdalnego dostępu typu RTU (ang. *remote terminal unit*), interfejsy HMI[39], system SCADA[40], kontrolery, sterowniki PLC[41], konwertery sygnałów, diody optyczne czy sensory i czujniki. Te z kolei powinny być chronione systemami i urządzeniami odpowiadającymi tym wskazanym dla środowiska korporacyjnego lub wyspecjalizowanymi dla środowisk automatyki przemysłowej – w zależności od potrzeb. Przedstawione przykłady nie są wyczerpujące ze względu na odmienną specyfikę środowisk w różnych przedsiębiorstwach. Mogą one stosować rozmaite podejścia do projektowania i utrzymania swojej infrastruktury teleinformatycznej, w zależności od nakładów finansowych czy zasobów ludzkich, którymi dysponują.

Częstymi problemami występującymi w obu środowiskach są: nieaktualne wersje oprogramowania podatne na ataki[42], brak świadomości użytkowników na temat zagrożeń oraz niestosowanie dobrych praktyk i standardów z dziedziny teleinformatyki i cyberbezpieczeństwa. Przykładowo w ataku za pomocą złośliwego oprogramowania WannaCry wykorzystywano m.in. niezaktualizowane oprogramowanie w postaci protokołu SMBv1[43].

Stosunkowo częstym typem ataków na środowiska automatyki przemysłowej są ataki na łańcuch dostaw. Atakujący podejmują takie działania, gdy nie mogą uzyskać bezpośredniego dostępu, czyli punktu wejścia (ang. *point of entry*), do docelowej infrastruktury. Mniejsi podwykonawcy, z zazwyczaj proporcjonalnie mniejszymi nakładami na bezpieczeństwo teleinformatyczne swojej firmy, są łatwiejszym celem. Do tego rodzaju ataku może dojść np. w przypadku, gdy dostawca – na podstawie umowy z daną organizacją – ma zdalny dostęp do jej przemysłowej infrastruktury teleinformatycznej. Atakujący mogą w ten sposób pozyskać dane uwierzytelniania do kont serwisowych w środowisku automatyki przemysłowej wybranej organizacji i prowadzić już bezpośrednio w niej dalsze działania ofensywne.

---

[39] HMI (ang. *human-machine interface*) – interfejs występujący między maszyną a jej operatorem, najczęściej w postaci graficznej reprezentacji procesu.

[40] SCADA (ang. *supervisory control and data acquisition*) – system teleinformatyczny nadzorujący przebieg procesu produkcyjnego.

[41] PLC (ang. *programmable logic controller*) – programowalny sterownik logiczny, służący do sterowania pracą maszyny.

[42] *Outdated Software*, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [dostęp: 15 XII 2024].

[43] M. Akbanov, V.G. Vassilakis, M.D. Logothetis, *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, „Journal of Telecommunications and Information Technology" 2019, t. 75, nr 1, s. 114–115. https://doi.org/10.26636/jtit.2019.130218.

Mechanizmy ochronne zasobów teleinformatycznych sektora energetycznego RP

Sposoby zabezpieczania zasobów teleinformatycznych sektora energetycznego RP, w tym sektora energetyki morskiej i okołomorskiej, można podzielić na zabezpieczenia indywidualne oraz państwowe, związane z działaniem określonych służb i instytucji.

Zabezpieczenia indywidualne operatora infrastruktury krytycznej

Istotnymi sposobami przeciwdziałania skutkom ewentualnego ataku mogą okazać się m.in. stosowanie urządzeń typu firewall, segmentacja sieci pozwalająca wyizolować potencjalnie zaatakowane urządzenia oraz restrykcyjna kontrola uprawnień kont użytkowników (ang. *identity and access management/privileged access management*, IAM/PAM) zgodnie z dobrymi praktykami środowiska branżowego[44]. Zdarza się, że panele sterowania infrastruktury środowisk automatyki przemysłowej są dostępne z poziomu sieci Internet – czasami nawet bez konieczności uwierzytelnienia użytkownika, co stwarza poważne ryzyko dla takiego systemu[45].

Ze względu na możliwość oddziaływania na siebie środowisk korporacyjnych oraz środowisk automatyki przemysłowej powinny być one zabezpieczone w sposób spójny, nietraktujący żadnego z obszarów jako mniej istotnego wymiaru bezpieczeństwa. Oba środowiska zazwyczaj wykorzystują wspólne elementy infrastruktury teleinformatycznej przedsiębiorstwa, choćby w postaci domeny. Oba zatem mogą stać się ofiarą ataku w przypadku niewłaściwego ich zabezpieczenia. Rozwiązania te powinny być chronione – jako niezbędnym minimum – m.in. za pomocą urządzeń typu firewall, mechanizmów uwierzytelniania wieloskładnikowego (ang. *multi-factor authentication*, MFA), systemów: antyDDoS; zarządzania informacjami i zdarzeniami zabezpieczeń (ang. *security information and event management*, SIEM); zarządzania, automatyzacji i reagowania na zdarzenia bezpieczeństwa (ang. *security orchestration, automation and response*, SOAR); wykrywania nieautoryzowanego dostępu (ang. *intrusion detection system*, IDS); zapobiegania nieautoryzowanemu dostępowi (ang. *intrusion prevention system*, IPS); zapobiegania wyciekowi danych (ang. *data loss prevention*, DLP); ochrony punktów końcowych (ang. *endpoint detection and response*, EDR); typu antywirus, a także IAM/PAM, serwerów z kopiami bezpieczeństwa (backup), filtrów poczty elektronicznej oraz UPS.

---

[44] *Security and Privacy Controls For Information Systems and Organizations*, NIST, September 2020, s. 19–20. https://doi.org/10.6028/NIST.SP.800-53r5.

[45] *Raport roczny z działalności CERT POLSKA 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf, s. 57–58 [dostęp: 16 VII 2025].

Co istotne, zgodnie z procedowanym projektem ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw przewiduje się m.in. wyznaczenie operatorom IK minimalnych standardów cyberbezpieczeństwa[46]. Może to skutkować poprawą bezpieczeństwa teleinformatycznego instytucji najważniejszych z punktu widzenia państwa. Te wymagania będą bazować na wynikach oceny ryzyka rozwiązań organizacyjno-technicznych przeprowadzonej przez dany podmiot. Jest to nowe podejście, w którym uwzględniono ewolucję zagrożeń i dezaktualizację w czasie zastosowanych zabezpieczeń, aby zapewnić ciągłość działań zabezpieczających.

Ponadto w ramach projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa[47] przewiduje się dokonywanie oceny ryzyka w odniesieniu do łańcucha dostaw w postaci dostawców i klientów biznesowych, z którymi podmiot chce współpracować. Celem jest zabezpieczenie sieci i systemów teleinformatycznych przedsiębiorcy przed potencjalnym atakiem na ten łańcuch. Zapisy zawarte w nowelizacji mogą się jeszcze zmienić w zakresie oceny ryzyka, zwłaszcza te dotyczące podmiotów określonych mianem dostawców wysokiego ryzyka. Zmiany mogą być podyktowane m.in. obawami społecznymi co do zgłoszonych propozycji, w tym arbitralnych i motywowanych politycznie decyzji skutkujących uznaniem podmiotu za dostawcę wysokiego ryzyka[48].

Państwowe formy zabezpieczenia operatora infrastruktury krytycznej

Pomimo rosnącego zagrożenia atakami na IK państwa rolą przedsiębiorcy nie jest przeznaczanie wszelkich dochodów z działalności na uodparnianie swojej spółki na dany typ zagrożenia. To państwo powinno ochraniać swoje interesy, w tym dbać o ciągłość funkcjonowania przez zapewnienie bezpieczeństwa procesom wytwarzania i dystrybucji energii elektrycznej na swoim terytorium. Te działania są realizowane m.in. przez Siły Zbrojne RP na podstawie art. 26 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* i aktów prawnych niższego rzędu, Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu na podstawie art. 5 i 6 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* oraz przez Policję na podstawie art. 1 ust. 2 pkt. 2–4 *Ustawy z dnia 6 kwietnia 1990 r.*

---

[46] *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw*, nr UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [dostęp: 16 VII 2025].

[47] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa*...

[48] M. Fraser, *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki*, CyberDefence24, 9 XI 2021 r., https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [dostęp: 18 VII 2025].

o Policji. Zadaniem tych instytucji jest rozpoznawanie zagrożeń bezpieczeństwa państwa i reagowanie na nie.

Działania z zakresu ochrony interesów sektora energetyki morskiej i okołomorskiej RP realizują m.in.:

- Marynarka Wojenna RP – jako rodzaj sił zbrojnych odpowiedzialny za zapewnienie bezpieczeństwa morskiego państwa,
- Morski Oddział Straży Granicznej – prowadzący bieżący nadzór i kontrolę nad obszarami morskimi,
- Wojska Specjalne w postaci jednostek wojskowych GROM oraz Formoza, które umożliwiają szybką odpowiedź na asymetryczne działania kinetyczne;
- Agencja Bezpieczeństwa Wewnętrznego – realizująca zadania zapobiegawcze związane z bezpieczeństwem państwa, IK oraz interesów ekonomicznych RP,
- Agencja Wywiadu – realizująca zadania przeciwdziałania zagrożeniom zewnętrznym względem RP oraz jej interesów i mienia,
- Policja – jako organ odpowiedzialny za zapewnienie ochrony bezpieczeństwa i porządku publicznego państwa,
- CSIRT GOV – odpowiedzialny za zabezpieczanie IK państwa w kontekście zagrożeń cyberbezpieczeństwa.

Większość wymienionych instytucji realizuje zadania ochronne, głównie związane z zagrożeniami o charakterze kinetycznym, zarówno symetrycznymi, jak i asymetrycznymi. Z kolei CSIRT GOV, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w ramach ABW, wykonuje swoje zadania na podstawie art. 26 pkt 3 i 7 oraz art. 27 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa i chroni m.in. operatorów IK w sferze cyfrowej państwa. Pozwala to na udzielanie pomocy tym operatorom w przypadku ataków ze strony m.in. grup APT czy sponsorowanych przez państwa.

Państwo polskie dostrzega zagrożenia dla swoich interesów w rejonie Morza Bałtyckiego i realizuje politykę ich zabezpieczania. Przykładem jest nowo sformowany zespół bojowy Jednostki Wojskowej Formoza, który ma umożliwić bardziej efektywne przeciwdziałanie zagrożeniom kinetycznym o wymiarze asymetrycznym w rejonie Morza Bałtyckiego[49].

[49] *Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, 22 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [dostęp: 10 XII 2024].

Należy pamiętać, że najprawdopodobniej nie wszystkie wskazane w artykule obiekty i inwestycje energetyczne wejdą w skład IK na podstawie kryteriów określonych w niejawnym załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej[50]. Może to wynikać z tego, że obiekty te, jako jeszcze niegotowe, mogły nie przejść procedury wyłonienia obiektów IK spośród ogółu infrastruktury państwa. Ze względu na unikatowy charakter inwestycji typu morskie farmy wiatrowe można rozważyć, czy państwo polskie nie powinno działać wyprzedzająco i uznać takie obiekty, ich instalacje czy części za IK jeszcze przed ich powstaniem. Dzięki temu już w momencie budowy lub modernizacji infrastruktury państwo objęłoby ją ochroną. Takie działania zapewniłyby kompleksowe podejście do problematyki zabezpieczenia interesów energetycznych państwa.

Podsumowanie

W związku z zagrożeniami, przede wszystkim ze strony grup APT oraz grup sponsorowanych przez państwo, dla obecnych i planowanych inwestycji w morską oraz okołomorską infrastrukturę energetyczną konieczne jest, aby państwo polskie zapewniało wsparcie w utrzymaniu predefiniowanego poziomu bezpieczeństwa narażonych organizacji i ich infrastruktury teleinformatycznej, w tym bezpieczeństwa w cyberprzestrzeni. Przy strategicznych projektach realizowanych na podstawie PEP2040 należy zabezpieczyć infrastrukturę teleinformatyczną od początku jej powstawania, zgodnie z podejściem *security by design*. Infrastruktura ta powinna być tworzona zgodnie z najlepszymi praktykami w branży cyberbezpieczeństwa, aby zminimalizować ryzyko skutecznego ataku.

Na podstawie przedstawionych materiałów można wywnioskować, że obecnie państwo polskie może w stopniu podstawowym zapewniać cyberbezpieczeństwo sektora energetyki morskiej oraz okołomorskiej. W czasach bezwzględnej rywalizacji w cyberprzestrzeni może to być niewystarczające, zwłaszcza jeśli weźmie się pod uwagę zagrożenia, jakie mogą się pojawić w przyszłości, oraz dostępne sposoby ich mitygacji. Brakuje działań wyprzedzających, które sprawiłyby, że projekty energetyczne o znaczeniu strategicznym dla bezpieczeństwa państwa byłyby zabezpieczane od początku ich cyklu rozwojowego (fazy planistyczno-koncepcyjnej). Ponadto, jak zostało to wskazane, zagrożenie może się zmaterializować w postaci nie tylko bezpośredniego ataku teleinformatycznego na organizację, lecz także – co staje się coraz częstsze – ataku na łańcuch dostaw. Podwykonawca może się

[50] *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

okazać dogodnym punktem dostępowym do infrastruktury organizacji docelowej. Bez poszerzenia działań zabezpieczających zarówno ze strony operatorów IK, jak i państwa ochrona może się okazać nieskuteczna i nieprzystająca do realiów. Konieczna może być ocena skutków proponowanych regulacji prawnych – w postaci nowelizacji ustaw o zarządzaniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa – w odniesieniu do ich skuteczności względem obecnych i przyszłych wyzwań w obszarze cyberbezpieczeństwa. Dzięki temu będzie można bardziej kompleksowo podejść do tej problematyki.

Bibliografia

Akbanov M., Vassilakis V.G., Logothetis M.D., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, „Journal of Telecommunications and Information Technology" 2019, t. 75, nr 1, s. 113–124. https://doi.org/10.26636/jtit.2019.130218.

Chen T.M., *Stuxnet, the Real Start of Cyber Warfare?*, „IEEE Network" 2010, t. 24, nr 6, s. 2–3. https://doi.org/10.1109/MNET.2010.5634434.

Krasznay C., *Case Study: The NotPetya Campaign*, w: *Információ- és kiberbiztonság*, B. Török (red.), Budapest 2020.

Nakov A., Nuño G., *Saudi Aramco and the Oil Market*, „Working Paper Series" 2011, nr 1354.

Security and Privacy Controls For Information Systems and Organizations, NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Siboni G., Kronenfeld S., *Iran and Cyberspace Warfare*, „Military and Strategic Affairs" 2012, t. 4, nr 3, s. 77–99.

Źródła internetowe

Baezner M., Robin P., *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf [dostęp: 16 VII 2025].

Behind the Rise of the Million Dollar Zero-Day Market, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [dostęp: 14 XII 2024].

Buchholz K., *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025 r., https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [dostęp: 16 VII 2025].

Buli N., Chestney N., Steitz Ch., *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023 r., https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [dostęp: 5 XII 2024].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20 VII 2021 r., https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 28 XI 2024].

Falliere N., Murchu L.O., Chien E., *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf [dostęp: 16 VII 2025].

Fraser M., *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki*, CyberDefence24, 9 XI 2021 r., https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [dostęp: 18 VII 2025].

Hultquist J., *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016 r., https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [dostęp: 15 XII 2024].

Kerttunen M., Hemmelskamp J., *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf [dostęp: 16 VII 2025].

Lorenz W., Zaręba S., *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2*, Polski Instytut Spraw Międzynarodowych, 29 IX 2022 r., https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [dostęp: 16 VII 2025].

Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski, Polityka, 2023 r., https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [dostęp: 15 XII 2024].

Outdated Software, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [dostęp: 15 XII 2024].

Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej, Ministerstwo Obrony Narodowej, 22 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [dostęp: 10 XII 2024].

Roncone G., Black D., Wolfram J., McLellan T., Simonian N., Hall R., Prokopenkov A., Perez D., Aytes L., Wahlstrom A., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024 r., https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 16 VII 2025].

SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf [dostęp: 6 VIII 2025].

Saudi Aramco przejmie udziały w gdańskiej rafinerii, CIRE, 12 I 2022 r., https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [dostęp: 14 XII 2024].

SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 5 XII 2024].

Styczynski J., Beach-Westmoreland N., *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [bmw] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [dostęp: 16 VII 2025].

Akty prawne

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

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2024 r. poz. 1077, ze zm.).

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

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2025 r. poz. 902).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2025 r. poz. 636, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 19 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Klimatu i Środowiska (DzU z 2023 r. poz. 2726).

Inne dokumenty

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

Polityka energetyczna Polski do 2040 r., Ministerstwo Klimatu i Środowiska, Warszawa 2021.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, nr UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [dostęp: 16 VII 2025].

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, nr UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [dostęp: 16 VII 2025].

Raport roczny z działalności CERT POLSKA 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf [dostęp: 16 VII 2025].

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

Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 119–152

 https://doi.org/10.4467/20801335PBW.25.006.22172

ARTYKUŁ

Ruchy antypaństwowe w Polsce i ich wpływ na sektor publiczny oraz bankowy

Anti-state movements in Poland and their impact on the public and banking sectors

PATRYK KRÓL

Autor niezależny

https://orcid.org/0000-0003-4079-8849

Abstrakt

Celem artykułu jest przedstawienie współczesnych ruchów antypaństwowych w Polsce, które inspirują się amerykańskim ruchem sovereign citizen. Autor omawia ich ideologię, metody działania, skalę popularności w internecie oraz zagrożenia, jakie mogą stwarzać dla porządku prawnego i społecznego w Polsce. W pracy autor wykorzystał metodę przeglądu literatury naukowej, a także analizę propagandowych i pseudoprawnych materiałów publikowanych przez polskie ugrupowania antypaństwowe. Wykazał, że polskie ruchy sovereign citizen, takie jak Zawodowy Polak czy Ruch II RP, adaptują amerykańskie metody do warunków krajowych. Autor przedstawił propozycje działań prewencyjnych, które mogłyby ograniczyć wpływ tych ruchów na polskie społeczeństwo i zapewnić lepszą ochronę struktur państwowych, w tym sektora bankowego. Zaproponował również wdrożenie działań edukacyjnych i legislacyjnych oraz monitorowanie działalności tych grup.

Słowa kluczowe

ruchy antypaństwowe, suwerenni obywatele, pseudoprawo, radykalizacja, destabilizacja państwa

Abstract

The purpose of this article is to present contemporary anti-state circles in Poland that are inspired by the US sovereign citizen movement. The author discusses their ideology, the methods of operation used, scale of popularity and the threats they may potentially pose to the legal and social order in Poland. In the study, the author used a review of scientific literature method, as well as an analysis of propaganda and pseudo-legal materials published by Polish anti-government organisations. Polish sovereign citizen movements, such as Zawodowy Polak (Professional Pole) or Ruch II RP (the Second Polish Republic movement) movements, have been shown to adapt the US methods to local contexts. The author presented proposals for preventive measures that could limit the impact of these movements on Polish society and provide better protection for state structures, including the banking sector. He also suggested implementing educational and legislative measures as well as monitoring the activities of these groups.

Keywords

anti-state movements, sovereign citizens, pseudo-law, radicalisation, state destabilisation

Wprowadzenie

Ruch sovereign citizen (pol. suwerenni obywatele) to antyrządowy ruch społeczny, który wyrósł na gruncie amerykańskich ruchów antypodatkowych oraz radykalnych i rasistowskich organizacji antypaństwowych z lat 60. i 70. XX w.[1] Z czasem jego zwolennicy zaczęli używać tzw. pseudoprawa, czyli zestawu fikcyjnych procedur i argumentów prawnych, w celu podważania obowiązującego porządku prawnego. Aby unikać obowiązków wobec państwa, np. płacenia podatków, mandatów czy innych zobowiązań administracyjnych, sympatycy ruchu tworzą skomplikowane, często bezzasadne pisma i prowadzą działania pseudoprawne. Wierzą, że w ten sposób zablokują lub przynajmniej opóźnią egzekwowanie prawa wobec nich[2].

Władze Stanów Zjednoczonych traktują ruch sovereign citizen z coraz większą powagą. Federalne Biuro Śledcze (Federal Bureau of Investigation, FBI)

[1] S.A. Kent, *Freemen, Sovereign Citizens, and the Challenge to Public Order in British Heritage Countries*, „International Journal of Cultic Studies" 2015, nr 6, https://skent.ualberta.ca/wp-content/uploads/2015/06/Freemen-Internl-J-of-Cultic-Studies.pdf, s. 1–15 [dostęp: 25 X 2024].

[2] A. Morozov, R. Bruinsma, J. Rudnick, *Assembly of viruses and the pseudo law of mass action*, „Biophysical Journal" 2009, t. 96, nr 3, s. 419a–420a.

zwróciło uwagę na agresywne zachowania jego członków i w 2010 r. sklasyfikowało go jako ruch terrorystyczny i ekstremistyczny[3]. Badania amerykańskich psychiatrów również potwierdzają, że sovereign citizen jest jednym z największych antyrządowych lub związanych z krajowym terroryzmem ugrupowań w Stanach Zjednoczonych. W latach 2014–2024 ponad dziesięciu funkcjonariuszy publicznych zostało rannych lub zabitych przez osoby wyznające ideologię sovereign citizen. Badania przeprowadzone z zastosowaniem Terrorist Radicalization Assessment Protocol (TRAP-18) wykazały, że istnieje związek między cechami zachowań członków tego ruchu a wzrostem ryzyka eskalacji przemocy. Po przeanalizowaniu zarówno przemocowych, jak i nieagresywnych zachowań osób powiązanych z ruchem sovereign citizen okazało się, że suma punktów w TRAP-18 jest dobrym wskaźnikiem predyspozycji jednostki do działalności terrorystycznej. Dotyczy to szczególnie tzw. samotnych wilków, czyli terrorystów samodzielnie planujących i organizujących ataki terrorystyczne. Warto zatem rozwijać badania nad wykorzystywaniem TRAP-18 w ocenie zagrożeń ze strony ugrupowań, które wykazują skłonności do przemocy[4].

Według raportów FBI przedstawiciele ruchu wielokrotnie stosowali przemoc, m.in. dokonywali morderstw[5] i napaści fizycznych. Grozili też sędziom, funkcjonariuszom organów ścigania i pracownikom instytucji państwowych[6], dokonywali oszustw finansowych[7] oraz posługiwali się fałszywymi dokumentami, w tym paszportami i prawami jazdy, fałszywymi tablicami rejestracyjnymi i pieniędzmi[8].

---

[3] FBI, *Domestic terrorism. The Sovereign Citizen Movement*, 13 IV 2010 r., https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement [dostęp: 15 XII 2024].

[4] D.J. Challacombe, P.A. Lucas, *Postdicting violence with sovereign citizen actors: An exploratory test of the TRAP-18*, „Journal of Threat Assessment and Management" 2019, t. 6, nr 1, s. 51–59. https://doi.org/10.1037/tam0000105.

[5] *Murder of Dallas Police Officer Marks Latest in String of Violent Sovereign Citizen Encounters with Law Enforcement*, Anti-Defamation League, 9 XII 2024 r., https://www.adl.org/resources/article/murder-dallas-police-officer-marks-latest-string-violent-sovereign-citizen [dostęp: 1 I 2025].

[6] FBI's Counterterrorism Analysis Section, *Sovereign Citizens. A Growing Domestic Threat to Law Enforcement*, FBI Law Enforcement Bulletin, 1 IX 2011 r., https://leb.fbi.gov/articles/featured-articles/sovereign-citizens-a-growing-domestic-threat-to-law-enforcement [dostęp: 1 I 2025].

[7] IRS Criminal Investigation, *Sovereign citizen sentenced to 9 years in prison for $3.4 million tax fraud scheme, filing a false lien, and absconding while on bond*, Press Release, 22 V 2024 r., https://www.irs.gov/compliance/criminal-investigation/sovereign-citizen-sentenced-to-9-years-in-prison-for-3-point-4-million-tax-fraud-scheme-filing-a-false-lien-and-absconding-while-on-bond [dostęp: 1 VII 2025].

[8] C. Meyer, *5 Common Crimes Committed by Sovereign Citizens*, Police1, 6 IX 2024 r., https://www.police1.com/community/articles/5-common-crimes-committed-by-sovereign-citizens-1KKxo-42li5FVeANM/ [dostęp: 1 I 2025].

Członkowie ruchu podszywają się też pod funkcjonariuszy policji lub dyplomatów i w ten sposób próbują uzyskać nienależne im przywileje lub immunitety.

W Polsce ruchy o charakterze antypaństwowym lub altpaństwowym[9] zaczęły się pojawiać w kilku ostatnich dekadach, po przemianach ustrojowych w 1989 r. W wielu przypadkach inspirują się one – świadomie lub nie – amerykańskim ruchem sovereign citizen, zarówno w sensie ideologicznym, jak i organizacyjnym. W pierwszych latach transformacji w Polsce odnotowano pojedyncze inicjatywy tego typu, np. działalność Marka Świętopełka-Zawadzkiego, o marginalnym charakterze. Wcześniej, w okresie Polskiej Rzeczpospolitej Ludowej, tego typu ruchy nie powstawały ze względu na ograniczony dostęp do informacji z zagranicy oraz brak sprzyjających warunków politycznych i społecznych. Aktywność zbliżona ideowo, np. Juliusza Nowiny-Sokolnickiego, od którego czerpie legitymację Jan Potocki, założyciel Ruchu II RP opisanego w dalszej części artykułu, rozwijała się wtedy na emigracji.

Ruchy anty- i altpaństwowe stały się bardziej aktywne dopiero w XXI w. Dało się to zauważyć zwłaszcza podczas pandemii COVID-19. Wprowadzenie restrykcji oraz zamknięcie wielu sektorów życia publicznego i gospodarki wywoływały frustrację w społeczeństwie i spotkały się z rosnącym sprzeciwem wobec państwowego aparatu kontroli. Ruch suwerennych obywateli wykorzystał ten moment. Zaproponował alternatywną retorykę wolnościową i narrację, w której państwo uznaje się za opresyjną strukturę, nieposiadającą realnej legitymacji.

Organizacje suwerennych obywateli to w Polsce nadal zjawisko niszowe. Ich popularność oraz skłonność do radykalizacji jednak wzrastają. Zwolennicy tych grup kwestionują legalność polskich władz i wprowadzają własne struktury, czyli alternatywne władze, sądy, tworzą własne wzory dokumentów i argumenty prawne, które wykorzystują do utrudniania pracy instytucji publicznych oraz wyrażania sprzeciwu wobec organów ścigania. Zdaniem autora artykułu działania te coraz częściej mają charakter zorganizowany i przyciągają nowych sympatyków, głównie za pośrednictwem internetu, w którym grupy te szerzą sceptycyzm wobec prawa i rządzących.

W artykule autor omówił korzenie ideologiczne polskich suwerennych obywateli, metody ich działania oraz wpływ tych działań na porządek w państwie. Przybliżył, w jaki sposób ruchy w Polsce adaptują amerykańskie wzorce do krajowych realiów oraz jakimi strategiami komunikacyjnymi i narzędziami się posługują. Przedstawił genezę oraz aktywność w ostatnich latach wybranych grup suwerennych obywateli, a także wykorzystywane przez nie sposoby szerzenia propagandy.

[9] Autor wprowadza to pojęcie na potrzeby artykułu. Przez ruchy altpaństwowe rozumie nie tylko te, które kwestionują legalność władzy i porządku prawnego, lecz także te, które próbują tworzyć własne państwa w państwie, ze swoimi dokumentami, symbolami, urzędami czy prawem. Cechą charakterystyczną tych ruchów jest dążenie do zignorowania porządku państwowego lub zastąpienia go równoległą strukturą opartą na własnych zasadach.

Zaproponował również działania prewencyjne, które mogłyby ograniczyć destabilizujący wpływ inicjatyw suwerennych obywateli na pracę organów państwowych, w tym zmiany legislacyjne, oraz strategie reagowania na potencjalne zagrożenia wynikające z ich działalności. Omówił ponadto postulaty regulacji prawnych służących zwalczaniu propagandy antypaństwowej i ochronie społeczeństwa przed wpływem ideologii związanych z ruchem sovereign citizen.

Wierzenia i pseudoprawne metody działania ruchu sovereign citizen

Pseudoprawo, stanowiące jeden z fundamentów ruchu sovereign citizen, wykształciło się jako charakterystyczny, złożony system metod i wierzeń, określany w literaturze nawet jako system ezoteryczny czy magiczny[10]. Ma on na celu destabilizację instytucji państwowych oraz uniknięcie przez zwolenników ruchu odpowiedzialności prawnej. Polega to m.in. na tworzeniu dokumentów i pism o absurdalnej treści, które są składane w urzędach z przekonaniem o ich mocy prawnej. Przedstawiciele ruchu zakładają, że przez odpowiedni dobór słów, strukturę tekstu, a także formę podpisu można symbolicznie i prawnie wyodrębnić się z systemu państwowego. Dokumenty sporządzane przez zwolenników ruchu sovereign citizen często są podpisywane czerwonym atramentem, co ma oznaczać, że podpisujący jest fizyczną „osobą z krwi i kości", w odróżnieniu od podpisu w kolorze czarnym lub niebieskim, mającym oznaczać „osobę prawną" lub „fikcję prawną"[11] (różnice między osobą fizyczną a prawną przedstawiono w tabeli 1). Czerwona barwa nawiązuje do praktyki oznaczania w niektórych stanach USA ważnych dokumentów. Traktuje się ją niemal jak magiczny znak odróżniający realnego człowieka od abstrakcyjnej osoby prawnej.

Tabela 1. Różnice między osobą prawną a osobą fizyczną według ideologii sovereign citizen.

	Osoba prawna	**Osoba fizyczna**
Nazwa w języku angielskim	*strawman*, *legal person*, *corporate entity*, *fictional entity*	*natural person*, *living man/woman*, *living soul*, *flesh and blood human*
Charakter	fikcyjna tożsamość stworzona przez państwo	realna, żywa istota

[10] Nie jest to jednolity zbiór zasad. Obejmuje różne praktyki i wierzenia, które są często sprzeczne ze sobą.

[11] *The Sovereigns: A Dictionary of the Peculiar*, Southern Poverty Law Center, 1 VIII 2010 r., https://www.splcenter.org/fighting-hate/intelligence-report/2010/sovereigns-dictionary-peculiar [dostęp: 14 VII 2024].

	Osoba prawna	Osoba fizyczna
Pisownia (przykłady)	wersaliki, np. JAN KOWALSKI	z dopiskiem przed nazwiskiem, np. Jan z rodu Kowalskich, często zapisywane kolorem czerwonym
Źródło istnienia	akt urodzenia, rejestracja w państwie	narodziny
Podległość prawna	podlega prawu publicznemu (administracyjnemu, podatkowemu itd.)	podlega tylko prawu naturalnemu (ang. *common law*)
Status wg państwa	uznawany jako obywatel, podatnik, podmiot prawny	nieuznawany jako odrębny byt prawny (według ideologii, ale nie w prawie)
Reprezentacja	reprezentuje ją numer PESEL, NIP, dokumenty urzędowe	wolna jednostka, która nie ma urzędowej reprezentacji
Typ podmiotu	konstrukcja prawna, konstrukt społeczny, jak firma czy spółka	człowiek z duszą, zdolny do suwerennego działania

Źródło: opracowanie własne.

Rozróżnienie między osobą prawną i osobą fizyczną, będące jednym z dogmatów ruchu, nawiązuje do teorii kukły (ang. *strawman theory*), według której każdy człowiek ma dwie osoby: prawną i fizyczną, a obowiązki prawne i zobowiązania podatkowe dotyczą wyłącznie tej pierwszej[12]. Zwolennicy tej teorii wierzą, że posługując się odpowiednimi formami podpisu, np. John-Robert: Doe w miejsce powszechnie stosowanego John Robert Doe, mogą uniknąć zobowiązań związanych z osobą prawną. Powszechną praktyką jest również umieszczanie symbolu copyright (©) przy imieniu i nazwisku. Ma to rzekomo chronić przed użyciem tych danych przez inne osoby lub instytucje bez zgody właściciela[13]. Członkowie ruchu po swoim imieniu i nazwisku dopisują także łacińskie *sui iuris* (pol. [osoby] swojego prawa), co ma oznaczać autonomię jednostki oraz odmowę uznania przepisów narzuconych przez organy państwowe.

[12] Na temat tej teorii zob. szerzej: *Redemption Theory/Strawman Theory*, Anti-Defamation League, https://extremismterms.adl.org/glossary/redemption-theorystrawman-theory [dostęp: 14 VII 2025].

[13] *The Sovereign Citizen Movement: Common Documentary Identifiers & Examples*, Anti-Defamation League, 5 XII 2016 r., https://www.adl.org/resources/reports/the-sovereign-citizen-movement-common-documentary-identifiers-examples [dostęp: 25 X 2024].

Innym rozpowszechnionym elementem pseudoprawnych wierzeń jest przekonanie, że rząd federalny zakłada każdej osobie po jej narodzinach tajne konto w skarbie państwa, na którym zabezpiecza się przewidywane zarobki tej osoby. Zwolennicy ruchu podejmują próby odzyskania dostępu do tych środków. W tym celu np. składają w amerykańskich urzędach formularz 1099-OID z nieprawdziwymi danymi, co prowadzi do oszustwa podatkowego. Za pomocą tej metody w 2016 r. ruch wyłudził od rządu ok. 43 mln dolarów[14].

Kolejną manipulacją ruchu sovereign citizen jest teoria związana z prawem morskim. Wywodzi się ona z błędnej interpretacji XVII-wiecznego brytyjskiego aktu prawnego *Cestui Que Vie Act* z 1666 r.[15] Umożliwiał on uznanie osoby za zmarłą po upływie siedmiu lat od zaginięcia, np. na morzu, gdy odnalezienie jej ciała było niemożliwe[16]. Powołując się na ten dokument, zwolennicy ruchu twierdzą, że po ukończeniu przez dziecko siódmego roku życia rząd zniewala jednostkę, traktując ją jak zaginioną w sensie prawnym oraz przejmuje kontrolę nad jej majątkiem. Przekonanie to znajduje odbicie w języku ruchu, w którym pojęcia związane z prawem morskim są wykorzystywane do argumentowania, że każde obywatelskie zobowiązanie finansowe jest w rzeczywistości wynikiem zniewolenia przez instytucje państwowe[17]. W tym zakresie członkowie ruchu odwołują się także do XIII-wiecznej *Magna Carty*[18].

Badacze wskazują także na rasistowskie aspekty ruchu sovereign citizen. Niektóre frakcje uznają za suwerennego obywatela jedynie osoby o białej skórze. Źródłem tego poglądu jest nieprawidłowa interpretacja 14. poprawki do Konstytucji

---

[14] A. Powers, *How Sovereign Citizens Helped Swindle $1 Billion From the Government They Disavow*, The New York Times, 29 III 2019 r., https://www.nytimes.com/2019/03/29/business/sovereign-citizens-financial-crime.html [dostęp: 25 X 2024].

[15] Ch. Koppelman, *Construction as Resistance: Constructing a desired and envisioned future to perceived oppression for the sovereign citizen milieu in the Netherlands*, Utrecht University 2024, https://studenttheses.uu.nl/bitstream/handle/20.500.12932/47667/h.c.koppelman_6919642_thesis_CSHR.pdf?sequence=1&isAllowed=y [dostęp: 1 VII 2025].

[16] Ch.M. Sarteschi, *Sovereign Citizens and QAnon: The Increasing Overlaps with a Focus on Child Protective Service (CPS) Cases*, „International Journal of Coercion, Abuse & Manipulation" 2023, t. 6. https://doi.org/10.54208/1000/0006/006.

[17] C. Kalinowski IV, *A Legal Response to the Sovereign Citizen Movement*, „Montana Law Review" 2019, t. 80, nr 2, s. 153–210, https://scholarworks.umt.edu/mlr/vol80/iss2/2/ [dostęp: 25 X 2024].

[18] *Magna Carta*, znana również jako *Magna Charta Libertatum* (Wielka Karta Wolności, ang. *The Great Charter*), to dokument wydany i podpisany przez króla Jana bez Ziemi w Anglii 15 czerwca 1215 r. Stanowił on formę umowy między monarchą a możnowładcami i był zarazem przywilejem ograniczającym władzę królewską, szczególnie w kwestiach finansowych (wprowadzenie podatków wymagało zgody rady królestwa) oraz sądowych (zakaz więzienia lub karania bez wyroku sądu). Dokument określał również prawa baronów i duchowieństwa, a także zakres wolności niższych warstw społecznych.

Stanów Zjednoczonych, która – zdaniem przedstawicieli tych frakcji – polega na tym, że czarnoskórzy Amerykanie stali się własnością rządu federalnego. To oznacza, że nie mają oni praw przysługujących suwerennym jednostkom, czyli białym obywatelom. W rzeczywistości poprawka dotyczy nadania praw i wolności wszystkim obywatelom Stanów Zjednoczonych, co było przyczynkiem do zniesienia niewolnictwa w tym kraju. Organizacja Southern Poverty Law Center zwraca uwagę na silne powiązania ruchu sovereign citizen z ekstremistycznymi i rasistowskimi organizacjami, dla których antypaństwowa retoryka stanowi narzędzie walki o zachowanie tzw. czystości rasowej oraz wyższości białej rasy[19].

Dyskurs ruchu sovereign citizen wykazuje również cechy zbliżone do psychotycznych struktur znaczeniowych, które Calum Lister Matheson w artykule pt. *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*[20] omawia z perspektywy psychoanalizy Jacques'a Lacana. Matheson sugeruje, że idea ruchu koncentruje się wokół odrzucenia pojęcia prawa, które zastępuje systemem znaków o niemal magicznym charakterze. Certyfikaty urodzenia czy fikcyjne tożsamości nabierają w nim dosłownego znaczenia. Język używany przez zwolenników ruchu sovereign citizen buduje wyizolowany porządek znaczeniowy, w którym odnajdują oni spójność oraz sens, jednocześnie odrzucając zasady rzeczywistego systemu prawnego. Zdaniem Mathesona zrozumienie tych psychotycznych struktur oraz mechanizmów może dać narzędzia do krytyki i reagowania na retorykę ruchu, którego destabilizacyjny potencjał tkwi zarówno w naruszaniu prawa, jak i w wywoływaniu napięć społecznych.

Ruchy w Polsce inspirowane ruchem sovereign citizen

W Polsce organizacje antypaństwowe, które inspirują się amerykańskim ruchem, są aktywne głównie w internecie. Na temat ich działalności brakuje literatury naukowej, a działania podejmowane przez państwo wobec tego środowiska nie są udokumentowane w takim stopniu jak w USA. Autor przedstawia najaktywniejszych suwerennych obywateli w Polsce i omawia metody ich działania.

Zawodowy Polak

Jedno ze środowisk suwerennych obywateli jest skupione wokół Tadeusza Cichockiego, a kanały komunikacji jego zwolenników to strona internetowa zawodowy-polak.pl oraz kanały YouTube Zawodowy Polak i @katerina404. Po wyborach

[19] *The Sovereigns: A Dictionary of the Peculiar…*

[20] C.L. Matheson, *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*, „Rhetoric Society Quarterly" 2018, t. 2, nr 48, s. 187–206.

samorządowych w Polsce, 25 października 2018 r. Cichocki opublikował w internecie *Dekret Zwierzchnika Władzy w Rzeczypospolitej Polskiej 1-2018*, na który powołują się w swoich dokumentach inni polscy sovereign citizens[21]. Zwolennicy Cichockiego przesyłają do jego wiadomości pisma, które kierują do różnych urzędów. Liczebność ruchu Zawodowy Polak jest trudna do oszacowania ze względu na jego nieformalny i zdecentralizowany charakter. Na 14 lipca 2025 r. na stronie zawodowy-polak.pl było opublikowanych 125 indywidualnych deklaracji samostanowienia i odpowiedzialności, z których ostatnia była z 15 lipca 2024 r.[22] Kanał na YouTube Zawodowy Polak w październiku 2024 r. miał 9470 subskrybentów. Trudno oszacować, ile z oglądających osób identyfikuje się z ruchem i bierze w nim aktywny udział. Przy nagraniu z 2 lipca 2024 r. pt. *Najemnicy NFUMiG Konstancin Jeziorna*, na którym zwolennik ruchu polemizuje z urzędniczką Wydziału Planowania Przestrzennego Urzędu Miasta i Gminy Konstancin-Jeziorna, widnieje 25 komentarzy, z których większość pozytywnie odnosi się do treści nagrania[23]. Skrótowiec NFUMiG oznacza Nielegalnie Funkcjonujący Urząd Miasta i Gminy. Przy kontaktach z instytucjami publicznymi zwolennicy ruchu Zawodowy Polak stosują skróty zaczynające się NF, a wobec urzędników dodają przed nazwą stanowiska – pełniący obowiązki, a po nazwie stanowiska – bez upoważnienia (rysunek 1).

Nielegalnie Funkcjonujący Sąd Rejonowy dla Warszawy – Woli
Zorganizowana Grupa Przestępcza
Do S Ł
pełniącego obowiązki prezesa sądu rejonowego bez upoważnienia
Do J S
pełniącej obowiązki sądziego bez upoważnienia

Rysunek 1. Przykład adresowania wiadomości do organów publicznych przez ruch Zawodowy Polak.

Źródło: pismo z 28 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) Syg. Akt I Co 3161/2, Zawodowy Polak, https://www.zawodowy-polak.pl/TB-NFSR-W-wa_Wola_28.05.2024.pdf [dostęp: 14 VII 2025]. Anonimizacji dokonał autor artykułu.

[21] T. Cichocki, *Dekret Zwierzchnika Władzy w Rzeczypospolitej Polskiej 1-2018*, https://www.tcichocki.pl/Dekret%20Zwierzchnika%20W%C5%82adzy%20w%20RP%201-2018%202018.10.25.pdf [dostęp: 25 X 2024].

[22] *Deklaracja Samostanowienia i Odpowiedzialności*, Zawodowy Polak, https://www.zawodowy-polak.pl/index.php?title=Deklaracja_Samostanowienia_i_Odpowiedzialno%C5%9Bci [dostęp: 15 XII 2024].

[23] *Najemnicy NFUMiG Konstancin Jeziorna*, kanał na YouTube Zawodowy Polak, 2 VII 2024 r., https://www.youtube.com/watch?v=jeH8LX0eYfY [dostęp: 1 VII 2025].

W przypadku ruchu Zawodowy Polak, podobnie jak innych ruchów sovereign citizen, trudno wskazać usystematyzowany system poglądów i wierzeń. Można zaobserwować raczej zbitkę różnych, niepowiązanych lub sprzecznych poglądów, wierzeń i teorii spiskowych. Na stronie zawodowy-polak.pl znajdują się zarówno dłuższe dokumenty i wypowiedzi, jak i krótkie chaotyczne hasła. Zwolennicy ruchu na podstawie m.in. art. 4 Konstytucji Rzeczpospolitej Polskiej określają się Zwierzchnikami Władzy[24], a jednocześnie zamieszczają na swojej stronie internetowej IV Konwencję Genewską[25] z zastrzeżeniami państw, które ją przyjęły. W innym miejscu strony są publikowane projekty i propozycje ruchu dotyczące prawa wyborczego[26]. Prezentowane są także antyreligijne treści Anne Marie Riezinger (vel Anne Von Reitz), samozwańczej Najwyższej Sędzi Alaski[27]. Wydaje się więc, że polski odłam ruchu sovereign citizen, poza tłumaczeniem oraz częściowym dostosowaniem pism amerykańskich zwolenników ruchu, nie wnosi nowych, oryginalnych koncepcji do ideologii antypaństwowych.

Warto zauważyć, że Zawodowy Polak, podobnie jak inni przedstawiciele ruchu sovereign citizen, odwołuje się do alternatywnych interpretacji prawa, których celem jest podważenie instytucji państwowych, w tym sądownictwa, administracji, oraz ich polityki. Zwolennicy ruchu często ignorują obowiązujące przepisy i normy prawne, gdyż uznają je za nieistniejące lub nielegalne, co prowadzi do niejednoznacznych i trudnych do przewidzenia działań na poziomie prawnym i społecznym.

Publikacje i wypowiedzi przedstawicieli Zawodowego Polaka mogą wydawać się skomplikowane, jednak opierają się na prostych, lecz błędnych założeniach dotyczących natury władzy, prawa oraz państwa. Zawierają dezinformację i manipulacje logiczne i jako takie mogą stanowić zagrożenie dla porządku publicznego i stabilności społecznej.

---

[24] Zob. np. akt oskarżenia z 4 XI 2024 r., Zawodowy Polak, https://www.zawodowy-polak.pl/KC-Akt_Oskarzenia-NFPR-4.11.2024.pdf [dostęp: 14 VII 2025]; pismo z 7 III 2024 r. dotyczące braku uprawnień do pełnienia funkcji sędziego, dyrektora i prezesa – dyskryminacji, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFSR-Grojec_7.03.2024.pdf [dostęp: 14 VII 2025].

[25] *IV Konwencja Genewska*, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=IV_Konwencja_Genewska [dostęp: 1 I 2025].

[26] *Prawo wyborcze*, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Prawo_wyborcze [dostęp: 1 I 2025].

[27] B.J. Kelley, *Interview with a sovereign: Judge Anna's World*, Southern Poverty Law Center, 15 XII 2017 r., https://www.splcenter.org/hatewatch/2017/12/15/interview-sovereign-judge-anna%E2%80%99s-world [dostęp: 1 I 2025]; *Report and Recommendation*, Case No. 1:16-cv-614, https://www.govinfo.gov/content/pkg/USCOURTS-ohsd-1_16-cv-00614/pdf/USCOURTS-ohsd-1_16-cv-00614-0.pdf [dostęp: 1 I 2025]; *Religia*, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Religia [dostęp: 9 VII 2025].

Podobieństwo Zawodowego Polaka do ruchu sovereign citizen jest widoczne głównie w publikacjach zamieszczanych na stronie zawodowy-polak.pl. Stanowią one wzorzec dla polskich suwerennych obywateli, którzy przygotowują swoje wersje tych pism do urzędów i firm w Polsce. Elementy zapożyczone od amerykańskiego ruchu sovereign citizen i wykorzystywane przez Zawodowego Polaka przedstawia rysunek 2. Są to:

1) rozróżnienie między osobą prawną a osobą fizyczną (z krwi i kości) – na grafice jest to czerwony podpis,
2) charakterystyczny zapis nazwiska, tj. dywiz między imionami, dopisek „syn" i „z rodu" przed nazwiskiem oraz znak copyright,
3) pieczęć z orłem stylizowana na pieczęć urzędową.


Formalną odpowiedź w tej sprawie pod rygorem jej nieważności należy adresować nie do osoby fizycznej, lecz do:

Zwierzchnik władzy i administracji w Rzeczypospolitej Polskiej
Syn H i J z rodu Ch : K - P

Zwierzchnik Władzy w Rzeczypospolitej Polskiej
Władza Zwierzchnia

Do wiadomości:
-Zwierzchnik władzy - administracji Rzeczypospolitej Polskiej;
-Tadeusz Cichocki t.cichocki@t.cichocki.pl Tel./fax (22) 756-16-41
- Europejski Trybunał Praw Człowieka, Międzynarodowy Trybunał Karny, Helsińska Fundacja Praw Człowieka - hfhr@hfhr.pl , ambasady i inni...

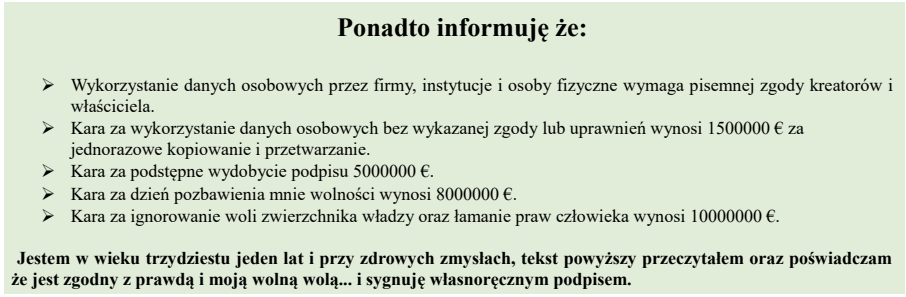
Rysunek 2. Przykład podpisu stosowanego przez ruch Zawodowy Polak.

Źródło: Pismo z 8 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) Syg. Akt: 4161-0.Ds 783.24, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFPR-Lukow_8.05.2024.pdf [dostęp: 14 VII 2024]. Anonimizacji dokonał autor artykułu.

Warto zauważyć, że twórca ruchu Zawodowy Polak w publikowanych dokumentach podpisuje się czcionką w kolorze czarnym, bez podpisu odręcznego, znaku copyright, dywizu między imionami i dopisku „z rodu" przed nazwiskiem[28]. Oznacza to, że metody stosowane przez osoby, które utożsamiają się z ruchem, mogą być tworzone niezależnie i doraźnie, według pomysłów tych osób. Ideologia i wierzenia ruchu są przez to niejednorodne, często nielogiczne, a nawet sprzeczne wewnętrznie.

[28] T. Cichocki, *Polki i Polacy – już czas wypowiedzieć posłuszeństwo nielegalnej władzy działającej na naszą szkodę!!! List otwarty*, https://www.tcichocki.pl/20150402_Wypowiedzenie_posluszenstwa_organom_panstwa.pdf [dostęp: 2 IV 2025].

Zwolennicy Zawodowego Polaka wskazują kary za podjęcie wobec nich określonych czynności (rysunek 3). Jest to wymierzone w funkcjonariuszy publicznych (głównie w policjantów), których do takich działań upoważniają ustawy, tj. *Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej* i *Ustawa z dnia 6 kwietnia 1990 r. o Policji*.



Ponadto informuję że:

- Wykorzystanie danych osobowych przez firmy, instytucje i osoby fizyczne wymaga pisemnej zgody kreatorów i właściciela.
- Kara za wykorzystanie danych osobowych bez wykazanej zgody lub uprawnień wynosi 1500000 € za jednorazowe kopiowanie i przetwarzanie.
- Kara za podstępne wydobycie podpisu 5000000 €.
- Kara za dzień pozbawienia mnie wolności wynosi 8000000 €.
- Kara za ignorowanie woli zwierzchnika władzy oraz łamanie praw człowieka wynosi 10000000 €.

Jestem w wieku trzydziestu jeden lat i przy zdrowych zmysłach, tekst powyższy przeczytałem oraz poświadczam że jest zgodny z prawdą i moją wolną wolą... i sygnuję własnoręcznym podpisem.

Rysunek 3. Fragment dokumentu ruchu Zawodowy Polak.

Źródło: D. Bryda, *Deklaracja Samostanowienia i Odpowiedzialności*, Zawodowy Polak, https://www.zawodowy-polak.pl/DB-Deklaracja_12.01.2024r.pdf [dostęp: 25 X 2024].

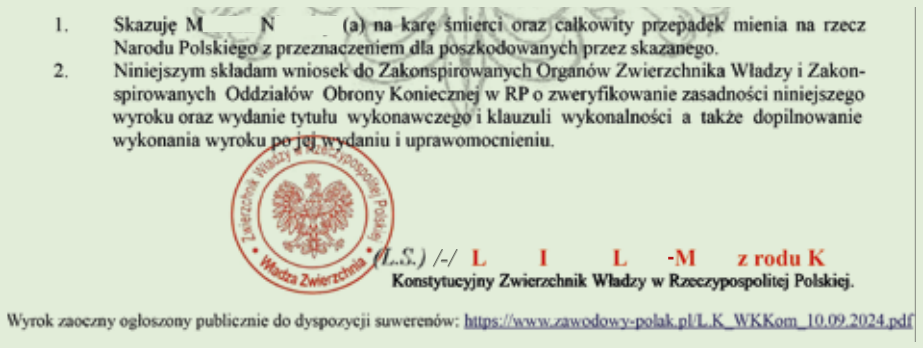
Na kanale YouTube Zawodowy Polak są publikowane treści przedstawiające teorie spiskowe ważne dla ruchu suwerennych obywateli, a także filmy z zarejestrowanymi wizytami zwolenników ruchu w urzędach publicznych, np. Zakładzie Ubezpieczeń Społecznych, urzędach gmin, obwodowych komisjach wyborczych[29]. Pokazywane są również konfrontacje z patrolami policji drogowej, zwykle kończące się podjęciem interwencji wobec zwolennika ruchu zakłócającego pracę funkcjonariuszy bądź prowadzące do zatrzymania lub udzielenia mandatu. Wielokrotnie interwencje policji były tematem filmów tzw. *commentary*, w których twórca odnosi się do innego nagrania. W jednym z przypadków interwencję policji komentował na prywatnym kanale inny policjant[30]. Zwrócił on uwagę m.in. na charakterystyczny język (zwolennik ruchu twierdził, że nie jest kierowcą, lecz człowiekiem). Z uwagi na profesjonalizm policjantów przeprowadzających interwencję oraz zachowanie osoby, wobec której była ona podejmowana, praca policji jest pozytywnie komentowana, a zachowanie zatrzymanego – negatywnie lub żartobliwie. Członkowie ruchu

[29] *Nie można nagrywać najemników i lokalu wyborczego w Kisielsku?*, kanał YouTube Zawodowy Polak, 9 VI 2024 r., https://www.youtube.com/watch?v=8nAon2vpOTQ [dostęp: 15 XII 2024].

[30] *„Nielegalne" zatrzymanie przez Policję i ZAWODOWY POLAK | Bagieta rozkłada interwencje #3*, kanał YouTube Sierżant Bagieta, 26 II 2020 r., https://www.youtube.com/watch?v=EgQWjQEDq_A [dostęp: 1 I 2025].

twierdzą, że działają w imieniu suwerena, czyli narodu polskiego, a swoje działania uzasadniają wywodami prawnymi, które nie znajdują odzwierciedlenia w obowiązujących przepisach. Powołują się przy tym na prawo naturalne, kwestionują legalność organów państwowych, podważają ich autorytet i kompetencje. W praktyce ich aktywność prowadzi do zakłócania pracy urzędów i policji.

Większość zarejestrowanych zachowań zwolenników ruchu można uznać za niegroźne pieniactwo, ale są też materiały o innym charakterze, np. film pt. *Kiedy powinieneś zastrzelić agenta?*. Jest to polskie tłumaczenie amerykańskiego nagrania pt. *When shoud you shoot a cop?*[31]. Radykalizację ruchu widać również na stronie głównej: zawodowy-polak.pl, na której wzywa się zwolenników ruchu do tworzenia (sic!) Zakonspirowanych Trybunałów Narodu Polskiego, które mają wydawać zaoczne wyroki śmierci na (…) *wrogów Rzeczypospolitej Polskiej i ich kolaborantów, w zgodzie z prawem naturalnym, polską racją stanu i własnym sumieniem*[32]. Autorzy apelu wzywają więc do samosądów na urzędnikach państwowych oraz przedstawicielach władzy. W odpowiedzi sympatycy ruchu zaczęli od 2024 r. zamieszczać na stronie zawodowy-polak.pl wyroki skazujące na karę śmierci wrogów poszczególnych członków ruchu. Wykonanie tych wyroków zleca się wspomnianym trybunałom (rysunek 4). Opublikowano np. akt oskarżenia wobec komornika sądowego zawierający groźbę karalną (tj. groźbę zasądzenia i wykonania kary śmierci)[33].


1. Skazuję M N (a) na karę śmierci oraz całkowity przepadek mienia na rzecz Narodu Polskiego z przeznaczeniem dla poszkodowanych przez skazanego.
2. Niniejszym składam wniosek do Zakonspirowanych Organów Zwierzchnika Władzy i Zakonspirowanych Oddziałów Obrony Koniecznej w RP o zweryfikowanie zasadności niniejszego wyroku oraz wydanie tytułu wykonawczego i klauzuli wykonalności a także dopilnowanie wykonania wyroku po jej wydaniu i uprawomocnieniu.

Zwierzchnik Władzy Rzeczypospolitej Polskiej Władza Zwierzchnia

(L.S.) /-/ L I L -M z rodu K
Konstytucyjny Zwierzchnik Władzy w Rzeczypospolitej Polskiej.

Wyrok zaoczny ogłoszony publicznie do dyspozycji suwerenów: https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf

Rysunek 4. Sentencja wyroku wydanego przez członka ruchu Zawodowy Polak.

Źródło: *Wyrok zaoczny w imieniu Zwierzchnika Władzy w Rzeczypospolitej Polskiej*, Zawodowy Polak, 10 IX 2024 r., https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf [dostęp: 25 X 2024]. Anonimizacji dokonał autor artykułu.

[31] *Kiedy powinieneś zastrzelić agenta?*, kanał YouTube Moron3k, https://youtu.be/AJ2HJWhmrdE?si=kbENyPyZmWGeG2_C [dostęp: 14 VII 2025].

[32] T. Cichocki, *Polki i Polacy – już czas*…, s. 10.

[33] T. Berkowska, *Akt oskarżenia*, Zawodowy Polak, https://www.zawodowy-polak.pl/TB_NFKS-MK--Akt_Oskarzenia-27.11.2024.pdf, s. 3 [dostęp: 1 I 2025].

Zarówno polscy, jak i amerykańscy suwerenni obywatele cechują się poglądami ksenofobicznymi. W USA są to głównie poglądy rasistowskie, w Polsce przeważa antysemityzm. Na stronie zawodowy-polak.pl można znaleźć przykład antysemickiego tekstu pt. *Protokoły Mędrców Syjonu*[34].

Ruch II RP

Założycielem Ruchu II RP jest podający się za hrabiego i prezydenta II RP na uchodźstwie Jan Zbigniew Potocki. Zdaniem Potockiego ostatnim legalnym prezydentem rządu II RP na uchodźstwie był Juliusz Nowina-Sokolnicki, a nie Ryszard Kaczorowski, i od niego czerpie pełnomocnictwo do dalszego pełnienia urzędu Prezydenta II RP. Nowina-Sokolnicki, choć mianowany przez Augusta Zaleskiego, był postacią niejednoznaczną, a jego nominacja budziła wątpliwości, m.in. dlatego że nie została oficjalnie ogłoszona w odpowiednich publikatorach. Zaleski wielokrotnie zmieniał swoich następców, co doprowadziło do równoległej działalności różnych ośrodków władzy na emigracji. Jednym z nich była linia Sokolnickiego, drugim – linia uznająca Kaczorowskiego za legalnego prezydenta. Dnia 22 września 1971 r. Zaleski wyznaczył Sokolnickiego na swojego następcę, co oznaczało odwołanie Stanisława Ostrowskiego. Jednak po śmierci Zaleskiego to Ostrowski został uznany za prezydenta przez główne emigracyjne ośrodki polityczne. Mimo to Sokolnicki utrzymywał, że jego nominacja była prawomocna. Doprowadziło to do sytuacji dwuwładzy w środowisku emigracyjnym[35]. Działalność Jana Zbigniewa Potockiego, nawiązująca do prezydentury Nowiny-Sokolnickiego, jest więc kontynuacją podziałów, które mają źródło w latach 70. XX w. Potocki, podobnie jak Sokolnicki, odwołuje się do legalizmu II RP i stara się legitymizować swoją działalność, opierając się na historycznych kontrowersjach wokół sukcesji prezydenckiej na uchodźstwie.

Przykładem jednej z głównych działalności Potockiego jest sprzedaż tzw. dowodów osobistych suwerena II Rzeczypospolitej Polskiej (rysunki 5 i 6).

---

[34] *Protokoły Mędrców Syjonu*, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Protoko%C5%82y_M%C4%99drc%C3%B3w_Syjonu [dostęp: 1 VII 2025].

[35] J. Majchrowski, *Kwestia sukcesji prezydenckiej na obczyźnie*, w: *Myśl polityczna: od historii do współczesności*, B. Stoczewska, M. Jaskólski (red.), Kraków 2000, s. 258, https://ruj.uj.edu.pl/server/api/core/bitstreams/2cc6a415-0de3-4172-bbd2-2cd16fce2235/content [dostęp: 1 I 2025].

Rysunek 5. Awers dowodu osobistego suwerena II Rzeczypospolitej Polskiej.

Źródło: K. Jesionowska, *Dowód osobisty suwerena II Rzeczypospolitej Polskiej*, Straż Graniczna, 3 XII 2021 r., https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II--Rzeczypospolitej-Polskiej.html [dostęp: 25 X 2024].

Rysunek 6. Rewers dowodu osobistego suwerena II Rzeczypospolitej Polskiej.

Źródło: K. Jesionowska, *Dowód osobisty suwerena II Rzeczypospolitej Polskiej*, Straż Graniczna, 3 XII 2021 r., https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II--Rzeczypospolitej-Polskiej.html [dostęp: 25 X 2024].

Chociaż te dokumenty nie są uznawane przez instytucje państwowe, nie widnieją również w międzynarodowych bazach (np. PRADO), to Potocki przekonuje, że posiadanie dowodu suwerena wiąże się z wieloma przywilejami, takimi jak brak obowiązku szczepień dzieci, niepodleganie poborowi wojskowemu (obecnie kwalifikacji wojskowej), niepodleganie egzekucji komorniczej, a także prawu podatkowemu w Polsce. Warto odnotować podobieństwo pod tym względem do

niemieckiego ruchu Reichsbürger (Obywateli Rzeszy), który również posługuje się dokumentami odwołującymi się do nieistniejącego obecnie państwa, a nie do jego aktualnej formy ustrojowej[36]. Potocki planuje wydawanie również metryk urodzenia, praw jazdy i paszportów.

Pisma, jakie Potocki zaleca swoim zwolennikom wysyłać do urzędów publicznych, są podobne do tych z ruchu Zawodowy Polak. Oba ruchy powołują się na niepodleganie prawu jako osoba z krwi i kości, stosują czcionkę w kolorze czerwonym w wybranych fragmentach pisma, twierdzą, że Polska nie jest państwem, lecz firmą zarejestrowaną w Amerykańskiej Komisji Papierów Wartościowych jako POLAND REPUBLIC OF[37]. W rzeczywistości wpis Rzeczypospolitej Polskiej do rejestru Amerykańskiej Komisji Papierów Wartościowych służy umożliwieniu sprzedaży obligacji na rynkach międzynarodowych i nie pociąga za sobą prawnomiędzynarodowych konsekwencji dla statusu RP i nie nadaje Polsce charakteru firmy[38].

W 2024 r. działalność Ruchu II RP przez jakiś czas ucichła ze względu na spory wewnętrzne i osadzenie Potockiego w zakładzie karnym. W 2025 r. jego zwolennicy reaktywowali ruch[39].

Demokracja i Sprawiedliwość oraz Trybunał Narodowy

Demokracja i Sprawiedliwość to jeleniogórskie stowarzyszenie, na którego czele stoi Grzegorz Niedźwiedzki. Sformowało ono ośmioosobowy Najwyższy Trybunał Narodowy[40], który pełni funkcję sądu ludowego. W celu uwierzytelnienia członkowie tego trybunału używają tóg sędziowskich własnego projektu (czarna toga z biało-czerwonym żabotem, lecz w przeciwieństwie do tych używanych przez Trybunał Konstytucyjny żabot ma wzór poziomy, a nie pionowy – zdjęcie 1). Jeden z członków ruchu, określany Prezydentem Wolnej Polski, używa również munduru

---

[36] J. Eichner, *„Reichsdeutsche" fordern bayerische Justiz heraus. Hier ist „deutsches Reichsgebiet"!*, Bayerischer Rundfunk, 23 IV 2016 r., https://www.br.de/nachricht/reichsbuerger-bayern-gerichtsvollzieher-100.html [dostęp: 25 X 2024].

[37] Ta sprawa była nawet przedmiotem interpelacji poselskiej posła Jarosława Sachajki w 2020 r. Zob. *Interpelacja nr 5712 w sprawie zarejestrowania firmy POLAND REPUBLIC OF w rejestrze Amerykańskiej Komisji Papierów Wartościowych*, Sejm RP, https://www.sejm.gov.pl/sejm9.nsf/interpelacja.xsp?typ=INT&nr=5712 [dostęp: 1 VII 2025].

[38] Ł. Starzewski, *Polska zarejestrowana jako firma w USA? RPO prosi MSZ o zbadanie skargi obywatela*, Rzecznik Praw Obywatelskich, 24 II 2020 r., https://www.rpo.gov.pl/pl/content/polska-zarejestrowana-jako-firma-w-usa-rpo-prosi-msz-o-zbadanie-skargi-obywatela [dostęp: 25 X 2024].

[39] W. Ferfecki, *Jan Zbigniew Potocki kontra współpracownicy. Bunt przeciw samozwańczemu prezydentowi*, Rzeczpospolita, 17 V 2024 r., https://www.rp.pl/polityka/art40374471-jan-zbigniew-potocki-kontra-wspolpracownicy-bunt-przeciw-samozwanczemu-prezydentowi [dostęp: 25 X 2024].

[40] *Najwyższy Trybunał Narodowy. Akt ustanowienia*, Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/najwyzszy-trybunal-narodowy/ [dostęp: 21 VII 2025].

Wojska Polskiego z dodanymi dystynkcjami Polskich Drużyn Strzeleckich. Wykorzystuje lukę w prawie, aby zbudować swój wizerunek na autorytecie wojska.

Zdjęcie 1. Posiedzenie Najwyższego Trybunału Narodowego.

Źródło: *Uchwała Najwyższego Trybunału Narodowego o nieważności wyroków w imieniu Rzeczypospolitej Polskiej*, trybunał-narodowy.pl, 13 XI 2024 r., https://www.trybunal-narodowy.pl/uchwala-najwyzszego-trybunalu-narodowego-o-niewaznosci-wyrokow-w-imieniu-rzeczypospolitej-polskiej/ [dostęp: 1 VII 2025]. Anonimizacji dokonał autor artykułu.

W 2021 r. Najwyższy Trybunał Narodowy skazał 24 funkcjonariuszy publicznych (w tym podwójnie wymieniono Zbigniewa Ziobrę jako ówczesnego prokuratora generalnego i ministra sprawiedliwości) na karę 15 lat pozbawienia wolności z obowiązkiem wykonywania prac społecznych, infamię, ostracyzm, pozbawienie prawa do emerytury z tytułu wykonywanego zawodu, pozbawienie praw publicznych, wpłaty 100 000 zł zadośćuczynienia na rzecz pokrzywdzonego, wpłaty 1 mln zł nawiązki na rzecz stowarzyszenia Demokracja i Sprawiedliwość oraz zobowiązał ich do publicznych przeprosin pokrzywdzonego, jako którego wskazano Grzegorza Niedźwiedzkiego.

Dnia 3 maja 2024 r. stowarzyszenie Demokracja i Sprawiedliwość powołało Rząd Wolnej Polski i wydało jego członkom pamiątkowe akty powołania i legitymacje[41]. Nagranie z powołania tego rządu[42] na 1 stycznia 2025 r. miało ok. 2000 odsłon,

[41] *Powołano Rząd Wolnej Polski*, Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/powolano-rzad-wolnej-polski/ [dostęp: 1 VII 2025].

[42] *Powołanie Rządu Wolnej Polski*, kanał YouTube Trybunał Narodowy, https://www.youtube.com/watch?v=1HyXzBXXfOs&t=1s [dostęp: 1 VII 2025].

a kanał na YouTube – 735 subskrybentów. Każdy film opublikowany przez stowarzyszenie ma przeciętnie ok. 800 wyświetleń.

Kolejną jednostką organizacyjną jest Trybunał Narodowy, który ma swoją siedzibę w Jeleniej Górze i jest powiązany personalnie ze stowarzyszeniem Demokracja i Sprawiedliwość. Zgodnie z odpisem KRS zamieszczonym na stronie internetowej trybunal-narodowy.pl jest to związek stowarzyszeń. Trybunał Narodowy w swoich decyzjach odwołuje się m.in. do teorii kukły, twierdząc że państwo nie może sądzić człowieka, a jedynie osoby prawne, w które przekształcono ludzi, oraz rozpowszechnia *Deklaracje Samostanowienia i Odpowiedzialności* ruchu Zawodowy Polak.

Ruch Teresy Garland

Częściowo podobny do ruchu sovereign citizen jest ruch Teresy Garland, która nazywa siebie Prezydentem Elektorskiej RP. Swój tytuł legitymizuje wynikiem samodzielnie zarządzonych i przeprowadzonych wyborów, w ramach których poprosiła zwolenników o przelewy w kwocie 1 zł na jej konto bankowe, z wpisem w tytule przelewu: głos. Zdecydowała się na takie działanie, gdyż nie mogła zebrać 1000 podpisów potrzebnych do zarejestrowania komitetu wyborczego przez Państwową Komisję Wyborczą[43]. Garland powołała również Tymczasową Radę Stanu Narodu Polskiego Społeczny Komitet Konstytucyjny, której jednym z członków jest Piotr Smolana, były poseł Samoobrony[44]. Działalność Teresy Garland polega głównie na wysyłaniu do urzędów gminnych i miejskich w całej Polsce petycji dotyczących m.in. utworzenia lokalnej straży energetycznej, ogłoszenia referendum ludowego[45], poparcia jej tymczasowego rządu, wyposażenia w broń każdego rdzennego mieszkańca Polski[46]. W 2022 r. Garland została zatrzymana przez policję[47],

[43] T. Garland, *24 III 2020 r. PKW TERESA GARLAND zgłoszenie kandydatury po raz trzeci*, Teresa Garland, https://teresagarlandprezydent.wordpress.com/2020/03/24/24-iii-2020r-pkw-teresa-garland-zgloszenie-kandydatury-po-raz-trzeci/ [dostęp: 1 I 2025].

[44] R. Gębuś, *Samozwańczy Rząd Tymczasowej Rady Stanu apeluje o poparcie do lęborskiej rady. Burmistrz powiadamia prokuraturę*, Lębork Nasze Miasto, 19 IV 2021 r., https://lebork.naszemiasto.pl/samozwanczy-rzad-tymczasowej-rady-stanu-apeluje-o-poparcie/ar/c15-8238215 [dostęp: 1 I 2025].

[45] *Samozwańcza prezydent sypnęła petycjami*, Super Tydzień Chełmski, 15 IV 2021 r., https://www.supertydzien.pl/artykul/10406,samozwancza-prezydent-sypnela-petycjami [dostęp: 1 I 2025].

[46] J. Sidorowicz, *Broń od gminy dla każdego rdzennego mieszkańca Starego Sącza? Jest petycja w sprawie programu „Broń palna plus"*, Kraków.Wyborcza.pl, 26 IX 2022 r., https://krakow.wyborcza.pl/krakow/7,44425,28955388,bron-od-gminy-dla-kazdego-rdzennego-mieszkanca-starego-sacza.html [dostęp: 1 I 2025].

[47] Ośrodek Monitorowania Zachowań Rasistowskich i Ksenofobicznych, *Teresa Garland będąca prorosyjską patocelebrytką w końcu zatrzymana przez policję*, Facebook, 28 IX 2022 r., https://www.facebook.com/osrodek.monitorowania/posts/teresa-garland-b%C4%99d%C4%85ca-

a Sąd Rejonowy w Wieliczce skierował ją na badania psychiatryczne[48]. Warto zauważyć, że wraz z zaostrzeniem konfliktu Garland z państwem polskim zaczęła ona używać coraz więcej sformułowań i postulatów charakterystycznych dla ruchu sovereign citizen, np. obywatel-suweren, osoba z krwi i kości, podważanie legalności sądu jako instytucji państwa. Na podstawie liczby subskrybentów kanału na YouTube @prezydentelektorski na 1 stycznia 2025 r. popularność ruchu Teresy Garland można szacować na ok. 660 osób. Ostatni film, z kwietnia 2024 r., ma ok. 800 wyświetleń. Teresa Garland komunikuje się ze swoimi zwolennikami za pośrednictwem bloga i profili na portalach vk.com (nagranie z grudnia 2024 r. według stanu na 1 stycznia 2025 r. ma 16 wyświetleń) czy gloria.tv.

Inni przedstawiciele ruchu sovereign citizen w Polsce

W Polsce działają również inne osoby i grupy tworzące alternatywne władze państwowe, np. Wojciech Edward Leszczyński – Leh XVII[49], Włodzimierz Julian Korab-Karpowicz – Prezydent RP *in spe*[50], Marek Świętopełk-Zawadzki[51], Mariusz Max Kolonko – Prezydent *ad interim* Stanów Zjednoczonych Polski[52]. Osoby te (z wyjątkiem Mariusza Kolonki) nawiązują do ruchów monarchistycznych, tworzą własne dokumenty altpaństwowe. Autor pominął ich działalność w tym artykule ze względu na mniejszą popularność i brak jednoznacznych nawiązań do ruchu sovereign citizen. Warto jednak obserwować aktywność tych osób z uwagi na potencjalny wzrost ich znaczenia w środowisku sovereign citizen, spowodowany np. zaprzestaniem lub zawieszeniem działalności przez popularniejsze ruchy.

---

prorosyjsk%C4%85-patocelebrytk%C4%85-w-ko%C5%84cu-zatrzymana-przez-policj/1917138658461258/ [dostęp: 1 I 2025].

[48] T. Garland, *Sprzeciw i apelacja na wyrok z dnia 12 X 2023r. o sygn. akt IIK 451/21 w Sądzie Rejonowym w Wieliczce*, Tymczasowa Rada Stanu, https://tymczasowaradastanu.wordpress.com/2023/11/24/teresa-garland-sprzeciw-i-apelacja-na-wyrok-z-dnia-12-x-2023r-o-sygn-akt-iik-451-21-w-sadzie-rejonowym-w-wieliczce/ [dostęp: 1 I 2025].

[49] W. Ferfecki, *Samozwańczy król Polski z darmowymi spotami w TVP*, Rzeczpospolita, 13 IX 2023 r., https://www.rp.pl/polityka/art39102811-samozwanczy-krol-polski-z-darmowymi-spotami-w-tvp [dostęp: 1 VII 2025].

[50] W. Ferfecki, *Filozof ogłosił się głową państwa*, Rzeczpospolita, 6 VIII 2020 r., https://www.rp.pl/polityka/art8857531-filozof-oglosil-sie-glowa-panstwa [dostęp: 1 VII 2025].

[51] J. Zaremba, *„Leczył" z zaburzeń psychicznych i masturbacji. „Książę" Świętopełk-Zawadzki na Narodowym Marszu Papieskim*, Gazeta.pl, 3 IV 2023 r., https://kobieta.gazeta.pl/kobieta/7,107881,29626596,leczyl-z-zabrzen-psychicznych-i-homoseksualizmu.html [dostęp: 1 VII 2025].

[52] G. Sajór, *Nie wytrzymał ciśnienia. Mariusz Max Kolonko po odejściu z dziennikarstwa został Prezydentem*, Press, 20 V 2022 r., https://www.press.pl/tresc/70879,[na-weekend]-nie-wytrzymal-cisnienia_--mariusz-max-kolonko-po-odejsciu-z-dziennikarstwa-zostal-presidentem [dostęp: 1 VII 2025].

Implikacje dla sektora finansowego (szczególnie bankowego)

Osoby utożsamiające się z ruchem Zawodowy Polak negują istnienie i legalność nie tylko instytucji rządowych, w tym policji i samorządowych, lecz także firm prywatnych z sektora bankowego i instytucji finansowych. Przykładem takich działań mogą być opublikowane na portalu ruchu Zawodowy Polak pisma skierowane do Ubezpieczeniowego Funduszu Gwarancyjnego oraz Santander Bank Polska S.A. W piśmie do Santander Bank[53] (określanym przez zwolenników ruchu jako Nielegalnie Funkcjonujący SANTANDER BANK POLSKA S.A., NFSBP S.A.) Beata Koźlik neguje możliwość domagania się przez bank spłaty zaciągniętego przez nią kredytu i przekazania go do windykacji przez podmiot zewnętrzny, a także zarzuca bankowi stosowanie tzw. klauzul abuzywnych. Na tę ostatnią okoliczność przedstawia dowody, którymi mają być brak odpowiedzi od dyrektora oddziału i prezesa banku, brak odpowiedzi od menadżera zespołu banku i rzecznika klienta, celowe wprowadzanie w błąd i manipulację przez udzielanie odpowiedzi naprzemiennie przez dwie osoby reprezentujące bank, a niebędące dokładnym adresatem korespondencji, a także (…) *brak wykazania niepodważalnych, udokumentowanych dowodów legalnych uprawnień*[54]. Metody stosowane przez ruch wobec podmiotów prywatnych są więc podobne do tych stosowanych wobec instytucji państwowych. Ponieważ sektor bankowy jest częścią infrastruktury krytycznej państwa[55], takie działania są szkodliwe nie tylko z punktu widzenia banku jako instytucji prywatnej, lecz także państwa.

Z kolei w piśmie do Ubezpieczeniowego Funduszu Gwarancyjnego (UFG) Arkadiusz Bosa kwestionuje legalność UFG oraz podważa status prawny przedstawicieli Funduszu. Nadawca pisma zarzuca UFG działanie na szkodę państwa i obywateli, przy czym powołuje się na brak udokumentowanych mandatów społecznych oraz zgodności z konstytucją. Żąda wykazania legalności uprawnień przedstawicieli UFG oraz wzywa do zaprzestania nielegalnych działań pod groźbą konsekwencji prawnych[56].

Na YouTube można znaleźć również nagrania, na których widać, jak Teresa Garland zakłóca konferencję z udziałem prezesa Narodowego Banku Polskiego

---

[53] B. Koźlik, *Doręczenie odpisu postanowienia zwierzchnika władzy w Rzeczypospolitej Polskiej*, Zawodowy Polak, 27 VI 2022 r., https://zawodowy-polak.pl/BK-ost_postanowienie_bank_27.06.2022.pdf [dostęp: 1 I 2025].

[54] Tamże.

[55] K. Piękoś, *Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków*, „Krakowskie Studia Małopolskie" 2017, nr 22, s. 106–113; *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

[56] A. Bosa, *Decyzja Zwierzchnika Władzy w Rzeczypospolitej Polskiej od której nie przysługuje zażalenie*, Zawodowy Polak, 13 VIII 2023 r., https://www.zawodowy-polak.pl/AB-NFUFG_13.08.2023.pdf [dostęp: 1 I 2025].

Adama Glapińskiego, a następnie zbliża się do niego na niebezpieczną odległość[57]. W kontekście zamachów na przedstawicieli sektora finansowego[58], a także bankowości centralnej[59] warto podkreślić, że dopuszczenie tak blisko członków ruchów antypaństwowych skrajnie krytycznych wobec jakiejkolwiek polityki monetarnej państwa jest nieodpowiedzialne i stanowi niedopatrzenie w zakresie ochrony prezesa NBP. Potencjalny zamach na osobę pełniącą tę funkcję to zagrożenie dla stabilności polityki pieniężnej[60]. Należy zauważyć, że zgodnie z *Ustawą z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa* prezes NBP nie jest podmiotem wymienionym w ustawie *per se*, mógłby natomiast być chroniony przez SOP na podstawie decyzji Prezesa Rady Ministrów.

Z uwagi na amerykańskie źródła ruchu warto zwrócić uwagę na przyjęte tam rozwiązania i metody postępowania wobec zwolenników ruchu sovereign citizen[61]. Może to stanowić punkt odniesienia dla polskich instytucji publicznych i sektora bankowego. W Stanach Zjednoczonych instytucje finansowe i sądy przyjęły zdecydowaną politykę wobec prób spłaty długów za pomocą tzw. fałszywych instrumentów finansowych, takich jak fikcyjne obligacje czy kupony emisyjne. Są one uznawane za nieważne i nie podlegają egzekucji. Amerykańskie sądy wielokrotnie wskazywały na bezzasadność argumentów przywoływanych przez członków ruchu. Określały je jako prawnie nieuzasadnione, co skutkowało ich natychmiastowym odrzuceniem bez potrzeby prowadzenia dalszego postępowania. Instytucje bankowe w USA są instruowane, jak postępować w sytuacji, gdy klient próbuje stosować praktyki, takie jak odwoływanie się do nieistniejącego konta w Departamencie Skarbu USA (United States Department of the Treasury), powoływanie się na nieadekwatne przepisy Kodeksu Handlowego (Uniform Commercial Code) lub żądanie anonimizacji swoich danych, w tym numeru ubezpieczenia społecznego. W takich przypadkach banki są zachęcane do pisemnego odrzucania takich żądań i informowania klientów o ich zobowiązaniach zgodnych z obowiązującymi umowami, a w niektórych przypadkach

---

[57] *Prezes NBP Glapiński, Teresa Garland i demokracja*, kanał YouTube Fides Polska TV, 16 XI 2018 r., https://www.youtube.com/watch?v=j1Bd4ZToToE [dostęp: 1 I 2025].

[58] J. Bielecki, *Amerykanie mają dość ubezpieczycieli*, Rzeczpospolita, 11 XII 2024 r., https://www.rp.pl/przestepczosc/art41568761-amerykanie-maja-dosc-ubezpieczycieli [dostęp: 1 VII 2025].

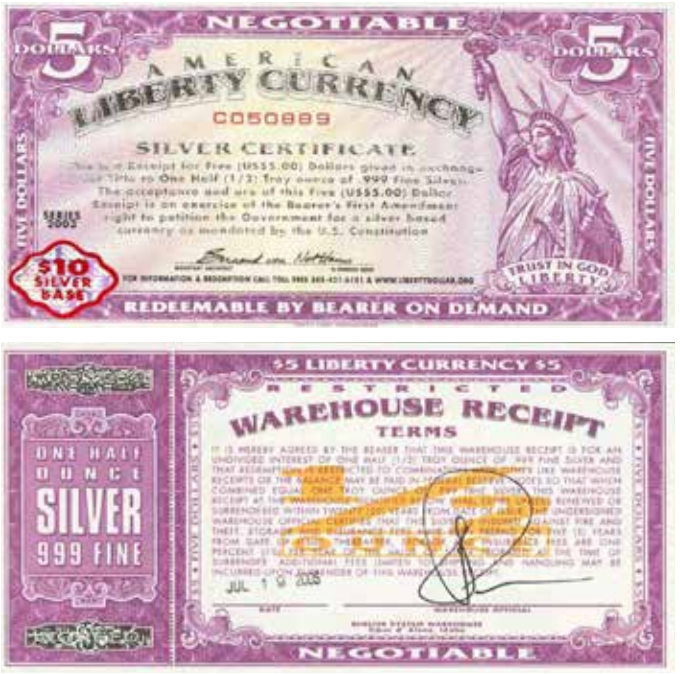
[59] *Top Russian central banker shot to death*, NBC News, 14 IX 2006 r., https://www.nbcnews.com/id/wbna14826889 [dostęp: 1 VII 2025].

[60] P. Król, *Analiza zamachów na osoby publiczne — skuteczność działań prewencyjnych służb bezpieczeństwa i konsekwencje polityczno-społeczne*, „Kwartalnik Kadry Kierowniczej Policji" 2024, nr 3, https://kwartalnik.akademiapolicji.edu.pl/images/stories/2024/3/krl.pdf [dostęp: 1 VII 2025].

[61] D. Spungen, *How Financial Institutions Should Handle „Sovereign Citizens"*, Amundsen Davis, 18 III 2024 r., https://www.amundsendavislaw.com/banking-brief-financial-services-insights/how-financial-institutions-should-handle-sovereign-citizens [dostęp: 1 I 2025].

mogą rozważyć zamknięcie konta klienta, jeśli przepisy prawa i warunki kontraktowe na to pozwalają. Amerykańskie doświadczenia pokazują, że kluczowym elementem w walce z ruchem sovereign citizen jest edukacja pracowników instytucji finansowych i administracyjnych w zakresie rozpoznawania cech charakterystycznych dla suwerennych obywateli.

Przyczynkiem do takiej polityki stała się m.in. sprawa prywatnej waluty produkowanej przez Bernarda von NotHausa o nazwie Liberty Dollar (ALD). Miała ona postać zarówno monet, jak i banknotów-certyfikatów (rysunek 8). Wartość Liberty Dollars odpowiadała odpowiedniej ilości złota lub srebra, na które można je było wymienić[62]. Działania te wzbudziły niepokój Rezerwy Federalnej (Federal Reserve System, FED) oraz Mennicy Stanów Zjednoczonych (United States Mint), które zaczęły postrzegać ten ruch jako zagrożenie dla stabilności systemu monetarnego i finansowego USA.



Rysunek 8. Przykładowy banknot Liberty Dollar – awers i rewers.

Źródło: Silver Certificates, NORFED Liberty Dollar, https://norfed.info/silver-certificates/ [dostęp: 1 I 2025].

[62] L.H. White, *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold*, „The Cato Journal" 2014, t. 34, nr 2, s. 281–301. http://dx.doi.org/10.2139/ssrn.2406983.

Długoletni spór, w którym organizacja emitująca Liberty Dollars przytaczała różne argumenty, m.in. związane z jedynie numizmatycznym charakterem ALD, zakończył się oskarżeniem i aresztowaniem Bernarda von NotHausa i trzech innych osób. NotHaus został skazany w marcu 2011 r. za produkowanie, posiadanie i sprzedaż własnych monet. Groziło mu nawet 15 lat więzienia oraz grzywna w wysokości 250 000 dolarów. Ponadto rząd mógł zająć majątek w postaci monet oraz metali szlachetnych wart 7 mln dolarów[63]. Ostatecznie skazano go na sześć miesięcy aresztu domowego z trzyletnim okresem próbnym. Na wniosek kuratora zwolniono go z okresu próbnego po roku.

Władze federalne określiły działalność organizacji emitującej Liberty Dollars jako próbę podważenia oficjalnej waluty USA i porównały ją do formy terrorystycznej działalności wewnętrznej, która może zaszkodzić stabilności gospodarczej kraju. Choć historycznie system wolnej bankowości (tj. bez monopolu banku centralnego na emisję pieniądza) charakteryzował się stabilnością, to dziś nie jest on rozwiązaniem problemów rynku finansowego, gdyż bankowość centralna to obecnie część polityki gospodarczej państwa, zwłaszcza jej funkcji stabilizacyjnej[64].

Sprzeciw władz USA wobec prób podważania autorytetu państwa i instytucji finansowych może być inspiracją do przyjęcia podobnej postawy w Polsce. W ten sposób jest możliwe ograniczanie wpływu ruchów antypaństwowych i minimalizacja zagrożeń, jakie mogą one wywołać dla stabilności finansowej państwa.

Podsumowanie i rekomendacje

Autor omówił rozwój, działalność oraz społeczne i prawne konsekwencje ruchów antypaństwowych w Polsce, których ideologia i metody działania są inspirowane amerykańskim ruchem sovereign citizen.

Kontakt przedstawicieli instytucji państwowych z członkami ruchu jest utrudniony ze względu na posługiwanie się przez nich specyficznym systemem pseudoprawnym, w którym są wypaczone podstawowe definicje prawne i administracyjne, a normy prawne stosowane wybiórczo i instrumentalnie. Przykładowo, członek ruchu neguje uprawnienia Policji wynikające z ustawy o Policji czy legalność władzy gminy, powołując się na *Ustawę z dnia 8 marca 1990 r. o samorządzie gminnym*,

[63] P.C. Mullan, *The Liberty Dollar and Bernard von NotHaus*, w: *A History of Digital Currency in the United States. New Technology in an Unregulated Market*, New York 2016, s. 87–109. http://dx.doi.org/10.1057/978-1-137-56870-0_3.

[64] P. Marszałek, *Rynek czy państwo w bankowości – bankowość centralna versus bankowość wolna*, „Ryzyko i Zrównoważony Rozwój" 2011, nr 70, s. 125–136.

by następnie powoływać się na ogólne rozporządzenie o ochronie danych[65] jako podstawę do żądania milionowych odszkodowań od policjantów podejmujących interwencję. Członkowie ruchu kwestionują też legalność decyzji organów państwowych i odmawiają uznawania dokumentów urzędowych, mandatów czy wezwań sądowych. Składają bezpodstawne skargi i zażalenia, do czego wykorzystują formalne procedury jako narzędzie destabilizacji instytucji publicznych i przeciążenia systemu administracyjnego. Podejmują również próby zakładania struktur quasi-państwowych, takich jak trybunały narodowe czy sądy obywatelskie, które wydają bezskuteczne prawnie wyroki. Tego rodzaju inicjatywy prowadzą do konfliktów z funkcjonariuszami publicznymi, które nierzadko kończą się aktami agresji słownej, a w skrajnych przypadkach – groźbami czy próbami zastraszania ze strony suwerennych obywateli.

Analiza tzw. pseudoprawnych technik, z których korzystają zwolennicy ruchów suwerennościowych zarówno w USA, jak i w Polsce, wykazała, że należy je traktować jako próbę zastraszania przedstawicieli instytucji państwowych. Ruch Zawodowy Polak posunął się nawet do publikacji wyroków śmierci na „zdrajców narodu". Takie działania i inne, np. propagowanie teorii spiskowych oraz zachęcanie do unikania odpowiedzialności prawnej, służą radykalizacji członków ruchu sovereign citizen w Polsce[66].

Ruch suwerennych obywateli w Polsce adaptuje amerykańskie wzorce, które dostosowuje do lokalnych realiów i specyfiki systemu prawnego, np. używanie pieczęci, podpisów w czerwonym atramencie czy też argumentacji bazującej na rzekomej podwójnej tożsamości obywatela jako osoby fizycznej i prawnej. Działania ruchu stanowią wyzwanie dla administracji publicznej oraz sektora bankowego, w który coraz częściej są one wymierzone. Polskie instytucje powinny rozważyć wdrożenie procedur wzorowanych na amerykańskich rozwiązaniach, takich jak:

- szkolenia pracowników w zakresie rozpoznawania charakterystycznych zachowań przedstawicieli ruchu i jego dokumentów,
- jednoznaczne odrzucanie pseudoprawnych roszczeń,
- konsekwentne reagowanie na wszelkie próby destabilizacji porządku publicznego.

[65] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*).

[66] B. Łódzki, *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej*, „Polityka i Społeczeństwo" 2017, t. 15, nr 4, s. 19–30. https://doi.org/10.15584/polispol.2017.4.2.

Edukacja urzędników publicznych

W Polsce urzędnicy zazwyczaj nie są odpowiednio przeszkoleni, aby skutecznie i zrozumiale objaśniać teorię prawa osobom, które próbują zakwestionować porządek prawny za pomocą pseudoprawnych pism. Obarczeni dużą liczbą spraw nie mają czasu na polemikę i rozbudowane tłumaczenia. Zdaniem autora może to powodować wzrost frustracji u osób identyfikujących się z ruchem suwerennych obywateli, których pytania o legalność władzy pozostają bez wyczerpującej odpowiedzi. Rozwiązaniem mogłoby być stworzenie poradnika dla pracowników administracji publicznej, podobnego do broszur wydawanych w Stanach Zjednoczonych[67], zawierających informacje o metodach i manipulacjach stosowanych przez zwolenników ruchu sovereign citizen, przykłady postępowania z nimi i wzory odpowiedzi na ich pisma kierowane do instytucji publicznych. Polski dokument tego typu mógłby zawierać wytyczne dotyczące postępowania wobec petentów posługujących się pseudoprawnymi argumentami oraz instrukcję postępowania w przypadku, gdy zakłócają oni pracę urzędu. Tego typu instrukcje nie tylko poprawiłyby jakość obsługi, lecz także mogłyby przyczynić się do sprawniejszego reagowania na próby destabilizacji działalności urzędów.

Problem braku skutecznych form odpowiedzi na działania polskich ruchów sovereign citizen wobec urzędów zauważa Bartosz Mendyk. Autor pochyla się nad problemem kolportowania przez Teresę Garland petycji, w których odwołuje się ona do teorii spiskowych, szerzy prorosyjską propagandę i używa mowy nienawiści wobec Żydów i Ukraińców[68]. Mendyk zwraca uwagę nie tylko na problematyczne do rozpatrzenia – z perspektywy urzędników – petycje, które zawierają żądania nieodnoszące się do potrzeb lokalnych wspólnot, lecz także na kwestię obowiązku publikacji takich petycji w Biuletynie Informacji Publicznej. W ten sposób materiały ruchu – w tym przypadku Teresy Garland – stają się bardziej dostępne. Mendyk zauważa, że pisma Teresy Garland nie spełniają przesłanek zawartych w *Ustawie z dnia 11 lipca 2014 r. o petycjach*, stanowią nadużycie prawa do petycji, a organ administracji publicznej może w takim wypadku stwierdzić takie nadużycie i pozostawić petycję bez rozpatrzenia i publikacji. Warto podkreślić, że instytucje państwowe i samorządowe, (…) *które w związku ze swą działalnością dowiedziały się*

[67] M. Crowell, *A Quick Guide to Sovereign Citizens*, „Administration of Justice Bulletin" 2015, nr 4, https://www.sog.unc.edu/sites/default/files/reports/aojb1504.pdf [dostęp: 1 VII 2025]; *A Quick Guide to Sovereign Citizens*, UNC School of Government, November 2013, https://www.sog.unc.edu/sites/www.sog.unc.edu/files/Sov%20citizens%20quick%20guide%20Nov%2013.pdf [dostęp: 1 I 2025].

[68] B. Mendyk, *Jak reagować na petycje pełne teorii spiskowych?*, Pismo Samorządu Terytorialnego „Wspólnota", 3 IV 2024 r., https://wspolnota.org.pl/newsletter/jak-reagowac-na-petycje-pelne-teorii-spiskowych [dostęp: 1 I 2025].

o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa[69].

Wprowadzenie przepisów ograniczających tzw. pieniactwo urzędowe

Ważnym aspektem omawianej problematyki jest zjawisko tzw. pieniactwa urzędowego. Należy przez to rozumieć składanie licznych bezzasadnych skarg czy pism, których celem jest przedłużenie postępowania lub zakłócenie pracy administracji. W literaturze zostało opisane dotychczas zjawisko pieniactwa sądowego[70]. Lech Jamróz podkreśla, że prawo do sądu nie jest absolutne i można je ograniczać w przypadku działań obstrukcyjnych lub złośliwych. Analogicznie można by podejść do pieniactwa urzędowego, które ma na celu sabotowanie pracy administracji publicznej. Obecnie prawo umożliwia penalizację zachowań zakłócających porządek publiczny na mocy art. 51 Kodeksu wykroczeń, jednak warto rozważyć, czy potrzebne są dodatkowe przepisy, które umożliwiłyby skuteczniejsze ograniczenie takich działań, zwłaszcza w przypadkach uporczywego lub zorganizowanego pieniactwa.

Regulacje w zakresie stosowania imitacji symboli państwowych i gróźb wobec instytucji

Polskie prawo nie przewiduje kary za tworzenie grafik imitujących pieczęcie państwowe, o ile różnią się one od obowiązujących choć jednym elementem. To umożliwia ruchowi suwerennych obywateli posługiwanie się grafikami, które dla postronnych obserwatorów mogą wyglądać na pieczęcie urzędowe. Przykładem jest stosowanie pieczęci fikcyjnych organów, historycznych insygniów państwowych lub nazw dawnych struktur państwa, co może wprowadzać w błąd zarówno obywateli, jak i pracowników urzędów. Aby ograniczyć potencjalne nadużycia w tym zakresie, ustawodawca mógłby wprowadzić przepisy regulujące użycie symboli i grafik łudząco podobnych do oficjalnych pieczęci i dokumentów.

Podsumowując, artykuł ukazuje zagrożenia, jakie ruchy inspirujące się amerykańskim ruchem sovereign citizen mogą wywołać dla porządku prawnego i bezpieczeństwa publicznego w Polsce. Skuteczna odpowiedź na działania suwerennych

---

[69] Art. 304 § 2 *Ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego*.

[70] L. Jamróz, *Prawo do sądu a zjawisko pieniactwa sądowego*, w: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (red.), Wrocław 2018, s. 495–504, https://repozytorium.uni.wroc.pl/dlibra/publication/95758/edition/89860/prawo-do-sadu-a-zjawisko-pieniactwa-sadowego-jamroz-lech [dostęp: 18 X 2024].

obywateli wymaga współpracy sektora publicznego i prywatnego, a także podjęcia działań edukacyjnych i legislacyjnych, mających na celu ograniczenie rozprzestrzeniania się tego rodzaju ideologii.

Bibliografia

Challacombe D.J, Lucas P.A., *Postdicting violence with sovereign citizen actors: An exploratory test of the TRAP-18*, „Journal of Threat Assessment and Management" 2019, t. 6, nr 1, s. 51–59. https://doi.org/10.1037/tam0000105.

Łódzki B., *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej*, „Polityka i Społeczeństwo" 2017, t. 15, nr 4, s. 19–30. https://doi.org/10.15584/polispol.2017.4.2.

Marszałek P., *Rynek czy państwo w bankowości – bankowość centralna versus bankowość wolna*, „Ryzyko i Zrównoważony Rozwój" 2011, nr 70, s. 125–136.

Matheson C.L., *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*, „Rhetoric Society Quarterly" 2018, t. 2, nr 48, s. 187–206.

Morozov A., Bruinsma R., Rudnick J., *Assembly of viruses and the pseudo law of mass action*, „Biophysical Journal" 2009, t. 96, nr 3, s. 419a–420a.

Mullan P.C., *The Liberty Dollar and Bernard von NotHaus*, w: *A History of Digital Currency in the United States. New Technology in an Unregulated Market*, New York 2016, s. 87–109. http://dx.doi.org/10.1057/978-1-137-56870-0_3.

Piękoś K., *Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków*, „Krakowskie Studia Małopolskie" 2017, nr 22, s. 106–113.

Sarteschi Ch.M., *Sovereign Citizens and QAnon: The Increasing Overlaps with a Focus on Child Protective Service (CPS) Cases*, „International Journal of Coercion, Abuse & Manipulation" 2023, t. 6. https://doi.org/10.54208/1000/0006/006.

White L.H., *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold*, „The Cato Journal" 2014, t. 34, nr 2, s. 281–301. http://dx.doi.org/10.2139/ssrn.2406983.

Źródła internetowe

Akt oskarżenia z dnia 4 XI 2024 r., Zawodowy Polak, https://www.zawodowy-polak.pl/KC--Akt_Oskarzenia-NFPR-4.11.2024.pdf [dostęp: 14 VII 2025].

A Quick Guide to Sovereign Citizens, UNC School of Government, November 2013, https://www.sog.unc.edu/sites/www.sog.unc.edu/files/Sov%20citizens%20quick%20guide%20Nov%2013.pdf [dostęp: 1 I 2025].

Berkowska T., *Akt oskarżenia*, Zawodowy Polak, https://www.zawodowy-polak.pl/TB_NF-KS-MK-Akt_Oskarzenia-27.11.2024.pdf [dostęp: 1 I 2025].

Bielecki J., *Amerykanie mają dość ubezpieczycieli*, Rzeczpospolita, 11 XII 2024 r., https://www.rp.pl/przestepczosc/art41568761-amerykanie-maja-dosc-ubezpieczycieli [dostęp: 1 VII 2025].

Bosa A., *Decyzja Zwierzchnika Władzy w Rzeczypospolitej Polskiej od której nie przysługuje zażalenie*, Zawodowy Polak, 13 VIII 2023 r., https://www.zawodowy-polak.pl/AB-NFUFG_13.08.2023.pdf [dostęp: 1 I 2025].

Bryda D., *Deklaracja Samostanowienia i Odpowiedzialności*, Zawodowy Polak, 12 I 2024 r., https://www.zawodowy-polak.pl/DB-Deklaracja_12.01.2024r.pdf [dostęp: 25 X 2024].

Cichocki T., *Dekret Zwierzchnika Władzy w Rzeczypospolitej Polskiej 1-2018*, Piaseczno, 25 X 2018 r., https://www.tcichocki.pl/Dekret%20Zwierzchnika%20W%C5%82adzy%20w%20RP%201-2018%202018.10.25.pdf [dostęp: 25 X 2024].

Cichocki T., *Polki i Polacy – już czas wypowiedzieć posłuszeństwo nielegalnej władzy działającej na naszą szkodę!!! List otwarty*, https://www.tcichocki.pl/20150402_Wypowiedzenie_posluszenstwa_organom_panstwa.pdf [dostęp: 2 IV 2025].

Crowell M., *A Quick Guide to Sovereign Citizens*, „Administration of Justice Bulletin" 2015, nr 4, https://www.sog.unc.edu/sites/default/files/reports/aojb1504.pdf [dostęp: 1 VII 2025].

Deklaracja Samostanowienia i Odpowiedzialności, Zawodowy Polak, https://www.zawodowy-polak.pl/index.php?title=Deklaracja_Samostanowienia_i_Odpowiedzialno%C5%9Bci [dostęp: 15 XII 2024].

Eichner J., *„Reichsdeutsche" fordern bayerische Justiz heraus. Hier ist „deutsches Reichsgebiet"!*, Bayerischer Rundfunk, 23 IV 2016 r., https://www.br.de/nachricht/reichsbuerger-bayern-gerichtsvollzieher-100.html [dostęp: 25 X 2024].

FBI, *Domestic terrorism. The Sovereign Citizen Movement*, 13 IV 2010 r., https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement [dostęp: 15 XII 2024].

FBI's Counterterrorism Analysis Section, *Sovereign Citizens. A Growing Domestic Threat to Law Enforcement*, FBI Law Enforcement Bulletin, 1 IX 2011 r., https://leb.fbi.gov/articles/featured-articles/sovereign-citizens-a-growing-domestic-threat-to-law-enforcement [dostęp: 1 I 2025].

Ferfecki W., *Filozof ogłosił się głową państwa*, Rzeczpospolita, 6 VIII 2020 r., https://www.rp.pl/polityka/art8857531-filozof-oglosil-sie-glowa-panstwa [dostęp: 1 VII 2025].

Ferfecki W., *Jan Zbigniew Potocki kontra współpracownicy. Bunt przeciw samozwańczemu prezydentowi*, Rzeczpospolita, 17 V 2024 r., https://www.rp.pl/polityka/art40374471-jan-zbigniew-potocki-kontra-wspolpracownicy-bunt-przeciw-samozwanczemu-prezydentowi [dostęp: 25 X 2024].

Ferfecki W., *Samozwańczy król Polski z darmowymi spotami w TVP*, Rzeczpospolita, 13 IX 2023 r., https://www.rp.pl/polityka/art39102811-samozwanczy-krol-polski-z-darmowymi-spotami-w-tvp [dostęp: 1 VII 2025].

Garland T., *24 III 2020 r. PKW TERESA GARLAND zgłoszenie kandydatury po raz trzeci*, Teresa Garland, https://teresagarlandprezydent.wordpress.com/2020/03/24/24-iii-2020r-p-kw-teresa-garland-zgloszenie-kandydatury-po-raz-trzeci/ [dostęp: 1 I 2025].

Garland T., *Sprzeciw i apelacja na wyrok z dnia 12 X 2023r. o sygn. akt IIK 451/21 w Sądzie Rejonowym w Wieliczce*, Tymczasowa Rada Stanu, https://tymczasowaradastanu.wordpress.com/2023/11/24/teresa-garland-sprzeciw-i-apelacja-na-wyrok-z-dnia-12-x-2023r-o-sygn-akt-iik-451-21-w-sadzie-rejonowym-w-wieliczce/ [dostęp: 1 I 2025].

Gębuś R., *Samozwańczy Rząd Tymczasowej Rady Stanu apeluje o poparcie do lęborskiej rady. Burmistrz powiadamia prokuraturę*, Lębork Nasze Miasto, 19 IV 2021 r., https://lebork.naszemiasto.pl/samozwanczy-rzad-tymczasowej-rady-stanu-apeluje-o-poparcie/ar/c15-8238215 [dostęp: 1 I 2025].

Interpelacja nr 5712 w sprawie zarejestrowania firmy POLAND REPUBLIC OF w rejestrze Amerykańskiej Komisji Papierów Wartościowych, Sejm RP, https://www.sejm.gov.pl/sejm9.nsf/interpelacja.xsp?typ=INT&nr=5712 [dostęp: 1 VII 2025].

IRS Criminal Investigation, *Sovereign citizen sentenced to 9 years in prison for $3.4 million tax fraud scheme, filing a false lien, and absconding while on bond*, Press Release, 22 V 2024 r., https://www.irs.gov/compliance/criminal-investigation/sovereign-citizen-sentenced-to-9-years-in-prison-for-3-point-4-million-tax-fraud-scheme-filing-a-false-lien-and-absconding-while-on-bond [dostęp: 1 VII 2025].

Jamróz L., *Prawo do sądu a zjawisko pieniactwa sądowego*, w: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (red.), Wrocław 2018, s. 495–504, https://repozytorium.uni.wroc.pl/dlibra/publication/95758/edition/89860/prawo-do-sadu-a-zjawisko-pieniactwa-sadowego-jamroz-lech [dostęp: 18 X 2024].

Jesionowska K., *Dowód osobisty suwerena II Rzeczypospolitej Polskiej*, Straż Graniczna, 3 XII 2021 r., https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II-Rzeczypospolitej-Polskiej.html [dostęp: 25 X 2024].

Kalinowski IV C., *A Legal Response to the Sovereign Citizen Movement*, „Montana Law Review" 2019, t. 80, nr 2, s. 153–210, https://scholarworks.umt.edu/mlr/vol80/iss2/2/ [dostęp: 25 X 2024].

Kelley B.J., *Interview with a sovereign: Judge Anna's World*, Southern Poverty Law Center, 15 XII 2017 r., https://www.splcenter.org/hatewatch/2017/12/15/interview-sovereign-judge-anna%E2%80%99s-world [dostęp: 1 I 2025].

Kent S.A., *Freemen, Sovereign Citizens, and the Challenge to Public Order in British Heritage Countries*, „International Journal of Cultic Studies" 2015, nr 6, https://skent.ualberta.ca/wp-content/uploads/2015/06/Freemen-Internl-J-of-Cultic-Studies.pdf, s. 1–15 [dostęp: 25 X 2024].

Kiedy powinieneś zastrzelić agenta?, kanał YouTube Moron3k, https://youtu.be/AJ2HJ-WhmrdE?si=kbENyPyZmWGeG2_C [dostęp: 14 VII 2025].

IV Konwencja Genewska, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=IV_Konwencja_Genewska [dostęp: 1 I 2025].

Koppelman Ch., *Construction as Resistance. Constructing a desired and envisioned future to perceived oppression for the sovereign citizen milieu in the Netherlands*, Utrecht University 2024, https://studenttheses.uu.nl/bitstream/handle/20.500.12932/47667/h.c.koppelman_6919642_thesis_CSHR.pdf?sequence=1&isAllowed=y [dostęp: 1 VII 2025].

Koźlik B., *Doręczenie odpisu postanowienia zwierzchnika władzy w Rzeczypospolitej Polskiej*, Zawodowy Polak, 27 VI 2022 r., https://zawodowy-polak.pl/BK-ost_postanowienie_bank_27.06.2022.pdf [dostęp: 1 I 2025].

Król P., *Analiza zamachów na osoby publiczne — skuteczność działań prewencyjnych służb bezpieczeństwa i konsekwencje polityczno-społeczne*, „Kwartalnik Kadry Kierowniczej Policji" 2024, nr 3, https://kwartalnik.akademiapolicji.edu.pl/images/stories/2024/3/krl.pdf [dostęp: 1 VII 2025].

Majchrowski J., *Kwestia sukcesji prezydenckiej na obczyźnie*, w: *Myśl polityczna: od historii do współczesności*, B. Stoczewska, M. Jaskólski (red.), Kraków 2000, s. 253–260, https://ruj.uj.edu.pl/server/api/core/bitstreams/2cc6a415-0de3-4172-bbd2-2cd16fce2235/content [dostęp: 1 I 2025].

Mendyk B., *Jak reagować na petycje pełne teorii spiskowych?*, Pismo Samorządu Terytorialnego „Wspólnota", 3 IV 2024 r., https://wspolnota.org.pl/newsletter/jak-reagowac-na-petycje-pelne-teorii-spiskowych [dostęp: 1 I 2025].

Meyer C., *5 Common Crimes Committed by Sovereign Citizens*, Police1, 6 IX 2024 r., https://www.police1.com/community/articles/5-common-crimes-committed-by-sovereign-citizens-1KKxo42li5FVeANM/ [dostęp: 1 I 2025].

Murder of Dallas Police Officer Marks Latest in String of Violent Sovereign Citizen Encounters with Law Enforcement, Anti-Defamation League, 9 XII 2024 r., https://www.adl.org/resources/article/murder-dallas-police-officer-marks-latest-string-violent-sovereign-citizen [dostęp: 1 I 2025].

Najemnicy NFUMiG Konstancin Jeziorna, kanał YouTube Zawodowy Polak, 2 VII 2024 r., https://www.youtube.com/watch?v=jeH8LX0eYfY [dostęp: 1 VII 2025].

Najwyższy Trybunał Narodowy. Akt ustanowienia, Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/najwyzszy-trybunal-narodowy/ [dostęp: 21 VII 2025].

Nie można nagrywać najemników i lokalu wyborczego w Kisielsku?, kanał YouTube Zawodowy Polak, 9 VI 2024 r., https://www.youtube.com/watch?v=8nAon2vpOTQ [dostęp: 15 XII 2024].

„Nielegalne" zatrzymanie przez Policję i ZAWODOWY POLAK | Bagieta rozkłada interwencje #3, kanał YouTube Sierżant Bagieta, 26 II 2020 r., https://www.youtube.com/watch?v=EgQWjQEDq_A [dostęp: 1 I 2025].

Ośrodek Monitorowania Zachowań Rasistowskich i Ksenofobicznych, *Teresa Garland będąca prorosyjską patocelebrytką w końcu zatrzymana przez policję*, Facebook, 28 IX 2022 r., https://www.facebook.com/osrodek.monitorowania/posts/teresa/garland-b%C4%99d%C4%85ca-prorosyjsk%C4%84-patocelebrytk%C4%85-w-ko%C5%84cu-zatrzymana-przez-policj/1917138658461258/ [dostęp: 1 I 2025].

Pismo z dnia 28 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) Syg. Akt I Co 3161/2, Zawodowy Polak, https://www.zawodowy-polak.pl/TB-NFSR-W-wa_Wola_28.05.2024.pdf [dostęp: 14 VII 2025].

Pismo z dnia 7 III 2024 r. dotyczące braku uprawnień do pełnienia funkcji sędziego, dyrektora i prezesa – dyskryminacji, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFSR-Grojec_7.03.2024.pdf [dostęp: 14 VII 2025].

Pismo z dnia 8 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) Syg. Akt: 4161-0.Ds 783.24, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFPR-Lukow_8.05.2024.pdf [dostęp: 14 VII 2024].

Powers A., *How Sovereign Citizens Helped Swindle $1 Billion From the Government They Disavow*, The New York Times, 29 III 2019 r., https://www.nytimes.com/2019/03/29/business/sovereign-citizens-financial-crime.html [dostęp: 25 X 2024].

Powołanie Rządu Wolnej Polski, kanał YouTube Trybunał Narodowy, https://www.youtube.com/watch?v=1HyXzBXXfOs&t=1s [dostęp: 1 VII 2025].

Powołano Rząd Wolnej Polski, Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/powolano-rzad-wolnej-polski/ [dostęp: 1 VII 2025].

Prawo wyborcze, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Prawo_wyborcze [dostęp: 1 I 2025].

Prezes NBP Glapiński, Teresa Garland i demokracja, kanał YouTube Fides Polska TV, 16 XI 2018 r., https://www.youtube.com/watch?v=j1Bd4ZToToE [dostęp: 1 I 2025].

Protokoły Mędrców Syjonu, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Protoko%C5%82y_M%C4%99drc%C3%B3w_Syjonu [dostęp: 1 VII 2025].

Redemption Theory/Starwman Theory, Anti-Defamation League, https://extremismterms.adl.org/glossary/redemption-theorystrawman-theory [dostęp: 14 VII 2025].

Religia, Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Religia [dostęp: 9 VII 2025].

Report and Recommendation, Case No. 1:16-cv-614, https://www.govinfo.gov/content/pkg/USCOURTS-ohsd-1_16-cv-00614/pdf/USCOURTS-ohsd-1_16-cv-00614-0.pdf [dostęp: 1 I 2025].

Sajór G., *Nie wytrzymał ciśnienia. Mariusz Max Kolonko po odejściu z dziennikarstwa został Presidentem*, Press, 20 V 2022 r., https://www.press.pl/tresc/70879,[na-weekend]-nie-wytrzymal-cisnienia_-mariusz-max-kolonko-po-odejsciu-z-dziennikarstwa-zostal-presidentem [dostęp: 1 VII 2025].

Samozwańcza prezydent sypnęła petycjami, Super Tydzień Chełmski, 15 IV 2021 r., https://www.supertydzien.pl/artykul/10406,samozwancza-prezydent-sypnela-petycjami [dostęp: 1 I 2025].

Sidorowicz J., *Broń od gminy dla każdego rdzennego mieszkańca Starego Sącza? Jest petycja w sprawie programu „Broń palna plus"*, Kraków.Wyborcza.pl, 26 IX 2022 r., https://krakow.wyborcza.pl/krakow/7,44425,28955388,bron-od-gminy-dla-kazdego-rdzennego-mieszkanca-starego-sacza.html [dostęp: 1 I 2025].

Silver Certificates, NORFED Liberty Dollar, https://norfed.info/silver-certificates/ [dostęp: 1 I 2025].

Spungen D., *How Financial Institutions Should Handle „Sovereign Citizens"*, Amundsen Davis, 18 III 2024 r., https://www.amundsendavislaw.com/banking-brief-financial-services-insights/how-financial-institutions-should-handle-sovereign-citizens [dostęp: 1 I 2025].

Starzewski Ł., *Polska zarejestrowana jako firma w USA? RPO prosi MSZ o zbadanie skargi obywatela*, Rzecznik Praw Obywatelskich, 24 II 2020 r., https://www.rpo.gov.pl/pl/content/polska-zarejestrowana-jako-firma-w-usa-rpo-prosi-msz-o-zbadanie-skargi-obywatela [dostęp: 25 X 2024].

The Sovereign Citizen Movement: Common Documentary Identifiers & Examples, Anti-Defamation League, 5 XII 2016 r., https://www.adl.org/resources/reports/the-sovereign-citizen-movement-common-documentary-identifiers-examples [dostęp: 25 X 2024].

The Sovereigns: A Dictionary of the Peculiar, The Southern Poverty Law Center, 1 VIII 2010 r., https://www.splcenter.org/fighting-hate/intelligence-report/2010/sovereigns-dictionary-peculiar [dostęp: 14 VII 2024].

Top Russian central banker shot to death, NBC News, 14 IX 2006 r., https://www.nbcnews.com/id/wbna14826889 [dostęp: 1 VII 2025].

Uchwała Najwyższego Trybunału Narodowego o nieważności wyroków w imieniu Rzeczypospolitej Polskiej, trybunał-narodowy.pl, 13 XI 2024 r., https://www.trybunal-narodowy.pl/uchwala-najwyzszego-trybunalu-narodowego-o-niewaznosci-wyrokow-w-imieniu-rzeczypospolitej-polskiej/ [dostęp: 1 VII 2025].

Wyrok zaoczny w imieniu Zwierzchnika Władzy w Rzeczypospolitej Polskiej, Zawodowy Polak, 10 IX 2024 r., https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf [dostęp: 25 X 2024].

Zaremba J., *„Leczył" z zaburzeń psychicznych i masturbacji. „Książę" Świętopełk-Zawadzki na Narodowym Marszu Papieskim*, Gazeta.pl, 3 IV 2023 r., https://kobieta.gazeta.pl/kobieta/7,107881,29626596,leczyl-z-zabrzen-psychicznych-i-homoseksualizmu.html [dostęp: 1 VII 2025].

Akty prawne

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

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – (Dz. Urz. UE L 119/1 z 4 V 2016 r.).

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (t.j. DzU z 2025 r. poz. 34, ze zm.).

Ustawa z dnia 11 lipca 2014 r. o petycjach (t.j. DzU z 2018 r. poz. 870).

Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (t.j. DzU z 2025 r. poz. 555).

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

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. DzU z 2025 r. poz. 383).

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. DzU z 2025 r. poz. 46, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2025 r. poz. 636).

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. DzU z 2024 r. poz. 1465, ze zm.).

Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. DzU z 2023 r. poz. 2119, ze zm.).

Patryk Król

Student studiów II stopnia na Uniwersytecie Ekonomicznym w Poznaniu.

Kontakt: patkro12@gmail.com

ARTYKUŁY RECENZYJNE

RECENZJE

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 155–164

https://doi.org/10.4467/20801335PBW.25.007.22173

RECENZJA

Mechanizmy ochrony ludności w redukcji ryzyka katastrof. Wybrane zagadnienia, Paweł Gromek, Mariusz Feltynowski, Monika Wojakowska (red.)[1]

JULIA W. TOCICKA

Zakład Prawa Podatkowego i Celnego,
Szkoła Główna Handlowa

https://orcid.org/0000-0003-1536-6817

Ochrona ludności, jako najważniejszy obowiązek państwa, koncentruje się wokół ochrony życia i zdrowia obywateli, mienia, dziedzictwa kulturowego oraz środowiska naturalnego w sytuacjach zagrożeń naturalnych i antropogenicznych. Współczesne zagrożenia to katastrofy naturalne oraz zagrożenia asymetryczne, terrorystyczne, cybernetyczne, hybrydowe, a także inne stwarzane przez człowieka, w tym zagrożenia militarne, gwałtownie i destrukcyjnie oddziałujące na populację, infrastrukturę oraz środowisko naturalne. Zapewnienie bezpieczeństwa ludności cywilnej przez organy władzy publicznej zawiera się

[1] *Mechanizmy ochrony ludności w redukcji ryzyka katastrof. Wybrane zagadnienia*, P. Gromek, M. Feltynowski, M. Wojakowska (red.), Toruń 2023, Wydawnictwo Adam Marszałek, 292 s.

w konstytucyjnej zasadzie ochrony życia[2], dlatego tak istotne jest dokładne określenie ram takich działań. Efektywne zarządzanie ochroną ludności wymaga przyjęcia kompleksowego podejścia, obejmującego zarówno zapobieganie katastrofom, przygotowanie i reagowanie na nie, jak i odbudowę (rekonstrukcję) po takich zdarzeniach. Skuteczność działań ochrony ludności wzrasta dzięki integracji nowoczesnych technologii, takich jak drony i systemy satelitarne, co pozwala na lepsze monitorowanie sytuacji kryzysowych i zarządzanie nimi. Nieodłącznym elementem zwiększania świadomości oraz przygotowania na wypadek katastrof jest edukacja społeczności lokalnych. Do lepszego zrozumienia ryzyka i zarządzania nim przyczynia się wymiana doświadczeń między państwami. Zjawiska, do pewnego momentu stanowiące jedynie wyzwanie dla danego podmiotu, w związku z dynamiką zmian zachodzących w jego środowisku wewnętrznym oraz zewnętrznym, ewoluują w zagrożenia, które mogą zakłócić prawidłowe funkcjonowanie oraz dalszy rozwój tego podmiotu.

Sytuacje powodujące zagrożenia bezpieczeństwa ludności często cechują się dużą nieprzewidywalnością i gwałtownością, przez co wymuszają na organach administracji publicznej podejmowanie natychmiastowych działań niekiedy bez odpowiedniego przygotowania oraz dostosowania do sytuacji. Liczba, specyfika i siła oddziaływania zagrożeń występujących w związku z rosnącym ryzykiem katastrof nierzadko przekraczają realne możliwości operacyjne państw. Odpowiedzią na potrzebę niesienia pomocy w sytuacjach, w których siły i środki poszczególnych krajów mogą okazać się niewystarczające, są międzynarodowe mechanizmy i działania organizacji bezpieczeństwa na rzecz ochrony ludności i redukcji ryzyka katastrof, take jak: System Oceny i Koordynacji Katastrof Organizacji Narodów Zjednoczonych (United Nations Disaster Assessment and Coordination, UNDAC)[3], Międzynarodowa Grupa Doradcza ds. Poszukiwań i Ratownictwa (The International Search and Rescue Advisory Group, INSARAG)[4], Organizacja Traktatu Północnoatlantyckiego (North Atlantic Treaty Organization, NATO) i Unijny Mechanizm Ochrony Ludności (EU Civil Protection Mechanism, UCPM). Mechanizmy te mają służyć podnoszeniu efektywności współdziałania podmiotów ratowniczych, zwiększaniu świadomości i odporności społecznej oraz skutecznej i skoordynowanej pomocy ludności cywilnej. W kontekście międzynarodowym odgrywają one

[2] Art. 30 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (DzU z 1997 r. nr 78 poz. 483, ze zm.).

[3] UNDAC jest częścią Biura Koordynacji Pomocy Humanitarnej (United Nations Office for the Coordination of Humanitarian Affairs, OCHA).

[4] INSARAG to sieć krajów i organizacji reagujących na katastrofy, zajmujących się miejskimi poszukiwaniami i ratownictwem (ang. *urban search and rescue*, USAR) oraz koordynacją działań operacyjnych w terenie.

najważniejszą rolę w budowaniu globalnej odporności na katastrofy. W związku z rosnącą liczbą takich zdarzeń coraz bardziej istotne staje się finansowanie tych mechanizmów. Środki przeznaczane na ten cel pochodzą z różnych źródeł, w tym budżetu państwa, funduszy unijnych oraz dotacji międzynarodowych. Dobre zarządzanie finansami jest niezbędne do utrzymania infrastruktury krytycznej, zakupu nowoczesnego sprzętu ratunkowego oraz realizacji programów szkoleniowych.

Organizacje pozarządowe mają istotny wkład w koordynację pomocy humanitarnej na poziomie międzynarodowym, a inwestycje w infrastrukturę odporną na katastrofy są bardzo ważne dla minimalizowania strat i szybkiego powrotu do normy. Podnoszenie standardów budowlanych i planowania przestrzennego może pozytywnie wpłynąć na zmniejszanie skutków katastrof. Współpraca z sektorem prywatnym pozwala na wykorzystanie jego zasobów i kompetencji specjalistów, które mogą okazać się bardzo przydatne w sytuacjach kryzysowych. Regularne ćwiczenia i symulacje scenariuszy katastrof pomagają w lepszym przygotowaniu się przez służby ratownicze na rzeczywiste zagrożenia.

Redukowanie ryzyka katastrof przez uruchamianie międzynarodowych mechanizmów ochrony ludności to bardziej praktyczne podejście względem klasycznego rozumienia zarządzania ryzykiem, tj. utożsamiania go z działaniami zapobiegawczymi, przygotowawczymi i rekonstrukcyjnymi. Najważniejszym komponentem holistycznego cyklu zarządzania ochroną ludności jest reagowanie. Integracja reagowania z fazami cyklu zarządzania ryzykiem katastrof umożliwia skoordynowaną i wszechstronną reakcję na zagrożenia o zasięgu międzynarodowym. W ten sposób dla państw dotkniętych katastrofami mechanizmy ochrony ludności nie tylko są wsparciem w radzeniu sobie z bezpośrednimi skutkami zagrożeń, lecz także przyczyniają się do budowania długotrwałej odporności przez wspieranie działań zapobiegawczych i przygotowawczych. Uwzględnienie reagowania jako fundamentalnego elementu zarządzania ochroną ludności pozwala lepiej się przygotować na nieprzewidziane sytuacje oraz ograniczyć ryzyko wystąpienia efektu kaskadowego, w którym jedno zagrożenie prowadzi do kolejnych. Właściwe reagowanie zatem jest kluczem do redukowania ryzyk wtórnych.

Badania nad problematyką ochrony ludności prowadzili w ostatnich latach m.in. Bogdan Michailiuk[5], Krzysztof R. Zieliński[6], Ewa Jakubiak[7], Paweł

[5] B. Michailiuk, *Ochrona ludności. Wybrane problemy*, Warszawa 2017.

[6] K.R. Zieliński, *Ochrona ludności. Zarządzanie kryzysowe*, Warszawa 2017.

[7] E. Jakubiak, *Rola Państwowej Straży Pożarnej w zakresie ochrony ludności. Ujęcie prawno-instytucjonalne*, Warszawa 2022.

Ł. Szmitkowski[8], Sławomir Górski[9], Jerzy Trocha[10], Katarzyna Płonka-Bielenin[11] oraz Wojciech Krasiński[12]. Rosnące zainteresowanie tym zagadnieniem świadczy zarówno o jego aktualności, jak i ogromnym znaczeniu dla bezpieczeństwa powszechnego. Współczesne zarządzanie bezpieczeństwem powinno opierać się na rozwiązaniach wykorzystujących istniejące struktury oraz systemy i tym samym zapewniających obywatelom bezpieczeństwo we wszystkich stanach gotowości obronnej państwa.

Ochrona ludności obejmuje coraz szerszy zakres działań mających na celu zapewnienie bezpieczeństwa każdej osobie na danym terytorium, niezależnie od jej statusu prawnego. Ustawa o ochronie ludności i obronie cywilnej[13] w art. 2 definiuje to pojęcie jako (…) *system składający się z organów administracji publicznej wykonujących zadania mające na celu zapewnienie bezpieczeństwa ludności przez ochronę życia i zdrowia ludzi, mienia, w tym zwierząt, infrastruktury niezbędnej do zaspokojenia potrzeb bytowych, dóbr kultury i środowiska w sytuacji zagrożenia, podmiotów wykonujących te zadania oraz zasobów ochrony ludności*. Ustawa wprowadziła ponadto rozwiązania systemowe służące skuteczniejszemu reagowaniu na współcześnie występujące zagrożenia w czasie pokoju oraz wojny. Umożliwia to przygotowanie podmiotów ochrony ludności do efektywnego działania w sytuacjach kryzysowych, niezależnie od źródeł zagrożeń. W przypadku działań wojennych, katastrof naturalnych czy spowodowanych przez człowieka jest konieczne podjęcie działań takich jak ewakuacja ludności, udzielenie jej pomocy medycznej, zapewnienie warunków przetrwania oraz zabezpieczenie mienia. Dotychczas wprowadzone regulacje prawne koncentrowały się na fazie reagowania, z możliwością rozszerzenia działań na etapy zapobiegania i odbudowy. Te rozwiązania cechowała jednak centralizacja z dominującą rolą administracji rządowej. Istnieje zatem potrzeba stworzenia jednolitych przepisów prawnych, jasno określających kompetencje organów, obowiązki obywateli oraz metody zwiększania świadomości społeczeństwa na temat bezpieczeństwa powszechnego. Należy również określić zadania ochrony ludności zgodnie z obowiązującymi ustawami, takimi jak ustawa o obronie

[8] P. Szmitkowski, *Ochrona ludności i obrona cywilna w systemie administracji publicznej*, Siedlce 2017.

[9] S. Górski, *Współczesna ochrona ludności. Aspekty prawne i organizacyjne*, Warszawa 2016.

[10] J. Trocha, *Propedeutyka ochrony ludności w Polsce. Problemy. Możliwości. Perspektywy*, Warszawa 2020.

[11] K. Płonka-Bielenin, *Analiza rozwiązań prawnych proponowanych w projekcie ustawy o ochronie ludności oraz o stanie klęski żywiołowej i ich skutki w praktyce*, „Przegląd Prawa Publicznego" 2024, nr 6, s. 98–112.

[12] W. Krasiński, *Civil Protection Of The Population Of Poland In Peacetime After 2007*, „Zeszyty Naukowe Akademii Sztuki Wojennej" 2018, nr 4(113), s. 73–84.

[13] *Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej* (DzU z 2024 r. poz. 1907).

Ojczyzny[14], ustawa o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[15] i ustawa o zarządzaniu kryzysowym[16].

Tej tematyki dotyczy zbiorowa publikacja zatytułowana *Mechanizmy ochrony ludności w redukcji ryzyka katastrof. Wybrane zagadnienia* pod redakcją Pawła Gromka, Mariusza Feltynowskiego oraz Moniki Wojakowskiej. Redaktorzy naukowi zawodowo są związani z Akademią Pożarniczą, a jednocześnie pełnią służbę w Państwowej Straży Pożarnej, która odgrywa istotną rolę w ochronie ludności. Celem autorów było usystematyzowanie wiedzy na temat mechanizmów ochrony ludności oraz przedstawienie nowych koncepcji dotyczących ich działania. Wydanie monografii poprzedziło proces legislacyjny procedowanej od wielu lat ustawy o ochronie ludności i obronie cywilnej, która weszła w życie 1 stycznia 2025 r.

Publikacja składa się z dziesięciu rozdziałów poprzedzonych wstępem. Redaktorzy wskazali w nim, że tematyka międzynarodowych mechanizmów ratownictwa w przypadku wystąpienia sytuacji kryzysowych jest wieloaspektowa oraz stanowi kierunek strategicznego rozwoju międzynarodowego wsparcia na rzecz ochrony ludności.

W rozdziale pierwszym autor skupił się na analizie międzynarodowych mechanizmów ochrony ludności, które w świetle teorii organizacji bezpieczeństwa odgrywają kluczową rolę w redukcji ryzyka katastrof[17]. Przedstawił podstawowe założenia teoretyczne dotyczące organizacji bezpieczeństwa oraz zarządzania ryzykiem katastrof. Szczególną uwagę poświęcił wspomnianym mechanizmom w ramach INSARAG, UNDAC, NATO oraz UCPM. Zostały one omówione pod względem ich struktury organizacyjnej, sposobu działania oraz efektywności w minimalizowaniu skutków katastrof. Badacz uwzględnił także wyzwania związane z koordynacją działań międzynarodowych i wsparciem dla państw dotkniętych skutkami katastrof. Stwierdził, że omówione mechanizmy mogą przyczynić się do ograniczenia sił i skutków oddziaływania i zmniejszenia podatności na zagrożenia oraz zwiększenia zdolności do radzenia sobie z katastrofami.

---

[14] *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny* (t.j. DzU z 2024 r. poz. 248, ze zm.).

[15] *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).

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

[17] P. Gromek, *Międzynarodowe mechanizmy ochrony ludności w redukcji ryzyka katastrof. Perspektywa teorii organizacji bezpieczeństwa*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 13–36.

Rozdział drugi dotyczy koncepcji kompleksowego wzmacniania odporności RP rozumianego jako element redukcji ryzyka katastrof[18]. Autor omówił polskie podejście systemowe do budowania i wzmacniania odporności, które porównał z podejściem NATO i Unii Europejskiej. Przedstawił również propozycje podziału funkcjonalnego odporności oraz ponoszenia odpowiedzialności za realizację zadań. Zaproponował wskaźniki i mierniki określające poziom odporności oraz plan działań służących wzmacnianiu odporności państwa i omówił ich potencjalny wpływ na ograniczenie ryzyka katastrof.

Autorki rozdziału trzeciego skoncentrowały się na zarządzaniu bezpieczeństwem klimatycznym jako najważniejszym elemencie redukcji ryzyka katastrof[19]. Badaczki omówiły jego istotę oraz aspekty formalnoprawne. Przedstawiły międzynarodowe i europejskie regulacje prawne w zakresie zarządzania bezpieczeństwem klimatycznym oraz zanalizowały działania polskiego rządu podejmowane na rzecz zwiększania jego efektywności. Rozdział kończy się przeglądem rozwiązań prewencyjnych wdrożonych na poziomie krajowym oraz wnioskami na temat ich skuteczności i rekomendacjami na przyszłość. Proces redukcji ryzyka katastrof klimatycznych wymaga szybkich reakcji, pogłębionych badań, transferu wiedzy i nowoczesnych rozwiązań systemowych mających na celu zmniejszenie tempa zmian klimatycznych[20].

W rozdziale czwartym omówiono ochronę przeciwpożarową lasów w kontekście unijnych mechanizmów gromadzenia informacji[21]. Zanalizowano w nim dane dotyczące sytuacji pożarowej w polskich lasach w latach 2019–2021, przyczyny pożarów, a także metody ich wykrywania oraz systemy przeciwpożarowe. Ponadto autor opisał rolę Europejskiego Systemu Informacji o Pożarach Lasów (European Forest Fire Information System, EFFIS) oraz przedstawił zagrożenia pożarowe na świecie. We wnioskach podkreślił konieczność doskonalenia mechanizmów ochrony lasów przed pożarami oraz zacieśniania współpracy międzynarodowej w tym zakresie.

---

[18] S. Łazarek, *Autorska koncepcja kompleksowego wzmacniania odporności Polski jako element redukcji ryzyka katastrof – perspektywa krajowa i międzynarodowa*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof*…, s. 37–75.

[19] M. Wojakowska, K. Kurowska, *Zarządzanie bezpieczeństwem klimatycznym w kontekście redukcji ryzyka katastrof – przegląd wdrożonych rozwiązań prewencyjnych na poziomie krajowym*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof*…, s. 76–113.

[20] Tamże, s. 113.

[21] M. Gebauer-Lewandowska, *Ochrona przeciwpożarowa lasu w perspektywie unijnych mechanizmów gromadzenia informacji*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof*…, s. 114–131.

Pożarów lasów w Europie dotyczy także rozdział piąty[22]. Szczegółowo omówiono w nim wpływ zmian klimatu na strategie UE w zwalczaniu pożarów lasów oraz rolę UCPM jako platformy współpracy międzynarodowej. Przedstawiono jego zasoby i działania podejmowane w jego ramach w celu walki z tego rodzaju pożarami. W ostatnich latach doszło na terenie UE do trzech wielkopowierzchniowych pożarów lasów (w Szwecji w 2018 r., Grecji w 2021 r. oraz we Francji w 2022 r.), w których gaszeniu uczestniczyły moduły z Polski (GFFFV Poznań, GFFFV Szczecin i GFFFV Wrocław)[23]. Na zakończenie rozdziału zaprezentowano wnioski *de lege ferenda* na temat skuteczności tych działań[24]. Długoletni trend wzrostowy (lata 2007–2021) związany z aktywacją mechanizmu do zwalczania skutków pożarów lasów jest skorelowany z długoletnim trendem rosnącej ekspansji pożarów lasów na terenie Europy. Poszerzenie polityki UCPM o dofinansowanie i wspieranie organizacji pozarządowych, wolontariatów oraz akcji promujących ochronę ludności i ochronę klimatu może przyczynić się do ograniczenia zagrożeń pożarowych[25].

Zastosowania UCPM poddał analizie również autor rozdziału szóstego, tym razem w kontekście budowy systemów bezpieczeństwa międzyregionalnego na przykładzie województwa śląskiego[26]. Przedstawił prawno-organizacyjne aspekty funkcjonowania UCPM oraz zasady jego aktywacji na poziomie regionalnym. Skupił się na szczegółowym omówieniu porozumień między jednostkami samorządu terytorialnego dotyczących współpracy i pomocy ratowniczej. Analiza objęła również mechanizmy koordynacji działań ratowniczych oraz zapobiegawczych, które są niezbędne do efektywnego reagowania na katastrofy. Rozdział kończy się wnioskami na temat skuteczności współpracy międzyregionalnej oraz rekomendacjami dotyczącymi usprawnień w zakresie ochrony ludności[27]. Autor przyjął, że UCPM mógłby stanowić parasol ochronny z uwagi na jego szeroki zakres zasobów uzupełniony o możliwości prowadzenia wspólnych działań ratowniczych na podstawie zawartych postanowień regionalnych.

W rozdziale siódmym autorka przedstawiła własne podejście do zarządzania bezpieczeństwem społeczności lokalnych w kontekście budowania kapitału

---

[22] S. Świerk, *Zastosowanie zasobów Unijnego Mechanizmu Ochrony Ludności jako sposób na walkę z pożarami lasów w Europie*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 132–158.

[23] Tamże, s. 155–156.

[24] Tamże, s. 157–158.

[25] Tamże, s. 158.

[26] P. Węgrzyn, *Unijny Mechanizm Ochrony Ludności w kontekście budowy systemów bezpieczeństwa międzyregionalnego na przykładzie województwa śląskiego*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 159–176.

[27] Tamże, s. 176.

społecznego oraz lokalnych mechanizmów redukcji ryzyka katastrof[28]. Skupiła się na zarządzaniu bezpieczeństwem na poziomie lokalnym, z uwzględnieniem strategii angażowania społeczności lokalnej w procesy decyzyjne. Przedstawiła model „strategiczne podejście – działanie lokalne – myślenie globalne", który integruje lokalne działania z globalnymi strategiami bezpieczeństwa. Analiza objęła korzyści płynące z budowania kapitału społecznego jako kluczowego elementu w zarządzaniu bezpieczeństwem oraz wpływ tych działań na zwiększenie odporności społeczności lokalnych na zagrożenia. Zaproponowane rozwiązania opierają się na trzech filarach wspomagających działania na rzecz bezpieczeństwa lokalnego, tj. think tankach, warsztatach szkoleniowych oraz lokalnych liderach bezpieczeństwa. Rozdział kończą wnioski i rekomendacje dotyczące wdrażania tych koncepcji na poziomie lokalnym w celu zwiększenia efektywności działań prewencyjnych i reagowania na katastrofy[29].

W ósmym rozdziale została poruszona tematyka globalnego efektu ograniczania lokalnych zagrożeń chemicznych[30]. Autorka omówiła zróżnicowane zagrożenia chemiczne, które mogą prowadzić do katastrof na szeroką skalę, oraz przedstawiła klasyfikację tych katastrof. Skoncentrowała się na metodach redukcji ryzyka związanego z zagrożeniami chemicznymi, z uwzględnieniem zarówno prewencji, jak i reagowania. Przedstawiła wnioski z dotychczasowych doświadczeń w zarządzaniu zagrożeniami chemicznymi przez omówienie najlepszych procedur oraz narzędzi stosowanych na poziomach lokalnym i globalnym. Należą do nich planowanie awaryjne, wewnętrzne i zewnętrzne plany operacyjno-ratownicze, kontrola zanieczyszczeń, działania mające na celu zminimalizowanie negatywnych skutków użycia chemikaliów, wybór alternatywnych substancji lub technologii oraz zmiana technologii wytwarzania produktów. Autorka podkreśliła, że przy wyborze najefektywniejszego narzędzia należy uwzględnić m.in.: stopień zagrożenia, efektywność, trwałość w czasie, koszty i korzyści dla różnych podmiotów, konsekwencje społeczno-ekonomiczne oraz obciążenie administracyjne. Zasugerowała dalsze doskonalenie metod ograniczania zagrożeń chemicznych przez zastosowanie innowacyjnych technologii i wzmocnienie współpracy międzynarodowej[31].

W rozdziale dziewiątym przedstawiono koncepcję rozwoju zdolności operacyjnych wojskowych straży pożarnych w warunkach wojennych i analizę potrzeb

[28] N. Piorun, *Autorskie podejście do zarządzania bezpieczeństwem społeczności lokalnych w kontekście budowania kapitału społecznego – perspektywa lokalnych mechanizmów redukcji ryzyka katastrof*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 177–204.

[29] Tamże, s. 204.

[30] J. Rakowska, *Globalny efekt ograniczania lokalnych zagrożeń chemicznych*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 205–219.

[31] Tamże, s. 217.

w tym zakresie[32]. Opisano ponadto organizację i funkcjonowanie Wojskowej Ochrony Przeciwpożarowej, w tym systemu szkolenia strażaków służących w wojskowych strażach pożarnych, który uwzględnia specyfikę działań w warunkach konfliktów zbrojnych, a także rekomendacje dotyczące poprawy przygotowania i wyposażenia tych służb. Omówiono wyzwania związane z adaptacją standardowych procedur straży pożarnych do warunków wojennych. Do najważniejszych z nich należy zaliczyć dostosowanie sytemu szkolenia i doskonalenia zawodowego strażaków oraz zasobów ratowniczych do potrzeb ochrony przeciwpożarowej Sił Zbrojnych RP. We wnioskach autor zwrócił uwagę na konieczność modernizacji systemów ochrony przeciwpożarowej w środowisku wojskowym oraz na potrzebę aktualizacji wykorzystywanych technologii i procedur, co zapewniłoby optymalną skuteczność działań prewencyjnych i reakcji na zagrożenia pożarowe w dynamicznie zmieniających się warunkach operacyjnych[33].

Rozdział dziesiąty dotyczy systemów bezzałogowych statków powietrznych (ang. *unmanned aerial system*, UAS)[34]. Przedstawiono w nim charakterystykę tej technologii oraz różne możliwości jej zastosowania w scenariuszach katastrof naturalnych i antropogenicznych. Autor przeprowadził szczegółowe studia trzech przypadków: pożaru w Biebrzańskim Parku Narodowym (19 kwietnia 2020 r.), osuwiska w Gjerdrum (30 grudnia 2020 r.) oraz awarii elektrowni jądrowej w Fukushimie (11 marca 2011 r.). W każdym z tych zdarzeń UAS odegrały istotną rolę w procesie monitorowania oraz zarządzania kryzysowego. Autor omówił korzyści płynące z ich zastosowania, takie jak zwiększenie efektywności działań ratowniczych, lepsze monitorowanie obszarów dotkniętych katastrofami oraz możliwość szybszego reagowania na zagrożenia. Rozdział kończy się wnioskami na temat kierunków rozwoju i integracji UAS w systemach zarządzania kryzysowego oraz rekomendacjami dotyczącymi wykorzystania tej technologii do redukcji ryzyka katastrof na szeroką skalę. Według recenzentki autor słusznie stwierdził, że minimalizacja sensorów, rozwój technologii transmisji danych, zawansowane algorytmy i programy do detekcji (np. Radiometric Data Toolset – RDT, Search and Rescue with Unmanned Aerial Vehicle – SARUAV) oraz zwiększenie niezawodności podzespołów przyczynią się do szerokiego zastosowania UAS przez służby ratownictwa[35].

---

[32] W. Szulc, *Koncepcja rozwoju zdolności operacyjnych wojskowych straży pożarnych na czas wojny*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 220–255.

[33] Tamże, s. 252.

[34] R. Fellner, *Zastosowanie systemów bezzałogowych statków powietrznych elementem zarządzania kryzysowego i redukcji ryzyka katastrof*, w: *Mechanizmy ochrony ludności w redukcji ryzyka katastrof…*, s. 256–271.

[35] Tamże, s. 271.

Recenzowana monografia może być bardzo pomocna w zrozumieniu istoty ochrony ludności w Polsce. Dostarcza kompleksowej wiedzy na ten temat, w tym prezentuje związane z nim aktualne wyzwania i strategie. Autorzy w sposób przejrzysty i merytoryczny analizują najważniejsze mechanizmy ochrony ludności, skupiając się na ich roli w redukcji ryzyka katastrof. Pozwala to na zrozumienie złożoności zagadnień oraz przedstawienie skutecznych strategii i narzędzi, które mogą zostać zastosowane w praktyce. Wiedza zawarta w recenzowanej książce może pomóc w lepszym przygotowaniu się rządzących, służb i mieszkańców/społeczeństwa do sytuacji nadzwyczajnych oraz w rozwijaniu skutecznych metod prewencji i reakcji. Publikacja jest wartościowym źródłem informacji zarówno dla specjalistów, jak i innych osób zainteresowanych problematyką bezpieczeństwa powszechnego. Szczegółowe *case studies* czynią ją wartościową lekturą dla organów administracji publicznej, służb ratunkowych oraz organizacji pozarządowych. Cennym uzupełnieniem monografii są liczne tabele i rysunki, ułatwiające czytelnikom dostęp do informacji zawartych w szczegółowych analizach i statystykach, a także bogata bibliografia. Recenzowana książka dostarcza nie tylko wiedzy teoretycznej, lecz także praktycznych narzędzi i wskazówek przydatnych przy analizach konkretnych sytuacji kryzysowych.

Dr Julia W. Tocicka

Specjalistka w zakresie prawa administracyjnego, prawniczka, finansistka, doktor w dziedzinie nauk społecznych. Absolwentka studiów podyplomowych z zarządzania cyberbezpieczeństwem oraz Szkoły Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych PCK. Odbyła staż naukowy w Podkarpackim Uniwersytecie Narodowym im. Wasyla Stefanyka w Iwano-Frankiwsku. Ekspertka w Ministerstwie Finansów, w Departamencie Podatków Dochodowych, menedżer ds. ryzyka w zakresie bezpieczeństwa informacji, delegatka OECD (Task Force on the Digital Economy) oraz Intra-European Organisation of Tax Administrations, członkini Polskiego Stowarzyszenia Profesjonalistów i Ekspertów Administracji Publicznej. Autorka kilkudziesięciu recenzowanych publikacji naukowych. Specjalizuje się w tematyce administracji publicznej, bezpieczeństwa finansowego, prawa podatkowego, międzynarodowego prawa podatkowego, prawa spółek handlowych i prawa finansowego.

Kontakt: jtocic@sgh.waw.pl

PRACE KONKURSOWE

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 167–194

https://doi.org/10.4467/20801335PBW.25.008.22174

ARTYKUŁ

Rola minerałów krytycznych i zasobów wodnych w produkcji zielonego wodoru[1]

The role of critical minerals and water resources in green hydrogen production

MARTA GRZYWACZ

Autorka niezależna

https://orcid.org/0009-0006-6620-5262

Abstrakt

Celem artykułu jest przedstawienie roli minerałów krytycznych i zasobów wodnych w produkcji zielonego wodoru. Omówiono czynniki ryzyka związane z wydobyciem tych minerałów, w tym jego wpływ na środowisko oraz dostępność wody w krajach produkcyjnych. Wskazano na poważne wyzwania związane z kumulowaniem produkcji minerałów krytycznych i zielonego wodoru w regionach o wysokim stresie wodnym, co może prowadzić do lokalnych konfliktów o dostęp do wody. Zidentyfikowano również zagrożenia wynikające ze skoncentrowania w kilku krajach wydobycia i rafinacji tych minerałów, mogącego powodować destabilizację łańcucha dostaw i ograniczenie rozwoju sektora zielonego wodoru. Zależność między tym sektorem i odnawialnymi źródłami energii

[1] Artykuł powstał na podstawie pracy licencjackiej pt. *Rola zielonego wodoru w zachowaniu bezpieczeństwa ekonomicznego państwa*, obronionej na Wydziale Społeczno-Ekonomicznym Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Autorka wykorzystała fragmenty rozdziału 2. *Zmienna geopolityka transformacji energetycznej – gospodarka wodorowa*. Praca została nagrodzona w XIII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

sprawia, że w teorii nie powinno być między nimi bezpośredniej konkurencji o minerały. W praktyce jednak oba sektory rywalizują o dostęp do wspólnych surowców niezbędnych do ich rozwoju. Wskazano innowacyjne rozwiązania, takie jak odsalanie wody morskiej, zaawansowane systemy chłodzenia oraz recykling surowców, które zmniejszą zależność sektora wodorowego od kluczowych zasobów. Konieczne jest także opracowanie prognoz uwzględniających zmiany klimatyczne i związane z nimi susze, aby umożliwić tworzenie długoterminowej strategii zarządzania zasobami wodnymi w kontekście rosnącego zapotrzebowania na wodę w sektorze wodorowym.

Słowa kluczowe zielony wodór, minerały krytyczne, zasoby wodne, stres wodny, elektroliza

Abstract This article examines the role of critical minerals and water resources in green hydrogen production. It discusses the risks associated with the extraction of these minerals, including environmental impacts and water availability in production regions. Significant challenges have been identified in relation to the accumulation of critical minerals and the production of green hydrogen in regions of high water scarcity, which can lead to local conflicts over access to water. The study also identifies risks arising from the geographical concentration of mineral extraction and refining in a limited number of countries, which could destabilise supply chains and limit the growth of the green hydrogen sector. While the interdependence of the renewable energy and hydrogen sectors suggests that in theory there is no direct competition for critical minerals, in practice these two sectors compete for access to the same resources that are essential for their development. The article points to innovative solutions including seawater desalination, advanced cooling systems and raw material recycling as ways to reduce the hydrogen sector's dependence on critical resources. Finally, it highlights the importance of developing predictive models that incorporate climate change and drought scenarios to facilitate the development of long-term strategies for sustainable water resource management in response to the hydrogen sector's increasing water needs.

Keywords green hydrogen, critical minerals, water resources, water stress, electrolysis

Wprowadzenie

Technologie wodorowe odgrywają coraz większą rolę w dążeniu do neutralności klimatycznej oraz w realizacji celów zrównoważonego rozwoju w sektorze energetycznym. Zielony wodór (GH_2), wytwarzany w procesie elektrolizy z wykorzystaniem odnawialnych źródeł energii (tj. energii słonecznej, wodnej, cieplnej i wiatrowej, dalej: OZE), stanowi obiecujące narzędzie do redukcji emisji w sektorach trudnych do elektryfikacji, takich jak przemysł ciężki czy transport dalekobieżny[2]. Obecnie zielony wodór odpowiada za mniej niż 1% całkowitej produkcji wodoru, co wskazuje na jego marginalne znaczenie w globalnym rynku wodoru[3]. Zgodnie z prognozami Międzynarodowej Agencji Energetycznej (International Energy Agency, IEA) do 2050 r. zielony wodór może stanowić jednak nawet 94% światowej produkcji wodoru i odpowiadać za ok. 14% globalnego zużycia energii[4]. Wzrost udziału zielonego wodoru w globalnym miksie energetycznym wiąże się z wieloma wyzwaniami, w tym z rosnącym zapotrzebowaniem na minerały krytyczne, niezbędne do produkcji elektrolizerów, systemów magazynowania energii oraz infrastruktury dla OZE.

Termin „minerały krytyczne" (ang. *critical minerals*) zyskał na znaczeniu w kontekście transformacji energetycznej, jaka nastąpiła po 2008 r. w USA, kiedy podjęto szeroką debatę na temat ich roli w technologiach czystej energii[5]. Dwa lata później został on formalnie przyjęty przez Unię Europejską[6]. W 2010 r. Departament Energii Stanów Zjednoczonych (United States Department of Energy, DOE) opublikował raport wskazujący na zasadniczą rolę minerałów krytycznych w rozwoju technologii czystej energii[7], co było podstawą do opracowania w 2018 r. listy tych minerałów[8]. Obecnie termin „minerały

[2] International Renewable Energy Agency, *Green Hydrogen: A guide to policy making*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2020/Nov/IRENA_Green_hydrogen_policy_2020.pdf, s. 7 [dostęp: 12 V 2024].

[3] International Energy Agency, *Critical Materials Strategy*, *Global Hydrogen Review 2024*, https://iea.blob.core.windows.net/assets/89c1e382-dc59-46ca-aa47-9f7d41531ab5/GlobalHydrogenReview2024.pdf, s. 59 [dostęp: 16 XI 2024].

[4] International Renewable Energy Agency, *World Energy Transitions Outlook 2023: 1.5°C Pathway*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Jun/IRENA_World_energy_transitions_outlook_2023.pdf, s. 48 [dostęp: 13 V 2024].

[5] National Research Council, *Minerals, Critical Minerals, and the U.S. Economy*, Washington 2008. https://doi.org/10.17226/12034.

[6] European Commission, *Critical raw materials for the EU*, Brussels 2010.

[7] U.S. Department of Energy, *Critical Materials Strategy*, Washington 2010.

[8] U.S. Department of Energy, *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*, Washington 2018.

krytyczne" jest stosowany powszechnie, a zagadnienia powiązane z tą problematyką stanowią przedmiot szerokich analiz, w tym raportów przygotowywanych przez Międzynarodową Agencję Energii Odnawialnej (International Renewable Energy Agency, IRENA) oraz IEA.

Celem artykułu jest analiza roli minerałów krytycznych oraz zasobów wodnych w produkcji zielonego wodoru oraz identyfikacja potencjalnych zagrożeń i wyzwań związanych z tym procesem. W kontekście wykonalności tej technologii oraz potencjalnego wpływu jej wdrożenia pojawiają się następujące pytania:

- Jakie minerały krytyczne są kluczowe dla rozwoju technologii zielonego wodoru?
- Czy produkcja minerałów niezbędnych do wytwarzania zielonego wodoru jest skoncentrowana w określonych krajach?
- Czy istnieją minerały, w przypadku których zielony wodór może konkurować z innymi technologiami czystej energii w obliczu rosnącego popytu?
- Jaki wpływ na zasoby wodne może mieć wydobycie oraz przetwarzanie minerałów wymaganych do masowego wdrożenia zielonego wodoru?

W artykule omówiono również innowacyjne rozwiązania technologiczne, które mogą przyczynić się do zrównoważonego wykorzystania minerałów krytycznych i zasobów wodnych w produkcji zielonego wodoru.

Autorka dokonała przeglądu literatury naukowej, raportów międzynarodowych instytucji, takich jak IEA, IRENA i Światowa Organizacja Handlu (World Trade Organization, WTO), analiz rynkowych, dokumentów rządowych oraz danych statystycznych.

Znaczenie minerałów krytycznych w produkcji zielonego wodoru

System energetyczny oparty na czystych technologiach zasadniczo różni się od tradycyjnego systemu opartego na paliwach kopalnych. Przeciętny samochód elektryczny wymaga sześciokrotnie większego zużycia surowców mineralnych niż pojazd spalinowy, a elektrownia wiatrowa na lądzie potrzebuje dziewięciokrotnie więcej surowców mineralnych niż elektrownia gazowa. Od 2010 r. średnia ilość minerałów potrzebnych do budowy nowej jednostki mocy wytwórczej wzrosła o 50%, co jest wynikiem rosnącego udziału OZE w globalnym miksie energetycznym. Zielony wodór, produkowany z OZE, jest również uzależniony od dostępności oraz

stabilności dostaw minerałów krytycznych[9]. Warto jednak zauważyć, że nie wszystkie minerały są klasyfikowane jako „krytyczne".

Termin „minerał krytyczny" nie ma jednej, powszechnie przyjętej definicji, a jego interpretacja może różnić się w zależności od kontekstu oraz podmiotu dokonującego oceny. Stopień krytyczności minerału zmienia się w czasie i zależy od potrzeb gospodarki, społeczeństwa oraz dostępności zasobów mineralnych. Fundamentalne pytanie brzmi: dla kogo dany minerał jest krytyczny? Każde państwo i sektor przemysłu mogą definiować ten termin odmiennie, z uwzględnieniem własnych kryteriów[10]. Chociaż wiele krajów i branż opiera się na tych samych minerałach w określonych zastosowaniach, to ich ogólne wymagania dotyczące minerałów mogą się znacznie różnić w zależności od specyfiki produktów i procesów produkcyjnych.

W 2023 r. rząd USA opublikował dokument *Critical Materials List*, w którym ocenił minerały pod kątem ich znaczenia dla globalnych łańcuchów dostaw technologii czystej energii, bezpieczeństwa narodowego oraz rozwoju gospodarczego. Według DOE minerał krytyczny to każdy minerał, pierwiastek, substancja lub materiał niebędący paliwem, który spełnia dwa kryteria: istnieje wysokie ryzyko zakłócenia dostaw oraz odgrywa istotną rolę w co najmniej jednej technologii w sektorze energetycznym[11]. Z tego powodu oprócz najczęściej używanych terminów „minerały krytyczne" lub „surowce krytyczne" funkcjonują także terminy „minerały strategiczne" i „minerały transformacji energetycznej"[12]. Na podstawie podanych dwóch kryteriów DOE zidentyfikował łącznie 50 minerałów krytycznych (tabela 1). W tym artykule autorka odnosi się do minerałów krytycznych dla transformacji energetycznej (ang. *critical materials for energy*[13]).

---

[9] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf, s. 5 [dostęp: 14 V 2024].

[10] L. Depraiter, S. Goutte, *The Role and Challenges of Rare Earths in the Energy Transition*, working papers, SSRN, 23 VI 2023 r., s. 7. http://dx.doi.org/10.2139/ssrn.4477111.

[11] U.S. Department of Energy, *Critical Materials Assessment 2023*, „Federal Register" 2024, t. 88, nr 149, https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16611.pdf, s. 51792 [dostęp: 16 XI 2024].

[12] M. Hendriwardani, I. Ramdoo, *Critical Minerals: A primer*, https://www.igfmining.org/wp-content/uploads/2022/11/critical-minerals-primer-en-WEB.pdf, s. 1 [dostęp: 13 XI 2024].

[13] Rozumienie pojęć „critical material" i „critical mineral" w ujęciu DOE zob. U.S. Department of Energy, *What Are Critical Materials and Critical Minerals?*, https://www.energy.gov/cmm/what-are-critical-materials-and-critical-minerals [dostęp: 17 I 2025] – przyp. red.

Tabela 1. Lista minerałów krytycznych według DOE (2023).

Minerały krytyczne	Minerały krytyczne dla transformacji energetycznej
aluminium, antymon, arsen, baryt, beryl, bizmut, cer, cez, chrom, cyna, cynk, cyrkon, dysproz, erb, europ, fluoryt, gadolin, gal, german, grafit, hafn, holm, ind, iryd, iterb, itr, kobalt, lantan, lit, lutet, magnez, mangan, neodym, nikiel, niob, pallad, platyna, prazeodym, rod, rubid, ruten, samar, skand, tantal, tellur, terb, tul, tytan, wanad, wolfram	aluminium, dysproz, fluor, gal, iryd, kobalt, krzem, lit, magnez, miedź, naturalny grafit, neodym, nikiel, platyna, prazeodym, stal elektryczna, terb, węglik krzemu

Źródło: opracowanie własne na podstawie: U.S. Department of Energy, *Critical Materials Assessment 2023*, „Federal Register" 2024, t. 88, nr 149, https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16611.pdf, s. 51792 [dostęp: 16 XI 2024]. Tłumaczenia w artykule pochodzą od autorki – dop. red.

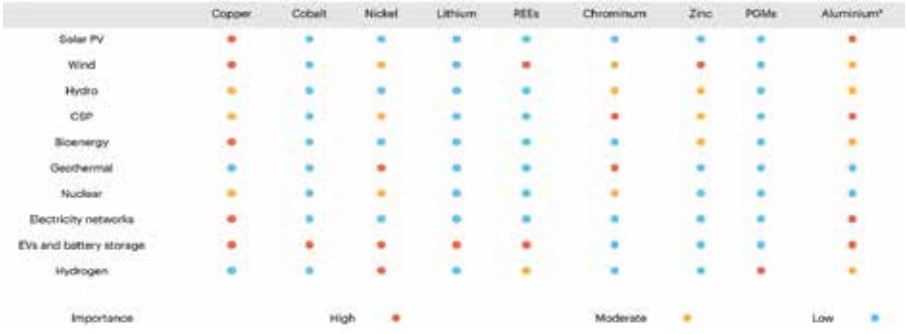
Ostateczna lista minerałów krytycznych obejmuje minerały ocenione jako *critical* (krytyczne), *near critical* (prawie krytyczne) lub *not critical* (niekrytyczne) w perspektywie średnioterminowej (2025–2035). Oceny te opierają się na dwóch kryteriach: znaczeniu dla sektora energetycznego oraz ryzyku związanym z ich dostępnością, które są szacowane na poziomach od niskiego do wysokiego (rysunek 1). Na przykład nikiel, platyna i iryd charakteryzują się zarówno wysokim ryzykiem dostaw, jak i dużym znaczeniem gospodarczym. Ich niedobór lub niestabilność na rynku mogą poważnie wpłynąć na rozwój technologii wodorowych oraz powiązanych branż, co może mieć konsekwencje dla całej gospodarki.

Rysunek 1. Ocena minerałów krytycznych pod względem ich znaczenia dla sektora energetycznego i dostępności w perspektywie średnioterminowej (2025–2035).

Źródło: U.S. Department of Energy, *What Are Critical Materials and Critical Minerals?*, https://www.energy.gov/cmm/what-are-critical-materials-and-critical-minerals [dostęp: 10 V 2024].

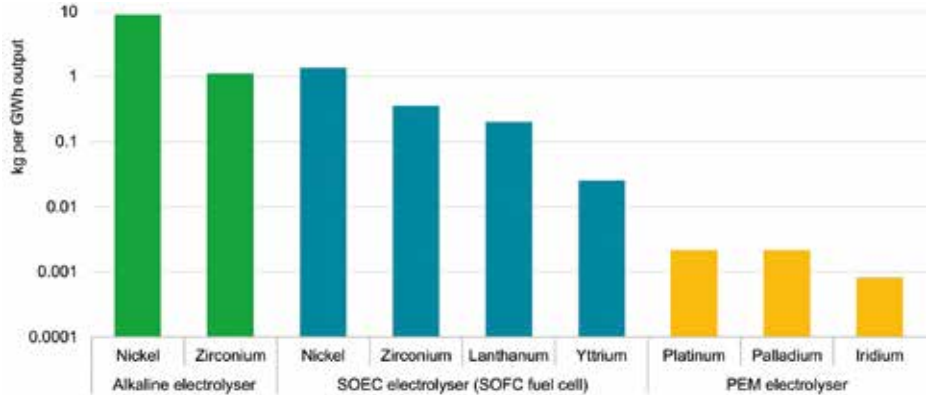
Zapotrzebowanie na minerały krytyczne do produkcji zielonego wodoru należy analizować w szerszym kontekście transformacji ku gospodarce niskoemisyjnej. Skala i rodzaj wymaganych minerałów zależą nie tylko od budowy elektrolizerów, lecz także od technologii OZE zasilających te urządzenia. Minerały są potrzebne do stworzenia infrastruktury przesyłowej, systemów magazynowania wodoru oraz ogniw paliwowych, które umożliwiają efektywne wykorzystanie wodoru jako nośnika energii. Istotnym elementem całego systemu są baterie magazynujące energię, które stabilizują dostawy z OZE i wspierają ciągłą pracę elektrolizerów. W tabeli 2 przedstawiono zapotrzebowanie na minerały krytyczne w różnych technologiach czystej energii. Część minerałów jest wykorzystywana w więcej niż jednej z nich, co może prowadzić do konkurencji o te same surowce. Ponadto rodzaj i ilość wymaganych minerałów różnią się w obrębie danej technologii.

Tabela 2. Zapotrzebowanie na minerały krytyczne w technologiach czystej energii.



Źródło: International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf, s. 45 [dostęp: 14 V 2024].

Zielony wodór jest wytwarzany w procesie elektrolizy wody, w którym są wykorzystywane elektrolizery oparte na minerałach krytycznych, takich jak: nikiel, cyrkon oraz metale z grupy platynowców (ang. *platinum group metals*, PGMs). Zapotrzebowanie na te surowce różni się w zależności od rodzaju elektrolizera – alkalicznego, PEM (ang. *proton exchange membrane*) lub SOEC (ang. *solid oxide electrolysis cell*), co zostało przedstawione na wykresie 1. Każdy z tych typów elektrolizerów ma specyficzne wymagania dotyczące minerałów, zależące od wydajności, skalowalności oraz warunków pracy danego elektrolizera.



Wykres 1. Szacunkowe zapotrzebowanie na minerały krytyczne dla trzech typów elektrolizerów.

Źródło: International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf, s. 111 [dostęp: 14 V 2024].

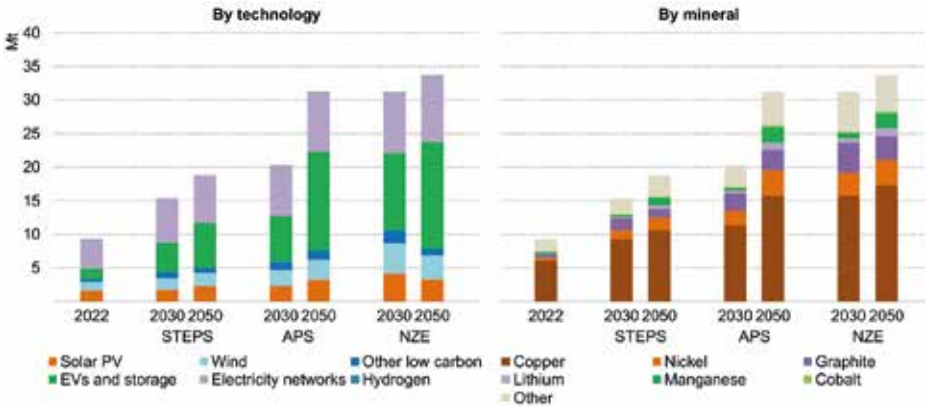
W elektrolizerze alkalicznym zapotrzebowanie na nikiel wynosi ok. 9 kg na każdą wyprodukowaną gigawatogodzinę (GWh) energii, a na cyrkon – ponad 1 kg na GWh. Z kolei elektrolizer stałotlenkowy (SOEC) ma niższe koszty materiałowe i wymaga ponad 1 kg niklu, 0,3 kg cyrkonu, 0,2 kg lantanowca oraz 0,02 kg itru na GWh produkcji. Elektrolizer z PEM potrzebuje najmniej minerałów krytycznych w porównaniu z innymi elektrolizerami: 0,002 kg platyny, 0,002 kg palladu i 0,001 kg irydu na GWh produkcji.

Kolejnym zagadnieniem jest zapotrzebowanie na minerały związane z budową OZE, które zasilają elektrolizery. Należy podkreślić, że całkowite zapotrzebowanie na minerały do produkcji energii odnawialnej znacznie przewyższa wymagania wynikające z budowy samych elektrolizerów. W przypadku morskich farm wiatrowych zapotrzebowanie na pierwiastki ziem rzadkich (ang. *rare earth elements*, REEs) jest szczególnie wysokie, głównie z uwagi na ich wykorzystanie w turbinach wiatrowych[14]. Do budowy tych turbin niezbędne są miedź, cynk, nikiel, chrom i aluminium. W produkcji paneli fotowoltaicznych duże znaczenie mają miedź i aluminium. Natomiast wytwarzanie pojazdów elektrycznych oraz systemów magazynowania energii w bateriach wymaga dużych ilości miedzi, kobaltu, niklu, litu, REEs oraz aluminium[15].

[14] J.E. Greenwald, M. Zhao, D.A. Wicks, *Critical mineral demands may limit scaling of green hydrogen production*, „Frontiers in Geochemistry" 2023, t. 1, s. 4. https://doi.org/10.3389/fgeoc.2023.1328384.

[15] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 45.

Rozwój technologii czystej energii, w tym zielonego wodoru, stanowi jeden z głównych czynników napędzających wzrost zapotrzebowania na minerały krytyczne, co wiąże się z dużymi wyzwaniami, które dotyczą zapewnienia stabilnych dostaw tych surowców. Międzynarodowa Agencja Energetyczna prognozuje, że do 2030 r. popyt na minerały krytyczne w sektorze energii odnawialnej może wzrosnąć nawet trzykrotnie. Analiza ta bazuje na trzech scenariuszach IEA (wykres 2): STEPS (Stated Policies Scenarios), APS (Announced Pledges Scenario) i NZE (Net Zero Emissions by 2050 Scenario)[16].



Wykres 2. Zapotrzebowanie na minerały krytyczne w technologii czystej energii w trzech scenariuszach IEA.

Źródło: International Energy Agency, *Critical Minerals Market Review 2023*, https://iea.blob.core.windows.net/assets/c7716240-ab4f-4f5d-b138-291e76c6a7c7/CriticalMineralsMarketReview2023.pdf, s. 63 [dostęp: 15 V 2024].

Wszystkie scenariusze wskazują na dynamiczny wzrost zapotrzebowania na minerały krytyczne. W scenariuszu APS prognozuje się, że do 2030 r. zapotrzebowanie wzrośnie ponaddwukrotnie, a do 2050 r. – aż trzykrotnie w porównaniu z poziomem z 2022 r. Z kolei w scenariuszu NZE, zakładającym szybsze tempo wdrażania technologii czystej energii, zapotrzebowanie na minerały krytyczne wzrośnie trzyipółkrotnie w stosunku do obecnych wartości, osiągnie poziom ponad 30 mln ton w 2030 r. i na tym poziomie utrzyma się również w 2050 r. Największy wpływ na ten wzrost mają pojazdy elektryczne oraz magazyny energii, ale

[16] International Energy Agency, *Critical Minerals Market Review 2023*, https://iea.blob.core.windows.net/assets/c7716240-ab4f-4f5d-b138-291e76c6a7c7/CriticalMineralsMarketReview2023.pdf, s. 65 [dostęp: 15 V 2024].

duży jest także wkład niskoemisyjnych źródeł energii i sieci elektroenergetycznych. W przypadku zielonego wodoru zapotrzebowanie na minerały krytyczne również będzie rosło, chociaż jego udział w całkowitym zapotrzebowaniu będzie mniejszy niż w przypadku innych technologii. Ponadto rozwój zielonego wodoru może napotkać trudności wynikające z ograniczonej dostępności REEs, których podaż jest obecnie silnie skoncentrowana w kilku regionach na świecie. Sytuację dodatkowo komplikuje rosnące zapotrzebowanie na te pierwiastki ze strony innych technologii czystej energii[17]. W przypadku elektrolizerów PEM zapotrzebowanie na iryd może przekroczyć w latach 40. XXI w. nawet 160% obecnej produkcji[18]. W związku z tym zapewnienie odpowiedniej podaży PGMs i REEs będzie poważnym wyzwaniem w skalowaniu produkcji zielonego wodoru.

Dostępność minerałów krytycznych i związana z tym geopolityka

Minerały krytyczne stają się coraz bardziej istotnym aspektem geopolityki, zwłaszcza w kontekście rosnącej rywalizacji między Stanami Zjednoczonymi a Chinami[19]. Głównym punktem tej rywalizacji jest strategiczna dominacja Chin nad łańcuchami dostaw minerałów krytycznych, co ma znaczący wpływ na politykę globalną[20]. Chiny produkują ponad 60% światowych zasobów REEs i posiadają niemal wszystkie zakłady rafinacji tych surowców. Inne państwa również zyskały dominującą pozycję w produkcji i wydobyciu najważniejszych minerałów, co zapewnia im przewagę strategiczną oraz przyciąga inwestorów. Przykładami są Demokratyczna Republika Konga (DRK) mająca 74-procentowy udział w globalnej produkcji kobaltu, Republika Południowej Afryki (RPA) produkująca 67% platyny, oraz Indonezja, na którą przypada 50% światowej produkcji niklu (tabela 3). Wiadome jest, że gdy zaopatrzenie w dany surowiec zależy od jednego państwa, łańcuch dostaw staje się bardziej podatny na zakłócenia niż wtedy, gdy źródeł jest kilka. Niektóre minerały, np. lit, są szeroko dostępne i mogą być pozyskiwane z różnych krajów, np.: Australii, Chile, Chin, Argentyny i Brazylii[21].

---

17 J.E. Greenwald, M. Zhao, D.A. Wicks, *Critical mineral demands*…, s. 1.

18 S. Moreira, T.J. Laing, *Sufficiency, sustainability, and circularity of critical materials for clean hydrogen*, Washington 2022, s. 10.

19 S. Kalantzakos, *The Race for Critical Minerals in an Era of Geopolitical Realignments*, „The International Spectator" 2020, t. 55, nr 3. https://doi.org/10.1080/03932729.2020.1786926.

20 Mo Ibrahim Foundation, *Africa's critical minerals: Africa at the heart of a low-carbon future*, https://mo.ibrahim.foundation/sites/default/files/2022-11/minerals-resource-governance.pdf, s. 2 [dostęp: 14 V 2024].

21 International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 30.

Tabela 3. Najwięksi producenci i największe rezerwy wybranych minerałów na świecie (2023).

Minerał krytyczny	Kraj o największej produkcji	Udział kraju w światowej produkcji (%)	Kraj z największymi zasobami	Udział kraju w światowych zasobach (%)
Platyna	RPA	67%	RPA	89%* (wszystkie PGMs)
Pallad	Rosja	44%	RPA	89%* (wszystkie PGMs)
Nikiel	Indonezja	50%	Indonezja	42%
Cyrkon	Australia	31%	Australia	74%
REEs	Chiny	69%	Chiny	40%
Kobalt	DRK	74%	DRK	55%
Grafit	Chiny	77%	Chiny	28%
Chrom	RPA	44%	Kazachstan	41%
Mangan	RPA	36%	RPA	32%
Boksyt	Australia	25%	Gwinea	25%
Miedź	Chile	23%	Chile	19%

Źródło: opracowanie własne na podstawie: U.S. Geological Survey, *Mineral Commodity Summaries 2024*. https://doi.org/10.3133/mcs2024.

Rozwój technologii zielonego wodoru opiera się na takich surowcach, jak PGMs i nikiel. Technologia PEM, zyskująca na znaczeniu w tym sektorze, wymaga zastosowania katalizatorów opartych na platynie i irydzie. Republika Południowej Afryki posiada aż 89% światowych rezerw PGMs, co czyni ją dominującym graczem. Natomiast technologia alkaliczna, w której jest używany nikiel, opiera się głównie na zasobach z Indonezji i Filipin. W kontekście transformacji energetycznej kobalt odgrywa najważniejszą rolę w produkcji baterii litowo-jonowych, wykorzystywanych w pojazdach elektrycznych, magazynowaniu energii oraz turbinach wiatrowych. Demokratyczna Republika Konga ma aż 55% światowych rezerw kobaltu i odpowiada za ponad 70% jego globalnej podaży. Na RPA przypada 44% globalnej produkcji chromu, stosowanego w technologiach energii słonecznej, geotermalnej, jądrowej, wodnej i wiatrowej, oraz ponad 32% światowych rezerw manganu, wykorzystywanego w odnawialnych źródłach energii, pojazdach elektrycznych

i magazynach energii[22]. Boksyt, podstawowy surowiec do produkcji aluminium, ma znaczenie w technologii niskoemisyjnej, zwłaszcza w ogniwach fotowoltaicznych[23]. Jedną czwartą światowych rezerw boksytu dysponuje Gwinea i jednocześnie jest drugim na świecie jego producentem, zaraz po Australii. Miedź, wykorzystywana w OZE, występuje w dużych ilościach w Chile, RPA i DRK. Złoża miedzi znajdują się również w Mauretanii, Mali, Maroku i Egipcie. Grafit, ważny składnik baterii litowo-jonowych stosowanych w pojazdach elektrycznych oraz systemach magazynowania energii, jest w dużej mierze produkowany w Chinach, ale także w Madagaskarze i Mozambiku, które zajmują odpowiednio drugie i trzecie miejsce na świecie pod względem produkcji tego surowca[24].

Z perspektywy geopolitycznej dominacja krajów afrykańskich w dostarczaniu surowców niezbędnych do produkcji technologii zielonego wodoru może znacznie zwiększyć ich znaczenie na arenie międzynarodowej, zwłaszcza w kontekście globalnej transformacji energetycznej. Rosnąca zależność od afrykańskich surowców wiąże się z nasileniem rywalizacji międzynarodowej o dostęp do tych zasobów[25]. Co więcej, wydobycie minerałów kluczowych dla transformacji energetycznej jest obecnie bardziej skoncentrowane geograficznie niż wydobycie ropy naftowej czy gazu ziemnego. W związku z tym nowy, zeroemisyjny system energetyczny może stać się bardziej podatny na niestabilność polityczną, ryzyko geopolityczne oraz ograniczenia eksportowe. Jak pokazuje wykres 3, przetwarzanie tych minerałów jest jeszcze bardziej skoncentrowane geograficznie niż ich wydobycie. W tej dziedzinie dominująca rola przypada Chinom.

Długoterminowa strategia Chin mająca na celu przejęcie kontroli nad całym łańcuchem dostaw rozpoczęła się już w 1992 r., kiedy zaczęły one nadawać priorytetowe znaczenie surowcom krytycznym. Polityka inwestowania w zagraniczne projekty wydobywcze skutecznie umacniała ich pozycję w tym sektorze[26]. Chociaż Australia i Chile odpowiadają za 70% światowej produkcji litu, to chińskie firmy państwowe kontrolują aż jedną trzecią tego rynku, głównie dzięki dominacji w sektorze rafinacji. W DRK, gdzie produkuje się prawie 70% światowego kobaltu,

[22] Mo Ibrahim Foundation, *Africa's critical minerals*…, s. 3–4 [dostęp: 14 V 2024].

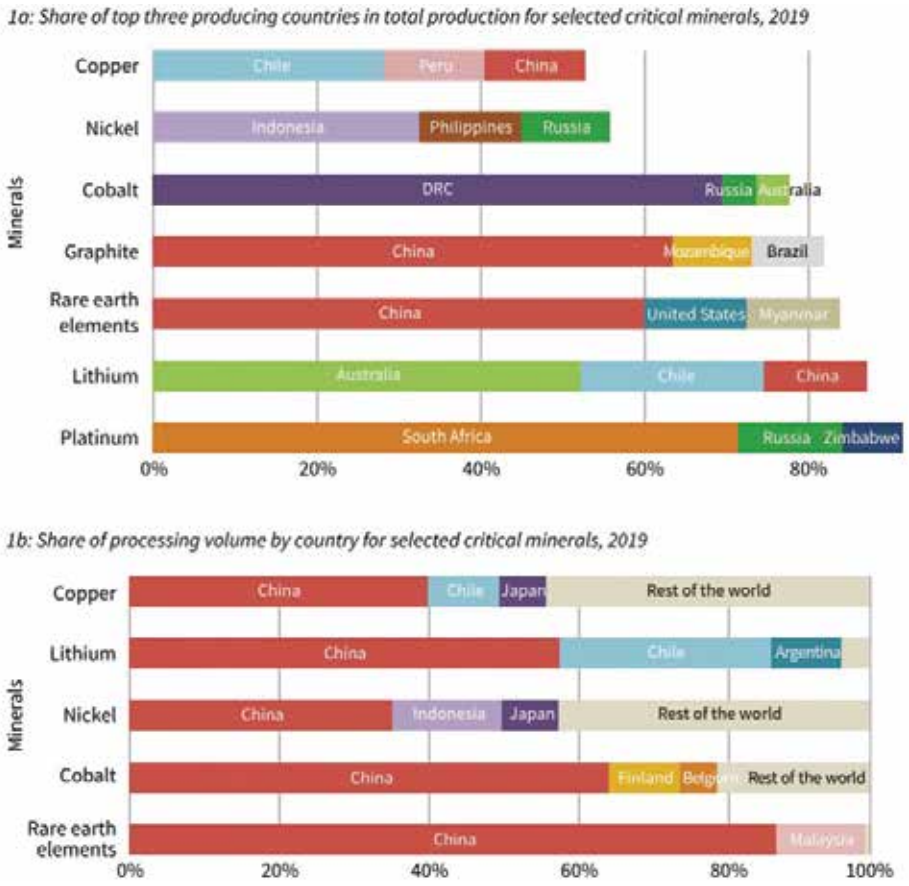
[23] P. Bosse i in., *The minerals essential to the energy and digital transitions: An opportunity for Africa?*, Agence Française de Développement, https://www.afd.fr/en/ressources/minerals-essential-energy-and-digital-transitions-opportunity-africa [dostęp: 14 V 2024].

[24] U.S. Geological Survey, *Mineral Commodity Summaries 2024*. https://doi.org/10.3133/mcs2024.

[25] J. Noailly i in., *The role of critical materials for the energy transition. Challenges and opportunities*, „Swiss Academies Reports" 2024, t. 19, nr 3, s. 5–6. https://doi.org/10.5281/zenodo.12168441.

[26] W.M. Morrison, R. Tang, *China's Rare Earth Industry and Export Regime: Economic and Trade Implications for the United States*, Washington 2012, https://digital.library.unt.edu/ark:/67531/metadc85418/, s. 1 [dostęp: 12 XI 2024].

chińskie przedsiębiorstwa kontrolują aż 80% jego wydobycia. Chiny inwestują także w rozwój przemysłu mineralnego w Indonezji. W 2024 r. chińskie firmy kontrolowały w tym kraju 82% produkcji niklu wykorzystywanego w bateriach[27].



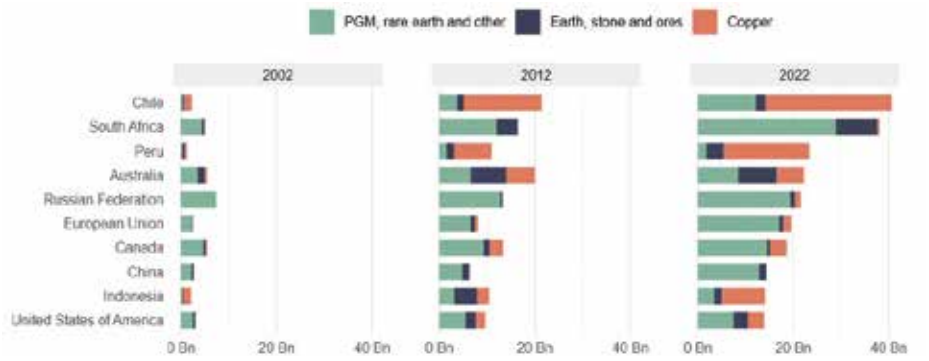
Wykres 3. Udział krajów w całkowitej produkcji i ilości przetworzonych minerałów krytycznych (2019).

Źródło: International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf, s. 30–31 [dostęp: 14 V 2024].

Rozwój rynku surowców krytycznych i związane z nim inwestycje wpływają na nowe dynamiki geopolityczne i zmianę globalnego układu sił. Zgodnie z danymi

[27] E. Kaboli, *Critical Minerals and Materials for Selected Energy Technologies*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R48149, s. 8 [dostęp: 12 XI 2024].

WTO w 2022 r. Chile miało 11% udziału i zajmowało pierwsze miejsce w globalnym eksporcie surowców krytycznych, a RPA, Peru, Australia i Rosja miały po ok. 6% światowego eksportu, co przedstawia wykres 4[28].



Wykres 4. Najwięksi eksporterzy minerałów krytycznych w latach 2002, 2012 i 2022 (w mld dolarów).

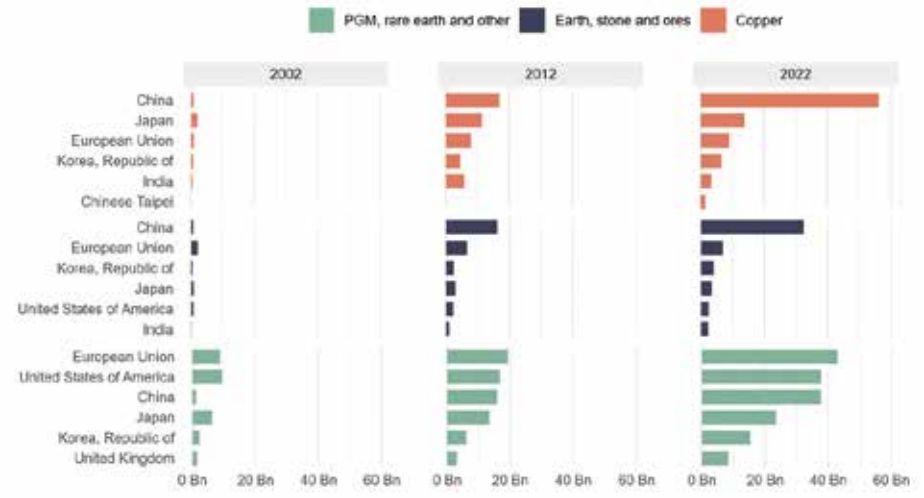
Źródło: M. Snoussi-Mimouni, S. Avérous, *High demand for energy-related critical minerals creates supply chain pressures*, World Trade Organization, 10 I 2024 r., https://www.wto.org/english/blogs_e/data_blog_e/blog_dta_10jan24_e.htm [dostęp: 12 V 2024].

Najczęściej eksportowanymi minerałami krytycznymi na świecie są miedź, PGMs oraz REEs. W eksporcie miedzi liderem jest Chile, odpowiadające za ponad jedną czwartą jej światowego eksportu. Na kolejnych miejscach są Peru (19%) i Indonezja (9%). Republika Południowej Afryki jest natomiast głównym eksporterem metali PGMs, REEs oraz innych minerałów niezbędnych do rozwoju technologii zielonego wodoru. W 2022 r. miała ona ok. 14% udziału w globalnym rynku. Wzrost znaczenia krajów eksportujących surowce krytyczne może spowodować dalsze zmiany w równowadze geopolitycznej na świecie.

Z drugiej strony, jak wynika z badania WTO, nie wszystkie kraje dysponują wystarczającymi rezerwami surowców mineralnych do ich wydobycia i eksportu. W związku z tym wiele państw jest uzależnionych od importu minerałów krytycznych, aby zaspokoić swoje potrzeby. Koncentracja produkcji rodzi obawy o potencjalne ograniczenia eksportowe oraz niestabilność geopolityczną, zwłaszcza w kontekście transformacji energetycznej. Sytuacja jest szczególnie problematyczna dla krajów UE, która niemal w całości polega na imporcie surowców

[28] M. Snoussi-Mimouni, S. Avérous, *High demand for energy-related critical minerals creates supply chain pressures*, World Trade Organization, 10 I 2024 r., https://www.wto.org/english/blogs_e/data_blog_e/blog_dta_10jan24_e.htm [dostęp: 12 V 2024].

z Chin. Dotyczy to zwłaszcza ogniw fotowoltaicznych, gdyż w skali globalnej UE wytwarza jedynie 4% surowców i 12% przetworzonych materiałów. Jeszcze trudniej jest w przypadku baterii litowo-jonowych, dlatego że udział UE w globalnej produkcji to zaledwie 2% surowców i 4% przetworzonych materiałów[29]. Analogicznie jak w eksporcie, najczęściej importowanymi minerałami są miedź, PGMs i REEs. Jak pokazuje wykres 5, Chiny importują znacznie więcej miedzi niż jakiekolwiek inne państwo i są największym importerem 13 z 17 minerałów z kategorii „Earth, stone and ore minerals"[30]. Z kolei UE jest największym importerem PGMs, REEs oraz innych minerałów i wyprzedza pod tym względem Stany Zjednoczone, Chiny i Japonię.



Wykres 5. Najwięksi importerzy minerałów krytycznych w latach 2002, 2012 i 2022 (w mld dolarów).

Źródło: M. Snoussi-Mimouni, S. Avérous, *High demand for energy-related critical minerals creates supply chain pressures*, World Trade Organization, 10 I 2024 r., https://www.wto.org/english/blogs_e/data_blog_e/blog_dta_10jan24_e.htm [dostęp: 12 V 2024].

[29] J. Noailly i in., *The role of critical materials*…, s. 6.

[30] „Earth, stone and ore minerals" – surowce obejmujące minerały przemysłowe, rudy metali oraz surowce skalne, takie jak: glina, fosforyty, skały budowlane i inne zasoby geologiczne wykorzystywane w zaawansowanych technologiach, przemyśle chemicznym oraz budownictwie.

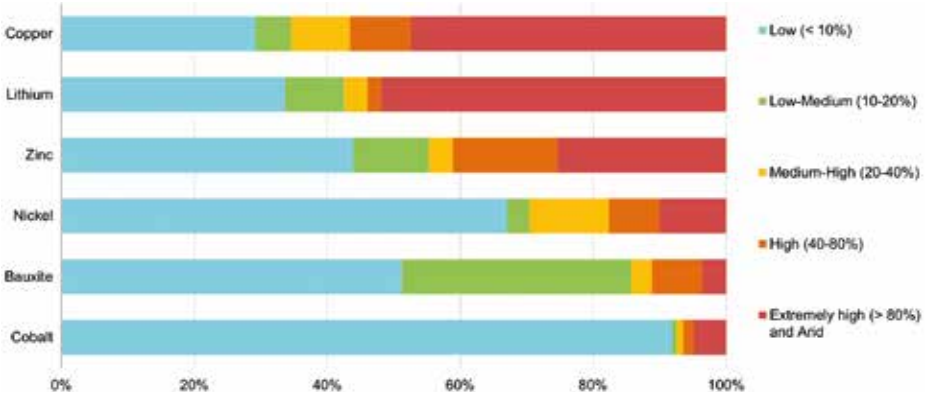
Wyzwania związane z łańcuchem dostaw minerałów krytycznych

Obawy dotyczące zmienności cen oraz bezpieczeństwa dostaw pozostają aktualne w nowoczesnym systemie energetycznym opartym na zielonym wodorze, elektryfikacji i odnawialnych źródłach energii. Fundamentalnym problemem jest wysoka koncentracja geograficzna produkcji tych minerałów, która w znacznym stopniu wpływa zarówno na ich dostępność, jak i wahania cen. Kraje członkowskie UE oraz USA są w dużym stopniu uzależnione od importu minerałów krytycznych, takich jak platyna, iryd czy nikiel, z RPA i Chin. Ta zależność stwarza zagrożenie dla stabilności dostaw w sektorze zielonego wodoru. Ponadto można wskazać cztery dodatkowe czynniki zwiększające ryzyko zawężenia rynku oraz cyklicznych wahań cen, które mogą spowolnić transformację energetyczną. Należą do nich: wysoka ekspozycja na ryzyko klimatyczne, spadek jakości zasobów mineralnych, problemy środowiskowe związane z wydobyciem oraz nierównowaga między podażą a popytem na minerały krytyczne[31].

W kontekście zwiększającego się ryzyka zmian klimatycznych szybko rozwijające się rynki minerałów krytycznych znajdujące się w Australii, Chinach i państwach afrykańskich są szczególnie narażone na zakłócenia spowodowane zjawiskami fizycznymi, takimi jak ekstremalne upały, powodzie czy trzęsienia ziemi. Jednym z najpoważniejszych zagrożeń pozostaje wysoki poziom stresu wodnego (ang. *water stress*) w krajach będących głównymi producentami minerałów krytycznych. Niedobór wody stanowi poważną barierę w wydobyciu, przetwarzaniu i dystrybucji tych surowców. Miedź i lit charakteryzują się szczególnie wysokim zapotrzebowaniem na wodę w procesach technologicznych, co czyni te procesy bardziej podatnymi na skutki niedoborów wody. Obecnie ponad 50% globalnej produkcji miedzi i litu jest zlokalizowane na obszarach dotkniętych wysokim poziomem stresu wodnego, co znacznie zwiększa ryzyko zakłóceń w ich dostępności i wpływa na stabilność globalnych łańcuchów dostaw (wykres 6)[32].

[31] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 11–12.

[32] Tamże, s. 12.



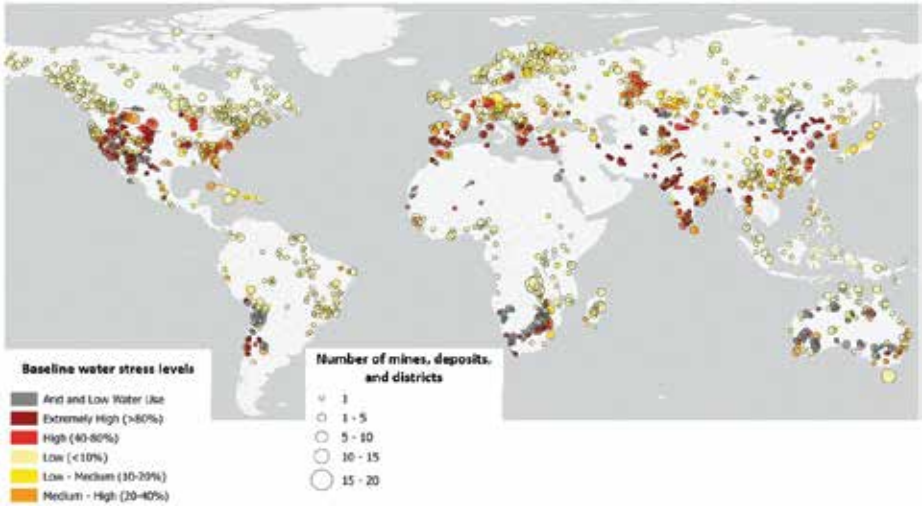
Wykres 6. Procentowy udział produkcji wybranych minerałów krytycznych w odniesieniu do poziomu stresu wodnego w 2020 r.

Źródło: International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf, s. 128 [dostęp: 14 V 2024].

Zgodnie z analizą przeprowadzoną przez World Resources Institute w 2023 r. co najmniej 16% kopalń, złóż i obszarów wydobycia najważniejszych minerałów znajdowało się w regionach świata, gdzie niedobór wody jest wysoki lub bardzo wysoki (rysunek 2). Niedobór ten jest szczególnie dotkliwy w krajach południowej Afryki, w tym w RPA, skąd pochodzi większość eksportowanych PGMs oraz REEs. Demokratyczna Republika Konga, największy producent kobaltu na świecie, oraz Chile, największy światowy eksporter miedzi, również są zaniepokojone poziomem konsumpcji wody i zanieczyszczeniem środowiska[33]. Międzynarodowa Agencja Energetyczna prognozuje, że odsetek kopalń zlokalizowanych na obszarach dotkniętych wysokim niedoborem wody będzie wzrastać[34].

[33] S. Lakshman, *More Critical Minerals Mining Could Strain Water Supplies in Stressed Regions*, World Resources Institute, 10 I 2024 r., https://www.wri.org/insights/critical-minerals-mining-water-impacts [dostęp: 13 V 2024].

[34] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 131.



Rysunek 2. Kopalnie, złoża i obszary wydobycia minerałów na świecie oraz poziom stresu wodnego.

Źródło: S. Lakshman, *More Critical Minerals Mining Could Strain Water Supplies in Stressed Regions*, World Resources Institute, 10 I 2024 r., https://www.wri.org/insights/critical-minerals-mining-water-impacts [dostęp: 13 V 2024].

Następny czynnik ryzyka to pogarszająca się jakość surowców mineralnych. W ostatnich latach jakość rud mineralnych systematycznie spada, co jest spowodowane wcześniejszą eksploatacją złóż o wyższej zawartości metalu. Do istnienia tego trendu dodatkowo przyczynia się postęp technologiczny umożliwiający eksploatację złóż o niższych parametrach. W przypadku kopalni miedzi średnia zawartość metalu w rudzie zmniejszyła się na świecie o ok. 25% w ciągu zaledwie 10 lat[35]. W Chile zawartość miedzi w rudzie obniżyła się aż o 30% w ciągu ostatnich 15 lat. Pogorszenie jakości rud skutkuje koniecznością zużycia większej ilości energii do pozyskania metalu, co z kolei zwiększa koszty produkcji, emisję gazów cieplarnianych i ilość odpadów[36].

Kolejnym negatywnym czynnikiem jest znaczny wzrost zapotrzebowania na surowce krytyczne. Ich wydobycie i transport prowadzą bowiem do wielu problemów środowiskowych, takich jak: zanieczyszczenie powietrza, skażenie wody i gleby toksycznymi substancjami, degradacja krajobrazu, utrata bioróżnorodności oraz nadmierna produkcja odpadów. Procesy te mają również niekorzystne skutki społeczne. Jednym

[35] G. Calvo i in., *Decreasing Ore Grades in Global Metallic Mining: A Theoretical Issue or a Global Reality?*, „Resources" 2016, t. 5, nr 4, 36. https://doi.org/10.3390/resources5040036.

[36] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 12.

z problemów jest wydawanie przez państwa licencji na wydobycie surowców prywatnym firmom, co często prowadzi do naruszenia praw lokalnych społeczności do ziemi[37].

Ryzyko wiąże się także z niedopasowaniem tempa zmian w strukturze popytu na minerały krytyczne do tempa rozwoju nowych projektów wydobywczych. Skutkiem tego jest duża zmienność cen na rynku tych surowców. Główne źródło zróżnicowania popytu wynika z niepewności związanej z ambitnymi celami klimatycznymi, które są ogłaszane i przyjmowane na poziomie międzynarodowym. Brak pewności co do scenariuszy przyszłości może stanowić barierę w podejmowaniu przez przedsiębiorstwa decyzji inwestycyjnych, co w nadchodzących latach może prowadzić do nierównowagi między podażą a popytem. Na przykład w najbliższym czasie oczekuje się nadwyżki podaży litu i kobaltu, a w przypadku wodorotlenku litu, niklu oraz niektórych REEs (np. neodymu i dysprozu) mogą z kolei wystąpić problemy z podażą z powodu wzrostu popytu[38].

Działania na rzecz poprawy bezpieczeństwa w łańcuchu dostaw minerałów krytycznych

W odpowiedzi na rosnące ryzyko związane z uzależnieniem od eksportu minerałów krytycznych z kilku krajów konieczne stanie się zdywersyfikowanie źródeł dostaw. Unia Europejska i Stany Zjednoczone powinny przyspieszyć rozwój alternatywnych źródeł surowców oraz inwestować w technologie recyklingu, aby zmniejszyć zależność od obecnych liderów rynku. Taka dywersyfikacja nie tylko poprawi stabilność łańcuchów dostaw, lecz także wesprze rozwój zielonego wodoru i innych technologii energetycznych. Zmniejszy to wpływ decyzji politycznych innych krajów na dostępność surowców.

W tym kontekście bardzo duże znaczenie mają innowacje technologiczne. Nowoczesne technologie wydobycia, optymalizacja procesów produkcyjnych, zmniejszenie zużycia materiałów oraz wprowadzenie nowych surowców mogą istotnie wpłynąć na redukcję zapotrzebowania na minerały. Przykładem może być rozwój baterii litowo-żelazowo-fosforanowych (oznaczanych jako LiFePO4 czy LFP), które ograniczają zależność od kobaltu i niklu[39]. Podobne innowacje pojawiające w innych sektorach, m.in. w ogniwach słonecznych i technologiach wodorowych, mogą

[37] M. Sengupta, *Environmental Impacts of Mining: Monitoring, Restoration, and Control*, wyd. 2, CRC Press 2021. https://doi.org/10.1201/9781003164012.

[38] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 120.

[39] R. Zilli, J. André, S. Bellucci, *Policy analysis: Securing sustainable critical raw material supply for clean energy in Europe*, European Energy Research Alliance 2023, https://www.eera-set.eu/component/attachments/?task=download&id=1235:EERA_Policy_Analysis_on_Critical_Raw_Materials_Layout_Digital-for-publication, s. 16 [dostęp: 13 V 2024].

zmniejszyć presję na zasoby naturalne. Przykładem może być zredukowanie o 40–50% w ciągu ostatnich dziesięciu lat zużycia srebra i krzemu w ogniwach słonecznych, co umożliwiło spektakularny wzrost ich wykorzystania. Dzięki ciągłemu doskonaleniu i usprawnianiu technologii elektrolizerów oczekuje się z kolei, że w następnej dekadzie zmniejszy się o połowę zapotrzebowanie na nikiel, cyrkon, aluminium, stal, platynę, iryd, lantan oraz itr[40]. W ramach prac badawczo-rozwojowych są prowadzone również badania nad innowacyjnymi rozwiązaniami, takimi jak magnesy trwałe niezawierające pierwiastków ziem rzadkich (REE-free), elektrolizery z membranami anionowymi niewymagającymi PGMs (PGM-free AEM) oraz integracja elektrolizy wody z alternatywnymi źródłami ciepła. Wdrożenie tych technologii może nie tylko poprawić efektywność energetyczną i materiałową produkcji zielonego wodoru, lecz także obniżyć jej koszty oraz zminimalizować negatywny wpływ na środowisko[41].

Oprócz innowacji technologicznych drugim elementem strategii ograniczania presji na zasoby naturalne jest rozwój efektywnych systemów recyklingu. Recykling zużytych produktów, zwłaszcza baterii, elektroniki czy komponentów energetycznych, pozwala na odzyskiwanie cennych surowców i zmniejszenie zapotrzebowania na nowe zasoby. Wdrożenie skutecznych systemów recyklingu, wspieranych normami dotyczącymi śladów węglowych materiałów, mogłoby poprawić ekonomiczną opłacalność tego procesu i sprawić, że stanie się on konkurencyjny wobec tradycyjnego wydobycia. Integracja tych rozwiązań z innowacjami w projektowaniu produktów o dłuższej trwałości i mniejszym zapotrzebowaniu na minerały może w dłuższej perspektywie zmniejszyć globalną presję na zasoby[42].

Ograniczenie zapotrzebowania na wydobycie minerałów krytycznych ma także pozytywny wpływ na zmniejszenie zużycia wody, co z kolei pomoże zredukować ryzyko lokalnych konfliktów o zasoby wodne i wesprze stabilność energetyczną w tych regionach. W rezultacie wdrożenie zrównoważonych strategii zarządzania wodą powinno stać się priorytetem dla organów odpowiedzialnych za politykę wodną i energetyczną. Należy również prowadzić dialog z lokalnymi społecznościami, które często borykają się z problemem zanieczyszczenia wód lub ich niedoboru. Uwzględnienie ich opinii w procesach decyzyjnych może przyczynić się do opracowania bardziej zrównoważonych praktyk, co zwiększy akceptację dla projektów wydobywczych. Takie podejście sprzyja efektywnemu zarządzaniu zasobami wodnymi i wspiera długoterminową stabilność łańcuchów dostaw.

Pomimo wdrożenia strategii dywersyfikacji dostaw, innowacji technologicznych oraz efektywnego recyklingu wciąż istnieje wyzwanie związane z nierównowagą

[40] International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*…, s. 14, 113.

[41] J.E. Greenwald, M. Zhao, D.A. Wicks, *Critical mineral demands*…, s. 5.

[42] J. Noailly i in., *The role of critical materials*…, s. 8.

między podażą a popytem na minerały krytyczne. Aby sprostać temu problemowi, niezmiernie ważne będzie zapewnienie przez rządy jasnych i stabilnych sygnałów dotyczących transformacji energetycznej. Polityka wspierająca inwestycje w sektor wydobycia oraz alternatywne źródła surowców będzie miała decydujący wpływ na przyszły rozwój rynku surowców. Jeśli przedsiębiorstwa nie będą miały zaufania do polityki energetycznej i klimatycznej poszczególnych krajów, podejmą decyzje inwestycyjne na podstawie bardziej zachowawczych prognoz. Może to spowolnić rozwój i utrudnić w przyszłości zapewnienie stabilności w łańcuchach dostaw minerałów. Podsumowując, tylko zintegrowana polityka wspierająca dywersyfikację źródeł, innowacje technologiczne oraz efektywny recykling może zapewnić bezpieczeństwo energetyczne państwa, zmniejszyć ryzyko kryzysów energetycznych i wzmocnić stabilność rynku surowców w perspektywie długoterminowej.

Zielony wodór a bezpieczeństwo wodne

Wykorzystanie wody oraz problem wysokiego poziomu stresu wodnego dotyczą nie tylko jej użycia w procesie wydobycia i przetwarzania minerałów krytycznych, lecz także produkcji zielonego wodoru. Do wytwarzania GH_2 stosuje się elektrolizery, które wymagają ultraczystej wody. Wysoki poziom czystości jest niezbędny ze względu na negatywny wpływ zanieczyszczeń (korozja sprzętu i powstawanie chloru) na trwałość stosu elektrolizera. Warto poznać dokładne zapotrzebowanie na wodę konieczną do produkcji zielonego wodoru, aby lepiej rozumieć wpływ tego procesu na zasoby wodne[43].

Elektroliza wody charakteryzuje się najmniejszym śladem wodnym spośród wszystkich procesów produkcji wodoru. Do wyprodukowania 1 kg wodoru potrzeba 9 kg wody. Dla porównania, produkcja wodoru z gazu ziemnego z zastosowaniem technologii wychwytywania i składowania dwutlenku węgla (ang. *carbon capture, utilization and storage*) zużywa od 13 do 18 kg wody na 1 kg wodoru, a proces zgazowania węgla wymaga od 40 do 86 kg wody na 1 kg wodoru, w zależności od zużycia wody przy wydobyciu węgla. Jeśli uwzględni się straty i nieefektywność procesu elektrolizy, trzeba przyjąć, że do wyprodukowania 1 kg wodoru potrzeba ok. 20 kg wody. Aby zobrazować wpływ produkcji zielonego wodoru na dostępność wody, można podać przykład elektrolizera o mocy 1 GW, który działa z efektywnością 75-procentową przez 8000 godzin rocznie (ok. 11 miesięcy) i produkuje 150 000 ton

[43] European Patent Office, International Renewable Energy Agency, *Patent insight report: Innovation trends in electrolysers for hydrogen production*, https://link.epo.org/web/patent_insight_report_innovation_trends_for_electrolysers_in_hydrogen_production_en.pdf, s. 5 [dostęp: 14 XI 2024].

wodoru. Przy zużyciu 20 kg wody na każdy kilogram wodoru proces ten pochłania ok. 3 mln ton wody rocznie. To odpowiada mniej więcej rocznemu zużyciu wody przez miasto liczące 70 000 mieszkańców[44]. W regionach, gdzie dostęp do wody jest ograniczony, takie zużycie może prowadzić do poważnych problemów, zwłaszcza w przypadku braku zrównoważonego zarządzania zasobami wodnymi.

Regiony o największym potencjale energii odnawialnej i przestrzeni do instalowania zakładów produkujących zielony wodór to jednocześnie obszary, w których problem niedoboru wody staje się coraz bardziej krytyczny. Całkowita roczna zdolność produkcyjna istniejących i działających zakładów produkujących zielony i niebieski wodór na świecie wynosi 1,7 Mt, z czego ok. 12% znajduje się na obszarach o wysokim deficycie wody. Planowane projekty w jeszcze większym stopniu będą narażone na problemy związane z jej niedoborem. Według zapowiedzi do 2030 r. 40% globalnej produkcji wodoru wytwarzanego metodą elektrolizy będzie zlokalizowane w regionach dotkniętych deficytem wody[45] (rysunek 3).

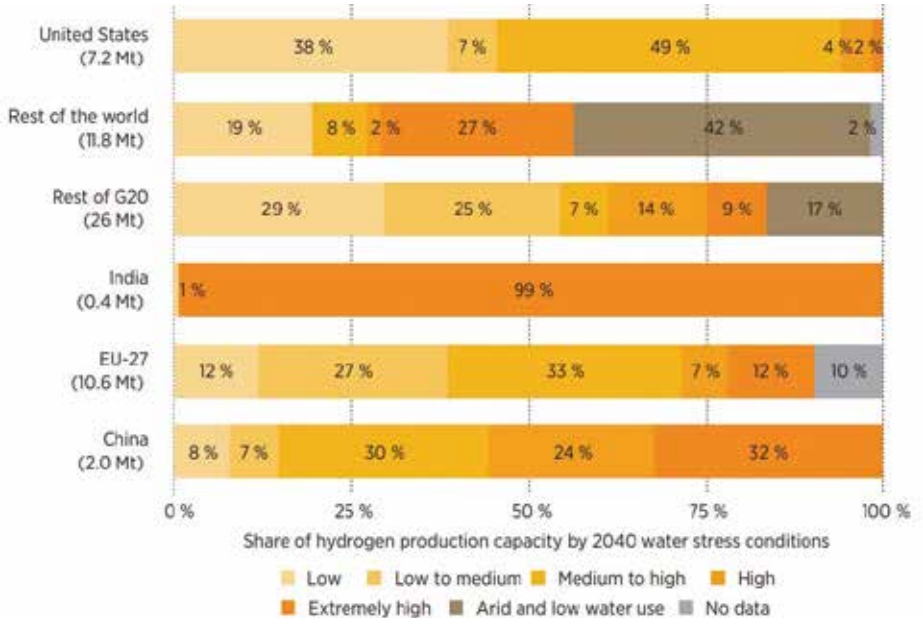
Rysunek 3. Planowane projekty elektrolizerów do produkcji zielonego wodoru oraz poziomy niedoboru wody do 2030 r.

Źródło: International Energy Agency, *Global Hydrogen Review 2024*, https://iea.blob.core.windows.net/assets/89c1e382-dc59-46ca-aa47-9f7d41531ab5/GlobalHydrogenReview2024.pdf, s. 91 [dostęp: 16 XI 2024].

[44] Tamże.

[45] International Renewable Energy Agency, Bluerisk, *Water for hydrogen production*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Dec/IRENA_Bluerisk_Water_for_hydrogen_production_2023.pdf, s. 38 [dostęp: 6 XI 2024].

Znaczna część planowanych mocy w zakresie produkcji zielonego wodoru ma być zlokalizowana w Australii, Europie Zachodniej, Azji Środkowej, Afryce Zachodniej oraz na Bliskim Wschodzie, przy czym wszystkie te regiony, z wyjątkiem Europy Zachodniej, borykają się z umiarkowanym lub wysokim deficytem wody. W Stanach Zjednoczonych projekty związane z produkcją zielonego i niebieskiego wodoru są w niewielkim stopniu narażone na problemy związane z jej niedoborem, jednak w pozostałych krajach G20 oraz w 71% państw reszty świata ponad 40% istniejących i planowanych mocy produkcyjnych znajduje się na obszarach o wysokim deficycie wody. Szczegółowy rozkład globalnych mocy produkcyjnych wodoru, zarówno istniejących, jak i planowanych, w zależności od poziomu niedoboru wody w 2040 r. i regionu, został przedstawiony na wykresie 7.



Wykres 7. Rozkład globalnych mocy produkcyjnych zielonego i niebieskiego wodoru (istniejących i planowanych) według poziomu deficytu wody w 2040 r.

Źródło: International Renewable Energy Agency, Bluerisk, *Water for hydrogen production*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Dec/IRENA_Bluerisk_Water_for_hydrogen_production_2023.pdf, s. 41 [dostęp: 6 XI 2024].

Niedobór wody stanowi jedno z największych wyzwań w kontekście rozwoju projektów wodorowych, zarówno w regionach, gdzie dostęp do niej już jest ograniczony, jak i w miejscach, które w przyszłości mogą zostać dotknięte suszami

w wyniku zmian klimatycznych. W celu przezwyciężenia tego problemu realizatorzy projektów wodorowych powinni rozważyć wykorzystanie różnych źródeł wody, tj. wód gruntowych, powierzchniowych, ścieków oraz wody morskiej.

Bardzo obiecującą strategią w obliczu niedoboru zasobów wodnych jest odsalanie wody morskiej. Chociaż wiąże się to z kosztami inwestycyjnymi, to stanowią one stosunkowo niewielką, wynoszącą zazwyczaj poniżej 2%, część całkowitych wydatków ponoszonych na realizację projektów wodorowych. Najczęściej wykorzystywany proces odsalania, jakim jest odwrócona osmoza, potrzebuje ok. 3–6 kWh energii elektrycznej na każdy metr sześcienny wody, co zwiększa koszt produkcji wodoru jedynie o ok. 0,05 dolara/kg[46].

Warto zaznaczyć, że obecna globalna zdolność produkcyjna zakładów odsalania wynosi ok. 145 mln metrów sześciennych dziennie. Jest to niemal dwukrotny wzrost w porównaniu z rokiem 2010. W 2023 r. instalacje odsalania działały w 45 krajach, m.in. w: Chinach, Arabii Saudyjskiej, Hiszpanii, Zjednoczonych Emiratach Arabskich i Stanach Zjednoczonych. Kraje te odpowiadają za ponad połowę światowej zdolności produkcji odsolonej wody. Szacuje się, że ok. 70% produkcji niskoemisyjnego wodoru planowanej na 2030 r. zostanie zlokalizowane w odległości do 100 km od wybrzeża, co umożliwia wykorzystanie wody morskiej jako głównego źródła. W przypadku projektów bardziej oddalonych od wybrzeża zastosowanie technologii odsalania również jest możliwe, jednak wiąże się z koniecznością budowy kosztownych rurociągów do transportu odsolonej wody[47].

Innym rozwiązaniem w zakresie oszczędności zasobów wodnych są nowoczesne technologie zarządzania ciepłem w procesach produkcji wodoru. Skuteczne systemy chłodzenia mogą znacznie zmniejszyć zapotrzebowanie na wodę i ograniczyć wpływ na środowisko. Alternatywne technologie chłodzenia, np. chłodzenie suche, systemy zamgławiania, systemy adiabatyczne dla chłodnic powietrznych typu Air Fin oraz systemy chłodni zamkniętych Tundracel, mają potencjał do zmniejszenia zapotrzebowania na wodę w porównaniu z tradycyjnymi metodami chłodzenia mokrego. Dodatkowo sama poprawa sprawności procesu elektrolizy ma bezpośredni wpływ na zmniejszenie zużycia wody – wzrost wydajności o 1% pozwala obniżyć zużycie wody o ok. 2%. Zastosowanie tych rozwiązań wspiera bardziej efektywną i zrównoważoną produkcję wodoru, co jest szczególnie istotne w regionach borykających się z deficytem zasobów wodnych[48].

[46] International Energy Agency, *Global Hydrogen Review 2024*…, s. 89–92.

[47] Tamże.

[48] Tamże, s. 93.

Wnioski

Transformacja energetyczna związana z przejściem na czystą energię prowadzi do coraz silniejszych powiązań między minerałami krytycznymi a sektorem energetycznym. Zapotrzebowanie na te surowce ściśle zależy od wykorzystywanej technologii czystej energii. W przypadku elektrolizerów istotną rolę odgrywają takie surowce, jak: nikiel, cyrkon, REEs oraz PGMs. Jednocześnie technologie OZE, niezbędne do produkcji zielonego wodoru, również wymagają podobnych materiałów, w tym niklu i REEs. Co więcej, same technologie OZE konkurują ze sobą o zasoby, takie jak aluminium, miedź czy wspomniane wcześniej REEs i nikiel. Konkurencja o minerały nie wynika bezpośrednio z relacji między OZE a zielonym wodorem, lecz z zapotrzebowania na te same surowce potrzebne do ich rozwoju.

Analiza wykazała, że istnieje wyraźna zależność między produkcją zielonego wodoru, dostępnością minerałów krytycznych a poziomem stresu wodnego w poszczególnych regionach. W regionach bogatych w złoża minerałów krytycznych występuje jednocześnie wysoki poziom stresu wodnego. Prognozy wskazują, że prawie połowa planowanych elektrolizerów do produkcji zielonego wodoru w 2030 r. zostanie zlokalizowana na obszarach dotkniętych niedoborami wody. Wysokie zapotrzebowanie na ultraczystą wodę w procesie elektrolizy, w połączeniu z ograniczonymi zasobami wodnymi, może prowadzić do konkurencji między gospodarką wodorową a gospodarką wodną, a w dłuższej perspektywie – do lokalnych konfliktów o dostęp do wody. Zminimalizowanie tego ryzyka wymaga wprowadzania zintegrowanych polityk dotyczących sektora wodnego i wodorowego, uwzględniających wzajemne zależności między tymi dwoma obszarami.

Wśród rekomendowanych rozwiązań technologicznych warto wymienić odsalanie wody morskiej, zaawansowane systemy chłodzenia, optymalizację procesów elektrolizy oraz recykling minerałów. Ich wdrożenie może znacznie ograniczyć wpływ produkcji wodoru na potrzebne zasoby i pozwolić na zrównoważony rozwój tej technologii. Brak takich rozwiązań może z kolei spowolnić transformację energetyczną, a jednocześnie zwiększyć jej koszty.

Analiza rynku minerałów krytycznych wskazuje na wysoką koncentrację produkcji. Prym wiodą tu Chiny, dominujące również w procesach rafinacji. Asymetrie w produkcji i przetwórstwie minerałów krytycznych mogą stanowić zagrożenie dla stabilności globalnego rynku wodorowego i dostępu do zasobów mineralnych. Koniecznością jest tworzenie zróżnicowanej sieci dostaw tych minerałów oraz rozwijanie rafinacji w innych krajach, aby zmniejszyć ryzyko monopolu. Zwłaszcza kraje importujące, w tym państwa UE i USA, powinny dywersyfikować źródła minerałów oraz rozwijać technologie recyklingu.

Dalsze badania powinny skupić się na opracowaniu wytycznych dla polityk zarządzania gospodarką wodną w regionach dotkniętych deficytem wody w kontekście rozwoju sektora wodorowego. Innym priorytetowym obszarem badań powinna być ocena efektywności i opłacalności alternatywnych technologii oraz rozwój modeli prognostycznych, które uwzględniają zmiany klimatyczne, w tym nasilające się zjawiska suszy, mogące wpłynąć na dostępność zasobów wodnych. Modele te mogłyby wspierać prognozowanie zapotrzebowania na wodę w sektorze wodorowym oraz opracowywanie strategii zarządzania zasobami wodnymi uwzględniających zmiany klimatyczne i rosnące zapotrzebowanie na zielony wodór.

Bibliografia

Calvo G., Mudd G., Valero A., Valero A., *Decreasing Ore Grades in Global Metallic Mining: A Theoretical Issue or a Global Reality?*, „Resources" 2016, t. 5, nr 4, 36. https://doi.org/10.3390/resources5040036.

Depraiter L., Goutte S., *The Role and Challenges of Rare Earths in the Energy Transition*, working papers, SSRN, 23 VI 2023 r. http://dx.doi.org/10.2139/ssrn.4477111.

European Commission, *Critical raw materials for the EU*, Brussels 2010.

Greenwald J.E., Zhao M., Wicks D.A., *Critical mineral demands may limit scaling of green hydrogen production*, „Frontiers in Geochemistry" 2023, t. 1. https://doi.org/10.3389/fgeoc.2023.1328384.

Kalantzakos S., *The Race for Critical Minerals in an Era of Geopolitical Realignments*, „The International Spectator" 2020, t. 55, nr 3. https://doi.org/10.1080/03932729.2020.1786926.

Moreira S., Laing T., *Sufficiency, sustainability, and circularity of critical materials for clean hydrogen*, Washington 2022.

National Research Council, *Minerals, Critical Minerals, and the U.S. Economy*, Washington 2008. https://doi.org/10.17226/12034.

Noailly J., Bauer Ch., Haller T., Hool A., *The role of critical materials for the energy transition. Challenges and opportunities*, „Swiss Academies Reports" 2024, t. 19, nr 3, s. 5–6. https://doi.org/10.5281/zenodo.12168441.

Sengupta M., *Environmental impacts of mining: Monitoring, restoration, and control*, wyd. 2, CRC Press 2021. https://doi.org/10.1201/9781003164012.

U.S. Department of Energy, *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*, Washington 2018.

U.S. Department of Energy, *Critical Materials Strategy*, Washington 2010.

U.S. Geological Survey, *Mineral Commodity Summaries 2024*. https://doi.org/10.3133/mcs2024.

Źródła internetowe

Bosse P., Gourdon J., Lapeyronie H., Normand E., *The minerals essential to the energy and digital transitions: An opportunity for Africa?*, Agence Française de Développement, https://www.afd.fr/en/ressources/minerals-essential-energy-and-digital-transitions-opportunity-africa [dostęp: 14 V 2024].

European Patent Office, International Renewable Energy Agency, *Patent insight report: Innovation trends in electrolysers for hydrogen production*, https://link.epo.org/web/patent_insight_report_innovation_trends_for_electrolysers_in_hydrogen_production_en.pdf [dostęp: 14 XI 2024].

Hendriwardani M., Ramdoo I., *Critical Minerals: A primer*, https://www.igfmining.org/wp-content/uploads/2022/11/critical-minerals-primer-en-WEB.pdf [dostęp: 13 XI 2024].

International Energy Agency, *Critical Minerals Market Review 2023*, https://iea.blob.core.windows.net/assets/c7716240-ab4f-4f5d-b138-291e76c6a7c7/CriticalMineralsMarketReview2023.pdf [dostęp: 15 V 2024].

International Energy Agency, *Global Hydrogen Review 2024*, https://iea.blob.core.windows.net/assets/89c1e382-dc59-46ca-aa47-9f7d41531ab5/GlobalHydrogenReview2024.pdf [dostęp: 16 XI 2024].

International Energy Agency, *The Role of Critical Minerals in Clean Energy Transitions*, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf [dostęp: 14 V 2024].

International Renewable Energy Agency, Bluerisk, *Water for hydrogen production*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Dec/IRENA_Bluerisk_Water_for_hydrogen_production_2023.pdf [dostęp: 6 XI 2024].

International Renewable Energy Agency, *Green Hydrogen: A guide to policy making*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2020/Nov/IRENA_Green_hydrogen_policy_2020.pdf [dostęp: 12 V 2024].

International Renewable Energy Agency, *World Energy Transitions Outlook 2023: 1.5°C Pathway*, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Jun/IRENA_World_energy_transitions_outlook_2023.pdf [dostęp: 13 V 2024].

Kaboli E., *Critical Minerals and Materials for Selected Energy Technologies*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R48149 [dostęp: 12 XI 2024].

Lakshman S., *More Critical Minerals Mining Could Strain Water Supplies in Stressed Regions*, World Resources Institute, 10 I 2024 r., https://www.wri.org/insights/critical-minerals-mining-water-impacts [dostęp: 13 V 2024].

Mo Ibrahim Foundation, *Africa's critical minerals: Africa at the heart of a low-carbon future*, https://mo.ibrahim.foundation/sites/default/files/2022-11/minerals-resource-governance.pdf [dostęp: 14 V 2024].

Morrison W.M., Tang R., *China's Rare Earth Industry and Export Regime: Economic and Trade Implications for the United States*, Washington 2012, https://digital.library.unt.edu/ark:/67531/metadc85418/ [dostęp: 12 XI 2024].

Snoussi-Mimouni M., Avérous S., *High demand for energy-related critical minerals creates supply chain pressures*, World Trade Organization, 10 I 2024 r., https://www.wto.org/english/blogs_e/data_blog_e/blog_dta_10jan24_e.htm [dostęp: 12 V 2024].

U.S. Department of Energy, *Critical Materials Assessment 2023*, „Federal Register" 2024, t. 88, nr 149, https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16611.pdf [dostęp: 16 XI 2024].

U.S. Department of Energy, *What Are Critical Materials and Critical Minerals?*, https://www.energy.gov/cmm/what-are-critical-materials-and-critical-minerals [dostęp: 10 V 2024].

Zilli R., André J., Bellucci S., *Policy analysis: Securing sustainable critical raw material supply for clean energy in Europe*, European Energy Research Alliance 2023, https://www.eera-set.eu/component/attachments/?task=download&id=1235:EERA_Policy_Analysis_on_Critical_Raw_Materials_Layout_Digital-for-publication [dostęp: 13 V 2024].

Marta Grzywacz

Ukończyła ekonomię na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Obecnie studentka Międzywydziałowych Studiów Ochrony Środowiska na Uniwersytecie Warszawskim, prowadzonych przez Uniwersyteckie Centrum Badań nad Środowiskiem Przyrodniczym i Zrównoważonym Rozwojem.

Kontakt: martagrzywacz8@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 195–216

https://doi.org/10.4467/20801335PBW.25.009.22175

ARTYKUŁ

Służby cywilne i żandarmeria w systemie wywiadowczym Francji w latach 1799–1815[1]

Civil services and military police in the intelligence system of France 1799–1815

SZYMON GŁÓWKA

Autor niezależny

https://orcid.org/0009-0008-2843-8035

Abstrakt

W artykule zanalizowano francuskie struktury wywiadowcze epoki napoleońskiej (1799–1815). Przedstawiono ich tworzenie, a także wyjątkowy charakter i znaczenie w historii nowożytnych systemów zarządzania informacją. Szczególną rolę w funkcjonowaniu służb cywilnych odgrywała tajna kontrola korespondencji, a także reorganizacja policji państwowej. Scharakteryzowano ponadto działalność kojarzoną z wywiadem wewnętrznym i kontrwywiadem, która w znacznym stopniu podlegała formacjom żandarmerii. Opisano kluczowe elementy centralizacji ustrojowej państwa, formalno-prawne ramy działania tajnej agentury oraz sposób realizacji poszczególnych zadań cyklu wywiadowczego na podstawie zachowanej dokumentacji. Podstawę analizy stanowią zarówno materiały źródłowe z epoki, jak i nowa literatura francuskojęzyczna.

[1] Artykuł powstał na podstawie pracy licencjackiej pt. *Szpiedzy Napoleona. System wywiadu i kontrwywiadu napoleońskiej Francji w latach 1804–1812*, obronionej na Wydziale Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego. Autor wykorzystał fragmenty rozdziałów 1., 2. i 3. Praca została nagrodzona w XIII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Słowa kluczowe szpiegostwo, historia wywiadu, Napoleon Bonaparte, wywiad francuski

Abstract The article analyses French intelligence structures during the Napoleonic era (1799–1815). Their origins as well as unique character and significance in the history of modern information management systems were presented. The pivotal role in the functioning of civil services was played by the secret monitoring of correspondence, as well as the reorganisation of the state police. Moreover, activities associated with domestic intelligence or counterintelligence, which were largely subordinate to military police formations were also characterised. Key elements of the state's systemic centralisation, the formal-legal framework for secret agency operations, and the modus operandi of specific intelligence missions based on preserved documentation were described. The analysis is based on both source materials from the era as well as new French-language literature.

Keywords espionage, history of intelligence, Napoleon Bonaparte, intelligence of France

Początek XIX w. to czas, w którym kształtowało się nowoczesne podejście do niejawnych aktywności państwa oraz samej informacji jako użytecznego narzędzia prowadzenia polityki i zapewniania bezpieczeństwa. Mimo to system wywiadowczy uformowany przez napoleońską Francję nie stał się dotychczas w literaturze polskojęzycznej przedmiotem zainteresowania w kontekście badań nad bezpieczeństwem. Nieliczne prace z tego zakresu[2] opowiadają o francuskim wywiadzie jedynie z polskiej perspektywy (głównie kampania rosyjska 1812 r.) w charakterze refleksji historycznej. W odmienny sposób ten problem został opisany w literaturze francuskiej, gdzie zainteresowanie historycznymi aspektami działalności wywiadowczej przeżywa w ostatnich latach mały renesans. Świadczy o tym liczba ukazujących się

[2] Zob. np. D. Milewski, *Napoleoński wywiad na Rosję w Księstwie Warszawskim przed wojną 1812 roku*, „Echa Przeszłości" 2010, nr 11, s. 145–172; K. Bobiatyński, *Wywiad działający z terenu Księstwa Warszawskiego przed wojną 1812 roku*, „Teka Historyka" 2001, z. 20, s. 19–59; A. Nieuważny, *Wywiady twarzą w twarz*, „Mówią Wieki" 2012, nr 2, s. 17–21; J. Skowronek, *Z magnackiego gniazda do napoleońskiego wywiadu. Aleksander Sapieha*, Warszawa 1992.

artykułów[3] oraz prac i monografii, jak np.: *Napoleon et le renseignement*[4]; *Renseignement et espionnage du Premier Empire à l'affaire Dreyfus*[5]; *Le secret de l'État: Surveiller, protéger, informer. XVIIe-XXIe siècle*[6]. Francuzi opisują, w jaki sposób funkcjonowały ówczesne struktury wywiadowcze. Wskazują także elementy procesualne, umieszczające wywiad napoleoński w szerszej perspektywie wyzwań (np. zapewnianie ładu wewnętrznego państwa po okresie rewolucji czy konieczność prowadzenia polityki państwa w obliczu permanentnego stanu wojny) oraz rozwoju nowożytnej myśli politycznej. Celem artykułu jest przybliżenie tej problematyki.

Uwagi wstępne

Struktura wywiadowcza napoleońskiej Francji rozwijała się w specyficznych warunkach, które charakteryzowały się m.in. nietypowymi uwarunkowaniami prawnymi, szczególnym rodzajem hierarchiczności wymiany informacji oraz nieformalnym charakterem szpiegostwa. Ta sytuacja była wynikiem osiągnięć epoki nowożytnej i kształtowała to, w jaki sposób ówcześni decydenci postrzegali rolę i działalność wywiadu.

W celu rzeczowej analizy systemów wywiadowczych przed ich profesjonalizacją na przełomie XIX i XX w. należy przyjąć możliwie szeroką definicję przedmiotu badania. Za taką można uznać tę autorstwa Petera Gilla i Marka Phythiana, zgodnie z którą: *Wywiad odnosi się do zakresu działań mających na celu utrzymanie lub wzmacnianie bezpieczeństwa poprzez dostarczanie specyficznej wiedzy o zagrożeniach i ryzykach, która pozwala na właściwą reakcję lub zapobieganie w wymiarze strategii, polityki i działania, włączywszy – w razie konieczności – tajne akcje*[7]. Takie podejście teoretyczne pozwala na uniknięcie nadużywanego w kontekście minionych wieków pojęcia szpiegostwa, które zamyka wieloletnią oraz zaawansowaną działalność wywiadowczą europejskich mocarstw w ramy wąskiej aktywności kojarzonej z literackimi przygodami płaszcza i szpady. Przyjęcie powyższej definicji

[3] Zob. np. M. Roucaud, *De l'opérationnel au policier: les officiers de Napoléon face à la pratique du renseignement*, „Napoleonica. La Revue" 2016, nr 27, s. 62–83.

[4] G. Arboit, *Napoléon et le renseignement*, Paris 2022.

[5] E. Denécé, B. Léthenet, *Renseignement et espionnage du Premier Empire à l'affaire Dreyfus*, Paris 2021.

[6] S.Y. Laurent, *Le secret de l'État: Surveiller, protéger, informer. XVIIe-XXIe siècle*, Paris 2015.

[7] P. Gill, M. Phythian, *Intelligence in an Insecure World*, Cambridge–Malden 2012, za: A. Gruszczak, *Studia wywiadowcze jako poddyscyplina nauk o bezpieczeństwie: kierunki rozwoju*, w: *Bezpieczeństwo. Dyscyplina nauki wobec funkcjonowania państwa*, R. Skarzyński, E. Kużelewska (red. nauk.), Białystok 2018, s. 72.

oznacza, że napoleoński wywiad należałoby postrzegać bardziej jako system zarządzania informacją niż zespół sformalizowanych służb.

Ponadto zarządzanie informacją w rewolucyjnej Francji stanowiło pewien wyjątek na tle państw ówczesnej Europy. Było to związane z hierarchicznością systemu wymiany informacji, który istotnie różnił się od innych modeli zarządzania. Ustrój państwa francuskiego opierał się (od 1799 r. realnie, a od 1804 r. również formalnie) na osobie Napoleona Bonaparte (1769–1821), który najpierw jako pierwszy konsul, a później jako cesarz reprezentował najwyższą władzę wojskową oraz cywilną. Co istotne, ta władza nie była jedynie symbolicznym, lecz faktycznym wyrazem kompetencji Napoleona, który aktywnie uczestniczył we wszelkich działaniach państwa – od wielkich kampanii, prawodawstwa cywilnego i uczestniczenia w komisjach Rady Państwa[8] po osobiste tworzenie państwowych orderów oraz hobbystyczne projektowanie umocnień fortyfikacyjnych[9]. Wszelkie akty niejawnego zdobywania informacji musiały być zatem ukierunkowane ostatecznie bezpośrednio na Napoleona oraz wymagały jego aprobaty w zakresie decydowania o ich następstwach. Raporty wysyłane przez francuskich informatorów przeglądała grupa decydentów, ograniczona do elit państwa, którzy – za przyzwoleniem Napoleona – mogli wykorzystywać informacje w celach politycznych. Struktura przekazywania istotnych informacji różniła się od współczesnych schematów służb wywiadowczych – osadzonych ustrojowo, poddanych kontroli innych władz i objętych regulaminami właściwymi służbom mundurowym. Napoleoński system zarządzania informacją można przedstawić za pomocą piramidy, na której szczycie znajduje się władca, a na samym dole: szpiedzy, informatorzy, funkcjonariusze i agenci. Pomiędzy końcami piramidy można umieścić kilkanaście odrębnych instytucji oraz organów konkurujących ze sobą.

Pomimo ukierunkowania systemu pozyskiwania informacji na głowę państwa systemy odpowiedzialne za realizację zadań wywiadowczych w istocie stanowiły odrębnie funkcjonujące struktury, niechętnie kooperujące w zakresie pozyskiwanych informacji. Po części było to spowodowane brakiem jednego organu koordynującego działania wywiadowcze. Wywiad dyplomatyczny podlegał Ministerstwu Spraw Zewnętrznych, wywiad wojskowy – sztabowi generalnemu Wielkiej Armii, a wywiad cywilny – Ministerstwu Policji. Co więcej, to zjawisko było następstwem personalnych uprzedzeń oraz politycznych ambicji poszczególnych decydentów, którzy często równolegle do działalności państwowej prowadzili prywatne archiwa

[8] A. Roberts, *Napoleon Wielki*, Warszawa 2015, s. 339; E. de Las Cases, *Memoriał ze św. Heleny*, t. 1, Gdańsk 2008, s. 221–223.

[9] W. Łysiak, *Napoleon fortyfikator [rozprawa doktorska]*, Warszawa 2012.

wywiadowcze, sabotowali działalność innych organów wywiadowczych[10] lub też w skrajnych przypadkach byli informatorami obcych wywiadów[11]. Doprowadzało to niejednokrotnie do wewnętrznych sporów i rywalizacji między wpływowymi ministrami oraz generałami, a jednocześnie mobilizowało wszystkie strony do wzmożonej pracy i czujności wobec konkurencji.

Dla zrozumienia istoty funkcjonowania struktur wywiadowczych w początkach XIX w. ważne jest poznanie modus operandi oraz formalnego statusu szpiegów (fr. *l'espion*) i informatorów (fr. *indicateurs* lub *moutons*). W epoce napoleońskiej wszelka działalność szpiegowska z prawnego punktu widzenia była definiowana jako przestępstwo karne oraz traktowana jako zdrada ojczyzny i jako taka stanowiła temat tabu[12]. Zbudowanie przeciwstawnej definicji nie było możliwe, gdyż agenci, szpiedzy oraz informatorzy nie byli oficjalnymi funkcjonariuszami państwa i nie pobierali jawnych wynagrodzeń za swoją pracę. Działali zatem w szarej strefie. Łączono w niej prowadzenie działalności szpiegowskiej z innym zawodem lub zajęciem, które – poza oczywistym aspektem kamuflażu – było też głównym źródłem pozyskiwanych informacji. Modus operandi szpiega był ściśle powiązany z jego funkcją społeczną, np. kapitan statku handlowego donosił o ruchach i położeniu innych jednostek morskich, agent policji informował o przebywających w okolicy obcokrajowcach, a zwerbowane damy dworskie wypytywały swoich kochanków o plany. Cechą epoki napoleońskiej jest także pojawienie się szpiegów pełniących funkcję prowokatorów politycznych, którzy wbrew zasadzie ścisłej tajności manipulowali emocjami grup

---

[10] Przykładem może być konflikt Fouché–Savary. Zob. J. Tulard, *Joseph Fouché*, Warszawa 2021, s. 154.

[11] Ta sugestia pojawia się w kontekście kariery ministra Charles'a Maurica de Talleyranda-Périgorda, zob. G. Arboit, *Napoléon et le renseignement*…, s. 189–191.

[12] W ten sposób, jako naruszenie bezpieczeństwa zewnętrznego państwa, szpiegostwo jest rozumiane m.in. we francuskim *Code pénal* z 1810 r. „**Art. 76** Każdy, kto dopuścił się machinacji lub utrzymywania kontaktów wywiadowczych z obcymi mocarstwami lub ich agentami, aby zachęcić je do działań wojennych lub podjęcia wojny przeciwko Francji, […] zostanie ukarany śmiercią, a jego majątek zostanie skonfiskowany. **Art. 77** Karą śmierci i konfiskatą majątku będzie także karany każdy, kto utrzymywał aktywne relacje z wrogami państwa w celu ułatwienia im wkroczenia na terytorium i terytoria zależne imperium francuskiego lub przekazania im miast twierdz, miejsc […] albo przez podważanie lojalności oficerów, żołnierzy, marynarzy i innych osób wobec cesarza i państwa, albo w jakikolwiek inny sposób. **Art. 78** Jeżeli korespondencja z podmiotami władzy nieprzyjacielskiej, niemająca na celu zbrodni wymienionych wcześniej, mimo wszystko kończyła się wydawaniem wrogom instrukcji szkodliwych dla sytuacji militarnej lub politycznej Francji lub jej sojuszników, osoby utrzymujące tę korespondencję zostaną ukarane wygnaniem, z zastrzeżeniem surowszych kar w przypadku, gdyby instrukcje te były wynikiem aktu szpiegostwa". Za: *Code pénal de 1810. Édition originale en version intégrale, publiée sous le titre: CODE DES DÉLITS ET DES PEINES*, https://ledroitcriminel.fr/la_legislation_criminelle/anciens_textes/code_penal_1810/code_penal_1810_1.htm [dostęp: 1 I 2025]. Tłumaczenia w artykule pochodzą od autora (dop. red.).

społecznych[13]. W ogólnym rozrachunku skuteczność działań wywiadowczych państwa opierała się na indywidualnych cechach i talentach agentów, którzy nie mieli ujednoliconych instrukcji oraz wypracowanych modeli pracy operacyjnej.

Kontrola korespondencji i Urząd Poczt

Przed rozpowszechnieniem się nowoczesnych środków komunikacji jednym z głównych źródeł pozyskiwania informacji o znaczeniu politycznym było szpiegostwo pocztowe. Nie tylko pozwalało ono na dyskretne pozyskanie informacji bez wiedzy nadawcy i właściwego odbiorcy danego komunikatu, lecz także umożliwiało zdobycie materialnego dowodu przeciwko autorowi i/lub adresatowi. Historia francuskiego Czarnego Gabinetu (fr. *Cabinet Noir*), czyli specjalnej komórki przeznaczonej do inwigilacji przesyłek pocztowych oraz szyfrowania tych, które nie powinny być odczytane przez osoby postronne, rozpoczęła się jeszcze w dobie *ancien régime* pod panowaniem Ludwika XV[14]. Problem inwigilacji i naruszania prywatności przesyłek pocztowych stał się czołowym hasłem rewolucjonistów, którzy w ramach zgromadzenia ustawodawczego już w grudniu 1789 r. zadekretowali nienaruszalność korespondencji, a rok później zamrozili działania Czarnego Gabinetu przez zniesienie jego państwowego finansowania[15].

Pomimo oficjalnego zakazu otwierania prywatnych listów do tej praktyki powrócono już na przełomie lat 1792 i 1793, a dodatkowo rozszerzono ją w okresie rządów Dyrektoriatu w 1796 r. Dekrety w tych kwestiach ograniczały się przede wszystkim do korespondencji zagranicznej. Odejście od rewolucyjnej powściągliwości w pozyskiwaniu informacji zainicjował zamach stanu 18 brumaire'a roku VIII (9 listopada 1799 r.), gdy do władzy doszedł Napoleon Bonaparte. Po latach tak opisywał on swoje zdanie w kwestii działalności Czarnego Gabinetu:

> Naruszenie tajności korespondencji datuje się we Francji na okres panowania Ludwika XIV, lecz to za Ludwika XV powstał *Cabinet Noir*. Nic nie zmieniłem w jego organizacji, postawiłem jedynie na jego czele człowieka o skrajnej

[13] „Agenci francuscy zostali jednocześnie rozproszeni po kontynencie, a szczególnie w Turcyi, buntując ludność i przygotowując umysły do przyjęcia zbawców Francuzów, a gabinet w Tuileryach nie szczędził w Konstantynopolu ani złota, ani podchlebstw, ani oszczerstw, dla pozyskania Mahometan przeciw Rosyi". Za: A. Czartoryski, *Sprawozdanie z roku 1804 dla Senatu*, w: A. Czartoryski, *Pamiętniki ks. Adama Czartoryskiego i korespondencya jego z cesarzem Aleksandrem I*, t. 2, Kraków 1905, s. 111.

[14] J. Piekałkiewicz, *Dzieje szpiegostwa*, Warszawa 1999, s. 177–178.

[15] A. Belloc, *Les postes françaises: recherches historiques sur leur origine, leur développement, leur législation*, Paris 1886, s. 257–258.

> uczciwości, nie pozwalając żadnemu z moich ministrów przeniknąć tych piekielnych tajemnic. Podsumowując, jest to zła instytucja, która przynosi więcej szkody niż pożytku. […] Najczęściej korzystałem z *Cabinet Noir*, aby poznać prywatną korespondencję moich ministrów, moich szambelanów, moich wielkich oficerów, nawet samego Berthiera i Duroca[16]. Ileż to razy odkrywałem ich zatajony wstręt do trudów wojny, ich zły humor wynikający z przebywania z dala od przyjemności Paryża i ich niechęć dla interesu państwa! Wszyscy byli mniej lub bardziej zbuntowani i wszyscy oni uważaliby się za straconych, gdyby wiedzieli, że znam przyczyny ich narzekań. Czasem jednak naruszenie tajemnicy listów było dla mnie przydatne. Cesarz miał już zdradzić nam kilka ciekawych szczegółów na ten temat, gdy nagle stwierdził: „Ale tu popełniam polityczną niedyskrecję. Poczytajmy zamiast tego *Delfinę*"[17].

Okres pierwszego cesarstwa oznacza zatem pełne przywrócenie finansowania Czarnego Gabinetu i rozszerzenie jego działalności na całość – istotnej dla bezpieczeństwa państwa – korespondencji prywatnej. Na jego czele stanął „człowiek o skrajnej uczciwości" – Antoine Marie Chamans de Lavalette (1769–1830). Był on kolejno uczestnikiem wojen włoskich, osobistym adiutantem Napoleona, generałem, przedstawicielem dyplomatycznym oraz komisarzem i Dyrektorem Generalnym Poczt w latach 1804–1814. Jako poczmistrz zarządzał wszystkimi francuskimi placówkami pocztowymi oraz sprawował funkcję dyrektora Czarnego Gabinetu. Pracę wywiadowczą w jego imieniu wykonywała grupa kilkudziesięciu osób, które w ramach struktur Urzędu Poczt starannie przeszukiwały korespondencję. Dyrektor odpowiadał za sporządzenie pojedynczego raportu, który codziennie dostarczano do Napoleona (ewentualnie do Rady Państwa). Skala działań Czarnego Gabinetu nie była jednak duża, a wizjom totalitarnym przeczą słowa Françoisa Barbé-Marboisa[18], który twierdził, że: (…) *spośród około 30 000 listów, które każdego wieczoru opuszczały Paryż w kierunku Francji i reszty świata, tylko dziesięć lub dwanaście było kopiowanych i to często jedynie we fragmentach po kilka linijek*[19].

---

[16] Louis-Alexandre Berthier (1753–1815) – generał, marszałek, minister wojny i szef sztabu Napoleona; Geraud Duroc (1772–1813) – generał, marszałek dworu cesarskiego. Berthier i Duroc byli w bliskim otoczeniu Napoleona. Zob. T. Dziekoński, *Życie marszałków francuzkich z czasów Napoleona*, Warszawa 1841, s. 1–5, 174–180.

[17] M. Montholon, *Récits de la captivité de l'empereur Napoléon à Sainte-Hélène*, t. 1, Paris 1847, s. 211–212.

[18] François Barbé-Marbois (1745–1837) – radca stanu, prezes cesarskiego Sądu Obrachunkowego. Zob. Napoléon & Empire, *Conseillers d'État du Consulat et de l'Empire*, https://www.napoleon-empire.org/institutions/liste-conseillers-etat-premier-empire.php [dostęp: 5 II 2025].

[19] A. Belloc, *Les postes françaises*…, s. 410.

Zadania wywiadowcze były znacznie skuteczniej realizowane przez Urząd Poczt w działaniach logistycznych. Lavalette, poza Czarnym Gabinetem, odpowiadał także za funkcjonowanie sieci kurierskiej, która nabierała szczególnego znaczenia podczas prowadzenia oddalonych o tysiące kilometrów kampanii wojennych. Koniecznością było codzienne dostarczanie cesarzowi całego pliku dokumentów, na które składały się wyciągi prasowe, raporty Czarnego Gabinetu oraz biuletyny policyjne. Dokumenty umieszczano w specjalnej skórzanej aktówce zdobionej napisem *Sa Majesté l'Empereur et Roi – Gazettes Étrangères*[20] i dostarczano przy pomocy kurierów pocztowych do osobistych sekretarzy Napoleona w jego otoczeniu.

Ciekawa z perspektywy ustrojowej jest także formalna współpraca Czarnego Gabinetu z Ministerstwem Policji, które często otrzymywało od niego informacje i jednocześnie uzyskiwało cele dalszej inwigilacji[21]. Jednak z obawy przed zbyt potężnym wzrostem znaczenia policji w okresie pierwszego cesarstwa obie instytucje pozostawały w swoistej separacji, a sam Lavalette demonstrował niechęć do ministra policji Josepha Fouchégo (1759–1820) przez dymisjonowanie dyrektorów pocztowych dostarczających poufne informacje policjantom bez jego zgody. Do 1802 r. przy Ministerstwie Policji funkcjonowało konkurencyjne biuro przechwyconych listów, które jednak nie spełniło pokładanych w nim nadziei ministra i zostało rozwiązane[22]. Działalność Czarnego Gabinetu w epoce napoleońskiej wskazuje, że sama instytucja nie była wyrazem inwigilacyjnych dążeń Napoleona, lecz raczej złem koniecznym. Odpowiedniki takich instytucji istniały także w innych mocarstwach europejskich.

Policja państwowa

Przed powstaniem nowoczesnych, wyspecjalizowanych agencji wywiadowczych w Europie zasadniczy ciężar wywiadu cywilnego opierał się zazwyczaj na rozmaitych formacjach policyjnych. W kontekście tego zagadnienia rewolucyjna Francja

[20] W tłumaczeniu: „Jego Królewska Mość Cesarz i Król – Gazety Zagraniczne". Do dzisiaj zachowało się kilka sztuk aktówek. Pozostają głównie w rękach prywatnych, przynajmniej jedna znajduje się w Luwrze. Zob. Louvre Collections, *Portefeuille à soufflet*, https://collections.louvre.fr/ark:/53355/cl010115454 [dostęp: 5 II 2025].

[21] W liście do ministra policji z 7 X 1807 r. Napoleon pisał: „Przesyłam Panu przechwyconą korespondencję od hrabiego Lille. Wydała mi się nader interesująca. Proszę, zdaj mi raport na temat wszystkiego, co możesz z niej wyciągnąć. Wydaje mi się, że pewną rolę odgrywać w tym może korespondencja Fauche Borela." Zob. *Correspondance de Napoléon I^er^*, t. 16, Paris 1864, s. 75.

[22] J. Tulard, *Joseph Fouché*…, s. 114.

stała się niejako wzorcem budowania nowoczesnych formacji policyjnych i szerzej – administracji bezpieczeństwa. Okres *ancien régime* charakteryzował się przestarzałym sposobem realizowania zadań policyjnych w ramach ówczesnej władzy sądowniczej (fr. *Garde des Sceaux*) lub armii. Zmiana nastąpiła w 1796 r., gdy utworzono Ministerstwo Policji odrębne od Ministerstwa Sprawiedliwości. Kolejną reformę systemową – ustawę z 28 Pluviôse roku VIII (z 17 lutego 1800 r.)[23] – zainicjował pierwszy konsul Bonaparte. Jej skutkiem było wprowadzenie administracyjnego systemu prefektur i wydzielenie z policji państwowej Paryskiej Prefektury Policji[24]. Skomplikowaną strukturę policyjną dopełniły tworzone kolejno od 1791 r. formacje żandarmerii oraz od 1804 r. policja Wielkiego Marszałka Dworu.

Istnienie wielu konkurencyjnych formacji policyjnych wymaga wyjaśnienia. Zasadniczą podstawą legislacyjną takiego stanu była wspomniana ustawa z 28 Pluviôse roku VIII (z 17 lutego 1800 r.), która formowała we Francji napoleoński system administracji terytorialnej. Kraj został podzielony na departamenty, okręgi i kantony, a władzę centralną reprezentowanli na prowincji prefekci zwani małymi cesarzami[25]. To oni byli odpowiedzialni za kwestie administracyjne i lokalną politykę bezpieczeństwa. Tym samym, na podstawie art. 13, 14, 15 tej ustawy, prefektom zostali podporządkowani wszyscy komisarze policji, obecni w każdym mieście powyżej 5000 mieszkańców. Pojawił się zatem legalny dualizm w nadzorze nad policją terytorialną, która podlegała zarówno prefektom, jak i ministrowi właściwemu do spraw policji (art. 14). Rozwiązanie to dało ministrowi policji proporcjonalnie dużą władzę i dostęp do ogromnej ilości informacji – wszelkie raporty byli zobowiązani składać mu od tej pory kolejno inspektorzy żandarmerii, prefekt policji Paryża, prefekci administracji departamentów, komisarze generalni, komisarze policji, merowie, a także inni urzędnicy. Wysoką pozycję ministerstwa, podbijaną w dodatku osobistymi ambicjami kierownika resortu Fouchégo, ograniczono przez stworzenie w ramach Paryża osobnych i autonomicznych stanowisk prefekta Sekwany (kwestie administracyjne) oraz paryskiego prefekta policji (sprawy bezpieczeństwa). Paryska Prefektura Policji miała olbrzymie znaczenie w kontekście bezpieczeństwa Francji, to stolicy dotyczyła bowiem większość zagrożeń politycznych, wywiadowczych, socjalnych i przestępczych. Jej prefekt, którym został nieprzychylny ministrowi policji Louis Nicolas Dubois (1758–1847), wykonywał swoje obowiązki pod nadzorem

[23] *Loi du 28 pluviôse an VIII*, https://carnetsdenotes.fr/loi_du_28_pluviose_an_8.htm [dostęp: 1 I 2025].

[24] Kontekst odrębnego systemu bezpieczeństwa i zarządzania kryzysowego dla Paryża względem reszty państwa francuskiego literatura przedmiotu nazywa najczęściej dosłownie „paryskim wyjątkiem" (fr. *l'exception parisienne*). Obecny był on zarówno w czasach *ancien régime*, jak i w epoce napoleońskiej.

[25] We Francji używa się określenia *empereurs au petit pied*, co oznacza dosłownie „cesarza na krótkich nogach". Tłumaczenie „mały cesarz" prawdopodobnie lepiej oddaje sens tego sformułowania.

wszystkich ministrów, co pozwalało mu na prowadzenie konkurencyjnej polityki wobec Fouchégo. W uogólnieniu można zatem wskazać kompetencyjny podział formacji policyjnych napoleońskiej Francji. Ministerstwu Policji przypisywano zadania policji politycznej i realizację zadań specjalnych, w tym wywiadowczych (fr. *haute police*, ang. *high policing*), Paryskiej Prefekturze Policji – funkcje porządkowe uzupełnione kompetencjami zwalczania przestępczości zorganizowanej, formacjom żandarmerii – funkcje policyjne na prowincji i w obrębie armii, a policjom dworskim – ochronę dostojników i budynków państwowych.

Resortem napoleońskiej policji w latach 1799–1810 kierował Fouché, książę Otranto, którego postać łączy się z rozkwitem francuskiej myśli wywiadowczej. Wielu badaczy nazywa go twórcą nowoczesnego modelu służb policyjnych[26], co wiąże się z jego wizją utworzenia tajnego ośrodka, w którym gromadzono by ważne informacje z większej części Europy. Program działalności Fouchégo dobrze opisują jego słowa:

> To z powodu braku refleksji nieustannie myli się policję i administrację. Administracja i policja postępują zupełnie inaczej. Administracja działa i przejawia się na oczach wszystkich, odwrotnie niż policja, która musi być tajna. Musi zawsze czuwać, zawsze działać, na ogół nie pokazując się, prawie nigdy się nie afiszując. [...] Policja taka, jaką sobie wyobrażam, musi mieć na celu zapobieganie przestępstwom i niedopuszczanie do nich, ograniczanie i powstrzymywanie tego, czego prawo nie przewidziało. To władza dyskrecjonalna w rękach rządu[27].

Ministrowi przypisuje się również znany bon mot, zgodnie z którym (…) *trzech ludzi dyskutujących wątpliwie o sprawach politycznych nie mogło spotkać się we Francji bez mojej wiedzy*[28]. Wyrażona w tych słowach pewność siebie oraz specyficzna metoda polityczna świadczą o ambicjach Fouchégo, a także o jego nowatorskim podejściu do wykorzystywania cywilnych instytucji państwa.

---

[26] J. Tulard, *Joseph Fouché*…, s. 7.

[27] Tamże, s. 81–82.

[28] J. Fouché, *Mémoires de Joseph Fouché, Duc d'Otrante. Ministre de la Police Générale*, Osnabrück 1966, s. 325. Memoriały zostały wydane w 1824 r. przez księgarza Gustave'a Le Rouge'a bez zgody i wiedzy nieżyjącego już Fouchégo, a także bez zatwierdzenia przez jego spadkobierców. Wydawca nigdy nie przedstawił rękopisu ani żadnego dowodu na autentyczność wspomnień, co doprowadziło do zmagań sądowych we Francji oraz poddawania treści pracy oczywistej krytyce. Wielu badaczy sugeruje jedynie apokryficzną wartość tego tekstu. Wskazują, że choć mógł nie pochodzić spod ręki samego Fouchégo, to z pewnością był oparty na dokumentach policyjnych i relacjach jego bliskich współpracowników. Zob. tamże, s. 277–282.

Wyznaczenie służbie policyjnej zupełnie nowego zakresu działania było możliwe dzięki rozbudowie aparatu policyjnego o nowe wydziały oraz biura. W budynkach przy paryskiej Quai Voltaire w ramach Ministerstwa Policji od 1804 r. funkcjonowało pięć wydziałów[29]:

1) wydział pierwszy wyznaczony do osobistych spraw ministra i jego zaleceń;
2) wydział drugi do spraw bezpieczeństwa powszechnego, odpowiedzialny za tajną działalność i wykrywanie spisków;
3) wydział trzeci przeznaczony do kontaktu z senackimi komisjami wolności prasy i wolności osobistej;
4) wydział czwarty przeznaczony do kontroli cudzoziemców oraz emigrantów;
5) wydział piąty odpowiadający za księgowość oraz rachunki.

Poza wydziałami równolegle funkcjonowały także biura, m.in. cenzorskie Biuro Gazet, Przedstawień Teatralnych, Drukarń i Księgarń[30]. Struktura wydziałów sugeruje też zakres działalności policyjnej – informowanie władz centralnych o ważnych wydarzeniach, kontrola osobista i korespondencji wszystkich cudzoziemców (skutek polityki paszportowej), a także władza cenzorska.

Dzięki pracy wydziałów pierwszego i drugiego Fouché, oprócz prowadzenia działalności jawnej, mógł rozwinąć na wielką skalę działalność tajną. Była ona wielopłaszczyznowa, odnosiła się zarówno do aktywności szpiegowskiej, jak i kontrwywiadowczej. Minister poza legalną siatką informatorów (komisarzy policji) miał do dyspozycji także prywatnych szpiegów i informatorów, których personalia są do dziś kwestią sporną. Dostępne są bezpośrednie dowody na współpracę m.in.: Gabriela Juliana Ouvrarda[31] (bankiera, finansisty, agenta Fouchégo), Barthélémy Hubera[32] (szwajcarskiego bankiera rezydującego w Londynie), Méhée de La Touche'a[33] (aktywisty politycznego, potrójnego agenta działającego w ramach finansowych Rosji, Anglii, Francji), Jeana G.M. Rocquesa de Montgaillarda[34] (agitatora politycznego znanego w środowisku agentury brytyjskiej i rojalistycznej). Niektóre relacje z epoki, szczególnie te wpisujące się w narrację o wszechwładzy Fouchégo,

[29] J. Tulard, *Joseph Fouché*…, s. 109–110.

[30] Biuro to zostało zastąpione dekretem cesarskim z 1810 r. przez Dyrekcję Generalną Drukarń i Księgarń, podlegającą Ministerstwu Spraw Wewnętrznych. Zob. *Le décret du 5 février 1810*, https://www.siv.archivesnationales.culture.gouv.fr/siv/rechercheconsultation/consultation/ir/consultationIR.action?irId=FRAN_IR_058772&details=true&gotoArchivesNums=false&udId=root&auSeinIR=true [dostęp: 1 I 2025].

[31] M. Stokle, *The bankers of Brumaire: the financiers behind Napoleon's Ascent*, PhD thesis, University of Glasgow, April 2020.

[32] G. Arboit, *Napoleon et le renseignement*…, s. 151.

[33] Tamże, s. 150–153.

[34] J. Fouché, *Mémoires de Joseph Fouché*…, s. 353.

sugerowały zwerbowanie przez niego nawet cesarzowej Józefiny oraz innych czołowych postaci dworu Napoleona. Warto zaznaczyć, że agenci Fouchégo działali również poza Francją. Wynikało to nie tylko z jego osobistych ambicji i polityki, lecz także z nieustannej ekspansji militarnej tego kraju, która w 1812 r. rozciągała się przez wpływy Imperium od Portugalii po Moskwę. Skuteczność agentów była stałym powodem trosk przeciwników Napoleona. Car Aleksander w liście z 31 stycznia 1811 r. pisał do księcia Czartoryskiego przebywającego w tym czasie na terytoriach przygranicznych Rosji i w samym Księstwie Warszawskim: *Co do twej osoby kochany książę, wiem z dobrego źródła, że jesteś śledzony przez policyę francuską, więc bądź ostrożnym wszędzie. Do wymiany listów użyję dróg, jakie mi wskazujesz, a dołączam tu dwa blankiety paszportowe na wypadek gdybyś potrzebował i chciał wysłać do mnie sobie zaufanego*[35].

Tajna działalność szpiegowska przekładała się w praktyce politycznej Fouchégo także na działania operacyjne, spośród których wyróżnia się sprawa brytyjskiego dyplomaty sir George'a Rumbolda – od 1803 r. ambasadora Wielkiej Brytanii przy państwach hanzeatyckich, który miał siedzibę w Hamburgu. Poza prowadzeniem placówki dyplomatycznej Rumbold był odpowiedzialny również za zbieranie informacji od szpiegów i informatorów brytyjskich, przede wszystkim z terytoriów Francji oraz państw niemieckich, będących w relacjach sojuszniczych z Francją. Współpracował on w tym zakresie z innymi brytyjskimi dyplomatami – Francisem Drakiem z Monachium i Spencerem Smithem ze Stuttgartu[36]. Dowody zebrane w tej sprawie oraz śledzenie ruchów angielskich informatorów sprawiły, że Fouché zlokalizował brytyjską komórkę wywiadowczą w siedzibie hamburskiego dyplomaty. Po uzyskaniu zgody od cesarza natychmiast wydał listowny rozkaz francuskim siłom okupującym sąsiedni Hanower[37]. Z zamiarem naruszenia prawa międzynarodowego 24 października 1804 r. ok. 250 żołnierzy oraz towarzyszący im agenci policji przekroczyli rzekę Elbe i zajęli siedzibę brytyjskiego ambasadora[38]. Oficjalnie został on porwany, a następnie wypuszczony po dwóch dniach, co dało agentom policji czas na szczegółowe przejrzenie dokumentów zgromadzonych pod Hamburgiem, które zdekonspirowały przynajmniej kilku brytyjskich informatorów i stanowiły cenne źródło informacji[39].

---

[35] A. Czartoryski, *Pamiętniki ks. Adama Czartoryskiego i korespondencya*…, s. 161.

[36] Nazwiska tych trzech dyplomatów padają w liście Fouché do marszałka Bernadotte z 3 X 1804 r. List zawiera rozkaz aresztowania sir Rumbolda w imieniu Ministerstwa Policji i cesarza Napoleona.

[37] *Correspondance de Napoléon I^er^*…, t. 10, s. 17.

[38] A. Roberts, *Napoleon Wielki*…, s. 369.

[39] J. Tulard, *Joseph Fouché*…, s. 126–127.

Niejawna aktywność policji przynosiła korzyści również w ramach polityki wewnętrznej państwa. Poza ludźmi Fouchégo za tę kwestię odpowiadał zarząd Paryskiej Prefektury Policji mieszczący się przy rue de Jérusalem. Paryska policja podlegała sekretariatowi składającemu się z trzech wydziałów podzielonych na biura[40]. Wydział pierwszy dysponował trzema biurami odpowiedzialnymi kolejno za tajnych agentów policji, paszporty cudzoziemców i cenzurę prasy. Wydział drugi zajmował się nadzorowaniem przestępstw (przede wszystkim morderstw, fałszerstw, kradzieży) oraz prowadzeniem związanego z nimi rejestru bezpieczeństwa. Wydział trzeci odpowiadał za sprawy gospodarcze i komunalne (dbanie o oświetlenie miejskie, prowadzenie akcji gaśniczych, oczyszczanie ulic itp.). Obok funkcjonariuszy przy prefekturze zorganizowano sieć agentów werbowanych z przedstawicieli wszystkich klas społecznych. Zaletą tajnej działalności było m.in. to, że przy paryskiej prefekturze utworzono w 1811 r. specjalną brygadę złożoną z byłych więźniów pod komendą byłego galernika Eugène François Vidocqa (1775–1857), którą uważa się za pierwszą profesjonalną jednostkę policji kryminalnej[41].

Najczęściej przytaczanym przykładem skuteczności wywiadu wewnętrznego policji francuskiej jest prawdopodobnie sprawa nieudanego zamachu na konsula Bonaparte z 24 grudnia 1800 r. W centrum Paryża grupka spiskowców wysadziła wóz wypełniony ładunkami wybuchowymi (tzw. machinę piekielną) nieopodal ulicy, którą Napoleon zmierzał powozem do opery. W wybuchu zginęło co najmniej 8 osób, a rannych zostało niespełna 100[42]. Od pierwszych godzin po zamachu w sprawę osobiście zaangażowali się Fouché oraz prefekt Dubois wraz ze śledczym Jeanem Henrym[43]. Błyskawiczne zbadanie miejsca zbrodni oraz powiązanych z nim osób szybko doprowadziło do pozyskania rysopisu jednego ze spiskowców. W tym samym czasie agenci policji włamywali się do punktów zbiórek konspiratorów i aresztowali współpracowników oraz członków rodzin potencjalnych spiskowców. Było to możliwe dzięki raportom tajnych informatorów, którzy już od lipca 1800 r. opisywali aktywność ekstremistów politycznych. Jeszcze w styczniu 1801 r. policji udało się aresztować dwóch zamachowców – Françoisa Josepha Carbona i Pierre'a Robinaulta de Saint-Régeanta[44]. Georges Cadoudal, przywódca wrogich

[40] Tamże, s. 84–86.

[41] Na temat życiorysu Vidocqa i kulis powstania paryskiej policji kryminalnej (fr. *Surete*) zob. szerzej: J. Savant, *La vie aventureuse de Vidocq*, Paris 1973.

[42] W *Mémoires de Joseph Fouché*… podano, że zginęło 20 osób, a 56 zostało poważnie rannych. Zob. J. Fouché, *Mémoires de Joseph Fouché*…, s. 215.

[43] J. Tulard, *Joseph Fouché*…, s. 95.

[44] A. Roberts, *Napoleon Wielki*…, s. 300–301.

Napoleonowi szuanów[45], odpowiedzialny za te działania, został aresztowany dopiero w 1804 r. przez policjantów paryskiej prefektury przy okazji organizowania kolejnego zamachu na Napoleona.

Spośród wszystkich aktywności wywiadowczych policji najważniejszą wydaje się realizacja tzw. cyklu wywiadowczego. Ministerstwo Policji na podstawie wiedzy własnej oraz przez wykorzystanie raportów innych organów realizowało gromadzenie informacji wywiadowczych. Następnie były one przetwarzane i analizowane, czym zajmowały się wydziały przy Quai Voltaire. Tekst biuletynu spisywał na podstawie dziesiątek raportów każdego dnia specjalny urzędnik Jean-Marie François. Następnie korygował go Pierre Marie Desmarest (szef wydziału drugiego), po czym biuletyn trafiał na biurko Fouchégo, który nanosił na dokument ostatnie, osobiste notatki. Kopię biuletynu umieszczano w archiwum policyjnym, a oryginał łączono w jednej teczce m.in. z raportami paryskiej prefektury, żandarmerii oraz materiałami prasowymi. Kurierzy pocztowi dystrybuowali powyższe materiały codziennie rano (od lipca 1804 r.) do rąk Napoleona, który czytał je najczęściej przy okazji kąpieli i porannej toalety. Biuletyn policyjny trafiał również do konkretnych komisji Rady Stanu[46]. Fouché stworzył w ten sposób doskonały system dystrybucji informacji wywiadowczych, którego współczesną reminiscencją jest amerykański *President's Daily Brief* – bliźniaczo podobny do francuskich biuletynów nie tylko w swoich intencjach, lecz także w wewnętrznej strukturze. Napoleoński biuletyn był podzielony tematycznie i obejmował kolejno: statystykę kryminalną, informacje o przechwyconych listach i agentach, odnotowane wystąpienia przeciwko władzy i inne rebelie, nowinki i trendy rynkowe, morale armii oraz społeczeństwa, planowane wystąpienia polityczne przeciwników cesarza oraz prawdopodobne ruchy obcych agentów[47].

Przykładowe fragmenty biuletynu z 14 czerwca 1805 r. w kolejności oryginalnej:

---

[45] Szuanie (fr. *les chouans*) – uczestnicy powstań z okresu rewolucji francuskiej. Wywodzili się z chłopstwa, które wspierało rojalistów oraz uchylało się od służby wojskowej na rzecz Republiki. Ze względu na lokalizację ognisk oporu szuanów w północnych departamentach Francji ich organizacja od 1795 r. nawiązywała stałe kontakty z brytyjską agenturą, która współpracowała z szuanami aż do ujęcia głównych liderów. Zob. E. Sparrow, *Secret Service. British Agents in France 1792–1815*, Woodbridge 1999.

[46] Francuska Rada Stanu (fr. *Conseil d'État*) została utworzona po zamachu stanu w 1799 r. jako główny ośrodek władzy wykonawczej. Zrzeszała m.in. ministrów, szefów organów, urzędników dworskich i nadzwyczajnych członków Rady Stanu, w tym ministra policji, który każdorazowo miał obowiązek przedstawienia najważniejszych informacji dotyczących bezpieczeństwa państwa. Rada pełniła także pewne funkcje kontrolne wobec policji i miała decydujący głos przy obsadzie stanowisk komisarzy.

[47] J. Hughes-Wilson, *The Secret State: A History of Intelligence and Espionage*, London 2017, s. 32–33.

Agenci angielscy: Generalny komisarz policji w Bordeaux melduje o wykonaniu wysłanego do niego pocztą nadzwyczajną rozkazu aresztowania (podejrzanego – dop. aut.) Laa (Biuletyn z dnia 19 tego miesiąca). Do aresztowania doszło trzy ligi przed Bordeaux. Nie znaleziono przy nim żadnych interesujących dokumentów na jego temat, żadnych wskazówek co do jego misji. W trakcie przesłuchania przyznał, że pochodzi z Anglii […]. Zostanie przeniesiony do Paryża, gdzie skonfrontuje się go albo z kobietą, której przekazał ostatnio przesyłkę, albo z Rosembergerem, jego towarzyszem podróży, podającym się z kolei za towarzysza podróży muzyka André. Uzyskaliśmy nowe informacje na temat André, który jest kojarzony z Laa. Wiemy z całą pewnością, że osiedlił się w Offenbach jako rytownik i handlarz nutami. […] jego dom był azylem Francuzów (antynapoleońskich – dop. aut.), którzy schronili się w Offenbach, zwłaszcza de Sanroberta – zarządcy księcia d'Enghien, opata Villeton – kapelana księcia Condé i innych. Otrzymywał dla nich z Londynu pensje, korespondencję i gazety wysyłane im przez księcia Monako. Poprzez swój handel utrzymuje kontakty w Anglii i na całej północy. Około rok temu odbył podróż do Anglii przez niemieckie miasto Husum wraz z Rosembergerem, swoim rzekomym sekretarzem; został następnie zakwalifikowany jako agent korespondencyjny wroga. **Departament Deux-Sèvres**: Prefekt informuje o sytuacji w okręgach Bressuire i Parthenay, gdzie właśnie odbył podróż […] na czele oddziału szaserów. W poprzednich latach wszyscy mieszkańcy chowali się i zamykali drzwi, gdy zbliżał się urzędnik lub kilku żołnierzy. Obecnie wszyscy okazują największą radość, rozpalają ogniska z okazji wstąpienia Jego Królewskiej Mości na tron Włoch, częstują żołnierzy, tańczą z nimi. **Veran Coignat**: człowiek zatrzymany w Lyonie, skazany zaocznie przez sąd karny Górnego Renu na karę śmierci za rozbój. Zaproponował udostępnienie pewnych rewelacji w związku ze znaczną kradzieżą popełnioną w Thermidorze XII roku w sklepie pana Gubiana, producenta jedwabiu w Lyonie, pod warunkiem że nie zostanie on postawiony przed trybunałem. Komisarz generalny złożył mu obietnicę i uzyskał od niego informacje, które doprowadziły do odkrycia skradzionych dóbr, a także syndyków i większości sprawców. […] **Różne wydarzenia**: […] Le Havre – Przybycie pruskiego statku *La Vigilance*. Komisarz generalny umieścił jedenastu marynarzy pod specjalnym nadzorem; Ille-et-Vilaine – niejaki Coesbone, były szuan, nadal wydaje się prowadzić aktywność agenturalną. Wiemy, że próbował w przebraniu kobiety zwerbować młodego mężczyznę w rejonie Paryża. […] **Raport prefekta policji**: do Paryża przybył węgierski hrabia de Jekete; Aresztowano trzynastu złodziei; Na giełdzie słabo, przy zamknięciu 60.35 […][48].

[48] E. d'Hauterive, *La police secrète du premier empire. Bulletins quotidiens adressés par Fouché à l'Empereur*, Paris 1908, s. 476–477.

Cesarskie biuletyny przetrwały w archiwach i stanowią podstawowe źródło wiedzy na temat decyzji strategicznych oraz politycznych Napoleona. Rola analizy, przetwarzania i dostarczania istotnych informacji politycznych sprawia, że policja stanowiła rzetelne źródło szczegółowej wiedzy dla Napoleona, który siłą rzeczy pozostawał w izolacji od problemów społeczeństwa oraz wydarzeń na odległych terenach.

Żandarmeria i żandarmeria elitarna

Koncepcja oddziałów policyjnych, które działałyby w ramach organizacyjnych wojsk lądowych na terytoriach peryferyjnych, uchodziła w nowożytnej Europie za nowatorski pomysł. Powołanie formacji żandarmów jest osiągnięciem rewolucyjnej Francji. Zgromadzenie Narodowe w 1791 r. powołało żandarmów na wzór działającej w okresie monarchii dworskiej policji marszałkowskiej (fr. *Maréchaussée*). Stworzenie tej formacji i jej zadania wynikały przede wszystkim z licznych obostrzeń obejmujących policję cywilną, która w ówczesnej Europie ograniczała swoją działalność jedynie do miast i głównych traktów komunikacyjnych. Żandarmeria miała zatem odpowiadać przede wszystkim za egzekwowanie prawa w obszarach wiejskich i podmiejskich. Bardzo często stanowiła jedyny aparat przymusu reprezentujący władzę centralną. W opinii wielu badaczy, w tym Michaela Broersa, to właśnie funkcjonowanie żandarmerii odegrało istotną rolę w ostatecznej kolonizacji wsi oraz powiązaniu tożsamości chłopów z państwem rozumianym jako zespół rządu i rozmaitych instytucji obradujących w stolicy[49].

Duże znaczenie dla rozwoju napoleońskiej żandarmerii mieli generał Étienne Radet (1762–1825) oraz marszałek Bon Adrien Jeannot de Moncey (1754–1842). Pierwszy z nich był praktykiem, który od czasu przejęcia kontroli w 1798 r. nad małym legionem żandarmerii w Awinionie reorganizował formację i uczynił z niej skuteczne wsparcie dla wojsk francuskich walczących we Włoszech. W wizji Radeta żandarmi mieli pełnić funkcję zbrojnego ramienia policyjnego, które niejako z zewnątrz miało zapewniać stabilizację peryferiów. Ponadto kariera żandarma miała być objęta licznymi obostrzeniami – w przeciwieństwie do wojska, za którym poruszały się dziesiątki markietanów, służących i członków rodzin – żandarmi zawsze byli skoszarowani poza obrębem zabudowań wsi i miast, nie mogli też z zasady pełnić służby w rodzimych departamentach, a co więcej, mieli kategoryczny zakaz

[49] M. Broers, *The Napoleonic Gendarmerie. The state on the periphery made real*, „Crime, History & Societies" 2016, t. 20, nr 1, s. 93. https://doi.org/10.4000/chs.1641.

bliższych kontaktów z miejscowymi[50]. Poza regulaminem i warunkami samej służby istotna była także pozycja żandarmerii w systemie polityczno-militarnym Francji. Szczególnie tą kwestią zajmował się marszałek de Moncey, który w 1801 r., w randze generała, został wyznaczony przez Bonapartego na stanowisko generalnego inspektora żandarmerii. Pod jego auspicjami w tym samym roku przeprowadzono reformę organizacyjną służby. Przekształcono żandarmerię w jednolity korpus, który podzielono kolejno na 26 legionów, dzielących się na dwa szwadrony po dwie kompanie każdy. Podstawową jednostką organizacyjną była brygada, składająca się z podoficera i pięciu żandarmów, która nadzorowała określony obszar każdego departamentu[51]. Liczebność formacji wynosiła między 12 000 (26 legionów w 1800 r.) a 30 000 (40 legionów w 1813 r.) ludzi[52].

Kwestią sporną pozostawał status żandarmów, który opierał się na łączeniu charakteru wojskowego z realizowaniem zadań cywilnych. Formacja formalnie podlegała Ministerstwu Wojny, lecz musiała współpracować także z Ministerstwem Policji, które usiłowało maksymalnie rozszerzać swoje wpływy. Do obowiązków generalnego inspektora żandarmerii należało sporządzanie regularnych raportów ministrowi policji[53] oraz przyjmowanie wskazówek operacyjnych dotyczących np. poszukiwanych przestępców. Ministerstwo Policji współpracowało także z żandarmerią w zakresie prowadzenia wywiadu wewnętrznego[54]. De Moncey dążył jednak do całkowitej separacji żandarmerii i nie pozwalał swoim oficerom na raportowanie bez jego wiedzy ministrowi policji.

Z punktu widzenia bezpieczeństwa państwa żandarmerii przypisuje się przede wszystkim kompetencje kontrwywiadowcze oraz kontrpowstańcze. Ściganie dezerterów, pacyfikacja rozruchów i obowiązki patrolowe sprawiały, że żandarmi mieli dobre rozeznanie w sytuacji lokalnej. Odzwierciedleniem tego są fragmenty biuletynów cesarskich, w których czytamy o: (…) *ludziach z Dordogne sprzeciwiających się utworzeniu nowej dynastii przez Napoleona*, o rozbijaniu grup przestępczych: (…) *w departamencie Orne*, *o ruchach przywódców szuańskich i ich obrocie gotówką*, a nawet o dwóch niepokornych emigrantach, którzy w Bourg-sous-la-Roche ośmielili się wyjść z mszy świętej (…) *w momencie rozpoczęcia Te Deum ku czci Cesarza*[55].

---

[50] Kwestia ta dotyczyła przede wszystkim zakazu małżeństw z miejscowymi kobietami. Praktyka ta pomimo zakazu była często spotykana, co skutkowało licznymi zwolnieniami ze służby, a nawet dezercjami. Zob. szerzej: M. Broers, *The Napoleonic Gendarmerie*…, s. 96.

[51] C. Emsley, *Gendarmes and the State in Nineteenth-Century Europe*, New York 1999.

[52] *Police et Gendarmerie dans l'Empire napoléonien*, J.O. Boudon (red.), Paris 2013, s. 23–24.

[53] G. Arboit, *Napoleon et le renseignement*…, s. 39.

[54] J. Fouché, *Mémoires de Joseph Fouché…*, s. 211.

[55] E. d'Hauterive, *La Police Secrète du Premier Empire…*, s. 27, 39, 62.

Przy okazji reformy z 31 lipca 1801 r.[56] postanowiono utworzyć również nową, wyjątkową ze względu na swój status formację elitarnej żandarmerii gwardii (fr. *Gendarmerie d'élite de la Garde*). Pomimo współdzielenia podobnej nazwy obie formacje miały zupełnie odmienny zakres działań i pełniły inne funkcje w systemie bezpieczeństwa Francji. W ramach konsularnych oddziałów gwardyjskich dwa szwadrony odpowiadały za utrzymanie bezpieczeństwa publicznego i ochronę budynków oraz przedstawicieli rządu. W 1804 r. formację usamodzielniono i przemianowano na elitarnych żandarmów gwardii cesarskiej, a w 1806 r. uczyniono z niej wyłącznie formację konną podzieloną na szwadrony, w skład której wchodziło łącznie ok. 500 ludzi. Charakter elitarnych żandarmów był zatem bardziej wojskowy niż policyjny. Do ich głównych zadań należały ochrona cesarza wraz z jego dworem oraz wypełnianie specjalnych zadań dowódcy, którym w 1801 r. został pułkownik, później generał, marszałek i minister policji Anne Jean Marie René Savary, książę Rovigo (1774–1833).

Postać Savarego jest kolejną z istotnych w historii francuskich struktur wywiadowczych. Pełnił on funkcję szefa cesarskiego biura wywiadu i kontrwywiadu wojskowego (fr. *Bureau des renseignements*) w latach 1804–1809, a po dymisji Fouchégo został mianowany ministrem policji (1810–1814). Elitarna żandarmeria uczestniczyła bezpośrednio w tej działalności, lecz jedynie w roli operacyjnego narzędzia wykorzystywanego m.in. w celu przekazywania korespondencji oraz interweniowania w miejscach niedostępnych dla regularnych sił. Stanowiła także doskonałe zaplecze finansowo-organizacyjne dla działalności szpiegowskiej swojego szefa. W ramach przynależności do żandarmerii swoje działania prowadził m.in. słynny osobisty szpieg Savarego – Karl Ludwig Schulmeister[57]. Istnieje przynajmniej kilka świadectw zaangażowania elitarnych żandarmów w akcje kontrwywiadowcze. Savary najpierw incognito, a później przy wsparciu swojej formacji tropił szuańskich spiskowców w Wandei między 1803 a 1804 r.[58] Zgodnie z biuletynami policyjnymi zlecał również zatrzymania potencjalnie niebezpiecznych ludzi, np. fałszerzy lub informatorów mających kontakty zagraniczne[59]. Elitarni żandarmi uczestniczyli także w niesławnym wtargnięciu na terytorium neutralnej Badenii i aresztowaniu Ludwika Antoniego de Bourbon-Condé, znanego jako książę d'Enghien[60], podejrzanego o aktywność szpiegowską i skazanego na wyrok śmierci.

---

[56] *L'arrêté du 12 thermidor an IX (31 juillet 1801)*, http://lecahiertoulousain.free.fr/Textes/arrete_an_9.html [dostęp: 1 I 2025].

[57] G. Arboit, *Napoleon et le renseignement*…, s. 345–346.

[58] E.M. de Saint-Hilairé, *George, Moreau i Pichegru*, w: *Napoleon*, Gdańsk 2009, s. 163–164.

[59] E. d'Hauterive, *La Police Secrète du Premier Empire*…, s. 178, 220.

[60] E.M. de Saint-Hilairé, *Książę d'Enghien*, w: *Napoleon*, Gdańsk 2009, s. 89–151.

Podsumowanie

Epoka napoleońska przyczyniła się do wzrostu znaczenia służb cywilnych w prowadzeniu niejawnej aktywności państwa francuskiego. Świadczy o tym niespotykany wcześniej rozwój instytucjonalny formacji policyjnych i żandarmerii. W ramach swoich aktywności utworzyły one skuteczną sieć informacyjną, za pomocą której regularnie przekazywano wiadomości najważniejszym decydentom w państwie. Warunki, w jakich pracowali funkcjonariusze publiczni, sprawiły, że ten system wykształcił nietypowe, charakterystyczne cechy.

Niewiadoma pozostaje odpowiedź na pytanie o losy francuskiej myśli wywiadowczej w kontekście przetrwania pierwszego cesarstwa na mapie politycznej Europy. Lata 1812–1814 oznaczały całkowity kolaps opisanego wyżej systemu, a także rozpad więzi personalnych, które wydawały się rdzeniem funkcjonowania półformalnych struktur szpiegowskich. Systemowa odporność służb cywilnych w związku z niepowodzeniami wojennymi również okazała się niewystarczająca – jeszcze w październiku 1812 r. zamach stanu przeprowadzony przez gen. Claude-François Maleta doprowadził do aresztowania ministra policji Savary'ego, co skompromitowało całą instytucję[61]. Porażka kampanii rosyjskiej z 1812 r. oznaczała również drastyczne ograniczenie dostępu do personelu (armia stała się priorytetem ratowania sytuacji na licznych frontach) oraz środków finansowych.

W ostatnich latach funkcjonowania pierwszego cesarstwa (1811–1814) widoczny był systematyczny wzrost znaczenia struktur wywiadu cywilnego dla Napoleona i jego interesów. W 1811 r. z inicjatywy Napoleona doprowadzono do utworzenia Biura Statystyk Zagranicznych (fr. *Bureau Statistique*)[62] przy Ministerstwie Spraw Zagranicznych oraz wprowadzenia *Dekretu dotyczącego organizacji policji cesarstwa*[63]. Uwagę przywiązywano także do logistycznego usprawnienia komunikacji w ramach wielkiego imperium – wydawano rozporządzenia organizujące system kurierski oraz inwestowano w nowe technologie, np. sieć telegraficzną[64]. Silna pozycja wysokiej policji, system prefekturalny, a także rozbudowane formacje żandarmerii przetrwały upadek napoleońskiego cesarstwa i stały się w XIX w. podstawą polityki bezpieczeństwa nie tylko samej Francji, lecz także innych państw europejskich, które kopiowały i implementowały skuteczne rozwiązania.

---

[61] Tenże, *Zamach Maleta w roku 1812*, w: *Napoleon*, Gdańsk 2009, s. 34–39.

[62] A. Nieuważny, *Wywiady twarzą w twarz*…, s. 18.

[63] *Règlement sur l'organisation de la police de l'Empire le 25 mars 1811*. Zob. O. Brun, J. Poirot, *Le renseignement français en 100 dates*, Paris 2021, s. 73–75.

[64] J.C. Quennevat, *Napoléon et les télécommunications*, „Revue du Souvenir Napoléonien" 1975, nr 280, s. 2–18.

Bibliografia

Arboit G., *Napoléon et le renseignement*, Paris 2022.

Belloc A., *Les postes françaises: recherches historiques sur leur origine, leur développement, leur législation*, Paris 1886.

Bobiatyński K., *Wywiad działający z terenu Księstwa Warszawskiego przed wojną 1812 roku,* „Teka Historyka" 2001, z. 20, s. 19–59.

Broers M., *The Napoleonic Gendarmerie. The state on the periphery made real*, „Crime, History & Societies" 2016, t. 20, nr 1, s. 91–105. https://doi.org/10.4000/chs.1641.

Brun O., Poirot J., *Le renseignement français en 100 dates*, Paris 2021.

*Correspondance de Napoléon I^er^*, t. 10, 16, Paris 1864.

Czartoryski A., *Sprawozdanie z roku 1804 dla Senatu*, w: A. Czartoryski, *Pamiętniki ks. Adama Czartoryskiego i korespondencya jego z cesarzem Aleksandrem I*, t. 2, Kraków 1905.

Denécé E., Léthenet B.*, Renseignement et espionnage du Premier Empire à l'affaire Dreyfus (XIXe siècle)*, Paris 2021.

d'Hauterive E., *La police secrète du premier empire: Bulletins quotidiens adressés par Fouché à l'Empereur*, Paris 1908.

Dziekoński T., *Życie marszałków francuzkich z czasów Napoleona*, Warszawa 1841.

Emsley C., *Gendarmes and the State in Nineteenth-Century Europe*, New York 1999.

Fouché J., *Mémoires de Joseph Fouché, Duc d'Otrante. Ministre de la Police Générale*, Osnabrück 1966.

Gill P., Phythian M., *Intelligence in an Insecure World*, Cambridge–Malden 2012.

Gruszczak A., *Studia wywiadowcze jako poddyscyplina nauk o bezpieczeństwie: kierunki rozwoju*, w: *Bezpieczeństwo. Dyscyplina nauki wobec funkcjonowania państwa*, R. Skarzyński, E. Kużelewska (red.), Białystok 2018.

Hughes-Wilson J., *The Secret State: A History of Intelligence and Espionage*, New York––London 2017.

Las Cases E. de, *Memoriał ze św. Heleny*, t. 1, Gdańsk 2008.

Laurent S.Y., *Le secret de l'État: Surveiller, protéger, informer. XVIIe-XXIe siècle*, Paris 2015.

Łysiak W., *Napoleon fortyfikator [rozprawa doktorska]*, Warszawa 2012.

Milewski D., *Napoleoński wywiad na Rosję w Księstwie Warszawskim przed wojną 1812 roku*, „Echa Przeszłości" 2010, nr 11, s. 145–172.

Montholon M., *Récits de la captivité de l'empereur Napoléon à Sainte-Hélène*, t. 1, Paris 1847.

Nieuważny A., *Wywiady twarzą w twarz*, „Mówią Wieki" 2012, nr 2, s. 17–21.

Piekałkiewicz J., *Dzieje szpiegostwa*, Warszawa 1999.

Police et Gendarmerie dans l'Empire napoléonien, J.O. Boudon (red.), Paris 2013.

Quennevat J.C., *Napoléon et les télécommunications*, „Revue du Souvenir Napoléonien" 1975, nr 280, s. 2–18.

Roberts A., *Napoleon Wielki*, Warszawa 2015.

Roucaud M., *De l'opérationnel au policier: les officiers de Napoléon face à la pratique du renseignement*, „Napoleonica. La Revue" 2016, nr 27, s. 62–83.

Saint-Hilairé E.M. de, *Napoleon*, Gdańsk 2009.

Savant J., *La vie aventureuse de Vidocq*, Paris 1973.

Skowronek J., *Z magnackiego gniazda do napoleońskiego wywiadu. Aleksander Sapieha*, Warszawa 1992.

Sparrow E., *Secret Service. British Agents in France 1792–1815*, Woodbridge 1999.

Stokle M., *The bankers of Brumaire: the financiers behind Napoleon's Ascent*, PhD thesis, University of Glasgow, April 2020.

Tulard J., *Joseph Fouché*, Warszawa 2021.

Źródła internetowe

Louvre Collections, *Portefeuille à soufflet*, https://collections.louvre.fr/ark:/53355/cl010115454 [dostęp: 5 II 2025].

Napoléon & Empire, *Conseillers d'État du Consulat et de l'Empire*, https://www.napoleon-empire.org/institutions/liste-conseillers-etat-premier-empire.php [dostęp: 5 II 2025].

Akty prawne

Code pénal de 1810. Édition originale en version intégrale, publiée sous le titre: CODE DES DÉLITS ET DES PEINES, https://ledroitcriminel.fr/la_legislation_criminelle/anciens_textes/code_penal_1810/code_penal_1810_1.htm [dostęp: 1 I 2025].

L'arrêté du 12 thermidor an IX (31 juillet 1801), http://lecahiertoulousain.free.fr/Textes/arrete_an_9.html [dostęp: 1 I 2025].

Le décret du 5 février 1810, https://www.siv.archivesnationales.culture.gouv.fr/siv/recherche-consultation/consultation/ir/consultationIR.action?irId=FRAN_IR_058772&details=true&gotoArchivesNums=false&udId=root&auSeinIR=true [dostęp: 1 I 2025].

Loi du 28 pluviôse an VIII, https://carnetsdenotes.fr/loi_du_28_pluviose_an_8.htm [dostęp: 1 I 2025].

Règlement sur l'organisation de la police de l'Empire le 25 mars 1811.

Szymon Główka

Student bezpieczeństwa narodowego na Wydziale Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego, historii na Wydziale Historycznym UJ oraz filozofii na Wydziale Filozoficznym UJ. Interesuje się zagadnieniami z pogranicza filozofii politycznej oraz nauk o bezpieczeństwie.

VARIA

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 219–232

https://doi.org/10.4467/20801335PBW.25.010.22176

VARIA

Bezpieczeństwo to wspólna sprawa!

W styczniu 2025 r. Polski Instytut Kontroli Wewnętrznej zorganizował konferencję pt. „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej". O wnioskach płynących z tego spotkania, roli kontroli wewnętrznej i zewnętrznej w zarządzaniu organizacją, dobrych praktykach i wyzwaniach w tym obszarze, jak również o potrzebie podnoszenia świadomości zagrożeń wśród pracowników zatrudnionych w podmiotach objętych statusem infrastruktury krytycznej, z **Ireneuszem Jabłońskim** i **Piotrem Grzybowskim**, członkami zarządu PIKW, rozmawia Daria Olender.

Ireneusz Jabłoński (z lewej) i Piotr Grzybowski

Daria Olender: Co zainspirowało Polski Instytut Kontroli Wewnętrznej do zorganizowania konferencji poświęconej zarządzaniu kryzysowemu i ochronie infrastruktury krytycznej?

Ireneusz Jabłoński: Przede wszystkim dynamicznie zmieniająca się sytuacja geopolityczna na świecie. Mieliśmy do czynienia z pandemią COVID-19, mamy wojnę w bliskim sąsiedztwie i inne konflikty, np. eskalację na linii Izrael–Palestyna. Jako kraj europejski zaczynamy zdawać sobie sprawę z dużego ryzyka zaistnienia zagrożeń i pozamilitarnych, i militarnych, które dotychczas postrzegaliśmy jedynie w kategorii potencjalnych. Pożar mostu Łazienkowskiego w Warszawie w 2015 r. spowodował, że zapaliła się czerwona lampka, zwłaszcza że jako przyczynę ekspertyzy wskazały podpalenie. Minęło kilka lat i doświadczyliśmy niemal symultanicznych pożarów – spłonęły Centrum Handlowe Marywilska 44 i składowiska odpadów, ogień wybuchł w pobliżu dużych fabryk i portów. To pokazało, jak ważne jest kompleksowe zadbanie o to, by nie dochodziło do takich zdarzeń. W PIKW, który zajmuje się problematyką zarządzania organizacją, uznaliśmy, że kwestie ważne dla bezpieczeństwa należy przedyskutować na szerszym forum.

Jesteśmy w przededniu wprowadzenia nowelizacji ustawy o zarządzaniu kryzysowym. Temat idealnie się wpisuje w te komponenty, o których traktuje model COSO opisany w publikacji *Kontrola wewnętrzna – zintegrowana struktura ramowa*[1]. W ramach tego modelu musimy zarządzać ryzykiem, identyfikować je, szacować i oceniać oraz właściwie na nie reagować. Nie można mówić o właściwym zarządzaniu organizacją, jeśli nie weźmie się pod uwagę sytuacji zewnętrznej. Jestem zdania, że jeśli dziś nie zajmiemy się zarządzaniem kryzysowym, to z czasem możemy nie mieć czego audytować i kontrolować. Kiedyś uważałem, że zarządzanie kryzysowe to problem innych, że powinien się o to martwić wojewoda czy inny samorządowiec. Dziś wiem, że to dotyczy każdego z nas. W PIKW doszliśmy do wniosku, że jeżeli w dobie tylu wyzwań i zagrożeń nie zaczniemy się tym tematem bardziej interesować, nie uwzględnimy go w programach naszych szkoleń, to zmniejszy się grono osób, które będą miały właściwe wyobrażenie o roli zarządzania kryzysowego.

[1] *Kontrola wewnętrzna – zintegrowana struktura ramowa*, Warszawa 2008, Polski Instytut Kontroli Wewnętrznej. COSO to akronim od angielskiej nazwy Internal Control – Integrated Framework. Wszystkie przypisy w tekście pochodzą od redakcji.

Podczas konferencji omówiliśmy najważniejsze zagadnienia związane z tym zarządzaniem, prześledziliśmy, jak ewoluuje prawo, by sprostać wyzwaniom dynamicznie zmieniającej się rzeczywistości. Dyskutowaliśmy m.in. o zmianach w polskim prawie, które są podyktowane unijnymi regulacjami – dyrektywą o odporności podmiotów krytycznych, tzw. dyrektywą CER, oraz dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, tzw. dyrektywą NIS 2, a także unijnym rozporządzeniem o cyfrowej odporności operacyjnej, tzw. rozporządzeniem DORA. Mówiliśmy również o ustawie o krajowym systemie cyberbezpieczeństwa, będącej odpowiedzią na dyrektywę NIS 2, a także o cyberbezpieczeństwie, rozwoju nowych technologii i ich wykorzystaniu w ochronie infrastruktury krytycznej. Skorzystam z okazji i podziękuję naszym prelegentom za inspirujące wystąpienia, praktyczne wskazówki i podzielenie się swoim doświadczeniem.

Piotr Grzybowski: Nowelizacja ustawy o zarządzaniu kryzysowym wprowadza wiele istotnych zmian, w tym rozszerzenie listy podmiotów o statusie infrastruktury krytycznej, co pozwoli skuteczniej chronić zasoby i systemy kluczowe dla funkcjonowania państwa. W dobie dynamicznych zmian w sytuacji geopolitycznej, ewoluujących zagrożeń oraz licznych, stale rosnących wyzwań związanych z bezpieczeństwem narodowym, konieczność adaptacji przepisów prawa do nowych realiów wydaje się priorytetem. Istotnym elementem nowelizacji jest ustanowienie funkcji koordynatora bezpieczeństwa infrastruktury krytycznej. Jego rolą będzie nie tylko nadzorowanie działań związanych z ochroną kluczowych zasobów, lecz także zapewnienie spójności i skuteczności podejmowanych działań na poziomie strategicznym. Rozwiązanie to ma na celu wzmocnienie współpracy między podmiotami odpowiedzialnymi za bezpieczeństwo, w tym – sektorem publicznym a prywatnym, co ma się przełożyć na podniesienie poziomu ochrony. To dowodzi rozumienia tego, że ochrona infrastruktury krytycznej jest zadaniem wymagającym zaangażowania wielu interesariuszy i kooperacji na wielu poziomach.

W kontekście organizacji konferencji dodam, że PIKW, którego początki sięgają lat 90., wywodzi się z edukacji. Jednym z naszych kluczowych zadań jest podnoszenie świadomości i szkolenie. Otwieramy oczy na problemy dostępności produktów, funkcjonalności usług, na bezpieczeństwo dnia codziennego, które, mam wrażenie, przez dekady wydawało się dane na zawsze. Woda w kranie, gaz w kuchence, prąd w gniazdku

nie podlegały wątpliwości. A teraz wojna i coraz liczniejsze akty sabotażu czy dywersji uświadomiły nam, że to może zostać zakłócone.

Świadomość konieczności ochrony infrastruktury krytycznej powinna dotyczyć każdego szczebla organizacji, od szeregowego pracownika po kadrę kierowniczą?

P. G.: Tak. Każdy powinien dbać o bezpieczeństwo i wiedzieć, że gramy do jednej bramki. Wydaje mi się, że wiele osób funkcjonuje jakby w uśpieniu – jest jak jest, ale koło toczy się dalej. Uważam, że wielu pracowników podmiotów posiadających infrastrukturę krytyczną nie jest w wystarczającym stopniu uświadamianych, jak ważna jest ich rola, jak istotne znaczenie dla społeczeństwa i państwa ma miejsce ich pracy. W PIKW chodzi nam o to, by osoby, które szkolimy, audytorzy, pełnili później funkcję „przekaźników" – by informowali kadrę kierowniczą danego podmiotu, co jest ważne w jego strukturze. Kierownictwo powinno z kolei przekazywać tę wiedzę podwładnym. Pracownik mający taką świadomość będzie czuł się bardziej odpowiedzialny za to, by dostrzec zaniechania czy niedociągnięcia i je zgłosić. Polityka kadrowa w takich miejscach powinna polegać na tym, by doceniać osoby na najniższych szczeblach.

I. J.: Kiedyś ktoś pokazał audytora w ten sposób, że umieścił w ramach piramidy poszczególne grupy pracowników – od szczebla niższego, przez średni i kierowniczy po prezesa, który znajduje się na samej górze i nie widzi wszystkiego, co się dzieje poniżej. Audytor natomiast stoi z boku i krytycznie przygląda się całości.

P. G.: Jest on osobą, która ma wskazywać luki, czynniki ryzyka. Ma pokazywać, co należy bądź można udoskonalić, a także zwracać uwagę na rolę procesu zarządzania kryzysowego i ochrony infrastruktury, zwłaszcza infrastruktury krytycznej. Ważne jest, by kadra zarządzająca w podmiocie poddanym audytowi ufała jego ocenie. Oczywiście, to od kierownika jednostki zależy, czy wdroży wnioski z audytu, czy zleci dodatkową analizę.

Według jakich kryteriów ocenia się dobre zarządzanie organizacją?

I. J.: Wiedza na ten temat jest zawarta w wytycznych COSO *Kontrola wewnętrzna – zintegrowana struktura ramowa*. Model zarządzania organizacją wynikający z tych wytycznych stanowi fundament działalności PIKW. Na jego kanwie skodyfikowano w ustawie o finansach publicznych[2] pojęcie kontroli zarządczej oraz określono standardy kontroli zarządczej dla sektora finansów publicznych. Wytyczne COSO, opublikowane w 1992 r., zrewidowane i zaktualizowane w 2013 r., pokazują organizację w praktycznym wymiarze oraz odpowiadają na pytanie, jak należy nią skutecznie zarządzać. Wszystkie działania, które obejmuje kontrola wewnętrzna, są realizowane przez człowieka bądź pod jego kontrolą, dlatego zawsze trzeba mieć na uwadze możliwość popełnienia błędów, zmowę pracowników czy niewłaściwe działanie pod presją kierownictwa lub czasu. Kompleksowy model zarządzania, jaki proponuje COSO, składa się z pięciu elementów, tj. środowiska kontroli, oceny ryzyka, działań kontrolnych, informacji i komunikacji, monitoringu. W organizacji powinny one działać w sposób zintegrowany i stwarzać ramy umożliwiające opis i analizę funkcjonującej w organizacji kontroli wewnętrznej, która zapewnia skuteczną realizację celów biznesowych. Polski Instytut Kontroli Wewnętrznej przetłumaczył wytyczne COSO, a następnie stosował i wdrażał rekomendowane rozwiązania w biznesie, jak również w sektorze finansów publicznych w celu zbudowania efektywnie działającego systemu kontroli wewnętrznej.

[2] *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych* (DzU z 2009 r. nr 157 poz. 1240). Zob. także: *Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych* (Dz. Urz. MF z 2009 r. nr 15 poz. 84).

Koncepcja ram COSO

Ramy COSO obejmują kilka ważnych stwierdzeń:

- Kontrola wewnętrzna jest procesem. Jest środkiem prowadzącym do celu, a nie celem samym w sobie.
- Kontrola wewnętrzna zależy od ludzi. To nie tylko polityka, podręczniki i formy, lecz także ludzie na każdym szczeblu organizacji.
- Rola kontroli wewnętrznej polega na dostarczaniu zarządzającym wyłącznie racjonalnego, a nie absolutnego zapewnienia, że cele będą osiągane.
- Kontrola wewnętrzna jest ukierunkowana na osiągnięcie celów organizacji w jednej bądź kilku odrębnych, lecz wzajemnie powiązanych kategoriach.

Pięć elementów ramowych kontroli wewnętrznej

1. Środowisko kontroli – baza dla pozostałych elementów kontroli wewnętrznej, nadaje ton organizacji, wpływając na świadomość. Czynniki środowiska kontroli obejmują uczciwość, wartości etyczne, styl kierownictwa operacyjnego, delegację systemów władzy, a także procesy zarządzania i rozwoju ludzi w organizacji.
2. Ocena ryzyka – bezwzględnie wymaga ustalenia celów organizacji, gdyż każdy podmiot, próbując wykorzystać rynkowe szanse, napotyka zagrożenia (zewnętrzne i wewnętrzne), które muszą zostać poddane ocenie. Identyfikacja i analiza ryzyka stanowią warunek ustalenia, w jaki sposób powinno się nim zarządzać.
3. Kontrola funkcjonowania – obejmuje kontrolę zgodności wielu różnorodnych działań (typu zgody, zezwolenia, weryfikacje, uzgodnienia, przeglądy działalności operacyjnej, podziały obowiązków) z obowiązującymi zasadami, procedurami i zarządzeniami. Działania kontrolne mają wymiar holistyczny – są prowadzone w całej organizacji, na wszystkich szczeblach i we wszystkich funkcjach.
4. Informacja i komunikacja – wymagają precyzji i transparentności. Systemy informacyjne odgrywają wiodącą rolę w systemach kontroli wewnętrznej, gdyż to one tworzą raporty zawierające informacje operacyjne, finansowe oraz te dotyczące zgodności. W szerszym znaczeniu skuteczna komunikacja musi zapewnić przepływ informacji z i do organizacji oraz w organizacji.
5. Monitoring – niezbędny nie tylko do oceny, lecz także do doskonalenia systemu kontroli wewnętrznej. Monitorowane procesy umożliwiają dokonanie oceny wydajności systemu w czasie, a wykrywane niespójności czy niedoskonałości można weryfikować i poprawiać i w ten sposób zapewniać ustawiczne korygowanie systemu.

Rozmawiamy o kontroli wewnętrznej, kontroli zarządczej, audycie. Wyjaśnijmy może, czym się różnią te pojęcia?

I. J.: Kontrola wewnętrzna jako pojęcie odnosi się do biznesu, w administracji natomiast mamy do czynienia z kontrolą zarządczą. Kontrola wewnętrzna to pewnego rodzaju dynamiczny system złożony z wielu mechanizmów i czynności, opisanych w procedurach, zarządzeniach, wymaganiach itd., występujący immanentnie w organizacjach, przedsiębiorstwach oraz jednostkach administracji rządowej i samorządowej. Ma on prowadzić do realizacji celów.

P. G.: Audyt ma charakter uzupełniający względem kontroli wewnętrznej rozumianej jako proces, stanowi element jej monitoringu i nie odpowiada za tę kontrolę. Jest ukierunkowany bardziej na usprawnienie organizacji niż na wykrywanie nieprawidłowości. To intensywnie rozwijający się obszar działania, w którym aktywnie uczestniczymy. Ideę audytu wewnętrznego zaczerpnęliśmy 20 lat temu z Zachodu i na dobre zagościła ona w naszym kraju wraz z przystąpieniem Polski do Unii Europejskiej.

I. J.: Dodam, że jest kontrola wewnętrzna jako proces, tj. z pięcioma elementami ramowymi, ale jest też kontrola wewnętrzna instytucjonalna, czyli komórka kontroli wewnętrznej, której pracownicy są odpowiedzialni za monitorowanie oraz wykrywanie naruszeń i incydentów i zapobieganie im.

P. G.: Ten model zarządzania, te pięć komponentów kontroli wewnętrznej, można odnieść także do organizacji zarządzającej infrastrukturą krytyczną, w której wszystko powinno być poukładane i spójne, aby zwiększyć gwarancję prawidłowego działania. Czasami rodzi to przesadę. Mamy np. teren, który kilka czy kilkanaście lat temu był przeznaczony pod infrastrukturę krytyczną, a teraz to puste pole, ale nadal strzeżone. Mamy etat, trzeba go wypełnić, mamy pieniądze pod koniec roku, trzeba je wydać, mimo że z początkiem kolejnego można byłoby je przeznaczyć na bardziej uzasadnioną inwestycję. To pokazuje, że nie zawsze właściwie wykorzystujemy siły i środki. Należy zatem bardziej skupić się na tym, czemu coś ma służyć, dostosować przepisy prawa, opracować adekwatne procedury, przeprowadzić konsultacje społeczne.

I. J.: We współpracy z Pawłem Cybulskim, byłym wiceministrem finansów oraz szefem Krajowej Administracji Skarbowej, opracowaliśmy

i wdrożyliśmy nowatorską procedurę kontroli biznesowej. Jej wdrożenie daje przedsiębiorcy solidne fundamenty do eliminowania nadużyć oraz świadczy o jego rzetelności i dobrej organizacji. Dzięki takiej procedurze firma może przedstawić inspektorowi kontroli skarbowej jasne, uporządkowane zasady działania i udowodnić, że podejmuje realne działania w zakresie zarządzania ryzykiem podatkowym. To było – i nadal jest – ważnym elementem budowania wiarygodności przedsiębiorstwa wobec organów administracji publicznej. W późniejszym etapie została wdrożona w Ministerstwie Finansów tzw. biała lista podatników VAT, która znacznie zwiększyła transparentność relacji gospodarczych. Ukazały się też wytyczne wskazujące na najistotniejsze elementy niezbędne do poprawnej weryfikacji własnych kontrahentów. Wspomniana procedura kontroli biznesowej to weryfikowanie kontrahenta zarówno pod kątem jego obecności na tej liście, jak i jego ogólnej kondycji finansowej, scoringu[3] oraz potencjalnych czynników ryzyka, które mogą się z nim wiązać. Świadome zarządzanie relacjami biznesowymi stało się więc nie tylko elementem dobrej praktyki, lecz także formą zabezpieczenia przed nieświadomym udziałem w mechanizmach wyłudzeń czy nadużyć podatkowych.

P. G.: Weryfikacja kontrahentów jest bardzo istotna zwłaszcza tam, gdzie w grę wchodzi bezpieczeństwo dostaw produktów i usług zapewniających funkcjonowanie strategiczne i rozwój państwa. Tam bezwzględnie należy być nadmiernie ostrożnym.

Wróćmy jeszcze do konferencji. Czy zaskoczyło Panów zainteresowanie tym spotkaniem?

I. J.: Tak, było naprawdę duże, zwłaszcza ze strony odbiorców ze wschodnich województw – z Podkarpacia, Podlasia i Lubelszczyzny. Uczestnicy podkreślali, że ważnym aspektem ich działalności jest świadomość w zakresie nowych wyzwań i zagrożeń, a także wiedza o działaniach, które mogą podjąć na poziomie lokalnym, by zminimalizować ryzyko, zwiększyć bezpieczeństwo bądź przynajmniej utrzymać je na akceptowalnym poziomie. Wydaje mi się, że uruchomiliśmy tym wydarzeniem pewien proces – rozpaliliśmy umysły tych, którzy do tej pory nie zdawali sobie sprawy z pewnych problemów, ale też tych, którzy mieli już ich

[3] Scoring – metoda oceny wiarygodności kredytowej.

świadomość, ale poszukiwali nowych rozwiązań. Dodam, że konferencja miała wyłącznie formułę stacjonarną, przygotowania do niej rozpoczęliśmy późno i nie była intensywnie promowana, więc tak duża frekwencja była dla nas zaskoczeniem.

P. G.: Tematyka zarządzania ryzykiem i ochrony infrastruktury krytycznej najwyraźniej jest aktualna dla wielu grup. Wolności i bezpieczeństwa nie dostaliśmy na zawsze i nie będziemy ich mieć, jeśli nie będziemy o nie dbać. Wymagamy tego od odpowiednich instytucji i podmiotów, zatem czują się one zobligowane do pogłębiania swojej wiedzy, poznawania nowych mechanizmów służących temu, aby jak najlepiej zabezpieczyć ciągłość dostaw usług kluczowych czy produktów niezbędnych do życia.

> **Duża popularność wydarzenia potwierdza potrzebę organizowania tego typu spotkań w gronie kontrolerów i audytorów. W mojej ocenie brak formuły online był właściwą decyzją. Dzięki temu mogły zostać poruszone tematy związane z bezpieczeństwem, które nie powinny trafić w eter.**

I. J.: Takie spotkania to świetna platforma wymiany doświadczeń i wzajemnych inspiracji. Uczestnicy konferencji podkreślali, że była to unikalna okazja, by wspólnie przeanalizować proponowane zmiany i wypracować rekomendacje odpowiadające wyzwaniom – tym aktualnym, i tym prognozowanym. Wśród naszych gości byli analitycy, umysły ścisłe, osoby, które znają technologie, produkcję, ale brakuje im wiedzy na temat całokształtu bezpieczeństwa. Wielu z nich doceniło odmienne doświadczenia prelegentów – ze sfery cyber, militarnej, metodyki ryzyka, ochrony środowiska, finansów czy spółek działających w różnych obszarach gospodarki. Przedstawienie bezpieczeństwa z kilku stron – od ochrony i kamer, przez zabezpieczenia w sferze prawnej czy cyber, po pracowników dopuszczających się sabotażu, czyli tzw. sześciopaku bezpieczeństwa, okazało się dobrym pomysłem. Uczestnicy chwalili też otwartość prelegentów na głosy z sali, dzięki czemu nie zabrakło pytań, ciekawych dyskusji i konstruktywnych wniosków ze strony przedstawicieli różnych branż i sektorów. Dotarcie do rynku z informacją to jedno, dotarcie skuteczne, czyli przekazanie jej w sposób zrozumiały dla odbiorcy, to drugie. Byli i tacy, którzy przyznali, że przed przyjściem na konferencję nie mieli świadomości wielu rzeczy, mimo że reprezentują podmiot ważny z punktu widzenia bezpieczeństwa państwa.

P. G.: Chciałbym dodać, że wśród pracowników jest teraz tendencja do hermetyczności, skupiania się na sobie i wąskim obszarze swojego działania. A praca w miejscu, które wiąże się np. z zapewnieniem ciągłości dostaw, wymaga szerszego myślenia. Bardzo często pracownicy zapominają o roli instytucji, w której pracują, a kierownicy o wadze tego, co nadzorują, że to nie są przykładowo tylko dwa tory i podsyp, lecz infrastruktura krytyczna o znaczeniu strategicznym. Podczas konferencji dyskutowaliśmy również o jednostkach wojskowych. Okazuje się, że strzegą nas wojskowi, których strzeże cywilny ochroniarz. To absurd. I nie twierdzę, że taki ochroniarz nie może być świetnie wyszkolony, ale to powinno podlegać weryfikacji.

W kuluarach miałem okazję porozmawiać o problemie, jakim jest utrzymanie ciągłości zarządzania organizacją. Niech dochodzi do zmian na stanowiskach kierowniczych, ale średni szczebel powinien realizować długofalową politykę firmy. W praktyce natomiast często mamy do czynienia z cykliczną wymianą. Nowi pracownicy dopiero się uczą, a tych doświadczonych już nie ma. Ktoś coś wcześniej zaczął, potem się tego nie kończy. A bywa też tak, że skoro tamci zaczęli, to trzeba to porzucić, bo pewnie było złe. W ten sposób powstaje chaos. Nierzadko wynika to z nadania politycznego. Taki nominat nie myśli długoterminowo, dba wyłącznie o tu i teraz. I tu otwiera się kolejny temat – planowanie strategiczne. Wektor bezpieczeństwa powinien być jednoznaczny i zapewniać stabilizację. Jeśli następuje zmiana kierunku myślenia, to musi ona mieć racjonalne uzasadnienie. Nie powinno być tak, że każda zmiana na kluczowych stanowiskach czy zmiana władzy powoduje rewolucję w funkcjonowaniu organizacji, gdyż to hamuje rozwój podmiotu, a czasem wręcz go uwstecznia. Rosnąca liczba obiektów o ważnym czy kluczowym znaczeniu dla bezpieczeństwa kraju wymaga uświadamiania pracowników – co już kilkukrotnie podkreślaliśmy – jak ważne jest ich miejsce i rola w systemie bezpieczeństwa państwa. Muszą mieć oczy szeroko otwarte i dostrzegać niebezpieczeństwa – i te rzeczywiste, i te ewentualne. Takie konferencje czy szkolenia powinny być cykliczne, by myślenie o bezpieczeństwie – również przez pryzmat wyzwań i zagrożeń – było na porządku dziennym i prowadziło do pewnego automatyzmu w działaniu. Warto np. przeprowadzać ćwiczenia ewakuacyjne czy ćwiczenia tzw. pamięci mięśniowej. To pozwoli minimalizować ryzyko, wykrywać i badać słabe strony, luki, podatności i dywersyfikować odpowiedzi na nie.

Jednym z walorów tej konferencji było zgromadzenie ludzi z doświadczeniem. Nawet ci prelegenci, którzy mieli stopnie naukowe, byli jednocześnie praktykami.

I. J.: Tego nauczyła nas organizacja studiów podyplomowych. Zrozumieliśmy, że na tym szczeblu edukacji kształcący się poszukują wykładowców z doświadczeniem praktycznym. Zaczynaliśmy od podziału pół na pół, jeśli chodzi o kadrę uczelnianą i praktyków, ale szybko się okazało, że ci pierwsi powielali materiał ze studiów I czy II stopnia bądź przekazywali suchy materiał. Kadra z zewnątrz wzbogacała go przykładami z pracy i służby, co pozwalało na unaocznienie problemów i sprzyjało podejmowaniu dyskusji.

P. G.: Wychodzimy z założenia, że studia podyplomowe mają dostarczyć narzędzi do pracy. Oczywiście, nie wykluczamy ludzi nauki, bo jeśli teoria współgra z praktyką, to mamy idealne połączenie. Można wtedy szerzej spojrzeć na dane zjawisko, powiązać różne jego aspekty. Staramy się angażować do współpracy osoby, które łączą nie tylko wiedzę i doświadczenie, lecz także umiejętność przekazu.

W konferencji wzięli udział, m.in. jako prelegenci, byli funkcjonariusze formacji mundurowych, służb, inspekcji i straży. Są oni szkoleniowcami również na kursach i studiach podyplomowych prowadzonych przez PIKW. Jak oceniają Panowie tę współpracę?

I. J.: W naszej działalności chętnie korzystamy ze wsparcia byłych i obecnych funkcjonariuszy i żołnierzy. Połączenie wiedzy i doświadczenia jest – jak już powiedziałem – bezcenne. Praktycy dają gotowe *case study*, a uczestnicy szkoleń mogą to przenieść na własny grunt, zweryfikować swój punkt widzenia. Dla nas pionierem takiej formuły szkoleniowej był insp. Marek Dyjasz, były dyrektor Biura Kryminalnego Komendy Głównej Policji. Opracował on szkolenie „Weryfikacja autentyczności dokumentów", które było impulsem do zmian na rynku. Obecnie na pozyskiwanie i analizę informacji patrzy się inaczej.

P. G.: Jako jedni z pierwszych zachęcaliśmy przedstawicieli służb do tego, by dzielili się swoją wiedzą i umiejętnościami. Dobrze jest, gdy audytor, będący kimś w rodzaju cywilnego policjanta, może rozwijać swoje umiejętności, ucząc się od tych, którzy dysponują zapleczem praktycznym. My to szkolenie uzupełniamy o wiedzę psychologiczną,

umiejętności miękkie, czerpiąc m.in. od psychologów policyjnych. Ta wymiana, w mojej ocenie, jest korzystna dla obu stron, gdyż dzięki takim spotkaniom funkcjonariusze mogą poszerzyć swoje wyobrażenie o tym, jakie są rzeczywiste, aktualne problemy. To wartość dodana.

Czy taka aktywność funkcjonariuszy wpływa waszym zdaniem na bardziej pozytywny odbiór służb?

P. G.: Zdecydowanie tak. Na tym rynku często funkcjonują ludzie, którzy są pasjonatami. Funkcjonariusze, którzy brali udział w konferencji czy nasi szkoleniowcy, to osoby z charyzmą. A tego właśnie oczekuje audytorium.

***

Ireneusz Jabłoński

Doświadczony trener biznesu w zakresie miękkich aspektów zarządzania organizacją. Członek zarządu i dyrektor operacyjny w Polskim Instytucie Kontroli Wewnętrznej, z którym jest związany od 20 lat. Posiada wykształcenie wyższe na kierunku zarządzanie, ze specjalizacją z psychologii zarządzania. Był trenerem wewnętrznym w koncernie energetycznym Vattenfall, uczestniczył w procesie prywatyzacji i restrukturyzacji Elektrociepłowni Warszawskich, następnie pracował jako menedżer HR w Totalizatorze Sportowym.

Piotr Grzybowski

Członek zarządu w Polskim Instytucie Kontroli Wewnętrznej, z którym jest związany od ponad 20 lat. Odpowiada głównie za finanse, usługi doradcze oraz organizację jednego z największych i najstarszych w Polsce branżowych wydarzeń konferencyjnych, jakim jest Międzynarodowy Kongres Kontroli, Audytu Wewnętrznego, Antykorupcji i Zwalczania Oszustw.

***

Konferencja „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej"

Warszawa, 22 stycznia 2025 r.

Infrastruktura krytyczna to krwiobieg naszego kraju, który dostarcza niezbędnych składników do życia. Jeśli przestanie funkcjonować, to wszystko inne również nie będzie mogło właściwie działać i spełniać swoich zadań lub celów.

Od elektrowni po sieci wodociągowe – nasza infrastruktura jest jak dom, który trzeba stale remontować i zabezpieczać. Ta konferencja to mapa drogowa do bezpieczniejszej przyszłości.

Mariusz Brzozowski, ekspert ds. antyterrorystycznej ochrony IK

Konferencja pt. „Ewolucja prawa w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej", w której wzięło udział 120 osób, zgromadziła specjalistów z obszaru bezpieczeństwa infrastruktury krytycznej. Problematyka poruszana podczas konferencji została zgrupowana w czterech blokach tematycznych.

Blok I – „Nowy porządek legislacyjny w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej", obejmujący wystąpienia:

1. „CER – nowatorskie rozwiązania w zarządzaniu bezpieczeństwem infrastruktury krytycznej".
2. „NIS 2 i DORA – dlaczego są istotne?".

Blok II – „Rozwój nowych technologii i ich wpływ na bezpieczeństwo", obejmujący wystąpienia:

1. „Zagrożenia cyber dla kluczowej infrastruktury RP".
2. „Cyberbezpieczeństwo z perspektywy atakującego. Zobacz, gdzie jest uchylone okno".
3. „Najlepszy zamek jest bezużyteczny, gdy stracimy klucze – bezpieczna orkiestracja kluczami kryptograficznymi".

Blok III – „Rozwój zasobów niezbędnych do życia – nowe wyzwania – nowe ramy prawne do ich ochrony", obejmujący wystąpienia:

1. „Ochrona transgranicznych inwestycji energetycznych".
2. „AI – jak wykorzystać potencjał rozwoju nowej technologii w bezpieczeństwie?".

Blok IV – „Połączenia potencjału wojskowego z cywilnym w ochronie infrastruktury krytycznej", obejmujący wystąpienia:

1. „Perspektywy zarządzania bezpieczeństwem morskiej infrastruktury krytycznej – koncepcja Cyfrowego Bałtyku".
2. „Zagrożenia wywiadowcze dla obiektów wojskowych i cywilnych – insider".

Uzupełnieniem wykładów były panele dyskusyjne z udziałem ekspertów reprezentujących różne obszary bezpieczeństwa.

Zdjęcie 1. Michał Krzykowski, prawnik, kierownik Laboratorium Infrastruktury Krytycznej i Energetyki WPiA UWM.

Zdjęcie 2. Radosław Kucik, ekspert ds. bezpieczeństwa, dyrektor sprzedaży w firmie Pentera.

Zdjęcie 3. Od lewej: Anna Mroczek (PGE S.A., PGE Baltica Sp. z o.o.), Artur Gębicz (IPS-SGB), Włodzimierz Cieślak (ekspert PISA), Gabriela Barwińska-Szczutkowska (RDOŚ w Bydgoszczy).

Zdjęcie 4. Alicja Hoc-Rolińska i Ireneusz Jabłoński z PIKW, prowadzący.

Zdjęcie 5. Paweł Cybulski, były wiceminister finansów i zastępca szefa Krajowej Administracji Skarbowej.

Źródło: materiały własne.

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 233–249

https://doi.org/10.4467/20801335PBW.25.011.22177

VARIA

Ochrona polskich obszarów morskich w teorii i praktyce

Duże tempo zmian w środowisku bezpieczeństwa powoduje, że konieczna jest szybka adaptacja do nowych wyzwań. Dotyczy to także domeny morskiej. Jakie są rzeczywiste i potencjalne zagrożenia w tym obszarze dla Rzeczypospolitej Polskiej? Co należy zrobić, by w sposób bardziej efektywny im przeciwdziałać? Jak zabezpieczać obiekty strategiczne usytuowane w polskich obszarach morskich? Na te pytania odpowiada **kmdr ppor. rez. Sebastian Kalitowski**, starszy oficer Marynarki Wojennej, były dowódca grupy specjalnej płetwonurków w Jednostce Wojskowej Formoza i oficer operacyjny wywiadu wojskowego. Pasjonat morza i ekspert w dziedzinie bezpieczeństwa morskiego. Doradza, uczy i dzieli się swoim bogatym doświadczeniem w ramach szkoleń i kursów, które organizuje i prowadzi wraz ze swoim zespołem profesjonalistów w pierwszej w Polsce i jednej z pierwszych w Europie firm z branży *maritime security*. Celem jest rzetelne przygotowanie specjalistów z zakresu ochrony obiektów portowych, morskiej infrastruktury krytycznej, morskich farm wiatrowych i statków.

Daria Olender: Panie Komandorze, czy we współczesnym środowisku morskim jest coś, co Pana zaskakuje?

Kmdr ppor. rez. Sebastian Kalitowski: Sytuacja geopolityczna i poziom zagrożeń na świecie w ostatnich dwóch latach znacznie się zmieniły. Nie należy zatem oczekiwać, że pozostanie to bez wpływu na globalną architekturę bezpieczeństwa morskiego. Długo wydawało się, że zagrożenia asymetryczne na morzu są właściwie rozpoznane i zdefiniowane – że mamy problemy z piractwem, terroryzmem, nielegalną imigracją, pasażerami na gapę, przemytem narkotyków, nielegalnymi połowami czy z cyberterroryzmem. Pojawiły się jednak nowe, np. wynikające z zakłócania sygnału GPS, wykorzystania statków z floty cieni oraz platform bezzałogowych. Wiele się zmieniło w związku z rozpoczętymi w 2023 r. działaniami Huti wymierzonymi w żeglugę międzynarodową, początkowo głównie w statki powiązane z Izraelem, co miało być wyrazem solidarności jemeńskich rebeliantów z Palestyną. Aktywność Huti próbują wykorzystać somalijscy piraci, którzy zwiększyli liczbę ataków w tym rejonie. Mam wrażenie, a wywiadem morskim i analizą bezpieczeństwa morskiego zajmuję się od 2007 r., że wszystko znacznie przyspieszyło w tym obszarze. To powoduje, że rozpoznanie zagrożeń i poszukiwanie skutecznych rozwiązań mitygujących ryzyko jest dużym wyzwaniem.

Jak ocenia Pan sytuację na Morzu Bałtyckim?

Bałtyk od 2023 r. stał się obszarem wysokiego ryzyka obok Morza Czarnego, Morza Czerwonego, Basenu Somalijskiego, zatok Perskiej i Omańskiej, Morza Południowochińskiego czy Zatoki Gwinejskiej. Obserwujemy na nim zwiększenie aktywności wywiadowczej, mapowanie dna przy morskiej infrastrukturze krytycznej (IK), sabotaże związane ze zrywaniem kabli podmorskich, sabotaże kinetyczne i niekinetyczne, zakłócenia systemu GNSS[1]. Rosja prowadzi na tym akwenie „wojnę cieni" wymierzoną w państwa Zachodu i NATO. Nie powinno to dziwić, bo przygotowywała się do niej od dziesięcioleci. Sporządzała m.in. matryce potencjalnych celów na morzu, ze świadomością, jak podatna na sabotaż i dywersję jest podwodna IK i jak wiele można osiągnąć,

[1] GNSS (ang. *Global Navigation Satellite System*) – Globalny System Nawigacji Satelitarnej. Wszystkie przypisy pochodzą od redakcji.

gdy zastosuje się środki poniżej progu wojny, ogólnodostępne i tanie. Do działań sabotażowych Rosjanie wykorzystują statki floty handlowej, aby nie można było uruchomić artykułu 5 traktatu północnoatlantyckiego. Wiedzą też, że takim działaniom niełatwo przypisać atrybucję i można wiarygodnie zaprzeczać sprawstwu. Jeśli w ciągu roku dochodzi średnio do ok. 200 uszkodzeń kabli podmorskich przez statki, które wloką kotwicę po dnie głównie z powodu ludzkich zaniedbań czy błędów, to trudno udowodnić umyślność takich działań. Wykorzystanie statków do sabotażu i dywersji jest znacznie tańsze niż użycie okrętów. Nie wspomnę już o maskowaniu i monitorowaniu. Rosjanie wiedzą, że są stale obserwowani przez siły NATO. Co ciekawe, stanowiska dowodzenia, okręty i jednostki Floty Bałtyckiej od września ubiegłego roku przeszły na systemy łączności *command and control communications* (C3), w paśmie VLF-SHF[2], których Rosjanie używają w czasie wojny. Wcześniej korzystali z nich podczas zimnej wojny.

Czy uprawnione jest stwierdzenie, że aktualna sytuacja w obszarze bezpieczeństwa morskiego to coś, z czym nie mieliśmy do czynienia od niemal 20 lat?

Tak, to prawda. Z podobną skalą zagrożeń mieliśmy do czynienia ok. 2008 r., kiedy doszło do nasilenia się piractwa w rejonie Rogu Afryki. Apogeum nastąpiło w 2010 r., gdy odnotowano 45 ataków na świecie, a 53 statki z 1174 marynarzami uprowadzono na wiele miesięcy dla okupu. Pomimo działań międzynarodowych i rozpoczęcia misji „Atalanta"[3], a także obecności kilku grup zadaniowych złożonych z okrętów przez wiele lat nie potrafiliśmy sobie poradzić z zagrożeniem w tym rejonie. Okazało się, że zwiększenie obecności marynarki wojennej nie rozwiązuje tego złożonego problemu. Wymierne efekty dało dopiero stworzenie systemu wielu współgrających elementów i przestrzeganie określonych zasad przez załogi statków.

[2] VLF (ang. *very low frequency*) – fale radiowe bardzo długie, o częstotliwości od 3 do 30 kHz, co odpowiada długości od 10 do 100 km. SHF (ang. *super high frequency*) – fale radiowe superkrótkie, o częstotliwości od 3 do 30 GHz i długości od 1 do 10 cm.

[3] European Union Naval Force Somalia – Operation Atalanta to wojskowa operacja morska Unii Europejskiej służąca zwiększeniu bezpieczeństwa w zachodniej części Oceanu Indyjskiego i na Morzu Czerwonym. Cele tej operacji to m.in.: ochrona transportów pomocy humanitarnej World Food Programme dla Somalii, eskortowanie okrętów z zaopatrzeniem dla sił operacji „Amisom" oraz udzielanie pomocy okrętom zaatakowanym przez piratów.

> **W kontekście Rogu Afryki dotknął Pan ważnej kwestii. Skuteczność wdrażanych rozwiązań w dużym stopniu zależy od odpowiedniego poziomu świadomości, przekonania o słuszności podjętych działań i zdyscyplinowania podczas ich realizacji.**

Te czynniki to fundament bezpieczeństwa. Świadomość sytuacyjna, przygotowanie członków załóg do incydentu ataku, stworzenie panic roomu zwanego na statkach cytadelą, ochrona pasywna oraz szersze wprowadzenie uzbrojonej ochrony – to elementy, które pozwoliły powstrzymać falę piractwa w Rogu Afryki. Moim zdaniem udało się to zrobić głównie dzięki działaniom prywatnych dostawców usług z zakresu bezpieczeństwa.

Na Bałtyku dobrze widać, jak Rosjanie wykorzystują to, że w krajach Zachodu brakuje świadomości dotyczącej działań hybrydowych. Dotychczas rozpoznawano i monitorowano okręty i siły Floty Bałtyckiej. Obecnie jednak Rosja posługuje się – jak już wspomniałem – statkami, a nie okrętami i siłami tej floty. W 2023 r. w ramach dziennikarskiego śledztwa niemieckich nadawców publicznych NDR i WDR oraz dziennika „Süddeutsche Zeitung" monitorowano rejsy rosyjskich statków badawczych, które według oficjalnej wersji prowadziły badania hydrograficzne na Bałtyku i Morzu Północnym. Na 400 przeanalizowanych rejsów w co najmniej 60 przypadkach stwierdzono operowanie statków w podejrzanie bliskiej odległości od obiektów IK. Jako przykład przywołam incydent z 17 maja 2025 r. Statek MV Sun z rosyjskiej floty cieni pływał w okolicach podwodnego kabla energetycznego SwePol Link. Zachowywał się, jakby chciał go zerwać za pomocą wleczonej kotwicy. Polska wysłała 20 maja w tamten rejon samolot patrolowo-rozpoznawczy M28B Bryza, a dzień później – okręt. Do momentu przybycia samolotu rosyjski tankowiec miał jednak dużo czasu nie tylko na sabotaż, lecz także na swobodne oddalenie się z miejsca działań. Na szczęście tym razem nie chodziło o zerwanie kabla, lecz o przetestowanie naszej gotowości do identyfikacji zagrożeń. Czego zabrakło po naszej stronie? Świadomości? Działań wywiadu morskiego, który powinien monitorować statki rosyjskiej floty cieni, przynajmmniej te poruszające się po polskiej wyłącznej strefie ekonomicznej (WSE), nie wspominając już o wodach terytorialnych? Powinniśmy wiedzieć, że statek określany w terminologii bezpieczeństwa morskiego jako „czerwona flaga" pojawił się w okolicach SwePol Link. Istnieje kilka, niestety bardzo drogich, narzędzi do monitorowania. Jedno z nich pozwala typować i śledzić podejrzane, nieintuicyjnie zachowujące

się jednostki, zmieniające nazwy i banderę, podszywające się pod statki, które już dawno zostały zezłomowane, czy wyłączające lub manipulujące nadajnikami AIS, czyli systemami automatycznej identyfikacji.

Powróćmy do problemu ewoluowania zagrożeń na morzu, wynikającego m.in. z wykorzystywania nowych technologii. Huti do atakowania statków używali np. dronów.

Gdy w 2021 r. doszło do ataku na tankowiec MT Mercer Street, który był pierwszym śmiertelnym atakiem terrorystycznym na statek przeprowadzonym z wykorzystaniem UAV[4], świat poznał kolejne zagrożenie. Zginęło wówczas dwóch członków załogi. Analizowaliśmy ten przypadek w Maritime Safety & Security, ale nie sądziliśmy, że tego typu ataki staną się tak powszechne i dwa lata później sparaliżują ruch na Morzu Czerwonym, Morzu Arabskim i w cieśninie Bab al-Mandab. Huti używali rakiet balistycznych i właśnie dronów, w tym dronów pływających. Działo się to na jednym z najważniejszych szlaków żeglugowych na świecie. Od rozpoczęcia patroli morskich w regionie w ramach operacji „Prosperity Guardian" i „Aspides" siły morskie Unii Europejskiej i brytyjska marynarka wojenna przechwyciły łącznie 32 bezzałogowe statki powietrzne, dwa drony pływające, a nawet jeden dron podwodny. Zniszczono również setki dronów typu Shahed, rakiet balistycznych i pocisków przeciwokrętowych.

Drony stały się istotnym elementem działań na morzu również podczas wojny rosyjsko-ukraińskiej.

To prawda, drony nawodne i podwodne są częścią działań asymetrycznych na Morzu Czarnym, a Ukraińcy dzięki nim skutecznie walczą ze znacznie silniejszymi siłami morskimi Federacji Rosyjskiej. Co więcej, wykorzystują te drony jako platformy do startów dronów latających FPV[5], a po uzbrojeniu skutecznie niszczą nimi cele powietrzne. Przykładowo, 2 maja 2025 r. w pobliżu Noworosyjska ukraiński dron morski zniszczył rosyjski samolot myśliwski Su-30. To był pierwszy w historii

[4] UAV (ang. *unmanned aerial vehicle*) – bezzałogowy statek powietrzny.

[5] FPV (ang. *first person view*, dosłownie: widok z pierwszej osoby) – to sposób sterowania dronem, w którym pilot widzi na żywo obraz przekazywany z drona.

wojen morskich przypadek, gdy dron pływający zniszczył nie jednostkę nawodną czy śmigłowiec przeciwnika, lecz samolot myśliwski.

Doświadczenia z działań wojennych na Morzu Czarnym pokazują, że platformę bezzałogową można dziś zbudować niemalże w warunkach garażowych, stworzyć ją na bazie skutera wodnego. Sterowana za pomocą łączności satelitarnej może wykonywać komendy operatora odległego nawet o 1000 km. W ten sposób Ukraińcy pozbawili Rosjan panowania na tym morzu. Koronnym przykładem schyłku teorii wojny morskiej adm. Alfreda Thayera Mahana[6] jest zniszczenie flagowego okrętu rosyjskiej Floty Czarnomorskiej – fregaty projektu 11356M Moskwa. Prawdopodobnie ta akcja będzie omawiana w uczelniach wojskowych i morskich. Rosja, widząc skuteczność ukraińskich dronów Sea Baby, Mamai, Magura, Magura V, Sea Baby II Awdijiwka oraz działań Huti na Morzu Czerwonym, również opracowała swoje bezzałogowe pojazdy nawodne. W ubiegłym roku Zakład Budowy Maszyn Kingisepp w Sankt Petersburgu zaprezentował pojazd o nazwie Oduvanchik. Dzięki możliwości przewożenia ładunku o masie do 600 kg stanowi on elastyczną platformę do realizacji misji o różnym charakterze. Rosjanie dysponują swoimi konstrukcjami dronów morskich: Riverine, Dandelion, Sargol.

Morskie farmy wiatrowe i inne obiekty morskiej IK mogą być atakowane tanimi improwizowanymi środkami bojowymi, takimi jak drony rekreacyjne FPV, których koszt produkcji i przygotowania do działań bojowych wynosi mniej niż 1000 euro. W konflikcie rosyjsko-ukraińskim są wykorzystywane tysiące takich dronów, także do ataków na instalacje energetyczne w Ukrainie i Rosji. Detonacja półtorakilogramowej bomby termobarycznej, wartej 1500 euro, może skutecznie przebić stalowy pancerz o grubości 40 mm. Lepiej znany ukraiński dron – AQ-400 Scythe wydaje się zbudowany głównie z drewna. Jego podawany zasięg to 750 km, ma on zdolność przenoszenia 32-kilogramowej głowicy bojowej. Koszt jednostkowy tych dronów stanowi ułamek ceny irańskich dronów Shahed, dostarczanych Rosji po 375 000 dolarów za sztukę.

[6] Alfred Thayer Mahan – amerykański oficer marynarki wojennej uważany za jednego z najwybitniejszych teoretyków strategii morskiej, zwany Clausewitzem wojny morskiej. Teoria wojny morskiej (doktryna Mahana) zakłada, że potęga morska stanowi klucz do sukcesu państwa zarówno w sferze gospodarczej, jak i militarnej. Najlepszym sposobem ochrony nowoczesnej floty handlowej jest budowa równie nowoczesnej floty wojennej. Dopiero połączenie tych flot decyduje o potędze państwa. Kraje pozbawione silnych flot nie rozwijają się cywilizacyjnie i ekonomicznie, co prowadzi do ich upadku.

Nie zapominajmy, że w ramach działań podprogowych Rosja może zaatakować za pomocą dronów również obiekty IK należące do Polski. Skuteczność, niskie koszty produkcji i trudności z jednoznaczną identyfikacją sprawców w przypadku ich wykorzystania do ataku czynią je idealną bronią nie tylko dla terrorystów, lecz także dla podmiotów państwowych prowadzących działania hybrydowe. W tym kontekście nasuwa mi się smutna refleksja dotycząca niedoceniania w Polsce znaczenia bezpieczeństwa morskiego. To nie tylko zaniedbywana i niedoinwestowana Marynarka Wojenna, lecz także zaprzepaszczenie rozwiązań w zakresie bezpieczeństwa, którymi kiedyś dysponowaliśmy. Niewiele osób wie, że w 2011 r. Akademia Marynarki Wojennej wraz z producentem łodzi Sportis zrealizowali projekt budowy bezzałogowej jednostki nawodnej o nazwie Edredon, przeznaczonej do wykorzystania w celach militarnych oraz do zabezpieczania morskiej IK przed atakami terrorystycznymi. Ten projekt był innowacją na skalę światową. Edredon był sterowany za pomocą fal radiowych, ale dziś można byłoby to bez problemu zmienić. Centrum Techniki Morskiej w Gdyni opracowało z kolei system Kryl. Reagował on na zagrożenia ze strony nurków, małych okrętów podwodnych oraz jednostek nawodnych. Niestety, prace badawczo-naukowe prowadzone w ramach obu tych projektów, wiążące się nie tylko z wysiłkiem naukowców, lecz także z dużymi nakładami finansowymi, nie zostały właściwie wykorzystane.

> **Może wprowadzane regulacje prawne przyniosą pozytywne zmiany w sektorze szeroko rozumianej ochrony. W Polsce doczekaliśmy się ustawy o ochronie ludności i obronie cywilnej, w toku nowelizacja ustawy o zarządzaniu kryzysowym. W tle mamy unijne dyrektywy: CER i NIS 2, rozporządzenie DORA[7]. Jak to się ma, Pana zdaniem, do ochrony morskiej i portowej infrastruktury krytycznej w naszym kraju?**

Ochrona od strony morza obiektów IK była podyktowana dotychczas głównie wymaganiami wynikającymi z międzynarodowego kodeksu

[7] CER – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych; NIS 2 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/255 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE; DORA – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego.

ISPS[8] oraz krajowymi przepisami będącymi odzwierciedleniem jego zapisów, tj. *Ustawą z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich*. Celem ISPS jest zwiększenie zabezpieczenia żeglugi i portów przed aktami przestępczości kryminalnej, piractwem i terroryzmem. Niestety, ten kodeks w niewielkim stopniu odpowiada na aktualne zagrożenia w domenie morskiej. Na przykład dzisiejsze środki bojowe wykorzystywane przez podmioty państwowe są znacznie bardziej zaawansowane i rozwinięte niż te, którymi dysponowali terroryści z Al-Kaidy czy ISIS. Kodeks ISPS nie nakładał na obiekt IK obowiązku ochrony od strony morza. W związku z tym na niektórych obiektach w Polsce nie było i nie ma takiej ochrony. Nie wspominając już o zabezpieczeniu podwodnym. Spełniano jedynie minimalne wymagania wynikające z ISPS i polskich przepisów prawnych. Co z tego, że na jednym z obiektów kończymy po wielu latach działania związane z uruchomieniem systemu identyfikacji zagrożeń w dolnej półsferze, skoro nawet jeśli odkryjemy pod wodą obecność płetwonurka dywersanta, to niewiele będziemy mogli z tą informacją zrobić. Pominę fakt, że prawdopodobieństwo przeprowadzenia ataku w ten sposób maleje w dobie możliwości wykorzystania platform autonomicznych. Po co wysyłać płetwonurków, którzy będą w stanie przenieść kilka kilogramów materiału wybuchowego w minach limpet, skoro prościej i skuteczniej skorzystać z drona z 400-kilogramową głowicą bojową, bo tyle mogły przenosić pierwsze ukraińskie drony Sea Baby. Dzisiaj, jak deklarują Ukraińcy, mogą one przenieść nawet do 1000 kg materiałów wybuchowych. Ostatnio wykorzystali oni, do kolejnej próby uszkodzenia mostu Krymskiego, drona UUV[9] Mariczka, który może przenieść ponad tonę ładunku wybuchowego. Inny ukraiński dron, TLK 150, przenoszący 150 kg ładunku wybuchowego, może być wodowany z jachtu czy motorówki, co umożliwia jego skryte wykorzystanie. Systemy detekcji podwodnej na naszych obiektach morskiej IK należało zatem mieć wiele lat temu i są podmioty, które o to zadbały. Myślenie, że wszystkie nasze obiekty morskiej IK są dziś w stanie sprostać wyzwaniom w sferze ochrony, oznacza brak świadomości. Przy obecnej taktyce użycia środków bojowych, nawet tych wykorzystywanych poniżej progu wojny, nie jesteśmy w stanie zabezpieczyć tych obiektów w stu procentach.

[8] International Ship and Port Facility Security Code (pol. Międzynarodowy Kodeks Ochrony Statku i Obiektu Portowego) powstał w 2002 r. w następstwie ataków terrorystycznych z 11 września 2001 r. Zaczął obowiązywać od 1 lipca 2004 r.

[9] UUV (ang. *unmanned underwater vehicle*) – bezzałogowy pojazd podwodny.

Budujmy jednak sensowne elementy ochrony warstwowej, które zmniejszą podatność na ataki, zamiast stosować półśrodki.

> **Trudno nie dostrzec analogii do trwających wiele lat działań związanych z zabezpieczeniem obiektów przed bezzałogowymi statkami powietrznymi.**

Przez długi czas myśleliśmy, że problem rozwiążą tabliczki z zakazami wchodzenia i lotów umieszczane przy takich obiektach. Niestety, nawet systemy przeciwdronowe do zakłócania częstotliwości pracy tych urządzeń mogą być nieskuteczne. Pokazują to doświadczenia w Ukrainie, gdzie drony atakują w roju, a częstotliwości pracy są zmieniane w czasie lotu albo dronami steruje się za pomocą kabli światłowodowych kupowanych za grosze na chińskich portalach aukcyjnych. Ta wojna daje nam najlepszą możliwość wglądu w taktykę rosyjskich działań. Do identyfikacji i prognozowania możliwości ataku z wykorzystaniem UAV niezbędne są wiedza i doświadczenie operatorów FPV. W ten sposób można myśleć o systemie doboru środków do ochrony warstwowej obiektów morskich.

Ochrona obszaru morskiego państwa przed zagrożeniami asymetrycznymi przez wiele lat była traktowana marginesowo. Zdarza się, że za bezpieczeństwo ważnych obiektów odpowiadają osoby bez odpowiedniej wiedzy i przygotowania. Wieloletnia polityka kadrowa promująca, także w sektorze bezpieczeństwa, ludzi z klucza partyjnego i mających koneksje, a już niekoniecznie wiedzę specjalistyczną, odcisnęła swoje piętno. Przerzucanie się zakresem odpowiedzialności, niedostatek profesjonalistów, brak znajomości aktualnej wywiadowczej analizy zagrożeń i niechęć do uczenia się oraz wyciągania wniosków prowadzą do tak nielogicznych działań, jak chociażby 200-metrowa strefa zakazu zbliżania się do jednego z naszych najważniejszych obiektów morskiej IK. Według mnie jest to jedynie próba przeniesienia popularnych rozwiązań ze wschodniej granicy kraju na grunt obiektu, który będzie atakowany w inny sposób niż przez wtargnięcie migrantów o nieuregulowanym statusie. Takie nieadekwatne do realnych zagrożeń działania dają jedynie złudne poczucie bezpieczeństwa.

Zdarzenia z ostatnich lat pokazały, jak mocno narażone na działania hybrydowe są instalacje morskie na Bałtyku i jak ważne jest wzmocnienie ich ochrony.

Od czasu rosyjskiej inwazji na Ukrainę na Morzu Bałtyckim dochodzi do wielu działań hybrydowych, o które oskarża się Federację Rosyjską. Uszkodzone zostały m.in. gazociągi Nord Stream, Nord Stream 2 i Balticconnector, a od października 2023 r. – co najmniej 11 kabli podmorskich. Naprawę Balticconnectora, uszkodzonego przez chiński statek MV Newnew Polar Bear, oszacowano na 35 mln euro, a kabla energetycznego EstLink2 – na ok. 60 mln euro. Inny chiński statek MV Yi Peng 3 uszkodził na Bałtyku kable optyczne C-Lion 1 i BCS East-West Interlink. Początkowo postrzegałem te zdarzenia jako wspólne działania Chin i Rosji, ale ze względu na możliwe tarcia między tymi krajami częściowo weryfikuję swój punkt widzenia. Twierdzenie przez rosyjską Federalną Służbę Bezpieczeństwa czy Służbę Wywiadu Zagranicznego, że postrzega chińskie Ministerstwo Bezpieczeństwa Państwowego jako wroga, i oskarżanie Chin o rekrutację rosyjskich naukowców, aby zdobywać informacje na temat rosyjskiej technologii wojskowej, badań arktycznych i technologii podwójnego zastosowania, nie wydają się dobrą płaszczyzną do współpracy wywiadowczej przy działaniach sabotażowych. Wzajemną nieufność potęguje też prowadzenie przez Chińczyków silnego wywiadu przeciwko Rosji. Jest bardzo prawdopodobne, że Chińczycy mają swój wkład w sabotaże IK na Bałtyku, tym bardziej że często stosują takie działania na Morzu Północnochińskim przeciwko Tajwanowi.

Warto dodać, że obecne działania Rosji w rejonie Bałtyku są kontynuacją wielu lat pracy rosyjskich służb wywiadowczych i powstałego w 1965 r. Głównego Zarządu Badań Głębinowych. GUGI to wyspecjalizowana służba, która nie jest częścią regularnej rosyjskiej marynarki wojennej, ale podlega bezpośrednio Ministerstwu Obrony jako organizacja wywiadowcza i zaangażowana w misje specjalne. Rosjanie od dawna mapowali morskie farmy wiatrowe, gazociągi, kable energetyczne i internetowe na wodach wokół Danii, Norwegii, Finlandii, Szwecji i Polski. Na podstawie źródeł otwartych zidentyfikowano 50 statków, które przez ostatnie 10 lat mogły prowadzić na Bałtyku i Morzu Północnym operacje wywiadowcze na rzecz Rosji. Państwo to od wielu lat uprawia agresywną politykę, do czego wykorzystuje działania hybrydowe, asymetryczne i dezinformację. Po fazie zbierania informacji przez statki badawcze

GUGI: Yantar i Admirał Władimirski oraz statki z floty cieni, które przez ostatnie lata zatrzymywały się nawet na kilkanaście dni niedaleko podmorskich kabli energetycznych i telekomunikacyjnych, weszliśmy w fazę testowania i nękania.

Jaki to ma związek z inwestycjami w regionie Morza Bałtyckiego planowanymi przez Polskę?

Rejon, w którym powstaną nasze morskie farmy wiatrowe, również mógł zostać rozpoznany przez Federację Rosyjską. Od września 2022 r. do kwietnia 2023 r. dwa statki MV WL Totma oraz MV WL Kirillov kotwiczyły na wodach polskiej WSE, tuż za pasem morza terytorialnego, w odległości 12,623 mil morskich od linii brzegowej na wysokości Dębek. Kotwiczyły na obszarze, który zamknięty w wielobok pokrywa powierzchnię 24 364 km^2. Jeśli skanowały dno, to taki obszar mogły zeskanować w rejonie, gdzie powstaną nasze morskie farmy wiatrowe i planuje się położenie kabla podwodnego. Oba statki pływające pod banderą Panamy należą do cypryjskiego armatora White Lake Shipping. W zarządzie tej firmy są Rosjanie, stanowią oni także większość kadry kierowniczej. W sierpniu 2022 r. White Lake Shipping, przez swoją firmę zależną Gravelor Shipping Line, zakupiło kilka statków, m.in. dwa wymienione, od rosyjskich państwowych firm leasingowych GTLK Asia M5 Limited i GTLK Asia M6 Limited, które są objęte unijnymi i amerykańskimi sankcjami. W czasie kotwiczenia w rejonie planowanej lokalizacji polskich morskich farm wiatrowych oba statki wyłączały – niezgodnie z prawem i konwencją SOLAS[10] – nadajniki AIS. Na tych nadajnikach miały zadeklarowany status „w oczekiwaniu na zlecenie". Co jakiś czas jednostki te płynęły do portu w Bałtijsku i wracały do polskiej WSE, aby rzucić kotwice w miejscu, gdzie nie ma żadnego kotwicowiska, i czekać ok. 13 mil morskich od brzegu na kolejne zlecenie. W ciągu siedmiu miesięcy powtórzyły te operacje kilka razy. Według mnie najbardziej logicznym wytłumaczeniem ich obecności jest mapowanie dna. Gdyby prowadziły obserwację, to postój w niewielkiej odległości od siebie byłby bez sensu. Jeśli ze względów politycznych Polska nie chciała skorzystać z prawa do wizyty na tych statkach, to na czas ich pobytu w naszej

[10] International Convention for the Safety of Life at Sea (pol. Międzynarodowa konwencja o bezpieczeństwie życia na morzu) z 1974 r.

WSE należało postawić przy nich jednostkę, jeśli nie Straży Granicznej czy Marynarki Wojennej, to chociaż Urzędu Morskiego, i monitorować je, zwłaszcza że były to statki państwa wrogo nastawionego do Polski. Nieskuteczne działania ze strony służb państwa, ograniczające się do lotów rozpoznawczych samolotem Bryza czy okazjonalnego patrolowania przez jednostkę Straży Granicznej rejonu kotwiczenia statków, to w mojej ocenie poważny błąd, który umożliwił Rosjanom zdobycie istotnych informacji wywiadowczych.

Czy jako były płetwonurek bojowy przygotowywany do działań dywersyjnych na morzu uważa Pan, że na Bałtyku istnieje zagrożenie również z ich strony?

Chociaż dziś znaczenie płetwonurków dywersantów może wydawać się mniejsze w kontekście wykorzystania platform bezzałogowych, to nadal mogą oni stanowić poważne zagrożenie. Wystarczy przypomnieć ataki na Nord Stream 1 i Nord Stream 2. Jedna z trzech hipotez mówi, że nitki rurociągów zostały zniszczone przez ukraińskich płetwonurków, którymi dowodził pułkownik Służby Bezpieczeństwa Ukrainy. Od lutego 2025 r. na Morzu Śródziemnym doszło do uszkodzeń czterech statków rosyjskiej floty cieni: MV Grace Ferrum, MV Seacharm, MV Seajewel oraz MV Vilamoura. Z charakteru uszkodzeń wynika, że zostały zaatakowane za pomocą min limpet. Wszystko wskazuje na to, że były to działania ukraińskich płetwonurków bojowych.

Dziś o siłach specjalnych Federacji Rosyjskiej nieco zapomnieliśmy. Na Bałtyku rolę pierwszoplanową powierzyła ona statkom handlowym i jednostkom badawczym GUGI. Obawiam się, że to celowe działanie psychologiczne ze strony Rosjan. Chodzi im o to, aby skupić uwagę państw NATO na działaniach hybrydowych i skłonić je do zaangażowania sił wojskowych w ochronę, czyli sił, które mogłyby stawić czoła ewentualnym regularnym działaniom bojowym przeciwnika. To kolejne z potencjalnych zagrożeń asymetrycznych. Płetwonurkowie rosyjskiego Specnazu są rozmieszczeni w Obwodzie Królewieckim w strukturach 390 Punktu Rozpoznawczego Specjalnego Przeznaczenia Floty Bałtyckiej (JW nr 43104) w mieście Parusnoje. Dysponują m.in. nowoczesnymi skuterami podwodnymi Black Shadow, zakupionymi od niemieckiej firmy Rotinor. Te praktycznie niewykrywalne skutery umożliwiają poruszanie się z prędkością ok. 7 węzłów na głębokości do 60 m

i pokonywanie dystansu do 50 km. Pozwala to wejść do rejonu działania spoza morza terytorialnego wynoszącego 12 mil morskich. Siły Specnazu, jak większość pododdziałów specjalnych, są wręcz stworzone do działań hybrydowych i mogą je realizować na Morzu Bałtyckim i w państwach regionu.

Jakie działania ma Pan na myśli?

Rozpoznanie obiektów morskiej IK i prowadzenie wobec nich działań dywersyjnych, w tym pod fałszywą flagą, podsłuch, niszczenie podwodnych kabli komunikacyjnych i sieci energetycznych, porywanie wartościowych celów i osób w rejonie wybrzeża. To wszystko się wpisuje w działania zgodne z doktryną Gierasimowa i jest elementem wojny podprogowej, która na każdym etapie może się przerodzić w otwarty konflikt.

Porozmawiajmy o rosyjskich działaniach wywiadowczych w Polsce wymierzonych w sektor morski. Pominę analizę i ocenę podatności z obszaru bezpieczeństwa osobowego, bo to temat na osobny wywiad.

Rosjanie zdobywają informacje na temat każdego interesującego ich obiektu jeszcze przed rozpoczęciem inwestycji. Warto wspomnieć, że w 2014 r. skazano obywatela RP, który od 2012 r. wykonywał zadania wywiadowcze – pozyskiwał informacje o Gazoporcie w Świnoujściu i osobach w nim zatrudnionych, brał udział w posiedzeniach sejmowej komisji ds. energetyki. Aby zobrazować skuteczność i rozmach działania rosyjskiego wywiadu w zdobywaniu informacji o polskich obiektach strategicznych, należy przypomnieć, że Gazoport w Świnoujściu został otwarty w 2015 r., a pierwszy gazowiec wpłynął do niego 11 grudnia 2015 r. Agent został więc aresztowany na długo przed otwarciem portu. W przypadku naszej nowej strategicznej inwestycji związanej z morskimi farmami wiatrowymi na Bałtyku Rosjanie pokazali, jak skutecznie pracują wywiadowczo. Zmapowali dno morskie, na którym zostaną one usadowione, i to jeszcze przed ostatecznym przydzieleniem działek inwestorom, co nastąpiło decyzją ministra infrastruktury w maju 2023 r. Jestem pewien, że rosyjski wywiad prowadzi również silne działania

operacyjne, aby pozyskać osobowe źródła agenturalne mające zarówno możliwości wywiadowcze, jak i wiedzę o powstającej inwestycji.

Rozwińmy wątek działań szpiegowskich Rosji.

Dotychczas rosyjski wywiad poszukiwał na terenie Polski przede wszystkim osób, które mają możliwości wywiadowcze, tj. mogą dostarczać cennych informacji, są zatrudnione w instytucjach lub obiektach interesujących dla wywiadu, są w partiach politycznych, w rządzie, mogą być wykorzystane w operacjach wpływu, mogą wspierać i zabezpieczać działalność wywiadowczą oraz pracę innych agentów czy też typować kandydatów na potencjalnych agentów. Obecnie do wykonywania prostych zadań, chociażby takich jak podkładanie ładunków zapalających, są poszukiwani także „agenci jednorazowi", czyli dywersanci bez specjalnej wiedzy i przeszkolenia. Kandydatem na takiego agenta może być każdy, kto posiada telefon komórkowy do robienia zdjęć obiektów, ma możliwość oznaczenia umownym znakiem obiektu do zniszczenia, potrafi umocować kamerę IP na drzewie, zostawić paczkę we wskazanym miejscu czy wzniecić ogień. Jedynym warunkiem wydaje się pobyt na terenie Polski. Należy zauważyć, że do 26 lutego 2023 r. na teren naszego kraju wjechało 9,797 mln osób narodowości ukraińskiej. W ubiegłym roku Agencja Bezpieczeństwa Wewnętrznego zatrzymała 16 członków siatki szpiegowskiej, w tym 12 Ukraińców, 3 Białorusinów i Rosjanina. Mieli oni prowadzić obserwację portów w Gdyni i Gdańsku, dworców kolejowych, np. w Rzeszowie, wojskowego lotniska w Jasionce używanego przez Stany Zjednoczone, a także zakładać kamery IP w pobliżu linii kolejowych, którymi transportowano sprzęt do Ukrainy. W przyszłości mieli zająć się też dywersją. Oczywiście do takiej działalności Rosjanie werbują również Polaków. Najbardziej znany przykład to sprawa Pawła K., który na lotnisku w Rzeszowie przygotowywał zamach na prezydenta Wołodymyra Zełenskiego.

Przykładów takich działań jest więcej. Do współpracy i zdobywania informacji wywiadowczych rosyjski wywiad agenturalny od wielu lat pozyskuje również marynarzy.

Agentów wśród marynarzy i osób mających możliwości wywiadowcze w sektorze morskim werbowały dwa ośrodki wywiadowcze GRU, czyli 1194 Centrum Wywiadowcze w Murmańsku i 264 Centrum Wywiadowcze w Kaliningradzie. Nie można wykluczyć, że ze względu na położenie i port morski praca typowniczo-werbunkowa mająca na celu pozyskiwanie źródeł osobowych i agentów mogła być prowadzona również siłami 73 Centrum Wywiadowczego w Sankt Petersburgu. Te komórki GRU miały niejako przypisane werbowanie zagranicznych marynarzy. Według raportu Baltic and International Maritime Council oraz International Chamber of Shipping z 2021 r.[11] rosyjscy marynarze stanowią 10,5% pracowników w żegludze międzynarodowej. Szacuje się, że jest ich obecnie 198 000. Dla rosyjskiego wywiadu to ogromna i cenna baza. Każdy marynarz musi mieć kontakt ze służbami specjalnymi przed rozpoczęciem pracy, przed otrzymaniem paszportu i książeczki żeglarskiej Seamans Book. W związku z wymogami konwencji STCW[12] co pięć lat muszą oni odnawiać większość szkoleń. Mają więc częsty kontakt z organami państwowymi, dzięki czemu służby wywiadowcze są w stanie ich kontrolować i wyznaczać im zadania do wykonania. Nie wyobrażam sobie, żeby marynarze ich nie realizowali. W najlepszym przypadku zostaliby pozbawieni możliwości wykonywania dobrze płatnego zawodu. Wykorzystanie rosyjskich marynarzy przez wywiad może być szerokie, m.in. polegać na zdobywaniu przez nich informacji o miejscach i obiektach morskich, do których przypływają ich statki, na typowaniu i wskazywaniu osób interesujących dla rosyjskiego wywiadu, a także przekazywaniu czy odbieraniu materiałów wywiadowczych. Załogi statków mogą poruszać się po strzeżonych obiektach portowych. Rosyjscy marynarze zawijają do nich statkami zarejestrowanymi pod banderami innymi niż rosyjska, dzięki czemu nie wzbudzają zbytnich podejrzeń i można im zlecać również działania sabotażowe na terenie obiektów portowych Europy Zachodniej.

[11] *Seafarer Workforce Report: The Global Supply and Demand for Seafarers in 2021*, https://www.bimco.org/products/publications/titles/seafarer-workforce-report/.

[12] International Convention on Standards of Training, Certification and Watchkeeping (pol. Międzynarodowa konwencja o wymaganiach w zakresie wyszkolenia marynarzy, wydawania świadectw oraz pełnienia wacht).

Rysunek 1. Obecne działania asymetryczne Federacji Rosyjskiej na Bałtyku.
Źródło: materiały własne S. Kalitowskiego.

Czego w związku z tym możemy się spodziewać w najbliższej przyszłości?

Łatwość werbowania agentów, którzy nie muszą mieć specjalnych umiejętności wywiadowczych, oraz brak konieczności długotrwałego procesu rozpracowania i osobistego kontaktu oficera wywiadu będą sprzyjać werbowaniu źródeł osobowych i sprawców aktów sabotażu w obiektach morskiej IK. W najbliższym czasie możemy się spodziewać działań sabotażowych w obiektach morskich, np. takich, do których doszło ostatnio w Hamburgu. Nieznani sprawcy uszkodzili silniki we fregacie FGS EMDEN (F266) przez wrzucenie kilku kilogramów stalowych wiórów. Z kolei na niemieckim okręcie FGS Homburg (M1068) poprzecinano w stoczni wiązki kabli, a na FGS Hessen (F221) „omyłkowo" nalano ropy do zbiornika wody pitnej. Sabotaż jest genialną bronią! Chociaż nie wygrywa się nim wojny, to niewielkim kosztem można sparaliżować funkcjonowanie, wzbudzić strach i niepokój, narazić zaatakowanego na ogromne straty i wydatki. Większość scenariuszy takich działań mieści się w sferze błędu ludzkiego czy braku profesjonalizmu. W ten sposób mogą być sabotowane nasze stocznie, porty, a także porty serwisowe i elementy łańcucha dostaw dla morskich farm wiatrowych. Dziwi mnie, że jeszcze nie było informacji o podejrzanych dronach latających nad

naszymi obiektami morskiej IK. Już kilka razy takie akcje miały miejsce w Niemczech czy Danii, gdzie roje dronów obserwacyjnych wystartowały ze statków na morzu. Skontrolowano podejrzane jednostki, ale nie znaleziono dowodów.

> **Panie Komandorze, dziękuję za trafne, czasem gorzkie, ale prawdziwe spostrzeżenia. Wierzę, że skłonią one do refleksji.**

Jestem zwolennikiem mówienia wprost i uświadamiania, gdzie mamy miękkie podbrzusze. Dotyczy to zwłaszcza sfer, w których w grę wchodzi szeroko pojmowane bezpieczeństwo. Nie łudźmy się, że Rosjanie o naszych słabościach dowiedzą się z tego wywiadu. Oni mają je bardzo dobrze rozpoznane! Poszukiwanie słabych miejsc i ich wzmacnianie to element budowania świadomości zagrożeń i motywacji do zwiększania bezpieczeństwa. Uczmy się na przykładzie Ukraińców, którzy wielokrotnie przyznali, że bagatelizowali zagrożenie. Nie wierzyli, że Rosjanie mogą zaatakować.

Chciałbym, aby ta rozmowa przyczyniła się do zwiększenia świadomości naszych polityków, decydentów oraz szefów służb na temat tego, jak ważny jest wywiad morski oraz właściwe rozpoznanie zagrożeń hybrydowych na Bałtyku. Trzeba nad tym zacząć pracować szybko i intensywnie, bo to zadanie na wczoraj. Nie możemy się oglądać na NATO, Stany Zjednoczone i inne kraje. Sami musimy zadbać o pozyskanie informacji wywiadowczych. Moim zdaniem to także ostatni dzwonek na rozwijanie szerokiej i silnej współpracy prywatno-państwowej w sektorze bezpieczeństwa morskiego.

Rozmawiała: Daria Olender

Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 251–258

https://doi.org/10.4467/20801335PBW.25.012.22178

VARIA

Bądź przyzwoity i konsekwentny! To pomaga w budowaniu bezpieczeństwa

Inspektor **dr Robert Żółkiewski** jest jednym z najbardziej doświadczonych funkcjonariuszy Policji. Uczestniczył w misjach zagranicznych – w Bośni i Hercegowinie, Kosowie, Iraku oraz Ukrainie. Pracował również w Kwaterze Głównej ONZ w Nowym Jorku i ukończył trzymiesięczne szkolenie w prestiżowej Akademii FBI w Quantico. Swoimi kompetencjami, m.in. w zakresie współpracy międzynarodowej, wspiera formację jako dyrektor Gabinetu Komendanta Głównego Policji[1]. O tym, z jakimi wyzwaniami wiąże się praca w regionach, w których toczą się konflikty, o służbie w Policji i roli współpracy oraz potrzebie zachowania równowagi między aktywnością zawodową i życiem osobistym rozmawia z Darią Olender.

[1] Wywiad został przeprowadzony 6 maja 2025 r. Od 20 maja 2025 r. Robert Żółkiewski pełni funkcję pełnomocnika Komendanta Głównego Policji ds. przygotowania rozwiązań organizacyjnych i prawnych związanych z planowaną reorganizacją Centrum Szkolenia Policji w Legionowie. Wszystkie przypisy w tekście pochodzą od redakcji.

Daria Olender: Jest Pan jednym z pierwszych funkcjonariuszy polskiej Policji, który ukończył prestiżową Akademię Federalnego Biura Śledczego w Quantico. Jak Pan wspomina to doświadczenie?

Insp. dr Robert Żółkiewski: Do FBI Academy dostałem się w 2009 r. Starałem się o to znacznie wcześniej, ale wtedy wysyłano tam policjantów z Centralnego Biura Śledczego[2], którzy walczyli z przestępczością zorganizowaną. To było najlepsze szkolenie w mojej ponadtrzydziestoletniej karierze.

Co Panu dał udział w FBI Academy?

Szkolenie to bardzo różni się od standardowych. Jest profilowane, gdyż uczestnik ma prawo wyboru większości przedmiotów. Obowiązkowych jest tylko kilka. Podczas mojej edycji policjanci z zagranicy musieli wziąć udział w zajęciach z zarządzania kryzysowego, prawa karnego i międzynarodowego oraz współpracy ze społeczeństwem i mediami. Razem ze mną szkoliło się 24 policjantów z całego świata oraz ok. 200 funkcjonariuszy z USA. W tak różnorodnej grupie stawiano na integrację oraz wymianę doświadczeń i dobrych praktyk. Uczyliśmy się pracy w zespole i budowania wspierających relacji międzyludzkich, czyli kompetencji miękkich. Nie zabrakło też zajęć praktycznych i aktywności fizycznej. Na sport był przeznaczony jeden dzień w tygodniu. Po trzech miesiącach, bo tyle trwało szkolenie, musieliśmy zaliczyć bieg na 10 km na torze przeszkód US Marines, czyli wspiąć się po linie, przebrnąć przez błoto do kolan itp. Nie było łatwo.

Czy coś szczególnie zapadło Panu w pamięć z tego szkolenia?

Bardzo inspirujące były spotkania z ciekawymi ludźmi, m.in. z szefem Centralnej Agencji Wywiadowczej, byłym szefem Federalnego Biura Śledczego czy z pilotem[3] Blackhawka, zestrzelonym w Mogadiszu, w Somalii. W pamięci utkwił mi policjant, który stracił wzrok na służbie.

[2] Obecnie: Centralne Biuro Śledcze Policji (CBŚP).

[3] Chodzi o amerykańskiego pilota Michaela Duranta, autora powieści *In the Company of Heroes* (New York 2004). Jego historię przedstawia film *Helikopter w ogniu* w reżyserii Ridleya Scotta.

To dramatyczne doświadczenie paradoksalnie otworzyło mu oczy na świat, na bliskich, na aktywność pozazawodową. Przez kolejne lata uczył innych funkcjonariuszy, że istotne są nie tylko praca, lecz także rodzina, nauka, hobby, że trzeba znaleźć czas na życie osobiste, zadbać o zdrowie psychiczne. Było to bardzo potrzebne, gdyż wówczas w Stanach Zjednoczonych podczas realizacji zadań służbowych ginęło ok. 400 policjantów rocznie, a drugie tyle śmiercią samobójczą z powodu stresu. Dziś więcej się mówi o tym problemie, uczy się funkcjonariuszy, jak sobie z nim radzić, ale wtedy to było dla mnie coś nowego.

Absolwenci Akademii FBI są zapraszani na cykliczne seminaria. Jaki jest cel tych spotkań?

Po ukończeniu trzymiesięcznego szkolenia stajemy się członkami Stowarzyszenia Absolwentów Akademii FBI. Jest to największa sieć *law enforcement* na świecie. O ile mnie pamięć nie myli, w 1965 r. ówczesny prezydent Stanów Zjednoczonych podjął decyzję, że w Akademii FBI będą się szkolić funkcjonariusze również z innych państw i od tego momentu ta sieć sukcesywnie się rozrasta. Absolwenci Akademii FBI corocznie spotykają się na tzw. *retraining sessions*, organizowanych w kilku regionach świata. W Europie sesje szkoleniowe odbywają się od ponad 30 lat, pierwsza była w Rumunii. Potem m.in. w Gruzji, na Cyprze, w Wielkiej Brytanii, Belgii, a ostatnio w Norwegii. W tym roku będziemy gościć w Macedonii. To okazja do odświeżenia i poszerzenia wiedzy, zapoznania się z rozwiązaniami wdrożonymi w innych państwach, podtrzymania kontaktów, ale także do promowania własnego kraju.

Z Pana inicjatywy takie spotkanie szkoleniowe odbyło się w Polsce.

Zaproponowałem to wspólnie z kolegami, którzy ukończyli Akademię. W 2014 r. do Warszawy przyjechało prawie 300 osób z ponad 30 państw, w tym John Boles – zastępca szefa FBI. Zgodnie z mottem tego wydarzenia *Bridging East and West* (pomost między Wschodem i Zachodem – dop. red.) rozmawialiśmy o tym, jak Polska odnajduje się w ówczesnej sytuacji geopolitycznej, jaką rolę może odegrać ze względu na swoje położenie geograficzne. Mamy bardzo dobrą współpracę z FBI, ale też z innymi służbami, przede wszystkim europejskimi. Wypracowane kontakty

pozwalają na szybszą reakcję na przestępstwa czy zagrożenia. Wykorzystujemy oczywiście głównie oficjalne kanały, ale czasami, gdy sytuacja tego wymaga, uruchamiamy także te nieoficjalne. Na marginesie dodam, że szkolenie ze współpracy międzynarodowej jest bardzo interesujące.

Udział w szkoleniach Akademii FBI to nie pierwsze Pana doświadczenie we współpracy międzynarodowej. Zaczynał Pan od misji zagranicznych.

Przygodę z misjami, wtedy zwanymi pokojowymi, rozpocząłem w 1998 r. Zakwalifikowałem się na misję ONZ do Bośni i Hercegowiny. Pracowałem po serbskiej stronie, w miejscowości Pale, gdzie znajdowała się m.in. rezydencja ówczesnego prezydenta. Pomagaliśmy społeczności lokalnej i pilnowaliśmy tzw. *zones of separation*. Były to strefy, które pełniły funkcję wewnętrznych granic. W ramach międzynarodowego nadzoru prowadziliśmy punkty kontrolne, tzw. *check points*, i monitorowaliśmy przepływ ludności. Dbaliśmy o to, aby Bośniacy i Serbowie nie kontaktowali się ze sobą, i przeciwdziałaliśmy zachowaniom mogącym podsycać konflikt. Byłem wtedy oficerem ds. przestrzegania praw człowieka i nad tymi tematami pracowałem z lokalną policją. To była bardzo ciekawa i potrzebna misja. Czas pokazał, że udało się zaprowadzić pokój w tym regionie.

Dokąd pojechał Pan w ramach kolejnej misji?

Do Kosowa. To była misja organizowana również pod egidą ONZ. Zostałem szefem stacji. Nadzorowałem ponad 100 osób z 30 krajów oraz 20 lokalnych pracowników, tłumaczy i kierowców. Zastępowaliśmy też lokalną policję, gdyż na początku 1999 r. tej formacji jeszcze tam nie było. Z czasem zaczęły powstawać szkoły policyjne. Naszym zadaniem było m.in. wyszkolenie funkcjonariuszy. Warto dodać, że nasi eksperci z Policji szkolą tam do dziś, przy czym obecnie jest to misja pod auspicjami Unii Europejskiej. W 2004 r., gdy służyłem już w Komendzie Głównej Policji, dostałem propozycję objęcia dowództwa Jednostki Specjalnej Polskiej Policji, która w Kosowie przebywała od 2000 r. lub 2001 r. Zostałem dowódcą VII zmiany tej jednostki, a po kilku latach – XII zmiany. Ogólnie na Bałkanach spędziłem ponad cztery lata i zostawiłem tam część życia i serca.

Zdjęcie 1. Podczas realizacji zadań na misji w Kosowie.
Źródło: materiały własne R. Żółkiewskiego.

Udział w misjach zagranicznych, zwłaszcza tych prowadzonych w rejonach konfliktów zbrojnych, wiąże się z wieloma wyzwaniami. Jakie kompetencje i cechy charakteru są Pana zdaniem potrzebne, aby sprostać pracy w tak trudnych warunkach?

Przypomina mi się szkolenie w Quantico. Przede wszystkim potrzebny jest profesjonalizm wyrażający się umiejętnością pracy w grupie, pod presją czasu, w stresie i stałym zagrożeniu. Trzeba mieć szacunek dla innych, wrażliwość na krzywdę ludzką, chęć i umiejętność niesienia pomocy. Ważne są także umiejętności negocjacyjne, wytrwałość w dążeniu do celu, zdolność do odnalezienia się w odmiennej rzeczywistości, poszanowanie dla prawa i tradycji kraju, w którym się służy i pomaga. Trudno w kilku zdaniach ująć to wszystko, a jeszcze trudniej realizować w rzeczywistości.

Jak przebiegała Pana służba po powrocie do kraju?

Z misji w Kosowie wróciłem w 2007 r. i otrzymałem propozycję pracy w Biurze Międzynarodowej Współpracy KGP. Potem objąłem stanowisko dyrektora Gabinetu Komendanta Głównego Policji. Myślę, że moimi atutami były doświadczenie, umiejętności językowe i kontakty

międzynarodowe, bardzo przydatne podczas realizacji zadań na poziomie kierownictwa Policji. Dużo się wtedy nauczyłem o zarządzaniu strategicznym i kryzysowym. Po różnych zawirowaniach i zmianach politycznych zostałem zwolniony z tego stanowiska, ale udało mi się kontynuować przygodę z misjami. Miałem okazję pracować w Kwaterze Głównej ONZ w Nowym Jorku, gdyż wygrałem konkurs na stanowisko Selection and Recruitment Officer. Moim zadaniem był nabór i dobór kadry policyjnej na misje ONZ. W Departamencie Policji ONZ pracowało ok. 80 funkcjonariuszy z całego świata, ja zajmowałem się m.in. misjami w Iraku, Liberii, Gwinei Bissau i Libii. Po ponaddwuletniej służbie w ONZ wróciłem do kraju i dostałem propozycję wyjazdu na misję doradczą w Ukrainie – The European Union Advisory Mission Ukraine. Zostałem szefem biura terenowego misji w Charkowie, przy terenach granicznych. To był gorący czas! Już wtedy widziałem, że konflikt między Rosją a Ukrainą wisi na włosku. Do kraju wróciłem ok. pół roku przed wybuchem wojny. Po kilku miesiącach dostałem propozycję wyjazdu na Misję Doradczą Unii Europejskiej w Iraku. Spędziłem półtora roku w Bagdadzie jako szef Wydziału Doradczego (*chief operations officer*). Zarządzałem zespołem 30 policjantów z całej Europy, którzy doradzali pracownikom Ministerstwa Spraw Wewnętrznych oraz Komendy Głównej Policji w Iraku. Prowadziliśmy też szkolenia, m.in. z zarządzania, planowania strategicznego i przestępczości zorganizowanej, terroryzmu, a także z prawa, gdyż wśród przedstawicieli irackich struktur administracyjnych zaległości w wiedzy prawnej sięgały lat 80.

Czego nauczyły Pana doświadczenia związane z pracą na misjach zagranicznych i w ONZ?

Przede wszystkim szacunku dla różnorodności. W Bośni i Kosowie służyli policjanci z ponad 50 krajów świata. Nie jest łatwo współpracować na co dzień z kimś, kto ma odmienne wyszkolenie, inne doświadczenia, spojrzenie na prawa i obowiązki, np. na użycie środków przymusu bezpośredniego. Nierzadko mierzyliśmy się z trudnymi sytuacjami, z których musieliśmy wybrnąć, aby uniknąć kłopotów, a nawet afer międzynarodowych. To była wymagająca praca. Ale było też dużo śmiechu, który najskuteczniej rozładowywał napięcia. Uświadomiłem sobie także, jak potrzebne jest istnienie ONZ. Brak takiej instytucji oznaczałby znacznie większą liczbę konfliktów zbrojnych na świecie.

Pana historia pokazuje, z jak ciekawymi wyzwaniami może się wiązać praca w Policji. Skądinąd wiadomo, że formacja mierzy się z problemem niedoborów kadrowych. W jaki sposób Komenda Główna Policji stara się zwiększyć zainteresowanie służbą?

W 2024 r. został skierowany do Sejmu projekt ustawy o zmianie niektórych ustaw w związku z tworzeniem oddziałów o profilu mundurowym oraz ułatwieniem powrotu do służby. Chodziło m.in. o zwiększenie z 3 do 5 lat możliwości powrotu do służby po przejściu na emeryturę bez konieczności zdawania testu wiedzy i przechodzenia badań psychologicznych. Chcieliśmy w ten sposób zachęcić doświadczonych policjantów do jak najszybszego powrotu. Z satysfakcją mogę stwierdzić, że te przepisy zaczęły obowiązywać[4]. Usprawniliśmy też procedury przyjęcia do służby kontrterrorystycznej, w Centralnym Biurze Zwalczania Cyberprzestępstw, a także w naszych uczelniach, szkołach policyjnych, w tym w Akademii Policji w Szczytnie. Dążymy do pozyskania osób, które mają wiedzę specjalistyczną, kwalifikacje czy wykształcenie przydatne dla danych komórek Policji. Pracowaliśmy także nad rozporządzeniem dotyczącym służby kontraktowej, aby policjanci, którzy odeszli na emeryturę, mogli wrócić na zasadzie kontraktu. W tle jest misja dla nich – sprawowanie opieki nad młodszymi kolegami i szkolenie ich. Kolejny pomysł dotyczył klas o profilu mundurowym w szkołach średnich. Obecnie mamy ponad 200 tego typu ośrodków. Chodziło o skrócenie uczniom tych klas postępowania kwalifikacyjnego do służby w Policji. Jest to jedna z istotnych zmian. Staramy się także promować na targach uczelni i targach pracy. Spotykamy się z uczniami i studentami. Mamy też ogłoszenia, które w formie krótkich filmów są publikowane m.in. w środkach komunikacji miejskiej.

Skupmy się na młodych ludziach. Kogo poszukujecie i co możecie zaoferować osobom, które rozważają wstąpienie do Policji?

Poszukujemy ludzi, którzy pragną pomagać innym, mają chęć nieść pomoc słabszym i potrzebującym, nawet z narażeniem życia, a jednocześnie są zdeterminowani do walki z przestępczością i chcą dbać

[4] *Ustawa z dnia 1 października 2024 r. o zmianie niektórych ustaw w związku z utworzeniem oddziałów o profilu mundurowym oraz ułatwieniem powrotu do służby w Policji i Straży Granicznej* (DzU z 2024 r. poz. 1562).

o porządek i bezpieczeństwo publiczne. Praca w Policji może być naprawdę ciekawa. To nieprzewidywalna przygoda oraz duże możliwości rozwoju, również w instytucjach międzynarodowych i na misjach zagranicznych. Mamy współpracę z Interpolem i Europolem, można zostać oficerem łącznikowym Policji na terenie innego państwa. W kraju także jest dużo możliwości rozwoju, czy to w pionach – śledczym, prewencji, cyberprzestępczości czy w laboratorium kryminalistycznym. Nie bez znaczenia pozostają prawa emerytalne, które się nabywa po 25 latach służby.

> **Mam nadzieję, że ta rozmowa skłoni wiele osób do wybrania tej drogi zawodowej, a funkcjonariuszy zainspiruje do poszerzania swoich kompetencji i inicjowania działań na rzecz szeroko pojmowanego bezpieczeństwa. Co by Pan powiedział, aby ich zachęcić do takiej aktywności?**

W kształtowaniu siebie i swojej kariery zawodowej warto być przyzwoitym, cierpliwym i konsekwentnym. To z kolei pomaga w budowaniu bezpieczeństwa!

Ladies and Gentlemen!

Internal security is a broad concept encompassing many aspects of the functioning of the state and lives of its citizens. It includes, among other things, public, constitutional, social, cultural, informational, economic, environmental and cyber security. Ensuring internal security is one of the most important tasks and serves as the foundation for the stability of the Republic of Poland, enabling uninterrupted socio-economic development and strengthening the country's position on the international stage.

As an editor-in-chief of the 'Internal Security Review', my intention is to ensure that the content presented covers the broadest possible range of issues related to the area of security, that it remains diverse and that the topics addressed are relevant and up to date. Together with the authors, under the watchful eyes of the reviewers and members of the Academic Editorial Board, we will conduct analyses and assessments, and based on these, put forward recommendations. We know, how crucial an informed and educated society is in ensuring security and preventing threats, which is why we want to share knowledge as broadly as possible. In addition to scientific articles, 'Internal Security Review' will publish interviews with experts as well as reports from workshops and scientific conferences on topics we find relevant. We also plan to continue publishing reviews of books related to security.

In this issue, Associate Professor Ilona Urych discusses the role of education from a systemic perspective. Her article is a critical reflection on educational programmes related to security at different levels of school education and in universities.

We are at a crucial point in terms of enhancing the resilience of the state and society. At the beginning of January 2025, a long-awaited Act on civil protection and civil defence came into force

in Poland. A book titled *Mechanisms of Civil Protection in Disaster Risk Reduction. Selected Issues*, edited by Fire Service officers: Paweł Gromek, Mariusz Feltynowski and Monika Wojakowska, is dedicated to the issues of civil security. Being familiar with this publication can help readers grasp the essence of civil protection in Poland, as Julia W. Tocicka, PhD, points out in her review. I encourage you to read it.

We are also expecting an amendment to the Act on crisis management that will include not only provisions of previously mentioned act, but will also introduce regulations concerning the EU civil protection mechanism and implement the Directive of the European Parliament and of the Council on the resilience of critical entities – specifically, the CER Directive – into the Polish legal system. Consequently, the 'Internal Security Review' could not omit issues related to the Polish critical infrastructure. Its protection has been the subject of many debates in the country. In January this year, I participated in a conference *The Evolution of Law in Crisis Management and Critical Infrastructure Protection*. In an interview for the 'Internal Security Review', Ireneusz Jabłoński and Piotr Grzybowski from the Polish Institute of Internal Control, which organised the event, talk about good practices and challenges in this field. In turn, David Cybulski discussed cybersecurity challenges in the offshore and coastal energy sector, particularly in relation to Poland's upcoming strategic energy projects in the Baltic Sea.

In this issue, we also dedicate considerable space to modern technologies. In the 'Competition entries' section, we present the article by Marta Grzywacz on the energy transition related to the shift to clean energy and the role of the hydrogen sector in maintaining the country's economic security. Jarosław Przyjemczak, PhD, and Małgorzata Wolbach wrote about the possibilities of using modern technologies and tools to support the process of threat monitoring. This issue also came up in an interview with Cmdr. Sebastian Kalitowski, during which we talked about safeguarding Polish maritime zones, among other things, from hybrid threats posed by the Russian Federation. The theme of espionage and other foreign influences is also present in the article by Marek Klasa, PhD, and Michał Klasa, who describe the Russian 'special military operation' as a failed *coup de main*, and – in a historical context – in Szymon Główka's contest paper analysing the intelligence and counterintelligence system in the Napoleonic France.

In recent years, much attention has been paid to the security of our borders. Łukasz Foryś, PhD, and Kornelia Stępień, PhD, analysed the impact of traffic control on combating cross-border crime. Security also involves countering extremist threats. Patryk Król described new anti-state movements in Poland, inspired by the US sovereign citizen movement, and presented proposals for preventive measures that could reduce the impact of these phenomena on Polish society.

I also encourage you to read the interview with Inspector Robert Żółkiewski, PhD, who spoke about the opportunities and possibilities offered by service in the uniformed forces. His interesting professional experiences may serve as encouragement for young people who wish to dedicate themselves to strengthening internal security of Poland.

I would like to thank the authors for presenting the results of their research efforts in the pages of the 'Internal Security Review', and the reviewers for their support in the substantive evaluation of the submitted content. I also extend may gratitude to the members of the newly established Academic Editorial Board and the editorial team.

Editor-in-Chief
Daria Olender, PhD

ARTICLES

Internal Security Review
2025, no. 32, pp. 265–283

https://doi.org/10.4467/20801335PBW.25.013.22179

ARTICLE

Security as an educational category. Contemporary trends

ILONA URYCH

War Studies University

https://orcid.org/0000-0003-4868-9460

Abstract

The aim of the article is to discuss contemporary trends in the approach to security as an educational category. The article characterises what security science entails within the framework of the school subject 'education for security' and in the education programmes of military classes. The educational offer of higher education institutions addressing security-related topics was also presented. Moreover, the study discussed the attitudes of teachers involved in education in the field of security in the face of the challenges of modern education. Changes in the security environment generate the need to conduct scientific research on education on security, including exploratory and utilitarian studies. The acquired knowledge should constitute a trigger for evaluation of the content of security-related education and serve to develop new procedures for state security.

Keywords

education, security, education for security, military classes, teacher, security sciences

Introduction

Since the beginning of Russia's invasion of Ukraine, scholarly works and expert opinions have been written on the defence capabilities of both countries, the European Union, and the multidimensional aspects of the war[1]. It is worth noting that this research issue not only prompts reflection on international, national or personal security, but also on educational needs in this area.

The word 'security' – originates from the Latin word *securites*, which is a derivative of the expression *sine cura*, or 'without care'. This points to the primordiality of the sense of threat in relation to the sense of security[2]. This means, as Wojciech Multan argues, that as long as we are not threatened by the loss of security, we do not realise what it is[3]. Ryszard Zięba, on the other hand, stresses that when exploring the essence of security, it is worth bearing in mind its relationship to the phenomenon of threat[4]. According to the researcher it is (…) *the certainty of existence and survival, the state of possession and the functioning and development of the entity*[5]. At the same time, he emphasises that this certainty is the result not only of the absence of threats, but also of the activity of the entity in question. It seems, therefore, that this is variable over time and therefore has the character of a social process[6].

Security as a social construct is distinguished especially within the constructivist approach, characteristic of the so-called Copenhagen School and scholars

---

1 See e.g.: A. Pacholczak, *Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, pp. 97–129. https://doi.org/10.4467/20801335PBW.24.015.19617; M. Zadorożna, M. Butuc, *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "Security and Defence Quarterly" 2024, no. 46(2), pp. 47–65. https://doi.org/10.35467/sdq/189686; Z. Wiktor, *Wojna w Ukrainie – przyczyny i skutki po ponad roku trwania* (Eng. War in Ukraine – causes and consequences after more than a year), "Studia Orientalne" 2023, vol. 12, no. 3(27), pp. 30–59. https://doi.org/10.15804/so2023302; K. Maciejewska-Mieszkowska, *Eskalacja wojny w Ukrainie jako czynnik determinujący poczucie zagrożenia bezpieczeństwa Polski w ocenie społecznej* (Eng. Escalation of the war in Ukraine as a determinant of the feeling of threat to Poland's security in the public assessment), "Środkowo-europejskie Studia Polityczne" 2023, no. 2, pp. 217–236. https://doi.org/10.14746/ssp.2023.2.12.

2 J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa* (Eng. Contemporary understanding of security), Warszawa 1996, p. 15.

3 W. Multan, *Bezpieczeństwo międzynarodowe ery nuklearnej* (Eng. International security of the nuclear age), Warszawa 1991, p. 22.

4 R. Zięba, *Teoria bezpieczeństwa* (Eng. Theory of security), in: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*, R. Zięba, S. Bieleń, J. Zając (sci. eds.), Warszawa 2015, p. 91.

5 Ibid., p. 87.

6 J. Kukułka, *Narodziny nowych koncepcji bezpieczeństwa* (Eng. Birth of new security concepts), Warszawa 1994, pp. 40–41.

gathered around Barry Buzan and Ole Wæver at the now defunct Copenhagen Peace Research Institute. Buzan, after the end of the Cold War, advocated the need to consider not only sovereign states but also non-state human collectivities in security analyses. He distinguished five sectors of security: military, political, economic, social as well as environmental, and was promoting the separation of further layers[7]. The need for changes in the understanding of the concept was also noted by Wæver. He emphasised the importance of a dualism-based conceptualisation of security, which, in the case of states, concerns the protection of sovereignty and, in relation to social groups, the preservation of their identity[8].

Various aspects of security are also being analysed in the Polish scientific community[9]. The interest in security can also be observed in the sphere of education[10]. The aim of this article is to discuss contemporary trends in the approach to security as an educational category. Four research problems are formulated in connection with the set objective:

1. What is security science about in the school subject 'education for security'?

---

7 B. Buzan, *New Patterns of Global Security in the Twenty-First Century*, "International Affairs" 1991, vol. 67, no. 3, p. 433.

8 O. Wæver, *Securization and Desecurization*, in: *On Security*, R.D. Lipschutz (ed.), New York 1995.

9 See e.g.: S. Koziej, *Wstęp do teorii i historii bezpieczeństwa* (Eng. Introduction to security theory and history), https://koziej.pl/wp-content/uploads/2018/12/BM-Cz-I-Podstawy-ewolucja-i-koncepcje.pdf [accessed: 14 I 2025]; S. Sulowski, *O rozwoju badań i postulacie interdyscyplinarności w naukach o bezpieczeństwie* (Eng. On the development of research and the demand for interdisciplinarity in security sciences), in: *Tożsamość nauk o bezpieczeństwie*, S. Sulowski (ed.), Toruń 2015, p. 33; *Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje* (Eng. Foundations of the security of the modern state (entity). Implications)), J. Pawłowski (sci. ed.), Warszawa 2015; R. Wróblewski, *Wprowadzenie do nauk o bezpieczeństwie* (Eng. Introduction to security sciences), Siedlce 2017; A. Glen, *Podstawy poznania bezpieczeństwa podmiotu. Aksjologia, ontologia, epistemologia, metodologia* (Eng. Foundations of cognition of subject security. Axiology, ontology, epistemology and methodology), Siedlce 2021; B. Wiśniewski, *Praktyczne aspekty bezpieczeństwa* (Eng. Practical aspects of security), Warszawa 2020; *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie* (Eng. Poland's national security in 21st century. Challenges and strategies), R. Jakubczak, J. Marczak (eds.), Warszawa 2011.

10 See e.g.: A. Pieczywok, *Przestrzeń edukacji dla bezpieczeństwa człowieka wobec niepewności i zagrożeń jego egzystencji* (Eng. The space of education for human security in the face of insecurity and threats to his existence), Bydgoszcz 2022; D. Kaźmierczak, M. Szumiec, *Człowiek we współczesnym świecie. Bezpieczeństwo, zdrowie, edukacja* (Eng. Man in a modern world. Security, health, education), Kraków 2021; I. Urych, A. Orzyłowska, *Wiedza o bezpieczeństwie w procesie dydaktycznym. Kontynuacja i rozwój myśli pedagogicznej* (Eng. Security education in the didactic proces. Continuation and development of pedagogical thought), Warszawa 2020; K. Krakowski, A. Gębczyńska, *Uwarunkowania dydaktyczne przygotowania obronnego państwa* (Eng. Didactic determinants of state defence preparedness), Warszawa 2018.

2. What are the characteristics education on security in the curriculum of military classes?
3. What are the characteristics of security-related curriculum content in the educational offer of universities?
4. What are the peculiarities of the attitude of the teacher of security education content towards the challenges of contemporary education?

In accordance with the aim of the research and the research problems related to description and diagnosis rather than verification research, the formulation of research hypotheses that could have an impact on the outcome of the research carried out was abandoned[11]. The problem situation was considered in the cognitive category, therefore the following research methods were used: analysis, synthesis, inference and abstraction[12], as well as the literature analysis and critique[13]. The conducted research was located in the field of social sciences in the discipline of security sciences[14].

Security education within the framework of the school subject 'education for security'

Security education is implemented within the framework of the school subject 'education for security'. Although the very concept of education for security emerged as early as 1994 during research on the national security system at the National Defence Academy[15], it was only in 2009 that a school subject under this name was introduced[16] and replaced defence training. It was dictated by the change of the nature of threats from military to non-military. The essence of the new subject was a comprehensive approach to security issues with the concentration

[11] M. Łobocki, *Metody i techniki badań pedagogicznych* (Eng. Methods and techniques of pedagogical research), Kraków 2016.

[12] M. Pelc, *Elementy metodologii badań naukowych* (Eng. Elements of scientific research methodology), Warszawa 2012, pp. 55–78.

[13] J. Pieter, *Zarys metodologii pracy naukowej* (Eng. Outline of research methodology), Warszawa 1975, p. 103.

[14] A. Misiuk, *O tożsamości nauk o bezpieczeństwie* (Eng. On the identity of security science), "Historia i Polityka" 2018, no. 23(30), pp. 9–19. https://doi.org/10.12775/HiP.2018.001.

[15] J. Świniarski, *Edukacja dla bezpieczeństwa jako najnowsza koncepcja wychowania metawojskowego i metaobronnego czasów globalizacji* (Eng. Education for security as the latest concept in meta-military and meta-defence education in times of globalisation), in: *Współczesne trendy w edukacji dla bezpieczeństwa. Kształcenie – wychowanie – motywowanie*, T. Szczurek (ed.), Warszawa 2011, p. 21.

[16] *Regulation of the Minister of National Education of 28 August 2009 on the implementation of security education.*

of educational activities on the issue of threats during times of peace, as well as ways of behaving in crisis situations, especially in the local environment.

The implementation of the subject 'education for security' of 30 hours in secondary school has been defined since 1 September 2009 by a regulation of the Minister of National Education[17]. After another education reform, according to which lower secondary schools were abolished and the time of education in primary and secondary schools was extended[18], since 1 September 2017 the subject of 'education for security' became compulsory also in class VIII of primary school to the extent of one hour per week. The educational content concerned state security, the organisation of rescue operations, health education and knowledge of first aid principles[19].

Another change to the teaching of security within the school subject 'education for security' took effect from the school year 2022/2023. The reason for the changes to the general education core curriculum for primary schools and secondary schools in the field of security education was stated as follows: *The growing threat to the state's security requires supplementing the learning objectives and teaching content of the subject of education for security with issues related to state defence, the acquisition of shooting skills and preparing students to deal with threats caused by warfare and the basics of tactical rescue*[20]. Thus, the section on health education included in the previous core curriculum for the subject 'education for security' was dropped in favour of a new section. In primary school, 'shaping of defence attitudes' was introduced, and in secondary school – 'defence education', implemented in order to master, among other things, shooting skills[21]. These are changes whereby the subject of 'education for security' is to include elements of building the defence capabilities of society.

---

[17] Ibid.

[18] *Regulation of the Minister of National Education of 14 February 2017 on the core curriculum for preschool education and the core curriculum for general education for primary schools, including for students with moderate or severe intellectual disabilities, general education in first-degree vocational secondary schools, general education for special needs vocational schools and general education for post-secondary schools.*

[19] *Regulation of the Minister of National Education of 14 June 2017 amending the regulation on the manner of implementation of education for security*.

[20] *Explanatory memorandum to the Regulation on the core curriculum of general education for upper secondary school, technical secondary school and upper secondary industrial school*, p. 3. The text of the explanatory memorandum is available at: https://www.gov.pl/web/nauka/edukacja-dla-bezpieczenstwa--rozporzadzenia-podpisane [accessed: 4 I 2025].

[21] Schools within the county that had access to ball guns, air guns, replicas, air soft guns, virtual shooting ranges or laser shooting ranges were required to teach shooting skills from the 2022/2023 school year. Schools within the county that did not have such access implemented this requirement as far as possible in the 2022/2023 and 2023/2024 school years.

In the school year 2024/2025, the ideas introduced for learning security are being continued. From this year onwards, systematic first aid training sessions are taking place from the first grades. The knowledge imparted at these courses is to be further developed at subsequent stages of education. In the core curriculum for grades I–III of primary school, first aid issues are part of the requirements in the area called 'achievements in human vital functions, health protection, safety and rest'. At further stages of education, first aid teaching is to be implemented during classes with the teacher who is to decide on the issue and the number of hours allocated to this subject. First aid knowledge is to be taught systematically, so that it can be better absorbed and consolidated. The lessons are to be practical and teach attitudes such as responsibility for others and readiness to help as well as to raise awareness of the importance of quick response in life-threatening situations[22].

Teaching about security in military class education programmes

Security-related content is also included in the curricula of military classes[23]. This term is now used in Poland to describe secondary school classes, which in addition to the curriculum adopted at a given school implement a programme of education for security, enriched with topics related to national defence, the history of the Polish armed forces and the shaping of patriotic attitudes among young people. Attractive education programmes are conducive to the achievement of ambitious didactic and educational goals in the area of security[24].

[22] *Regulation of the Minister of Education of 20 May 2024 on the outline curricula for public schools.*

[23] Security content is also included in the curricula of other uniformed classes, e.g. police, firefighting, Border Guard, Prison Service or Customs Service. However, none of these classes has an institutionally defined and coherent educational programme, which means that these classes function within the framework of pedagogical innovations specific to the schools in question. Only military classes, formerly occurring in the formula of certified military uniform classes and now military preparation units, have an educational programme that is consistent across the board, so it is their programme that is considered in this article.

[24] On the aims and programmes of education in military classrooms, see in more detail: I. Urych, *Military Innovations in Secondary Schools in Poland as a Manifestation of Strengthening National Security within the Meaning of Articles 5 and 26 of the Polish Constitution,* "Przegląd Prawa Konstytucyjnego" 2020, no. 6(58), pp. 461–474. https://doi.org/10.15804/ppk.2020.06.37; L. Kanarski et al., *Wstępna diagnoza funkcjonowania klas mundurowych – wyniki badań pilotażowych* (Eng. Preliminary diagnosis of the functioning of uniformed classes – results of a pilot study), in: *Klasy mundurowe. Od teorii do dobrych praktyk*, A. Skrabacz, I. Urych, L. Kanarski (eds.), Warszawa 2016, pp. 71–82.

Nowadays, military classes can function in the formulas of[25]: pedagogical innovations in defence education (since 2002)[26], certified military uniform classes (since 2017)[27] and military preparation units (since 2020)[28]. The multiplicity of these forms of education may cause some difficulties in grasping them. In order to indicate contemporary trends of education in the security area, military preparation classes are briefly characterised as a result of the recent reorganisation of military classes[29].

Military preparation units were introduced on 1 September 2020 in secondary schools[30]. This was the result of work on the introduction of a systemic solution for the operation of military classes. This solution was based on conclusions and experiences gained from successive editions of the pilot programme implemented in military certified uniformed classes. It consisted of 185 lesson hours of theoretical and practical classes and a five-day camp in military training conditions within the subject of 'military education'.

The curriculum of the military preparation units in accordance with the regulation of the Minister of National Defence includes training in the form of 180 hours of compulsory educational classes. The theoretical part consists of 70 lessons at school and the practical part consists of 60 lessons conducted in a patron military unit. The training ends with a 50-hour training camp held at the beginning of the final year of schooling. A permit to run a military preparation unit shall be issued by the Minister of National Defence on the application of the authority running the school[31]. Upon approval, the minister provides financial support in the form of targeted grants. The scope of the assistance provided is strictly defined and includes: clothing of pupils (its pattern has been developed), supplementing with equipment necessary for the conduct of classes, running of the class (e.g. transporting pupils for classes to military units), infrastructural investment at school (e.g. an air rifle range

[25] See in more detail: I. Urych, *Współczesne paradygmaty kształcenia obronnego młodzieży* (Eng. Contemporary paradigms of youth defence education), "Bellona" 2022, no. 3(210), pp. 113–126.

[26] Pedagogical innovations – innovative curricular, organisational or methodological solutions aimed at improving the quality of school work. See: § 1 point 1 of the *Regulation of the Minister of National Education and Sport of 9 April 2002 on the conditions for conduct of innovative and experimental activities by public schools and institutions.*

[27] See: *Pilot programme to support secondary schools running divisions of Certified Military Uniformed Classes*, Ministerstwo Obrony Narodowej.

[28] See: Training programme in military preparation units, annex to the *Regulation of the Minister of National Defence of 21 May 2020 on training in the military preparation unit*.

[29] *Act of 19 July 2019 amending act – Education Law and the Act on the financing of educational tasks*.

[30] Ibid.

[31] Ibid., Article 28a(6).

or a physical fitness track)[32]. The grant is conditional on a minimum of 22 pupils per unit. It is granted in the year of the opening of the first unit, and the purchased property is to serve the school in subsequent years. The school can apply for another grant four years after receiving the first funding.

Students studying in military preparation units, in addition to acquiring knowledge and skills suitable for the first stage of training as a soldier in the Polish Armed Forces, have the possibility to undergo a shortened preparatory service and, as a consequence, to become a soldier in the personal reserves of the Polish Armed Forces, or to enter active military service. In addition, a graduate of such a unit may undergo 12 days of basic training, after which he or she may receive additional points in recruitment to military universities.

It is worth citing the rationale behind the creation of such units:

> The possibility of creating military preparation units in schools, as a systemic solution, is a way to meet social expectations and needs, and to increase the dissemination of education in the field of defence, to which the Ministry of National Defence attaches particular importance. The results that the Ministry of National Defence wants to achieve are the replenishment of the personnel reserves of the Armed Forces, the Territorial Defence Forces with volunteers, in the longer term increasing the size of the Armed Forces, as well as strengthening defence education in society[33].

Curricular content in the field of security in higher education programmes

Security-related curriculum content is also found in higher education. New fields of study have been created, e.g.: national security, internal security, international security, information security. These are also topics covered as part of many postgraduate programmes (adult education). This can include courses such as: education for security, international military relations, special services or in-service training in the implementation of training in military preparation units[34].

---

[32] *Regulation of the Minister of National Defence of 7 August 2020 on support for the body running the military preparation unit.*

[33] *Oddziały przygotowania wojskowego* (Eng. Military preparation units), Wojsko Polskie, https://www.wojsko-polskie.pl/zostanzolnierzem/odzialy-przygotowania-wojskowego/ [accessed: 5 I 2025].

[34] *Oferta studiów podyplomowych (rok akademicki 2024/2025)* (Eng. Postgraduate studies on offer (academic year 2024/2025)), Akademia Sztuki Wojennej, https://www.wojsko-polskie.pl/aszwoj/studia-podyplomowe/ [accessed: 5 I 2025].

The security-related content of the bachelor's and master's degree programmes, both full-time and part-time, covers a wide range of theoretical and practical elements of contemporary security, understanding of its threats and its prevention. Graduates of such studies should possess a body of knowledge and skills in broadly defined security, needed to understand the principles of the functioning of the state, its security systems, the role of institutions and bodies responsible for ensuring national, internal and international security or cyber security. In addition, they gain competencies in planning and organising as well as leading people, which are essential in emergencies. Graduates can be employed in central and local government administration, where tasks concerning defence preparations, maintaining defence readiness and continuity of the state's functioning, analysing and forecasting threats to national or international security, as well as countering other types of threats are carried out[35]. Graduates of security studies are also future employees of, for example: Ministry of National Defence, Ministry of Foreign Affairs, special services, Police, Border Guard, Municipal Police, Military Police, Government Centre for Security, Territorial Defence Forces, Polish Institute of International Affairs and other scientific and analytical entities or EU institutions.

Security-related curricular content in the educational offer of higher education institutions is also provided in specialised courses (in-service training and continuing education) that emphasise this issue. For example, at the War Studies University, defence courses are conducted for persons in charge of the performance of defence tasks and those carrying out these tasks in the public administration as well as at entrepreneurs on whom the obligation to perform defence tasks has been imposed. The main objective of such courses is (…) *to familiarise participants with the principles of security and defence, elements of security policy and the organisation and principles of functioning of the state defence system in terms of the role of individual participants in the defence system of the Republic of Poland*[36].

Curricular content related to security is taught also in doctoral studies in the field of social sciences in the discipline of security sciences. It is worth recalling that, according to the current legal conditions, doctoral training can only take place in doctoral schools[37].

---

[35] *Bezpieczeństwo narodowe i obrona powszechna* (Eng. National security and general defence), Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/bezpieczenstwo-narodowe-licencjackie/ [accessed: 7 I 2025].

[36] *Szkoła Administracji Obronnej* (Eng. School of Defence Administration), Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/szkola-administracji-obronnej/ [accessed: 7 I 2025].

[37] *Act of 20 July 2018 – The Law on Higher Education and Science*, Article 198(1–5).

The new model of education with security-related curriculum content in the educational offer of universities requires a change in the way of education and basing it on the 'new culture of learning'[38]. According to the paradigms of modern education, its essence should be the process of independent knowledge acquisition as a result of the research activity undertaken. A modern university should use the intellectual potential of both university lecturers and students, enable them to learn effectively, to learn and to understand contemporary reality. It is worth noting that the skills currently being taught, the knowledge and values transferred may be different from the needs that will occur in the future. Therefore, tertiary education in specific areas of security should prevent this as much as possible, anticipate the expectations of the future, prepare students and trainees for the different threats that dynamically changing realities may bring. This makes the list of security areas open and requires further cognitive and research exploration, and a university teacher is a person who not only teaches others, but also educates themselves.

The teacher educating in the field of security in the face of the challenges of contemporary education

In considering security as an educational category, it is difficult not to refer directly to the role of teachers responsible for the teaching and learning process in primary and secondary schools, as well as university lecturers. The effectiveness of education largely depends on their experience, knowledge and skills. This thought was aptly formulated by Ryszard Stępień: *The leading role in such education should be played by adequately prepared teachers, whose task is to impart to students such a body of knowledge and skills as to enable them to take effective action and accurate decisions* (…). *In this way, after leaving school young people will enter adult life well prepared not only to fulfil their professional duties, but also to ensure their own and others' security*[39].

When analysing the literature[40] on the attitude of the teacher delivering the security-related content towards the challenges of contemporary education, it is

[38] J. Szymaniak, *Pojęcie kultury i wspólnotowości szkolnej. "Nowa kultura uczenia się"* (The concept of school culture and community. 'The new culture of learning'), "Studia Gdańskie. Wizje i rzeczywistość" 2014, vol. 11, pp. 28–42.

[39] R. Stępień, *Teoretyczne zagadnienia edukacji dla bezpieczeństwa* (Eng. Theoretical issues in education for security), in: *Materiały* z konferencji: edukacja dla bezpieczeństwa dzieci i młodzieży, R. Stępień (ed.), Warszawa 1999, p. 15.

[40] See eg.: I. Urych, A. Orzyłowska, *Wiedza o bezpieczeństwie*…; *Nauczyciel szkoły wyższej w procesie dydaktyczno-wychowawczym. Implikacje teoretyczne i praktyczne* (Eng. The teacher in higher education in the teaching and learning process – theoretical and practical implications), I. Urych

worth noting the opinion of experts in this field[41]. They emphasise that the challenge of contemporary education is the predisposition of candidates to become teachers of education for security, military classes or lecturers at universities or security-related courses. A passion for the subject being taught seems to be fundamental here. In addition, practitioners who are well versed in the theory and principles of teaching this type of class, or teachers with military training, would be most desirable in this role. Their morale and their representation of pro-citizen and pro-social values are also important, as well as other qualities of a good teacher, such as strong intrinsic motivation, friendliness and high personal culture.

Representatives of the military scientific community believe that an important supplement to the preparation for the profession of a teacher who educates in the content in question is the mastery of military teaching methodology within the courses at the Ministry of National Defence training centres and centres or completion of basic military training. Formal preparation, in the form of courses and postgraduate studies in broadly defined security education and defence education, as well as providing pedagogical, psychological and methodological preparation, would be valuable.

In contrast, experts are critical of the preparation of teachers on the basis of online knowledge with the omission of legitimate doctrines, regulations and instructions. There are opinions that the process of preparing teachers conveying security-related content should be analogous to the education of vocational subject teachers. In addition, the continuous teacher education should be supported by e-learning platforms, which would include all the necessary and systematically updated news on the education of military classes in particular. In other words, the challenge of modern education is to ensure that teachers have access to the relevant theoretical and practical knowledge necessary for teaching.

(sci. ed.), Warszawa 2019; I. Urych, *Potencjał obronny klas wojskowych. Teoretyczno-empiryczne aspekty kształcenia obronnego* (Eng. The defence potential of military classes. Theoretical and empirical aspects of defence education), Warszawa 2019; I. Urych, A. Orzyłowska, *Nauczyciel klas mundurowych. Wyzwania i oczekiwania podmiotów publicznych wobec pedagogów* (Eng. The teacher of uniformed classes. Challenges and expectations of public actors towards educators), in: *Edukacja jutra. Formy wzbogacania wychowania i zmniejszania zagrożeń społecznych*, A. Kamińska, P. Oleśniewicz (sci. eds.), Warszawa 2019, pp. 119–131.

[41] A qualitative analysis of empirical material constituting a fragment of a larger study on diagnosing the broadly understood potential of uniformed classes with a military profile. Experts included representatives of the military academic community, Ministry of National Defence officials who substantively supervise the educational process in military classes, headmasters of schools in which uniformed classes operate, and teachers of these classes. The research was conducted among 12 experts. Diagnostic survey and interview technique were used in it.

On the subject of preparing teachers who share security-related content, two solutions emerge emphasising the different stages of their education. The first one, which is easier to implement, emphasises the need to organise further, continuous education of teachers and to prepare for them a rich offer of courses, trainings, postgraduate studies, also in a remote form. The second is innovative in nature and envisages the creation of an extensive teacher education programme that provides thorough pedagogical preparation and knowledge of security and defence in general. Such studies could be conducted jointly by several universities and thus enrich the process of preparing future teachers with research ventures, specialisations and reciprocal internships, which would increase the creative potential (synergy effect), as well as foster the modernisation and optimisation of the system of educating teachers of security-related content.

Another challenge in contemporary education concerns the self-awareness of teaching staff. With their attitudes towards their profession, teachers of education for security, military classes or higher education or security-related courses reveal a lack of understanding of the duties of their profession, i.e. the transmission of knowledge, skills and behavioural patterns so that the subjects of education, as well as the various social groups to which they belong, can develop. In other words, teaching staff are challenged to acquire or increase their self-awareness of the expectations that the state and society have placed on them. At the same time, there is a noticeable lack of a broader view of the social roles played by teachers, which have an impact on shaping the attitudes and worldview of students, which in a broader perspective affects, among other things, the national defence policy, social engagement or the building of civil society. In addition, mention should be made of the low level of social competence of those in the profession and their attachment to traditional encyclopaedism.

The modern teacher also struggles with a number of general problems. In 2019, the Centre for Public Opinion Research (CBOS) conducted a survey in which respondents indicated the professions they held in highest regard. The most respected profession among the public is the firefighter (94% of surveyed Poles indicated this profession as being held in high esteem by the public). In second place is the nurse (89% of indications of high esteem)[42]. Both of these professions are characterised by high social utility, as it is inscribed in them to help others. It is interesting to note that these qualities can also be attributed to teacher, yet this profession is not at the top of the ranking – it ranked seventh (77% of respondents indicated high regard). It is worth noting that, compared to the 1980s, a decrease in

[42] M. Omyła-Rudzka, *Które zawody poważamy* (Eng. Which professions do we hold in a high esteem), "Komunikat z badań CBOS" 2019, no. 157.

high esteem can be observed for the academic professor (7 percentage points) and the teacher in general (4 percentage points). The greatest declines in recognition were recorded in the 1990s. It is encouraging that in recent years there has been a small but nonetheless growing appreciation of the work of teachers[43]. It seems that the prestige of individual professions is to some extent shaped by the situation on the labour market, and this – in the case of the teaching profession – is not satisfactory.

Conclusions

The reflection on the issue addressed in the article stems from an observation concerning the consideration of security from an educational perspective, both in public discourse and in academic debate. The aim of the article was to discuss contemporary trends related to the consideration of security as an educational category. The analysis carried out made it possible to answer the research problems posed and to formulate the following conclusions:

1. The primal need to be safe, i.e. the striving for survival and development, implies educational activities aimed at supporting the educated in shaping the quality of life in accordance with the didactic and educational ideals adopted in a given society. Education as an intentional process of developmental changes of the educated subjects includes the processes of upbringing and schooling, i.e. activities conducive to the development of individuals, their attainment of the desired knowledge and skills, as well as the formation of attitudes and activity for the common good, i.e. security in the following dimensions: individual and collective, local and state, spatial and procedural.
2. The diversity of expectations of security science in the school subject 'education for security', military classes, higher education or security-related courses may provide a rationale for the preparation of training programmes for teacher candidates specialising not only in a particular subject or educational stage, but more broadly in the discipline of security science.
3. The teacher specialising in security education in the face of the challenges of modern education adopts various attitudes – from those aiming at continuous developing his/her competences and more effective working methods to passivity, lack of development and the transmission

[43] Ibid., p. 7.

of learned knowledge based on encyclopaedism. The latter attitude may be indicative of the fact that teaching staff in both primary, secondary and tertiary education is solely focused on obtaining financial gain and other advantages through their work. In such a situation, the fundamental duty of education about security, for security and in security as a contribution to the multifaceted effort of societies to persist and develop is lost.

4. The outlined complexity of security issue as an educational category provides a basis for permanent scientific research in this area. At the same time, they should have not only an exploratory purpose, but also a utilitarian one – the theoretical knowledge gained may constitute imperatives for changes in the content of security-related education. It seems that it is also necessary to give this knowledge an operational character, necessary for its application in the form of universally binding procedures. They will be effective models of behaviour in crisis situations for already educated citizens, but also for institutions of an aid character, services, government and local government administration, and more broadly – different entities acting for the benefit of security. Thus, they will become a determinant of their statutory activity. In view of this, it is desirable that the results of research in the discipline of security sciences should serve to develop procedures that would eliminate socio-political relations based on divisions and discrimination, indicating layers of subordinators and subordinated, i.e. serve to develop the same rights and duties of each citizen for the security of the state.

The content presented in the article does not exhaust the complex issue of security as an educational category, it does highlight some trends in the contemporary conditions of this sphere of *praxis* and *doctrina*. Thus, in the author's thought, they may inspire practitioners to reflect on the complexity of educational processes concerning security, and theorists to further research. The issues raised are challenging, especially for educators whose research and teaching practice is concerned with security. Meeting the challenges is often not easy, but it is in line with the idea of security as the overriding need, value and purpose of any real-world entity. A sense of security is essential for the survival of this entity, its functioning, development and achieving interests, both individual and collective[44].

[44] *Bezpieczeństwo* (Eng. Security), in: *Słownik terminów z zakresu bezpieczeństwa*, J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (sci. eds.), Toruń 2020, pp. 20–21.

Bibliography

Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie (Eng. Poland's national security in 21st century. Challenges and strategies), R. Jakubczak, J. Marczak (eds.), Warszawa 2011.

Buzan B., *New Patterns of Global Security in the Twenty-First Century*, "International Affairs" 1991, vol. 67, no. 3, pp. 431–451. https://doi.org/10.2307/2621945.

Glen A., *Podstawy poznania bezpieczeństwa podmiotu. Aksjologia, ontologia, epistemologia, metodologia* (Eng. Foundations of cognition of subject security. Axiology, ontology, epistemology and methodology), Siedlce 2021.

Kanarski L., Koter M., Loranty K., Urych I., *Wstępna diagnoza funkcjonowania klas mundurowych – wyniki badań pilotażowych* (Eng. Preliminary diagnosis of the functioning of uniformed classes – results of a pilot study), in: *Klasy mundurowe. Od teorii do dobrych praktyk*, A. Skrabacz, I. Urych, L. Kanarski (eds.), Warszawa 2016, pp. 71–82.

Kaźmierczak D., Szumiec M., *Człowiek we współczesnym świecie. Bezpieczeństwo, zdrowie, edukacja* (Eng. Man in a modern world. Security, health, education), Kraków 2021.

Krakowski K., Gębczyńska A., *Uwarunkowania dydaktyczne przygotowania obronnego państwa* (Eng. Didactic determinants of state defence preparedness), Warszawa 2018.

Kukułka J., *Narodziny nowych koncepcji bezpieczeństwa* (Eng. Birth of new security concepts), Warszawa 1994.

Łobocki M., *Metody i techniki badań pedagogicznych* (Eng. Methods and techniques of pedagogical research), Kraków 2016.

Maciejewska-Mieszkowska K., *Eskalacja wojny w Ukrainie jako czynnik determinujący poczucie zagrożenia bezpieczeństwa Polski w ocenie społecznej* (Eng. Escalation of the war in Ukraine as a determinant of the feeling of threat to Poland's security in the public assessment), "Środkowoeuropejskie Studia Polityczne" 2023, no. 2, pp. 217–236. https://doi.org/10.14746/ssp.2023.2.12.

Misiuk A., *O tożsamości nauk o bezpieczeństwie* (Eng. On the identity of security science), "Historia i Polityka" 2018, no. 23(30), pp. 9–19. https://doi.org/10.12775/HiP.2018.001.

Multan W., *Bezpieczeństwo międzynarodowe ery nuklearnej* (Eng. International security of the nuclear age), Warszawa 1991.

Nauczyciel szkoły wyższej w procesie dydaktyczno-wychowawczym. Implikacje teoretyczne i praktyczne (Eng. The teacher in higher education in the teaching and learning process – theoretical and practical implications), I. Urych (sci. ed.), Warszawa 2019.

Omyła-Rudzka M., *Które zawody poważamy* (Eng. Which professions do we hold in a high esteem), "Komunikat z badań CBOS" 2019, no. 157.

Pacholczak A., *Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, pp. 97–129. https://doi.org/10.4467/20801335PBW.24.015.19617.

Pelc M., *Elementy metodologii badań naukowych* (Eng. Elements of scientific research methodology), Warszawa 2012.

Pieczywok A., *Przestrzeń edukacji dla bezpieczeństwa człowieka wobec niepewności i zagrożeń jego egzystencji* (Eng. The space of education for human security in the face of insecurity and threats to his existence), Bydgoszcz 2022.

Pieter J., *Zarys metodologii pracy naukowej* (Eng. Outline of research methodology), Warszawa 1975.

Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje (Eng. Foundations of the security of the modern state (entity). Implications), J. Pawłowski (sci. ed.), Warszawa 2015.

Słownik terminów z zakresu bezpieczeństwa (Eng. Dictionary of security terms), J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (sci. eds.), Toruń 2020.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa* (Eng. Contemporary understanding of security), Warszawa 1996.

Stępień R., *Teoretyczne zagadnienia edukacji dla bezpieczeństwa* (Eng. Theoretical issues in education for security), in: *Materiały z konferencji: edukacja dla bezpieczeństwa dzieci i młodzieży*, R. Stępień (ed.), Warszawa 1999.

Sulowski S., *O rozwoju badań i postulacie interdyscyplinarności w naukach o bezpieczeństwie* (Eng. On the development of research and the demand for interdisciplinarity in security sciences), in: *Tożsamość nauk o bezpieczeństwie*, S. Sulowski (ed.), Toruń 2015.

Szymaniak J., *Pojęcie kultury i wspólnotowości szkolnej. "Nowa kultura uczenia się"* (Eng. The concept of school culture and community. 'The new culture of learning'), "Studia Gdańskie. Wizje i rzeczywistość" 2014, vol. 11, pp. 28–42.

Świniarski J., *Edukacja dla bezpieczeństwa jako najnowsza koncepcja wychowania metawojskowego i metaobronnego czasów globalizacji* (Eng. Education for security as the latest concept in meta-military and meta-defence education in times of globalisation), in: *Współczesne trendy w edukacji dla bezpieczeństwa. Kształcenie – wychowanie – motywowanie*, T. Szczurek (ed.), Warszawa 2011, pp. 7–43.

Urych I., *Military Innovations in Secondary Schools in Poland as a Manifestation of Strengthening National Security within the Meaning of Articles 5 and 26 of the Polish Constitution*, "Przegląd Prawa Konstytucyjnego" 2020, no. 6(58), pp. 461–474. https://doi.org/10.15804/ppk.2020.06.37.

Urych I., *Potencjał obronny klas wojskowych. Teoretyczno-empiryczne aspekty kształcenia obronnego* (Eng. The defence potential of military classes. Theoretical and empirical aspects of defence education), Warszawa 2019.

Urych I., *Współczesne paradygmaty kształcenia obronnego młodzieży* (Eng. Contemporary paradigms of youth defence education), "Bellona" 2022, no. 3(210), pp. 113–126. https://doi.org/10.5604/01.3001.0016.1952.

Urych I., Orzyłowska A., *Nauczyciel klas mundurowych. Wyzwania i oczekiwania podmiotów publicznych wobec pedagogów* (Eng. The teacher of uniformed classes. Challenges and expectations of public actors towards educators), in: *Edukacja jutra. Formy wzbogacania wychowania i zmniejszania zagrożeń społecznych*, A. Kamińska, P. Oleśniewicz (sci. eds.), Warszawa 2019, pp. 119–131.

Urych I., Orzyłowska A., *Wiedza o bezpieczeństwie w procesie dydaktycznym. Kontynuacja i rozwój myśli pedagogicznej* (Eng. Security education in the didactic process. Continuation and development of pedagogical thought), Warszawa 2020.

Wæver O., *Securization and Desecurization*, in: *On Security*, R.D. Lipschutz (ed.), New York 1995.

Wiktor Z., *Wojna w Ukrainie – przyczyny i skutki po ponad roku trwania* (Eng. War in Ukraine – causes and consequences after more than a year), "Studia Orientalne" 2023, vol. 12, no. 3(27), pp. 30–59. https://doi.org/10.34862/rmb.2023.2.5.

Wiśniewski B., *Praktyczne aspekty bezpieczeństwa* (Eng. Practical aspects of security), Warszawa 2020.

Wróblewski R., *Wprowadzenie do nauk o bezpieczeństwie* (Eng. Introduction to security sciences), Siedlce 2017.

Zadorożna M., Butuc M., *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "Security and Defence Quarterly" 2024, no. 46(2), pp. 47–65. https://doi.org/10.35467/sdq/189686.

Zięba R., *Teoria bezpieczeństwa* (Eng. Theory of security), in: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*, R. Zięba, S. Bieleń, J. Zając (sci. eds.), Warszawa 2015.

Internet sources

Bezpieczeństwo narodowe i obrona powszechna (Eng. National security and general defence), Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/bezpieczenstwo-narodowe-licencjackie/ [accessed: 7 I 2025].

Koziej S., *Wstęp do teorii i historii bezpieczeństwa* (Eng. Introduction to security theory and history), https://koziej.pl/wp-content/uploads/2018/12/BM-Cz-I-Podstawy-ewolucja-i--koncepcje.pdf [accessed: 14 I 2025].

Oddziały przygotowania wojskowego (Eng. Military preparation units), Wojsko Polskie, https://www.wojsko-polskie.pl/zostanzolnierzem/odzialy-przygotowania-wojskowego/ [accessed: 5 I 2025].

Oferta studiów podyplomowych (rok akademicki 2024/2025) (Eng. Postgraduate studies on offer (academic year 2024/2025)), Akademia Sztuki Wojennej, https://www.wojsko-polskie.pl/aszwoj/studia-podyplomowe/ [accessed: 5 I 2025].

Szkoła Administracji Obronnej (Eng. The War Studies University), Wojsko Polskie, https://www.wojsko-polskie.pl/aszwoj/szkola-administracji-obronnej/ [accessed: 7 I 2025].

Legal acts

Act of 19 July 2019 amending act – Education Law and the Act on the financing of educational tasks (consolidated text, Journal of Laws of 2019, item 1681, 2248).

Act of 20 July 2018 – The Law on Higher Education and Science (consolidated text, Journal of Laws of 2024, item 1571, as amended).

Regulation of the Minister of Education of 20 May 2024 on the outline timetables for public schools (Journal of Laws of 2024, item 781).

Regulation of the Minister of National Defence of 7 August 2020 on support for the body running the military preparation unit (Journal of Laws of 2020, item 1390).

Regulation of the Minister of National Defence of 21 May 2020 on training in the military preparation unit (Journal of Laws of 2020, item 977).

Regulation of the Minister of National Education of 14 June 2017 amending the regulation on the manner of implementation of education for security (Journal of Laws of 2017, item 1239).

Regulation of the Minister of National Education of 14 February 2017 on the core curriculum for preschool education and the core curriculum for general education for primary schools, including for students with moderate or severe intellectual disabilities, general education in first-degree vocational secondary schools, general education for special needs vocational schools and general education for post-secondary schools (Journal of Laws of 2017, item 356).

Regulation of the Minister of National Education of 28 August 2009 on the implementation of security education (Journal of Laws of 2009, no. 139, item 1131).

Regulation of the Minister of National Education and Sport of 9 April 2002 on the conditions for the conduct of innovative and experimental activities by public schools and institutions (Journal of Laws of 2002, no. 56, item 506).

Other documents

Pilot programme to support secondary schools running divisions of Certified Military Uniformed Classes, Ministerstwo Obrony Narodowej.

Explanatory memorandum to the Regulation on the core curriculum of general education for upper secondary school, technical secondary school and upper secondary industrial school, https://www.gov.pl/web/nauka/edukacja-dla-bezpieczenstwa--rozporzadzenia-podpisane [accessed: 4 I 2025].

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

Associate professor in security sciences, Vice Dean for Student Affairs at the Faculty of National Security at the War Studies University. She conducts training for civilian and military personnel in the area of pedagogical development as well as leadership and social competences. Her research interests are: military education, security education, social security, health security, leadership, security psychology, interdisciplinarity of security sciences.

Contact: i.urych@akademia.mil.pl

Internal Security Review
2025, no. 32, pp. 285–300

https://doi.org/10.4467/20801335PBW.25.014.22180

ARTICLE

Traffic control and the fight against cross-border crime

ŁUKASZ FORYŚ

Police Academy in Szczytno

https://orcid.org/0000-0003-1241-8722

KORNELIA STĘPIEŃ

Police Academy in Szczytno

https://orcid.org/0000-0002-8804-0765

Abstract

Cross-border crime, despite numerous actions taken by entities responsible for ensuring security, poses a serious challenge for law enforcement agencies. The aim of this article is to analyse cross-border crime from the perspective of an officer serving on the road and to indicate – based on a review of literature and statistical data – the importance of traffic control in combating this crime. The authors point out the impact of free movement within the Schengen area and the European Union on this type of crime.

Keywords

security, cross-border crime, control, traffic, Schengen area, European Union

Introduction

EU transport policy supports the building of a modern infrastructure network that provides both safer and faster travel. In doing so, it promotes the deployment of digital solutions, which on the one hand, streamline transport chains and make it easier to move around using different modes of transport, and on the other hand, enable crime.

Transport is an essential part of everyone's life. According to information published by the European Commission (EC), between 2011 and 2019, the share of passenger cars in passenger transport in the EU fell from 73.1% to 69.8%. In 2020, this share increased to 81.9%, and in 2021 it fell slightly to 79.7%. The share of aircraft in this transport increased from 10.9% in 2011 to 15% in 2019, but fell to 5.7% in 2020 and was 7.3% in 2021. Other transport modes showed similar patterns, with a sharp decline in 2020 followed by a partial recovery in 2021[1]. The changes in 2020 followed the COVID-19 pandemic crisis, which affected overall transport use and made people more likely to choose private cars over public transport. A similar relationship can be seen in relation to the war in Ukraine. People who fled the affected areas in large numbers mainly opted for road transport. It is the most popular mode of transport among both individuals and businesses. This is influenced by the extensive road network, easy access to motor vehicles and the ability to efficiently transport large amounts of cargo at one time. Vehicles have also been used for years for criminal activities, e.g. smuggling drugs, people, goods, works of art, exotic animals, etc., as well as for terrorist attacks, which has been particularly evident in recent years[2]. Sporadic traffic controls are a factor that encourages criminal groups to use this particular mode of transport because of the low risk of exposing their activities.

Furthermore, transport plays an important role in the European economy. It accounts for more than 9% of gross value added in the European Union and nearly 11 million people are employed in transport services[3]. As societies become more mobile, EU policy has supported transport systems to address their main problems, including infrastructure, congestion, safety, pollution, among others. To address these, the EC has taken numerous measures, including the creation

[1] *Statistics Explained*, Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=456757 [accessed: 10 XII 2024].

[2] For example, from 14 VII 2016 to 1 XI 2017, there were at least seven jihadist attacks using a vehicle (14 VII 2016 – Nice, 19 XII 2016 – Berlin, 22 III and 3 VI 2017 – London, 7 IV 2017 – Stockholm, 17 VIII 2017 – Barcelona, 31 X 2017 – New York).

[3] *Safe, sustainable and connected transport*, European Union, https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_en [accessed: 10 XII 2024].

of a Single European Transport Area over the last decade. The aim was to remove barriers between transport modes and national systems, improve integration or facilitate the emergence of international and multimodal operators[4].

The number of service providers in the transport industry on a global scale continues to increase, with more and more interdependencies emerging between them. The system of the global economy is influenced by changes both in the economy itself and in other areas, which have resulted in a noticeable increase in the role of Asian countries, especially China and India, in the world economy, the integration of the economies of Central and Eastern Europe into the world economic circuit, a significant decrease in transport costs, multilateral liberalisation of trade, deregulation of telecommunications markets, rapid progress in the implementation of achievements in information and telecommunications technology[5]. Faced with a changing reality, security actors need to analyse their actions, improve existing procedures, skills and introduce new technologies to counter crime.

Traffic control is most often associated with actions taken by authorised authorities, e.g. the Police, to ensure safety and order on the roads. It includes, among other things, checking documents, the technical condition of vehicles, drivers' compliance with traffic regulations and testing their sobriety. However, according to the authors, the possibilities of using traffic control to ensure safety are much broader. When carrying out such checks, police officers can verify persons and items in the Police ICT systems, as well as cargo, luggage and their conformity with the documents held (where required).

The purpose of this article is to discuss cross-border crime from the perspective of an officer on duty on the road and to indicate, on the basis of a literature review and statistical data, the importance of traffic control in combating this crime.

The concept of cross-border crime

Pursuant to *Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union*:

[4] Ł. Foryś, R. Gwardyński, M. Żuber, *Wybrane aspekty bezpieczeństwa dotyczące mobilności człowieka* (Eng. Selected safety aspects of human mobility), Szczytno 2024, p. 61.

[5] Ibid., p. 62.

> (1) The main motive for cross-border organised crime, including mafia-type criminal organisation, is financial gain. As a consequence, competent authorities should be given the means to trace, freeze, manage and confiscate the proceeds of crime. However, the effective prevention of and fight against organised crime should be achieved by neutralising the proceeds of crime and should be extended, in certain cases, to any property deriving from activities of a criminal nature.
> (2) Organised criminal groups operate without borders and increasingly acquire assets in Member States other than those in which they are based and in third countries. There is an increasing need for effective international cooperation on asset recovery and mutual legal assistance.
> (3) Among the most effective means of combating organised crime is providing for severe legal consequences for committing such crime, as well as effective detection and the freezing and confiscation of the instrumentalities and proceeds of crime.
> (4) Although existing statistics are limited, the amounts recovered from proceeds of crime in the Union seem insufficient compared to the estimated proceeds. Studies have shown that, although regulated by Union and national law, confiscation procedures remain underused[6].

According to Piotr Kozłowski, Andrzej Wawrzusiszyn's definition of cross-border crime indicates that:

> (…) cross-border crime is one of the forms of organised crime. It is a dynamic phenomenon, which undergoes constant changes and modifications depending on the area and methods of operation as well as the category of smuggled goods. Cross-border crime is capable of adapting rapidly to local needs and of filling the demand for services and goods in short supply, generating profit margins for the organisers of the crime. Existing border traffic and the international exchange of goods try to exploit cross-border crime for their purposes[7].

Cross-border crime is defined as criminal activities that are carried out within or breach the borders of different countries. It is often associated with transnational

[6] *Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union*.

[7] P. Kozłowski, *Przestępczość transgraniczna w latach 2015–2017 zagrożeniem dla bezpieczeństwa wewnętrznego państwa w świetle danych statystycznych Bieszczadzkiego Oddziału Straży Granicznej w Przemyślu* (Eng. Cross-border crime in 2015-2017 as a threat to the state's internal security in the light of statistical data from the Bieszczady Border Guard Unit in Przemyśl), "Współczesne Problemy Zarządzania" 2020, vol. 8, no. 1(16), p. 86. https://doi.org/10.52934/wpz.86.

organised crime, which adopts a network structure. This type of crime poses a serious threat to the state security system due to: (…) *the long-term effects of cross-border organised crime activity, the origins of which are to be found in the so-called secondary effects of criminal groups. Given that organised crime groups gain certain material benefits as a result of their illegal activities, it must also be assumed that the resources they gain can and are used to influence the situation of individual countries, their economies and consequently their security*[8]. Cross-border crime includes, inter alia, smuggling of goods, drugs, weapons, waste, works of art, nuclear and radioactive materials, as well as terrorism. The manner, forms and extent of cross-border organised crime activity varies greatly between countries and depends on a number of factors, e.g. socio-economic conditions, government policy and stability, the legal system and law enforcement. It is very difficult to assess the scale of the phenomenon and its impact on the security of states and the international system. As Paweł Lubiewski notes:

> Contemporary socio-political conditions generate a number of problems, which the state administration has to cope with and to learn to handle unknown ones as soon as possible. Undoubtedly, the state border is this field of state administration activity. (…) In relation to the problem of protecting the borders of a modern state, the dual character of border protection is clearly discernible, manifested on the one hand in the need to protect the integrity of the border, and on the other hand in the need to protect against a number of serious threats penetrating it into the state[9].

This is one of the main reasons why, nowadays, a single institution is not sufficient to protect the borders. In the Polish reality, this responsibility is entrusted, to varying degrees, to several institutions performing tasks in different areas of state activity.

Security efforts must be comprehensive and interdisciplinary. According to Andrzej Czop, the determinants that cause a particular threat to the state border are: (…) *terrorism, especially Islamic terrorism, uncontrolled migration flows, organised crime, sanitary and epidemiological contamination. The need to protect the border against organised smuggling, especially of: narcotics and psychotropic drugs, radioactive*

[8] P. Kuzior, *Transgraniczna przestępczość zorganizowana – asymetryczne zagrożenie* (Eng. Cross-border organised crime – an asymmetric threat), "Prawo Europejskie w Praktyce" 2008, no. 12(54), pp. 29–30.

[9] P. Lubiewski, *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa* (Eng. Borders of the Republic of Poland as a challenge to state security), "Przegląd Policyjny" 2019, special issue, p. 66. https://doi.org/10.5604/01.3001.0013.6700.

materials, hazardous waste, weapons, ammunition and other means of warfare, stolen cars, alcohol, cigarettes and works of art, was also pointed out[10].

The Schengen area – a European area without internal borders

Rules in force in the Schengen area since 1995[11]:

> (…) abolish internal border controls, while harmonising and reinforcing protection of the area's external borders. Once inside the Schengen area, people can travel from one country to another without being subjected to border checks. However, national authorities may check people at or close to internal borders if police information and experience warrant stepping up surveillance temporarily. Schengen also includes a common visa policy for short stays by non-EU citizens and helps participating countries to join forces in the fight against crime with the aid of police and judicial cooperation[12].

The Schengen Information System is being improved with a view to providing Europeans with greater security. The Schengen area is one of the pillars of European integration. Free movement gives EU residents the right to live, study, work and receive benefits (medical, pensions) throughout the community. All associated countries in the Union belong to the Schengen area, except Ireland, which maintains its opt-out clause, and Cyprus, which plans to join the Schengen area. EU countries have agreed to abolish border controls at air and sea borders for people travelling to and from Bulgaria and Romania from 31 March 2024[13]. In addition, four non-EU countries are part of the Schengen area: Iceland, Norway, Switzerland and Liechtenstein (Figure 1).

According to statistics, the EU's external borders were crossed illegally 1.83 million times in 2015. It was possible to reduce this number to 355 300 times

[10] A. Czop, *Służby specjalne w systemie ochrony granic Rzeczypospolitej Polskiej* (Eng. Special services in the border protection system of the Republic of Poland), "Przegląd Policyjny" 2019, special issue, p. 129. https://doi.org/10.5604/01.3001.0013.6698.

[11] *Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders.*

[12] *Schengen: a guide to the European border-free zone*, European Parliament, 17 VI 2019, https://www.europarl.europa.eu/topics/en/article/20190612STO54307/schengen-a-guide-to-the-european-border-free-zone [accessed: 13 VI 2025].

[13] *Schengen: what issues affect the border-free zone?*, European Parliament, 29 V 2018, https://www.europarl.europa.eu/topics/en/article/20180525STO04311/schengen-what-issues-affect-the-border-free-zone [accessed: 11 XII 2024].

in 2023[14]. Still, managing migration and external border security is a challenge for Europe.

Figure 1. Schengen States

Source: *Schengen: a guide to the European border-free zone*, European Parliament, 17 VI 2019, https://www.europarl.europa.eu/topics/en/article/20190612STO54307/schengen-a-guide-to-the-european-border-free-zone [accessed: 13 VI 2025].

The action taken by the EP contributes to strengthening the common asylum policy, develops legal migration in line with the needs of Member States, promotes the integration of third-country nationals and stops illegal migration. The Internal Security Fund aims to combat cross-border threats such as terrorism, organised crime and cybercrime. These challenges have triggered significant developments

[14] *Irregular border crossings into EU so far this year highest since 2016*, Frontex, 11 XII 2023, https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-so-far-this-year-highest-since-2016-hZ9xWZ [accessed: 11 XII 2024].

in the creation of tools and agencies such as the Schengen Information System, the Visa Information System, the European Border and Coast Guard Agency (Frontex) and the Entry Exit System (EES)[15] at the external borders of the Schengen area. Their role is to detect criminals, terrorists or other persons posing a threat. Travellers not requiring a visa will in future be screened before arrival in the EU using the European Travel Information and Authorisation System (ETIAS)[16], which will become operational in the last quarter of 2026[17].

In the Schengen area, road transport, especially car transport, is the most common mode of transport. This is due to the ease of movement without border controls, which is particularly beneficial for freight and passenger transport.

Schengen area - border control

According to the information provided on EP websites: *The increased influx of third-country nationals into the Schengen area, which is expected to increase even further in the future (by 2025, around 300 million third-country nationals will have legally crossed into the Schengen area for a short-term visit), and concerns about the security of the EU's external borders have led to the need for new rules on the management of the Schengen area's external borders*[18]. According to the EC data:

> (…) more than 1.25 billion journeys are made within the Schengen area every year. Internal border controls have been abolished within the Schengen Area, but states have retained the right to reinstate temporary controls in case of serious threats to public policy or internal security. Since 2015, in the wake of the migration crisis, as well as the increase of cross-border terrorist threats, a number of Schengen states reintroduced such controls (…). The Covid-19 pandemic also pushed many EU countries to reintroduce border controls in an attempt to contain the spread of the virus. In December 2021, the European Commission proposed an update of the rules governing the Schengen area, aiming to ensure that reintroducing internal border controls remains a measure of last resort and promote the use of alternative measures instead such as targeted police checks and enhanced police cooperation. MEPs have

[15] The EES system will start operating on 12 X 2025. See: *Entry/Exit System (EES)*, https://travel-europe.europa.eu/en/ees [accessed: 11 XII 2024].

[16] *Zarządzanie granicami zewnętrznymi* (Eng. Management of external borders), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/zarzadzanie-granicami-zewnetrznymi#:~:text=SIS%20%E2%80%93%20System%20Informacyjny [accessed: 11 XII 2024].

[17] *ETIAS*, https://travel-europe.europa.eu/en/etias [accessed: 11 IV 2025].

[18] *EU entry/exit system: a modern solution for secure borders*, European Parliament, 25 X 2017, https://www.europarl.europa.eu/topics/en/article/20171023STO86604/eu-entry-exit-system-a-modern-solution-for-secure-borders [accessed: 11 XII 2024].

on several occasions argued against the frequent reintroduction of controls, which hampers the free movement of people across the EU[19].

In April 2024, the European Parliament approved an update of the Schengen rules. Time limits for internal border controls were established. The EU Council approved the update in May 2024. The Schengen Borders Code gives Member States the possibility to temporarily reintroduce border control at internal borders in the event of a serious threat to public order or internal security. They may exercise this right as a last resort, in exceptional situations, and this must respect the principle of proportionality[20].

In February 2024, Parliament's Committee on Civil Liberties, Justice and Home Affairs approved an agreement reached with national governments modifying the rules on the control of persons at the EU's external borders[21]. *The rules apply when travellers who do not fulfil the entry conditions of an EU country are apprehended crossing a border point irregularly, are rescued at sea, or who apply for international protection at an external border crossing point*[22]. Checks may be carried out on persons found within the EU who have evaded border control and do not have the appropriate authorisation. Checks are to include: (…) *identification, fingerprinting, security checks, and preliminary health and vulnerability assessment*[23]. According to the regulations, this procedure should take up to seven days. A system for monitoring activities in this regard is in place: (…) *in each EU country to protect fundamental rights of people undergoing screening*[24]. In turn: (…) *as an alternative to internal border controls, the new rules for a more resilient Schengen area promote police cooperation in border regions to address unauthorised movements within the Schengen area. Apprehended non-EU citizens with irregular status often arrive from another EU country so if the two countries hold joint patrols, the irregular*

[19] *Schengen: enlargement of Europe's border-free area*, European Parliament, 23 II 2018, https://www.europarl.europa.eu/topics/en/article/20180216STO98008/schengen-enlargement-of-europe-s-border-free-area [accessed: 11 XII 2024].

[20] *Countering irregular migration: better EU border management*, European Parliament, 30 VI 2017, https://www.europarl.europa.eu/topics/en/article/20170627STO78419/countering-irregular-migration-better-eu-border-management [accessed: 13 XII 2024].

[21] *Asylum and migration: Civil Liberties committee endorses a new legal framework*, European Parliament, 14 II 2024, https://www.europarl.europa.eu/news/en/press-room/20240212IPR17628/asylum-and-migration-civil-liberties-committee-endorses-the-agreements [accessed: 13 XII 2024].

[22] *Countering irregular migration: better EU border management*…

[23] Ibid.

[24] Ibid.

migrants may be transferred back to the first EU country[25]. The European Parliament wants to exclude several categories of people, including minors.

The state of security in Poland in 2019-2020

According to the data published by the Police for 2020[26], 786 302 crimes were committed in Poland, i.e. 36 475 less than in 2019, and their detection rate increased and amounted to 73.9%[27]. In 2020, 9121 cars were stolen, i.e. 3% more compared to 2019 (8856 cars), and the detection rate for this type of crime increased by 1.9%. In 2020, there were 656 homicides in Poland, up to 125 more than in 2019. In addition, 199 020 economic crimes were recorded – 9427 more than in 2019. In the same year, police officers secured criminals' property worth a total of PLN 867 049 023, and in 2020, property worth PLN 930 118 572. Officers of the Central Bureau of Police Investigation (CBŚP), whose main tasks are to identify and neutralise criminal groups, often in cooperation with Polish and foreign institutions, collected trial material and presented charges against more than 3200 people (in 2019 – almost 3800). In 2019, 1836 suspects were charged with leading or participating in an organised criminal group (in 2020 – over 2000). It has also been possible to dismantle the financial background of criminal groups and secure the assets of suspects for future penalties. In 2020, property in the amount of over PLN 700 million was secured and over 10 t of drugs were prevented from reaching the black market, of which over 4 t were seized outside Poland. Narcotic and psychotropic drugs were also secured, as well as large quantities of precursors, which stopped the production of further drugs. In addition, 31 synthetic drug laboratories and 75 cannabis plantations were closed down.

Efforts to combat tobacco crime were also carried out in 2020. Twenty cigarette factories were dismantled (the same number as in 2019). More than 190 million cigarettes (approx. 212 million cigarettes in 2019) and more than 306 t of tobacco (more than 324 t in 2019) were secured. In addition, the services of EU countries, thanks to information provided by CBŚP officers, identified the activities of criminal groups on their territory. Four operating cigarette factories were dismantled and approximately 48 million cigarettes and over 123 t of tobacco cut

[25] Ibid.

[26] The last safety information published by the Police is from early 2021.

[27] All data in *The state of security in Poland in 2019-2020* section of the article is taken from: *Podsumowujemy 2020 rok w Policji* (Eng. We recap 2020 in the Police), https://statystyka.policja.pl/st/raporty/roczne-raporty-statyst/226911,Podsumowujemy-2020-rok-w-Policji.html [accessed: 10 XII 2024].

were secured. Significantly: (…) *the results achieved by the CBŚP and the operations carried out were also possible thanks to cooperation with the Public Prosecutor's Office, police officers of Provincial Police Headquarters, Border Guard, Central Anticorruption Bureau, Internal Security Agency, National Revenue Administration, Chief Sanitary Inspectorate, General Inspector of Financial Information and other Polish institutions*[28]. In addition, CBŚP officers, often with the support of Europol and Eurojust, cooperated with the services and institutions of many countries. The criminal activities analysed are also related to organised crime, often taking the form of cross-border crime. Criminal groups use means of transport (especially road transport), which allow for efficient movement of persons and goods.

Traffic control and safety

Traffic control is the action taken by law enforcement agencies to ensure road safety. It involves monitoring and enforcing traffic laws, including speed limits, parking bans, driving under the influence of alcohol or drugs, and other laws designed to protect road users. Controls may be routine or result from specific incidents, such as road accidents. In Poland, road traffic controls are performed by: Police[29], Border Guard (SG), Road Transport Inspection and Municipal Police. The officers, on the basis of the regulations in force, have specific powers with respect to road traffic control. The performance of tasks by the aforementioned entities is most often associated with ensuring road traffic safety. Due to the changing geopolitical situation in the world and the geographical location of Poland, it is necessary to change the approach to road traffic control, inter alia in relation to the developing cross-border crime.

An increasing number of unaccompanied migrant minors are reported. There are six guarded centres for foreigners (SOCs) in Poland, with a total of 962 places. In 2023, 1903 foreigners were admitted to them, including 32 unaccompanied minors. Due to the large number of unaccompanied minors who have arrived in Poland since the beginning of April 2024, the care facilities are overcrowded. The minors remain in SOCs and SG facilities because there is nowhere to direct them[30].

---

[28] Ibid.

[29] Ł. Foryś, *Zapewnienie bezpieczeństwa w związku z kontrolą ruchu drogowego* (Eng. Ensuring safety in connection with traffic control), in: *Bezpieczeństwo w perspektywie transdyscyplinarnej*, A.W. Filipek (ed.), Siedlce 2022, pp. 88–102.

[30] A. Rodowicz, *Nieletni migranci. Gdy nie uda się ich wypchnąć za druty, trafiają w tryby niewydolnego systemu* (Eng. Juvenile migrants. When they fail to be pushed back behind the wire, they end up in the cogs of an inefficient system), OKO.press, 3 VIII 2024, https://oko.press/maloletni-migranci-polska-granica-ani-prawa-ani-opieki [accessed: 18 XII 2024].

According to the Border Guard Headquarters spokesperson, in the first half of 2024, the Border Guard detained 243 minors (56 girls and 187 boys) who had illegally crossed the Polish border[31]. After apprehending a minor who has illegally crossed the border and is unaccompanied, the Border Guard must apply to the court for placement of the minor in a care facility or a SOC[32]. Agnieszka Matejczuk, a lawyer from the Association for Legal Intervention, points out that: (…) *when a detained minor is under 15 years of age, he must be taken to an intervention facility. If they are over 15 years of age but make a request for protection, they should also be referred to such a facility. Those between 15 and 18 years of age can be placed in a SOC for the duration of the so-called return procedure, i.e. aiming at deportation*[33].

Undoubtedly, the issue of underage irregular migrants requires separate regulations, providing them with adequate care and protection, while at the same time complying with current border control standards.

The introduction of internal border controls will be possible in accordance with the Schengen Borders Code – in justified cases involving, for example, an identified and imminent threat of terrorism, initially for a period of up to 6 months, extendable to 18 months, and in exceptional cases even longer with the consent of the EU Council. If the threat persists, a decision of the EU Council will be able to authorise further border controls, especially when this involves a serious threat to several countries at the same time[34]. It is also worth mentioning that in Poland there has been for many years close cooperation between national border, police and judicial services and their counterparts in the Member States, which helps to maintain public safety and order.

Road traffic controls are important in the fight against cross-border crime for several reasons. They can help detect the illegal transport of goods such as drugs, weapons or excisable goods. Police officers on duty on the road can cooperate with police officers from other countries and with the Border Guard or the Customs and Tax Service to combat smuggling more effectively. If, during a roadside check, officers come across persons who have crossed the border illegally, then cooperation with border control authorities is crucial. Very often cross-border crime is of an organised nature. Roadside checks can help identify and apprehend criminal groups that use transport networks to carry out their activities.

---

31 Ibid.

32 *Act of 12 December 2013 on foreigners*.

33 A. Rodowicz, *Nieletni migranci*…

34 *Countering irregular migration: better EU border management*…

Summary

Both traffic control and the fight against cross-border crime are complex processes undertaken by numerous actors, including international cooperation. The geopolitical changes taking place in the modern world pose a major challenge for entities responsible for ensuring safety. The traffic control measures taken focus primarily on improving safety by reducing the number of people injured and killed in road accidents.

Armed conflicts or humanitarian crises can lead to increased migratory movements. This can cause an increase in the number of vehicles on the roads and require more effective traffic control and management. In response to new threats, countries may introduce changes to traffic legislation, which may affect international cooperation and procedures in place.

In the Schengen area, internal border controls have been abolished, requiring more efficient management of external borders. This implies advanced tools, information systems and better coordination between countries. New technologies, such as traffic monitoring systems, number plate recognition systems or drones can contribute to better traffic management on roads and border monitoring, more efficient detection of offenders, more effective search for people and countering threats such as terrorist attacks. However, their implementation requires investment and training of personnel, as well as appropriate regulations and procedures.

Traffic controls at borders and strategic points can effectively hinder the smuggling of persons and illegal goods, which is one of the main elements of cross-border crime. Joint operations and the exchange of information between countries can increase the effectiveness of road checks and thus the fight against crime, as they hit organised crime groups. Another important element is the noticeable presence of control services on the roads, which can act as a deterrent to potential criminals and reduce the undertaking of illegal activities such as smuggling.

Geopolitical changes pose many challenges to states, including the need to introduce innovative solutions to improve road safety, both in road traffic and in other areas. At the same time, it should be remembered that cross-border crime is a complex phenomenon that requires cooperation, including international cooperation, and effective tools to combat it. Road traffic control can be considered one of them. A broader view of the activities undertaken by officers with respect to road traffic participants, provides an opportunity to create more effective tools to improve road safety, ensure public safety and order, and thus prevent and combat crime, including cross-border crime. The authors identified factors determining the road traffic control procedure and the cross-border crime facilitated by free movement in the Schengen area. Attention should be drawn to the systemic nature

of the issue in question, which requires coordinated action by various institutions. The considerations made in the article provide a starting point for deeper insight and indicate the need for an interdisciplinary approach to research related to this issues.

Bibliography

Czop A., *Służby specjalne w systemie ochrony granic Rzeczypospolitej Polskiej* (Eng. Special services in the border protection system of the Republic of Poland), "Przegląd Policyjny" 2019, special issue, pp. 98–130. https://doi.org/10.5604/01.3001.0013.6698.

Foryś Ł., *Zapewnienie bezpieczeństwa w związku z kontrolą ruchu drogowego* (Eng. Ensuring safety in connection with traffic control), in: *Bezpieczeństwo w perspektywie transdyscyplinarnej*, A.W. Filipek (ed.), Siedlce 2022, pp. 88–102.

Foryś Ł., Gwardyński R., Żuber M., *Wybrane aspekty bezpieczeństwa dotyczące mobilności człowieka* (Eng. Selected safety aspects of human mobility), Szczytno 2024.

Kozłowski P., *Przestępczość transgraniczna w latach 2015–2017 zagrożeniem dla bezpieczeństwa wewnętrznego państwa w świetle danych statystycznych Bieszczadzkiego Oddziału Straży Granicznej w Przemyślu* (Eng. Cross-border crime in 2015–2017 as a threat to the state's internal security in the light of statistical data from the Bieszczady Border Guard Unit in Przemyśl), "Współczesne Problemy Zarządzania" 2020, vol. 8, no. 1(16), pp. 83–95. https://doi.org/10.52934/wpz.86.

Kuzior P., *Transgraniczna przestępczość zorganizowana – asymetryczne zagrożenie* (Eng. Cross-border organised crime – an asymmetric threat), "Prawo Europejskie w Praktyce" 2008, no. 12(54).

Lubiewski P., *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa* (Eng. Borders of the Republic of Poland as a challenge to state security), "Przegląd Policyjny" 2019, special issue, pp. 49–66. https://doi.org/10.5604/01.3001.0013.6700.

Internet sources

Asylum and migration: Civil Liberties committee endorses a new legal framework, European Parliament, 14 II 2024, https://www.europarl.europa.eu/news/en/press-room/20240212IPR17628/asylum-and-migration-civil-liberties-committee-endorses-the--agreements [accessed: 13 XII 2024].

Countering irregular migration: better EU border management, European Parliament, 30 VI 2017, https://www.europarl.europa.eu/topics/en/article/20170627STO78419/countering-irregular-migration-better-eu-border-management [accessed: 13 XII 2024].

Entry/Exit System (EES), https://travel-europe.europa.eu/en/ees [accessed: 11 XII 2024].

ETIAS, https://travel-europe.europa.eu/en/etias [accessed: 11 IV 2025].

EU entry/exit system: a modern solution for secure borders, European Parliament, 25 X 2017, https://www.europarl.europa.eu/topics/en/article/20171023STO86604/eu-entry-exit-system-a-modern-solution-for-secure-borders [accessed: 11 XII 2024].

Irregular border crossings into EU so far this year highest since 2016, Frontex, 11 XII 2023, https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-so-far-this-year-highest-since-2016-hZ9xWZ [accessed: 11 XII 2024].

Podsumowujemy 2020 rok w Policji (Eng. We recap 2020 in the Police), https://statystyka.policja.pl/st/raporty/roczne-raporty-statyst/226911,Podsumowujemy-2020-rok-w-Policji.html [accessed: 10 XII 2024].

Rodowicz A., *Nieletni migranci. Gdy nie uda się ich wypchnąć za druty, trafiają w tryby niewydolnego systemu* (Eng. Juvenile migrants. When they fail to be pushed back behind the wire, they end up in the cogs of an inefficient system), OKO.press, 3 VIII 2024, https://oko.press/maloletni-migranci-polska-granica-ani-prawa-ani-opieki [accessed: 18 XII 2024].

Safe, sustainable and connected transport, European Union, https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_en [accessed: 10 XII 2024].

Schengen: a guide to the European border-free zone, European Parliament, 17 VI 2019, https://www.europarl.europa.eu/topics/en/article/20190612STO54307/schengen-a-guide-to-the-european-border-free-zone [accessed: 13 VI 2025].

Schengen: enlargement of Europe's border-free area, European Parliament, 23 II 2018, https://www.europarl.europa.eu/topics/en/article/20180216STO98008/schengen-enlargement-of-europe-s-border-free-area [accessed: 11 XII 2024].

Schengen: what issues affect the border-free zone?, European Parliament, 29 V 2018, https://www.europarl.europa.eu/topics/en/article/20180525STO04311/schengen-what-issues-affect-the-border-free-zone [accessed: 11 XII 2024].

Statistics Explained, Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=456757 [accessed: 10 XII 2024].

Zarządzanie granicami zewnętrznymi (Eng. Management of external borders), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/zarzadzanie-granicami-zewnetrznymi#:~:text=SIS%20%E2%80%93%20System%20Informacyjny [accessed: 11 XII 2024].

Legal acts

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Official Journal of the EU L 77/1 of 23 March 2016).

Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union (Official Journal of the EU L 127/39 of 29 IV 2014).

Act of 12 December 2013 on foreigners (consolidated text, Journal of Laws 2024, item 769, as amended).

Łukasz Foryś, PhD

Doctor of social sciences in the discipline of security sciences. His academic activity focuses on the issues of internal security with particular emphasis on public safety and order, transport and road safety. Author of scientific papers on these issues. Co-organiser and participant of national and international scientific conferences.

Contact: l.forys@apol.edu.pl

Kornelia Stępień, PhD

Doctor of law in the field of law, criminology, assistant professor at the Institute of Legal Sciences of the Faculty of Security and Legal Sciences of the Police Academy in Szczytno. Author of scientific articles published in specialist press and collective works related to criminology, juvenile crime and victimology. The author's scientific and research interests focus on the issues of social pathologies, as well as determinants of demoralisation and juvenile delinquency and the prevention of these phenomena. She is also interested in the phenomenology of contemporary negative social phenomena, issues of social exclusion and resocialisation.

Contact: k.stepien@apol.edu.pl

Internal Security Review
2025, no. 32, pp. 301–332

https://doi.org/10.4467/20801335PBW.25.015.22181

ARTICLE

Russian 'special military operation' as a failed coup de main. An intelligence analysis perspective

MAREK KLASA

War Studies University

https://orcid.org/0000-0003-0863-5601

MICHAŁ KLASA

Independent author

https://orcid.org/0009-0001-1412-0383

Abstract

The authors analyse the invasions and accompanying intelligence activities as *coup de main* operations, understood not as strict execution of the art of war, but rather as a *coup d'état* carried out by external forces on the territory of the attacked state. *Coup de main* as an effective surprise attack requires the use of offensive counterintelligence infiltration and the pacification of the opponent with police-type forces. In the article, these mechanisms are analysed using the example of Soviet actions in countries perceived by Moscow as its sphere of influence, the annexation of Crimea by the Russian Federation in 2014 and the Russian invasion of Ukraine in 2022 historical experience from the Russian invasion of Ukraine in 2022 which the authors compare to the invasion of Czechoslovakia by Warsaw Pact troops in 1968. Understanding this model of aggression requires presenting instruments for analysing how the authoritarian state operates.

Keywords

coup de main, *coup d'état*, Ukraine, infiltration, intelligence analysis, situational logic

Introduction

The subject of the research described in this article is a specific type of actions directed against state authorities and their coercive apparatus, defined by the term *coup de main* (English: blow with a hand). This concept, taken from English-language literature, primarily from the thought of Edward Luttwak, will be described in more detail later in the text.

The aim of this article is to analyse the Russian Federation's (RF) actions in its two acts of aggression against Ukraine: in 2014 and 2022, as *coup de main* operations according to the operational definition adopted. The realisation of the research objective can contribute both to the awareness of the threat of this type of actions and increase resilience to them.

The authors made the following research assumptions: total institutions[1], which can include both the armed forces and the administrative apparatus in authoritarian states, have a hidden agenda, referred to in sociology as the second life of the total institution[2]. Applying this concept to the operational practice of authoritarian states, one can see significant discrepancies between the formal doctrine of the use of armed forces and their actual use. This is discernible in the activities of the Soviet Army, including interventions in countries that were formal allies of the USSR, counter-guerrilla and expeditionary activities[3]. The Russian Federation has taken over this legacy, and its military actions (in Chechnya in 1994–1996 and 1999–2000, in Georgia in 2008, in Syria in 2015–2024[4] and in Ukraine since 2014) have been far from the assumptions of war between state actors similar in capability. From this follows the second assumption made by the authors – the experience of the use of military force in post-World War II operations that influenced the functioning of the Russian Armed Forces in peacetime (time 'P') and their modus operandi during the invasion of Ukraine in 2022.

---

1 According to Erving Goffmann: "A 'total institution' is a place of residence and work where a large number of like-situated individuals, cut off from the wider society for an appreciable period of time, together lead an enclosed, formally administered round of life". Quoted after: *The Characteristics of Total Institutions*, in: *A Sociological Reader on Complex Organizations*, A. Etzioni (sci. ed.), New York 1961, p. xiii.

2 Ibid., pp. 312–338.

3 Cf. В. Триандафиллов, *Характер операций современных армий*, Москва 1929 (V. Triandafillov, *Kharakter operatsiy soveremennykh armiy*, Moskva 1929); H. Hermann, *Operacyjny wymiar walki zbrojnej* (Eng. Operational dimention of armed struggle), Toruń 2004, pp. 129–131; M. Depczyński, L. Elak, *Rosyjska sztuka operacyjna w zarysie* (Eng. Russian operational art in outline), Warszawa 2020, pp. 233–244, 282–294.

4 The Russian intervention in Syria continued even after the full-scale war with Ukraine had begun.

The research limitation adopted is the narrowing of the research base to a case study of two Russian operations against Ukraine – the annexation of Crimea in 2014 and a full-scale invasion in early 2022, as well as the juxtaposition of the latter with the assumptions of the Warsaw Pact military intervention in Czechoslovakia in 1968 analysed on the basis of documentation of the operation "Danube".

An extensive study of the 1968 intervention in Czechoslovakia, both in terms of the use of force itself and the impact on other countries, primarily the so-called Eastern Bloc, was carried out by: Kent DeBenedictis, Jacques Rupnik, Alexander Stykalin, Slavomír Michálek, Ljubodrag Dimić, Miklós Mitrovits, Mirosław Szumiło, Mihail Gruev, Michal Štefanský and Jakub Drábik as well as Kieran Williams. Important contributions to the examined issues were made by Alex Hughes, Marek Świerczek and Edward Luttwak[5].

The authors of the article used qualitative, heuristic and theoretical research, which they supplemented with structured analytical techniques according to classification of Randolph H. Pherson and Richards J. Heuer.

Coup de main – operational definition

The term *coup de main* is used to describe the use of armed force by an aggressor[6] who, wishing to effect a change of political power[7] in an attacked state[8], enters its territory

[5] See in detail: K. DeBenedictis, *Russian "Hybrid Warfare" and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*, London 2022; *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (ed.), Stuttgart 2021 (the authors of the chapters: J. Rupnik, A. Stykalin, S. Michálek, L. Dimić, M. Mitrovits, M. Szumiło, M. Gruev, M. Štefanský, J. Drábik); K. Williams, *The Prague Spring and its aftermath: Czechoslovak Politics, 1968–1970*, Cambridge 1997, pp. 112–143; A. Hughes, *Plan Z. Reassessing Security-Based Accounts of Russia's Invasion of Ukraine*, "Journal of Advanced Military Studies" 2023, vol. 14, no. 2, pp. 174–208. https://doi.org/10.21140/mcuj.20231402009; M. Świerczek, *Yezhov's infiltration model and the Russian Federation's seizure of Crimea*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, pp. 385–411. https://doi.org/10.4467/20801335PBW.24.016.19618; M. Świerczek, *2014 takeover of the SBU headquarters in Lugansk as an example of the operation of the Russian special services*, "Przegląd Bezpieczeństwa Wewnętrznego" 2023, no. 28, pp. 278–312. https://doi.org/10.4467/20801335PBW.23.012.17662; E.N. Luttwak, *Zamach stanu. Podręcznik* (Eng. Coup d'état. A practical handbook), Warszawa 2017.

[6] The aggressor can be both a state and a non-state actor.

[7] This change can be carried out while maintaining the formal independence of the attacked state, e.g. by staffing the puppet government controlled by the aggressor.

[8] In all the cases studied by the authors, the *coup de main* was carried out against state authorities, which, however, does not constitute *per se* evidence that it can only be referred to state actors. The authors want to emphasise this because of the popular argumentation between 2001 and 2022 regarding the "uniqueness" (non-state actors were supposed to be an exception to the rules of strategy) of state

with his forces (troops), usually in a marching formation. He assumes that, thanks to the shock effect induced, he will not encounter effective resistance. The preferred form of overpowering the opponent is the psychological impact – as a result of this, the victim of aggression will not put up (armed) fight and thus will not become a defender[9]. Firebombing is used tactically when the victim of the aggression resists (becoming a defender) or to enhance the shock effect on a non-resisting victim (e.g. bombing of non-resisting military installations or terrorist bombing of civilians). The logic of the use of force in such actions differs from that used in open armed conflict, where the potentials of the parties are similar (near-peer conflict).

Four detailed hypotheses were formulated for the study described in this article:

1. The actions defined by the operational definition of *coup de main* have a strategy of their own, different from the classical logic of armed conflict and similar to the logic of *coup d'état*. Theoretical methods were adopted as a means of verifying this hypothesis, including the development of an operational definition of *coup de main* and its application to selected cases included in the research base.
2. The decision to carry out a "special military operation" as a *coup de main* should not be explained solely as a mistake by a rational actor or a psychological portrait of a leader, but rather as a modelling of the organisation's behaviour projecting into the planning process.

actors and the inapplicability of the knowledge concerning them (especially the oeuvre of the strategy classics) to non-state actors. Cf. the words of Christopher Bassford: "[…] in a dazzling display of historical forgetfulness […] our national security community appears to be stunned to discover that warfare can be waged by groups other than Weberian states. […] Prompted by what evidently appears to many writers to be the utterly new kind of warfare waged by organizations like, say, Al Qaeda, they spin out bold new buzzwords designed, shaman-style, to capture the spirit of this earthshakingly new innovation by giving it a name. Some popular examples are "non-state war" and "Fourth- (or Fifth-) Generation War" […] or […] "the New Warfare" […] Possibly the most misleading (to the few who are equipped to assign any meaning whatsoever to the phrase) is "non-trinitarian war" a term coined by […] Martin van Creveld to encapsulate a new, allegedly "non-Clausewitzian" approach to theorizing about war". See: Ch. Bassford, *Na palcach wokół trójcy Clausewitza* (Eng. On a tiptoe around Clausewitz's Trinity), "Kwartalnik Bellona" 2017, vol. 688, no. 1, p. 73.

[9] Cf. the words of Clausewitz: "War actually takes place more for the defensive than for the conqueror, for invasion only calls forth resistance, and it is not until there is resistance that there is war. A conqueror is always a lover of peace (as Buonaparte always asserted of himself); he would like to make his entry into our state unopposed; in order to prevent this, we must choose war, and therefore also make preparations, that is in other words, it is just the weak, or that side which must defend itself, which should be always armed in order not to be taken by surprise". See: C. von Clausewitz, *On war* (The quotation was excerpted from the original available on the website: https://ebook-mecca.com/online/On%20War%20-%20Carl%20von%20Clausewitz.pdf).

Structured analytical techniques were used to verify this hypothesis (Table 1). The results of each method are presented in Tables 3 and 4.

3. The seizure of Crimea and the first phase of the Russian invasion of Ukraine in the Kyiv, Kharkiv and Kherson directions were *coup de main* operations, similar in their objectives to the 1968 intervention in Czechoslovakia. Historical analogies, inference and abstracting were used to verify it, the results of which are included in Table 5.
4. A prerequisite for a successful *coup de main* operation is intelligence infiltration. Its scale determined the success of the operation in 2014 and its failure in 2022. The same methods were used to verify it as for the third hypothesis.

Coup de main as a practice of the Russian Federation

The analysis of the circumstances, objectives and consequences of *coup de main* operations requires an appropriate methodology. Research based on the two models considered: political-military decision-making and the functioning of an authoritarian state such as the RF, uses cause and effect relationships analysis[10]. The article takes as its starting point the structured analytical techniques according to Pherson and Heuer's classification, described in Table 1, together with their application.

Table 1. Structured analytical techniques determining cause and effect relationships and application of these techniques in the article.

Name of analytical technique	Description	Application in the article
Situation logic *Red Hat*	The expert opinion to adopt the reasoning of the entity under investigation	Elements of the *Red Hat* methodology underpin the analysis. For the purposes of the article, the opinions of: • Hieronim Grala and Witold Jurasz[11],

[10] R.H. Pherson, R.J. Heuer, *Structured Analytic Techniques for Intelligence Analysis*, [n.p.] 2020, pp. 361–387.

[11] Hieronim Grala and Witold Jurasz were selected for *Red Hat* analysis as Polish, expert sources with practical experience in diplomacy on Russian territory.The following interviews were analysed: *Czy Jurij Andropow był twórcą pierestrojki?* (Eng. Was Yuri Andropov the founder of perestroika?) – *Oblicza historii series*, YouTube, 14 V 2024, https://www.youtube.com/watch?v=vbbcuNYaxkU [accessed: 30 VI 2024]; *ROSYJSKI KRĄG WŁADZY* (Eng. Russian power circle) – *Kulisy historii series Episode. 120*, YouTube, 1 VII 2023, https://www.youtube.com/watch?v=szr-pwtxV0U [accessed: 30 VI 2024]; *Rosja Putina – obsesja neoimperialnej potęgi* (Eng. Putin's Russia – obsession of neo-imperial power) |

Name of analytical technique	Description	Application in the article
Situation logic *Red Hat*	The expert opinion to adopt the reasoning of the entity under investigation	• Andrij Kharuk and Mikhail Zhirokhov[12], • Kamil Galeev[13], • William Spaniel[14] and Mark Galeotti[15]

Czwartki w DeBeKa #1, YouTube, 29 II 2024, https://www.youtube.com/watch?v=rUAgEnRAllw [accessed: 30 VI 2024]; *Nie będzie końca wojny bez końca Putina: prof. Hieronim Grala* (Eng. There will be no end to war without an end to Putin: prof. Hieronim Grala) – didaskalia, YouTube, 16 IV 2023, https://www.youtube.com/watch?v=uTlrecy9m80 [accessed: 30 VI 2024]; *Debata "Co dalej z Rosją?" – Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J.M. Nowakowski* (Eng. The debate "What next for Russia?" – Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J.M. Nowakowski), YouTube, 4 XII 2023, https://www.youtube.com/watch?v=Gk45gw7ECHY [accessed: 30 VI 2024]; *Elity Zachodu tęsknią za przewidywalną Rosją* (Eng. Western elites yearn for a predictable Russia) | *Prof. Hieronim Grala*, YouTube, 10 VI 2023, https://www.youtube.com/watch?v=KaU41GKpNmY [accessed: 30 VI 2024].

[12] Andriy Kharuk and Mikhail Zhirokhov were chosen for *Red Hat's* analysis as Ukrainian, expert sources with access to a considerable amount of information from soldiers involved in the fighting relatively recently. Sources used for the *Red Hat* analysis: А. Харук, М. Жирохов, *Бойова хроніка 2022 року*, Київ 2024 (A. Kharuk, M. Zhirokhov, *Boyova khronika 2022 roku*, Kiiv 2024), pp. 49–203; М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (M. Zhirokhov, *Nevidbutiy blitskrig: oborona ayerodromiv Gostomelyu ta Vasil'kova, lyutiy 2022 roku*, Chernigiv 2022), pp. 4–69; idem, *Війна танків. Україна, лютий-серпень 2022*, Чернігів 2023 (M. Zhirokhov, *Viyna tankiv. Ukraïna, lyutiy-serpen' 2022*, Chernigiv 2023), pp. 4–88.

[13] Kamil Galeev was identified for *Red Hat* analysis as an anti-government (opposition) Russian source whose credibility is difficult to assess, but is often corroborated by other sources analysed. Galeev should be characterised more as a writer of OSINT reports than as a scientist, but his observations are a valuable addition to attempts to understand the situational logic in the case at hand. See: K. Galeev (@kamilkazani), entry on the portal X, 28 II 2022, https://x.com/kamilkazani/status/1498377757536968711?lang=en [accessed: 30 IX 2024]. Other oppositional Russian sources, such as Maxim Katz and Mikhail Zygar, were not adopted to develop situational logic theses within *Red Hat* technique.

[14] William Spaniel was chosen as an English-speaking expert for the *Red Hat* analysis. He is Associate Professor of the University of Pittsburgh specialising in game theory and its application to strategy and policy analysis. Sources used for the *Red Hat* analysis: W. Spaniel, *What Caused the Russia-Ukraine War (And How Will It End?)*, e-book; idem, *How Ukraine Survived: Inside the Strategy to Stop Russia's Invasion*, e-book; idem, *Why Russia Miscalculated Ukraine: A Self-Inflicted Disaster in Three Acts,* YouTube, 24 I 2023, https://www.youtube.com/watch?v=8YkGrKQXZxE [accessed: 25 I 2023]; idem, *The Hidden Battle that Saved Ukraine,* YouTube, 3 I 2023, https://www.youtube.com/watch?v=hh9xT9d6SJU [accessed: 25 I 2023]; idem, *The "Battle" of Crimea: Inside Russia's Playbook to Capture the Peninsula*, YouTube, 15 III 2023, https://www.youtube.com/watch?v=Ijmoz2VfjrQ [accessed: 25 IX 2024].

[15] Mark Galeotti was selected for *Red Hat's* analysis as a second English-speaking expert. He works as a senior researcher and a coordinator in the Centre for European Security, Institute

Name of analytical technique	Description	Application in the article
Situation logic *Red Hat*	The expert opinion to adopt the reasoning of the subject under investigation	are synthesised. The experts were selected on the basis of the methodology defined by Józef Kozłowski[16]
Application of theory	Application of theory and models to clarify the circumstances and conditions under which certain phenomena occur	The article draws on: • Edward Luttwak's model of *coups d'état* concerning the discrepancy between the nominal[17] and actual chain of command, psychological knowledge of the fight-or-flight mechanism or the absence of active resistance, • Graham T. Allison's models of state decision-making[18]
Historical analogies	Attempting to understand the processes taking place through comparison with historical counterparts	The analysis points to similarities with other operations of this type: the invasion of Czechoslovakia by Warsaw Pact troops in 1968, the capture of Crimea in 2014 as a *coup de main* operation and the Russian invasion of Ukraine in 2022

of International Relations Prague. Sources used for the *Red Hat* analysis: M. Galeotti, *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [n.p.] 2023; idem, *Putin's wars. From Chechnya to Ukraine*, Oxford 2022; idem, *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022, https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins-security-council-meeting-a76522 [accessed: 1 IX 2024].

[16] J. Kozłowski, *Practical dimension of issues related to assessing the reliability of sources and the trustworthiness of data and information*, "Przegląd Bezpieczeństwa Wewnętrznego" 2023, no. 29, pp. 323–358. https://doi.org/10.4467/20801335PBW.23.032.18774.

[17] E.N. Luttwak, *Zamach stanu. Podręcznik*…, p. 59.

[18] G. Allison, P. Zelikow, *Essence of Decision. Explaining the Cuban Missile Crisis*, Addison-Wesley Educational Publishers Inc., 1999, pp. 18–25. Other techniques, which will be omitted in the article, can also be used for this type of analysis. They do, however, provide useful instrumentation for more elaborate studies devoted to, for example, the concept of the intelligence dyad or the degrees of military involvement in state policy according to Samuel Edward Finer.

Name of analytical technique	Description	Application in the article
Historical analogies	Attempting to understand the processes taking place through comparison with historical counterparts	In the event of a shortage of information on the Soviets, the authors of this article will reason per analogiam with the structures of the People's Republic of Poland (PRL) or other socialist states during the Cold War period

Source: own elaboration based on: R.H. Pherson, R.J. Heuer, *Structured Analytic Techniques for Intelligence Analysis*, [n.p.] 2020, pp. 361–387.

Within the *Red Hat* method, described in Table 1, three situational logic theses based on expert opinions were formulated.

1. Instead of analysing Russia as a rational actor and psychological analyses of Vladimir Putin as the sole leader, the "collective Putin" should be analysed – organisational and palace models of power structures.
2. Although Russia exposes its armed forces and presents itself primarily as a military power, the army's role in politics is minor. The factor that influences the state (among other things, the thinking of the leaders) is the Federal Security Service (FSB) and it is the most important power ministry.
3. The Russian military acts in practice as a pacification force. Official doctrine does not have much impact in the armed conflicts of the last few decades. The year 2022 was the first time since the end of the World War II that Russian troops had to face a regular army of a well-armed enemy on the battlefield.

The decision-making models described by Graham Allison were then applied to the RF: the state as a rational actor, organisational behaviour and government policy (Table 2).

Table 2. Decision-making models according to Graham Allison in relation to Russian Federation.

Model	Description in the context of Russian Federation
State as Rational Actor Model – in which the behaviour of the state in the international space is compared to the actions of a conscious individual (person)	To this model can be attributed Russia's actions in strict terms of international politics as an entity seeking, among other things: • to subjugate Ukraine as a satellite state, annexing part or all of its territory depending on the outcome of the invasion,

Model	Description in the context of Russian Federation
State as Rational Actor Model – in which the behaviour of the state in the international space is compared to the actions of a conscious individual (person)	• to strengthen its position vis-à-vis the US and NATO by demonstrating its capacity in Eastern Europe, thus increasing the chances of accepting ultimatums towards the Alliance's eastern flank
Organisational Behaviour Model – state actions as a result of structures, procedures and established ways of operating services and institutions	Organisational Behaviour Model may point to several organisational entities inside Russia that influenced the planning and conduct of the war, including: FSB, Main Intelligence Directorate of the General Staff of the Armed Forces of the RF (GRU), Main Operational Directorate of the General Staff of the Armed Forces of the RF, Special Operations Forces Command. In the context of the 2014 annexation of Crimea, a key planning role was played by the Main Operational Directorate, whose head is customarily the first deputy Chief of the General Staff. The authority probably had some of the plans prepared back in the 1990s. Despite occasional disagreements with the Ministry of Defence, the Main Operational Directorate of the Armed Forces of the Russian Federation was tasked with planning the details of the annexation of Crimea, which was successful thanks in part to planning work starting as early as January, even before political decisions were made at the highest level. The FSB and the GRU also played a significant part in the final preparations. In 2011, the Special Operations Forces Command was established to direct special military operations. Its role has grown steadily since the successful annexation of Crimea and intervention in Syria, although its prestige translating into an increased role in the context of the 2022 invasion of Ukraine could be seen as a mistake in the approach to using special forces as selective frontline attack units[19]. As a result of the links to the Governmental Politics Model, the key influence on the decisions taken by the RF considered in the article is primarily the special services with the FSB as the factor with the greatest influence on power, with the role of the armed forces as an effector with limited influence on central decisions. It should be noted that in the Russian intelligence organisation, the FSB is responsible for the post-Soviet area, which shows that the so-called near abroad states are not treated as a "full-fledged foreign country"

[19] A. Liflyandchick, D. Jones, S. Fabian, *The Fall from Grace of Russian SOF: The Danger of Forgetting Lessons Learned*, Irregular Warfare Center: Insights, vol. 1, no. 8, September 2023.

Model	Description in the context of Russian Federation
Governmental Politics Model – palace model, analysing dependencies arising from personality traits and mutual connections, leaders' immediate environment, etc.	According to thesis 1 of situational logic, the decisions of the collective with the greatest influence on state policy should be analysed

Source: own elaboration based on: M. Galeotti, *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [n.p.] 2023, pp. 22–23.

The seizure of Crimea in 2014 as a successful coup de main

The prelude to the invasion of 24 February 2022 was the decision eight years earlier to launch the annexation of Crimea[20] by the Security Council of the Russian Federation (Russian: Совет Безопасности Российской Федерации). Its implementation led to the annexation by the RF of the Autonomous Republic of Crimea – part of Ukraine. The complex nature of this type of operation requires two aspects to be examined: hard power and political. The analysis of the meetings of the Security Council of the RF is significant in that both decisions were adopted at meetings with very similar memberships[21].

The first issue in terms of hard power is the ratio of Ukrainian and Russian forces on the Crimean Peninsula in 2014, which, according to estimates published by Defence Express, were initially evenly matched. Russia had around 18 300 military personnel, including 11 000 Black Sea Fleet sailors, 2000 naval infantry

[20] William Spaniel speculates that the decision may have been taken even earlier. For example, the Russian medal "For the Recapture of Crimea" indicates the time of the operation from 20 II to 18 III. Yet on 20 II there was an incident in Cherkasy, used by Russia for propaganda. See: W. Spaniel, *The "Battle" of Crimea: Inside Russia's Playbook*…

[21] The meeting was attended by: Dmitry Medvedev, Valentina Matviyenko, Sergei Naryshkin, Sergei Ivanov, Nikolai Patrushev, Rashid Nurgaliyev, Sergei Lavrov, Vladimir Kolokoltsev, Sergei Shoigu, Alexander Bortnikov, Mikhail Fradkov and Boris Gryzlov. Unfortunately, the Kremlin has not published a transcript or recording of this meeting, making it impossible to compare the proceedings of the meetings prior to the annexation of Crimea on 27 II 2014 and the full-scale invasion on 24 II 2022, according to open sources. See: *Meeting with permanent members of the Security Council*, Kremlin.ru, 21 II 2014, http://en.kremlin.ru/events/president/news/20301 [accessed: 24 IX 2024]. Galeotti claims that only representatives of the force ministries (so-called siloviki) actually attended this meeting, but only the head of the defence ministry, Shoigu, took a rather cautious stance, for fear of international repercussions. See: M. Galeotti, *Putin's wars. From Chechnya to Ukraine*…, p. 170.

and 5300 Spetsnaz. Another 15 000 troops were waiting at the Kerch Strait from the Krasnodar Krai side[22]. Ukraine was initially to have 14 600 soldiers and sailors[23]. However, the ratio of forces was rapidly changing in favour of Russia, which moved an additional 6000 troops to the Crimea.

The second issue in terms of hard power is the pace at which territory was seized. From 27 February to 4 March, Russia managed to take control of major cities, including the capital of the Autonomous Republic of Crimea – Simferopol, as well as the Perekop Isthmus, which connects the Crimean Peninsula to the rest of Ukraine. The Armed Forces of the RF blocked Ukrainian units in Balaklava, Sevastopol, Belbek, Saki, Eupatoria, Novozerny, Chornomorsk, Theodosia, Kerch, Vesele and Dzhankoi. Russian air operations, including Il-76 transport flights to airfields in Sevastopol and Gvardeysk or helicopter flights in other parts of the peninsula, were in no way disrupted. Russian troops were also carrying out reconnaissance for 3 km beyond the Crimean borders, into the Kherson region.

A peculiarity of the annexation of Crimea was that Russian troops were already present on the peninsula as a result of agreements with Ukraine, and the sites of their permanent dislocation were very close to Ukrainian military infrastructure. Russian units, both those leaving Black Sea Fleet military bases and those dislocated to the peninsula from Russian territory, were able to move quickly around Crimea without having to cross the protected state border.

'Special military operation' – planning considerations, organisational behaviour model

In July 2021, Russia created a cell (based on the 5th FSB Service[24]) responsible for planning the invasion. Its task was to investigate Ukraine's vulnerability to

[22] *Standoff. A chronicle of Russian invasion of Crimea*, Defense Express, 4 III 2014, https://web.archive.org/web/20230226183728/https://issuu.com/ukrainian_defense_review/docs/chronicles-of-russian-aggression-cr [accessed: 13 VII 2025].

[23] A. Wilk, *Russian military intervention in Crimea*, Ośrodek Studiów Wschodnich, 5 III 2014, https://www.osw.waw.pl/en/publikacje/analyses/2014-03-05/russian-military-intervention-crimea [accessed: 29 IX 2024].

[24] The Federal Security Service of the Russian Federation is divided into "services" distinguished by numbers, like the General Staff branches. Number 5 is the Service for Operational Information and International Relations (Russian: *Служба оперативной информации и международных связей*, SOIMS). It is responsible for liaising with foreign services, including the SBU. It should be noted that the head of the 5th Service, Colonel-General Sergey Beseda, in 2003–2004 headed the Directorate for Coordination of Operational Information of Analysis, Forecast and Strategic Planning of the FSB of the RF, a unit conducting intelligence on the territory of the countries of the Commonwealth

intervention, with the attitude of Ukrainian society, as illustrated by opinion polls, taken as its primary determinant. The results of surveys of Ukrainian public opinion, taken into account, indicated low trust in those in power, indifference to the political situation and focus on economic problems, while describing a full-scale military conflict between Russia and Ukraine as unlikely. Analyses indicated that energy, heating and finance were key areas of public concern[25]. In retrospect, it can be seen as an over-interpretation by the Russian side of the results of the opinion polls – drawn up on the basis of the everyday problems discussed in the surveys – which did not take into account the radical mobilisation of society to resist in the face of armed aggression[26]. Meanwhile, it was the issues of the socio-economic crisis in Ukraine, labour emigration and electricity or gas bills, among others, that were an important part of Putin's speech on 21 February 2022[27]. This seems an appropriate clue for further research based on the decision-making models (described in Table 2), given that most studies in this area point to a Russian error in the assessment of the situation only in terms of the FSB overestimating its network of agents on Ukrainian territory[28] or overestimating the capabilities of its own forces and underestimating those of the enemy[29].

---

of Independent States, after years of the absence of a foreign intelligence division in the FSB structure. He was in Kyiv during Euromaidan and, prior to the 2022 invasion, was responsible for both the formation of the fifth column on Ukrainian territory and analytical work on preparations for the invasion. See: A. Soldatov, *The True Role of the FSB in the Ukrainian Crisis*, The Moscow Times, 15 IV 2014, https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985 [accessed: 28 IX 2024]; M. Minkina, *FSB. Gwardia Kremla* (Eng. FSB. Kremlin's guard), Warszawa 2016, p. 93, 175.

[25] M. Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022, p. 7.

[26] If the information provided by the Royal United Services Institute is true, this should be considered a serious error of intelligence analysis. Although it is not possible to categorise it precisely without access to the content of these reports, it can be assumed that this was a form of, for example, evaluation error in the form of a lack of critical evaluation of the selection and assessment of public opinion surveys. Cf. J. Kozłowski, *Metody, techniki i narzędzia analityczne* (Eng. Methods, techniques and analytical tools), part III, Warszawa 2024.

[27] "Since 2014, water bills increased by almost a third, and energy bills grew several times, while the price of gas for households surged several dozen times. Many people simply do not have the money to pay for utilities. They literally struggle to survive". Quoted after: *Обращение Президента Российской Федерации*, Президент России (*Obrashcheniye Prezidenta Rossiyskoy Federatsii*, Prezident Rossii), 21 II 2022, http://kremlin.ru/events/president/news/67828 [accessed: 27 IX 2024].

[28] A.S. Bowen, *Russia's War in Ukraine: Military and Intelligence Aspects*, Congressional Research Service Report, Washington 2023, p. 6.

[29] M. Minkina, *Rosyjskie instrumentarium wpływu, nękania i prowokacji* (Eng. Russian instrumentation of influence, harassment and provocation), Siedlce 2023, pp. 186–188.

The effectiveness of the troops used in operations against Georgia in 2008 was also insufficient according to the Russian authorities, so reforms and investment in the Armed Forces of the RF were undertaken. After their introduction, the annexation of Crimea in March 2014 and the irregular operations conducted in the Lugansk and Donetsk regions were successful, as was the Russian intervention in the civil war in Syria in September 2015. During a visit to Moscow in November 2021, CIA chief William Burns assessed that the Russians were confident in their readiness to seize Ukraine and that their demonstrations of force were not intended to be mere attempts at intimidation[30]. This assessment was exaggerated as a result of the developing tendency in authoritarian systems of power to limit criticism, emphasised by a culture of *vranyo*[31] that made it impossible to eradicate the problem of corruption in the military. The "special military operation" plan envisaged that from the tenth day of the invasion, the leading role of the ground troops would be replaced by the assumption of control of the operation by Russian special services and Rosgvardia forces, whose task would be to pacify possible popular discontent and establish an occupation authority. In preparation for the invasion, the FSB trained with the Airborne Forces of the Russian Federation (VDV) to carry out tasks described in English-language military terminology as kill-or-capture[32]. Subsequently, the plan was to conduct flat searches and set up filtration camps to create files of material for use by offensive counter-intelligence, as well as to select and intimidate Ukrainians who were to be deported to Russia. It was planned to bring teachers and officials from Russia to the occupied territories to re-educate Ukrainians. Once the Ukrainian government and parliament had been eliminated, a pro-Russian "Peace Movement" would be elevated to power. An important element of the planning was the seizure of Ukrainian nuclear power plants and the establishment of military bases and armament depots there, with the aim of blackmailing the conquered population with energy and of politically blackmailing European states with the threat of radioactive contamination[33]. Preparations for the invasion, in the form of troop concentration and deployment,

[30] W. Spaniel, *How Ukraine Survived*…

[31] *Standoff. A chronicle of Russian invasion of Crimea*…

[32] Cf. B. Jagodziński, *Działania i rozwój jednostek specjalnych* (Eng. The activities and the development of special units), "Przegląd Bezpieczeństwa Wewnętrznego" 2022, vol. 12, no. 22, p. 169; Ł. Kułaga, *Używanie dronów w celu zwalczania międzynarodowego terroryzmu w świetle „ius in bello"* (Eng. The use of drones in combating international terrorism in the light of the "ius in bello"), "Zeszyty Prawnicze" 2017, vol. 17, no. 1, p. 109. https://doi.org/10.21697/zp.2017.17.1.05.

[33] M. Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting*…, pp. 10–11.

were carried out under the guise of exercises "West-2021" (Russian: Запад-2021) and exercises "Allied Decisiveness-2022" (Russian: Союзная решимость-2022).

Decision-making circles of the Russian Federation – governmental politics model

The statements from the Security Council of the RF meeting of 21 February 2022 (published a day later), a prelude to the war, could be the subject of analysis for a simplified governmental politics model. The meeting can be described as a test of strength by the "collective Putin", given the obscured cameras in the meeting room, as well as Putin's statement that he was testing his advisers with the conduct of these talks[34]. Mark Galeotti analyses this meeting as an indicator of the division into groups of individual participants (Table 3). In the conclusion of his article, Galeotti also highlighted a noticeable division between the President's trusted people and the institutional staff sitting in the Security Council of the RF[35]. The role of the other participants was not analysed.

Table 3. Russian government policy model – division into factions in the Security Council of the Russian Federation.

Determination of the fraction	Members
warriors	Alexander Bortnikov, Nikolai Patrushev, Sergei Shoigu
reliable	Valentina Matviyenko, Dmitry Medvedev, Vladimir Kolokoltsev
sceptical	Sergei Lavrov, Mikhail Mishustin, Dmitry Kozak
reluctant	Sergei Naryshkin

Source: own elaboration based on: M. Galeotti, *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022, https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins-security-council-meeting-a76522 [accessed: 1 IX 2024].

[34] *Заседание Совета Безопасности* (*Zasedaniye Soveta Bezopasnosti*), YouTube, 22 II 2022, https://www.youtube.com/watch?v=_YRUlb_7T9o [accessed: 28 IX 2024].

[35] M. Galeotti, *The Personal Politics of Putin's Security Council Meeting*…

Table 4 provides a description of the speeches made by 15 participants of the Security Council of the Russian Federation meeting on 21 February 2022.

Table 4. Russian government policy model – description of the speeches made by participants at the Security Council of the Russian Federation meeting of 21 February 2022, in order of appearance.

First name and surname	Position	Comment
Vladimir Putin	President	He focused on the threat to annexed Crimea from Ukraine's possible accession to NATO
Sergei Lavrov[36]	Minister of Foreign Affairs	He pointed to the possibility of further talks with the US
Dmitry Kozak[37]	Deputy Chief of Staff of the Presidential Executive Office, representative at the Minsk talks	He stated the lack of prospects for further negotiations and asked about the possibility of considering the annexation of the so-called Donetsk People's Republic (DPR) and Lugansk People's Republic (LPR). Putin dismissed Kozak's question in a rather disrespectful manner and instead mentioned the need to recognise the sovereignty of these republics
Alexander Bortnikov[38]	Director of the Federal Security Service (FSB)	He spoke primarily about border security in the regions neighbouring Ukraine and the influx of refugees from the territories of the separatist republics

[36] While Lavrov's political position was strong during Medvedev's presidency, in the context of both the 2014 and 2022 decisions, Lavrov appeared to be outside the inner circle of decision-making. It is an open question whether he was pushed away from it or whether he moved away of his own accord.

[37] Born and raised in Ukraine. Specialist in steered separatism operations in the so-called near abroad, in particular in Transnistria, Moldova. His position in power circles was weak and limited to confidence in his substantive competence with the president (In Putin's inner circle, Galeotti distinguishes between officials who owe their position to substantive competence useful in governing the state (meritocracy), and those trusted by the president whose influence stems from close relations with him (coterie)). See: O. Sukhov, *From Olympics to Crimea, Putin Loyalist Kozak Entrusted With Kremlin Mega-Projects*, The Moscow Times, 28 III 2014, https://www.themoscowtimes.com/2014/03/27/from-olympics-to-crimea-putin-loyalist-kozak-entrusted-with-kremlin-mega-projects-a33409 [accessed: 1 IX 2024]. Kozak maintained contact with Andriy Yermak, Head of the Office of the President of Ukraine Volodymyr Zelensky. See: K. Skorkin, *Why President Zelensky Is Purging His Inner Circle*, Carnegie, 15 IV 2024, https://carnegieendowment.org/russia-eurasia/politika/2024/04/why-president-zelensky-is-purging-his-inner-circle?lang=en [accessed: 28 IX 2024].

[38] Coming from the Department of Economic Security (4th Department), together with Patrushev, can be considered the closest circle of the president.

First name and surname	Position	Comment
Sergei Shoigu[39]	Minister of Defence	He conveyed propaganda messages about Ukraine's alleged shelling of Lugansk and Donetsk, the humanitarian catastrophe in the separatist republics, Ukraine's readiness to invade these territories, the conduct of terrorist activities and Ukraine's attempts to obtain nuclear weapons
Dmitry Medvedev	Deputy Chairman of the Security Council	He referred to the experience of the 2008 war with Georgia and said that the US conducts special operations around the world all the time, and then the superpowers go back to talking to each other anyway, to the exclusion of states that are objects, not subjects, of superpower policy
Vyacheslav Volodin	Chairman of the State Duma	On behalf of the State Duma, he requested the recognition of the DPR and LPR
Valentina Matviyenko	Chairwoman of the Federation Council	She argued that Western weapons could be taken over by "nationalists and Banderites". This may indicate the lack of awareness of the "denazification" argument (after Maxim Katz of Alexei Navalny's Anti-Corruption Foundation – discrepancies in the rhetoric used by the various participants in the meeting were indicative of who was privy to the plan to carry out the invasion at the time the meeting was held) to be used as one of the pretexts for invasion
Igor Krasnov	Procurator-General of the RF	Speech was cut from the official transcript
Nikolai Patrushev[40]	secretary of the Security Council	He focused on the unreasonableness of further talks, especially with non-US actors

[39] Hailing from an ethnic minority, he has not formed an effective oligarchic faction with others from the inner circle of power. Continuously in ministerial positions since 1994. He can be characterised as a loyal contractor with limited powers of his own who does not infringe status quo. Transferred to the army from the structures of the Ministry for Emergencies, he did not continue Anatoly Serdyukov's reforms and focused on activities of superficial nature. See: W. Jurasz, H. Grala, *Wataha Putina* (Eng. Putin's pack), Warszawa 2023, p. 74.

[40] Patrushev is a former Head of the FSB, who, due to his close relationship with Putin back in the 1990s, must be considered part of the inner circle of power. Interested in continuity of influence, he entrusted his sons with important positions. Grala attributes to him a critical assessment of the unity of the Russian elite on the eve of the invasion, which did not appear in the recording of the meeting of the Security Council of the RF. Ibid., p. 65.

First name and surname	Position	Comment
Mikhail Mishustin	Prime Minister	He assessed the ability of Russia's economy to perform in the event of Western sanctions
Sergei Naryshkin	Head of the Foreign Intelligence Service	He called for "giving one more chance to Western partners to influence Ukraine", supposedly in agreement with Nikolai Patrushev, but with such a different way of arguing that this position should be interpreted as a recommendation to refrain from invasion. Moreover, he mixed up the issues of recognition of sovereignty and annexation of the separatist republics. During the meeting, Putin treated him in a humiliating manner[41]
Vladimir Kolokoltsev	Minister of Internal Affairs	He limited himself to invectives against Ukraine and Western countries
Igor Shchyogolev	Representative of the President in the Central Federal District	He limited himself to invectives against Ukraine and Western countries
Viktor Zolotov	Head of Rosgvardia	He limited himself to invectives against Ukraine and Western countries

Source: own elaboration based on: *Заседание Совета Безопасности* (*Zasedaniye Soveta Bezopasnosti*), YouTube, 22 II 2022, https://www.youtube.com/watch?v=_YRUlb_7T9o [accessed: 28 IX 2024].

After the failures of the invasion, Sergei Shoigu lost his position and his deputy Timur Ivanov was arrested on corruption charges[42]. Andrei Belousov, who came from a scientific and industrial background[43], became Minister of Defence. The position of secretary of the Council was lost to Nikolai Patrushev, who, however, later returned to the Council as an advisor[44]. In turn, Sergei Ivanov returned to the permanent

[41] Naryshkin's relationship with Putin's circle and the FSB can be described as complicated due to the organisational conflict between the FSB and the SVR (Foreign Intelligence Service) and the "court" role of the security service in the power system.

[42] М. Кац, *Арестован замминистра обороны Иванов* (*Arestovan zamministra oborony Ivanov*), YouTube, 24 IV 2024, https://www.youtube.com/watch?v=5p4S7AKBPOg [accessed: 28 IX 2024].

[43] Organisational combination of scientific institutions and industrial plants, characteristic of the Russian defence and advanced dual-purpose technology industry. See: И.В. Устинович, *Научно-промышленный комплекс как одна из форм взаимодействия организаций*, "Труды БГТУ" 2023 (I.V. Ustinovich, *Nauchno-promyshlennyy kompleks kak odna iz form vzaimodeystviya organizatsiy,* "Trudy BGTU" 2023), vol. 5, no. 2, pp. 72–77.

[44] *Putin to keep demoted ally Patrushev on Russia's Security Council*, Reuters, 12 VII 2024, https://www.reuters.com/world/europe/putin-keep-demoted-ally-patrushev-russias-security-council-2024-06-11/

composition of the gremium (to a minor position, but according to expert opinions, the personal composition of the gremium is more important than formal positions in this regard). It is worth adding that, after the failures of the 2022 invasion plan, the role of this gremium has indeed diminished[45].

Hughes pointed to the lack of in-depth analyses on the impact of political and fractional decisions and stressed that simple or even trivial conclusions (mistake, underestimation of the opponent) prevail in the literature[46]. The authors would like to point out that the service-organisational (organisational behaviour model) and government-official (governmental politics model) models, although presented in a general manner, may allow this impasse to be broken.

Russia's invasion of Ukraine in 2022 as unsuccessful coup de main

The Russian invasion of Ukraine launched on 24 February 2022 was met with divergent reactions from the public and decision-making centres in the Western world. Statements by politicians and evacuations of diplomatic personnel suggested that Ukraine would not withstand the onslaught of Russian troops[47]. Ukraine's effective resistance came as a surprise to many. The effectiveness of this resistance dramatically changed the assessment of the military power of the RF. The Russian government's decision to launch an invasion with forces insufficient (in terms of the art of war[48]) to control such a large territory was seen as an irrational action[49]. Taking into account the situational logic, this is the realisation of a scenario previously observed in Hungary (1956), Czechoslovakia (1968) or Afghanistan (1979). Russia's use of the term "special military operation" is seen as a purely propaganda exercise

[accessed: 28 IX 2024]; *Security Council structure*, President of Russia, http://www.en.kremlin.ru/structure/security-council/members [accessed: 28 IX 2024].

[45] G. Kuczyński, *Zmiany w Radzie Bezpieczeństwa Federacji Rosyjskiej* (Eng. Staff reshuffles in Russia's Security Council), Warsaw Institute, 14 II 2023, https://warsawinstitute.org/pl/zmiany-w-radzie-bezpieczenstwa-federacji-rosyjskiej/ [accessed: 28 IX 2024].

[46] A. Hughes, *Plan Z. Reassessing Security-Based…*, pp. 174–208.

[47] See for example: S. Westfall, *These countries are withdrawing embassy staffers from Ukraine amid growing fears of an invasion by Russia*, The Washington Post, 14 II 2022, https://www.washingtonpost.com/world/2022/01/25/ukraine-embassy-evacuations/ [accessed: 21 IX 2024]; S. Walker, *'It is past time to leave Ukraine': western diplomats flee Kyiv*, The Guardian, 13 II 2022, https://www.theguardian.com/world/2022/feb/13/it-is-past-time-to-leave-ukraine-western-diplomats-flee-kyiv [accessed: 21 IX 2024].

[48] Example calculation, see: C.A. Lawrence, *The Battle for Kyiv. The fight for Ukraine's capital*, [n.p.] 2023, pp. 50–64.

[49] T. Cooper et al., *War in Ukraine. Volume 2: Russian Invasion, February 2022*, Warwick 2023, p. 33.

to suppress the truth about the war[50]. The analysis conducted makes it possible to determine why, in the understanding of the Russian leadership, the failed attempt to control Ukraine in February 2022 was to be carried out as a "special military operation" rather than a conventional war. Due to the mixed nature of the operations, which utilised the force structures of the Ministry of Defence and Internal Affairs as well as intelligence structures, there is a conceptual confusion.

While in the east of Ukraine Russian troops acted methodically, most likely on the basis of much pre-prepared plans, in the north the Armed Forces of the RF assumed rapid movement in columns in a marching formation to reach the strategic objective, Kyiv. The priority *coup de main* component in the area was the landing of aeromobile troops at Hostomel Airport to enable the airlift of a significant VDV forces, which was still to be joined by forces based in Belarus. An attack on Kyiv from a northerly direction on the right bank of the Dnieper (for the Ukrainian side – the Polesia Operational Region) may have seemed particularly promising to Russian planners because of the shortest distance to cover, the lack of need to ford the Dnieper and the lack of permanent dislocation of large units of the Ukrainian Armed Forces (Ukrainian: Збройні сили України) in this section. The area of planned activities was secured exclusively by units of the State Border Guard Service of Ukraine (Ukrainian: *Державна прикордонна служба України*), the National Guard of Ukraine (Ukrainian: *Національна гвардія України*) and 200 guards of the Chernobyl Nuclear Power Plant[51] (Ukrainian: *Чорнобильська атомна електростанція*, ChNPP). Moreover, the exclusion zone around the defunct nuclear power plant was a large, virtually uninhabited area (100–150 people in 2600 km^2) that could be easily controlled. The radiation risk was considered negligible from a military point of view[52]. What was important for Russian planners, however, was that Ukraine's major defence exercise "Blizzard-2022" (Ukrainian: Заметіль-2022) did not envisage significant fighting in this section. According to an analysis of the operational area, the Russians have concentrated troops there under the pretext of the "Allied Resolve-2022" exercises running from 10 to 20 February 2022. Significant forces were dislocated to the right bank of the Dnieper on the Belarusian side.

---

[50] Cf. *Dylematy rosyjskiej propagandy. "Specjalna operacja wojskowa straciłaby sens"* (Eng. Dilemmas of Russian propaganda. "A special military operation would lose its meaning"), Onet, 27 XII 2022, https://wiadomosci.onet.pl/swiat/dylematy-rosyjskiej-propagandy-specjalna-operacja-wojskowa-stracilaby-sens/2f1tlb0 [accessed: 21 IX 2024]; M. Hess, *Vladimir Putin finally calls Russia's 'special military operation' a war*, UnHerd, 21 II 2023, https://unherd.com/newsroom/vladimir-putin-finally-calls-russias-special-military-operation-a-war/ [accessed: 21 IX 2024].

[51] М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю*…, p. 11.

[52] А. Харук, М. Жирохов, *Бойова хроніка*…, p. 50.

The Russians owed their initial successes in the Polesia Operational Region primarily to the correctly executed elements of a *coup de main* operation, i.e. a surprise attack from the territory of Belarus, whose Defence Minister, Viktor Khrenin, declared in talks with Ukraine's political leadership that he ruled out an attack by Russian troops from that territory[53]. Ukrainian border and National Guard units were successfully surprised and failed to blow up the road and rail bridges in the area. The seized vehicles of these units were in turn used to provoke Russian sabotage and reconnaissance groups. These groups reached Kyiv and operated on equipment with Ukrainian markings, thus creating chaos in the defenders' positions until reconnaissance and sabotage groups (Russian: Диверсионно-разведывательная группа, ДРГ) were dismantled[54]. As the 167 soldiers of the 1st Regiment of Key Facilities Protection of the National Guard of Ukraine were neither trained in armoured vehicle combat nor equipped with the appropriate weaponry, they surrendered when Russian tanks and transporters entered the ChNPP. The defenders were further disadvantaged by the espionage activities of the SBU officer recruited by the Russians, Andryi Naumov, who passed on defence plans for the area to the enemy and also had contacts in the formations protecting the exclusion zone. The surprise caused by the Hostomel landing is, in turn, linked to the controversial role of double agent Denys Kiryeyev, who – despite having warned the authorities in Kyiv of a possible attack – was eliminated by the SBU[55]. While Western sources underestimated the airport's defenders and stated that Hostomel's defensive positions were indicated by a Russian agent located in Antonov[56], Ukrainian sources did not confirm this information. On the contrary, resistance by the territorial airfield defence unit posed a significant obstacle to the landing and resulted in a loss of equipment, men and time relative to the action plan, as the battlefield evidence confirms[57]. Despite the withdrawal of the territorial defence forces from the airfield and barracks buildings after running out of ammunition and the difficulty of the Ukrainian rapid reaction forces to fully eliminate the elite Russian formations, the destruction of the airstrip by Ukrainian artillery eliminated the threat of VDV transport aircraft landing at the airfield. They were forced to

[53] М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю*…, pp. 4–9.

[54] Ibid., pp. 10–19.

[55] B. Forrest, *Russian Spy or Ukrainian Hero? The Strange Death of Denys Kiryeyev*, The Wall Street Journal, 18 I 2023, https://www.wsj.com/articles/russian-spy-or-ukrainian-hero-the-strange-death-of-denys-kiryeyev-11674059395 [accessed: 29 IX 2024].

[56] W. Spaniel, *How Ukraine Survived: Inside the Strategy to Stop Russia's Invasion*, e-book.

[57] *Destination Disaster: Russia's Failure At Hostomel Airport*, Oryx, 13 IV 2022, https://www.oryxspioenkop.com/2022/04/destination-disaster-russias-failure-at.html [accessed: 29 IX 2024].

land on Belarusian territory. On the other hand, sabotage and diversionary actions against the Vasylkovo airfield failed to disable this base from use[58].

During the attack, the Russian columns did not carry out adequate reconnaissance, infantry rushes with combat infantry vehicles or artillery or sapper preparation until they were forced to do so by the resistance of the defenders[59], a feature of *coup de main* type operations. Therefore, the stretched Russian columns that had not occupied towns in the Sumy and Chernihiv oblasts, such as Glukhov, Konotop, Nizhyn, Sumy, Romny and Priluki, found it increasingly difficult to secure logistics against the Ukrainian Armed Forces attacks. At the time of the attack on 9 March 2022 on sub-Kyiv Brovary, these were incorrectly secured supply lines of almost 400 km[60]. If the defender's resistance had been overpowered by the infiltration of offensive counter-intelligence, the logistical difficulties would not have been so onerous as to be a decisive obstacle to the continuation of the operation. Meanwhile, contrary to the assumptions of the planners of "the special military operation", in the face of resistance and attacks by Ukraine's defenders on the transport columns, the logistics of the most advanced troops were paralysed. Consequently, the Kyiv operation as a *coup de main* ended in failure.

The direct attack on Kharkiv was based primarily on Spetsnaz columns launching raid-type attacks using lightly armoured Tigr vehicles. An attempt to seize a selected administrative facility on the march was not possible due to resistance from the defenders and instead the assault group captured a school building. After prolonged fighting, however, it was dismantled. It should be noted that the Spetsnaz units were held back and eliminated in the urbanised area by units of the Ukrainian National Guard and improvised units from, among others, the Ivan Kozhedub National University of the Air Force in Kharkiv, or tanks at the disposal of the Military Institute of Tank Troops in Kharkiv[61]. In turn, a column of the Mobile Special Purpose Detachment, OMON (Russian: отряд мобильный особого назначения), was destroyed on the approach to the city, near the village of Vesele, by Ukrainian tanks from the 92nd Brigade, against which the forces assigned to suppress the demonstration had neither the appropriate armament nor training[62].

---

58 М. Жирохов, *Невідбутий бліцкриг*…, pp. 60–70.

59 А. Харук, М. Жирохов, *Бойова хроніка*…, pp. 35–36.

60 For comparison – the longest "jump" made by Russian columns in the Crimea from Kerch to Armiansk was 288 km in favourable conditions.

61 А. Харук, М. Жирохов, *Бойова хроніка*…, pp. 111–118.

62 М. Жирохов, *Війна танків. Україна, лютий-серпень 2022*…, pp. 49–54.

The Russians' only operational successes were in the Kherson direction, where they managed to take over the hydroelectric power station at Nova Kakhovka, the Antonovsky Bridge and the cities of Kherson, Mikolaiv and Voznesensk (where the aeromobile component was used more effectively than in Hostomel[63]). Some of these achievements can also be attributed to the intelligence infiltration of Ukrainian power structures, especially the SBU[64].

The operation on the Kyiv direction thus had the characteristic features of *coup de main*, while the operations on the Donbas front had the character of classical military actions. They did not presuppose the breaking of resistance by means of suddenness of action and overwhelming use of force, but a classic frontal assault with the intention of pushing the enemy out of occupied positions, after prior fire preparation (artillery as well as air and rocket).

As outlined in the *Introduction*, the authors considered the 1968 Operation "Danube" as an appropriate historical analogy for the Russian operation in 2022. It was an operation that exemplified the real-life activities of the Soviet Army, conducted in conjunction with the Allies, and both the preparations for and the conduct of the operation have numerous common features that can be analysed in terms of the *coup de main* characteristics adopted for the purposes of the article. A comparison of the first phase of the 2022 Russian invasion of Ukraine as a failed *coup de main* operation with the invasion of Czechoslovakia in 1968 by the 2nd Army of the Polish Army as part of the Joint Armed Forces of Warsaw Pact is shown in the Table 5.

Table 5. Comparison of the modus operandi of Warsaw Pact troops against Czechoslovakia in Operation "Danube" in 1968 with the actions of the Russian Federation troops in the first phase of the invasion of Ukraine on the Kyiv direction in 2022.

Characteristic feature	Operation "Danube" 1968	The first phase of the invasion of Ukraine on the Kyiv direction in 2022
Deception	Preparations for the invasion were carried out under the guise of the "Cloudy Summer 1968" exercises.	Preparations for the invasion were carried out under the guise of exercises "West-2021" and "Allied Decisiveness-2022"

[63] А. Харук, М. Жирохов, *Бойова хроніка*…, pp. 165–173.

[64] K. Gustafson et al., *Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022*, "Intelligence and National Security" 2024, vol. 39, no. 3, p. 405. https://doi.org/10.1080/02684527.2024.2322214.

Characteristic feature	Operation "Danube" 1968	The first phase of the invasion of Ukraine on the Kyiv direction in 2022
Grouping	The 10th and 11th Armoured Divisions were deprived of their rocket artillery, heavy engineering equipment and part of their logistics component. The same changes applied to the 4th Mechanised Division in the 2nd Army reserve. The forces used in the operation were reinforced with aeromobile and long-range reconnaissance units	The Russian grouping on the northern and southern fronts was distinctive. A large part of the force was in a marching formation and belatedly transitioned into a fighting formation, despite encountering determined resistance. This was particularly evident on the northern front, where Russian forces had around 70 000 troops, of which around 15 000–30 000 were in a column stretching 64 km at its peak marching towards Kyiv. The composition of these forces was also unusual, where, in addition to units of the Armed Forces of the RF[65], the forces included: the 141st Special Motorised Regiment (Chechen), units of Rosgvardia (Special Rapid Response Unit – SOBR), OMON and the Private Military Company Redut
Pace	Time to reach targets 70–100 km from the border: 6–12 hours towards Prague and Brno. Another 12 hours for 4th Mechanised Division to reach designated targets near Prague	Documents seized near Kherson in spring 2022 indicate that, for example, the 1st Battalion Tactical Group from the 810th Guards Naval Infantry Brigade was expected to reach targets between Odessa and Mikolaiv, 200 km from its initial positions, between 20 February and 6 March 2022
Blockades	The 4th Mechanised Division and the 27th Tank Regiment from the 5th Armoured Division were tasked with blocking the Czechoslovak garrisons in the towns of Mladá Boleslav and Milovice. Reinforced by tanks and reconnaissance units of the 6th Airborne Division from the 16th Mechanised Division, they were, in turn, to block garrisons in the towns: Rychów, Kostelec nad Labem, Rokytnice v Orlických horách and Červená Voda	In 2022, the Russians failed to blockade garrisons as they did in Crimea in 2014

[65] The units of the Armed Forces of the Russian Federation on the Northern Front in the period 24 II–8 IV 2022 included operational formations: 1st Guards Tank Army, 35th, 36th Combined Arms Armies; tactical formations: 90th Guards Tank Division, 11th Guards Airborne Brigade, 31st Guards Airborne Brigade.

Characteristic feature	Operation "Danube" 1968	The first phase of the invasion of Ukraine on the Kyiv direction in 2022
Subsidiary units	The 15th regiment of the Internal Defence Forces was to blockade the garrison in Krnov	A large part of the Russian grouping was made up of Rosgvardia, OMON and SOBR troops
Power ratio between defender and aggressor	It was assumed that the defenders would have 19 820 troops against 14 400 aggressor troops, 456–490 tanks, 350–405 armoured personnel carriers. The assumed ratio of forces between the Polish Army[66] and the Czechoslovak People's Army was: – troops (total): 1:1,4 – tanks: 1:1,1 – armoured personnel carriers: 1,3:1. With combat readiness in mind, it was assumed that the ratio of forces would level off at 1:1. In this regard, it can be noted that the 2nd Army operation carried out did not envisage a ratio of forces appropriate for an offensive (the aggressor was not large enough relative to the defender)[67]	The invasion was carried out with some 190 000 Russian troops, which, against a defender force of some 196 600 and 102 000 militia officers, gives a ratio of 1:1,57. Data on the size of the Ukrainian forces varies, but it is clear that the Russian forces did not have the numerical superiority (3:1) appropriate for an offensive[68]
Command, control, communication and intelligence objectives (C3I)	Particular attention was paid to the takeover of television and radio transmission centres in Czechoslovakia, as well as airports. Control of means of communication was crucial to enable increased propaganda activities, and airfields could enable air transport for invading forces. The operation failed due to insufficient research into the Czechoslovak communications system, creating the need to seize the facility[69]	The inability to destroy Ukrainian command and communications systems resulted in the failure to achieve the political objectives of the "special military operation" through both a *coup d'état* (an attempt to put Viktor Medvedchuk in power in Kyiv) and a *coup de main* in Ukraine's main cities, which ultimately forced Russian forces to retreat

[66] Unofficially: the People's Army of Poland (LWP). The way this name is written is controversial. Cf. H.Z. Figura, *Ludowe Wojsko Polskie czy Wojsko Polskie?* (Eng. People's Army or Polish Army), "Kwartalnik Bellona" 2015, vol. 681, no. 2, pp. 215–218.

[67] AIPN, The collection of documents on the Warsaw Pact, *Operation "Danube" on the intervention of Warsaw Pact members in Czechoslovakia*, vol. 1 ref. no. BU 02958/1: Operational issues of the General Staff of the Polish Army, vol. 2 ref. no. BU 02958/2: Operational reports of the General Staff of the Polish Army. The 2nd Army report on the course of operation "Danube".

[68] *The Military Balance 2022. The annual assessment of global military capabilities and defence economics*, [n.p.] 2022.

[69] For the purposes of researching communications interruption operations, it is possible to

Characteristic feature	Operation "Danube" 1968	The first phase of the invasion of Ukraine on the Kyiv direction in 2022
External intervention	The plan included the possibility that NATO forces from the Federal Republic of Germany might intervene to support the Czechoslovaks, risking a change in the nature of the operation from pacification to combat	No information on the inclusion of a foreign military intervention option in the "special military operation" plans
Logistics	Much of the logistics was based on rail transport, as the capacity of road transport was insufficient	"Special military operation" was planning in isolation from doctrinal patterns regarding the use of military force in conventional conflict. The formations were prepared for a short conflict. Logistical support could not keep up with the operation. The use of Russian forces was not in line with either the logistical capabilities or the way the Russian army was organised. Logistics were only adapted to operations in the Donbas in 2022[70], which were already classic frontline operations and not *coup de main*
Air component	The Polish Army's airborne units operated as part of the land component. In Prague, Soviet paratroopers of civilian aircraft managed to take over the airport by impersonating civilian aircraft. This enabled the air transport of invading troops and material directly to the capital of Czechoslovakia	Russia's attempt to take control of Hostomel airfield near Kyiv correlated with the arrival of a column of ground forces from Belarus across the Pripyat marshes was a key premise of the execution of *coup de main*. The failure to capture the airfield near the capital was one of the main factors behind the failure of the operation and the start of the conventional war in other areas

Source: own elaboration based on: AIPN, The collection of documents on the Warsaw Pact, *Operation "Danube" on the intervention of Warsaw Pact members in Czechoslovakia*, vol. 1 ref. no. BU 02958/1: Operational issues of the General Staff of the Polish Army, vol. 2 ref. no. BU 02958/2: Operational reports of the General Staff of the Polish Army. The 2nd Army report on the course

speculate whether the cautious planning of Operation "Malwa" prior to the declaration of martial law in 1981 by the General Staff of the Polish Army was due to the failure of Operation "Danube" in this regard. See: AIPN, the Ministry of the Interior in Warsaw [1944] 1954–1990, *Case object code-named 'Gotowość'* (Readiness) *concerning the introduction of martial law. Archival materials transferred from Division XII of Department II of the Ministry of the Interior to the Archive of the 'C' Bureau MSW,* ref. no. BU 0236/254.

[70] P. Schwartz et al., *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023, p. 68.

of operation "Danube"; А. Харук, М. Жирохов, *Бойова хроніка 2022 року*, Київ 2024 (A. Kharuk, M. Zhirokhov, *Boyova khronika 2022 roku*, Kyyiv 2024); М. Жирохов, *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (M. Zhirokhov, *Nevidbutiy blitskrig: oborona ayerodromiv Gostomelyu ta Vasil'kova, lyutiy 2022 roku*, Chernigiv 2022); *The Military Balance 2022. The annual assessment of global military capabilities and defence economics*, [n.p.] 2022; M. Zabrodskyi, J. Watling, O.V. Danylyuk, N. Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022; M. Štefanský, *"Operation Danube"*, in: *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (ed.), Stuttgart 2021; P. Schwartz, A. Fink, J. Waller, M. Kofman, B. Lennox, M. Chesnut, *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023.

Summary

As part of the research, the authors addressed the issue of a specific use of force, defined by the term *coup de main* for the purpose of creating an operational definition, subsequently used to verify the working hypotheses, according to the research methods adopted.

The research objective of analysing the actions of the RF in its two acts of aggression against Ukraine, in 2014 and 2022, as a *coup de main* operation was achieved by verifying the subsequent working hypotheses using the selected research methods.

The authors draw three conclusions:

1. *Coup de main* operations may be conducted by Russia in the future.
2. With regard to Ukraine, this model for the use of force, used successfully in 2014, has run out of steam in 2022. It may provide a viable model for possible Russian intervention in Belarus and Kazakhstan, as well as in the NATO eastern flank states of Lithuania, Latvia and Estonia, particularly in those areas with a large Russian minority.
3. As indicated in the analytical section of the article, the success of this type of operation requires proper infiltration of the enemy, which is highly unlikely in the case of Poland, which was neither part of the USSR nor has a large Russian minority. On the other hand, due to Warsaw's geographical proximity to the Belarusian border, the security of the capital should be considered in the event of an attempt at bold surprise action to defeat the opponent with a single blow, i.e. a classically understood *coup de main*.

It can also be presumed that the perception of Russian decision-makers is crucial in choosing the method of achieving a political objective by conducting a military operation. It should be assumed that internal conditions within Russian decision-making structures (including factional issues) will be more important

than intersubjective factors of a geopolitical nature, such as a country's membership of international organisations. The internal stability of a particular state that is a potential target of a *coup de main* operation may play a greater role than, for example, the presence of a large Russian minority on its territory.

Bibliography

Allison G., Zelikow P., *Essence of Decision. Explaining the Cuban Missile Crisis*, Addison-Wesley Educational Publishers Inc., 1999.

Bassford Ch., *Na palcach wokół trójcy Clausewitza* (Eng. On a tiptoe around Clausewitz's Trinity), "Kwartalnik Bellona" 2017, vol. 688, no. 1, pp. 73–100.

Clausewitz C. von, *On war*, The quotation was excerpted from the original available on the website: https://ebook-mecca.com/online/On%20War%20-%20Carl%20von%20Clausewitz.pdf.

Cooper T., Fontanellaz A., Crowther E., Sipos M., *War in Ukraine. Volume 2: Russian Invasion, February 2022*, Warwick 2023.

Depczyński M., Elak L., *Rosyjska sztuka operacyjna w zarysie* (Eng. Russian operational art in outline), Warszawa 2020.

Figura H.Z., *Ludowe Wojsko Polskie czy Wojsko Polskie?* (Eng. People's Army or Polish Army), "Kwartalnik Bellona" 2015, vol. 681, no. 2, pp. 215–218.

Galeotti M., *Putin takes Crimea 2014. Grey-zone warfare opens the Russia-Ukraine conflict*, [n.p.] 2023.

Galeotti M., *Putin's wars. From Chechnya to Ukraine*, Oxford 2022.

Gustafson K. et al., *Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022*, "Intelligence and National Security" 2024, vol. 39, no. 3, pp. 400–419. https://doi.org/10.1080/02684527.2024.2322214.

Hermann H., *Operacyjny wymiar walki zbrojnej* (Eng. Operational dimention of armed struggle), Toruń 2004.

Hughes A., *Plan Z. Reassessing Security-Based Accounts of Russia's Invasion of Ukraine*, "Journal of Advanced Military Studies" 2023, vol. 14, no. 2, pp. 174–208. https://doi.org/10.21140/mcuj.20231402009.

Jagodziński B., *Działania i rozwój jednostek specjalnych* (Eng. The activities and the development of special units), "Przegląd Bezpieczeństwa Wewnętrznego" 2020, vol. 12, no. 22, pp. 167–184.

Jurasz W., Grala H., *Wataha Putina* (Eng. Putin's pack), Warszawa 2023.

Kozłowski J., *Metody, techniki i narzędzia analityczne* (Eng. Methods, techniques and analytical tools), part III, Warszawa 2024.

Kozłowski J., *Practical dimension of issues related to assessing the reliability of sources and the trustworthiness of data and information*, "Przegląd Bezpieczeństwa Wewnętrznego" 2023, no. 29, pp. 323–358. https://doi.org/10.4467/20801335PBW.23.032.18774.

Kułaga Ł., *Używanie dronów w celu zwalczania międzynarodowego terroryzmu w świetle „ius in bello"* (Eng. The use of drones in combating international terrorism in the light of the "ius in bello"), "Zeszyty Prawnicze" 2017, vol. 17, no. 1, pp. 107–134. https://doi.org/10.21697/zp.2017.17.1.05.

Lawrence C.A., *The Battle for Kyiv. The fight for Ukraine's capital*, [n.p.] 2023.

Liflyandchick A., Jones D., Fabian S., *The Fall from Grace of Russian SOF: The Danger of Forgetting Lessons Learned*, Irregular Warfare Center: Insights, vol. 1, no. 8, September 2023.

Luttwak E.N., *Zamach stanu. Podręcznik* (Eng. Coup d'état. A practical handbook), Warszawa 2017.

Minkina M., *FSB. Gwardia Kremla* (Eng. FSB. Kremlin's guard), Warszawa 2016.

Minkina M., *Rosyjskie instrumentarium wpływu, nękania i prowokacji* (Eng. Russian instrumentation of influence, harassment and provocation), Siedlce 2023.

Pherson R.H., Heuer R.J., *Structured Analytic Techniques for Intelligence Analysis*, [n.p.] 2020.

Spaniel W., *How Ukraine Survived: Inside the Strategy to Stop Russia's Invasion*, e-book.

Spaniel W., *What Caused the Russia-Ukraine War (And How Will It End?)*, e-book.

Štefanský M., *"Operation Danube"*, in: *Operation Danube Reconsidered. The International Aspects of the Czechoslovak 1968 Crisis*, J. Drabik (ed.), Stuttgart 2021.

The Characteristics of Total Institutions, in: *A Sociological Reader on Complex Organizations*, A. Etzioni (sci. ed.), New York 1961.

Russian and Ukrainian literature

Харук А., Жирохов М., *Бойова хроніка 2022 року*, Київ 2024 (Kharuk A., Zhirokhov M., *Boyova khronika 2022 roku*, Kyyiv 2024).

Триандафиллов В., *Характер операций совеременных армий*, Москва 1929 (Triandafillov V., *Kharakter operatsiy soveremennykh armiy*, Moskva 1929).

Устинович И.В., *Научно-промышленный комплекс как одна из форм взаимодействия организаций*, "Труды БГТУ" 2023 (Ustinovich I.V., *Nauchno-promyshlennyy kompleks kak odna iz form vzaimodeystviya organizatsiy*, "Trudy BGTU" 2023), vol. 5, no. 2, pp. 72–77.

Жирохов М., *Невідбутий бліцкриг: оборона аеродромів Гостомелю та Василькова, лютий 2022 року*, Чернігів 2022 (Zhirokhov M., *Nevidbutiy blitskrig: oborona ayerodromiv Gostomelyu ta Vasil'kova, lyutiy 2022 roku*, Chernigiv 2022).

Жирохов М., *Війна танків. Україна, лютий-серпень 2022*, Чернігів 2023 (Zhirokhov M., *Viyna tankiv. Ukraïna, lyutiy-serpen' 2022*, Chernigiv 2023).

Internet sources

Czy Jurij Andropow był twórcą pierestrojki? (Eng. Was Yuri Andropov the founder of perestroika?) – *Oblicza historii series*, YouTube, 14 V 2024, https://www.youtube.com/watch?v=vbbcuNYaxkU [accessed: 30 VI 2024].

Debata „Co dalej z Rosją?" – Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J. M. Nowakowski (Eng. The debate "What next for Russia?" – Hieronim Grala, Witold Jurasz, Janusz Onyszkiewicz, J. M. Nowakowski), YouTube, 4 XII 2023, https://www.youtube.com/watch?v=Gk45gw7ECHY [accessed: 30 VI 2024].

Destination Disaster: Russia's Failure At Hostomel Airport, Oryx, 13 IV 2022, https://www.oryxspioenkop.com/2022/04/destination-disaster-russias-failure-at.html [accessed: 29 IX 2024].

Dylematy rosyjskiej propagandy. "Specjalna operacja wojskowa straciłaby sens" (Eng. Dilemmas of Russian propaganda. "A special military operation would lose its meaning"), Onet, 27 XII 2022, https://wiadomosci.onet.pl/swiat/dylematy-rosyjskiej-propagandy-specjalna-operacja-wojskowa-stracilaby-sens/2f1tlb0 [accessed: 21 IX 2024].

Elity Zachodu tęsknią za przewidywalną Rosją (Eng. Western elites yearn for a predictable Russia) | *Prof. Hieronim Grala*, YouTube, 10 VI 2023, https://www.youtube.com/watch?v=KaU41GKpNmY [accessed: 30 VI 2024].

Forrest B., *Russian Spy or Ukrainian Hero? The Strange Death of Denys Kiryeyev*, The Wall Street Journal, 18 I 2023, https://www.wsj.com/articles/russian-spy-or-ukrainian-hero-the--strange-death-of-denys-kiryeyev-11674059395 [accessed: 29 IX 2024].

Galeev K. (@kamilkazani), entry on the portal X, 28 II 2022, https://x.com/kamilkazani/status/1498377757536968711?lang=en [accessed: 30 IX 2024].

Galeotti M., *The Personal Politics of Putin's Security Council Meeting*, The Moscow Times, 22 II 2022, https://www.themoscowtimes.com/2022/02/22/the-personal-politics-of-putins--security-council-meeting-a76522 [accessed: 1 IX 2024].

Hess M., *Vladimir Putin finally calls Russia's 'special military operation' a war*, UnHerd, 21 II 2023, https://unherd.com/newsroom/vladimir-putin-finally-calls-russias-special-military-operation-a-war/ [accessed: 21 IX 2024].

Kuczyński G., *Zmiany w Radzie Bezpieczeństwa Federacji Rosyjskiej* (Eng. Staff reshuffles in Russia's Security Council), Warsaw Institute, 14 II 2023, https://warsawinstitute.org/staff-reshuffles-in-russias-security-council/ [accessed: 28 IX 2024].

Meeting with permanent members of the Security Council, Kremlin.ru, 21 II 2014, http://en.kremlin.ru/events/president/news/20301 [accessed: 24 IX 2024].

Nie będzie końca wojny bez końca Putina: prof. Hieronim Gala (Eng. There will be no end to war without an end to Putin: prof. Hieronim Grala) – *didaskalia #6*, YouTube, 16 IV 2023, https://www.youtube.com/watch?v=uTlrecy9m80 [accessed: 30 VI 2024].

Putin to keep demoted ally Patrushev on Russia's Security Council, Reuters, 12 VII 2024, https://www.reuters.com/world/europe/putin-keep-demoted-ally-patrushev-russias-security-council-2024-06-11/ [accessed: 28 IX 2024].

Rosja Putina – obsesja neoimperialnej potęgi (Eng. Putin's Russia – obsession of neo-imperial power) | *Czwartki w DeBeKa #1*, YouTube, 29 II 2024, https://www.youtube.com/watch?v=rUAgEnRAllw [accessed: 30 VI 2024].

ROSYJSKI KRĄG WŁADZY (Eng. Russian power circle) – *Kulisy historii series Episode. 120*, YouTube, 1 VII 2023, https://www.youtube.com/watch?v=szr-pwtxV0U [accessed: 30 VI 2024].

Security Council structure, President of Russia, http://www.en.kremlin.ru/structure/security-council/members [accessed: 28 IX 2024].

Skorkin K., *Why President Zelensky Is Purging His Inner Circle*, Carnegie, 15 IV 2024, https://carnegieendowment.org/russia-eurasia/politika/2024/04/why-president-zelensky-is-purging-his-inner-circle?lang=en [accessed: 28 IX 2024].

Soldatov A., *The True Role of the FSB in the Ukrainian Crisis*, The Moscow Times, 15 IV 2014, https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985 [accessed: 28 IX 2024].

Spaniel W., *The "Battle" of Crimea: Inside Russia's Playbook to Capture the Peninsula*, YouTube, 15 III 2023, https://www.youtube.com/watch?v=Ijmoz2VfjrQ [accessed: 25 IX 2024].

Spaniel W., *The Hidden Battle that Saved Ukraine*, YouTube, 3 I 2023, https://www.youtube.com/watch?v=hh9xT9d6SJU [accessed: 25 I 2023].

Spaniel W., *Why Russia Miscalculated in Ukraine: A Self-Inflicted Disaster in Three Acts*, YouTube, 24 I 2023, https://www.youtube.com/watch?v=8YkGrKQXZxE [accessed: 25 I 2023].

Standoff. A chronicle of Russian invasion of Crimea, Defense Express, 4 III 2014, https://issuu.com/ukrainian_defense_review/docs/chronicles-of-russian-aggression-cr [accessed: 24 IX 2024].

Sukhov O., *From Olympics to Crimea, Putin Loyalist Kozak Entrusted With Kremlin Mega-Projects*, The Moscow Times, 28 III 2014, https://www.themoscowtimes.com/2014/03/27/from-olympics-to-crimea-putin-loyalist-kozak-entrusted-with-kremlin-mega-projects-a33409 [accessed: 1 IX 2024].

Walker S., *'It is past time to leave Ukraine': western diplomats flee Kyiv*, The Guardian, 13 II 2022, https://www.theguardian.com/world/2022/feb/13/it-is-past-time-to-leave-ukraine-western-diplomats-flee-kyiv [accessed: 21 IX 2024].

Westfall S., *These countries are withdrawing embassy staffers from Ukraine amid growing fears of an invasion by Russia*, The Washington Post, 14 II 2022, https://www.washingtonpost.com/world/2022/01/25/ukraine-embassy-evacuations/ [accessed: 21 IX 2024].

Wilk A., *Russian military intervention in Crimea*, Ośrodek Studiów Wschodnich, 5 III 2014, https://www.osw.waw.pl/en/publikacje/analyses/2014-03-05/russian-military-intervention-crimea [accessed: 29 IX 2024].

Russian internet sources

Заседание Совета Безопасности (*Zasedaniye Soveta Bezopasnosti*), YouTube, 22 II 2022, https://www.youtube.com/watch?v=_YRUlb_7T9o [accessed: 28 IX 2024].

Кац М., *Арестован замминистра обороны Иванов* (Kats M., *Arestovan zamministra oborony Ivanov*), YouTube, 24 IV 2024, https://www.youtube.com/watch?v=5p4S7AKBPOg [accessed: 28 IX 2024].

Обращение Президента Российской Федерации, Президент России (*Obrashcheniye Prezidenta Rossiyskoy Federatsii*, Prezident Rossii), 21 II 2022, http://kremlin.ru/events/president/news/67828 [accessed: 27 IX 2024].

Other documents

Bowen A.S., *Russia's War in Ukraine: Military and Intelligence Aspects*, Congressional Research Service Report, Washington 2023.

Schwartz P., Fink A., Waller J., Kofman M., Lennox B., Chesnut M., *Russian Military Logistics in the Ukraine War. Recent Reforms and Wartime Operations*, September, Stuttgart 2023.

The Military Balance 2022. The annual assessment of global military capabilities and defence economics, [n.p.] 2022.

Zabrodskyi M., Watling J., Danylyuk O.V., Reynolds N., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, Royal United Services Institute, 30 XI 2022.

Archival sources

AIPN, Ministry of the Interior in Warsaw [1944] 1954–1990, ref. no. BU 0236/254.

AIPN, The collection of documents on the Warsaw Pact, ref. no. BU 02958/1, ref. no. BU 02958/2.

Marek Klasa, PhD

Doctor of social sciences in the discipline of security sciences. Assistant professor at the National Security Faculty, War Studies University in Warsaw.

Contact: m.klasa@akademia.mil.pl

Michał Klasa

Graduate of postgraduate studies in analytical and information operations in the field of security at the Institute of Military History of the War Studies University in Warsaw.

Internal Security Review
2025, no. 32, pp. 333–343

https://doi.org/10.4467/20801335PBW.25.016.22182

ARTICLE

The European Union project SAFE-CITIES. More effective monitoring of threats in public spaces

MAŁGORZATA WOLBACH

The Polish Platform for Homeland Security

https://orcid.org/0009-0005-1837-0389

JAROSŁAW PRZYJEMCZAK

The Faculty of Law and Administration
of University of Business and Administration in Gdynia

https://orcid.org/0000-0003-3923-8078

Abstract

Nowadays, human activity is supported by modern technologies and tools. Many of these solutions are used in areas that have so far been resistant to change, as their nature and the applicable regulations did not allow for modifications. Such areas include public spaces which, by virtue of their role, are publicly accessible and open most of the time. In the article, the authors presented the assumptions of the SAFE-CITIES – project aimed at ensuring the highest possible level of protection for public spaces in the face of the growing threat of terrorism – and described selected technologies and tools, created as part of the project, supporting the processes of monitoring threats. They also discussed related projects addressed by the European Union.

Keywords

Safe-Cities, European Union, public space, services responsible for safety, new technologies, threat monitoring

Introduction

Due to the expansion of large cities and urban agglomerations, the difficulties associated with their functioning are multiplying[1]. The basic ones include, among others, problems related to communication, environment, administration, order and maintaining an appropriate level of security, especially in open, publicly accessible facilities or areas. Therefore, an important feature of existing or planned security systems is the ability to detect threats early, enabling the relevant entities to respond quickly to incidents. Due to the number and diverse nature of events that may occur in these spaces, it is impossible to prepare for all of them. The managers of these places should focus on the specific scenarios.

Economic, social and political changes create conditions conducive to the spread of hatred, extremist behaviour and conspiracy theories, which creates the risk of an increase in the number of planned and carried out terrorist attacks. Due to the constant threat of terrorism, the security of public spaces is one of the most important challenges for those responsible for security of contemporary European cities. As the data shows, the number of terrorist attacks in Europe remains high. According to the latest report on terrorist threats in the European Union prepared by Europol, in 2023, in seven Member States (France, Italy, Germany, Spain, Belgium, Greece, Luxembourg), a total of 120 terrorist attacks were recorded, of which 98 were carried out, 9 failed and 13 were foiled[2].

Attack planners are increasingly using the latest technological advances not only for propaganda and recruitment purposes, but also to search for new methods of attack, e.g. using artificial intelligence. The widespread availability of training materials, including on the internet, means that such individuals can easily acquire knowledge about attack tactics, weapons production methods and drone operation. In addition, virtual environments can provide a space for realistic training simulations for terrorists, which can facilitate to prepare for the attacks.

In the face of these challenges, it is extremely important to implement and continuously improve modern technologies that support the process of monitoring and analysing threats to the security of public spaces. Such solutions allow public and non-public entities responsible for security not only to combat threats more effectively, but also to prepare for potential attacks. In response to these needs,

[1] See in more detail, e.g.: A. Kaya, M. Koc, *Over-Agglomeration and Its Effects on Sustainable Development: A Case Study on Istanbul*, "Sustainability" 2019, vol. 11, no. 1. https://doi.org/10.3390/su11010135.

[2] Europol, *European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, pp. 5–11 [accessed: 13 III 2025].

numerous actions are being undertaken at various organisational levels. Their aim is to support institutions in ensuring the security of publicly accessible facilities and areas.

When it comes to safety, a variety of strategies and solutions should be used[3]. One of the most important European projects is the SAFE-CITIES[4]. Its implementation will enable more effective surveillance of public spaces. The article aims to present the objectives of this project and to describe selected technologies and tools developed as part of this initiative. The research question was: what kind of security initiatives will the EU undertake that will improve safety in public places? As part of their research, the authors used methods such as analysis, synthesis and inference. For formal and procedural reasons, they were unable to describe in detail some of the project assumptions as well as the technologies and tools developed. Some of them had been passed on for further work aimed at improving their performance and possible commercial use. Moreover, one of the initiatives described is still in progress and the results are not yet known.

SAFE-CITIES project

The SAFE-CITIES project[5] was aimed to ensure the highest possible level of protection for public spaces, primarily in areas such as proper risk management and the use of modern technologies that enable a transition from scattered action to a more comprehensive and systematic security and vulnerability assessment (SVA). As part of the project, the risks in public spaces were thoroughly analysed and strategies were developed to prevent its increase and mitigate the effects of potential terrorist threats. These actions are to be supported by an advanced interactive platform consisting of a variety of interconnected tools. These tools will enable detailed risk analyses to be carried out and will help to identify potential vulnerabilities in the locations under investigation.

The most important assumptions of the SAFE-CITIES project, which was completed on 30 June 2025, was the close cooperation between public and private entities, as well as the involvement of citizens in the process of shaping urban security

[3] J. Przyjemczak, *Wstęp* (Eng. Introduction) in: *Zadanie specjalne – człowiek, technologia, instytucja*, pt. 4, J. Przyjemczak (sci. ed.), Gdynia 2024, p. 7.

[4] European Commission SAFE-CITIES project under Horizon Europe: HORIZON-CL3-2021-FCT-01-07: Enhanced preparedness for attacks in public spaces, https://cordis.europa.eu/project/id/101073945 [accessed: 22 VII 2025].

[5] See: *SAFE-CITIES*, https://safe-cities.eu/ [accessed: 13 III 2025].

strategies, while maintaining their open nature. This was intended to enable more effective threat forecasting, faster response to incidents and better coordination of the activities of the services responsible for security. Another advantage was the opportunity to test innovative methods of minimising the effects of attacks during the project. These methods were to adapt security systems to dynamically changing threats.

SAFE-CITIES project partners

The project was implemented by a consortium consisting of 17 partners from eight EU countries: Italy, Cyprus, the Netherlands, Greece, Poland, Belgium, Finland, Slovenia, and one non-EU country, the United Kingdom. The role of coordinator was held by STAM[6], a private engineering company from Italy specialising in innovative technological solutions in the field of security, including the development of tools to support decision-making based on risk assessment and scenario simulation in crisis situations for critical infrastructure and soft targets[7]. Other partners included:

- technology companies developing analytical and simulation tools: IANUS Technologies (Cyprus)[8], D-Visor (Netherlands)[9], Thridium (United Kingdom)[10];
- research institutes and universities developing methodologies for assessing risk and vulnerability: National Centre for Scientific Research 'Demokritos' (Greece), University of Bologna (Italy), International Institute of Sociology in Gorizia (Italy), Università Verde di Bologna APS in Bologna (Italy);
- entities representing end users and key stakeholders for the effective implementation of solutions, such as: the Ministries of the Interior of Cyprus, Finland, Slovenia, the Provincial Police Headquarters in Gdańsk (Poland), the Red Cross in Gorizia (Italy), the municipality of Nova Gorica (Slovenia), the municipality of Gorizia (Italy), the Confederation of European Security Services (Belgium) and the Polish Platform for Homeland Security (Poland).

---

[6] *STAM – Mastering Excellence*, https://www.stamtech.com/ [accessed: 13 III 2025].

[7] Soft targets that may be attacked by terrorists include both physical and human targets that are not covered by special legal protection and are therefore vulnerable to terrorist attacks due to the ease with which they can be carried out. See in more detail: A. Hołub, *Obiekty ataków terrorystycznych* (Eng. Targets of terrorist attacks), "Przegląd Policyjny" 2018, no. 4, p. 18.

[8] *IANUS Technologies*, https://ianus-technologies.com/ [accessed: 13 III 2025].

[9] *D-Visor*, https://www.d-visor.nl/ [accessed: 13 III 2025].

[10] *Thridium*, https://thridium.com/t4s/ [accessed: 13 III 2025].

Thanks to the cooperation of the above-mentioned entities, the initiative took into account the interests of a large group of recipients. This also made it possible to obtain extensive technological, practical and substantive support in the area of the issues addressed.

SAFE-CITIES tools

Innovative solutions based on knowledge and tools provided by partners, tailored to current needs and changing technologies have been developed within SAFE-CITIES[11].

SBS

Scenario Builder & Serious Gaming Simulator (SBS) is an advanced tool for creating and simulating threat scenarios, specifically simulations of mass events and other events taking place in crowded spaces. It allows for realistic representation of dynamic interactions between people and response methods to various threats. With its help, one can create and configure threat scenarios in a realistic 3D environment. The simulator uses, among other things, blueprint objects in conjunction with a timeline, which enables the modelling of complex sequences of events, the customisation of character behaviour and the simulation of security system responses. Based on the data obtained, users can generate and edit three-dimensional spaces by importing CAD, BIM and BFX models, and accurately reproduce real locations. The tool allows for the configuration of both static elements, such as security measures and urban infrastructure, and dynamic elements, including the behaviour of individuals and crowds, security services, as well as strategic places of a given space, e.g. entry and exit points, communication routes and technical nodes. This also allows for the implementation of ready-made scenarios in multiplayer mode, such as realistic training simulations or so-called serious games, where participants can take on different roles. It is an ideal training environment for all entities involved in ensuring public order. The system offers realistic threat simulations covering various complex scenarios, including bomb attacks, arson, knife attacks, shootings, and drone attacks with explosive charges, allowing for comprehensive risk analysis and safety procedures. This is also helpful during virtual reality (VR) sessions, providing an even more immersive experience, increasing the effectiveness of training and allowing safety procedures to be practised in conditions close to real life. As an important training tool, SBS enables more effective security planning as well as faster and more effective response in crisis situations, thereby increasing the level of security in public spaces.

[11] *SAFE-CITIES Architecture*, https://safe-cities.eu/tools/ [accessed: 22 VII 2025].

SERVE

SEcuRity Vulnerability assessment (SERVE) is an interactive tool to assess the risk and vulnerability of public spaces to various threats and the degree of attractiveness of attack targets in any public space. The system's functionality simplifies and streamlines the security analysis as well as offers a comprehensive approach to this process. With SERVE, users can mark the areas under analysis directly on a map or floor plan. The tool also offers the option of selecting threats from a predefined list, thus personalising the risk assessment depending on the specifics of the selected area. It also enables the analysis of various types of risks, such as terrorist attacks, fires or chemical hazards, and thus the precise adaptation of security strategies to specific scenarios or situations. The analysis covers three aspects: risk, impact of risk and the attractiveness of a given public space to attackers. The process is supported by an interactive wizard that guides the user through a set of questions to help determine the level of threat. Each of these three indicators has a separate, customised set of questions. The tool has been equipped with a number of advanced options, such as the ability to import, export and integrate data or modify information such as existing security measures, obstacles, urban infrastructure elements and surveillance systems. SERVE provides a detailed analysis of the vulnerability of an area in the context of specific threats as well as more effective planning and implementation of preventive measures. With its intuitive interface, advanced analysis functions and wide range of applications, the system is an indispensable tool for security experts.

SCoreboard

This is an intelligent analytical tool designed for monitoring and visualising data. Its most important function is to process and present simulation results in real time in a clear and useful way for users. It enables a comprehensive assessment of potential threats and analysis of crisis scenarios. The system visualises key indicators in an intuitive form, enabling quick interpretation of results and support for operational activities. Its easy-to-use interface, provides quick access to simulation results and easy situational analysis in dynamically changing conditions. The implementation of SCoreboard increases the effectiveness of crisis management and improves the coordination of services. The tool supports both the operational planning and threat response phases by providing necessary data for strategic decision-making.

Related projects

The SAFE-CITIES project was modelled on European initiatives funded by the European Commission, focusing on public safety, crisis management and new technologies supporting the protection of urban spaces, in order to build a more resilient, smart and safe urban environment in Europe.

ENLETS

European Network of Law Enforcement Technology Services (ENLETS) is a European network of public order services whose main objective is to monitor security-related technologies, disseminate best practices among European law enforcement agencies and initiate research and development projects in the field of combating crime[12]. The network has been operating since 2008 and brings together representatives from 27 EU Member States, the United Kingdom and Norway. It is supported by national contact points (NCPs), which act as liaisons between individual Member States and ENLETS management groups. An important part of the network's activities are the technology interest groups (TIGs), which bring together experts and practitioners in selected technological areas from various European services. One of the groups focuses on issues related to public order. ENLETS plays an important role in promoting cooperation as well as the exchange of knowledge and experience between European public order services. Cooperation between ENLETS and SAFE-CITIES contributes to a better match between technology and the real needs of public safety services.

PRECRISIS

The project was to develop innovative intelligent solutions in the field of public safety, supporting law enforcement agencies, emergency services, safety managers and other stakeholders[13]. Its main objectives were to strengthen public-private cooperation and integrate modern technologies with best practices in security management. As part of PRECRISIS, tools were developed, tested and implemented to enable more effective security in public spaces. The project was based on expert knowledge, good practices and a privacy-by-design approach, ensuring compliance with data protection and privacy requirements. The SAFE-CITIES and PRECRISIS projects shared a common goal: to increase safety in public spaces through the use of innovative technologies, threat analysis and cooperation between multiple stakeholders. The project was completed on 30 April 2025.

[12] *ENLETS*, https://enlets.eu/ [accessed: 14 III 2025].

[13] *PRECRISIS*, https://precrisis-project.eu/ [accessed: 14 III 2025].

SHRINES

The project focused on increasing the safety and security of places of worship. It was a multidisciplinary network of cooperation bringing together people of many faiths[14]. Its main objectives were to raise awareness of the threats occurring in places of worship and to develop innovative technological solutions and preventive measures serving to protect these places. SHRINE was a network connecting various religious communities, law enforcement agencies and local authorities jointly assessed risk factors, exchanged experiences and identified opportunities for cooperation in the area of protecting religious sites. SAFE-CITIES and SHRINES were based on cooperation between public institutions, social organisations and the technology sector, as well as promoted an innovative approach to risk management and critical infrastructure protection. The project was completed on 31 January 2025.

APPRAISE

The initiative aimed to quickly identify and implement measures that would prevent an attack from being carried out or spreading, or would make it possible to stop it. The main objective was to ensure the security of public spaces without restricting citizens' freedoms by minimising or completely eliminating the threat of attacks. The resulting solutions were to provide capabilities for predicting and identifying criminal and terrorist acts as well as to strengthen operational cooperation between services responsible for security before, during and after an attack. During the project, existing technologies were adapted or new ones were created, and the results of the work were tested in near-real conditions. As part of the tests, numerous study visits and pilot projects were organised to check the correct functioning of individual systems and technologies and to improve them on an ongoing basis. Such tests took place in Ljubljana, Bilbao, Gdańsk and Turin.

The conclusion of this initiative that came to end at the beginning of 2024[15] did not mean the end of work on the solutions developed. This is only the beginning of building a compact and uniform warning and analysis system designed to monitor public spaces and alert the appropriate emergency services when a threat arises, as well as to detect anomalies in human behaviour in order to achieve the highest possible level of situational awareness. The efforts of those involved in the APPRAISE project are being continued as part of other initiatives aimed at improving security[16].

---

[14] *SHRINES*, https://shrines-project.eu/ [accessed: 14 III 2025].

[15] *APPRAISE*, https://appraise-h2020.eu/ [accessed: 14 III 2025].

[16] See in more detail: J. Przyjemczak, N. Czyżewska, *APPRAISE project. Building a security system for public spaces*, "Terrorism – Studies, Analiyses, Prevention" 2024, no. 5, pp. 411–421. https://doi.org/10.4467/27204383TER.24.015.19403.

SAFE-CITIES, by focusing on analysing the vulnerability of cities to threats and implementing simulation tools, complemented the activities of APPRAISE and provided additional data and models used to improve the effectiveness of crisis management systems.

Summary

Contemporary cities and urban agglomerations face an increasing number of challenges related to ensuring the safety of public spaces, especially in the face of the growing threat of terrorist attacks. The SAFE-CITIES project was intended to increase resilience to emerging threats and improve the safety of public spaces, including by the use of modern technologies, better coordination of actions and more effective risk management. The systems implemented as part of this project enable the identification of infrastructure weaknesses and the development, based on the data obtained, more effective protection strategies. Thanks to advanced data analysis, they allow for better forecasting of threats and more accurate decision-making. Interactive training and simulations increase the preparedness of services for real incidents and improve their communication and coordination, which speeds up the response to crisis situations.

On 27 March 2025 in Nova Gorica (Slovenia), the solutions developed within the project were demonstrated. For many key security stakeholders, it was a unique opportunity to learn first-hand about technologies aimed at ensuring safety in cities. The participants were able to take part in a special training session based on defined scenarios, aimed at the trying out of the tools and methodologies developed. Such projects contribute to building resilience to threats and provide excellent material for further work in the broadly understood area of security.

Bibliography

Hołub A., *Obiekty ataków terrorystycznych* (Eng. Targets of terrorist attacks), "Przegląd Policyjny" 2018, no. 4, pp. 18–26.

Kaya A., Koc M., *Over-Agglomeration and Its Effects on Sustainable Development: A Case Study on Istanbul*, "Sustainability" 2019, vol. 11, no. 1. https://doi.org/10.3390/su11010135.

Przyjemczak J., *Zadanie specjalne – człowiek, technologia, instytucja* (Eng. Special task – man, technology, institution), pt. 4, J. Przyjemczak (sci. ed.), Gdynia 2024.

Przyjemczak J., Czyżewska N., *APPRAISE project. Building a security system for public spaces*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 411–421. https://doi.org/10.4467/27204383TER.24.015.19403.

Internet sources

APPRAISE, https://appraise-h2020.eu/ [accessed: 14 III 2025].

D-Visor, https://www.d-visor.nl/ [accessed: 13 III 2025].

ENLETS, https://enlets.eu/ [accessed: 14 III 2025].

European Commission SAFE-CITIES project under Horizon Europe: HORIZON-CL-3-2021-FCT-01-07: Enhanced preparedness for attacks in public spaces, https://cordis.europa.eu/project/id/101073945 [accessed: 22 VII 2025].

Europol, *European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [accessed: 13 III 2025].

IANUS Technologies, https://ianus-technologies.com/ [accessed: 13 III 2025].

PRECRISIS, https://precrisis-project.eu/ [accessed: 14 III 2025].

SAFE-CITIES, https://safe-cities.eu/ [accessed: 13 III 2025].

SHRINES, https://shrines-project.eu/ [accessed: 14 III 2025].

STAM – Mastering Excellence, https://www.stamtech.com/ [accessed: 13 III 2025].

Thridium, https://thridium.com/t4s/ [accessed: 13 III 2025].

Małgorzata Wolbach

Senior Project Implementation Specialist at the Polish Platform for Homeland Security (PPHS). She holds a master's degree in homeland security and a bachelor's degree in criminology from the Police Academy in Szczytno. At PPHS, she is responsible for the implementation and execution of projects financed by EU programmes, with a particular emphasis on projects related to hybrid threats and public space security.

Contact: malgorzata.wolbach@ppbw.pl

Jarosław Przyjemczak, PhD

Doctor of social sciences in the field of security sciences, research and teaching staff member at the Institute of Security and Sociology at the Pomeranian University in Słupsk. Retired Deputy Inspector of Police. Participant in numerous domestic and international police and non-police courses and training programmes related to counter-terrorism. He completed, among others, a strategic counter-terrorism and terrorist threats course in Bramshill, United Kingdom, organised by the CEPOL Police College within Europol. Member of the Polish Association for National Security. Author of numerous publications on security, special police units and medical rescue. Scientific editor of the periodical publication Zadanie specjalne – człowiek, technologia, instytucja (Eng. Special Task – Man, Technology, Institution). Initiator and organiser of the educational and training event 'Paramedyk' (Eng. Paramedic). He is a paramedic, lifeguard, diving instructor, shooting and battlefield rescue instructor.

Contact: jarek.przyjemczak@wp.pl

Internal Security Review
2025, no. 32, pp. 345–364

https://doi.org/10.4467/20801335PBW.25.017.22183

ARTICLE

Cybersecurity in the offshore and coastal energy sector of the Republic of Poland

DAVID CYBULSKI

Independent author

https://orcid.org/0009-0003-9195-4407

Abstract

The purpose of the article is to discuss the level of cybersecurity of Poland's offshore and coastal energy sector in the context of planned strategic energy projects. The author presented selected cyberattacks on elements of other states' energy sector, he also discussed, among other things, on the basis of *Energy Policy of Poland until 2040*, Poland's planned activities related to energy infrastructure in the Baltic Sea region. He identified threats to Poland's offshore and coastal energy sector, which include: the activities of APT groups and state-sponsored groups, business rivals and hacktivists. He presented the methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks.

Keywords

cybersecurity, cyberattacks, APT groups, energetics, energy sector

Introduction

With the ever-increasing digitalisation in society, it is essential to continuously develop existing electricity generation capacity. Decision-makers, aware of the need to modernise the state's existing energy infrastructure, to comply with EU regulations[1] and the expected increase in the country's demand for electricity, took steps to define strategic goals and projects for the energy sector in the long term. This led to the creation of a plan for the development of the Polish state's energy sector, the *Energy Policy of Poland until 2040* (hereinafter: PEP2040).

Offensive actions in the Baltic Sea against projects such as Nord Stream 1 and Nord Stream 2[2], undersea C-Lion 1 telecommunication cable or Estlink 2 power connection show how the security of energy infrastructure is under threat these days[3]. The pursuit of national energy projects in the northern Poland and in its exclusive economic zone increases the degree of computerisation of the energy sector's resources. This enhances the enemy's ability to impact the ICT infrastructure of the Polish energetics. Therefore, it is necessary to review the current state of cybersecurity of Poland's developing offshore and coastal energy sector, as well an answer to the question to what extent it is resilient to threats.

One of the ways in which criminals, including terrorists, and international legal entities (states) exert influence is through their direct or indirect impact on the energy sector of the other party, known as the high-value target. An attack, including ICT, that leads to the cessation of the production and distribution of a specific energy demand may result in the temporary or permanent inability of the state to function. In order to mitigate the risk, the Polish legislator decided, on the basis of Article 3 point 2 letter (a) of the *Act of 26 April 2007 on crisis management*, to classify energy supply systems, energy raw materials and fuels as critical infrastructure (CI). The Act on crisis management imposes certain obligations on CI operators to ensure its proper protection. Additionally, under the *Act of 5 July 2018 on the National Cybersecurity System*[4], CI operators have been

---

1 *Polityka energetyczna Polski do 2040 r.* (Eng. Energy Policy of Poland until 2040), Ministry of Climate and Environment, Warszawa 2021, pp. 3–4.

2 W. Lorenz, S. Zaręba, *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2* (Eng. Consequences of the explosion of the Nord Stream 1 and 2 pipelines), Polski Instytut Spraw Międzynarodowych, 29 IX 2022, https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [accessed: 16 VII 2025].

3 K. Buchholz, *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025, https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [accessed: 16 VII 2025].

4 An amendment to this act is currently being processed. See: *Draft law amending the Act on the National Cybersecurity System and certain other acts*, no. UC32, https://www.gov.pl/web/premier/

obliged to ensure an adequate level of cybersecurity within their entities in order to minimise the risk of an ICT security incident.

The purpose of this article is to discuss the level of ICT security in the offshore and coastal energy sector of the RP in the context of planned strategic energy projects. It presents selected cyberattacks on elements of the energy sector in other countries and discusses, among other things, on the basis of the *Energy Policy of Poland until 2040*, Poland's planned actions related to energy infrastructure in the Baltic Sea region. The threats to the Polish offshore and maritime energy sector were identified, including the activities of APT groups[5] and state-sponsored groups, business rivals, hacktivists. The methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks were also presented.

Examples of cyberattacks targeting the energy sector

The energy infrastructure of the states during the first two decades of the 21st century has been the victim of many successful attacks targeting, among other things, ICT systems and networks. The first well-known cyber offensive of this type was an attack carried out in 2010 against the ICT infrastructure of the uranium enrichment centre in the city of Natanz, Iran, using Stuxnet software. The facility was designed for electricity production and to meet Iran's strategic interests in acquiring its own nuclear deterrent capability. The operation, code-named 'Olimpic Games', was carried out in cooperation by, among others, the United States of America and the State of Israel[6]. Since it was not possible to carry out an attack or sabotage the facility by kinetic means, it was decided to launch a cyberattack instead. Potential weak points in the facility's ICT infrastructure were identified, which, if successfully targeted, would prevent or significantly hinder the continuation of the uranium enrichment process in Natanz. The most destructive method of harming Iran's nuclear strategy was considered to be destruction of the uranium enrichment

projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [accessed: 16 VII 2025].

[5] APT (advanced persisted threat) group – a type of advanced cybercriminal group consisting of skilled cybersecurity and ICT specialists who are capable of carrying out advanced ICT attacks on specific entities.

[6] M. Baezner, P. Robin, *Hotspot Analysis: Stuxnet*, Zurych 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf, pp. 7–8 [accessed: 16 VII 2025].

centrifuges[7]. Since the facility did not have direct access to the internet, the attackers decided to infect the internal ICT systems by connecting a USB flash drive with software. The infected centrifuges (more precisely, the programmable logic drivers that controlled them), began to work according to a schedule set by the attackers. Approx. 11–17% of centrifuges at the centre in Natanz were damaged[8], which led to a 15% decrease in nuclear fuel production[9]. In addition, it is suspected that approx. 100 000 other devices were unintentionally infected when the Stuxnet virus unexpectedly began to spread worldwide via the internet[10]. It remains arguably the most well-known case of an attack on ICT system carried out against another country and its energy infrastructure.

Another example of operations in cyberspace targeting elements of a country's energy sector was the 2012 attack on the Kingdom of Saudi Arabia's state-owned company, Saudi Aramco Oil Company (hereinafter: Saudi Aramco), which is the largest resource company in the world. According to calculations by the European Central Bank from 2011, Saudi Arabia was responsible for about 12% of global oil production up to 2009 (with the majority of extraction carried out by Saudi Aramco)[11]. The attack on Saudi Aramco was most likely carried out by cybercriminal group APT33, linked to the Islamic Republic of Iran[12]. The paralysis of the company's ICT systems was carried out using the Shamoon virus. More than 30 000 workstations were infected. This programme spread to other workstations (a behaviour typical of malicious software classified as a worm) and overwrote files in the device's operating system, rendering the infected computer unusable[13].

Ukraine was the victim of another significant attack targeting a country's energy infrastructure. It was carried out on 23 December 2015, against three regional electricity distribution companies: Prykarpattyaoblenergo, Kyivoblenergo and Chernivtsioblenergo. These companies were responsible for the transmission

7 Ibid., p. 4.

8 Ibid., p. 9.

9 T.M. Chen, *Stuxnet, the Real Start of Cyber Warfare?*, "IEEE Network" 2010, vol. 24, no. 6, p. 3. https://doi.org/10.1109/MNET.2010.5634434.

10 N. Falliere, L.O. Murchu, E. Chien, *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf, p. 5 [accessed: 16 VII 2025].

11 A. Nakov, G. Nuño, *Saudi Aramco and the Oil Market*, "Working Paper Series" 2011, no. 1354, p. 9.

12 G. Siboni, S. Kronenfeld, *Iran and Cyberspace Warfare*, "Military and Strategic Affairs" 2012, vol. 4, no. 3, p. 90.

13 It is worth noting, that since November 2022, the Saudi Aramco (Aramco Overseas Company B.V.) owns 30% stake in Gdańsk Refinery. See: *Saudi Aramco przejmie udziały w gdańskiej rafinerii* (Eng. Saudi Aramco to acquire stake in Gdańsk Refinery), CIRE, 12 I 2022, https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [accessed: 14 XII 2024].

of electricity in the Ivano-Frankivsk, Kyiv and Chernivtsi regions, respectively. According to information from the US Cybersecurity and Infrastructure Security Agency (CISA), it is estimated that around 225 000 people were left without electricity for approx. six hours[14]. Moreover, institutions in the government, media, railway transport and mining sectors were also targeted[15]. The attack began (following a phase of open-source reconnaissance of the companies' infrastructure and initial operational preparations) with a phishing campaign distributed to employees of the aforementioned institutions. By opening an attachment in an email, employees unknowingly infected their organisations' networks with a malicious Trojan software[16] called BlackEnergy 3[17]. The malware then connected to C2 servers[18], after which the cybercriminals deployed tools on the infected workstations to extract authentication data and conducted reconnaissance of the attacked companies' internal networks. They gained the ability to log into these systems and networks as well as review the existing ICT infrastructure. After that, they uploaded additional malicious software, called KillDisk, which was to launch upon the operating system restart. The attackers turned off the uninterrupted power supplies (UPS) for selected servers, including those responsible for ICT services, then they activated the power switches. In this way, they disconnected at least 27 electrical substations from the network and cut off electricity supply to aforementioned approx. 225 000 people[19]. Then they uploaded their own patch to the switch management system to stop any further remote control of the switches. After that, the attackers carried out a DoS attack[20] on the call centre of Kyiv's energy distributor. This prevented customers from reporting power outages. The final stage of the operation was the pre-planned shutdown of the UPS devices, which triggered

[14] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20 VII 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [accessed: 28 XI 2024].

[15] J. Styczynski, N. Beach-Westmoreland,*When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [n.p.] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, pp. 5–7, 30–39 [accessed: 16 VII 2025].

[16] Trojan – a type of a computer virus that imitates legitimate programmes and functions.

[17] This is a RAT Trojan (remote access trojan) enabling the attacker to remotely access the victim's workstation.

[18] C2 server (Command & Control) – infrastructure used by the attacker to control and manage systems and devices under his control, including the compromised infrastructure.

[19] SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf, p. 11 [accessed: 6 VIII 2025].

[20] DoS (denial of service) – a type of attack aimed at disrupting the availability of a specific service.

the launch of malicious software called KillDisk upon system reboot. Its purpose was to destroy all data and logs stored on the devices, significantly hindering subsequent analysis that could have identified the causes of the event and possible countermeasures.

It is assumed that the cyberattack on the Ukrainian energy distributors was carried out by at least one cybercriminal state-sponsored group, i.e. APT44, which is linked to the Russian state apparatus[21]. The group is believed to operate under the authority of the Main Intelligence Directorate of the General Staff of the Russian Federation (Russian: Главное управление Генерального штаба Вооруженных Сил Российской Федерации, GRU)[22]. This kind of groups are often a political tool at the disposal of the Russian state.

Another cyberattack targeting various sectors of the Ukrainian state, including the energy sector, took place in 2017. As with the attacks in 2015, these activities were attributed to group APT44[23]. The name of the attack comes from the malicious NotPetya software used in the attack, which was characterised by its ease of lateral movement, disk encryption capabilities and destructive nature. Initially, NotPetya was identified as a type of ransomware[24], however, it did not include any decryption keys that would allow the infected device to be restored to a usable state or its files to remain intact. Such programmes are referred to as wiper. The attack targeted the Ukrainian state and the broadly understood ICT infrastructure located on its territory. However, due to the presence of many branches of foreign companies in Ukraine and the specific nature of the software used (the fastest propagation across the network), the reach of the attack quickly exceeded Ukraine's digital borders and the virus spread globally at a speed not previously observed[25]. In response to cyberattack, the federal government of the United States held six citizens of the Russian Federation criminally accountable – GRU officers[26].

---

[21] J. Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016, https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [accessed: 15 XII 2024].

[22] G. Roncone et al., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, p. 2, 7 [accessed: 16 VII 2025].

[23] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf, pp. 3–4 [accessed: 16 VII 2025].

[24] Ransomware – a type of malicious software that blocks an access to data on a computer or network and demands a ransom for restoring it.

[25] The ease with which NotPetya software was able to infect subsequent workstations and servers was made possible by combining two tools, i.e. Mimikatz and EternalBlue.

[26] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents*…, pp. 3–4.

As mentioned, the attack aimed to infect as many ICT devices in Ukraine as possible and was therefore not directly targeted at the energy sector. However, this sector did not escape the impact of the virus. The victims of the attack included Kyivenergo and Ukrenergo – companies responsible for the distribution of electricity in Ukraine at both the local and national levels[27]. This incident demonstrates that entities in the energy sector must protect themselves not only against targeted threats, but also against general threats faced by other sectors. This significantly broadens the scope of threat monitoring.

In 2023, the Reuters news agency reported that, the Russian Federation made Ukraine's energy sector a priority target of cyberattacks following the invasion[28]. According to reports from this agency, the Security Service of Ukraine (Ukrainian: Служба безпеки України, SBU) determined that, Russia carries out an average of 10 attacks per day. These includes attempts to disable parts of Ukraine's energy infrastructure. This showed that cyberspace functions like a system of interconnected vessels. An example is the attack on a Ukrainian satellite, which resulted in the unavailability of the remote monitoring system for more than 5800 wind turbines in Germany[29].

Since the beginning of the invasion of Ukraine, offensive operations in cyberspace targeting the energy infrastructure of other European countries have been carried out. One of them was a series of attacks conducted in 2023 against Danish CI operators. These attacks were described in a report by SektorCERT – the computer security incident response team responsible for protecting Denmark's CI sector[30]. According to the report, this was the largest and most costly attack ever carried out against this infrastructure. The perpetrators targeted parts of industrial control systems (ICS) in companies and gained access to the ICT infrastructure of 22 entities within the energy sector. All the attacks were carried out simultaneously, they were prepared carefully well in advance and the attackers had knowledge of where to conduct offensive operations[31]. SektorCERT faced the challenge of simultaneously handling incidents affecting 16 attacked institutions, along with additional six

[27] C. Krasznay, *Case Study: The NotPetya Campaign*, in: *Információ- és kiberbiztonság*, B. Török (ed.), Budapest 2020, p. 486.

[28] N. Buli, N. Chestney, Ch. Steitz, *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023, https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [accessed: 5 XII 2024].

[29] Ibid.

[30] SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [accessed: 5 XII 2024].

[31] Ibid., p. 10.

that were targeted during a second wave of attacks. SektorCERT attributed these subsequent attacks to another, as yet unidentified, cybercriminal group, which was employing new attack tools, including numerous 0-day vulnerabilities[32]. This indicates a high level of skills in discovering such vulnerabilities or financial resources to purchase information about security flaws from other cybercriminal groups[33]. It is suspected that group APT44[34] was behind the attacks (or at least some of them). Notably, SektorCERT determined that the sources of the attacks at their peak originated from IP addresses that, according to geolocation data, pointed to Poland and Ukraine[35].

Identification of energy sector resources in the maritime area of the RP

In PEP2040, a significant emphasis has been placed on the country's offshore and coastal energy subsector. This is demonstrated by the following actions listed in this document:

- establishment of offshore wind farms in Poland's exclusive economic zone, which are expected to reach capacity to generate electricity of approx. 11 GW by 2040,
- creation of main installation terminal (port) specialising in servicing the supply chain for offshore wind farms,
- expansion of the transmission network in the northern and north-western parts of Poland in order to adapt the Polish power system for receiving and transmitting energy generated, among other sources, by offshore wind power plants,
- import of natural gas via the Baltic Pipe since 2022. Possible import of 10 billion m^3 of natural gas and an export – 3 billion m^3,
- increase of the regasification capacity of the LNG terminal in Świnoujście to 8.3 billion m^3 of natural gas,

[32] 0-day vulnerability – a vulnerability that has not been publicly acknowledged by the vendor and for which no official software update exists to mitigate the vulnerability.

[33] *Behind the Rise of the Million Dollar Zero-Day Market*, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [accessed: 14 XII 2024].

[34] *The attack against Danish, critical infrastructure*…, pp. 14–16.

[35] Ibid., p. 26.

- construction of a natural gas regasification terminal in the Gulf of Gdańsk (FSRU terminal[36]) with a nominal capacity of 4.5 billion m^3 of gas,
- expansion of gas pipelines in the northern and central parts of Poland to enable the transport of gas from the FSRU terminal further inland,
- possible expansion of the Kosakowo Underground Gas Storage Facility in Dębogórze,
- increasing the crude oil storage capacity at the oil terminal and the PERN base in Gdańsk to approx. 1.9 billion m^3,
- construction of a second line of the Pomeranian Pipeline to optimise the transport of crude oil from the Naftoport in Gdańsk further inland,
- increasing the production capacity of the Gdańsk Refinery in the area of petrochemicals,
- extraction of crude oil from deposits located in the Baltic Sea and on the Norwegian continental shelf,
- identification of new crude oil and natural gas deposits in the Baltic Sea and on the Norwegian continental shelf,
- enabling LNG bunkering in Poland's four largest ports: Gdańsk, Gdynia, Szczecin and Świnoujście,
- establishment of a submarine direct current connection between Poland and Lithuania (and more broadly, the Baltic States) with a planned capacity of 700 MW (220 kV),
- potential use of hydropower resources.

This list could be supplemented with existing energy infrastructure that is not mentioned in PEP2040 but is, to some extent, concentrated around the country's offshore or coastal energy sector – such as the submarine interconnection between Sweden and Poland via the SwePol Link cable line with a capacity of 600 MW (450 kV) as well as crude oil and liquid fuel storage facilities: Dębogórze, Świnoujście, Trzebież, Szczecin, Koszalin, Ugoszcz, Gdańsk. It is likely that almost all of Poland's demand for natural gas will be covered by supplies from the direction of the Baltic Sea, primarily through the Baltic Pipe. Offshore wind farms are expected to become one of the three main pillars of Poland's future energy mix, meeting approx. 18% of the country's energy demand[37]. In addition, the electricity generated by the planned nuclear power plant, which is to be located in the Pomeranian Voivodeship, should also be taken into account, as the power system (mainly the transmission

[36] FSRU (floating storage regasification unit) – a floating unit used for regasification of natural gas.

[37] *Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski* (Eng. Offshore wind farms key to Poland's energy transition), Polityka, 2023, https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [accessed: 15 XII 2024].

infrastructure) being developed in the northern part of Poland will be expanded and adapted to share transmission infrastructure with this nuclear power plant as well as, among others, offshore wind farms located in at least two shoals: the Middle Bank (Ławica Środkowa) and the Słupsk Bank (Ławica Słupska). This means that any cybersecurity threats related to the distribution of electricity from the planned offshore wind farms and the nuclear power plant will have a significant impact on both projects, considerably hindering their operation.

As part of the identification of energy sector resources in the maritime area of the RP and the related threats, additional entities that influence the shape of Poland's energy sector in the context of offshore and coastal energy have been taken into account, namely: the maritime offices in Gdynia and Szczecin, as well as the Ministry of Climate and Environment (as the office serving the minister responsible for the 'energy' area of public administration)[38].

Types of potential adversaries for the ICT resources of companies in the Polish energy sector

It can be anticipated that the investments undertaken in the Polish energy sector will generate relatively high profits, particularly for companies that form the backbone of this sector. This may encourage cybercriminals to carry out offensive actions against these entities. However, such actions do not necessarily have to be motivated by financial gain alone. Significant threats may also come from APT groups, state-sponsored or state-linked cybercriminal groups, business rivals and hacktivists.

The greatest threat that should be considered when assessing the resilience of one's own ICT systems and networks currently comes from APT groups. The aim of their precise attacks are usually the most critical companies and institutions. These operations can last for many months or even years, involving careful reconnaissance of the target, preparation of dedicated tools tailored to the victim's identified weaknesses, maintaining gained access to the systems and evading detection.

Another type of threat comes from cybercriminal groups that are state-sponsored or state-affiliated. They often operate (like APT groups) on a contractual basis, including selling their services to other actors. The aim of state-sponsored actors, which are not a part of APT groups, is more likely to involve short-term

[38] § 1(2) point 1 of the *Regulation of the Prime Minister of 19 December 2023 on the detailed scope of activities of the Minister of Climate and Environment*.

and/or medium-term activities focused, for example, on disrupting the operations of an organisation or conducting propaganda.

Business rivals may pose a threat in the context of stealing or otherwise attempting to obtain information about the status of ongoing projects and the companies carrying them out. This constitutes unfair competition: based on data theft, a business rival may attempt to harm the planned investment, the company executing it or adjust their own investment plans in response to the adversary's actions. Such harmful activities can be carried out directly by the business rival alone, but it is much more common practice to outsource this to an external actor (cybercriminal group) with no formal connection to the client.

The last group mentioned are hacktivists, who carry out their activities in cyberspace for ideological reasons. Their motivation to take action usually stems from political events. Hacktivists can attack both government institutions in the heat of the moment (e.g. after a decision by the authorities that they did not accept) or targeting companies whose business, environmental, pricing or public relations policies provokes their opposition.

The actors described above may attempt sabotage, infiltration or destruction of ICT infrastructure supporting energy projects. Therefore, it is essential that the entities responsible for these projects and decision-makers conduct risk analyses and develop security plans, so that the threat of a cyberattack can be reduced to an acceptable level.

Moreover, it is also worth noting that the presence of companies with foreign capital in the Polish energy market may encourage adversaries to carry out offensive actions targeting the capital invested in energy projects in Poland. One example is the Gdańsk Refinery, in which a significant stake is owned by a subsidiary of the Saudi Aramco capital group. Such activities may be of particular interest to hacktivists and business rivals.

ICT resources in the offshore energy sector enterprises and types of attacks against them

The resources that an organisation in the energy sector, including offshore energy, must protect to prevent a cybersecurity incident can be divided into two groups of the so-called ICT infrastructure environments. These are corporate environments and industrial control system environments.

Different systems and devices, due to the nature of their functions, may be used for office tasks and for activities that ensure the operation of industrial machinery necessary for the production or distribution of electricity. Although

in theory it is possible to completely separate these two environments, in practice they are often interdependent. An example of this is the need for authorised user from the corporate network or a user from external company providing machine maintenance services to take corrective actions in the industrial control system environment through remote access.

In a mature organisation, the corporate environment typically uses such systems and devices as: its own domain, domain controller, web servers, email servers, database servers, business applications and endpoints (workstations, printers) etc. Regardless of the specifics of the corporate environment, it should be adequately protected due to the risks to the continuity of business operations, its impact on the industrial control systems and its dependence on them.

In the industrial control system environment of a large enterprise, which includes entities responsible for the production and distribution of electric energy, there should be systems and devices such as: remote terminal units (RTU), HMI interfaces[39], SCADA system[40], controllers, PLCs[41], signal converters, optical diodes, as well as sensors and detectors. These, in turn, should be protected by systems and devices similar to those used in corporate environments or specialised for industrial control system environments, depending on specific needs. The examples presented are not exhaustive due to the varying nature of environments in different enterprises, which may adopt diverse approaches to the design and maintenance of their ICT infrastructure, depending on available financial and human resources.

Common problems occurring in both environments include: outdated software versions that are vulnerable to attacks[42], a lack of user awareness about threats as well as the failure to apply good practices and standards in the field of ICT and cybersecurity. For example, in an attack using malware WannaCry, outdated software in the form of the SMBv1 protocol was used[43].

A relatively common type of attack targeting industrial control system environments is a supply chain attack. Attackers take such actions when are unable to gain direct access – that is, a point of entry – to the target infrastructure.

---

[39] HMI (human-machine interface) – interface between the machine and its operator, most often in the form of a graphical representation of the process.

[40] SCADA (supervisory control and data acquisition) – ICT system supervising the course of the production process.

[41] PLC (programmable logic controller) – used to control the operation of a machine.

[42] *Outdated Software*, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [accessed: 15 XII 2024].

[43] M. Akbanov, V.G. Vassilakis, M.D. Logothetis, *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, "Journal of Telecommunications and Information Technology" 2019, vol. 75, no. 1, pp. 114–115. https://doi.org/10.26636/jtit.2019.130218.

Smaller subcontractors, who usually have proportionally lower investments in their company's security, are an easier target. Such an attack can occur, for example, when the supplier, under an agreement with the organisation, has remote access to its industrial ICT infrastructure. In this way, attackers can obtain authentication data for service accounts within the organisation's industrial control system and conduct further offensive operations directly there.

Protective mechanisms for the ICT resources of Polish energy sector

Ways to secure ICT resources of Polish energy sector, including the offshore and coastal energy sector, can be divided into individual and state-level security measures related to the activities of specific services and institutions.

Individual security measures of CI operator

Important ways to counteract the effects of a potential attack include, among others, the use of firewall devices, network segmentation allowing potentially compromised devices to be isolated, and strict control of user account privileges (identity and access management / privileged access management, IAM/PAM) in line with best practices of industry environment[44]. It happens that control panels for industrial control system infrastructure are accessible from the internet, sometimes even without requiring user authentication, which poses a serious risk to such a system[45].

Due to the possibility of mutual interaction between corporate environments and industrial control system environments, they should be secured in a consistent manner that does not treat either area as a less important dimension of security. Both environments usually utilise shared elements of the enterprise's ICT infrastructure, such as the same domain. Therefore, both can become victims of an attack if not properly secured. These solutions should be protected by, among other things, devices and systems such as firewalls, multi-factor authentication (MFA), sytems: Anti-DDoS; security information and event management (SIEM); security orchestration, automation and response (SOAR); intrusion detection system (IDS); intrusion prevention system (IPS); data loss prevention (DLP); endpoint detection and response (EDR); antivirus software, as well as IAM/PAM solutions, servers with backup copies (backup), email filters and UPS.

---

[44] *Security and Privacy Controls For Information Systems and Organizations*, NIST, September 2020, pp. 19–20. https://doi.org/10.6028/NIST.SP.800-53r5.

[45] *Raport roczny z działalności CERT POLSKA 2023* (Eng. CERT Polska Annual Report for 2023), https://cert.pl/uploads/docs/Raport_CP_2023.pdf, pp. 57–58 [accessed: 16 VII 2025].

Importantly, according to the draft law amending the Act on crisis management and certain other acts currently under consideration, it is planned, among other things, to impose minimum cybersecurity standards on CI operators[46]. This may result in improved ICT security for institutions that are crucial from the state's perspective. These requirements will be based on the results of a risk assessment of organisational and technical solutions carried out by the given entity. This is a new approach that takes into account the evolution of threats and the time-based depreciation of implemented safeguards, in order to ensure the continuity of security measures.

Furthermore, under the draft law amending the Act on the National Cybersecurity System[47], it is planned to conduct risk assessments related to the supply chain, including suppliers and business customers with whom the entity intends to cooperate. Such an assessment will aim to ensure the security of the entrepreneur's networks and ICT systems against potential supply chain attacks. The proposed amendment may still change in scope regarding risk assessment, especially the provisions concerning entities designated as high-risk suppliers. Changes may be dictated by, among other things, public concerns related to submitted proposals, including arbitrary and politically motivated decisions that could result in an entity being classified as a high-risk supplier[48].

State-level security measures for CI operator

Despite the growing threat of attacks on the country's CI, it is not the role of an entrepreneur to allocate all company revenues to making the enterprise resilient to a given type of threat. It is the state that should protect its interests, including by ensuring the continuity of its functioning through the security of electricity generation and distribution processes within its territory. These tasks are carried out, among others, by the Armed Forces of the RP under Article 26 of the *Constitution of the Republic of Poland of 2 April 1997* and subordinate legislation, the Internal Security Agency and the Foreign Intelligence Agency based on Articles 5 and 6 of the *Act of 24 May 2002 on the Internal Security Agency and*

[46] *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw* (Eng. Draft law amending the Act on the crisis management and certain other acts), no. UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [accessed: 16 VII 2025].

[47] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa...*

[48] M. Fraser, *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki* (Eng. Business groups criticise the National Cybersecurity System amendment. High-risk suppliers to be reconsidered), CyberDefence24, 9 XI 2021, https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [accessed: 18 VII 2025].

the Foreign Intelligence Agency as well as the Police based on Article 1(2) points 2–4 of the *Act of 6 April 1990 on the Police*. The role of these institutions is to identify threats to national security and to respond accordingly.

Activities related to the protection of the interests of Poland's offshore and coastal energy sector are carried out by, among others:

- the Polish Navy – as the branch of the armed forces responsible for ensuring the country's maritime security,
- the Maritime Border Guard Unit – which provides ongoing supervision and control of maritime areas,
- Special Forces in the form of military units GROM and Formoza – which enable a rapid response to asymmetric kinetic operations,
- the Internal Security Agency – carrying out preventive tasks related to national security, CI and economic interests of the RP,
- the Foreign Intelligence Agency – carrying out tasks to counter external threats to the RP and its interests and property,
- the Police – as an authority tasked with safeguarding national security and public order,
- CSIRT GOV – responsible for protecting the state's CI in the context of cybersecurity threats.

Most of the listed institutions carry out protective tasks, mainly related to kinetic threats, both symmetric and asymmetric. In turn, CSIRT GOV, which stands for the Computer Security Incident Response Team, operating within the framework of the Internal Security Agency, carries out its activities on the basis of Article 26 points 3 and 7 as well as Article 27 point 1 of the Act on the National Cybersecurity System and protects, among others, CI operators in the state's digital sphere. This enables assistance to be provided to these operators in the event of attacks by, among others, APT and state-sponsored groups.

It is worth noting that Poland recognises threats to its interests in the Baltic Sea region and pursues a policy aimed at securing them. For instance, a new combat team within the Formoza Military Unit was formed, which is intended to enable more effective counteraction against kinetic threats of an asymmetric nature in the Baltic Sea area[49].

[49] *Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej* (Eng. Another combat team is being formed in Formoza. It is a response to contemporary military and non-military threats to the operation of critical infrastructure), Ministerstwo Obrony Narodowej, 22 VIII 2023, https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [accessed: 10 XII 2024].

It should be noted that probably not all of energy facilities and investments mentioned in the article will be included in the CI, based on the criteria specified in classified Annex No. 2 to the National Critical Infrastructure Protection Program[50]. This may result from the fact that these facilities, still under development, may not yet have undergone the procedure for selecting CI objects from among the state's overall infrastructure. Due to the unique nature of investments such as offshore wind farms, one could consider whether Poland should act proactively and designate these facilities, their installations or parts thereof, as CI even before their completion. This would enable the state to protect the infrastructure as soon as it is built or modernised. Such an approach would constitute a comprehensive strategy for safeguarding the state's energy interests.

Summary

Due to threats posed primarily by APT groups and state-sponsored groups to current and planned investments in offshore and coastal energy infrastructure, it is necessary for the Polish state to provide support to ensure a predefined level of security for exposed organisations and their ICT infrastructure, including security in cyberspace. For strategic projects implemented under PEP2040, ICT infrastructure should be secured from the very beginning of its development, in line with *security by design* approach. This infrastructure should be created in accordance with industry best practices in the cybersecurity industry, in order to minimise the risk of effective attack.

Based on the presented materials, it can be inferred that the Polish state is currently only basically prepared to ensure cybersecurity for the offshore and coastal energy sector. In the era of ruthless competition in cyberspace, this may prove insufficient, especially considering the threats that may emerge in the future and the available ways to mitigate them. There is a lack of proactive measures to ensure that energy projects of strategic importance to national security are secured from the very beginning of their development cycle (planning and conceptual phases). Furthermore, as indicated, a threat may materialise not only through a direct cyberattack on an organisation but also – which is becoming increasingly common – through an attack on the supply chain. The subcontractor may turn out to be a convenient entry point to the target organisation's infrastructure. Without expansion of security measures by both the CI operators and the state, the security

[50] *Narodowy Program Ochrony Infrastruktury Krytycznej* (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

may prove ineffective and inadequate in the face of evolving realities. It may be necessary to assess the impact of new regulations, such as amendments to the Act on crisis management and the Act on National Cybersecurity System, to evaluate their effectiveness in addressing current and future cybersecurity challenges. This could enable a more comprehensive approach to the issue.

Bibliography

Akbanov M., Vassilakis V.G., Logothetis M.D., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, "Journal of Telecommunications and Information Technology" 2019, vol. 75, no. 1, pp. 113–124. https://doi.org/10.26636/jtit.2019.130218.

Chen T.M., *Stuxnet, the Real Start of Cyber Warfare?*, "IEEE Network" 2010, vol. 24, no. 6, pp. 2–3. https://doi.org/10.1109/MNET.2010.5634434.

Krasznay C., *Case Study: The NotPetya Campaign*, in: *Információ- és kiberbiztonság*, B. Török (ed.), Budapest 2020.

Nakov A., Nuño G., *Saudi Aramco and the Oil Market*, "Working Paper Series" 2011, no. 1354.

Security and Privacy Controls For Information Systems and Organizations, NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Siboni G., Kronenfeld S., *Iran and Cyberspace Warfare*, "Military and Strategic Affairs" 2012, vol. 4, no. 3, pp. 77–99.

Internet sources

Baezner M., Robin P., *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf [accessed: 16 VII 2025].

Behind the Rise of the Million Dollar Zero-Day Market, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [accessed: 14 XII 2024].

Buchholz K., *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025, https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [accessed: 16 VII 2025].

Buli N., Chestney N., Steitz Ch., *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023, https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [accessed: 5 XII 2024].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20 VII 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [accessed: 28 XI 2024].

Falliere N., Murchu L.O., Chien E., *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf [accessed: 16 VII 2025].

Fraser M., *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki* (Eng. Business groups criticise the National Cybersecurity System amendment. High-risk suppliers to be reconsidered), CyberDefence24, 9 XI 2021, https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [accessed: 18 VII 2025].

Hultquist J., *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016, https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [accessed: 15 XII 2024].

Kerttunen M., Hemmelskamp J., *Major Cyber Incidents: NotPetya*, March 2023, https://europoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf [accessed: 16 VII 2025].

Lorenz W., Zaręba S., *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2* (Eng. Consequences of the explosion of the Nord Stream 1 and 2 pipelines), Polski Instytut Spraw Międzynarodowych, 29 IX 2022, https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [accessed: 16 VII 2025].

Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski (Eng. Offshore wind farms key to Poland's energy transition), Polityka, 2023, https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [accessed: 15 XII 2024].

Outdated Software, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [accessed: 15 XII 2024].

Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej (Eng. Another combat team is being formed in Formoza. It is a response to contemporary military and non-military threats to the operation of critical infrastructure), Ministerstwo Obrony Narodowej, 22 VIII 2023, https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [accessed: 10 XII 2024].

Roncone G., Black D., Wolfram J., McLellan T., Simonian N., Hall R., Prokopenkov A., Perez D., Aytes L., Wahlstrom A., *APT44: Unearthing Sandworm*, 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [accessed: 16 VII 2025].

SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS--and-Electricity-Information-Sharing-and.pdf [accessed: 6 VIII 2025].

Saudi Aramco przejmie udziały w gdańskiej rafinerii (Eng. Saudi Aramco to acquire stake in Gdańsk refinery), CIRE, 12 I 2022, https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [accessed: 14 XII 2024].

SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [accessed: 5 XII 2024].

Styczynski J., Beach-Westmoreland N., *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [n.p.] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [accessed: 16 VII 2025].

Legal acts

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

Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws of 2024, item 1077, as amended).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text, Journal of Laws of 2025, item 902).

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

Regulation of the Prime Minister of 19 December 2023 on the detailed scope of activities of the Minister of Climate and Environment (Journal of Laws of 2023, item 2726).

Other documents

Narodowy Program Ochrony Infrastruktury Krytycznej (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

Polityka energetyczna Polski do 2040 r. (Eng. Energy Policy of Poland until 2040), Ministry of Climate and Environment, Warszawa 2021.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Eng. Draft law amending the Act on the National Cybersecurity System and certain other acts), no. UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [accessed: 16 VII 2025].

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (Eng. Draft law amending the Act on the crisis management and certain other acts), no. UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [accessed: 16 VII 2025].

Raport roczny z działalności CERT POLSKA 2023 (Eng. CERT Polska Annual Report for 2023), https://cert.pl/uploads/docs/Raport_CP_2023.pdf [accessed: 16 VII 2025].

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

Internal Security Review
2025, no. 32, pp. 365–400

https://doi.org/10.4467/20801335PBW.25.018.22184

ARTICLE

Anti-state movements in Poland and their impact on the public and banking sectors

PATRYK KRÓL

Independent author

https://orcid.org/0000-0003-4079-8849

Abstract

The purpose of this article is to present contemporary anti-state circles in Poland that are inspired by the US sovereign citizen movement. The author discusses their ideology, the methods of operation used, scale of popularity and the threats they may potentially pose to the legal and social order in Poland. In the study, the author used a review of scientific literature method, as well as an analysis of propaganda and pseudo-legal materials published by Polish anti-government organisations. Polish sovereign citizen movements, such as Zawodowy Polak (Professional Pole) or Ruch II RP (the Second Polish Republic movement) movements, have been shown to adapt the US methods to local contexts. The author presented proposals for preventive measures that could limit the impact of these movements on Polish society and provide better protection for state structures, including the banking sector. He also suggested implementing educational and legislative measures as well as monitoring the activities of these groups.

Keywords

anti-state movements, sovereign citizens, pseudo-law, radicalisation, state destabilisation

Introduction

The sovereign citizen movement is an anti-government social phenomenon that grew out of the US anti-tax movements as well as the radical and racist anti-state organisations of the 1960s and 1970s[1]. As it developed, its proponents began to use what is known as pseudo-law, i.e. a set of fictitious procedures and legal arguments, in order to undermine the existing legal order. The movement's supporters, in order to avoid obligations to the state, such as paying taxes, fines or other administrative obligations, formulate complicated, often baseless letters and carry out pseudo-legal actions. They believe that in this way they will block or at least delay the application of the law against them[2].

The sovereign citizen movement is being treated with increasing seriousness by the US authorities. The Federal Bureau of Investigation (FBI) took note of the aggressive behaviour of its members and classified it as a terrorist and extremist movement in 2010[3]. Research by US psychiatrists also confirms that sovereign citizen movement is one of the largest anti-government or domestic terrorism-related groups in the United States. Between 2014 and 2024, more than a dozen public officials were injured or killed by those adhering to the sovereign citizen ideology. Research using Terrorist Radicalization Assessment Protocol (TRAP-18) has shown that there is a link between behavioural characteristics of members of this movement and an increase in the risk of escalation of violence. After analysing both violent and non-agressive behaviours of people associated with the sovereign citizen movement, it was found that the sum of scores in the TRAP-18 is a good indicator of an individual's predisposition for terrorist activity. This especially concerns so-called lone wolves – terrorists who independently plan and organise terrorist attacks. Therefore, it is worthwhile to develop research on the use of TRAP-18 in assessing threats posed by groups that exhibit tendencies toward violence[4].

---

1 S.A. Kent, *Freemen, Sovereign Citizens, and the Challenge to Public Order in British Heritage Countries*, "International Journal of Cultic Studies" 2015, no. 6, https://skent.ualberta.ca/wp-content/uploads/2015/06/Freemen-Internl-J-of-Cultic-Studies.pdf, pp. 1–15 [accessed: 25 X 2024].

2 A. Morozov, R. Bruinsma, J. Rudnick, *Assembly of viruses and the pseudo law of mass action*, "Biophysical Journal" 2009, vol. 96, no. 3, pp. 419a–420a.

3 FBI, *Domestic terrorism. The Sovereign Citizen Movement*, 13 IV 2010, https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement [accessed: 15 XII 2024].

4 D.J. Challacombe, P.A. Lucas, *Postdicting violence with sovereign citizen actors: An exploratory test of the TRAP-18*, "Journal of Threat Assessment and Management" 2019, vol. 6, no. 1, pp. 51–59. https://doi.org/10.1037/tam0000105.

According to FBI reports, representatives of the movement have repeatedly used violence, including murders[5] and physical assaults. They have been known to threaten judges, law enforcement officers and employees of state institutions[6], committed financial fraud[7] and used forged documents, including passports, licence plates, driver's licences and counterfeit money[8]. The members of the movement also impersonate police officers or diplomats and thus try to obtain undue privileges or immunities.

In Poland, movements of an anti-state or alt-state nature[9] have begun to emerge over the last few decades. In many cases, they are inspired – consciously or not – by the US sovereign citizen movement both in ideological and organisational terms. In the first years of transition in Poland, isolated initiatives of this type were recorded, such as the activities of Marek Świętopełk-Zawadzki, marginal in nature. Earlier, during the People's Republic of Poland, these types of movements did not emerge due to limited access to information from abroad and the lack of favourable political and social conditions. Ideologically similar activities, such as those of Juliusz Nowina-Sokolnicki – from whom Jan Potocki, the founder of the Ruch II RP described later in the article, draws his legitimacy – were developing in exile at this time.

It is only in the 21st century that anti-state movements have started to show more activity. This was particularly evident during COVID-19 pandemic. The introduction of restrictions and the shutdown of many sectors of public life and the economy caused frustration in the society and led to growing opposition

---

5 *Murder of Dallas Police Officer Marks Latest in String of Violent Sovereign Citizen Encounters with Law Enforcement*, Anti-Defamation League, 9 XII 2024, https://www.adl.org/resources/article/murder-dallas-police-officer-marks-latest-string-violent-sovereign-citizen [accessed: 1 I 2025].

6 FBI's Counterterrorism Analysis Section, *Sovereign Citizens. A Growing Domestic Threat to Law Enforcement*, FBI Law Enforcement Bulletin, 1 IX 2011, https://leb.fbi.gov/articles/featured-articles/sovereign-citizens-a-growing-domestic-threat-to-law-enforcement [accessed: 1 I 2025].

7 IRS Criminal Investigation, *Sovereign citizen sentenced to 9 years in prison for $3.4 million tax fraud scheme, filing a false lien, and absconding while on bond*, Press Release, 22 V 2024, https://www.irs.gov/compliance/criminal-investigation/sovereign-citizen-sentenced-to-9-years-in-prison-for-3-point-4-million-tax-fraud-scheme-filing-a-false-lien-and-absconding-while-on-bond [accessed: 1 VII 2025].

8 C. Meyer, *5 Common Crimes Committed by Sovereign Citizens*, Police1, 6 IX 2024, https://www.police1.com/community/articles/5-common-crimes-committed-by-sovereign-citizens-1KKxo-42li5FVeANM/ [accessed: 1 I 2025].

9 The author introduces this term for the purposes of the article. By alt-state movements, he means not only those that challenge the legality of the authorities and the legal order but also those that attempt to create their own states within the state, with their own documents, symbols, offices or laws. A characteristic feature of these movements is their aim to ignore the state order or to replace it with a parallel structure based on their own rules.

to the state apparatus of control. The sovereign citizen movement took advantage of this moment, offering an alternative rhetoric of freedom and a narrative in which the state is portrayed as an oppressive structure lacking genuine legitimacy.

In Poland, sovereign citizen organisations remain a niche phenomenon. However, their popularity and tendency towards radicalisation are increasing. Supporters of these groups question the legitimacy of the Polish authorities and introduce their own structures, i.e. alternative authorities, courts, they create their own model documents and legal arguments, which they use to hinder the work of public institutions and to voice opposition to law enforcement authorities. According to the author, these activities are increasingly taking on an organised character and attracting new supporters, mainly through the internet, where these groups spread scepticism towards the law and those in power.

The author discusses the ideological roots of Polish sovereign citizens, their methods of operation and their impact on the order in state. He also outlines how these movements in Poland adapt the US models to domestic context and what communication strategies and tools they use in their activities. He presents the origins and recent activities of selected sovereign citizens groups, as well as methods they use to spread propaganda. He also proposes preventive measures that could limit destabilising impact of sovereign citizens initiatives on the functioning of state institutions, including legislative changes and strategies for responding to potential threats arising from their activities. Moreover, he discusses proposals for legal regulations aimed at combating anti-state propaganda and protecting society from the influence of ideologies related with the sovereign citizen movement.

The beliefs and pseudo-legal methods of the sovereign citizen movement

Pseudo-law, which is one of the foundations of the sovereign citizen movement, has developed as a distinctive and complex system of methods and beliefs in the literature even described as an esoteric or magical system[10]. Its aim is to destabilise state institutions and avoid legal responsibility by the movement's supporters. It involves, among others, the creation of documents and letters with absurd content, which are submitted to offices with the belief that they have legal force. The movement's representatives assume that through the right choice of words, the structure of the text, as well as the form of the signature, one can symbolically and legally

[10] It is not a uniform set of principles, it encompasses a variety of practices, techniques and beliefs that are often contradictory.

separate oneself from the state system. Documents prepared by supporters of the movement are often signed in red ink to signify that the signatory is a physical and real 'flesh and blood person', as opposed to a signature in black or blue, which is supposed to signify a 'legal person' or 'legal fiction'[11] (the differences between a natural person and a legal person are presented in Table 1). The use of the red colour refers to the practice in some US states of marking important documents. It is treated almost like a magical symbol that distinguishes the real human being from the abstract legal entity.

Table 1. Differences between a legal person and a natural person according to sovereign citizen ideology.

	Legal person	**Natural person**
Name in English	*strawman*, *legal person*, *corporate entity*, *fictional entity*	*natural person*, *living man/woman*, *living soul*, *flesh and blood human*
Character	fictitious identity created by the state	real, living being
Spelling (examples)	capital letters, e.g. JAN KOWALSKI	with a note before the name, e.g. Jan from the Kowalski family, often written in red
Source of existence	birth certificate, registration in the country	birth
Legal subordination	is subject to public law (administrative, tax etc.)	is subject only to common law
Status by country	recognised as a citizen, taxpayer, legal entity	not recognised as a separate legal entity (according to ideology, but not in law)
Representation	is represented by a PESEL number (personal identification number), NIP number (tax identification number), official documents	free entity that has no official representation
Entity type	legal structure, social construct, such as a company or a partnership	person with a soul, capable of sovereign action

Source: own elaboration.

[11] *The Sovereigns: A Dictionary of the Peculiar*, Southern Poverty Law Center, 1 VIII 2010, https://www.splcenter.org/fighting-hate/intelligence-report/2010/sovereigns-dictionary-peculiar [accessed: 14 VII 2024].

The distinction between a legal person and a natural person, which is one of the movement's dogmas, relates to the strawman theory, according to which every human being has two persons: a legal and a physical person, and that legal obligations and tax liabilities apply only to the former[12]. Supporters of this theory believe that by using appropriate forms of signature, such as John Robert: Doe in place of the commonly used John Robert Doe, they can avoid the liabilities associated with a legal entity. It is also a common practice to place the copyright symbol (©) next to the name and the surname. This allegedly protects against the use of this data by other individuals or institutions without the owner's consent[13]. Members of the movement also add the Latin *sui iuris* ([persons] of one's own right) after their name to signify individual autonomy and a refusal to recognise regulations imposed by state authorities.

Another widespread element of pseudo-legal beliefs is the conviction that the federal government opens a secret account for each person at birth in the national treasury, where the person's projected future earnings are secured. The movement's supporters are making attempts to reclaim access to these funds. To do so, for example, they file a form 1099-OID with false data with US authorities, which amounts to tax fraud. In 2016, the movement defrauded the government of approx. USD 43 million using this method[14].

Another manipulation of the sovereign citizen movement is a theory related to maritime law. It derives from a misinterpretation of a 17th century British piece of legislation, the *Cestui Que Vie Act* of 1666[15]. This act allowed for a person lost at sea to be declared dead after seven years of disappearance, e.g. at sea, where finding person's body was impossible[16]. Supporters of the movement citing the document

[12] On this theory, see in more detail: *Redemption Theory/Strawman Theory*, Anti-Defamation League, https://extremismterms.adl.org/glossary/redemption-theorystrawman-theory [accessed: 14 VII 2025].

[13] *The Sovereign Citizen Movement: Common Documentary Identifiers & Examples*, Anti-Defamation League, 5 XII 2016, https://www.adl.org/resources/reports/the-sovereign-citizen-movement-common-documentary-identifiers-examples [accessed: 25 X 2024].

[14] A. Powers, *How Sovereign Citizens Helped Swindle $1 Billion From the Government They Disavow*, The New York Times, 29 III 2019, https://www.nytimes.com/2019/03/29/business/sovereign-citizens-financial-crime.html [accessed: 25 X 2024].

[15] Ch. Koppelman, *Construction as Resistance: Constructing a desired and envisioned future to perceived oppression for the sovereign citizen milieu in the Netherlands*, Utrecht University 2024, https://studenttheses.uu.nl/bitstream/handle/20.500.12932/47667/h.c.koppelman_6919642_thesis_CSHR.pdf?sequence=1&isAllowed=y [accessed: 1 VII 2025].

[16] Ch.M Sarteschi, *Sovereign Citizens and QAnon: The Increasing Overlaps with a Focus on Child Protective Service (CPS) Cases*, "International Journal of Coercion, Abuse & Manipulation" 2023, no. 6. DOI:10.54208/1000/0006/006.

claim that once a child reaches the age of seven, the government enslaves the individual, treating them as legally missing and taking control of their property. This belief is reflected in the language of the movement, where concepts related to maritime law are used to argue that any civil financial obligation is in fact the result of enslavement by state institutions[17]. In this respect, members of the movement also refer to the 13th century *Magna Carta*[18].

Researchers also point to the racist aspects of the sovereign citizen movement. Some factions consider only white-skinned people to be sovereign citizens. The source of this view is an incorrect interpretation of the 14th Amendment to the US Constitution, which is that black Americans – according to this faction of the movement – have become the property of the federal government. This means that they do not have the rights of sovereign individuals, i.e. white citizens. In fact, this amendment is about giving rights and freedoms to all citizens of the United States, which was the reason for the abolition of slavery in this country. Southern Poverty Law Center organisation draws attention to the strong links between the sovereign citizen movement and extremist and racist organisations, for which anti-state rhetoric is a tool in the fight to preserve so-called racial purity and the superiority of the white race[19].

The discourse of the sovereign citizen movement also exhibits features similar to the psychotic structures of meaning that Calum Lister Matheson discusses from the perspective of Jacques Lacan's psychoanalysis in his article *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*[20]. Matheson suggests that the idea of the movement centres around the rejection of the notion of law, which it replaces with a system of signs of an almost magical nature. In it, birth certificates or fictitious identities take on a literal meaning. The language used by the supporters of sovereign citizen movement builds an isolated order of meaning in which they find coherence and sense while rejecting the principles of the actual legal system. In Matheson's

---

17 C. Kalinowski IV, *A Legal Response to the Sovereign Citizen Movement*, "Montana Law Review" 2019, vol. 80, no. 2, pp. 153–210, https://scholarworks.umt.edu/mlr/vol80/iss2/2/ [accessed: 25 X 2024].

18 *Magna Carta*, also known as *Magna Carta Libertatum* (The Great Charter), is a document issued and signed by King John of England on 15 June 1215. It constituted a form of agreement between the monarch and the barons and was simultaneously a privilege limiting royal power, particularly in financial matters (the introduction of taxes required the consent of the kingdom's council) and judicial matters (prohibition of imprisonment or punishment without a court verdict). The document also defined the rights of the barons and clergy, as well as the scope of freedoms for the lower social classes.

19 *The Sovereigns: A Dictionary of the Peculiar…*

20 C.L. Matheson, *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*, "Rhetoric Society Quarterly" 2018, vol. 2, no. 48, pp. 187–206.

view, an understanding of these psychotic structures and mechanisms can provide tools for criticism and respond to the rhetoric of a movement whose destabilising potential lies in both violating the law as well as creating social tensions.

Movements in Poland inspired by the sovereign citizen movement

In Poland, anti-state organisations that are inspired by the US movement are mainly active online. There is a lack of academic literature about their activities, and state actions towards this community are not documented to the same extent as in the United States. The author presents the most active sovereign citizens in Poland and discusses their methods of operation.

Zawodowy Polak (Professional Pole)

One community of sovereign citizens is centred around Tadeusz Cichocki, and the communication channels of his supporters are the website zawodowy-polak.pl and the YouTube channels Zawodowy Polak and @katerina404. On 25 October 2018, after the local elections, Cichocki published online a *Decree of the Head of Authority* that other Polish sovereign citizens refer to in their documents[21]. Cichocki's supporters include him in a carbon copy when they send letters to various offices. The size of Zawodowy Polak movement is difficult to estimate due to its informal and decentralised nature. On 14 July 2025, there were 125 individual declarations of self-determination and responsibility published on zawodowy-polak.pl, the last of which is dated 15 July 2024[22]. In October 2024, the YouTube channel Zawodowy Polak had 9470 subscribers. It is difficult to estimate how many of those watching identify with the movement and take an active part in it. The video of 2 July 2024 entitled *Najemnicy NFUMiG Konstancin Jeziorna* (English: Mercenaries of NFUMiG Konstancin Jeziorna), in which a supporter of the movement argues with a clerk of the Department of Spatial Planning of the City and Municipality of Konstancin-Jeziorna, features 25 comments, most of which are positive about

[21] T. Cichocki, *Dekret Zwierzchnika Władzy w Rzeczypospolitej Polskiej 1-2018* (Eng. Decree of the Head of Authority in the Republic of Poland 1-2018), Piaseczno, 25 X 2018, https://www.tcichocki.pl/Dekret%20Zwierzchnika%20W%C5%82adzy%20w%20RP%201-2018%202018.10.25.pdf [accessed: 25 X 2024].

[22] *Deklaracja Samostanowienia i Odpowiedzialności* (Eng. Declaration of self-determination and responsibility), Zawodowy Polak, https://www.zawodowy-polak.pl/index.php?title=Deklaracja_Samostanowienia_i_Odpowiedzialno%C5%9Bci [accessed: 15 XII 2024].

the content of the video[23]. The acronym NFUMiG stands for Illegally Operating City and Municipal Authority. Supporters of Zawodowy Polak use abbreviations beginning with 'NF' (Illegally Operating) when dealing with public institutions, and when dealing with civil servants add: 'pełniący obowiązki'('acting') – before the job title and 'bez upoważnienia' ('without authority') after the job title (Figure 1).

Nielegalnie Funkcjonujący Sąd Rejonowy dla Warszawy – Woli
Zorganizowana Grupa Przestępcza
Do S Ł
pełniącego obowiązki prezesa sądu rejonowego bez upoważnienia
Do J S
pełniącej obowiązki sądziego bez upoważnienia

Figure 1. Example of addressing messages to public authorities by Zawodowy Polak movement.

Source: Letter of 28 V 2024 on brazen violations of constitutional rights, dignity, human and civil liberties (…) Ref. no. I Co 3161/2, Zawodowy Polak, https://www.zawodowy-polak.pl/TB-NFSR-W-wa_Wola_28.05.2024.pdf [accessed: 14 VII 2024]. Anonymisation was performed by the author of the article.

In the case of Zawodowy Polak movement, as with other sovereign citizen movements it is difficult to identify a systematised system of views and beliefs. Rather, one can observe a cluster of different, unrelated or contradictory views, beliefs and conspiracy theories. The website zawodowy-polak.pl includes longer documents and statements as well as short chaotic slogans. Supporters of the movement on the basis of, inter alia, art. 4 of the Constitution of the Republic of Poland refer to themselves as the Heads of Authority[24], while posting on their website the Fourth Geneva Convention[25] with the reservations of the states that have adopted it. Elsewhere

[23] *Najemnicy NFUMiG Konstancin Jeziorna* (Eng. Mercenaries of NFUMiG Konstancin Jeziorna), YouTube channel Zawodowy Polak, 2 VII 2024, https://www.youtube.com/watch?v=jeH8LX0eYfY [accessed: 1 VII 2025]

[24] See e.g.: Akt oskarżenia z dnia 4 XI 2024 r. (Eng. Indictment act of 4 XI 2024), Zawodowy Polak, https://www.zawodowy-polak.pl/KC-Akt_Oskarzenia-NFPR-4.11.2024.pdf [accessed: 14 VII 2025]; Pismo z dnia 7 III 2024 r. dotyczące braku uprawnień do pełnienia funkcji sędziego, dyrektora i prezesa – dyskryminacji (Eng. Letter of 7 III 2024 on the lack of qualifications to hold the position of discrimination judge, director and president), Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFSR-Grojec_7.03.2024.pdf [accessed: 14 VII 2025].

[25] *IV Konwencja Genewska* (Eng. IV Geneva Convention), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=IV_Konwencja_Genewska [accessed: 1 I 2025].

on the site, the movement's drafts and proposals on electoral law are published[26]. Also presented is the anti-religious content of Anne Marie Riezinger (aka Anne Von Reitz), self-proclaimed Alaska Superior Court Judge[27]. It seems, therefore, that the Polish faction of the sovereign citizen movement, apart from the translation and partial adaptation of the writings of the movement's US proponents, does not bring new, original concepts to the anti-state ideologies.

It is worth noting that Zawodowy Polak, like other representatives of the sovereign citizen movement, appeals to alternative interpretations of the law aimed at undermining state institutions, including the judiciary, administration and politics. The movement's supporters often ignore existing laws and legal norms, deeming them non-existent or illegal, which leads to ambiguous and difficult to predict actions at the legal and social level.

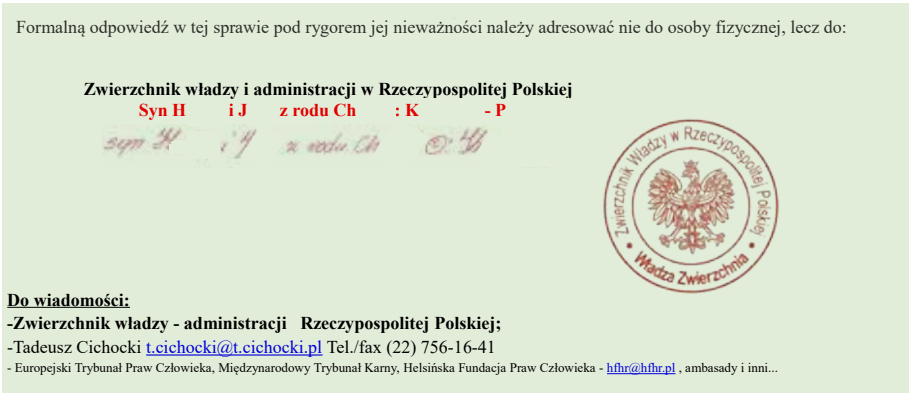
The publications and statements of representatives of Zawodowy Polak may appear complex, but they are based on simple but flawed assumptions about the nature of power, law and the state. They include disinformation and logical manipulation and as such may pose a threat to public order and social stability.

The similarity of Zawodowy Polak to sovereign citizen movement is mainly visible in the writings published on the website zawodowy-polak.pl. They are exemplary for Polish sovereign citizens, who prepare their versions of these letters for offices and companies all over Poland. Elements borrowed from the US sovereign citizen movement used by Zawodowy Polak are shown in Figure 2. These are:

1) distinction between a legal person and a natural person (of flesh and blood) – a red signature in the graphic,
2) characteristic way of writing the name, i.e. a hyphen between given names, the addition of 'son of' and 'of the family' before the surname, as well as a copyright mark,
3) seal with an eagle stylised as an official seal.

[26] *Prawo wyborcze* (Eng. Electoral law), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Prawo_wyborcze [accessed: 1 I 2025].

[27] B.J. Kelley, *Interview with a sovereign: Judge Anna's World*, Southern Poverty Law Center, 15 XII 2017, https://www.splcenter.org/hatewatch/2017/12/15/interview-sovereign-judge-anna%E2%80%99s-world [accessed: 1 I 2025]; *Report and Recommendation*, Case No. 1:16-cv-614, https://www.govinfo.gov/content/pkg/USCOURTS-ohsd-1_16-cv-00614/pdf/USCOURTS-ohsd-1_16-cv-00614-0.pdf [accessed: 1 I 2025]; *Religia* (Eng. Religion), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Religia [accessed: 9 VII 2025].


Formalną odpowiedź w tej sprawie pod rygorem jej nieważności należy adresować nie do osoby fizycznej, lecz do:

Zwierzchnik władzy i administracji w Rzeczypospolitej Polskiej
Syn H i J z rodu Ch : K - P

Zwierzchnik Władzy w Rzeczypospolitej Polskiej
Władza Zwierzchnia

Do wiadomości:
-Zwierzchnik władzy - administracji Rzeczypospolitej Polskiej;
-Tadeusz Cichocki t.cichocki@t.cichocki.pl Tel./fax (22) 756-16-41
- Europejski Trybunał Praw Człowieka, Międzynarodowy Trybunał Karny, Helsińska Fundacja Praw Człowieka - hfhr@hfhr.pl , ambasady i inni...

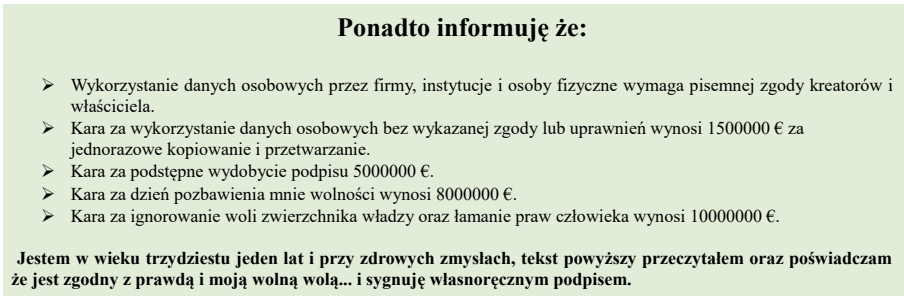
Figure 2. Example of signature used by Zawodowy Polak movement. Anonymisation was performed by the author of the article.

Source: Pismo z dnia 8 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) (Eng. Letter of 8 V 2024 on brazen violations of constitutional rights, dignity, human and civil liberties) Ref. no.: 4161-0.Ds 783.24, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFPR-Lukow_8.05.2024.pdf [accessed: 14 VII 2024]. Anonymisation was performed by the author of the article.

It is worth noting that the founder of Zawodowy Polak movement signs published documents using black font, without a handwritten signature, copyright mark, hyphen between given names or the phrase 'of the family' before the surname[28]. This means that the methods used by individuals who identify with the movement can be created independently and on *ad hoc* basis, according to each person's ideas. As a result, the ideology and beliefs of the movement are inconsistent, often illogical, and even internally contradictory.

Supporters of Zawodowy Polak movement indicate penalties for taking certain actions against them (see Figure 3). This is aimed at public officials (mainly police officers), who are authorised to carry out such actions under the law, such as: the *Act of 24 May 2013 on direct coercive measures and firearms* and the *Act of 6 April 1990 on the Police*.

[28] T. Cichocki, *Polki i Polacy – już czas wypowiedzieć posłuszeństwo nielegalnej władzy działającej na naszą szkodę!!! List otwarty* (Eng. Polish women and men – it is time to declare disobedience to the illegitimate authorities acting to our detriment!!! An open letter), https://www.tcichocki.pl/20150402_Wypowiedzenie_posluszenstwa_organom_panstwa.pdf [accessed: 2 IV 2025].



Ponadto informuję że:

- Wykorzystanie danych osobowych przez firmy, instytucje i osoby fizyczne wymaga pisemnej zgody kreatorów i właściciela.
- Kara za wykorzystanie danych osobowych bez wykazanej zgody lub uprawnień wynosi 1500000 € za jednorazowe kopiowanie i przetwarzanie.
- Kara za podstępne wydobycie podpisu 5000000 €.
- Kara za dzień pozbawienia mnie wolności wynosi 8000000 €.
- Kara za ignorowanie woli zwierzchnika władzy oraz łamanie praw człowieka wynosi 10000000 €.

Jestem w wieku trzydziestu jeden lat i przy zdrowych zmysłach, tekst powyższy przeczytałem oraz poświadczam że jest zgodny z prawdą i moją wolną wolą... i sygnuję własnoręcznym podpisem.

Figure 3. Excerpt from a document of Zawodowy Polak movement.

Source: D. Bryda, *Deklaracja Samostanowienia i Odpowiedzialności* (Eng. Declaration of self-determination and responsibility), 12 I 2024, https://www.zawodowy-polak.pl/DB-Deklaracja_12.01.2024r.pdf [accessed: 25 X 2024].

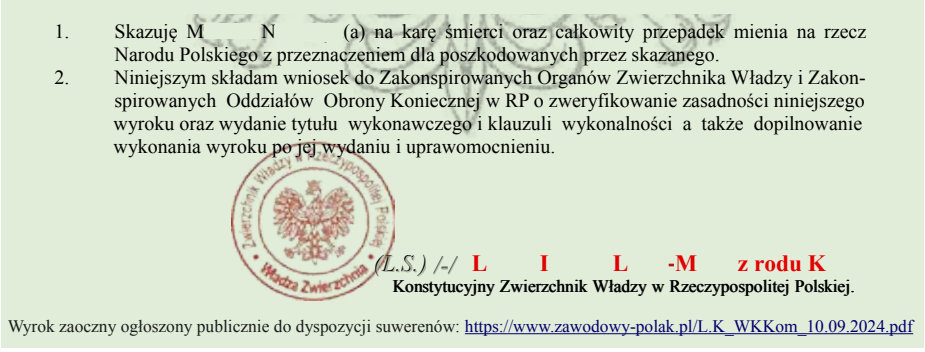
On the YouTube channel Zawodowy Polak, content is published presenting conspiracy theories important to the sovereign citizen movement, as well as videos documenting visits by movement supporters to public offices, such as the Social Insurance Institution (ZUS), municipal offices or local election commissions[29]. Confrontations with traffic police patrols are also shown, usually ending with an intervention against a supporter of the movement who disrupts the work of officers or resulting in detention or the issuing of a fine. Police interventions have often been the subject of so-called commentary videos, in which the creator responds to another video. In one case, a police officer commented on an intervention on his private channel[30]. He drew attention, among other things, to the characteristic language (the supporter of the movement claimed that he was not a driver but a human being). Due to the professionalism of the police officers conducting the intervention and the behaviour of the person subjected to it, the police work is commented on positively, while the behaviour of the detained person is commented on negatively or humorously. Members of the movement claim that they act on behalf of the sovereign, meaning the Polish nation, and justify their actions with legal arguments that have no basis in the applicable law. They refer to natural law, question the legality of state authorities and undermine their authority and

[29] *Nie można nagrywać najemników i lokalu wyborczego w Kisielsku?* (Eng. Can't the mercenaries and the polling station in Kisielsk be recorded?), YouTube channel Zawodowy Polak, 9 VI 2024, https://www.youtube.com/watch?v=8nAon2vpOTQ [accessed: 15 XII 2024].

[30] „*Nielegalne*" *zatrzymanie przez Policję i ZAWODOWY POLAK | Bagieta rozkłada interwencje #3* (Eng. 'Illegal' Police detention and ZAWODOWY POLAK | Bagieta *breaks down interventions #3*), YouTube channel Sierżant Bagieta, 26 II 2020, https://www.youtube.com/watch?v=EgQWjQEDq_A [accessed: 1 I 2025].

competences. In practice, their activities lead to disruptions in the work of public offices and the Police.

Most of the recorded behaviour of the movement's supporters can be considered harmless vexatious litigation, but there is also a content of a different nature, for instance, a video titled *When should you shoot a cop?*[31].The radicalisation of the movement is also visible on the main website: zawodowy-polak.pl, where supporters are called upon to create (sic!) Clandestine Tribunals of the Polish Nation, which are supposed to issue in absentia death sentences on (…) *the enemies of the Republic of Poland and their collaborators, in accordance with natural law, the Polish national interest and their own conscience*[32]. The authors of this appeal are therefore calling for vigilante justice against state officials and representatives of the authorities. In response, from 2024 onwards, sympathisers of the movement have begun posting death sentences for the enemies of individual members on the zawodowy-polak.pl website. The execution of these sentences is assigned to the aforementioned tribunals (Figure 4). For instance, an indictment against a court bailiff has been published, containing a criminal threat (i.e. the threat of imposing and carrying out the death penalty)[33].



1. Skazuję M N (a) na karę śmierci oraz całkowity przepadek mienia na rzecz Narodu Polskiego z przeznaczeniem dla poszkodowanych przez skazanego.
2. Niniejszym składam wniosek do Zakonspirowanych Organów Zwierzchnika Władzy i Zakonspirowanych Oddziałów Obrony Koniecznej w RP o zweryfikowanie zasadności niniejszego wyroku oraz wydanie tytułu wykonawczego i klauzuli wykonalności a także dopilnowanie wykonania wyroku po jej wydaniu i uprawomocnieniu.

Zwierzchnik Władzy w Rzeczypospolitej Polskiej
Władza Zwierzchnia

(L.S.) /-/ **L I L -M z rodu K**
Konstytucyjny Zwierzchnik Władzy w Rzeczypospolitej Polskiej.

Wyrok zaoczny ogłoszony publicznie do dyspozycji suwerenów: https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf

Figure 4. The wording of a sentence issued by a member of Zawodowy Polak movement. Anonymisation was performed by the author of the article.

Source: *Wyrok zaoczny w imieniu Zwierzchnika Władzy w Rzeczypospolitej Polskiej* (Eng. A sentence passed in absentia on behalf of the Head of Authority in the Republic of Poland), Zawodowy Polak, 10 IX 2024, https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf [accessed: 25 X 2024]. Anonymisation was performed by the author of the article.

[31] *Kiedy powinieneś zastrzelić agenta?* (Eng. When should you shoot a cop?), YouTube channel Moron3k, https://youtu.be/AJ2HJWhmrdE?si=kbENyPyZmWGeG2_C [accessed: 14 VII 2025].

[32] T. Cichocki, *Polki i Polacy – już czas*…, p. 10.

[33] T. Berkowska, *Akt oskarżenia* (Eng. Indictment act), https://www.zawodowy-polak.pl/TB_NFKS-MK-Akt_Oskarzenia-27.11.2024.pdf, p. 3 [accessed: 1 I 2025].

Both Polish and US sovereign citizens are characterised by xenophobic views. In the United States, these are mainly racist views, while in Poland antisemitism predominates. On the zawodowy-polak.pl website, one can find an example of an antisemitic text titled: *Protokoły Mędrców Syjonu* (The Protocols of the Sages of Zion)[34].

Ruch II RP (The Second Polish Republic movement)

The founder of the Ruch II RP movement is claiming to be a count and the president of the Second Polish Republic in exile Jan Zbigniew Potocki. According to Potocki, the last legitimate president of the Second Polish Republic's government in exile was Juliusz Nowina-Sokolnicki, not Ryszard Kaczorowski, and it is from him that he derives his mandate to continue holding the office of President of the Second Polish Republic. Although Nowina-Sokolnicki was appointed by August Zaleski, he was a controversial figure, and his appointment raised doubts, partly because it was never officially announced in the appropriate official publications. Zaleski repeatedly changed his successors, that led to the parallel existence of various centres of power in exile. One of these was the Sokolnicki line, while the other recognised Kaczorowski as the legitimate president. On 22 September 1971, Zaleski appointed Sokolnicki, as his successor, which meant the dismissal of Stanisław Ostrowski. However, after Zaleski's death, it was Ostrowski who was recognised as a president by main political centres of the émigré community. Despite this, Sokolnicki maintained that his appointment was valid. This led to a situation of dual power within the émigré circles[35]. The activities of Jan Zbigniew Potocki, which refer to Nowina-Sokolnicki presidency, are therefore a continuation of the divisions that originated in the 1970s. Like Sokolnicki, Potocki appeals to the legal continuity of the Second Polish Republic and seeks to legitimise his actions by invoking the historical controversies surrounding the presidential succession in exile.

One of the main activities of Potocki is the sale of so-called identity cards of the sovereign of the Second Polish Republic (Figures 5 and 6).

[34] *Protokoły Mędrców Syjonu* (Eng. The protocols of the Sages of Zion), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Protoko%C5%82y_M%C4%99drc%C3%B3w_Syjonu [accessed: 1 VII 2025].

[35] J. Majchrowski, *Kwestia sukcesji prezydenckiej na obczyźnie* (Eng. The question of presidential succession in exile), in: *Myśl polityczna: od historii do współczesności*, B. Stoczewska, M. Jaskólski (eds.), Kraków 2000, p. 258, https://ruj.uj.edu.pl/server/api/core/bitstreams/2cc6a415-0de3-4172-bbd2-2cd16fce2235/content [accessed: 1 I 2025].

Figure 5. Front of the identity card of the sovereign of the Second Polish Republic.

Source: K. Jesionowska, *Dowód osobisty suwerena II Rzeczypospolitej Polskiej* (Eng. ID of the sovereign of the Second Polish Republic), Straż Graniczna, 3 XII 2021, https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II-Rzeczypospolitej-Polskiej.html [accessed: 25 X 2024].

Figure 6. Back of the identity card of the sovereign of the Second Polish Republic.

Source: K. Jesionowska, *Dowód osobisty suwerena II Rzeczypospolitej Polskiej* (Eng. ID of the sovereign of the Second Polish Republic), Straż Graniczna, 3 XII 2021, https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II-Rzeczypospolitej-Polskiej.html [accessed: 25 X 2024].

Although these documents are not recognised by state institutions and are not listed in international databases (e.g. PRADO), Potocki claims that possessing a sovereign ID comes with various privileges, such as exemption from the obligation to vaccinate children, exemption from military draft (currently military qualification), immunity from enforcement by court bailiffs and exemption from Polish tax law. It is worth noting the similarity in this regard to the German

Reichsbürger (Reich Citizens) movement, which also uses documents referring to a state that no longer exists rather than its current constitutional form[36]. Potocki is also planning to issue birth certificates, driving licences and passports.

The letters, that Potocki advises his supporters to send to public offices are similar to those used by Zawodowy Polak movement. Both movements claim that, as flesh and blood individuals, they are not subject to the law. They use red font for selected parts of their letters and maintain that Poland is not a state but a company registered in the United States Securities and Exchange Commission as: POLAND REPUBLIC OF[37]. In reality, the entry of the Republic of Poland into the register of the US Securities and Exchange Commission serves to facilitate the sale of bonds on international markets and does not have any legal or international consequences for the status of the RP, it does not give Poland the status of a company[38].

In 2024, the activities of Ruch II RP movement quieted down for a time due to internal disputes and Potocki's imprisonment. In 2025, his supporters reactivated the movement[39].

Demokracja i Sprawiedliwość (Democracy and Justice) and the National Tribunal

Demokracja i Sprawiedliwość (English: Democracy and Justice) is an association based in Jelenia Góra, led by Grzegorz Niedźwiedzki. It has formed an eight-member Supreme National Tribunal[40], which acts as a people's court. To lend the credibility,

---

[36] J. Eichner, *"Reichsdeutsche" fordern bayerische Justiz heraus. Hier ist „deutsches Reichsgebiet"!*, Bayerischer Rundfunk, 23 IV 2016, https://www.br.de/nachricht/reichsbuerger-bayern-gerichtsvollzieher-100.html [accessed: 25 X 2024].

[37] This issue was even a subject of a parliamentary interpellation by the MP Jarosław Sachajko in 2020. See: *Interpelacja nr 5712 w sprawie zarejestrowania firmy POLAND REPUBLIC OF w rejestrze Amerykańskiej Komisji Papierów Wartościowych* (Eng. Interpellation no. 5712 concerning registration of POLAND REPUBLIC OF in the register of the US Securities Exchange Commission), Sejm RP, https://www.sejm.gov.pl/sejm9.nsf/interpelacja.xsp?typ=INT&nr=5712 [accessed: 1 VII 2025].

[38] Ł. Starzewski, *Polska zarejestrowana jako firma w USA? RPO prosi MSZ o zbadanie skargi obywatela* (Eng. Poland registered as a company in the USA? The Ombudsman asks the Ministry of Foreign Affairs to investigate citizen's complaint), Rzecznik Praw Obywatelskich, 24 II 2020, https://www.rpo.gov.pl/pl/content/polska-zarejestrowana-jako-firma-w-usa-rpo-prosi-msz-o-zbadanie-skargi-obywatela [accessed: 25 X 2024].

[39] W. Ferfecki, *Jan Zbigniew Potocki kontra współpracownicy. Bunt przeciw samozwańczemu prezydentowi* (Eng. Jan Zbigniew Potocki vs. colleagues. Rebellion against the self-appointed president), Rzeczpospolita, 17 V 2024, https://www.rp.pl/polityka/art40374471-jan-zbigniew-potocki-kontra-wspolpracownicy-bunt-przeciw-samozwanczemu-prezydentowi [accessed: 25 X 2024].

[40] *Najwyższy Trybunał Narodowy. Akt ustanowienia* (Eng. The Supreme National Tribunal. Act of Establishment), Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/najwyzszy-trybunal-narodowy/ [accessed: 21 VII 2025].

the members of this tribunal wear judge's robes of their own design (a black robe with a white and red jabot, but unlike the official robes used by the Constitutional Tribunal, the jabot has a horizontal pattern rather than a vertical one – see Photo 1). One member of the movement, who calls himself the President of Free Poland, also wears a Polish Army uniform with additional insignia of the Polish Riflemen's Units. He exploits a legal loophole to build his image on the authority of the military.

Photo 1. The session of the Supreme National Tribunal.

Source: *Uchwała Najwyższego Trybunału Narodowego o nieważności wyroków w imieniu Rzeczypospolitej Polskiej* (Eng. Resolution of the Supreme National Tribunal on the invalidity of judgments in the name of the Republic of Poland), trybunał-narodowy.pl, 13 XI 2024, https://www.trybunal-narodowy.pl/uchwala-najwyzszego-trybunalu-narodowego-o-niewaznosci-wyrokow-w-imieniu-rzeczypospolitej-polskiej/ [accessed: 1 VII 2025]. Anonymisation was performed by the author of the article.

In 2021, the Supreme National Tribunal sentenced 24 public officials (including Zbigniew Ziobro, who was the then Prosecutor General and once as the Minister of Justice) to 15 years of imprisonment with an obligation to perform community service, infamy, social ostracism, loss of the right to a pension related to their profession, deprivation of civil rights, payment of PLN 100 000 in compensation to the victim, payment of PLN 1 million in compensatory damages to Demokracja i Sprawiedliwość association, and ordered them to issue a public apology to the victim, who was identified as Grzegorz Niedźwiedzki.

On 3 May 2024, Demokracja i Sprawiedliwość association established the Government of Free Poland and issued commemorative certificates

of appointment and membership IDs to its members[41]. The video of the formation of this government[42] on 1 January 2025 had approx. 2000 views, and the YouTube channel – 735 subsribers. Each video published by the association averages approx. 800 views.

Another organisational unit is the National Tribunal, which is based in Jelenia Góra and is personally connected with Demokracja i Sprawiedliwość association. According to the National Court Register (KRS) extract published on its website trybunal-narodowy.pl, it is a union of associations. In its decisions, the National Tribunal refers, among others, to the puppet theory, claiming that the state cannot judge a human being, only legal entities into which people have allegedly been transformed. Tribunal also distributes *Declaration of Self-determination and Responsibility* of Zawodowy Polak movement.

The movement of Teresa Garland

The movement led by Teresa Garland, who calls herself the President of the Electoral Republic of Poland, is partially similar to sovereign citizen movement. She legitimises her title with the result of an election that she organised and conducted herself, in which she asked her supporters to transfer 1 PLN to her bank account with the transfer title: vote. She decided to do this because she was unable to gather 1000 signatures required to register an electoral committee with the National Electoral Commission[43]. Garland also established Provisional Council of State of the Polish Nation Social Constitutional Committee, whose one member is Piotr Smolana, a former MP of Samoobrona party[44]. Teresa Garland's activity mainly involves sending petitions to municipal and city offices across Poland concerning, among others, the establishment of a local energy guard, the announcement

[41] *Powołano Rząd Wolnej Polski* (Eng. The Government of Free Poland was established), Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/powolano-rzad-wolnej-polski/ [accessed: 1 VII 2025].

[42] *Powołanie Rządu Wolnej Polski* (Eng. Establishment of the Government of Free Poland), YouTube channel Trybunał Narodowy, https://www.youtube.com/watch?v=1HyXzBXXfOs&t=1s [accessed: 1 VII 2025].

[43] T. Garland, *24 III 2020 r. PKW TERESA GARLAND zgłoszenie kandydatury po raz trzeci* (Eng. 24 III 2020 PKW TERESA GARLAND application for the third time), Teresa Garland, https://teresagarlandprezydent.wordpress.com/2020/03/24/24-iii-2020r-pkw-teresa-garland-zgloszenie-kandydatury-po-raz-trzeci/ [accessed: 1 I 2025].

[44] R. Gębuś, *Samozwańczy Rząd Tymczasowej Rady Stanu apeluje o poparcie do lęborskiej rady. Burmistrz powiadamia prokuraturę* (Eng. Self-appointed Government of the Provisional Council of State appeals for support to Lębork council. The mayor notifies the public prosecutor's office), Lębork Nasze Miasto, 19 IV 2021, https://lebork.naszemiasto.pl/samozwanczy-rzad-tymczasowej-rady-stanu-apeluje-o-poparcie/ar/c15-8238215 [accessed: 1 I 2025].

of people's referendum[45], support for her provisional government and the arming of every indigenous inhabitant of Poland[46]. In 2022, Garland was detained by the Police[47], and the District Court in Wieliczka ordered her to undergo psychiatric evaluation[48]. It is worth noting that as the conflict between Garland and the Polish state intensified, she began to use more and more phrases and demands characteristic of the sovereign citizen movement, such as: citizen-sovereign, flesh and blood person and challenging the legality of the court as a state institution. Based on the number of subscribers to the YouTube channel @prezydentelektorski channel, as of 1 January 2025 the popularity of the movement of Teresa Garland can be estimated at approx. 660 people. The latest video from April 2024 has approx. 30 views. Teresa Garland communicates with her supporters through a blog and profiles on platforms like vk.com (the video from December 2024 as of 1 January 2025 has 16 views) or gloria.tv.

Other representatives of sovereign citizen movement in Poland

In Poland, there are also other individuals and groups creating alternative state authorities, for example, Wojciech Edward Leszczyński – Leh XVII[49], Włodzimierz

[45] *Samozwańcza prezydent sypnęła petycjami* (Eng. Self-appointed president filed petitions), Super Tydzień Chełmski, 15 IV 2021, https://www.supertydzien.pl/artykul/10406,samozwancza-prezydent-sypnela-petycjami [accessed: 1 I 2025].

[46] J. Sidorowicz, *Broń od gminy dla każdego rdzennego mieszkańca Starego Sącza? Jest petycja w sprawie programu „Broń palna plus"* (Eng. Arms from the municipality for every native of Stary Sącz? There is a petition on the 'Firearms plus' programme), Kraków.Wyborcza.pl, 26 IX 2022, https://krakow.wyborcza.pl/krakow/7,44425,28955388,bron-od-gminy-dla-kazdego-rdzennego-mieszkanca-starego-sacza.html [accessed: 1 I 2025].

[47] *Ośrodek Monitorowania Zachowań Rasistowskich i Ksenofobicznych, Teresa Garland będąca prorosyjską patocelebrytką w końcu zatrzymana przez policję* (Eng. Teresa Garland pro- Russian scandalous celebrity finally detained by the Police), Facebook, 28 IX 2022, https://www.facebook.com/osrodek.monitorowania/posts/teresa-garland-b%C4%99d%C4%85ca-prorosyjsk%C4%85-patocelebrytk%C4%85-w-ko%C5%84cu-zatrzymana-przez-policj/1917138658461258/ [accessed: 1 I 2025].

[48] T. Garland, *Sprzeciw i apelacja na wyrok z dnia 12 X 2023r. o sygn. akt IIK 451/21 w Sądzie Rejonowym w Wieliczce* (Eng. Objection and appeal against the judgment of 12 X 2023 ref. no. IIK 451/21 in the District Court in Wieliczka), Tymczasowa Rada Stanu, https://tymczasowaradastanu.wordpress.com/2023/11/24/teresa-garland-sprzeciw-i-apelacja-na-wyrok-z-dnia-12-x-2023r-o-sygn-akt-iik-451-21-w-sadzie-rejonowym-w-wieliczce/ [accessed: 1 I 2025].

[49] W. Ferfecki, *Samozwańczy król Polski z darmowymi spotami w TVP* (Eng. Self-appointed king of Poland with free spots in TVP), Rzeczpospolita, 13 IX 2023, https://www.rp.pl/polityka/art39102811-samozwanczy-krol-polski-z-darmowymi-spotami-w-tvp [accessed: 1 VII 2025].

Julian Korab-Karpowicz – President of the RP *in spe*[50], Marek Świętopełk-Zawadzki[51], Mariusz Max Kolonko – President of the United States of Poland *ad interim*[52]. These individuals (with the exception of Mariusz Kolonko) refer to monarchist movements and create their own alt-state documents. The author omitted their activities in this article due to their lesser popularity and lack of clear connections to the sovereign citizen movement. However, it is worth monitoring their activities because of the potential increase in their significance within the sovereign citizen environment, caused, for instance, by the cessation or suspension of activities by more popular movements.

Implications for the financial sector (particularly banking)

Individuals identifying with Zawodowy Polak movement deny the existence and legitimacy not only of government institutions, including the Police and local governments, but also private companies in the banking sector and financial institutions. An example of such actions are letters published on Zawodowy Polak movement platform and addressed to the Insurance Guarantee Fund (UFG) as well as to Santander Bank Polska S.A. In a letter to Santander Bank[53] (described by the movement's supporters as Illegally Operating SANTANDER BANK POLSKA S.A., NFSBP S.A.), Beata Koźlik denies the bank's right to demand repayment of the loan she took out and to transfer it for collection by an external entity. She also accuses the bank of using so-called abusive clauses. As evidence for this last

[50] W. Ferfecki, *Filozof ogłosił się głową państwa* (Eng. Philosopher declared himself head of state), Rzeczpospolita, 6 VIII 2020, https://www.rp.pl/polityka/art8857531-filozof-oglosil-sie-glowa-panstwa [accessed: 1 VII 2025].

[51] J. Zaremba, *„Leczył" z zaburzeń psychicznych i masturbacji. „Książę" Świętopełk-Zawadzki na Narodowym Marszu Papieskim* (Eng. He 'treated' for mental disorders and masturbation. 'Prince' Świętopełk-Zawadzki at the National Papal March), Gazeta.pl, 3 IV 2023, https://kobieta.gazeta.pl/kobieta/7,107881,29626596,leczyl-z-zabrzen-psychicznych-i-homoseksualizmu.html [accessed: 1 VII 2025].

[52] G. Sajór, *Nie wytrzymał ciśnienia. Mariusz Max Kolonko po odejściu z dziennikarstwa został Prezydentem* (Eng. He couldn't withstand the pressure. Mariusz Max Kolonko became President after leaving journalism), Press, 20 V 2022, https://www.press.pl/tresc/70879,[na-weekend]-nie-wytrzymal-cisnienia_-mariusz-max-kolonko-po-odejsciu-z-dziennikarstwa-zostal-prezydentem [accessed: 1 VII 2025].

[53] B. Koźlik, *Doręczenie odpisu postanowienia zwierzchnika władzy w Rzeczypospolitej Polskiej* (Eng. Delivery of a copy of the order of the head of authority in the Republic of Poland), Zawodowy Polak, 27 VI 2022, https://zawodowy-polak.pl/BK-ost_postanowienie_bank_27.06.2022.pdf [accessed: 1 I 2025].

point, she presents the lack of responses from the branch director and the bank's president, the lack of replies from the bank's team manager and the customer ombudsman, as well as deliberate misleading and manipulation by having two different bank representatives answer her letters alternately – people who were not the exact addressees of her correspondence, as well as (…) *lack of indisputable, documented evidence of legal authority*[54]. The methods used by the movement against private entities are therefore similar to these used against state institutions. Since the banking sector is a part of the country's critical infrastructure[55], such actions are harmful not only from the perspective of the bank as a private institution but also from the perspective of the state.

In turn, in the letter to the Insurance Guarantee Fund (UFG) Arkadiusz Bosa challenges the legality of the UFG and questions the legal status of the Fund's representatives. The sender of the letter accuses the UFG of acting to the detriment of the state and citizens, referring to the absence of documented social mandates and compliance with the constitution. He demands proof of the legal authority of the UFG's representatives and calls for an immediate end to any illegal activities under threat of legal consequences[56].

Videos can also be found on YouTube showing Teresa Garland's disrupting a conference attended by the President of the National Bank of Poland (NBP) Adam Glapiński, and then approaching him at a dangerous distance[57]. In the context of past attacks on representatives of the financial sector[58] and central banking[59], it is worth to emphasise that allowing members of anti-state movements, who are extremely critical of any form of state monetary policy, to get so close is irresponsible and represents a serious lapse in the security measures protecting the President of NBP.

---

[54] Ibid.

[55] K. Piękoś, *Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków* (Eng. Cyberattacks on banking systems and critical infrastructure – analysis of selected cases), "Krakowskie Studia Małopolskie" 2017, no. 22, pp. 106–113.

[56] A. Bosa, *Decyzja Zwierzchnika Władzy w Rzeczypospolitej Polskiej od której nie przysługuje zażalenie* (Eng. Decision of the Head of Authority in the Republic of Poland against which there is no right of appeal), 13 VIII 2023, https://www.zawodowy-polak.pl/AB-NFUFG_13.08.2023.pdf [accessed: 1 I 2025].

[57] *Prezes NBP Glapiński, Teresa Garland i demokracja* (Eng. President of the NBP Glapiński, Teresa Garland and democracy), YouTube channel Fides Polska TV, 16 XI 2018, https://www.youtube.com/watch?v=j1Bd4ZToToE [accessed: 1 I 2025].

[58] J. Bielecki, *Amerykanie mają dość ubezpieczycieli* (Eng. Americans are fed up with insurers), Rzeczpospolita, 11 XII 2024, https://www.rp.pl/przestepczosc/art41568761-amerykanie-maja-dosc-ubezpieczycieli [accessed: 1 VII 2025].

[59] *Top Russian central banker shot to death*, NBC News, 14 IX 2006, https://www.nbcnews.com/id/wbna14826889 [accessed: 1 VII 2025].

A potential attack on the person holding such a position poses a threat to the stability of monetary policy[60]. It is worth noting that according to the *Act of 8 December 2017 on the State Protection Service*, the President of the NBP is not an entity listed in the Act *per se*, however, he could be protected by the State Protection Service (SOP) on the basis of the Prime Minister's decision.

Due to US sources of the movement, it is worth paying attention to the solutions adopted there and the methods of dealing with supporters of the sovereign citizen movement[61]. This could serve as a point of reference for Polish public institutions and the banking sector. In the United States, financial institutions and courts have adopted a firm policy towards attempts to repay debts using so-called fake financial instruments, such as fictitious bonds or emission coupons. These are deemed invalid and are not enforceable. US courts have repeatedly pointed out the lack of merit in the arguments presented by members of the movement. They have described them as legally unfounded, which has resulted in their immediate dismissal without the need for further proceedings. Banking institutions in the United States are instructed on how to proceed when a client attempts to use practices such as referring to a non-existing account in the United States Department of the Treasury, invoking irrelevant Uniform Commercial Code regulations or demanding the anonymisation of their data, including their social security number. In such cases, banks are encouraged to reject such requests in writing and to inform clients of their obligations under applicable agreements. In some cases, they may also consider closing the client's account if permitted by law and contractual terms. American experience shows that a key element in combating the sovereign citizen movement is the educating employees of financial and administrative institutions on how to recognise the characteristics typical of sovereign citizens.

One of the factors that contributed to such a policy was, among others, the case of a private currency produced by Bernard von NotHaus called Liberty Dollar (ALD). It consisted of both coins and banknotes in the form of certificates (Figure 8). The value of the Liberty Dollars corresponded to a specific amount

[60] P. Król, *Analiza zamachów na osoby publiczne – skuteczność działań prewencyjnych służb bezpieczeństwa i konsekwencje polityczno-społeczne* (Eng. Analysis of assassinations on public figures – effectiveness of preventive actions by security forces and political and social consequences), "Kwartalnik Kadry Kierowniczej Policji" 2024, no. 3, https://kwartalnik.akademiapolicji.edu.pl/images/stories/2024/3/krl.pdf [accessed: 1 VII 2025].

[61] D. Spungen, *How Financial Institutions Should Handle "Sovereign Citizens"*, Amundsen Davis, 18 III 2024, https://www.amundsendavislaw.com/banking-brief-financial-services-insights/how-financial-institutions-should-handle-sovereign-citizens [accessed: 1 I 2025].

of gold and silver for which it could be exchanged[62]. These actions caused concern within the Federal Reserve System (FED) and the United States Mint, which began to view this move as a threat to the stability of the US monetary and financial system.

Figure 8. Exemplary Liberty Dollar banknote – front and back.

Source: Silver Certificates, NORFED Liberty Dollar, https://norfed.info/silver-certificates/ [accessed: 1 I 2025].

A long-standing dispute, in which the organisation issuing Liberty Dollars presented various arguments, including those related to the purely numismatic nature of ALD, ended with the indictment and arrest of Bernard von NotHaus and three other people. In March 2011, NotHaus was convicted for producing, possessing and selling his own coins. He faced up to 15 years in prison and a fine of USD 250 000. Additionally, the government was able to seize assets in the form

[62] L.H. White, *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold*, "The Cato Journal" 2014, vol. 34, no. 2, pp. 281–301. http://dx.doi.org/10.2139/ssrn.2406983.

of coins and precious metals worth USD 7 million[63]. Ultimately, he was sentenced to six months of house arrest with a three-year probation period. At the probation officer's request, he was released from probation after one year.

Federal authorities described the activities of organisation issuing Liberty Dollars as an attempt to undermine the official US currency and compared it to a form of domestic terrorism that could harm the country's economic stability. Although historically the free banking system (i.e. without a central bank monopoly on currency issuance) was characterised by stability, today it is not seen as a solution to the problems of the financial market, since central banking is now an integral part of the state's economic policy, particularly its stabilisation function[64].

The US authorities' opposition to attempts to undermine the authority of the state and financial institutions can serve as an inspiration for adopting a similar stance in Poland. This approach makes it possible to limit the influence of anti-state movements and minimise the threats they may pose to the country's financial stability.

Summary and recommendations

The author discussed the development, activities as well as social and legal consequences of anti-state movements in Poland, whose ideology and methods are inspired by the US sovereign citizen movement.

Contact between representatives of state institutions and members of the movement is difficult due to their use of a specific pseudo-legal system, in which basic legal and administrative definitions are distorted and legal norms are applied selectively and instrumentally. For instance, a member of the movement denies the authority of the Police granted by the Police Act or the legitimacy of municipal authorities, citing the *Act of 8 March 1990 on municipal self-government*, only to later invoke the General Data Protection Regulation[65] as a basis to demand million-dollar compensations from police officers conducting interventions. The members

[63] P.C. Mullan, *The Liberty Dollar and Bernard von NotHaus*, in: *A History of Digital Currency in the United States. New Technology in an Unregulated Market*, New York 2016, pp. 87–109. http://dx.doi.org/10.1057/978-1-137-56870-0_3.

[64] P. Marszałek, *Rynek czy państwo w bankowości – bankowość centralna versus bankowość wolna* (Eng. Market or government in banking – central banking vs. free banking), "Ryzyko i Zrównoważony Rozwój" 2011, no. 70, pp. 125–136.

[65] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

of the movement also challenge the legality of decisions made by state authorities and refuse to recognise official documents, fines or court summons. They file baseless complaints and appeals, using formal procedures as tools to destabilise public institutions and overload the administrative system. They also attempt to establish quasi-governmental structures, such as national tribunals or citizens' courts, which issue legally ineffective rulings. These initiatives lead to conflicts with public officials, often resulting in verbal aggression and, in extreme cases, threats or attempts at intimidation by sovereign citizens.

An analysis of so-called pseudo-legal techniques used by supporters of sovereignty movements in both the USA and Poland showed that these should be treated as attempts to intimidate representatives of state institutions. Zawodowy Polak movement even went as far as publishing death sentences for 'traitors of the nation'. Such actions, along with others, like promoting conspiracy theories and encouraging avoidance of legal responsibility, serve to radicalise members of the sovereign citizen movement in Poland[66].

The sovereign citizen movement in Poland adapts US patterns, adjusting them to local realities and the specific characteristics of the Polish legal system, for instance, the use of seals, signatures in red ink or arguments based on the alleged dual identity of a citizen as both a natural and a legal person. The activities of the movement pose a challenge to public administration and the banking sector, which are increasingly being targeted. Polish institutions should consider implementing procedure modelled on the US solutions, such as:

- training employees to recognise the characteristic behaviours of movement members and their documents,
- unequivocally rejecting pseudo-legal claims,
- consistently responding to any attempts to destabilise public order.

Education of public officials

In Poland, officials are generally not sufficiently trained to effectively and clearly explain legal theory to individuals who attempt to challenge the legal order using pseudo-legal documents. Burdened with a high volume of cases, they do not have time for extensive debates and detailed explanations. According to the author, this may lead to increased frustration among people identifying with the sovereign citizen movement, whose questions about the legitimacy of the authorities

[66] B. Łódzki, *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej* (Eng. Fake news – disinformation in online media and forms of combating it in the international space), "Polityka i Społeczeństwo" 2017, vol. 15, no. 4, pp. 19–30. https://doi.org/10.15584/polispol.2017.4.2.

remain unanswered in a comprehensive manner. A solution could be to develop a handbook for public administration employees, similar to brochures published in the United States[67], containing information about the methods and manipulations used by sovereign citizen supporters, examples of how to deal with them and templates for responding to their letters addressed to public institutions. The Polish document of this kind could include guidelines on how to deal with applicants who use pseudo-legal arguments, as well as instructions on how to proceed when they disrupt the functioning of an office. This type of instructions would not only improve the quality of service but could also contribute to more effective responses to attempts to destabilise the operations of public offices.

The problem of the lack of effective ways to respond to the actions of Polish sovereign citizen movement towards public offices has been noted by Bartosz Mendyk. The author addresses the problem of Teresa Garland distributing petitions in which she refers to conspiracy theories, spreads pro-Russian propaganda, and uses hate speech against Jews and Ukrainians[68]. Mendyk points out not only the problematic nature of these petitions, which, from the perspective of officials, contain demands unrelated to the needs of local communities, but also the issue of the obligation to publish such petitions in the Bulletin of Public Information (BIP). In this way, the movement's materials – in this case Teresa Garland's – become more accessible. Mendyk notices that Teresa Garland's letters do not meet the requirements set out in the *Act of 11 July 2014 on petitions*, constitute an abuse of the right to petition, and that a public administration body may, in such a case, determine that such an abuse has occurred and leave the petition without consideration and without publication. It is worth to emphasise, that state and local government institutions (…) *which, in connection with their activities, become aware of the commission of an offence prosecuted ex officio are obliged to immediately notify the public prosecutor or the Police and to undertake the necessary measure – until the arrival of the authority responsible for prosecuting offences or until that authority issues an appropriate order – in order to prevent the destruction of traces and evidence of the offence*[69].

---

[67] M. Crowell, *A Quick Guide to Sovereign Citizens*, "Administration of Justice Bulletin" 2015, no. 4, https://www.sog.unc.edu/sites/default/files/reports/aojb1504.pdf [accessed: 1 VII 2025]; *A Quick Guide to Sovereign Citizens*, UNC School of Government, November 2013, https://www.sog.unc.edu/sites/www.sog.unc.edu/files/Sov%20citizens%20quick%20guide%20Nov%2013.pdf [accessed: 1 I 2025].

[68] B. Mendyk, *Jak reagować na petycje pełne teorii spiskowych?* (Eng. How to respond to petitions full of conspiracy theories?), Pismo Samorządu Terytorialnego "Wspólnota", 3 IV 2024, https://wspolnota.org.pl/newsletter/jak-reagowac-na-petycje-pelne-teorii-spiskowych [accessed: 1 I 2025].

[69] Article 304 § of the Act of 6 June 1997 – *Code of criminal procedure*.

Introduction of provisions limiting so-called institutional vexatious litigation

An important aspect of the discussed issue is the phenomenon of so-called institutional vexatious litigation. This should be understood as the submission of numerous groundless complaints or letters with the aim of prolonging proceedings or disrupting the work of the administration. So far, the phenomenon of vexatious litigation has been described in the literature in the context of judiciary[70]. Lech Jamróz emphasises, that the right to access to a court is not absolute and may be restricted in cases of obstructive or malicious actions. Similarly, the same approach could be applied to vexatious behaviour in public administration, which aims to sabotage the work of public authorities. Currently, the law allows for the penalisation of behaviour disrupting public order under the Article 51 of the Code of petty crimes, however, it is worth to consider if additional provisions are needed to more effectively limit such actions, particularly in cases of persistent or organised vexatious conduct.

Regulations concerning the use of imitations of state symbols and threats against institutions

The Polish law does not provide for penalties for creating graphics that imitate state seals, as long as they differ from the official versions by at least one element. This allows the sovereign citizen movement to use graphics, that to an uninformed observer, may appear to be official seals. An example of this is the use of seals of fictitious bodies, historical state insignia or the names of former state structures, which can mislead both citizens and public officials. To limit potential abuses in this area, the legislator could introduce provisions regulating the use of symbols and graphics that closely resemble official seals and documents.

In conclusion, the article presents the threats that movements inspired by the US sovereign citizen movement may pose to the legal order and public security in Poland. An effective response to the actions of sovereign citizens requires cooperation between the public and private sectors, as well as educational and legislative measures aimed at limiting the spread of such ideologies.

[70] L. Jamróz, *Prawo do sądu a zjawisko pieniactwa sądowego* (Eng. The right to a fair trial and the phenomenon of judicial litigation), in: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (eds.), Wrocław 2018, pp. 495–504, https://repozytorium.uni.wroc.pl/dlibra/publication/95758/edition/89860/prawo-do-sadu-a-zjawisko-pieniactwa-sadowego-jamroz-lech [accessed: 18 X 2024].

Bibliography

Challacombe D.J., Lucas P.A., *Postdicting violence with sovereign citizen actors: An exploratory test of the TRAP-18*, "Journal of Threat Assessment and Management" 2019, vol. 6, no. 1, pp. 51–59. https://doi.org/10.1037/tam0000105.

Łódzki B., *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej* (Eng. Fake news – disinformation in online media and forms of combating it in the international space), "Polityka i Społeczeństwo" 2017, vol. 15, no. 4, pp. 19–30. https://doi.org/10.15584/polispol.2017.4.2.

Marszałek P., *Rynek czy państwo w bankowości – bankowość centralna versus bankowość wolna* (Eng. Market or government in banking – central banking vs. free banking), "Ryzyko i Zrównoważony Rozwój" 2011, no. 70, pp. 125–136.

Matheson C.L., *Psychotic Discourse: The Rhetoric of the Sovereign Citizen Movement*, "Rhetoric Society Quarterly" 2018, vol. 2, no. 48, pp. 187–206.

Morozov A., Bruinsma R., Rudnick J., *Assembly of viruses and the pseudo law of mass action*, "Biophysical Journal" 2009, vol. 96, no. 3, pp. 419a–420a.

Mullan P.C., *The Liberty Dollar and Bernard von NotHaus*, in: *A History of Digital Currency in the United States. New Technology in an Unregulated Market*, New York 2016, pp. 87–109. http://dx.doi.org/10.1057/978-1-137-56870-0_3.

Piękoś K., *Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków* (Eng. Cyberattacks on banking systems and critical infrastructure: analysis of selected cases), "Krakowskie Studia Małopolskie" 2017, no. 22, pp. 106–113.

Sarteschi Ch.M., *Sovereign Citizens and QAnon: The Increasing Overlaps with a Focus on Child Protective Service (CPS) Cases*, "International Journal of Coercion, Abuse & Manipulation" 2023, vol. 6. https://doi.org/10.54208/1000/0006/006.

White L.H., *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold*, "The Cato Journal" 2014, vol. 34, no. 2, pp. 281–301. http://dx.doi.org/10.2139/ssrn.2406983.

Internet sources

Akt oskarżenia z dnia 4 XI 2024 r. (Eng. Indictment act of 4 XI 2024), Zawodowy Polak, https://www.zawodowy-polak.pl/KC-Akt_Oskarzenia-NFPR-4.11.2024.pdf [accessed: 14 VII 2025].

A Quick Guide to Sovereign Citizens, UNC School of Government, November 2013, https://www.sog.unc.edu/sites/www.sog.unc.edu/files/Sov%20citizens%20quick%20guide%20Nov%2013.pdf [accessed: 1 I 2025].

Berkowska T., *Akt oskarżenia* (Eng. Indictment act), Zawodowy Polak, https://www.zawodowy-polak.pl/TB_NFKS-MK-Akt_Oskarzenia-27.11.2024.pdf [accessed: 1 I 2025].

Bielecki J., *Amerykanie mają dość ubezpieczycieli* (Eng. Americans are fed up with insurers), Rzeczpospolita, 11 XII 2024, https://www.rp.pl/przestepczosc/art41568761-amerykanie--maja-dosc-ubezpieczycieli [accessed: 1 VII 2025].

Bosa A., *Decyzja Zwierzchnika Władzy w Rzeczypospolitej Polskiej od której nie przysługuje zażalenie* (Eng. Decision of the Head of Authority in the Republic of Poland against which there is no right of appeal), Zawodowy Polak, 13 VIII 2023, https://www.zawodowy-polak.pl/AB-NFUFG_13.08.2023.pdf [accessed: 1 I 2025].

Bryda D., *Deklaracja Samostanowienia i Odpowiedzialności* (Eng. Declaration of self-determination and responsibility), Zawodowy Polak, 12 I 2024, https://www.zawodowy-polak.pl/DB-Deklaracja_12.01.2024r.pdf [accessed: 25 X 2024].

Cichocki T., *Dekret Zwierzchnika Władzy w Rzeczypospolitej Polskiej 1-2018* (Eng. Decree of the Head of Authority in the Republic of Poland 1-2018), Piaseczno, 25 X 2018, https://www.tcichocki.pl/Dekret%20Zwierzchnika%20W%C5%82adzy%20w%20RP%201-2018%202018.10.25.pdf [accessed: 25 X 2024].

Cichocki T., *Polki i Polacy – już czas wypowiedzieć posłuszeństwo nielegalnej władzy działającej na naszą szkodę!!! List otwarty* (Eng. Polish women and men – it is time to declare disobedience to the illegitimate authorities acting to our detriment!!! An open letter), https://www.tcichocki.pl/20150402_Wypowiedzenie_posluszenstwa_organom_panstwa.pdf [accessed: 2 IV 2025].

Crowell M., *A Quick Guide to Sovereign Citizens*, "Administration of Justice Bulletin" 2015, no. 4, https://www.sog.unc.edu/sites/default/files/reports/aojb1504.pdf [accessed: 1 VII 2025].

Deklaracja Samostanowienia i Odpowiedzialności (Eng. Declaration of self-determination and responsibility), Zawodowy Polak, https://www.zawodowy-polak.pl/index.php?title=Deklaracja_Samostanowienia_i_Odpowiedzialno%C5%9Bci [accessed: 15 XII 2024].

Eichner J., *"Reichsdeutsche" fordern bayerische Justiz heraus. Hier ist „deutsches Reichsgebiet"!*, Bayerischer Rundfunk, 23 IV 2016, https://www.br.de/nachricht/reichsbuerger-bayern-gerichtsvollzieher-100.html [accessed: 25 X 2024].

FBI, *Domestic terrorism. The Sovereign Citizen Movement*, 13 IV 2010, https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement [accessed: 15 XII 2024].

FBI's Counterterrorism Analysis Section, *Sovereign Citizens. A Growing Domestic Threat to Law Enforcement*, FBI Law Enforcement Bulletin, 1 IX 2011, https://leb.fbi.gov/articles/featured-articles/sovereign-citizens-a-growing-domestic-threat-to-law-enforcement [accessed: 1 I 2025].

Ferfecki W., *Filozof ogłosił się głową państwa* (Eng. Philosopher declared himself head of state), Rzeczpospolita, 6 VIII 2020, https://www.rp.pl/polityka/art8857531-filozof-oglosil-sie-glowa-panstwa [accessed: 1 VII 2025].

Ferfecki W., *Jan Zbigniew Potocki kontra współpracownicy. Bunt przeciw samozwańczemu prezydentowi* (Eng. Jan Zbigniew Potocki vs. colleagues. Rebellion against the self-appointed president), Rzeczpospolita, 17 V 2024, https://www.rp.pl/polityka/art40374471-jan-zbigniew-potocki-kontra-wspolpracownicy-bunt-przeciw-samozwanczemu-prezydentowi [accessed: 25 X 2024].

Ferfecki W., *Samozwańczy król Polski z darmowymi spotami w TVP* (Eng. Self-appointed king of Poland with free spots in TVP), Rzeczpospolita, 13 IX 2023, https://www.rp.pl/polityka/art39102811-samozwanczy-krol-polski-z-darmowymi-spotami-w-tvp [accessed: 1 VII 2025].

Garland T., *24 III 2020 r. PKW TERESA GARLAND zgłoszenie kandydatury po raz trzeci* (Eng. 24 III 2020 PKW TERESA GARLAND application for the third time), Teresa Garland, https://teresagarlandprezydent.wordpress.com/2020/03/24/24-iii-2020r-pkw-teresa-garland-zgloszenie-kandydatury-po-raz-trzeci/ [accessed: 1 I 2025].

Garland T., *Sprzeciw i apelacja na wyrok z dnia 12 X 2023r. o sygn. akt IIK 451/21 w Sądzie Rejonowym w Wieliczce* (Eng. Objection and appeal against the judgment of 12 X 2023 ref. no. IIK 451/21 in the District Court in Wieliczka), Tymczasowa Rada Stanu, https://tymczasowaradastanu.wordpress.com/2023/11/24/teresa-garland-sprzeciw-i-apelacja-na-wyrok-z-dnia-12-x-2023r-o-sygn-akt-iik-451-21-w-sadzie-rejonowym-w-wieliczce/ [accessed: 1 I 2025].

Gębuś R., *Samozwańczy Rząd Tymczasowej Rady Stanu apeluje o poparcie do lęborskiej rady. Burmistrz powiadamia prokuraturę* (Eng. Self-appointed Government of the Provisional Council of State appeals for support to Lębork council. The mayor notifies the public prosecutor's office), Lębork Nasze Miasto, 19 IV 2021, https://lebork.naszemiasto.pl/samozwanczy-rzad-tymczasowej-rady-stanu-apeluje-o-poparcie/ar/c15-8238215 [accessed: 1 I 2025].

Interpelacja nr 5712 w sprawie zarejestrowania firmy POLAND REPUBLIC OF w rejestrze Amerykańskiej Komisji Papierów Wartościowych (Eng. Interpellation no. 5712 concerning registration of POLAND REPUBLIC OF in the register of the US Securities Exchange Commission), Sejm RP, https://www.sejm.gov.pl/sejm9.nsf/interpelacja.xsp?typ=INT&nr=5712 [accessed: 1 VII 2025].

IRS Criminal Investigation, *Sovereign citizen sentenced to 9 years in prison for $3.4 million tax fraud scheme, filing a false lien, and absconding while on bond*, Press Release, 22 V 2024, https://www.irs.gov/compliance/criminal-investigation/sovereign-citizen-sentenced-to-9-years-in-prison-for-3-point-4-million-tax-fraud-scheme-filing-a-false-lien-and-absconding-while-on-bond [accessed: 1 VII 2025].

Jamróz L., *Prawo do sądu a zjawisko pieniactwa sądowego* (Eng. The right to a fair trial and the phenomenon of judicial litigation), in: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (eds.), Wrocław 2018, pp. 495–504, https://repozytorium.uni.wroc.pl/dlibra/publication/95758/edition/89860/prawo-do-sadu-a-zjawisko-pieniactwa-sadowego-jamroz-lech [accessed: 18 X 2024].

Jesionowska K., *Dowód osobisty suwerena II Rzeczypospolitej Polskiej* (Eng. ID of the sovereign of the Second Polish Republic), Straż Graniczna, 3 XII 2021, https://www.slaski.strazgraniczna.pl/sm/aktualnosci/43765,Dowod-osobisty-suwerena-II-Rzeczypospolitej-Polskiej.html [accessed: 25 X 2024].

Kalinowski IV C., *A Legal Response to the Sovereign Citizen Movement*, "Montana Law Review" 2019, vol. 80, no. 2, pp. 153–210, https://scholarworks.umt.edu/mlr/vol80/iss2/2/ [accessed: 25 X 2024].

Kelley B.J., *Interview with a sovereign: Judge Anna's World*, Southern Poverty Law Center, 15 XII 2017, https://www.splcenter.org/hatewatch/2017/12/15/interview-sovereign-judge-anna%E2%80%99s-world [accessed: 1 I 2025].

Kent S.A., *Freemen, Sovereign Citizens, and the Challenge to Public Order in British Heritage Countries*, "International Journal of Cultic Studies" 2015, no. 6, https://skent.ualberta.ca/wp-content/uploads/2015/06/Freemen-Internl-J-of-Cultic-Studies.pdf [accessed: 25 X 2024].

Kiedy powinieneś zastrzelić agenta? (Eng. When should you shoot a cop?), YouTube channel Moron3k, https://youtu.be/AJ2HJWhmrdE?si=kbENyPyZmWGeG2_C [accessed: 14 VII 2025].

IV Konwencja Genewska (Eng. IV Geneva Convention), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=IV_Konwencja_Genewska [accessed: 1 I 2025].

Koppelman Ch., *Construction as Resistance. Constructing a desired and envisioned future to perceived oppression for the sovereign citizen milieu in the Netherlands*, Utrecht University 2024, https://studenttheses.uu.nl/bitstream/handle/20.500.12932/47667/h.c.koppelman_6919642_thesis_CSHR.pdf?sequence=1&isAllowed=y [accessed: 1 VII 2025].

Koźlik B., *Doręczenie odpisu postanowienia zwierzchnika władzy w Rzeczypospolitej Polskiej* (Eng. Delivery of a copy of the order of the head of authority in the Republic of Poland), Zawodowy Polak, 27 VI 2022, https://zawodowy-polak.pl/BK-ost_postanowienie_bank_27.06.2022.pdf [accessed: 1 I 2025].

Król P., *Analiza zamachów na osoby publiczne – skuteczność działań prewencyjnych służb bezpieczeństwa i konsekwencje polityczno-społeczne* (Eng. Analysis of assassinations on public figures – effectiveness of preventive actions by security forces and political and social consequences), "Kwartalnik Kadry Kierowniczej Policji" 2024, no. 3, https://kwartalnik.akademiapolicji.edu.pl/images/stories/2024/3/krl.pdf [accessed: 1 VII 2025].

Majchrowski J., *Kwestia sukcesji prezydenckiej na obczyźnie* (Eng. The question of presidential succession in exile), in: *Myśl polityczna: od historii do współczesności*, B. Stoczewska, M. Jaskólski (eds.), Kraków 2000, pp. 253–260, https://ruj.uj.edu.pl/server/api/core/bitstreams/2cc6a415-0de3-4172-bbd2-2cd16fce2235/content [accessed: 1 I 2025]

Mendyk B., *Jak reagować na petycje pełne teorii spiskowych?* (Eng. How to respond to petitions full of conspiracy theories?), Pismo Samorządu Terytorialnego "Wspólnota", 3 IV 2024, https://wspolnota.org.pl/newsletter/jak-reagowac-na-petycje-pelne-teorii-spiskowych [accessed: 1 I 2025].

Meyer C., *5 Common Crimes Committed by Sovereign Citizens*, Police1, 6 IX 2024, https://www.police1.com/community/articles/5-common-crimes-committed-by-sovereign-citizens-1KKxo42li5FVeANM/ [accessed: 1 I 2025].

Murder of Dallas Police Officer Marks Latest in String of Violent Sovereign Citizen Encounters with Law Enforcement, Anti-Defamation League, 9 XII 2024, https://www.adl.org/resources/article/murder-dallas-police-officer-marks-latest-string-violent-sovereign-citizen [accessed: 1 I 2025].

Najemnicy NFUMiG Konstancin Jeziorna (Eng. Mercenaries of NFUMiG Konstancin Jeziorna), YouTube channel Zawodowy Polak, 2 VII 2024, https://www.youtube.com/watch?v=jeH8LX0eYfY [accessed: 1 VII 2025].

Najwyższy Trybunał Narodowy. Akt ustanowienia (Eng. The Supreme National Tribunal. Act of Establishment), Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/najwyzszy-trybunal-narodowy/ [accessed: 21 VII 2025].

Nie można nagrywać najemników i lokalu wyborczego w Kisielsku? (Eng. Can't the mercenaries and the polling station in Kisielsk be recorded?), YouTube channel Zawodowy Polak, 9 VI 2024, https://www.youtube.com/watch?v=8nAon2vpOTQ [accessed: 15 XII 2024].

„Nielegalne" zatrzymanie przez Policję i ZAWODOWY POLAK | Bagieta rozkłada interwencje #3 (Eng. 'Illegal' Police detention and ZAWODOWY POLAK | Bagieta *breaks down interventions #3*), YouTube channel Sierżant Bagieta, 26 II 2020, https://www.youtube.com/watch?v=EgQWjQEDq_A [accessed: 1 I 2025].

Ośrodek Monitorowania Zachowań Rasistowskich i Ksenofobicznych, *Teresa Garland będąca prorosyjską patocelebrytką w końcu zatrzymana przez policję* (Eng. Teresa Garland pro-Russian scandalous celebrity finally detained by the Police), Facebook, 28 IX 2022, https://www.facebook.com/osrodek.monitorowania/posts/teresa-garland-b%C4%99d%C4%85ca-prorosyjsk%C4%85-patocelebrytk%C4%85-w-ko%C5%84cu-zatrzymana-przez-policj/1917138658461258/ [accessed: 1 I 2025].

Pismo z dnia 28 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) (Eng. Letter of 28 V 2024 on brazen violations of constitutional rights, dignity, human and civil liberties) Ref. no. I Co 3161/2, Zawodowy Polak, https://www.zawodowy-polak.pl/TB-NFSR-W-wa_Wola_28.05.2024.pdf [accessed: 14 VII 2024].

Pismo z dnia 7 III 2024 r. dotyczące braku uprawnień do pełnienia funkcji sędziego, dyrektora i prezesa – dyskryminacji (Eng. Letter of 7 III 2024 on the lack of qualifications to hold the position of discrimination judge, director and president), Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFSR-Grojec_7.03.2024.pdf [accessed: 14 VII 2025].

Pismo z dnia 8 V 2024 r. dotyczące bezczelnego łamania konstytucyjnych praw, godności, wolności człowieka i obywatela (…) (Eng. Letter of 8 V 2024 on brazen violations of constitutional rights, dignity, human and civil liberties) Ref. no.: 4161-0.Ds 783.24, Zawodowy Polak, https://www.zawodowy-polak.pl/KC-NFPR-Lukow_8.05.2024.pdf [accessed: 14 VII 2024].

Powers A., *How Sovereign Citizens Helped Swindle $1 Billion From the Government They Disavow*, The New York Times, 29 III 2019, https://www.nytimes.com/2019/03/29/business/sovereign-citizens-financial-crime.html [accessed: 25 X 2024].

Powołanie Rządu Wolnej Polski (Eng. Establishment of the Government of Free Poland), YouTube channel Trybunał Narodowy, https://www.youtube.com/watch?v=1HyXzBXXfOs&t=1s [accessed: 1 VII 2025].

Powołano Rząd Wolnej Polski (Eng. The Government of Free Poland was established), Demokracja i Sprawiedliwość, https://demokracjaisprawiedliwosc.pl/powolano-rzad-wolnej-polski/ [accessed: 1 VII 2025].

Prawo wyborcze (Eng. Electoral law), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Prawo_wyborcze [accessed: 1 I 2025].

Prezes NBP Glapiński, Teresa Garland i demokracja (Eng. President of the NBP Glapiński, Teresa Garland and democracy), YouTube channel Fides Polska TV, 16 XI 2018, https://www.youtube.com/watch?v=j1Bd4ZToToE [accessed: 1 I 2025].

Protokoły Mędrców Syjonu (Eng. The protocols of the Sages of Zion), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Protoko%C5%82y_M%C4%99drc%C3%B3w_Syjonu [accessed: 1 VII 2025].

Redemption Theory/Strawman Theory, Anti-Defamation League, https://extremismterms.adl.org/glossary/redemption-theorystrawman-theory [accessed: 14 VII 2025].

Religia (Eng. Religion), Zawodowy Polak, https://zawodowy-polak.pl/index.php?title=Religia [accessed: 9 VII 2025].

Report and Recommendation, Case No. 1:16-cv-614, https://www.govinfo.gov/content/pkg/USCOURTS-ohsd-1_16-cv-00614/pdf/USCOURTS-ohsd-1_16-cv-00614-0.pdf [accessed: 1 I 2025].

Sajór G., *Nie wytrzymał ciśnienia. Mariusz Max Kolonko po odejściu z dziennikarstwa został Presidentem* (Eng. He couldn't withstand the pressure. Mariusz Max Kolonko became President after leaving journalism), Press, 20 V 2022, https://www.press.pl/tresc/70879,[na-weekend]-nie-wytrzymal-cisnienia_-mariusz-max-kolonko-po-odejsciu-z-dziennikarstwa-zostal-presidentem [accessed: 1 VII 2025].

Samozwańcza prezydent sypnęła petycjami (Eng. Self-appointed president filed petitions), Super Tydzień Chełmski, 15 IV 2021, https://www.supertydzien.pl/artykul/10406,samozwancza-prezydent-sypnela-petycjami [accessed: 1 I 2025].

Sidorowicz J., *Broń od gminy dla każdego rdzennego mieszkańca Starego Sącza? Jest petycja w sprawie programu „Broń palna plus"* (Eng. Arms from the municipality for every native of Stary Sącz? There is a petition on the 'Firearms plus' programme), Kraków.Wyborcza.pl, 26 IX 2022, https://krakow.wyborcza.pl/krakow/7,44425,28955388,bron-od-gminy-dla-kazdego-rdzennego-mieszkanca-starego-sacza.html [accessed: 1 I 2025].

Silver Certificates, NORFED Liberty Dollar, https://norfed.info/silver-certificates/ [accessed: 1 I 2025].

Spungen D., *How Financial Institutions Should Handle "Sovereign Citizens"*, Amundsen Davis, 18 III 2024, https://www.amundsendavislaw.com/banking-brief-financial-services-insights/how-financial-institutions-should-handle-sovereign-citizens [accessed: 1 I 2025].

Starzewski Ł., *Polska zarejestrowana jako firma w USA? RPO prosi MSZ o zbadanie skargi obywatela* (Eng. Poland registered as a company in the USA? The Ombudsman asks the Ministry of Foreign Affairs to investigate citizen's complaint), Rzecznik Praw Obywatelskich, 24 II 2020, https://www.rpo.gov.pl/pl/content/polska-zarejestrowana-jako-firma-w-usa-rpo-prosi-msz-o-zbadanie-skargi-obywatela [accessed: 25 X 2024].

The Sovereign Citizen Movement: Common Documentary Identifiers & Examples, Anti-Defamation League, 5 XII 2016, https://www.adl.org/resources/reports/the-sovereign-citizen-movement-common-documentary-identifiers-examples [accessed: 25 X 2024].

The Sovereigns: A Dictionary of the Peculiar, The Southern Poverty Law Center, 1 VIII 2010, https://www.splcenter.org/fighting-hate/intelligence-report/2010/sovereigns-dictionary-peculiar [accessed: 14 VII 2024].

Top Russian central banker shot to death, NBC News, 14 IX 2006, https://www.nbcnews.com/id/wbna14826889 [accessed: 1 VII 2025].

Uchwała Najwyższego Trybunału Narodowego o nieważności wyroków w imieniu Rzeczypospolitej Polskiej (Eng. Resolution of the Supreme National Tribunal on the invalidity of judgments in the name of the Republic of Poland), trybunał-narodowy.pl, 13 XI 2024, https://www.trybunal-narodowy.pl/uchwala-najwyzszego-trybunalu-narodowego-o-niewaznosci-wyrokow-w-imieniu-rzeczypospolitej-polskiej/ [accessed: 1 VII 2025].

Wyrok zaoczny w imieniu Zwierzchnika Władzy w Rzeczypospolitej Polskiej (Eng. A sentence passed in absentia on behalf of the Head of Authority in the Republic of Poland), Zawodowy Polak, 10 IX 2024, https://www.zawodowy-polak.pl/L.K_WKKom_10.09.2024.pdf [accessed: 25 X 2024].

Zaremba J., *„Leczył" z zaburzeń psychicznych i masturbacji. „Książę" Świętopełk-Zawadzki na Narodowym Marszu Papieskim* (Eng. He 'treated' for mental disorders and masturbation. 'Prince' Świętopełk-Zawadzki at the National Papal March), Gazeta.pl, 3 IV 2023, https://kobieta.gazeta.pl/kobieta/7,107881,29626596,leczyl-z-zabrzen-psychicznych-i-homoseksualizmu.html [accessed: 1 VII 2025].

Legal acts

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

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

Act of 8 December 2017 on the State Protection Service (consolidated text, Journal of Laws of 2025, item 34, as amended).

Act of 11 July 2014 on petitions (consolidated text, Journal of Laws of 2018, item 870).

Act of 24 May 2013 on direct coercive measures and firearms (consolidated text, Journal of Laws of 2025, item 555).

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

Act of 6 June 1997 The penal code (consolidated text, Journal of Laws of 2025, item 383).

Act of 6 June 1997 Code of criminal procedure (consolidated text, Journal of Laws of 2025, item 46, as amended).

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

Act of 8 March 1990 on municipal self-government (consolidated text, Journal of Laws of 2024, item 1465, as amended).

Act of 20 May 1971 Code of petty offences (consolidated text, Journal of Laws of 2023, item 2119, as amended).

Patryk Król

Second-cycle student at Poznań University of Economics and Business.

Contact: patkro12@gmail.com

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Kontakt / Contact
tel. / phone (+48) 22 58 58 613
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Druk / Print
Mazowieckie Centrum Poligrafii Sp. z o.o.
ul. Ciurlionisa 4, 05-270 Marki
tel. 505 727 782