PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Zespół redakcyjny

dr Daria Olender (redaktor naczelny)
Maria Kiszczyc (sekretarz Redakcji)
Aleksandra Dąbała, Aneta Olkowska, Izabela Paczesna, Monika Sikora (redakcja, korekta)
Sylwia Kłobuszewska (tłumaczenie, korekta wersji anglojęzycznej)
Agnieszka Dębska, Izabela Laskus-Rock (skład)

Projekt okładki

Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2026

ISSN 2080-1335
e-ISSN 2720-0841

Punkty MEiN: 20

Numer zamknięto i oddano do druku w październiku 2026 r.

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

Artykuły wyrażają poglądy autorów

Deklaracja o wersji pierwotnej

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

Wersje językowe

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

Indeksacja w bazach danych

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się w bazach:
ERIH PLUS, Directory of Open Access Journals, Central and Eastern European Online Library, Central European Journal of Social Science and Humanities, Index Copernicus i Polska Bibliografia Naukowa (PBN)

Zgłaszanie tekstów

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

Rada naukowa

dr Paweł Chomentowski, Agencja Bezpieczeństwa Wewnętrznego
dr hab. Eugeniusz Cieślak, ekspert niezależny
dr Marcin Fiedziukiewicz, PhD, MRSC Royal Society of Chemistry, ekspert niezależny
prof. dr hab. Ewa Gruza, Uniwersytet Komisji Edukacji Narodowej w Krakowie
dr Agnieszka Jakóbowska, ekspert niezależny
dr Robert Lach, ekspert niezależny
prof. dr hab. Andrzej Mania, Uniwersytet Jagielloński
dr hab. inż. Bogdan Michailiuk, prof. ASzWoj, Akademia Sztuki Wojennej
prof. dr hab. Andrzej Pieczywok, Uniwersytet Kazimierza Wielkiego
dr hab. Agata Tyburska, prof. AP, Akademia Policji w Szczytnie
dr hab. Jakub Zięty, prof. UWM, Uniwersytet Warmińsko-Mazurski w Olsztynie

Recenzenci 35 numeru

dr Agata Andruszkiewicz
David Cybulski
dr Irena Doroszkiewicz
dr Łukasz Foryś
r. pr. Krzysztof Kołtan
dr hab. inż. Witalis Pellowski, prof. AWL
dr Jacek Pietraszewski
dr hab. inż. Zdzisław Polcikiewicz, prof. UMK
dr Dariusz Pożaroszczyk
dr Jarosław Przyjemczak
dr hab. Ilona Urych, prof. ASzWoj
prof. dr hab. Waldemar Zubrzycki

SPIS TREŚCI

Wstęp redaktora naczelnego 7

ARTYKUŁY

Tomasz Gergelewicz
Informacja jako narzędzie wojny kognitywnej w kontekście wojny hybrydowej 15

Janusz Leżoń
Wsparcie układu pozamilitarnego przez Wojska Obrony Terytorialnej jako element regulacji ograniczających efektywne wykorzystanie formacji w sytuacjach kryzysowych 39

Michał Antoniuk
Bezpieczeństwo wewnętrzne w erze cyfrowej – wyzwania i kierunki rozwoju 71

Radosław Korda
Erozja odporności państwa jako wyzwanie dla bezpieczeństwa wewnętrznego – propozycja ramy analitycznej umożliwiającej wczesne rozpoznawanie zagrożeń społecznych i instytucjonalnych 91

Łukasz Cymbaluk
Państwo Islamskie w Chorasanie a potencjalne zagrożenie dla bezpieczeństwa Polski 113

Paweł Łuszcz
Sposób postępowania funkcjonariuszy Służby Więziennej z osadzonymi należącymi do struktur przestępczości zorganizowanej – środki bezpieczeństwa i nadzoru 135

Marcin Hubicki
Służby wywiadu i bezpieczeństwa Chińskiej Republiki Ludowej – struktura, reformy i nadzór nad służbami w erze Xi Jinpinga 149

ARTYKUŁY RECENZYJNE / RECENZJE

Iwona Osłowska
Bezpieczeństwo miasta wobec współczesnych wyzwań, Natalia Moch 187

Wojciech Dylewski
Szkic do studium przypadku – *Śpiące psy*... Marka Świerczka 199

PRACE KONKURSOWE

Anna Nastuła
Rola oraz możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa Rzeczypospolitej Polskiej 227

Kamil Leśniewski
Kryminalistyczne aspekty pobierania próbek węgla kamiennego dla celów postępowania karnego 255

VARIA

Mikrobiologia w służbie ochrony dziedzictwa kulturowego
Wywiad z dr Magdaleną Dydą 287

O bezpieczeństwie w zmieniającym się świecie
Wywiad z dr. hab. inż. Marianem Żuberem 299

Szanowni Państwo!

Gdy obejmowałam stanowisko redaktora naczelnego „Przeglądu Bezpieczeństwa Wewnętrznego" (PBW), założyłam sobie szerokie, interdyscyplinarne podejście do problematyki bezpieczeństwa wewnętrznego, traktując je jako zjawisko wielowymiarowe. 35 numer, który mam przyjemność Państwu zarekomendować, jest wyrazem tej perspektywy. Nadal, co w pełni zrozumiałe, gorącym tematem pozostaje wojna hybrydowa. Jednym z jej narzędzi jest informacja, która okazuje się równie niebezpieczna jak tradycyjne środki walki. Rozwój nowoczesnych technologii oraz bezrefleksyjne przyjmowanie informacji przez społeczeństwo sprawiają, że wojna kognitywna może być skutecznym mechanizmem wrogiego wpływu. Charakterystyki i uporządkowania zasadniczych pojęć związanych z tym tematem podjął się płk dr Tomasz Gergelewicz. Słuszna wydaje się jego konstatacja, że za pomocą dezinformacji, na którą składają się m.in. fake newsy, manipulacja faktami i szum informacyjny, agresor może modyfikować postawy i zachowania grupy docelowej w sposób zgodny ze swoimi intencjami i celami.

Ważną rolę w takich działaniach odgrywa cyberprzestrzeń. Warto przypomnieć, że październik to Europejski Miesiąc Cyberbezpieczeństwa. Ma to być czas działań zwiększających świadomość społeczną w tym zakresie. W to zadanie wpisuje się artykuł Michała Antoniuka, który przeanalizował wpływ technologii cyfrowych na charakter zagrożeń wewnętrznych oraz funkcjonowanie instytucji odpowiedzialnych za bezpieczeństwo państwa. Autor zauważa, że jego ochrona obejmuje również zapewnienie bezpieczeństwa infrastrukturze cyfrowej i danym, przeciwdziałanie dezinformacji, a także budowanie odporności społeczeństwa na zagrożenia informacyjne. Oznacza to odejście od tradycyjnego modelu skoncentrowanego

na reagowaniu po wystąpieniu zagrożenia na rzecz modelu opartego na zarządzaniu ryzykiem i wzmacnianiu odporności.

Tematykę zagrożeń instytucjonalnych oraz odporności państwa i społeczeństwa porusza także dr inż. Radosław Korda. Wychodzi on z założenia, że współczesne państwa są relatywnie dobrze przygotowane do reagowania na zdarzenia kryzysowe, gorzej natomiast identyfikują procesy długotrwałej erozji w sferach: społecznej, instytucjonalnej i informacyjnej. W artykule proponuje trójpoziomową ramę analityczną, która umożliwi obserwację symptomów osłabienia odporności państwa przed wystąpieniem jawnego kryzysu.

O zarządzaniu w sytuacji jego zaistnienia pisze z kolei ppłk Janusz Leżoń. Art. 25 znowelizowanej w 2026 r. ustawy o zarządzaniu kryzysowym (ZK) traktuje o możliwości wykorzystania w takiej sytuacji Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP). W systemie ZK istotną rolę odgrywają Wojska Obrony Terytorialnej (WOT), wspierając administrację publiczną w przypadku zagrożeń o charakterze niemilitarnym. Autor wskazuje, że obowiązujące regulacje prawne odnoszące się do użycia SZ RP, w tym WOT, w sytuacjach kryzysowych wymagają gruntownej analizy i zmian, polegających m.in. na przyznaniu WOT większej autonomii w realizacji zadań. Pozwoliłoby to na optymalne wykorzystywanie potencjału tych rodzajów wojsk w działaniach podejmowanych w tego rodzaju sytuacjach.

W problematykę dotyczącą formacji mundurowych wpisuje się artykuł ppłk. dr. Pawła Łuszcza, który pochylił się nad środkami bezpieczeństwa i nadzoru pozostającymi w dyspozycji funkcjonariuszy Służby Więziennej (SW) przy postępowaniu z osadzonymi należącymi do struktur przestępczości zorganizowanej. Autor przyjmuje, że podstawą właściwego podejścia powinna być gruntowna wiedza o osadzonych oraz wymiana informacji między komórkami SW. Nie tylko zwiększy to poziom bezpieczeństwa osadzonych i funkcjonariuszy SW, lecz także może pozytywnie wpłynąć na oddziaływania prowadzone przez organy śledcze i postępowania sądowe.

W PBW istotnym obszarem problemowym jest bezpieczeństwo rozpatrywane w kontekście zagrożeń i wyzwań pochodzących z otoczenia zewnętrznego państwa. Mimo że Polska nie znajduje się w centrum zainteresowania tzw. Państwa Islamskiego, to w ramach dżihadystycznej ideologii tego ugrupowania jest klasyfikowana – z uwagi na przynależność do szeroko pojętego Zachodu – jako jedna z wrogich demokracji. W Polsce organizacja ta może tworzyć sieci

operacyjne, podejmować próby radykalizacji i rekrutacji młodych ludzi czy pozyskania funduszy. Zachęcam do lektury artykułu dr. Łukasza Cymbaluka, w którym autor przedstawia specyfikę działalności Państwa Islamskiego w Chorasanie oraz podejmuje próbę identyfikacji potencjalnych zagrożeń, jakie może ono stwarzać dla bezpieczeństwa Rzeczypospolitej Polskiej.

Jednym z najważniejszych aktorów na arenie międzynarodowej pozostają Chiny. Marcin Hubicki podjął się analizy współczesnej struktury aparatu wywiadowczego i bezpieczeństwa Chińskiej Republiki Ludowej, z uwzględnieniem roli kierowniczo-nadzorczej Komunistycznej Partii Chin (KPCh), po reformach przeprowadzonych w latach 2013–2025 przez sekretarza generalnego KPCh Xi Jinpinga. Z uwagi na specyfikę przedmiotu analizy jej wyniki nie dostarczają wyczerpującej wiedzy na temat aktywności operacyjnej chińskich służb. Pozwalają jednak na identyfikację podstawowych mechanizmów ich biurokratycznego funkcjonowania i nadzoru nad nimi, umożliwiając zrozumienie roli tych instytucji w systemie bezpieczeństwa Chin.

W dziale Prace konkursowe prezentujemy dwa artykuły, które powstały na podstawie rozpraw doktorskich nagrodzonych w konkursie Szefa ABW. Dr Anna Nastuła opisała możliwości wykorzystania wywiadu jawnoźródłowego w zapewnieniu bezpieczeństwa RP, z uwzględnieniem aspektów prawnych i pozaprawnych. OSINT ma dziś kluczowe znaczenie w wielu sektorach – od cyberbezpieczeństwa, przez biznes i korporacje, po dziennikarstwo śledcze. Dostęp do aktualnych, sprawdzonych informacji to też jeden z najważniejszych czynników wpływających na stabilność i odporność państwa.

Dość wąskiej problematyki dotyczy drugi z artykułów. Dr Kamil Leśniewski swoją rozprawę doktorską poświęcił zagadnieniu pobierania próbek węgla kamiennego na potrzeby postępowania karnego, z uwzględnieniem zasad taktyki kryminalistycznej oraz wymogów procedury karnej. Autor, prawnik z wykształcenia, podkreśla, że sprawne prowadzenie czynności wykrywczo-dowodowych w sprawach dotyczących przestępczości na szkodę spółek węglowych wymaga posiadania przez osoby odpowiedzialne za te czynności odpowiedniego przygotowania i rozeznania w specyfice górniczej.

Jednym z mniej oczywistych wymiarów bezpieczeństwa państwa jest ochrona jego dziedzictwa kulturowego – dzieł sztuki, zbiorów archiwalnych i muzealnych. O tym, jak poważne zagrożenie stanowią

dla nich grzyby czy bakterie, rozmawiamy z dr Magdaleną Dydą, która zajmuje się zabezpieczaniem muzealiów przed szkodliwym wpływem czynników biologicznych. W rozmowie wiele uwagi poświęcamy praktycznym aspektom zapobiegania tego rodzaju zagrożeniom, również w sytuacji konfliktu zbrojnego.

O wielowymiarowości i potrzebie holistycznego podejścia do problematyki bezpieczeństwa mówi z kolei w wywiadzie dr hab. inż. Marian Żuber, prof. ANS i UPWr, współorganizator III Międzynarodowej Konferencji Naukowej z cyklu „Współczesne bezpieczeństwo. Wyzwania. Szanse. Zagrożenia". Jej uczestnicy dyskutowali o wojnie hybrydowej, zagrożeniach w cyberprzestrzeni, niekontrolowanej ekspansji sztucznej inteligencji, znaczeniu proxy wars dla stabilności świata, roli obrony cywilnej we współczesnym konflikcie zbrojnym, zagrożeniach związanych ze zmianami klimatycznymi, a także o doświadczeniach płynących z wojny rosyjsko-ukraińskiej. Zdaniem Profesora w obliczu dynamicznego rozwoju technologii i zmian geopolitycznych tradycyjne podejście do obronności państwa nie jest już wystarczające.

W tym numerze PBW publikujemy również recenzje dwóch książek. Jedną z nich jest monografia *Bezpieczeństwo miasta wobec współczesnych wyzwań* Natalii Moch. Badania przeprowadzone przez autorkę książki służą budowaniu przyjaznej przestrzeni miejskiej i poczucia bezpieczeństwa wśród mieszkańców, którzy w obecnym czasie mogą obawiać się różnego rodzaju zagrożeń wpływających na ich codzienne życie. Do zapoznania się z tą pozycją zachęca dr Iwona Osłowska. Kolejną książką są *Śpiące psy. Rosyjskie gry agenturalne wobec Urzędu Ochrony Państwa początkiem lat 90. XX w.* autorstwa Marka Świerczka. Krytyczną analizę publikacji poświęconej sprawie byłego funkcjonariusza Służby Bezpieczeństwa, który szpiegował na rzecz radzieckiego, a następnie rosyjskiego wywiadu wojskowego GRU, przygotował płk Wojciech Dylewski.



Śp. płk rez. dr hab. inż. Zdzisław Polcikiewicz, prof. UMK

6 II 1959–7 VIII 2026

Na zakończenie chciałabym podzielić się smutną informacją. Prace nad tym wydaniem PBW przerwała wiadomość o odejściu naszego recenzenta – płk. rez. dr. hab. inż. Zdzisława Polcikiewicza, prof. UMK, oficera Wojska Polskiego, wspaniałego dowódcy, naukowca i wychowawcy licznych pokoleń żołnierzy i studentów. Rodzina, przyjaciele i wychowankowie wspominają Go jako człowieka wielu talentów, o rzadko spotykanej życzliwości i radości życia. W 2026 r. ukazała się monografia *W służbie wojsku i nauce. Księga Jubileuszowa dedykowana prof. Zdzisławowi Polcikiewiczowi*, która jest wyrazem uznania dla dorobku naukowego oraz wieloletniej służby wojskowej i pracy akademickiej Pana Profesora.

Nasze czasopismo miało przywilej korzystania ze wsparcia prof. Zdzisława Polcikiewicza przy powstawaniu kolejnych wydań. Pomimo ciężkiej choroby podjął się On również recenzji artykułu do tego numeru. Wiadomość o śmierci Pana Profesora przyjęliśmy z ogromnym żalem. W imieniu całego zespołu wydawnictwa ABW składam Jego bliskim wyrazy głębokiego współczucia.

Redaktor naczelny
dr Daria Olender

ARTYKUŁY

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 15–37
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.021.24170

ARTYKUŁ

Informacja jako narzędzie wojny kognitywnej w kontekście wojny hybrydowej

Information as a tool of cognitive warfare in the context of hybrid warfare

TOMASZ GERGELEWICZ

Wyższa Szkoła Bezpieczeństwa i Ochrony w Warszawie
https://orcid.org/0000-0002-9145-5099

Abstrakt Informacja stała się potężną bronią, którą można porównać do tradycyjnych środków walki. Rozwój technologii i podatność społeczeństw na szkodliwe narracje sprzyjają wrogim działaniom informacyjnym, które w domenie poznawczej mogą doprowadzić do wojny kognitywnej. Celem artykułu jest uporządkowanie oraz charakterystyka pojęć związanych z tą wojną. Główny problem badawczy można sprowadzić do pytania: jaką rolę odgrywa informacja we wrogich działaniach prowadzonych w domenie kognitywnej? Proces badawczy oparto m.in. na analizie literatury polsko- i anglojęzycznej, źródeł branżowych czy mediów społecznościowych.

Słowa kluczowe wojna kognitywna, wojna informacyjna, wojna hybrydowa, dezinformacja, wojna psychologiczna

Abstract Information has become a powerful weapon, comparable to traditional means of warfare. The development of technology along with societies' susceptibility to harmful narratives facilitates hostile information activities, which in the cognitive domain may lead

to cognitive warfare. The aim of this article is to systematise and characterise the concepts related to this warfare. The main research problem can be summarise as follows: what role does information play in hostile activities carried out in the cognitive domain? The research process is based on an analysis of Polish and English literature, professional sources, and social media.

Keywords cognitive warfare, information warfare, hybrid warfare, disinformation, psychological warfare

Wprowadzenie

Informacja stała się bronią w rękach agresorów i może być równie niebezpieczna jak tradycyjne środki walki. Rozwój nowoczesnych technologii oraz społeczeństwo bezkrytycznie przyjmujące informacje powodują, że wojna kognitywna[1] może być postrzegana jako skuteczny mechanizm wrogiego wpływu.

Zrozumienie szkodliwych działań w domenie kognitywnej wymaga przede wszystkim poznania roli informacji, dlatego autor podjął się usystematyzowania pojęć związanych z wojną kognitywną. Charakteryzuje zagadnienia dotyczące m.in. zagrożeń hybrydowych, środowiska informacyjnego, operacji informacyjnych, działań psychologicznych oraz dezinformacji. Zauważa, że pojęcia takie jak: dezinformacja, operacje informacyjne, fake news czy manipulacja zbyt często są używane w przestrzeni publicznej jako synonimy. Ponadto nadużywa się pojęcia wojny hybrydowej.

Celem artykułu jest odpowiedź na pytanie: w jaki sposób informacja jest wykorzystywana we wrogich działaniach w domenie kognitywnej? W artykule oparto się na metodzie analitycznej, która posłużyła do wyodrębnienia poszczególnych obszarów ważnych w dyskursie o roli informacji w wojnie, oraz metodzie syntezy, zastosowanej do wskazania punktów stycznych poszczególnych obszarów i relacji przyczynowo-skutkowej pomiędzy informacją a wojną kognitywną.

Temat wykorzystania informacji w celu prowadzenia wrogich działań jest obecny w krajowym i zagranicznym dyskursie publicznym i naukowym. Materiał źródłowy stanowi zatem zarówno polsko-, jak i anglojęzyczna literatura przedmiotu. Jako źródła wykorzystano także branżowe portale internetowe i media społecznościowe, ponieważ wiedza ekspercka w przedmiotowym obszarze nie zawsze jest dostępna w publikacjach naukowych.

[1] Więcej w podrozdziale: *Wojna kognitywna*.

Środowisko informacyjne

Do prowadzenia pogłębionej dyskusji nad wojną kognitywną jest konieczne zrozumienie problematyki informacji i środowiska informacyjnego. Wiesław Flakiewicz wskazuje, że informacja to (…) *czynnik, który zwiększa naszą wiedzę o otaczającej nas rzeczywistości*[2]. Informacja stała się także narzędziem walki, a polem walki – środowisko informacyjne, będące przestrzenią funkcjonowania społeczeństwa. Zatem informacja w kontekście przedmiotowej dyskusji jest ujęta jako zasób konkretnych danych, który może być wykorzystany jako narzędzie walki w środowisku informacyjnym.

Na środowisko informacyjne składa się kilka elementów. Adam Łapszyński wskazuje, że są to: (…) *informacja sama w sobie, odbiorcy (osoby i organizacje), którzy ją odbierają, przetwarzają i przekazują, oraz przestrzeń, w której się pojawia*[3]. Nawiązuje on do komunikacji, w której można wyróżnić m.in. nadawcę, odbiorcę, informację i przestrzeń. Marc J. Romanych uważa, że środowisko informacyjne to (…) *zbiór (ang. aggregate) osób, organizacji lub systemów, który gromadzi, przetwarza lub rozpowszechnia informacje; obejmuje także samą informację*[4]. W tym przypadku można zaobserwować analogię do cyklu informacyjnego czy też wywiadowczego, w którym informacja jest pozyskiwana, gromadzona, przetwarzana i rozpowszechniana[5]. Biuro Bezpieczeństwa Narodowego (BBN) podkreśla wysoką rangę środowiska informacyjnego jako kluczowego komponentu w planowaniu bezpieczeństwa państwa. Wskazuje takie obszary środowiska informacyjnego, jak m.in.: cyberprzestrzeń, komunikacja strategiczna i bezpieczeństwo poznawcze[6].

W nawiązaniu do środowiska informacyjnego warto wyjaśnić, czym jest przestrzeń informacyjna. Definiuje się ją m.in. jako nieciągłe i niejednorodne skupisko źródeł informacji – (…) *obiektów (rzeczywistych lub wirtualnych), z których dana*

---

[2] J. Frąś, *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" 2011, nr 21, s. 32.

[3] A. Łapszyński, *Monitoring the Information Environment In the Baltic Sea Region*, „The Baltic Amber. Multinational Corps Northeast Magazine" 2020, s. 28. Tłumaczenia w tekście pochodzą od autora (dop. red.).

[4] M.J. Romanych, *Visualizing the Information Environment*, „Military Intelligence Professional Bulletin" 2003, t. 29, nr 3, s. 5.

[5] Zob. szerzej: L. Dalinczuk, *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego*, w: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (red. nauk.), Biała Podlaska 2021, s. 176–183.

[6] *Biuro Bezpieczeństwa Narodowego 2015–202*5, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209,Biuro-Bezpieczenstwa-Narodowego-2015-2025.html, s. 52 [dostęp: 28 IX 2026].

osoba może skorzystać jako ze źródeł informacji[7]. Małgorzata Kisilowska twierdzi, że przestrzeń informacyjna to wielowymiarowy, dynamiczny, otwarty zbiór treści (danych i informacji), ich nośników oraz użytkowników[8].

W dyskursie o środowisku i przestrzeni informacyjnej należy uwzględnić także infosferę. Według Michaela Vlahosa to (…) *połączenie (fuzja) wszystkich światowych sieci komunikacyjnych, baz danych i zasobów informacji w rozległą, różnorodną sieć wymiany elektronicznej*[9]. Problematykę tę poruszył również Luciano Floridi. Według niego infosfera (…) *opisuje całe środowisko informacyjne, na które składają się wszystkie podmioty informacyjne (ang. informational entities), oraz czynniki informacyjne (komunikaty, dane, informacje), ich własności, interakcje, procesy i wzajemne relacje. Środowisko to jest porównywalne z cyberprzestrzenią (która jest tylko jednym z jego regionów)*[10]. Nawiązując do cyberprzestrzeni, Mirosław Karpiuk wskazuje, że (…) *szybkość, dostępność i ograniczona odpowiedzialność związane z obiegiem informacji w cyberprzestrzeni powodują, że jest to obszar infosfery idealnie nadający się do przekazywania treści fałszywych*[11].

Scharakteryzowanie tych pojęć ma na celu ułatwienie zrozumienia pola walki informacyjnej. Autor zaznacza, że na potrzeby rozwiązania problemu badawczego przestrzeń informacyjną oraz infosferę należy sprowadzić do wspólnego mianownika i wskazać je jako elementy środowiska informacyjnego.

Środowisko informacyjne, w którym przenikają się informacje, niesie ze sobą różnorodne zagrożenia. Wrogie wykorzystanie informacji w ramach prowadzenia operacji informacyjnych (ang. *information operations – infoops*) może prowadzić do wojny informacyjnej. Jej celem jest (…) *zakłócenie procesów decyzyjnych, wprowadzenie przeciwników w błąd, kształtowanie pożądanych opinii i percepcji społecznych, organizowanie działań antyrządowych oraz osłabienie woli przeciwnika, przy czym aspekty wpływu i techniczne są często traktowane jako nierozerwalna całość*[12]. Andrew Borden wskazuje, że

---

[7] C. McKnight, *The Personal Construction of Information Space*, „Journal of the American Society for Information Science" 2000, t. 51, nr 8, s. 730. https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8.

[8] M. Kisilowska, *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2011, nr 2, s. 49. https://doi.org/10.36702/zin.666.

[9] M. Vlahos, *Entering the Infosphere*, „Journal of International Affairs" 1998, t. 51, nr 2, s. 498.

[10] L. Floridi, *A Look into the Future Impact of ICT on our Lives*, „The Information Society" 2007, t. 23, nr 1, s. 59. https://doi.org/10.1080/01972240601059094.

[11] W.M. Karpiuk, *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, „Cybersecurity and Law" 2024, nr 2, s. 235.

[12] M. Calkayis, *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025 r., https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/ [dostęp: 6 XI 2025].

(…) *to wszelkie działania mające na celu odmowę, wykorzystanie, korupcję lub zniszczenie informacji wroga i jej funkcji; chroniąc jednocześnie przed tymi działaniami i wykorzystując własne wojskowe funkcje informacyjne*[13]. Jak ujęto w Koncepcji Obronnej Rzeczypospolitej Polskiej (…) *choć w przyszłości wojny będą wciąż prowadzone przede wszystkim za pomocą środków kinetycznych, znaczenie będą zyskiwać również inne metody walki. Cyberprzestrzeń oraz pole walki informacyjnej już teraz stają się frontem nowego rodzaju*[14].

Podsumowując, środowisko informacyjne – w kontekście prowadzonych rozważań – należy ująć jako przestrzeń, w której przenikają się informacje mogące zostać wykorzystane do wrogiego oddziaływania informacyjnego.

Dezinformacja

W ramach działań hybrydowych – przez operacje informacyjne i oddziaływanie psychologiczne – są stosowane narzędzia, które mają umożliwić wywieranie negatywnego wpływu na grupę docelową. Jednymi z najskuteczniejszych środków w tym zakresie są: wykorzystanie nieprawdziwych informacji, tzw. fake newsów, manipulacja faktami i tworzenie szumu informacyjnego, które składają się na proces dezinformacji (ang. *disinformation*)[15]. Autor celowo ujmuje ją jako proces, gdyż obejmuje elementy wpływu informacyjno-psychologicznego, które agresor wykorzystuje w sposób zaplanowany w czasie i przestrzeni, aby osiągnąć konkretne cele.

Instrukcja Oddziału II Sztabu Głównego Wojska Polskiego z maja 1926 r. wyjaśnia, że dezinformacja polega na (…) *podaniu wywiadowi przeciwnika wiadomości ukrywających własne zamierzenia* (…) *oraz na zmuszaniu go do traktowania informacji podanej przez wywiad własny jako prawdziwej, względnie zmuszaniu wywiadu obcego do analizy inspirowanych wiadomości*[16]. Eksperci z Instytutu Kościuszki uważają, że (…) *dezinformacja (ang. disinformation) to celowe tworzenie oraz rozprzestrzenianie nieprawdziwych informacji w celu manipulacji. Kluczowym elementem dezinformacji jest celowość i świadomość*[17]. Według Richarda Deacona

[13] A. Borden, *What Is Information Warfare?*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf, s. 1 [dostęp: 20 V 2024].

[14] *Koncepcja Obronna Rzeczypospolitej Polskiej*, Ministerstwo Obrony Narodowej, Warszawa 2017, s. 36–37.

[15] Termin pojawił się wiosną 1926 r. w londyńskim miesięczniku „The Whitehall Gazette & St. James's Review".

[16] A. Pepłoński, *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944*, Kraków 2011, s. 335.

[17] *Z tarczą! Jak chronić się przed dezinformacją?*, K. Mikulski, M. Krawczyk (red.), Kraków 2021, s. 9.

dezinformacja to sfabrykowane świadectwa, taktyka oczerniania oraz sfałszowane dokumenty wykorzystane do zdyskredytowania przeciwnika[18]. Dezinformacja została opisana także jako wprowadzanie w błąd dla taktycznych i strategicznych korzyści: wizerunkowych, politycznych, finansowych i militarnych[19]. Według Roberta Nogackiego i Krzysztofa Surdyka pod pojęciem dezinformacji można rozumieć także metodę maskowania polegającą na celowym rozpowszechnianiu fałszywych informacji o maskowanym obiekcie, jego strukturze i działaniach. Wskazują oni, że dezinformacja obejmuje prowadzenie specjalnych operacji, działań mających na celu ukrycie tajemnic, wprowadzanie w błąd w kwestiach związanych z problemami politycznymi, gospodarczymi, naukowymi, technicznymi, wojskowymi i skłonienie przeciwnika do podjęcia decyzji i działań, które byłyby korzystne dla strony wprowadzającej w błąd[20].

Wielka Encyklopedia Radziecka definiuje dezinformację jako (…) *rozpowszechnianie za pośrednictwem prasy i radia wiadomości fałszywych w celu wprowadzenia w błąd opinii publicznej*[21]. Według *Espionage: An Encyclopedia of Spies and Secrets* dezinformacja to (…) *tworzenie i rozpowszechnianie wprowadzających w błąd lub fałszywych informacji w celu wyrządzenia szkody wizerunkowi kraju wybranego za cel*[22]. Parlament Europejski określa dezinformację jako:

> (…) celowo zmanipulowane treści rozpowszechniane, aby wprowadzić odbiorców w błąd i osiągnąć określone cele – strategiczne, polityczne lub ekonomiczne. Często rozpowszechniają ją podmioty, których celem jest podważanie zaufania do instytucji demokratycznych lub wpływanie na wyniki wyborów. Dezinformacja zagraża demokracji, ponieważ zniekształca debatę publiczną, prowadzi do polaryzacji społeczeństwa i utrudnia obywatelom podejmowanie świadomych decyzji wolnych od manipulacji i ingerencji[23].

[18] *Disinformation*, w: R. Deacon, *Spyclopaedia*, London 1989, s. 400.

[19] I.M. Pacepa, R.J. Rychlak, *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Gliwice 2015, s. 9–11, 50–56.

[20] R. Nogacki, K. Surdyk, *Teoria i praktyka działań dezinformacyjnych*, Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020 r., https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html [dostęp: 19 VIII 2025].

[21] A. Golitsyn, *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984, s. 4–5.

[22] *Disinformation*, w: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002, s. 69.

[23] *Dezinformacja: 10 kroków, by chronić siebie i innych*, Parlament Europejski, 11 VI 2025 r., https://www.europarl.europa.eu/topics/pl/article/20250603STO28720/dezinformacja-10-krokow-by-chronic-siebie-i-innych [dostęp: 21 X 2025].

Inna definicja wskazuje, że dezinformacja to (…) *celowe rozpowszechnianie fałszywych lub wprowadzających w błąd informacji w celu osiągnięcia określonych celów, takich jak manipulacja opinią publiczną, osłabianie zaufania do instytucji czy wprowadzanie zamieszania. Dezinformacja może przybierać różne formy, takie jak fałszywe wiadomości, teorie spiskowe, przekłamania czy wyolbrzymianie faktów*[24]. Katarzyna Bąkowicz stwierdza, że (…) *dezinformacja jest świadomie rozpowszechniana w określonych przez nadawcę celach, często wykorzystując kanały przyspieszające jej rozpowszechnianie i poszerzające jej zasięg do szerokiego grona odbiorców. Jest to strategiczne i skalkulowane działanie, mające na celu osiągnięcie konkretnych efektów, angażujące wszystkie elementy procesu informacyjnego*[25]. Jak wskazano w „Przeglądzie Nauk o Obronności", dezinformacja stanowi bezpośrednie zagrożenie bezpieczeństwa państwa i może oddziaływać na politykę w obszarze obrony, w tym na jej cele strategiczne związane z zapewnieniem niepodległości. Ponadto może ingerować w mechanizmy demokratyczne i prowadzić do podważenia stabilności państwa oraz do nieprawidłowości w funkcjonowaniu organów władzy publicznej[26].

Teoretyk sztuki wojennej Sun Tzu w traktacie *Sztuka wojny* napisał, że podczas wojny zwycięstwo bez walki jest najważniejszą umiejętnością: (…) *wszelkie działania wojenne opierają się na podstępie. Dlatego, gdy jesteśmy zdolni atakować, musimy sprawiać wrażenie niezdolnych; gdy używamy wojsk, powinniśmy wyglądać na bezczynnych; gdy jesteśmy blisko, musimy sprawić, by wróg uważał, że jesteśmy daleko* (…)[27]. Były oficer francuskiego wywiadu Vladimir Volkoff przedstawił dezinformację jako działanie, które ma na celu usankcjonowanie wrogich idei wśród członków atakowanych społeczeństw. Wówczas jest ona prowadzona systematycznie, z wykorzystaniem mass mediów i kierowana do opinii publicznej. Ponadto wskazywał, że dezinformacja jest ukierunkowana na zmianę biegu wydarzeń i wiąże się z destabilizacją społeczeństwa przeciwnika[28]. Według NASK (…) *ostateczne cele dezinformacji to wzbudzenie strachu, utrata zaufania do instytucji i polaryzacja społeczna* (…). *Dezinformacja podważa zaufanie do instytucji publicznych, nauki czy mediów.*

---

[24] *Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie*, Serwis Rzeczypospolitej Polskiej, 10 VIII 2023 r., https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie [dostęp: 27 X 2025].

[25] K. Bąkowicz, *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje*, „Zeszyty Naukowe Akademii Górnośląskiej" 2023, nr 10, s. 127–137. https://doi.org/10.53259/2023.10.13.

[26] K. Kaczmarek, M. Karpiuk, C. Melchior, *Disinformation as a Threat to State Security*, „Przegląd Nauk o Obronności" 2024, nr 20, s. 47. https://doi.org/10.37055/pno/205780.

[27] S. Tzu, *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf, s. 8 [dostęp: 27 IX 2025].

[28] V. Volkoff, *Psychosocjotechnika. Dezinformacja. Oręż wojny*, Warszawa 1991, s. 7–8.

Sprzyja destabilizacji państwa i podsycaniu podziałów społecznych[29]. Policja także podaje, że dezinformacja to (…) *fałszywe lub wprowadzające w błąd treści, które mogą przybierać formę postów, artykułów, filmów czy nagrań audio. Jej celem jest umyślne wyrządzenie szkody publicznej lub osiągnięcie zysku*[30].

Sojusz Północnoatlantycki poświęca wiele uwagi dezinformacji i strategiom jej zwalczania. W *NATO 2022 Strategic Concept* wymieniono najważniejsze grupy zagrożeń, zwłaszcza ze strony Rosji, którym musi sprostać NATO. W dokumencie podkreślono potrzebę inwestowania w zdolności odstraszania i obrony przed przymusem politycznym, ekonomicznym, energetycznym, informacyjnym oraz pozostałymi taktykami hybrydowymi[31]. Dowództwo NATO ds. Transformacji (Allied Command Transformation, ACT) stwierdza, że (…) *różni zewnętrzni aktorzy próbują podważyć jedność Sojuszu i wpłynąć na nasze społeczeństwa* (…). *Kampanie informacyjne, nieprawdziwe wiadomości czy teorie spiskowe są wykorzystywane do rozbijania państw i polaryzowania opinii publicznej*[32]. W sprawozdaniu specjalnym Europejskiego Trybunału Obrachunkowego wskazano, że (…) *dezinformacja stanowi poważny problem w zorganizowanych społeczeństwach. Za sprawą mediów społecznościowych i nowych technologii zmieniła się skala tego zjawiska oraz szybkość, z jaką nieprawdziwe lub wprowadzające w błąd informacje mogą dotrzeć do zamierzonych i niezamierzonych odbiorców*[33]. W komunikacie Komisji Europejskiej na temat skali i zasięgu dezinformacji podano kilka przyczyn jej rozprzestrzeniania się, np. szybkie zmiany kulturowe, społeczne i ekonomiczne, które powodują m.in. wzrost napięć społecznych, a także transformację mediów i dużą popularność platform internetowych[34]. Jak twierdzi Bąkowicz, łatwość rozpowszechniania dezinformacji warunkują również czynniki wpływające na nieodpowiedzialne podejście społeczeństw do informacji, takie jak:

---

[29] *Chroń się przed dezinformacją*, NASK, https://www.nask.pl/instytut/dla-ciebie/dezinfo [dostęp: 19 IX 2025].

[30] *Czy wiesz jak chronić się przed dezinformacją?*, Komenda Powiatowa Policji w Oławie, 24 XI 2024 r., https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html [dostęp: 15 IX 2025].

[31] *NATO 2022 Strategic Concept*, NATO, 29 VII 2022 r., https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept [dostęp: 9 XII 2024].

[32] *Protecting the Alliance Against the Threat of Cognitive Warfare*, YouTube, 9 V 2023 r., https://www.youtube.com/watch?v=4Pn57uoyYEA [dostęp: 5 XI 2025].

[33] *Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany. Sprawozdanie specjalne*, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_PL.pdf [dostęp: 15 X 2025].

[34] J. Balcewicz, *Zwalczanie dezinformacji w internecie: podejście europejskie*, Cyberpolicy NASK, 26 IV 2018 r., https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie [dostęp: 17 X 2025].

selektywność ludzkiej percepcji, brak zainteresowania rzetelną informacją, bezgraniczna wiara człowieka w autorytet innych osób obniżająca krytycyzm[35].

Warto zwrócić uwagę na różnicę pomiędzy dezinformacją a misinformacją. Ta druga określana jest jako treść nieprawdziwa, tworzona bez wrogich intencji[36], wprowadzająca w błąd w wyniku np. braku wiedzy czy mylenia faktów. Podmiot udostępniający misinformację może wierzyć, że przekazuje informację prawdziwą[37].

Przykładem państwa dezinformującego na szeroką skalę jest Federacja Rosyjska. W Koncepcji Obronnej Rzeczypospolitej Polskiej stwierdzono, że: (…) *rosyjska polityka jest wysoce skoordynowana z operacjami służb specjalnych, w tym środkami aktywnymi (np. działaniami dezinformacyjnymi) stosowanymi wobec innych państw*[38]. Kreml prowadzi kampanie dezinformacyjne, które mają na celu nie tylko maskowanie bieżących aktywności Rosji względem własnych obywateli, lecz przede wszystkim zbudowanie zmanipulowanego trwałego obrazu NATO jako sojuszu ofensywnego[39]. W rosyjskiej koncepcji wojny nowej generacji typowy konflikt zbrojny musi być poprzedzony rywalizacją polityczną, informacyjną i psychologiczną, podczas której istnieje dogodna przestrzeń do wywierania wpływu na przeciwnika, osłabienia jego morale, a tym samym zmniejszenia jego woli walki, a także kreowania go jako winnego eskalacji[40]. Walerij Gierasimow stwierdził, że (…) *rola niemilitarnych środków w osiąganiu celów politycznych i strategicznych naszego państwa znacząco wzrosła w ostatnich latach i w wielu aspektach są one ważniejsze niż siła zbrojna i samo uzbrojenie*[41]. Wrogie działania w przestrzeni informacyjnej FR dotyczą m.in.: podważania wiarygodności państw na arenie międzynarodowej i przedstawiania ich jako rusofobicznych oraz osłabiania ich pozycji na forum UE i NATO w kwestii polityki wobec Kremla[42].

---

35 K. Bąkowicz, *Praktyczne rozumienie dezinformacji*…

36 L. Tomala, *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie*, Nauka w Polsce, 7 II 2021 r., https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak [dostęp: 15 X 2025].

37 Szkolenie „Understanding Disinformation" prowadzone przez Kancelarię Premiera Wielkiej Brytanii (materiały w posiadaniu autora).

38 *Koncepcja Obronna Rzeczypospolitej Polskiej*…, s. 23.

39 *Dlaczego obca propaganda jest skuteczna w obszarze obronności*?, Stop Fake Org, 5 VIII 2019 r., https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/ [dostęp: 29 X 2025].

40 M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 21–23.

41 T. Otłowski, *Rosyjskie myślenie o wojnie*, „Polska Zbrojna" 2021, nr 5, s. 82.

42 Z. Zielonka, K. Rumiński, *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017, s. 47.

Zdaniem Michała Oleksiejuka Rosja kreuje swój wizerunek jako państwa zagrożonego i destabilizowanego przez siły zewnętrzne. W wyniku tego rosyjskie społeczeństwo ma być przekonane, że Rosja jest oblężoną twierdzą[43]. Olga Wasiuta i Sergiusz Wasiuta odnotowują, że Rosja nie szanuje niezależności sąsiadów, a w działaniach wykorzystuje działania informacyjne, zastraszanie gospodarcze czy napięcia religijne[44]. Autorzy piszą: (…) *w ostatnich latach Rosja zwiększyła zdolności wszystkich rodzajów swoich sił zbrojnych, rozbudowuje systemy walki radioelektronicznej, zdolności wywiadowcze, cybernetyczne oraz programy kosmiczne, militaryzuje obwód kaliningradzki, wywiera wpływ na debatę polityczną w krajach NATO i UE, podsyca polaryzację społeczeństw* (…)[45]. Jean-Christophe Boucher i Ofer Fridman w badaniach prowadzonych nad rosyjskimi działaniami na platformach społecznościowych Telegram oraz X wskazują na wielkoskalowe obce ingerencje i manipulacje informacją (ang. *foreign information manipulation and interference*, FIMI)[46] prowadzone przez Kreml, które były dopasowane do konkretnych grup docelowych w wybranych państwach[47]. Katarzyna Kwiatkowska-Moskalewicz we wnioskach z analizy treści na platformie Sputnik stwierdza, że (…) *obrana przez Rosję „strategia pasożytnicza" polega na kopiowaniu i przejmowaniu zachodnich wzorców przez nadawanie im przeciwstawnego wektora znaczeń* (…). *Rosyjska polityka informacyjna jest jednym z frontów prowadzonej przez Federację Rosyjską wojny hybrydowej prowadzonej przeciwko Polsce i Zachodowi*[48]. Uwzględniając powyższe, należy podkreślić, że FR w XXI w. stała się studium przypadku państwa, które prowadzi wrogą imperialistyczną politykę opartą w znacznej mierze na działaniach hybrydowych na bezprecedensową skalę.

Autor zauważa, że dezinformację tworzą trzy zasadnicze narzędzia wpływu informacyjnego: nieprawdziwe informacje, tzw. fake newsy, manipulacja faktami i szum informacyjny. Pierwsze z nich obejmuje informacje, które zostały wytworzone,

[43] M. Oleksiejuk, *Rosyjski syndrom oblężonej twierdzy*, Warsaw Institute, 31 VIII 2020 r., https://warsawinstitute.org/pl/rosyjski-syndrom-oblezonej-twierdzy/ [dostęp: 29 VIII 2025].

[44] *Encyklopedia Bezpieczeństwa*, t. 5, O. Wasiuta, S. Wasiuta (red.), https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf [dostęp: 2 XII 2025].

[45] Tamże.

[46] To pojęcie zaproponowane przez Europejską Służbę Działań Zewnętrznych (European External Action Service) w celu prowadzenia dyskursu nad zewnętrznym wrogim wpływem informacyjnym. Zob. szerzej: *Creation of the European External Action Service*, European Union External Action, 19 VIII 2021 r., https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [dostęp: 20 XII 2025].

[47] *Counter-FIMI Toolbox for Diplomats. A Conceptual Framework*, https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf, s. 6 [dostęp: 2 IX 2026].

[48] K. Moskalewicz-Kwiatkowska, *Pasożytnicza strategia rosyjskiej propagandy*, Warszawa 2024, s. 7–8.

aby wprowadzić w błąd i są celowo lub przypadkowo rozpowszechniane[49]. Fake news w odpowiednim kontekście może mieć pozorne cechy prawdziwej informacji. Drugim narzędziem jest manipulacja faktami, czyli (…) *wykorzystywanie jakichś okoliczności, naginanie lub przeinaczanie faktów w celu udowodnienia swoich racji lub wpływania na cudze poglądy i zachowania*[50]. Manipulacja użyta w celu dezinformacji jest szczególnie niebezpieczna, ponieważ trudno ją zweryfikować. Szum informacyjny (ang. *information noise*) z kolei polega na generowaniu wielu sprzecznych lub podobnych do siebie informacji. Ułatwia to uwiarygodnienie fake newsów, sprzyja manipulacji faktami i rozprasza uwagę użytkownika infosfery. Odbiorca traci zdolność określenia, na czym powinien się skupić i jak szacować wartość poszczególnych informacji. Paulina Piasecka zwraca uwagę, że szum informacyjny polega na zalewaniu przestrzeni informacyjnej wszechobecnymi i nieautoryzowanymi informacjami. Podczas działań ofensywnych taki szum może skutecznie maskować cele i działania agresora[51].

Ważną rolę w kreowaniu narracji i generowaniu szumu informacyjnego odgrywają media. Jak stwierdza Chiara de Franco: (…) *narracje tworzone przez media, zwłaszcza wokół jednej lub więcej sytuacji, faktycznie tworzą efekt rzeczywistości, która oddziałuje nie tylko na ogół społeczeństwa, lecz także na decydentów. Te narracje stanowią pośrednią rzeczywistość, która ingeruje w proces decyzyjny, ponieważ wpływa na postrzeganie poszczególnych sytuacji, które z kolei mają wpływ na podejmowanie decyzji*[52]. Dlatego media powinny stanowić przestrzeń dla wiarygodnej i rzetelnej informacji, a także odgrywać rolę bezstronnego i niezależnego źródła odpowiadającego wysokim standardom etycznym[53].

Podsumowując, dezinformację należy traktować jako wrogi i celowy proces wykorzystania fake newsów, zmanipulowanych faktów i szumu informacyjnego, aby wymusić błędną ocenę rzeczywistości i doprowadzić do podjęcia decyzji zgodnych z wolą agresora**.**

---

[49] *Rozpoznawanie nieprawdziwych informacji*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji [dostęp: 20 III 2023].

[50] Hasło: manipulacja, *Słownik języka polskiego*, https://sjp.pwn.pl/sjp/manipulacja;2481186 [dostęp: 10 IX 2025].

[51] N. Gorzelnik, *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media*, INN Poland, 28 III 2022 r., https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad [dostęp: 28 VIII 2024].

[52] C. de Franco, *Media Power and the Transformation of War*, New York 2012, s. 47.

[53] *Recommendation of the Committee of Ministers to member states on the remit of public service media in the information society* (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec(2007)3, https://search.coe.int/cm?i=09000016805d6bc5 [dostęp: 14 IX 2025].

Wojna psychologiczna

Charakteryzując wojnę kognitywną, należy omówić pojęcie operacji psychologicznych (ang. *psychological operations – psyops*), ponieważ stanowią one istotę narzędzi wpływu w domenie poznawczej. NATO definiuje operacje psychologiczne jako: (…) *planowane działania psychologiczne, wykorzystujące metody komunikacji oraz inne środki, skierowane do zatwierdzonych grup odbiorców, mające na celu wpływanie na postrzeganie, postawy i zachowania, co wpływa na osiąganie celów politycznych i wojskowych*[54]. Operacje psychologiczne mogą być ujęte w ramy wojny psychologicznej, co wskazuje m.in. na bardziej zróżnicowane cele, w tym polityczne i strategiczne, szerszy zakres działania, dłuższy czas trwania czy większy wachlarz środków przeznaczonych do jej prowadzenia.

Zgodnie z definicją *Słownika języka polskiego* wojna psychologiczna to (…) *planowe wywieranie presji na jakieś państwo za pomocą propagandy ideologicznej, gróźb i zastraszania*[55]. *Wielki słownik języka polskiego* definiuje wojnę psychologiczną jako (…) *wywieranie presji na jakieś państwo, organizację lub grupę za pomocą gróźb, zastraszania czy nieprzychylnej propagandy*[56]. Kolejna definicja wskazuje na zespół działań (…) *bazujących na wszechstronnej wiedzy z zakresu spektrum zachowań człowieka i charakteryzuje się wykorzystaniem narzędzi i działań wpływających na zachowania społeczne, tak aby stworzyć możliwości sterowania społecznego rozumianego jako umiejętność skłonienia danej populacji do realizacji określonych celów*[57]. W *Vademecum Bezpieczeństwa Informacyjnego* wojnę psychologiczną zdefiniowano jako (…) *planowe stosowanie propagandy oraz pokrewnych środków informacji publicznej w celu wywarcia wpływu na opinię publiczną, uczucia, postawę i zachowanie się nieprzyjaciela oraz grup cudzoziemskich, tak, aby pomóc w realizowaniu polityki państwa i jego celów oraz zadań wojskowych*[58]. Jak pisze Marcin Olechowski, przy prowadzeniu wojny psychologicznej wyróżnia się trzy zasadnicze poziomy: strategiczny, realizowany w ramach sojuszy przez rządy i najwyższe dowództwa wojskowe; taktyczny, który towarzyszy akcjom zbrojnym na poziomie pola walki; oraz działania konsolidujące,

[54] NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

[55] Hasło: wojna psychologiczna, *Słownik języka polskiego*, https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html [dostęp: 20 XI 2025].

[56] Hasło: wojna psychologiczna, *Wielki słownik języka polskiego*, https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna [dostęp: 20 XI 2025].

[57] Hasło: wojna psychologiczna, *Encyklopedia Bezpieczeństwa Narodowego*, https://encyklopedia.revite.pl/articles/view/643 [dostęp: 20 XI 2025].

[58] Hasło: wojna psychologiczna, *Vademecum Bezpieczeństwa Informacyjnego*, https://vademecum-bezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/ [dostęp: 26 XI 2025].

prowadzone wobec ludności cywilnej na obszarze będącym pod kontrolą własną lub sojuszniczą[59]. Wskazuje to na szeroki zakres działań psychologicznych, co bezpośrednio wiąże się z zaawansowaniem wojny kognitywnej.

Podsumowując, wojna psychologiczna jest zasadniczym elementem wojny kognitywnej. Są to wrogie działania wykorzystujące oddziaływanie psychologiczne, aby wpływać na grupę docelową. Wojna kognitywna natomiast obejmuje szerszy kontekst wrogich działań prowadzących do zmiany sposobu postrzegania rzeczywistości przez tę grupę.

Wojna kognitywna

Wojna kognitywna według Komponentu Wojsk Obrony Cyberprzestrzeni to (…) *wojna na umysły, gdzie kluczowym polem bitwy staje się informacja. W przeciwieństwie do tradycyjnych działań wojennych, które koncentrują się na fizycznym pokonaniu przeciwnika, wojna kognitywna dąży do zdobycia kontroli nad umysłami ludzi* (…)[60]. Podczas TEDx Talks wojnę kognitywną ujęto następująco: (…) *to działania kształtujące postawy i zachowania poprzez wpływanie lub zakłócanie poznania (emocjonalnie nasyconego obrazu świata) danej populacji w celu uzyskania przewagi nad przeciwnikiem i osłabienia jego odporności*[61]. W ramach prowadzenia wojny kognitywnej wykorzystuje się szeroką gamę narzędzi często zintegrowanych z działaniami gospodarczymi, dyplomatycznymi i wojskowymi[62]. Niina Meriläinen stwierdza, że wojna kognitywna (…) *umocniła swoją pozycję na poziomach strategicznym, operacyjnym i taktycznym. Poprzez oddziaływanie na postawy, przekonania i sposoby rozumowania, a także na tworzone przez nie relacje przyczynowo-skutkowe, wojna kognitywna jednocześnie je kształtuje i wpływa na zachowania ludzi, skłaniając ich do realizacji celów przeciwnika*[63]. Agnieszka Szczygielska wskazuje z kolei na podobieństwo

---

[59] M. Olechowski, *Wojna psychologiczna – próba zdefiniowania pojęcia*, „Wiedza Obronna" 2018, wydanie podwójne t. 262–263, nr 1–2, s. 98. https://doi.org/10.34752/ahf8-sd31.

[60] *Dezinformacja*, https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dezinformacja/ [dostęp: 28 IX 2025].

[61] A. Karalus, *Czym jest wojna kognitywna?*, YouTube, 28 I 2025 r., https://www.youtube.com/watch?v=YXIOrA_rNGY [dostęp: 5 XI 2025].

[62] N. Bugayova, K. Stepanenko, *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf, s. 1 [dostęp: 28 IX 2026].

[63] N. Meriläinen, *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, „Proceedings of the 6th International Conference on AI Research, Italy 2025, s. 306. https://doi.org/10.34190/icair.5.1.4353.

wojny kognitywnej do wojen: informacyjnej, cybernetycznej i psychologicznej. Twierdzi, że (…) *we wszystkich tych wojnach można dostrzec różne formy wpływania na ludzi, na ich procesy myślowe, mentalność, poczucie bezpieczeństwa, na ludzkie poznanie. Wojna kognitywna jednak jest w pełni skierowana na ludzki umysł, na jego możliwości i zakłócenie procesów poznawczych*[64]. Także w „Journal of Modern Science" wskazano cechy łączące wiele metod oddziaływania i podkreślono, że wojna kognitywna to (…) *połączenie wojny informacyjnej, wywiadu, inwigilacji i rozpoznania oraz wojny elektronicznej i operacji psychologicznych, jak również operacji cybernetycznych wykorzystujących infrastrukturę cyfrową i sieciową*[65]. O skali prowadzenia wojny kognitywnej pisano również w „Joint Force Quarterly": (…) *w najszerszym ujęciu wojna kognitywna nie ogranicza się do sfery wojskowej ani instytucjonalnej* (…). *Jej celem jest cały kapitał ludzki danego państwa*[66]. Na atypowy zakres zagrożeń wynikających z wojny kognitywnej zwrócono uwagę także w „The Defence Horizon Journal". Wskazano, że powinna ona być postrzegana odmiennie od tradycyjnych koncepcji. Jej oddziaływanie nie dotyczy bowiem ani terytorium, ani dominacji nad zasobami, lecz jest to konflikt pomiędzy różnymi percepcjami, przekonaniami, a nawet zderzenie kultur czy cywilizacji[67]. Sojusz Północnoatlantycki definiuje wojnę kognitywną jako:

> Działania prowadzone w synchronizacji z innymi instrumentami władzy, mające na celu oddziaływanie na postawy i zachowania poprzez wpływanie na ochronę oraz/lub zakłócanie procesów poznawczych jednostek i grup w celu uzyskania przewagi. Działania te są bardzo zróżnicowane i mogą obejmować wspierające lub sprzeczne elementy kulturowe bądź spersonalizowane – psychologia społeczna, teoria gier oraz etyka stanowią istotne czynniki wpływające[68].

---

[64] A. Szczygielska, *Wojna kognitywna – źródła i zasadnicze cechy*, „Kwartalnik Bellona" 2025, t. 720, nr 1, s. 39–40. https://doi.org/10.5604/01.3001.0055.1652.

[65] A. Skrabacz, A. Pajka, B. Więckowski, *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych*, „Journal of Modern Science" 2025, s. 711. https://doi.org/10.13166/jms/203647.

[66] M.J. Cheatham i in., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/ [dostęp: 4 XI 2025].

[67] P.B.M.J. Pijpers, *On Cognitive Warfare: The Anatomy of Disinformation*, The Defence Horizon Journal, 21 III 2024 r., https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/ [dostęp: 26 X 2025].

[68] *Cognitive Warfare: Strengthening and Defending the Mind*, NATO, 5 IV 2023 r., https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ [dostęp: 15 XI 2025].

Podsumowując, wojna kognitywna to zintegrowane oddziaływanie psychologiczne na poziomach strategicznym, operacyjnym i taktycznym w celu wpływania na postawy i zachowania grup docelowych i tym samym kształtowania postrzegania rzeczywistości zgodnie z interesami agresora i uzyskania przewagi we wszystkich kluczowych obszarach funkcjonowania państwa.

Wojna hybrydowa

W nowoczesnych konfliktach[69] wykorzystuje się szerokie spektrum instrumentów oddziaływania. Według Hanny Smith na działania hybrydowe składają się jawne i niejawne działania, militarne i niemilitarne środki, oraz m.in. wywiad czy operacje cybernetyczne[70]. Jest to połączenie (…) *metod konwencjonalnych i niekonwencjonalnych (tj. dyplomatycznych, militarnych, ekonomicznych i technologicznych), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe*[71].

Artur Gruszczak wskazuje, że na wojnę hybrydową składają się elementy: wojen klasycznych i nowoczesnych, konfliktów asymetrycznych, przełomowych technologii wojskowych i prymitywnych narzędzi oddziaływania, walki o terytoria i zasoby oraz sporów o tożsamość i wartości, a także konfrontacji radykalizmu i kosmopolityzmu[72].

Autor niniejszego artykułu proponuje określić wojnę hybrydową jako wielowymiarowe wrogie działania łączące elementy kinetyczne i niekinetyczne, regularne i nieregularne, symetryczne i asymetryczne, konwencjonalne i niekonwencjonalne, które przy wykorzystaniu operacji informacyjnych i działań psychologicznych wpływają na sposób myślenia i działania grupy docelowej (tabela 1).

---

[69] Autor celowo używa terminu nowoczesny, a nie współczesny, ponieważ jego zdaniem to zasoby i potencjał do prowadzenia wojny definiują jej charakter, a nie (tylko) czasy, w których jest prowadzona.

[70] H. Smith, *Countering Hybrid Threats*, w: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (red.), Paris 2019, s. 16.

[71] *Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018 [dostęp: 22 X 2025].

[72] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red. nauk.), Warszawa 2011, s. 11.

Tabela 1. Elementy wojny hybrydowej.

ELEMENTY WOJNY HYBRYDOWEJ	
Kategoria	**Cechy i charakterystyka**
Rodzaj rażenia	**kinetyczne:** wykorzystanie siły fizycznej i mocy rażenia (działanie ludzi i sprzętu). Pożądanym efektem jest zniszczenie siły żywej i infrastruktury przeciwnika Przykład: wojska niszczą się wzajemnie, wykorzystując żołnierzy, czołgi, samoloty, systemy rakietowe itd.
	niekinetyczne: wykorzystanie innych niż kinetyczne środki rażenia do prowadzenia walki, także tzw. *soft power*[73] Przykład: przeciwnik prowadzi operacje informacyjne, ataki cybernetyczne na infrastrukturę krytyczną, werbuje tajnych współpracowników
Status sił i środków	**regularne:** działania prowadzone przez formalne, zorganizowane i umundurowane siły zbrojne państwa. Działania w ramach międzynarodowego prawa konfliktów zbrojnych, zazwyczaj scentralizowane, planowane i realizowane zgodnie z przyjętymi doktrynami wojskowymi Przykład: dwie armie państwowe walczą przeciwko sobie
	nieregularne: działania prowadzone przez nieformalne, zorganizowane siły (np. partyzanckie). Są nierównomiernie rozłożone w czasie i przestrzeni. Zazwyczaj wykorzystywane przez siły mniej liczne i o słabszym potencjale militarnym Przykład: partyzanci organizują zasadzki w lasach i niszczą konwoje z amunicją, ludność cywilna okupowanych terenów organizuje powstanie przeciwko okupantowi

[73] *Soft power* to „sposób oddziaływania na innych za pomocą pozamilitarnych i pozaekonomicznych środków (…). Atrakcyjność, budowa wizerunku, przekonanie do własnych racji, wreszcie narzucenie pewnej wizji czy narracji innym (…)", w: A. Rzegocki, *Soft power – niedoceniana siła*, w: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (red. nauk.), Kraków 2013, s. 158.

ELEMENTY WOJNY HYBRYDOWEJ	
Kategoria	**Cechy i charakterystyka**
Porównanie potencjałów	**symetryczne:** walczące strony dysponują porównywalnym potencjałem do prowadzenia wojny Przykład: dwie armie mają podobną liczbę żołnierzy i sprzętu oraz podobne możliwości technologiczne i uwarunkowania państwowe do prowadzenia wojny
	asymetryczne: walczące strony dysponują znacząco różnym potencjałem militarnym, a także zdecydowanie różnią się w zakresie możliwości technologicznych i uwarunkowań państwowych do prowadzenia wojny. Istotą tych działań jest wykorzystanie sił i środków, które będą skuteczne przy dużych różnicach potencjału Przykład: hakerzy włamują się do państwowego systemu teleinformatycznego i paraliżują ruch pociągów w kraju (mała grupa walczy z państwem), terrorysta przeprowadza zamach bombowy na infrastrukturę państwa
Formy i metody	**konwencjonalne:** tradycyjne formy i metody prowadzenia walki przy wykorzystaniu sił i środków z zasady przeznaczonych do tego celu Przykład: wykorzystanie karabinów, czołgów czy pocisków rakietowych
	niekonwencjonalne: formy i metody inne niż tradycyjne, wykorzystujące siły i środki nieprzeznaczone do prowadzenia wojny Przykład: wykorzystanie improwizowanych ładunków wybuchowych umieszczonych w zabawkach dla dzieci, koktajle Mołotowa, bojowe zastosowanie dronów cywilnych, pas szahida[74]

Źródło: opracowanie własne.

Podsumowując, wojna hybrydowa stanowi kumulację odmiennych form, metod i technik wrogiego działania: o różnych potencjałach, w wielu domenach i w różnych środowiskach. Jest także pojęciem uniwersalnym, które pozwala omawiać zagrożenia złożone i atypowe.

[74] Pas szahida – pas lub kamizelka, wypełniona materiałem wybuchowym i wyposażona w detonator, używana przez zamachowców samobójców. Zob. hasło: pas szahida, *Wielki słownik języka polskiego*, https://wsjp.pl/haslo/podglad/85144/pas-szahida [dostęp: 14 XII 2025].

Podsumowanie

Autor skupił się na uporządkowaniu i charakterystyce podstawowych pojęć w dyskursie nad wrogim wykorzystaniem informacji w ramach wojny kognitywnej w kontekście wojny hybrydowej. Podkreślił, że postrzeganie domeny poznawczej jako przestrzeni wrogich działań prowadzi do wyodrębnienia zjawiska wojny kognitywnej, która łączy operacje informacyjne i działania psychologiczne. Wojna ta jest zaawansowaną formą działań wykorzystujących informację i wpływ psychologiczny, umożliwiającą osiągnięcie przewagi na polu walki. Jej celem jest modyfikowanie przez agresora postaw i zachowań grupy docelowej w taki sposób, aby były one zgodne z jego wolą.

Rosnące zagrożenia hybrydowe ukazują nowy wymiar walki o umysły, a możliwość wpływania na postrzeganie rzeczywistości czyni sferę kognitywną teatrem wrogich działań oraz istotnym wymiarem współczesnych konfliktów. Autor podkreśla, że w związku ze zwiększającym się arsenałem nowoczesnych technologii świat stanie w obliczu nowej odsłony zimnej wojny, która sparaliżuje wykorzystanie kinetycznych środków walki w obawie przed zniszczeniem współczesnych cywilizacji. Wówczas będzie prowadzona totalna wojna kognitywna mająca na celu ukierunkowanie postrzegania rzeczywistości.

Bibliografia

Bąkowicz K., *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje*, „Zeszyty Naukowe Akademii Górnośląskiej" 2023, nr 10, s. 127–137. https://doi.org/10.53259/2023.10.13.

Dalinczuk L., *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego*, w: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (red. nauk.), Biała Podlaska 2021, s. 176–183.

Disinformation, w: R. Deacon, *Spyclopaedia*, London 1989.

Disinformation, w: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002.

Floridi L., *A Look into the Future Impact of ICT on our Lives*, „The Information Society" 2007, t. 23, nr 1, s. 59–64. https://doi.org/10.1080/01972240601059094.

Franco C. de, *Media Power and the Transformation of War*, New York 2012.

Frąś J., *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" 2011, nr 21, s. 29–41.

Golitsyn A., *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red. nauk.), Warszawa 2011, s. 9–17.

Kaczmarek K., Karpiuk M., Melchior C., *Disinformation as a Threat to State Security*, „Przegląd Nauk o Obronności" 2024, nr 20, s. 45–54. https://doi.org/10.37055/pno/205780.

Karpiuk W.M., *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, „Cybersecurity and Law" 2024, nr 2, s. 234–245.

Kisilowska M., *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2011, nr 2, s. 35–52. https://doi.org/10.36702/zin.666.

Koncepcja Obronna Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Warszawa 2017.

Łapszyński A., *Monitoring the Information Environment In the Baltic Sea Region*, „The Baltic Amber. Multinational Corps Northeast Magazine" 2020.

McKnight C., *The Personal Construction of Information Space*, „Journal of the American Society for Information Science" 2000, t. 51, nr 8, s. 730–733. https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8.

Meriläinen N., *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, „Proceedings of the 6th International Conference on AI Research", Italy 2025, s. 306–312. https://doi.org/10.34190/icair.5.1.4353.

Moskalewicz-Kwiatkowska K., *Pasożytnicza strategia rosyjskiej propagandy*, Warszawa 2024.

NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

Olechowski M., *Wojna psychologiczna – próba zdefiniowania pojęcia*, „Wiedza Obronna" 2018, wydanie podwójne t. 262–263, nr 1–2, s. 91–106. https://doi.org/10.34752/ahf8-sd31.

Otłowski T., *Rosyjskie myślenie o wojnie*, „Polska Zbrojna" 2021, nr 5, s. 80–82.

Pacepa I.M., Rychlak R.J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Gliwice 2015.

Pepłoński A., *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944*, Kraków 2011.

Romanych M.J., *Visualizing the Information Environment*, „Military Intelligence Professional Bulletin" 2003, t. 29, nr 3, s. 5–8.

Rzegocki A., *Soft power – niedoceniana siła*, w: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (red. nauk.), Kraków 2013, s. 155–160.

Skrabacz A., Pajka A., Więckowski B., *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych*, „Journal of Modern Science" 2025, s. 706–722. https://doi.org/10.13166/jms/203647.

Smith H., *Countering Hybrid Threats*, w: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (red.), Paris 2019.

Szczygielska A., *Wojna kognitywna – źródła i zasadnicze cechy*, „Kwartalnik Bellona" 2025, t. 720, nr 1, s. 27–46. https://doi.org/10.5604/01.3001.0055.1652.

Vlahos M., *Entering the Infosphere*, „Journal of International Affairs" 1998, t. 51, nr 2, s. 497–525.

Volkoff V., *Psychosocjotechnika. Dezinformacja. Oręż wojny*, Warszawa 1991.

Wojnowski M., *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 13–39.

Z tarczą! Jak chronić się przed dezinformacją?, K. Mikulski, M. Krawczyk (red.), Kraków 2021.

Zielonka Z., Rumiński K., *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017.

Źródła internetowe

Balcewicz J., *Zwalczanie dezinformacji w internecie: podejście europejskie*, Cyberpolicy NASK, 26 IV 2018 r., https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie [dostęp: 17 X 2025].

Biuro Bezpieczeństwa Narodowego 2015–2025, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209,Biuro-Bezpieczenstwa-Narodowego-2015-2025.html [dostęp: 28 IX 2026].

Borden A., *What Is Information Warfare?*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf [dostęp: 20 V 2024].

Bugayova N., Stepanenko K., *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf [dostęp: 28 IX 2026].

Calkayis M., *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025 r., https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/ [dostęp: 6 XI 2025].

Cheatham M.J., Geyer A.M., Nohle A.P., Vazquez J.E., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/ [dostęp: 4 XI 2025].

Chroń się przed dezinformacją, NASK, https://www.nask.pl/instytut/dla-ciebie/dezinfo [dostęp: 19 IX 2025].

Cognitive Warfare: Strengthening and Defending the Mind, NATO, 5 IV 2023 r., https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ [dostęp: 15 XI 2025].

Counter-FIMI Toolbox for Diplomats. A Conceptual Framework, https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf [dostęp: 2 IX 2026].

Creation of the European External Action Service, European Union External Action, 19 VIII 2021 r., https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [dostęp: 20 XII 2025].

Czy wiesz jak chronić się przed dezinformacją?, Komenda Powiatowa Policji w Oławie, 24 XI 2024 r., https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html [dostęp: 15 IX 2025].

Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany. Sprawozdanie specjalne, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_PL.pdf [dostęp: 15 X 2025].

Dezinformacja, https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dezinformacja/ [dostęp: 28 IX 2025].

Dezinformacja: 10 kroków, by chronić siebie i innych, Parlament Europejski, 11 VI 2025 r., https://www.europarl.europa.eu/topics/pl/article/20250603STO28720/dezinformacja-10-krokow-by-chronic-siebie-i-innych [dostęp: 21 X 2025].

Dlaczego obca propaganda jest skuteczna w obszarze obronności?, Stop Fake Org, 5 VIII 2019 r., https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/ [dostęp: 29 X 2025].

Encyklopedia Bezpieczeństwa, t. 5, O. Wasiuta, S. Wasiuta (red.), https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf [dostęp: 2 XII 2025].

Encyklopedia Bezpieczeństwa Narodowego, Encyklopedia Bezpieczeństwa, t. 5, O. Wasiuta, S. Wasiuta (red.), https://encyklopedia.revite.pl/articles/view/643 [dostęp: 20 XI 2025].

Gorzelnik N., *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media*, INN Poland, 28 III 2022 r., https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad [dostęp: 28 VIII 2024].

Karalus A., *Czym jest wojna kognitywna?*, YouTube, 28 I 2025 r., https://www.youtube.com/watch?v=YXIOrA_rNGY [dostęp: 5 XI 2025].

NATO 2022 Strategic Concept, NATO, 29 VII 2022 r., https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept [dostęp: 9 XII 2024].

Nogacki R., Surdyk K., *Teoria i praktyka działań dezinformacyjnych*, Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020 r., https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html [dostęp: 19 VIII 2025].

Oleksiejuk M., *Rosyjski syndrom oblężonej twierdzy*, Warsaw Institute, 31 VIII 2020 r., https://warsawinstitute.org/pl/rosyjski-syndrom-oblezonej-twierdzy/ [dostęp: 29 VIII 2025].

Pijpers P.B.M.J., *On Cognitive Warfare: The Anatomy of Disinformation*, The Defence Horizon Journal, 21 III 2024 r., https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/ [dostęp: 26 X 2025].

Protecting the Alliance Against the Threat of Cognitive Warfare, YouTube, 9 V 2023 r., https://www.youtube.com/watch?v=4Pn57uoyYEA [dostęp: 5 XI 2025].

Rozpoznawanie nieprawdziwych informacji, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji [dostęp: 20 III 2023].

Słownik języka polskiego, https://sjp.pwn.pl/sjp/manipulacja;2481186 [dostęp: 10 IX 2025].

Słownik języka polskiego, https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html [dostęp: 20 XI 2025].

Tomala L., *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie*, Nauka w Polsce, 7 II 2021 r., https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak [dostęp: 15 X 2025].

Tzu S., *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf [dostęp: 27 IX 2025].

Vademecum Bezpieczeństwa Informacyjnego, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/ [dostęp: 26 XI 2025].

Wielki słownik języka polskiego, https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna [dostęp: 20 XI 2025].

Wielki słownik języka polskiego, https://wsjp.pl/haslo/podglad/85144/pas-szahida [dostęp: 14 XII 2025].

Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie, Serwis Rzeczypospolitej Polskiej, 10 VIII 2023 r., https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie [dostęp: 27 X 2025].

Inne dokumenty

Recommendation of the Committee of Ministers to member states on the remit of public service media in the information society (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec(2007)3, https://search.coe.int/cm?i=09000016805d6bc5 [dostęp: 14 IX 2025].

Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018 [dostęp: 22 X 2025].

Płk dr Tomasz Gergelewicz

Doktor nauk w dyscyplinie nauk o bezpieczeństwie. Zajmuje się badaniem wpływu operacji informacyjnych na bezpieczeństwo oraz praktycznym budowaniem odporności społecznej na zagrożenia kognitywne. Doświadczenia z obszaru komunikacji strategicznej i przeciwdziałania dezinformacji zdobywał w Centrum Operacyjnym Ministra Obrony Narodowej oraz w Akademickim Centrum Komunikacji Strategicznej przy Akademii Sztuki Wojennej. Działalność dydaktyczną i publicystyczną realizuje w obszarze strategii bezpieczeństwa, komunikacji strategicznej i przeciwdziałania wrogim operacjom informacyjnym, w tym wykorzystaniu technologii opartych na sztucznej inteligencji.

Kontakt: t.gergelewicz@wp.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 39–70
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.022.24171

ARTYKUŁ

Wsparcie układu pozamilitarnego przez Wojska Obrony Terytorialnej jako element regulacji ograniczających efektywne wykorzystanie formacji w sytuacjach kryzysowych

Support of the non-military system by the Territorial Defence Forces as an element of regulations limiting the effective use of formations in crisis situations

JANUSZ LEŻOŃ

3 Podkarpacka Brygada Obrony Terytorialnej w Rzeszowie

https://orcid.org/0009-0004-8911-0616

Abstrakt

Obserwowane zaangażowanie Wojsk Obrony Terytorialnej (WOT) w realizację zadań z zakresu zarządzania kryzysowego może budzić przekonanie, że ta formacja działa na podstawie innych zasad niż wojska operacyjne i jako służba jest wykorzystywana w sytuacjach kryzysowych w spo sób automatyczny i natychmiastowy. Cel artykułu to odpowiedź na pytanie: czy obowiązujące regulacje prawne dotyczące użycia Sił Zbrojnych RP umożliwiają efektywne (powszechne, natychmiastowe, niezwłoczne) wykorzystanie WOT w systemie zarządzania kryzysowego? Autor dokonuje analizy roli WOT w systemie zarządzania kryzysowego. Wskazuje podstawy prawne użycia formacji do wsparcia układu pozamilitarnego w sytuacjach kryzysowych i zwraca uwagę na występujące w tym zakresie ograniczenia formalnoprawne. Ponadto przedstawia działania podjęte przez WOT w celu usprawnienia procedur użycia formacji w sytuacjach kryzysowych. Autor wskazał

również niezbędne zmiany, które umożliwią optymalne i efektywne wykorzystanie WOT do realizacji zadań z zakresu zarządzania kryzysowego.

Słowa kluczowe zarządzanie kryzysowe, Wojska Obrony Terytorialnej, procedury aktywacji sił zbrojnych, elementy systemu zarządzania kryzysowego

Abstract The involvement of the Territorial Defence Forces (WOT) in the implementation of crisis management tasks, may give rise to the belief that this formation operates on the basis of different principles than the operational forces, and is used as a service in crisis situations in an automatic and immediate manner. The aim of the article is to answer the question: do the current legal regulations governing the use of the Polish Armed Forces allow for the effective (widespread, immediate, prompt) deployment of the WOT in the crisis management system? The author analyses the role of the WOT in the crisis management system. He indicates the legal basis for the use of the formation to support the non-military system in crisis situations and draws attention to the formal and legal limitations in this area. Furthermore, he presents the actions taken by the WOT to improve the procedures for the use of the formation in crisis situations. The author highlighted necessary changes in order to optimally and effectively use the WOT to carry out crisis management tasks.

Keywords crisis management, Territorial Defence Forces, procedures for activation of the armed forces, elements of the crisis management system

Wprowadzenie

Wejście w życie ustawy o obronie Ojczyzny (dalej: u.o.o.)[1] wprowadziło nowe zadania dla Wojsk Obrony Terytorialnej (WOT) w obszarze zarządzania kryzysowego. Jednym z tych zadań, realizowanych zarówno w czasie pokoju, jak i kryzysu, jest wspieranie elementów podsystemu niemilitarnego w realizacji zadań z zakresu zarządzania kryzysowego, tj. udział w niezwłocznym i powszechnym reagowaniu na zagrożenie o charakterze niemilitarnym. Oprócz ustawy te kwestie reguluje doktryna użycia WOT, w której wskazano szeroki zakres aktywności tych

[1] *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny.*

wojsk w zależności od celów, potrzeb i rozwoju sytuacji, a także skategoryzowano i pogrupowano działania stosownie do stanu gotowości obronnej państwa[2]. Interpretując wprost te zapisy, można odnieść wrażenie, że pododdziały WOT realizują takie działania automatycznie. Mogą o tym świadczyć użyte w doktrynie sformułowania „niezwłocznym", „powszechnym". W rzeczywistości tak nie jest[3]. Zgodnie z tymi przepisami WOT są traktowane na równi z pozostałymi rodzajami Sił Zbrojnych RP. Ustawodawca nie przewidział oddzielnego trybu uruchomienia sił WOT do realizacji zadań z zakresu zarządzania kryzysowego[4], mimo że na podstawie u.o.o. dowódca WOT jest odpowiedzialny za: planowanie, koordynację i wykonywanie zadań związanych z udziałem oddziałów i pododdziałów Sił Zbrojnych RP w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działań w zakresie ochrony mienia, akcjach poszukiwawczych oraz akcjach ratowania lub ochrony zdrowia i życia ludzkiego, a także za udział w realizacji zadań z zakresu zarządzania kryzysowego[5].

Każde użycie sił zbrojnych musi być poprzedzone wnioskiem wojewody, w sytuacji kiedy użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające[6]. Katalog zadań został określony w ustawie o zarządzaniu kryzysowym (dalej u.z.k.)[7] bez rozróżnienia na rodzaje wojsk.

Problem badawczy wyraża pytanie: czy obowiązujące regulacje prawne dotyczące użycia Sił Zbrojnych RP umożliwiają efektywne (powszechne, natychmiastowe, niezwłoczne) wykorzystanie WOT w systemie zarządzania kryzysowego? Odpowiedź na nie wymaga zidentyfikowania szczegółowych problemów w postaci pytań:

1. Jakie akty prawne regulują kwestie wsparcia układu pozamilitarnego przez Siły Zbrojne RP w sytuacjach kryzysowych?
2. Jakie są procedury aktywacji wydzielonych sił i środków sił zbrojnych do zadań z zakresu zarządzania kryzysowego?
3. Jakie działania podjęły WOT w celu usprawnienia tych procedur?
4. W jaki sposób można zoptymalizować wykorzystanie WOT do realizacji zadań z zakresu zarządzania kryzysowego?

Autor przyjął następującą hipotezę badawczą: obowiązujące regulacje prawne ograniczają możliwość pełnego wykorzystania potencjału WOT w systemie

---

[2] *Wojska Obrony Terytorialnej w operacji*, DD-3.40, Warszawa 2018, s. 14–16.

[3] J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego*, „Kwartalnik Bellona" 2026, t. 724, nr 1, s. 150. https://doi.org/10.5604/01.3001.0055.6961.

[4] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

[5] Art. 22 ust. 2 pkt 6 u.o.o.

[6] Art. 14 ust. 2 pkt 4 ustawy o zarządzaniu kryzysowym.

[7] Tamże, art. 25 ust. 3.

zarządzania kryzysowego (SZK). Ograniczenia wynikają przede wszystkim z zamkniętego katalogu realizowanych zadań z zakresu zarządzania kryzysowego, nieprzewidującego zagrożeń cechujących się sporą dynamiką, złożonością i nieprzewidywalnością[8], oraz z obowiązujących procedur aktywacji Sił Zbrojnych RP do realizacji zadań z zakresu zarządzania kryzysowego.

Zagrożenia takie jak klęski żywiołowe, w Polsce wywołane najczęściej przez powodzie i podtopienia, są stosunkowo łatwe do przewidzenia i neutralizacji. Nie można tego powiedzieć o zagrożeniach związanych z różnego rodzaju konfliktami, które mogą prowadzić do destabilizacji nawet całych państw[9]. Najgroźniejsze wydają się te o charakterze hybrydowym, mające znamiona zarówno działań militarnych, jak i niemilitarnych, obejmujące szerokie spektrum działań, takich jak: akty dywersji i sabotażu, dezinformacja, cyberataki czy presja migracyjna, z którą Polska mierzy się od 2021 r.[10] System zarządzania kryzysowego musi być zdolny do natychmiastowej reakcji chroniącej punkty ważne dla funkcjonowania lokalnych społeczności i całego państwa[11]. W tym kontekście struktura organizacyjna WOT, ich powszechność oraz przede wszystkim możliwości realizacji różnych działań wskazują, że pełniejsze i efektywniejsze wykorzystanie pododdziałów

[8] S. Smoleński, *Procedury zarządzania kryzysowego*, „Zeszyty Naukowe SGSP" 2022, nr 84, s. 149–160. http://dx.doi.org/10.5604/01.3001.0016.1807.

[9] W. Walczak, *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej*, „Przedsiębiorczość i Zarządzanie" 2009, t. 10, nr 8, s. 98–101; A. Bieńkowska, Z. Kral, A. Zabłocka-Kluczka, *Istota i ewolucja zarządzania kryzysowego*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2005, nr 1092, s. 25–32.

[10] K. Kociubiński, V. Shadurski, *Zagrożenia hybrydowe dla bezpieczeństwa Polski ze strony Białorusi po 2020 r.*, „Wschodnioznawstwo" 2024, t. 18, s. 231–253. https://doi.org/10.4467/20827695WSC.24.015.20630; M. Chudoba, *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej*, „Studia Bezpieczeństwa Narodowego" 2023, z. 29, nr 3, s. 121–140. https://doi.org/10.37055/sbn/173489; E. Jakubiak, *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie*, „Studia Bezpieczeństwa Narodowego" 2022, t. 24, nr 2, s. 71–82. https://doi.org/10.37055/sbn/151015; W. Skomra, K. Wojtasik, *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK*, „Terroryzm – studia, analizy, prewencja" 2025, wydanie specjalne: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, s. 13–34. https://doi.org/10.4467/27204383TER.25.001.21504; A. Zaręba, *Dezinformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cyberseciurity)*, „Cybersecurity and Law" 2025, t. 13, nr 1, s. 95–107; M. Czuryk, *Status prawny samorządu terytorialnego w sferze zarządzania kryzysowego*, „Cybersecurity and Law" 2024, t. 12, nr 2, s. 174–186. http://dx.doi.org/10.35467/cal/188567; J. Leżoń, M. Bojarczuk, J. Traciak, *Znaczenie działań niekinetycznych w nowoczesnych siłach zbrojnych*, „Polityka i Społeczeństwo" 2025, t. 23, nr 1, s. 174–190. https://doi.org/10.15584/polispol.2025.1.10; Z. Śliwa, A.K. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, „Wiedza Obronna" 2022, t. 278, nr 1, s. 89–107. https://doi.org/10.34752/2022-d278.

[11] W. Goleński, D. Zimny, *Przygotowanie państwa na zagrożenia hybrydowe*, „Kontrola Państwowa" 2024, nr 5, s. 18–37.

WOT byłoby możliwe wtedy, gdyby formacja funkcjonowała jako tzw. komponent terytorialny będący integralną częścią szeroko pojmowanej obrony terytorialnej[12]. Istotą tej obrony jest m.in. podejmowanie decyzji na szczeblu lokalnym, adekwatnie do sytuacji i potrzeb zarówno w czasie pokoju, kryzysu, jak i wojny[13].

Artykuł ma charakter analityczno-problemowy i opiera się na jakościowym podejściu badawczym. Jako główną metodę badawczą wykorzystano analizę treści[14]. Ponadto zastosowano metody syntezy, definiowania, abstrahowania oraz interpretacji. Pozwoliły one na charakterystykę badanych zjawisk oraz stanowiły podstawę do identyfikacji ograniczeń, które uniemożliwiają efektywne wykorzystanie WOT w SZK.

Autor nieprzerwanie od 2017 r. pełni służbę w WOT na różnych stanowiskach. Prezentowane treści są zatem wynikiem zarówno analiz regulacji prawnych, jak i oceny funkcjonowania procedur zarządzania kryzysowego w realnych działaniach. Autor jest również twórcą wielu obowiązujących rozwiązań w zakresie organizacji SZK w brygadzie obrony terytorialnej prezentowanych w artykule.

Definicje zarządzania kryzysowego i sytuacji kryzysowej

System zarządzania kryzysowego jest kluczowym elementem bezpieczeństwa państwa, reagującym niemal w każdej sytuacji kryzysowej[15]. Pojęcie zarządzania kryzysowego nie ma jednoznacznej definicji wśród polskich badaczy[16]. Podchodzą oni do tego terminu w dwojaki sposób. Pierwszy dotyczy definicji określonej ściśle w u.z.k., drugi odnosi się do problematyki zarządzania jako wyodrębnionej części nauki[17]. Zgodnie z tematem artykułu do dalszej analizy przyjęto zapisy u.z.k. Zarządzanie kryzysowe jest w niej traktowane jako (…) *działalność organów administracji*

[12] J. Leżoń, J. Traciak, J. Zaguła, *Wojska Obrony Terytorialnej rodzajem Sił Zbrojnych – teoria czy rzeczywistość?*, „Kwartalnik Bellona" 2025, t. 722, nr 3, s. 80. http://dx.doi.org/10.5604/01.3001.0055.4501.

[13] J. Marczak, R. Jakubczak, *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP*, https://www.researchgate.net/publication/337929735_Raport_strategiczny_Sily_Zbrojne_RP_w_drugiej_dekadzie_XXI_wieku_Koncepcja_strategiczna_Obrony_Terytorialnej_RP [dostęp: 8 VI 2026].

[14] E. Kalinowska, *Analiza treści jako technika badawcza*, „Dyskursy Młodych Andragogów / Adult Education Discourses" 2001, nr 2, s. 15–31. https://doi.org/10.34768/dma.vi02.286.

[15] P. Szmitkowski, *Plany zarządzania kryzysowego w świetle nowych regulacji prawnych*, „Doctrina. Studia Społeczno-Polityczne" 2016, t. 13, nr 13, s. 208.

[16] S. Smoleński, *Procedury zarządzania kryzysowego*…, s. 157.

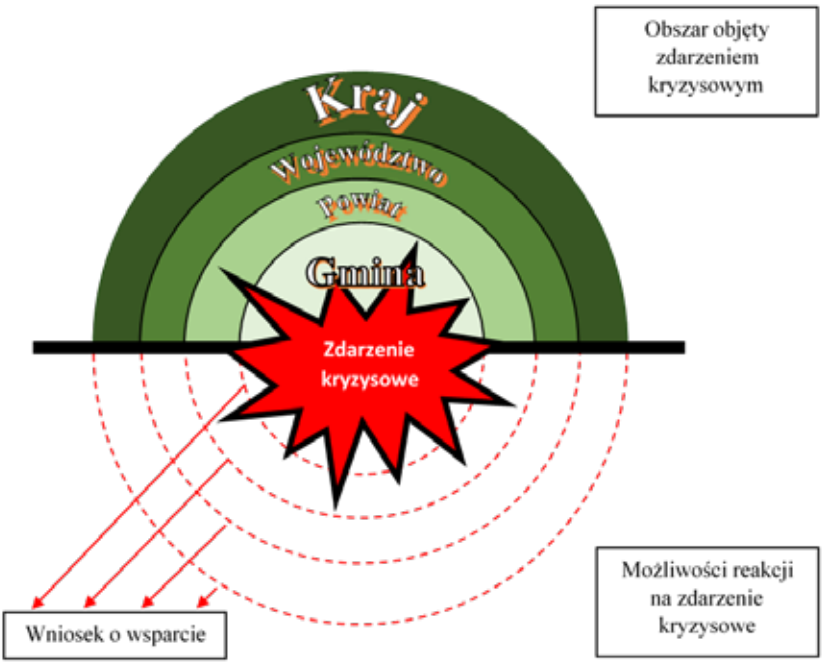
[17] P. Gromek, *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne*, „Zeszyty Naukowe SGSP" 2017, t. 63, nr 3, s. 23.

publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej[18]. Istotę tej definicji stanowi planowanie działań we wszystkich fazach zarządzania kryzysowego, tj.: reagowania, przygotowania, zapobiegania i odtwarzania. W ustawie zdefiniowano również pojęcie sytuacji kryzysowej jako (…) *sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków* (…)[19].

Z tych zapisów wynika, że o sytuacji kryzysowej możemy mówić wtedy, kiedy siły i środki administracji publicznej są niewystarczające i powodują znaczne ograniczenia w działaniu. Ta definicja wpisuje się w istotę zarządzania kryzysowego, którą, jak wcześniej wskazano, jest planowanie działań. Należy zwrócić uwagę także na hierarchiczność SZK oraz tego implikacje. To, co dla danego szczebla organizacyjnego jest sytuacją kryzysową, niekoniecznie jest nią na wyższym szczeblu organizacyjnym. Wynika to ze zdolności reagowania przez dany szczebel na określoną sytuację. Na przykład znaczne podtopienia na terenie jednej gminy i wyczerpanie się jej możliwości reakcji będą oznaczać dla tej gminy sytuację kryzysową (rysunek 1). Nie będzie to sytuacja kryzysowa dla powiatu, w skład którego wchodzi ta gmina, z uwagi na znacznie większe możliwości działania z wykorzystaniem dostępnych sił, środków i zasobów. Analogiczna sytuacja dotyczy kolejnych szczebli organizacyjnych.

[18] Art. 2 u.z.k.

[19] Tamże.



Rysunek 1. Zasięg sytuacji kryzysowej a możliwości reakcji na zdarzenie.

Źródło: opracowanie własne.

Organizacja zarządzania kryzysowego w aspekcie użycia sił zbrojnych

Obszar wsparcia administracji przez siły zbrojne jest regulowany aktami prawnymi. W tabeli 1 przedstawiono te najważniejsze, które odnoszą się do zaangażowania wojska, w tym WOT, w szeroko pojęty obszar kryzysowy. Zasadniczym aktem prawnym, wykorzystywanym w najszerszym zakresie, jest u.z.k.

Tabela 1. Wykaz aktów prawnych regulujących użycie sił zbrojnych w sytuacjach kryzysowych.

Akt prawny	Zakres zadań dla sił zbrojnych	Organ wnioskujący	Organ decyzyjny	Akt wykonawczy
Ustawa o obronie Ojczyzny	Ogólne uprawnienia dowódcy WOT w zakresie planowania, koordynacji i wykonywania zadań związanych z udziałem oddziałów i pododdziałów Sił Zbrojnych RP w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działań w zakresie ochrony mienia, akcjach poszukiwawczych oraz akcjach ratowania lub ochrony zdrowia i życia ludzkiego, a także udziału w realizacji zadań z zakresu zarządzania kryzysowego. Operacja wojskowa w czasie pokoju. Zadania prowadzone w celu zapewnienia bezpieczeństwa zewnętrznego państwa	Rada Ministrów	Prezydent	
Ustawa o stanie klęski żywiołowej	Zadania zgodne z „Planem reagowania kryzysowego". Działania ratownicze lub prewencyjne, wykonywane w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia	Wojewoda	Minister Obrony Narodowej	Rozporządzenie Rady Ministrów w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu

Akt prawny	Zakres zadań dla sił zbrojnych	Organ wnioskujący	Organ decyzyjny	Akt wykonawczy
Ustawa o zarządzaniu kryzysowym	Zadania z zakresu zarządzania kryzysowego, zgodnie z wojewódzkim planem zarządzania kryzysowego	Wojewoda	Minister Obrony Narodowej	
Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi	Zadania określone przez Głównego Inspektora Sanitarnego lub wojewodę	Wojewoda, Główny Inspektor Sanitarny	Minister Obrony Narodowej	
Ustawa o stanie wyjątkowym	Zgodnie z rozporządzeniem Rady Ministrów. Zadania wyznaczone przez Ministra Obrony Narodowej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych	Prezes Rady Ministrów	Prezydent	Rozporządzenie Rady Ministrów w sprawie szczegółowych zasad użycia oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej w czasie stanu wyjątkowego

Akt prawny	Zakres zadań dla sił zbrojnych	Organ wnioskujący	Organ decyzyjny	Akt wykonawczy
Ustawa o Straży Granicznej	Zadania ustalone przez Ministra Obrony Narodowej w porozumieniu z ministrem właściwym do spraw wewnętrznych	Prezes Rady Ministrów	Prezydent	Rozporządzenie Rady Ministrów w sprawie współdziałania Straży Granicznej oraz oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej
Ustawa o Policji	Zadania ustalone przez Ministra Obrony Narodowej w porozumieniu z ministrem właściwym do spraw wewnętrznych	Prezes Rady Ministrów	Prezydent	Rozporządzenie Rady Ministrów w sprawie użycia oddziałów i pododdziałów Policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego
Ustawa o działaniach antyterrorystycznych	Działania antyterrorystyczne, o charakterze terrorystycznym, w tym działania kontrterrorystyczne	Minister ds. Wewnętrznych	Minister Obrony Narodowej	Rozporządzenie Rady Ministrów w sprawie szczegółowych warunków i sposobu organizacji współdziałania oddziałów i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych Rzeczypospolitej Polskiej w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego

Akt prawny	Zakres zadań dla sił zbrojnych	Organ wnioskujący	Organ decyzyjny	Akt wykonawczy
Ustawa o ochronie żeglugi i portów morskich	Zapewnienie ochrony głównie statkom, obiektom portowym oraz związanej z nimi infrastrukturze	Minister ds. Wewnętrznych	Minister Obrony Narodowej	Rozporządzenie Rady Ministrów w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej ochrony
Ustawa o stanie wojennym	Na zasadach określonych w ustawie o ochronie ludności i obronie cywilnej oraz ustawie o zarządzaniu kryzysowym			
Ustawa o ochronie ludności i obronie cywilnej	Na zasadach określonych w ustawie		Minister Obrony Narodowej lub Naczelny dowódca Sił Zbrojnych Rzeczpospolitej Polskiej	

Źródło: opracowanie własne.

Regulacje dotyczące realizacji zadań z zakresu zarządzania kryzysowego można podzielić na trzy kategorie, które odnoszą się do charakteru zdarzenia: niemilitarny, hybrydowy oraz w czasie stanu wojennego i wojny. Wydaje się, że poruszanie się w tej materii ułatwiłaby konsolidacja aktów prawnych. Zaproponowana kategoryzacja może być pomocna, zwłaszcza w odniesieniu do realizacji określonych zadań oraz organów uprawnionych do wnioskowania o wsparcie sił zbrojnych oraz organów decyzyjnych.

Istotne jest również to, że każde użycie sił zbrojnych powinno być podporządkowane zapisom u.z.k. Artykuł 25 ust. 9 tej ustawy stanowi, że użycie doraźnych zgrupowań zadaniowych w sytuacji kryzysowej nie może zagrozić zdolności sił zbrojnych do realizacji zadań wynikających z Konstytucji RP i ratyfikowanych umów międzynarodowych. Ten zapis nie odnosi się jednak do pozostałych aktów prawnych regulujących użycie wojska do zadań z zakresu zarządzania kryzysowego. Czy istnieje zatem pełna dowolność w tym obszarze?

Artykuł 26 Konstytucji określa, że Siły Zbrojne RP służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic. Jest to ogólny zapis, niemniej wyraża stałą gotowość sił zbrojnych do działania w celu zapewnienia szeroko pojętego bezpieczeństwa państwa. Istotny element tej gotowości to odpowiednie wyszkolenie sił zbrojnych. Decydenci przy podejmowaniu decyzji o użyciu sił zbrojnych w sytuacjach kryzysowych powinni mieć na względzie realizację zaplanowanych istotnych ćwiczeń przygotowujących oddziały i pododdziały do realizacji zadań zgodnych z ich wojennym przeznaczeniem.

Obowiązujące przepisy dotyczące tego, jaki szczebel organizacyjny i w jakiej sytuacji może planować użycie sił zbrojnych i wnioskować o nie, są jednoznaczne i nie dają takiej możliwości gminom i powiatom. Decyzja o użyciu sił zbrojnych, w tym WOT, zapada na szczeblu ministerialnym. Podobne rozwiązania funkcjonują w dwóch krajach bałtyckich (Litwa, Łotwa)[20] oraz państwach nordyckich (Norwegia, Szwecja, Finlandia)[21]. Należy jednak zauważyć, że formacje obrony terytorialnej Litwy i Łotwy są integralną częścią wojsk lądowych[22]. W Norwegii, Szwecji oraz Finlandii formacje obrony terytorialnej, podobnie jak w Polsce, stanowią

[20] M. Gikiewicz, *Współczesny wymiar ochrony ludności i obrony cywilnej*, t. 1: *Wybrane państwa basenu Morza Bałtyckiego*, Warszawa 2026; J. Trocha, *Norweski system bezpieczeństwa cywilnego a uwarunkowania zagrożeń kryzysowych i wojennych kraju*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2017, t. 22, nr 2, s. 230–246.

[21] J. Grzela, *Obrona terytorialna w państwach nordyckich*, „Bezpieczeństwo. Teoria i Praktyka" 2017, t. 28, nr 3, s. 207–223.

[22] T. Małysa, *Wojska obrony terytorialnej w państwach bałtyckich*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3, s. 233.

odrębny rodzaj sił zbrojnych, ale ich struktura, wyposażenie oraz zadania wynikają z gwardyjskiego charakteru formacji[23]. Nieco inne rozwiązania przyjęto w Estonii, ponieważ uprawnienia o użyciu sił Estońskiej Ligii Obrony przekazano jej dowódcy. Działa ona na zasadzie obrony terytorialnej i realizuje zadania z taką samą intensywnością w czasie pokoju, kryzysu czy wojny[24]. Model estoński w największym stopniu odpowiada poglądom autora dotyczącym nowoczesnej obrony terytorialnej, jej roli i zadań we wszystkich stanach gotowości obronnej państwa.

W świetle krajowych regulacji prawnych z wnioskiem do ministra obrony narodowej o wsparcie przez siły zbrojne występuje szczebel wojewódzki. Ta zasada z jednej strony ogranicza zagrożenie nadinterpretacją określonych sytuacji kryzysowych prowadzącą do nieuzasadnionego wykorzystania wojska. Z drugiej strony pozbawia najniższe szczeble organizacyjne korzystania z istotnego wsparcia, jakiego mogą udzielić siły zbrojne. W tym kontekście należałoby poddać analizie obowiązujące zasady, mając na uwadze możliwości i potencjał WOT, zwłaszcza wynikający z terytorialności, szybkości reakcji, integracji z lokalnymi społecznościami. W obecnych uwarunkowaniach prawnych gminom i powiatom na etapie planowania pozostaje jedynie możliwość wnioskowania do szczebla nadrzędnego o wsparcie sił zbrojnych. Sprawia to, że obowiązujące zgodnie z przepisami prawa plany zarządzania kryzysowego gmin są stosunkowo ubogie, a standardowe procedury operacyjne traktują pobieżnie poszczególne zagrożenia.

Jak zauważa Franciszek Krynojewski, ekspert ds. obrony cywilnej, każda gmina musi mieć własny plan zarządzania kryzysowego, przygotowany na podstawie oceny zagrożenia dla konkretnej miejscowości i gminy i do nich dostosowany, choć można powielić pewne procedury i rozwiązania[25]. Taki plan musi przewidywać m.in. wybór miejsca zbiórki ewakuowanych, oznaczenie autokarów do ewakuacji, oznakowanie dróg ewakuacyjnych. Opracowane procedury postępowania są wdrażane natychmiastowo bez zbędnej zwłoki, co w przypadkach dynamicznych zjawisk odgrywa kluczową rolę w walce z żywiołem. Gminne plany są tak istotne, ponieważ wojewódzki plan zarządzania kryzysowego jest sumą powiatowych planów, na które

[23] Nie stanowią oddzielnego komponentu obrony terytorialnej obok wojsk operacyjnych, lecz są ich częścią, ponadto pozbawione terytorialnych organów dowodzenia realizują zadania w oderwaniu od lokalnych potrzeb na rzecz celów operacyjnych ustalanych poza strukturami terytorialnymi.

[24] U. Staśkiewicz, *Kaitseliit – estońska organizacja cywilna działająca na rzecz obronności państwa i bezpieczeństwa ludności*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, t. 69, nr 1, s. 16–25. https://doi.org/10.52097/eppism.8882.

[25] *Każda gmina musi mieć swój plan zarządzania kryzysowego. Nie może być kopiuj-wklej*, Portal Samorządowy, 20 IX 2024 r., https://www.portalsamorzadowy.pl/zmiany-w-prawie/kazda-gmina-musi-miec-swoj-plan-zarzadzania-kryzysowego-nie-moze-byc-kopiuj-wklej,570960.html [dostęp: 12 III 2026].

z kolei składają się gminne plany zarządzania kryzysowego. Krajowy plan zarządzania kryzysowego jest natomiast zbiorem wojewódzkich i resortowych planów. Każdy plan kolejnego wyższego szczebla organizacyjnego zawiera zatem elementy planu niższego szczebla, co tworzy hierarchiczną zależność między nimi. W konsekwencji jeśli plany na najniższym szczeblu nie będą szczegółowe, nie należy spodziewać się szczegółowości w planach wyższych szczebli. Opinie takie jak: „brak koordynacji", „spóźniona reakcja wojska", „bezsilność służb" wyrażane często w czasie sytuacji kryzysowej są najprawdopodobniej winą człowieka, który nie poradził sobie z podjęciem decyzji. Za przykład może posłużyć powódź na Dolnym Śląsku w 2024 r. Brak lub opóźnienie decyzji o zarządzeniu ewakuacji prewencyjnej w wielu przypadkach naraziły mieszkańców zagrożonych terenów na utratę życia lub zdrowia[26]. Tak było np. w Głuchołazach, gdzie zbyt późne podjęcie ewakuacji wymagało użycia do niej specjalistycznego sprzętu, w tym wojskowego[27].

W tym kontekście jeszcze większego znaczenia nabiera właściwie pojmowana i organizowana obrona terytorialna. Jej podstawą jest współdziałanie wszystkich elementów organizacyjnych (służby, straże, WOT)[28]. Działania skoncentrowane na ochronie terytorium powinny umożliwiać maksymalne wykorzystanie potencjału, w szczególności WOT działających razem z pozostałymi służbami, co tworzy pewnego rodzaju komponent nowoczesnej struktury obronnej państwa[29].

Pododdziały WOT, owszem, są przewidziane do realizacji zadań z zakresu zarządzania kryzysowego, jednak w świetle obowiązujących regulacji prawnych na zasadach tożsamych jak całe siły zbrojne. W opinii autora nie oznacza to zatem ani „niezwłoczności", ani „powszechności"[30]. Wszystko zależy od sytuacji, skali

[26] M. Kupryjańczyk, K. Lech, Ł. Derkacz, *Rola ratownictwa medycznego w systemie zarządzania kryzysowego na przykładzie powodzi w powiecie nyskim w 2024 roku*, „Kwartalnik Bellona" 2026, nr 4, s. 201–215. https://doi.org/10.5604/01.3001.0055.5824.

[27] *Powódź na południu Polski. Ewakuacje mieszkańców, lista miejscowości*, TVN24, 15 IX 2024 r., https://tvn24.pl/najnowsze/powodz-na-poludniu-polski-ewakuacje-mieszkancow-lista-miejscowosci-st8087871 [dostęp: 8 VI 2026].

[28] P. Wywiał, *Działania przeciwdywersyjne wojsk obrony terytorialnej w kontekście rosyjskiej dywersji na Ukrainie*, w: *Bezpieczeństwo Polski w warunkach członkostwa w Unii Europejskiej*, A. Żebrowski, Ł. Zweiffel, K. Kowalska (red. nauk.), Kraków 2018, s. 284–297; P. Żukowski, *Rola Terytorialnej Służby Wojskowej w systemie bezpieczeństwa militarnego Rzeczypospolitej Polskiej*, „Studia Bezpieczeństwa Narodowego" 2020, t. 17, nr 1, s. 157–166. https://doi.org/10.37055/sbn/144285.

[29] Z. Polcikiewicz, *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski*, „Acta Scientifica. Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2016, t. 7, nr 1, s. 399–413; R. Jakubczak, *Wybrane kwestie teorii Obrony Terytorialnej*, w: *Bezpieczeństwo, zarządzanie, medycyna i kultura fizyczna. Wybrane zagadnienia*, t. 4, J. Telak i in. (red.), Gdańsk 2020, s. 15–35.

[30] J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego*…, s. 150.

zjawiska, sił i środków możliwych do użycia przez wojewodę w pierwszej kolejności z udziałem służb do tego przewidzianych[31]. Wątpliwe jest zatem twierdzenie, że pododdziały WOT są ustawowo przewidziane do likwidacji skutków klęsk żywiołowych. Sytuacja ta wielokrotnie była z jednej strony powodem frustracji ludności, a z drugiej – konieczności podejmowania trudnych decyzji dotyczących użycia WOT. Powszechne przekonanie o tym, że z chwilą wejścia w życie u.o.o. całkowicie zmienił się SZK, nie ma odzwierciedlenia w obowiązujących przepisach[32], ponieważ u.z.k. z 2007 r. nie uległa zmianie. To wskazuje na trudność odnalezienia się dowódców oraz organów odpowiedzialnych za ochronę ludności w dużej liczbie aktów prawnych dotyczących wsparcia układu pozamilitarnego przez siły zbrojne oraz na konieczność nowelizacji przepisów prawa. Celem zmian powinno być dostosowanie uregulowań do sytuacji, w której w siłach zbrojnych występuje formacja WOT funkcjonująca na zupełnie innych zasadach niż pozostałe części sił zbrojnych, zdolna do wsparcia społeczności lokalnych „tu i teraz", bez zbędnych formalności, procedur prawnych i decyzji zapadających na szczeblu ministerialnym.

Procedury użycia Wojsk Obrony Terytorialnej w zarządzaniu kryzysowym

Niezależnie od wskazanych nieścisłości WOT mają predyspozycje zarówno do realizacji zadań z zakresu zarządzania kryzysowego[33], jak i kierowania nimi. SZK WOT stanowi integralną część SZK resortu obrony narodowej. Dowództwo WOT pełni funkcję Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej (CZK MON). Brygady obrony terytorialnej oraz brygady obrony pogranicza realizują zadania z zakresu zarządzania kryzysowego w swoich stałych rejonach odpowiedzialności wydzielonymi do tego celu modułami zadaniowymi. Zgodnie z u.o.o. dowódca WOT jest odpowiedzialny za planowanie, koordynację i wykonywanie zadań związanych z udziałem oddziałów i pododdziałów sił zbrojnych w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działań w zakresie ochrony mienia, akcjach poszukiwawczych oraz akcjach ratowania lub ochrony zdrowia i życia ludzkiego, a także udziału w realizacji zadań z zakresu zarządzania

[31] Państwowa Straż Pożarna, Policja, Ochotnicza Straż Pożarna, inne służby, straże, inspekcje.

[32] T. Stelmach, *Reorganizacja systemu zarządzania kryzysowego resortu obrony narodowej*, „Problemy Techniki Uzbrojenia" 2023, t. 163, nr 1, s. 39–55. https://doi.org/10.5604/01.3001.0053.5917.

[33] M. Klisz, *Utworzenie Wojsk Obrony Terytorialnej jako odpowiedź na nowe zagrożenia bezpieczeństwa państwa*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3, s. 70.

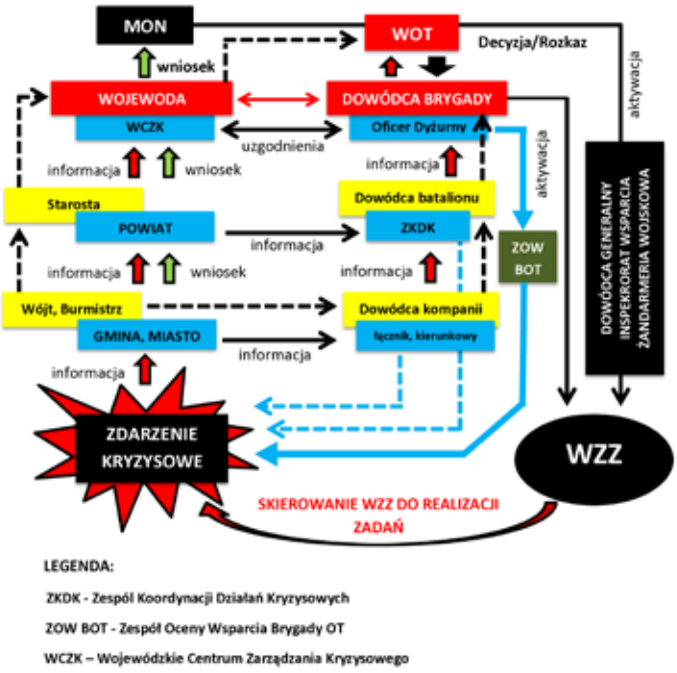
kryzysowego[34]. Jedną z przyczyn przyjęcia takiego rozwiązania było przeświadczenie o możliwości natychmiastowego użycia WOT w sytuacjach kryzysowych. Jest to słuszna i zasadna idea, wymaga jednak zmian wielu przepisów. Obecna forma może powodować stosowanie przez decydentów tzw. drogi na skróty i przyjmowanie jej w pewnym sensie za procedurę działania. Aby mogła zadziałać zasada „powszechności" i „natychmiastowości" działań WOT w sytuacjach kryzysowych, konieczne są zmiany legislacyjne.

Koordynacja zadań z zakresu zarządzania kryzysowego, usprawnienie procedur

Pomimo pewnych ograniczeń natury prawnej zainicjowano, na podstawie rozkazu dowódcy WOT, działania mające na celu ulepszyć koordynację zadań z zakresu zarządzania kryzysowego zarówno na szczeblu WOT, jak i poszczególnych województw. Wprowadzono sposób postępowania odnoszący się do umownych procedur, a następnie opracowano reguły, które usprawniły działania z zakresu zarządzania kryzysowego. Dotyczyły one przede wszystkim: sposobu przesyłania wniosków wojewodów o wsparcie sił zbrojnych, utrzymywania stałego kontaktu, sposobu wymiany informacji pomiędzy brygadami obrony terytorialnej a poszczególnymi Wojewódzkimi Centrami Zarządzania Kryzysowego (WCZK), sposobu działania i aktywacji Zespołów Reagowania Kryzysowego (ZRK) poszczególnych brygad oraz zasad wymiany informacji między jednostkami wojskowymi stacjonującymi na terenie województwa.

Następnie wdrożono działania mające na celu usprawnienie procesu decyzyjnego prowadzącego do skierowania sił w rejon działań kryzysowych. Rysunek 2 przedstawia drogę i sposób postępowania poszczególnych podmiotów zaangażowanych w SZK.

[34] Art. 22 ust. 2 pkt 6 u.o.o.



Rysunek 2. Schemat postępowania o skierowanie Sił Zbrojnych RP do zadań z zakresu zarządzania kryzysowego.

Źródło: opracowanie własne na podstawie dokumentów wewnętrznych WOT.

Dzięki skróceniu ścieżki decyzyjnej skraca się również czas reakcji na zdarzenie. Ułatwiają to następujące czynniki:

- ścisła współpraca pomiędzy wojewodą, dowódcą brygady wspieranym przez Zespół Oceny Wsparcia (ZOW) a dowódcą WOT – szefem CZK MON. Jej efektem jest sprawne procedowanie wniosku o wsparcie siłami i środkami wydzielonymi z sił zbrojnych zakończone wydaniem stosownych dokumentów decyzyjno-rozkazodawczych i skierowaniem Wojskowego Zgrupowania Zadaniowego (WZZ) w rejon realizacji zadań;
- krótki łańcuch dowodzenia: dowódca WOT (szef CZK MON) – dowódca brygady. Występowanie jedynie dwóch podmiotów w łańcuchu decyzyjnym pozwala na szybką i sprawną reakcję, w odróżnieniu np. od łańcucha: dowódca WOT – dowódca generalny Rodzajów Sił Zbrojnych RP – dowódca dywizji – dowódca brygady – i nierzadko dowódca jednostki wojskowej, występującego w przypadku konieczności użycia wojsk operacyjnych;

- stała współpraca i wymiana informacji ze wszystkimi jednostkami wojskowymi stacjonującymi na terenie województwa;
- działanie w terenie elementów systemu zarządzania kryzysowego (ESZK), takich jak Zespół Koordynacji Działań Kryzysowych (ZKDK) i otrzymywanie dzięki temu na bieżąco informacji na temat sytuacji w rejonie dotkniętym zdarzeniem kryzysowym.

Ostatni z wymienionych czynników ma duży wpływ na szybkość i skuteczność działania. Występowanie struktur WOT w każdym województwie, powiecie, gminie przekłada się na współdziałanie również w ramach zadań z zakresu zarządzania kryzysowego[35]. W zasadzie kluczowe znaczenie w SZK WOT ma zorganizowany i funkcjonujący SZK w brygadzie, czyli w dużym uproszczeniu – w województwie. Zgodnie z u.z.k. odpowiedzialnym za zarządzanie kryzysowe w województwie jest wojewoda, wspierany przez Wojewódzki Zespół Zarządzania Kryzysowego (WZZK), w skład którego, decyzją ministra obrony narodowej, wchodzi dowódca brygady obrony terytorialnej[36]. To on wspomaga wojewodę w zakresie możliwości wsparcia siłami i środkami sił zbrojnych poprzez doradzanie mu w kwestii wydzielenia określonych oddziałów, pododdziałów do realizacji zadań z zakresu zarządzania kryzysowego. Istota działania w uproszczeniu polega na równoległym przekazywaniu informacji (meldunków) o zdarzeniu kryzysowym w pionie administracji terenowej oraz pionie dowódczym WOT, przy zachowaniu poziomej wymiany informacji między samorządem a wojskiem. Pomocne w tym względzie okazało się utworzenie ESZK takich jak: ZOW[37], Zespół Wsparcia Odbudowy (ZWO)[38],

[35] I. Wróbel, *Perspektywy współdziałania wojsk obrony terytorialnej z administracją publiczną w zwalczaniu klęsk żywiołowych*, „Bezpieczeństwo. Teoria i Praktyka" 2017, t. 28, nr 3, s. 143.

[36] *Decyzja Ministra Obrony Narodowej Z-4 z 6 maja 2022 r. w sprawie Systemu Zarządzania Kryzysowego resortu obrony narodowej*.

[37] Nieetatowy podmiot wykonawczy dowódcy brygady, stanowiący element SZK WOT, przeznaczony do prowadzenia rozpoznania i oceny poziomu zagrożenia w danym województwie w związku z wystąpieniem lub prawdopodobieństwem zaistnienia sytuacji kryzysowej oraz określenia potrzeby użycia sił i środków z zasobów resortu obrony narodowej do wsparcia organów administracji publicznej – definicja DWOT. Zob. także: B. Składanek, *Rola Wojsk Obrony Terytorialnej w systemie zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego" 2021, z. 20, s. 18. http://dx.doi.org/10.37055/sbn/146280.

[38] Nieetatowy podmiot wykonawczy dowódcy brygady stanowiący element SZK WOT, przeznaczony do świadczenia doradztwa i udzielania pomocy w zakresie przywracania niezbędnych warunków funkcjonowania poszkodowanej ludności oraz infrastruktury po wystąpieniu sytuacji kryzysowej (katastrofy naturalnej lub cywilizacyjnej) w danym województwie oraz oceny możliwości wsparcia organów administracji publicznej przez wydzielone siły i środki z zasobów resortu obrony narodowej po zakończeniu działania WZZ – definicja DWOT. Zob. także: B. Składanek, *Rola Wojsk Obrony Terytorialnej*…, s. 18.

ZRK brygady[39], ZKDK batalionu lekkiej piechoty[40]. Doradzają one organom administracji publicznej co do możliwości wykorzystania potencjału sił zbrojnych w określonej sytuacji kryzysowej[41].

Sprawność SZK WOT jest uzależniona od sposobu organizacji SZK poszczególnych brygad obrony terytorialnej. Istotę SZK brygady stanowią ESZK, które są istotne z punktu widzenia koordynowania działań przez dowódcę brygady w województwie. Najważniejszym z tych elementów jest ZRK, działający na podstawie opracowanych stałych procedur operacyjnych. Z racji tak skonstruowanego SZK dowódca brygady jako stały przedstawiciel WZZK ma wpływ na kształt wniosku o użycie sił zbrojnych skierowanego do MON. Dodatkowo może na tym etapie wydać wytyczne do przygotowania tych sił oraz zaopiniować bądź zaproponować gotowe rozwiązania do CZK MON (którego funkcję w istocie pełni Taktyczne Centrum Operacyjne DWOT). Skraca to znacznie drogę i czas potrzebny na aktywację pozostałych ESZK, zwłaszcza modułów zadaniowych.

W skład SZK brygady obrony terytorialnej wchodzą oprócz dowódcy brygady m.in.:

- organ dowodzenia dowódcy brygady (oficer dyżurny brygady);
- ZRK brygady;
- organy dowodzenia podległych pododdziałów (ZKDK batalionu lekkiej piechoty), służba dyżurna batalionu;
- moduły zadaniowe – siły i środki planowane i wydzielane do realizacji zadań z zakresu zarządzania kryzysowego, elementy wsparcia dowodzenia i koordynacji działań (ZOW, ZWO)[42].

Szczególnego znaczenia w kontekście przedstawionego skrócenia procedur nabiera procedowanie wniosku przesłanego do MON. Zdarzenie kryzysowe pojawia się nagle. Wymaga szybkich, trafnych decyzji podejmowanych przez odpowiednie organy. Potrzebne są do tego procedury, które w obliczu powagi i rangi sytuacji oraz deficytu czasu pozwalają właściwie realizować ten proces. Rysunek 3 przedstawia

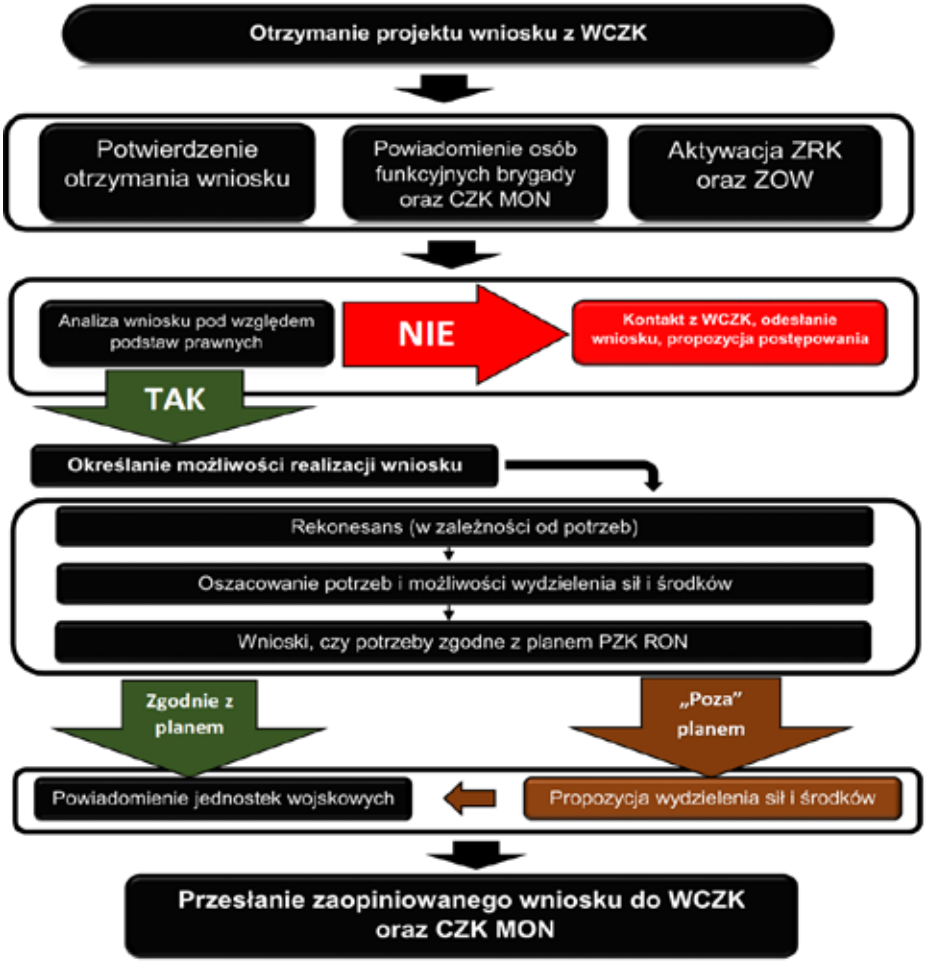
[39] Zorganizowany, przygotowany i rozmieszczony zgodnie z decyzją dowódcy brygady zespół specjalistów zapewniający sprawną realizację zadań we wszystkich fazach procesu zarządzania kryzysowego (zapobiegania, przygotowania, reagowania oraz odbudowy) – definicja DWOT.

[40] Nieetatowy podmiot wykonawczy dowódcy batalionu stanowiący element SZK brygady, przeznaczony do planowania i koordynacji działań kryzysowych a także monitorowania sytuacji w Stałym Rejonie Odpowiedzialności, utrzymywania kontaktu i wymiany informacji z powiatowymi i gminnymi ogniwami zarządzania kryzysowego oraz ZRK brygady – definicja DWOT.

[41] T. Smal, R. Balcerzyk, *System zarządzania kryzysowego w kontekście wykorzystania podmiotów militarnych,* „Zeszyty Naukowe Politechniki Śląskiej" 2017, nr 114, s. 445–446.

[42] Na podstawie SZK 3 Podkarpackiej Brygady Obrony Terytorialnej (materiały własne autora).

jedną z takich obowiązujących procedur opartych na realizacji określonych czynności w określonej kolejności na podstawie dokumentów normatywnych[43].



Rysunek 3. Procedowanie wniosku o wsparcie sił zbrojnych.

Źródło: opracowanie własne na podstawie SZK 3 Podkarpackiej Brygady Obrony Terytorialnej.

Istotnym elementem we wskazanym postępowaniu jest analiza pod względem formalnoprawnym wniosku o wsparcie sił zbrojnych, aby uniknąć błędów mogących prowadzić do jego odrzucenia. Tym bardziej osoby funkcyjne w brygadzie

[43] Tamże.

muszą dysponować niezbędną wiedzą z zakresu prawodawstwa obejmującego użycie sił zbrojnych w tym zakresie. Mowa tutaj nie tylko o u.z.k., lecz także o innych regulacjach prawnych przewidujących możliwość wsparcia różnych podmiotów przez siły zbrojne.

Zespół reagowania kryzysowego jako najważniejszy element systemu zarządzania kryzysowego brygady

Organizację kierowania i współdziałania poszczególnych elementów oparto na wszechstronnej, zarówno poziomej, jak i pionowej wymianie informacji między podmiotami wojskowymi oraz podmiotami administracji cywilnej.

Kluczowym elementem SZK brygady jest ZRK, którego najważniejsze zadania to współdziałanie z WCZK, kierowanie wydzielonymi siłami i środkami resortu obrony narodowej przewidzianymi do realizacji zadań z zakresu zarządzania kryzysowego oraz koordynowanie działań[44]. Element ten wymaga zatem odpowiedniej struktury, opierającej się na stałych komponentach: kierownictwo, grupa planowania, grupa monitorowania, analizy i oceny ryzyka, oraz na elementach tworzonych doraźnie (według potrzeb), tj.: specjalistów dowództwa, obsługi kancelaryjnej, koordynatora przestrzeni powietrznej, grupy dowodzenia i koordynacji działań oraz grupy wsparcia działań. Zespół wykonuje określone czynności zarówno w czasie pokojowego funkcjonowania[45], jak i w czasie kryzysu (aktywacja sił i środków)[46]. Istotą działania ZRK jest zapewnienie sprawnego, zorganizowanego i terminowego wydzielenia sił i środków w sytuacji kryzysowej oraz dowodzenia nimi podczas wykonywania zadań. Tym procesem kieruje (do czasu rozwinięcia ZRK w przypadku wystąpienia sytuacji kryzysowej) w początkowym okresie służba dyżurna brygady,

[44] Przyjęte rozwiązania organizacji SZK na szczeblu lokalnym sprawdziły się m.in. podczas powodzi błyskawicznej w Pawłosiowie w powiecie jarosławskim na Podkarpaciu. 18 kwietnia 2025 r. przez teren województwa podkarpackiego przeszła gwałtowna burza. W ciągu 20 minut intensywne opady deszczu z gradem spowodowały lawinę błotną, która zalała ponad 150 posesji w tej miejscowości. Przez całe popołudnie i noc strażacy wspólnie z innymi służbami, m.in. żołnierzami WOT, usuwali skutki kataklizmu. Tak szybka reakcja żołnierzy WOT była możliwa właśnie dzięki realizacji określonego sposobu (procedur) postępowania, pomimo że do zdarzenia doszło w Wielki Piątek w godzinach popołudniowych. Zob. *Powódź w Pawłosiowie*, Jednostki Państwowej Straży Pożarnej – Komenda Powiatowa Państwowej Straży Pożarnej w Jarosławiu, 20 IV 2025 r., https://www.gov.pl/web/kppsp-jaroslaw/powodz-w-pawlosiowie [dostęp: 9 VI 2026].

[45] Przez „pokojowe funkcjonowanie" rozumie się planową codzienną działalność prowadzoną przez jednostkę wojskową, w której nie zachodzi potrzeba aktywacji ESZK.

[46] Przez „kryzys" rozumie się sytuację, w której zachodzi konieczność aktywacji ESZK oraz wydzielenia sił i środków do wsparcia administracji publicznej do realizacji zadań z zakresu reagowania kryzysowego.

a następnie dowódca brygady poprzez ZRK. Zespół realizuje zadania od momentu wpłynięcia rozkazu/sygnału nakazującego jego aktywację do momentu zakończenia działań.

Do podstawowych zadań ZRK w czasie pokojowego funkcjonowania należy monitorowanie oraz analizowanie możliwości wystąpienia w województwie zagrożeń o charakterze kryzysowym oraz utrzymywanie współpracy z Wojewódzkim Wydziałem Bezpieczeństwa i Zarządzania Kryzysowego. Przepływ informacji pomiędzy WCZK a służbą dyżurną brygady jest realizowany przez systemy teleinformatyczne na zasadach określonych regulaminem ogólnym[47]. W czasie kryzysu główne zadanie ZRK to kierowanie podległymi siłami i środkami celem przeciwdziałania sytuacji kryzysowej oraz koordynacja działań we współdziałaniu z przedstawicielami WCZK.

Realizacja wskazanych zadań będzie możliwa tylko wówczas, gdy osoby funkcyjne wchodzące w skład ZRK będą odpowiednio przygotowane, będą miały niezbędną wiedzę i doświadczenie w działaniach z zakresu zarządzania kryzysowego. Czy jest to możliwe w obecnych uwarunkowaniach strukturalnych brygad obrony terytorialnej? Realizacja dotychczasowych zadań przez WOT w różnych sytuacjach kryzysowych prowadzi do wniosku, że tak. Można zadać jednak pytania, czy te zadania są realizowane na najwyższym poziomie, czy można robić to lepiej, efektywniej. W opinii autora jak najbardziej. Na uwagę zasługuje, z reguły pomijana w różnego rodzaju analizach działań WOT w sytuacjach kryzysowych, realizacja zadań we wszystkich fazach zarządzania kryzysowego, tj. zapobiegania, przygotowania, reagowania oraz odbudowy. W większości przypadków analizie poddaje się jedynie dwie ostatnie fazy. Są one najbardziej charakterystyczne z punktu widzenia efektów użycia sił i środków w reagowaniu kryzysowym. Nie należy jednak zapominać o zapobieganiu i przygotowaniu. Reagowanie natomiast to skutek często złej, niepełnej, błędnej realizacji zadań w ramach faz przygotowania i zapobiegania, wymagające tworzenia procedur ad hoc i podejmowania działań bez przygotowania[48].

Obowiązki dowódców brygad

Na dowódców brygad zostały nałożone obowiązki w każdej fazie reagowania kryzysowego[49]. Umowny podział czterech faz na dwie grupy wynika z charakteru zadań. Można założyć, że pierwsze dwie fazy są typowym elementem przygotowawczym, w ramach

[47] *Zarządzenie Nr 7/MON Ministra Obrony Narodowej z dnia 28 kwietnia 2023 r. w sprawie wprowadzenia do użytku „Regulaminu ogólnego żołnierza Wojska Polskiego"*.

[48] T. Wierzbica, *System zarządzania kryzysowego na szczeblu gminy*, https://gdansk.frdl.pl/static/upload/store/frdl/ANALIZY_CELOWE/ANALIZA_CELowa_System-zarzadzania-kryzysowego.pdf, s. 14–17 [dostęp: 19 III 2026].

[49] Plan użycia Wojsk Obrony Terytorialnej w sytuacjach kryzysowych (dokument wewnętrzny).

którego monitoruje się zagrożenia, planuje się stosowne siły i środki do ewentualnej neutralizacji tych zagrożeń, tworzy się procedury postępowania na wypadek zaistnienia sytuacji kryzysowej oraz prowadzi się szkolenia dla wszystkich podmiotów zaangażowanych w zarządzanie kryzysowe. Fazy reagowania i odbudowy są wymiernym, realnym działaniem w terenie w celu niedopuszczenia do eskalacji zagrożenia, minimalizowania i usuwania jego skutków. Zadania dowódcy brygady w tych fazach koncentrują się na:

- organizacji rozpoznania rejonów objętych sytuacją kryzysową oraz ocenie poziomu zagrożenia przez skierowanie w rejon ZOW;
- rozwinięciu niezbędnych ESZK i osiągnięciu pełnej gotowości wydzielonych sił i środków do udziału w zapobieganiu skutkom kryzysu lub ich usuwaniu;
- dowodzeniu WZZ (przyjętymi w podporządkowanie siłami i środkami resortu obrony narodowej, wydzielonymi do realizacji zadań z zakresu zarządzania kryzysowego);
- analizie i szacowaniu kosztów oraz strat poniesionych podczas działania podległych jednostek wojskowych wydzielonych do działania w sytuacji kryzysowej;
- współdziałaniu z władzami samorządowymi w zakresie doradztwa i oceny możliwości wsparcia usuwania skutków kataklizmów, po zakończeniu realizacji zadań WZZ, poprzez ZWO;
- analizie i ocenie podjętych działań; aktualizacji w razie potrzeby planów użycia podległych sił i środków w sytuacjach kryzysowych.

Te zadania dowódca brygady realizuje w większości przez powołany przez siebie ZRK. Zatem w jego skład powinni wchodzić specjaliści, niewykonujący na co dzień innych obowiązków służbowych[50].

Funkcjonującą obecnie „nieetatową" strukturę (komórka funkcjonalna) na szczeblu brygady w postaci ZRK należy traktować jako rozwiązanie doraźne, przejściowe. Docelowo powinna zostać utworzona „etatowa" komórka zdolna do realizacji zadań we wszystkich fazach zarządzania kryzysowego.

Podsumowanie

Przeprowadzona analiza potwierdziła przyjętą hipotezę badawczą. Wojska Obrony Terytorialnej odgrywają istotną rolę w SZK, ale regulacje prawne ograniczają możliwość pełnego wykorzystania ich potencjału. Obowiązujące przepisy odnoszące się do kwestii użycia sił zbrojnych, w tym WOT, do realizacji zadań wsparcia podsystemu niemilitarnego wymagają gruntownej analizy i zmian pozwalających na optymalne i efektywne wykorzystywanie potencjału tych wojsk.

[50] J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego*…, s. 151.

Zdaniem autora należy rozszerzyć katalog zadań możliwych do realizacji przez nie oraz uprawnień dowódców brygad do decydowania o użyciu podległych sił i środków. Dzięki temu struktura organizacyjna formacji, powszechność oraz jej możliwości będą podstawą do traktowania jej jako komponentu terytorialnego obok wojsk operacyjnych. Decyzje dowódców brygad byłyby podejmowane wyłącznie na wniosek wojewody i dotyczyłyby tylko realizacji zadań na terenie określonego województwa (stałego rejonu odpowiedzialności brygady) zgodnie z zatwierdzonym przez ministra obrony narodowej resortowym planem zarządzania kryzysowego. Nie istniałoby wówczas ryzyko rozproszenia kompetencji. Wręcz przeciwnie, tę sytuację należy postrzegać jako powierzenie dodatkowych uprawnień dowódcom brygad odpowiedzialnym za militarny element zarządzania kryzysowego w województwie, zwłaszcza że niejako pełnią oni funkcję terytorialnych organów dowodzenia stanowiących podstawowy element obrony terytorialnej[51]. Możliwość samodzielnego wydzielania sił przez dowódców brygad obrony terytorialnej nie stoi również w sprzeczności z konstytucyjnymi zasadami zachowania neutralności w sprawach politycznych oraz podlegania cywilnej i demokratycznej kontroli nad siłami zbrojnymi. Nie zostałyby bowiem w żaden sposób naruszone zasady cywilnej kontroli nad nimi[52], a jednocześnie dowódcom wojskowym pozostawiony byłby obszar *military command*, który oznacza dowodzenie, kierowanie podległymi pododdziałami w realizacji celów i zadań wytyczonych przez władze polityczne państwa przy wykorzystaniu dostępnych sił i środków[53].

WOT wielokrotnie udowodniły swoją przydatność w realizacji zadań z zakresu zarządzania kryzysowego. Wystarczy wspomnieć ich zaangażowanie i udział w operacjach takich jak: „Odporna wiosna"[54], „Niezawodna pomoc"[55] czy

[51] R. Jakubczak, *Strategiczna refleksja nad wojskami obrony terytorialnej*, „Kwartalnik Bellona", t. 687, nr 4, s. 21–41.

[52] A. Fałkowski, *Gen. Fałkowski: jakie zasady demokratycznej kontroli nad wojskiem*, Defence24, 12 X 2023 r., https://defence24.pl/polityka-obronna/gen-falkowski-jakie-zasady-demokratycznej-kontroli-nad-wojskiem [dostęp: 8 VI 2026].

[53] Z. Trejnis, *Meandry w kwestii cywilnej kontroli nad Siłami Zbrojnymi w RP po 1989 roku*, „Studia Orientalne" 2022, t. 24, nr 4, s. 11. https://doi.org/10.15804/so2022401.

[54] Operacja zorganizowana w związku z pandemią COVID-19, która pojawiła się w Polsce na początku marca 2020 r. WOT zostały zaangażowane w działania przeciwkryzysowe od 6 marca 2020 r. Działania były prowadzone w ramach operacji „Odporna wiosna" (od czerwca 2020 r. została przekształcona w „Trwałą odporność") w siedmiu głównych obszarach, m.in.: wsparcie szpitali i służb sanitarnych, budowa odporności indywidualnej i społecznej oraz wsparcie: samorządów, Agencji Rezerw Materiałowych, Policji, Straży Granicznej czy Urzędu Lotnictwa Cywilnego. Zob. *Podsumowanie operacji „Odporna Wiosna"*, Wojska Obrony Terytorialnej, 2 VI 2020 r., https://media.terytorialsi.wp.mil.pl/informacje/520508/podsumowanie-operacji-odporna-wiosna [dostęp: 14 III 2025].

[55] Operacja dotycząca migracji ludności z Ukrainy objętej rosyjską agresją. W jej ramach były

„Feniks"[56]. Ponadto według badań CBOS 94% Polaków pozytywnie oceniło w 2024 r. działania podejmowane w czasie powodzi przez służby, takie jak Straż Pożarna czy WOT (w tym 71% oceniło te działania zdecydowanie dobrze)[57]. Właściwe prowadzenie tych działań było możliwe dzięki usprawnieniu działania SZK w zakresie umożliwiającym szybsze i sprawniejsze wydzielanie wojska do realizacji zadań z zakresu zarządzania kryzysowego. Inicjatywa własna pozwoliła na utworzenie ESZK, takich jak ZRK, ZOW czy ZKDK, ściśle współpracujących z organami administracji terenowej (państwowej i samorządowej). Utrzymywanie stałego kontaktu i wymiana informacji pomiędzy WCZK a brygadami obrony terytorialnej, jak również na niższych szczeblach organizacyjnych (powiat – batalion, gmina – kompania), pozwala na efektywne i szybkie generowanie potrzeb w zakresie użycia sił zbrojnych do wsparcia działań kryzysowych.

Wbrew powszechnym oczekiwaniom, przekonaniom oraz potrzebom w polskim prawodawstwie brakuje zapisów pozwalających na niemal natychmiastowe wsparcie lokalnych społeczności w sytuacjach kryzysowych. Potraktowanie WOT w regulacjach prawnych w taki sam sposób jak pozostałe rodzaje sił zbrojnych nie pozwala na ich optymalne wykorzystanie w ramach zarządzania kryzysowego. Aby to zmienić, można zrealizować następujące propozycje:

1. Nowelizacja u.z.k. w zakresie:
   - możliwości wydzielania i kierowania przez dowódców brygad obrony terytorialnej podległych sił i środków do realizacji zadań z zakresu zarządzania kryzysowego,
   - rozszerzenia katalogu zadań wymienionego w art. 25 ust. 3 u.z.k.,
   - zmiany definicji sytuacji kryzysowej, aby nie była bezpośrednio powiązana z dostępnymi możliwościami reakcji lub przeciwdziałania. Przy takim założeniu autor proponuje następującą definicję: „sytuacja wpływająca lub mogąca negatywnie wpłynąć na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wymagająca

realizowane zadania związane ze wsparciem wojewodów, samorządów i instytucji, odpowiedzialnych za organizację pomocy uchodźcom (głównie relokacja i zakwaterowanie). Zob. *Decyzja Nr 82/DWOT MON z dnia 18 marca 2022 r. w sprawie wsparcia wojewodów w związku z podejmowanymi działaniami wobec uchodźców z Ukrainy w ramach operacji pk. „NIEZAWODNA POMOC"*.

[56] Wieloetapowa i wielomiesięczna operacja związana z naprawianiem skutków powodzi i podtopień na całym obszarze objętym klęską żywiołową. Operacja miała na celu odbudowę zniszczonych miejsc. Zob. *Rusza operacja Feniks – Wojsko Polskie wspiera odbudowę terenów dotkniętych powodzią*, Serwis Rzeczypospolitej Polskiej – Ministerstwo Obrony Narodowej, 23 IX 2024 r., https://www.gov.pl/web/obrona-narodowa/rusza-operacja-feniks-wojsko-polskie-wspieraiodbudowe-terenow-dotkniętych-powodzia [dostęp: 14 III 2025].

[57] *Wielka powódź – jej zasięg oraz oceny działań ratunkowych*, „CBOS Flash" 2024, nr 40, s. 2.

stosownego (kryzysowego) działania właściwych organów administracji publicznej ze względu na konieczność użycia i koordynacji ponadstandardowych sił i środków".

2. Zmiana struktur brygad obrony terytorialnej polegająca na wprowadzeniu etatowych ZRK.
3. Rezygnacja z dualizmu w dowodzeniu. Obecnie za zarządzanie kryzysowe odpowiedzialny jest zarówno dowódca WOT, jak i dowódca operacyjny Rodzajów Sił Zbrojnych RP, stosownie do przysługujących uprawnień, które wynikają nie tylko z decyzji ministra obrony narodowej[58], lecz także z dotyczących tego regulacji prawnych. Optymalnym rozwiązaniem wydaje się powierzenie całości zadań z zakresu zarządzania kryzysowego jednej osobie[59].
4. Zmiana procedur w zakresie użycia sił zbrojnych do realizacji zadań z zakresu zarządzania kryzysowego, polegająca na uzyskaniu przez WOT pewnej autonomii w zakresie wsparcia lokalnych społeczności na podstawie następujących założeń:
   – zasady postępowania obowiązują w czasie zarówno pokoju, jak i wojny (w razie konieczności wsparcia obrony cywilnej siłami zbrojnymi);
   – podział wsparcia sił zbrojnych na te realizowane przez komponent operacyjny i te realizowane przez komponent terytorialny;
   – potraktowanie WOT jako elementu zarządzania kryzysowego, którym dysponuje wojewoda na terenie województwa.

Interesującą propozycję przedstawiają Janusz Leżoń i Julian Traciak[60]. Obejmuje ona konkretne zmiany legislacyjne, mające na celu przede wszystkim rozszerzenie uprawnień dowódców brygad obrony terytorialnej, uproszczenie i modyfikację istniejących procedur uruchamiania sił i środków do realizacji zadań z zakresu zarządzania kryzysowego, co zwiększy rolę WOT w SZK.

Wskazane działania wydają się koniecznością. Paradoksem jest to, że brygady obrony terytorialnej przeznaczone doktrynalnie do realizacji zadań w swoich stałych rejonach odpowiedzialności są właściwie pozbawione takiej możliwości w sytuacji kryzysowej. Decyzje o ich użyciu do wsparcia lokalnych społeczności zapadają bowiem na szczeblu ministerialnym (centralnym). Jest to poniekąd sprzeczne z istotą funkcjonowania obrony terytorialnej.

---

[58] *Decyzja nr Z-4/MON Ministra Obrony Narodowej z dnia 6 maja 2022 r. w sprawie Systemu Zarządzania Kryzysowego resortu obrony narodowej*.

[59] Przy założeniu, że w systemie zarządzania kryzysowego WOT będą traktowane na odrębnych zasadach od wojsk operacyjnych, rodzi się uzasadniona wątpliwość, a zarazem pole do dyskusji będącej odpowiedzią na pytanie: kto powinien pełnić funkcję CZK MON przy jednoczesnym założeniu realizacji tego zadania w okresie pokoju, kryzysu oraz wojny?

[60] J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego*…, s. 149–155.

Bibliografia

Bieńkowska A., Kral Z., Zabłocka-Kluczka A., *Istota i ewolucja zarządzania kryzysowego*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2005, nr 1092, s. 25–32.

Chudoba M., *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej,* „Studia Bezpieczeństwa Narodowego" 2023, z. 29, nr 3, s. 121–140. https://doi.org/10.37055/sbn/173489.

Czuryk M., *Status prawny samorządu terytorialnego w sferze zarządzania kryzysowego*, „Cybersecurity and Law" 2024, t. 12, nr 2, s. 174–186. http://dx.doi.org/10.35467/cal/188567.

Gikiewicz M., *Współczesny wymiar ochrony ludności i obrony cywilnej*, t. 1: *Wybrane państwa basenu Morza Bałtyckiego*, Warszawa 2026.

Goleński W., Zimny D., *Przygotowanie państwa na zagrożenia hybrydowe*, „Kontrola Państwowa" 2024, nr 5, s. 18–37.

Gromek P., *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne*, „Zeszyty Naukowe SGSP" 2017, t. 63, nr 3, s. 21–33.

Grzela J., *Obrona terytorialna w państwach nordyckich*, „Bezpieczeństwo, Teoria i Praktyka" 2017, t. 28, nr 3, s. 207–223.

Jakubczak R., *Strategiczna refleksja nad wojskami obrony terytorialnej*, „Kwartalnik Bellona" 2016, t. 687, nr 4, s. 21–41.

Jakubczak R., *Wybrane kwestie teorii Obrony Terytorialnej*, w: *Bezpieczeństwo, zarządzanie, medycyna i kultura fizyczna. Wybrane zagadnienia*, t. 4, J. Telak, D. Skalski, E. Zieliński, D. Czarnecki (red.), Gdańsk 2020, s. 15–35.

Jakubiak E., *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie*, „Studia Bezpieczeństwa Narodowego" 2022, t. 24, nr 2, s. 71–82. https://doi.org/10.37055/sbn/151015.

Kalinowska E., *Analiza treści jako technika badawcza*, „Dyskursy Młodych Andragogów / Adult Education Discourses" 2001, nr 2, s. 15–31. https://doi.org/10.34768/dma.vi02.286.

Klisz M., *Utworzenie Wojsk Obrony Terytorialnej jako odpowiedź na nowe zagrożenia bezpieczeństwa państwa*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3, s. 63–78.

Kociubiński K., Shadurski V., *Zagrożenia hybrydowe dla bezpieczeństwa Polski ze strony Białorusi po 2020 r.*, „Wschodnioznawstwo" 2024, t. 18, s. 231–253. https://doi.org/10.4467/20827695WSC.24.015.20630.

Kupryjańczyk M., Lech K., Derkacz Ł., *Rola ratownictwa medycznego w systemie zarządzania kryzysowego na przykładzie powodzi w powiecie nyskim w 2024 roku*, „Kwartalnik Bellona" 2024, t. 723, nr 4, s. 201–215. https://doi.org/10.5604/01.3001.0055.5824.

Leżoń J., Bojarczuk M., Traciak J., *Znaczenie działań niekinetycznych w nowoczesnych siłach zbrojnych*, „Polityka i Społeczeństwo" 2025, t. 23, nr 1, s. 174–190. https://doi.org/10.15584/polispol.2025.1.10.

Leżoń J., Traciak J., *W kierunku efektywnego zarządzania kryzysowego*, „Kwartalnik Bellona" 2026, t. 724, nr 1, s. 145–157. https://doi.org/10.5604/01.3001.0055.6961.

Leżoń J., Traciak J., Zaguła J., *Wojska Obrony Terytorialnej rodzajem Sił Zbrojnych – teoria czy rzeczywistość?*, „Kwartalnik Bellona" 2025, t. 722, nr 3, s. 71–88. http://dx.doi.org/10.5604/01.3001.0055.4501.

Małysa T., *Wojska obrony terytorialnej w państwach bałtyckich*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 3, s. 225–236.

Polcikiewicz Z., *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski*, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2016, t. 7, nr 1, s. 399–413.

Składanek B., *Rola Wojsk Obrony Terytorialnej w systemie zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego" 2021, z. 20, s. 11–20. http://dx.doi.org/10.37055/sbn/146280.

Skomra W., Wojtasik K., *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK*, „Terroryzm – studia, analizy, prewencja" 2025, wydanie specjalne: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, s. 13–34. https://doi.org/10.4467/27204383TER.25.001.21504.

Smal T., Balcerzyk R., *System zarządzania kryzysowego w kontekście wykorzystania podmiotów militarnych*, „Zeszyty Naukowe Politechniki Śląskiej" 2017, z. 114, s. 443–454.

Smoleński S., *Procedury zarządzania kryzysowego*, „Zeszyty Naukowe SGSP" 2022, nr 84, s. 149–160. http://dx.doi.org/10.5604/01.3001.0016.1807.

Staśkiewicz U., *Kaitseliit – estońska organizacja cywilna działająca na rzecz obronności państwa i bezpieczeństwa ludności*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, t. 69, nr 1, s. 16–25. https://doi.org/10.52097/eppism.8882.

Stelmach T., *Reorganizacja systemu zarządzania kryzysowego resortu obrony narodowej*, „Problemy Techniki Uzbrojenia" 2023, t. 163, nr 1, s. 39–55. https://doi.org/10.5604/01.3001.0053.5917.

Szmitkowski P., *Plany zarządzania kryzysowego w świetle nowych regulacji prawnych*, „Doctrina. Studia Społeczno-Polityczne" 2016, t. 13, nr 13, s. 209–220.

Śliwa Z., Olech A.K., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, „Wiedza Obronna" 2022, t. 278, nr 1, s. 89–107. https://doi.org/10.34752/2022-d278.

Trejnis Z., *Meandry w kwestii cywilnej kontroli nad Siłami Zbrojnymi w RP po 1989 roku*, „Studia Orientalne" 2022, t. 24, nr 4, s. 9–39. https://doi.org/10.15804/so2022401.

Trocha J., *Norweski system bezpieczeństwa cywilnego a uwarunkowania zagrożeń kryzysowych i wojennych kraju*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2017, t. 22, nr 2, s. 230–246.

Walczak W., *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej*, „Przedsiębiorczość i Zarządzanie" 2009, t. 10, nr 8, s. 98–101.

Wielka powódź – jej zasięg oraz oceny działań ratunkowych, „CBOS Flash" 2024, nr 40.

Wróbel I., *Perspektywy współdziałania wojsk obrony terytorialnej z administracją publiczną w zwalczaniu klęsk żywiołowych*, „Bezpieczeństwo. Teoria i Praktyka" 2017, t. 28, nr 3, s. 131–150.

Wywiał P., *Działania przeciwdywersyjne wojsk obrony terytorialnej w kontekście rosyjskiej dywersji na Ukrainie*, w: *Bezpieczeństwo Polski w warunkach członkostwa w Unii Europejskiej*, A. Żebrowski, Ł. Zweiffel, K. Kowalska (red. nauk.), Kraków 2018, s. 284–297.

Zaręba A., *Dezinformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cyberseciurity)*, „Cybersecurity and Law" 2025, t. 13, nr 1, s. 95–107.

Żukowski P., *Rola Terytorialnej Służby Wojskowej w systemie bezpieczeństwa militarnego Rzeczypospolitej Polskiej*, „Studia Bezpieczeństwa Narodowego" 2020, t. 17, nr 1, s. 157–166. https://doi.org/10.37055/sbn/144285.

Źródła internetowe

Fałkowski A., *Gen. Fałkowski: jakie zasady demokratycznej kontroli nad wojskiem*, Defence24, 12 X 2023 r., https://defence24.pl/polityka-obronna/gen-falkowski-jakie-zasady-demokratycznej-kontroli-nad-wojskiem [dostęp: 8 VI 2026].

Każda gmina musi mieć swój plan zarządzania kryzysowego. Nie może być kopiuj-wklej, Portal Samorządowy, 20 IX 2024 r., https://www.portalsamorzadowy.pl/zmiany-w-prawie/kazda-gmina-musi-miec-swoj-plan-zarzadzania-kryzysowego-nie-moze-byc-kopiuj-wklej,570960.html [dostęp: 12 III 2026].

Marczak J., Jakubczak R., *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP*, https://www.researchgate.net/publication/337929735_Raport_strategiczny_Sily_Zbrojne_RP_w_drugiej_dekadzie_XXI_wieku_Koncepcja_strategiczna_Obrony_Terytorialnej_RP [dostęp: 8 VI 2026].

Podsumowanie operacji „Odporna Wiosna", Wojska Obrony Terytorialnej, 2 VI 2020 r., https://media.terytorialsi.wp.mil.pl/informacje/520508/podsumowanie-operacji-odporna-wiosna [dostęp: 14 III 2025].

Powódź na południu Polski. Ewakuacje mieszkańców, lista miejscowości, TVN24, 15 IX 2024 r., https://tvn24.pl/najnowsze/powodz-na-poludniu-polski-ewakuacje-mieszkancow-lista-miejscowosci-st8087871 [dostęp: 8 VI 2026].

Powódź w Pawłosiowie, Jednostki Państwowej Straży Pożarnej – Komenda Powiatowa Państwowej Straży Pożarnej w Jarosławiu, 20 IV 2025 r., https://www.gov.pl/web/kppsp-jaroslaw/powodz-w-pawlosiowie [dostęp: 9 VI 2026].

Rusza operacja Feniks – Wojsko Polskie wspiera odbudowę terenów dotkniętych powodzią, Serwis Rzeczypospolitej Polskiej – Ministerstwo Obrony Narodowej, 23 IX 2024 r., https://www.gov.pl/web/obrona-narodowa/rusza-operacja-feniks-wojsko-polskie-wspieraiodbudowe-terenow-dotkniętych-powodzia [dostęp: 14 III 2025].

Wierzbica T., *System zarządzania kryzysowego na szczeblu gminy*, https://gdansk.frdl.pl/static/upload/store/frdl/ANALIZY_CELOWE/ANALIZA_CELowa_System-zarzadzania-kryzysowego.pdf [dostęp: 19 III 2026].

Akty prawne

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

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (DzU z 2024 r. poz. 1907, ze zm.).

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

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2025 r. poz. 194, ze zm.).

Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (t.j. DzU z 2025 r. poz. 1675, ze zm.).

Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (t.j. DzU z 2024 r. poz. 597, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2026 r. poz. 574, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. DzU z 2026 r. poz. 157).

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, ze zm.).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. DzU z 2025 r. poz. 112).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (t.j. DzU z 2026 r. poz. 720).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. DzU z 2025 r. poz. 1684, ze zm.).

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. DzU z 2025 r. poz. 532, ze zm.).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j. DzU z 2026 r. poz. 367, ze zm.).

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

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. DzU z 2026 r. poz. 662, ze zm.).

Rozporządzenie Rady Ministrów z dnia 18 marca 2025 roku w sprawie gotowości obronnej państwa (DzU z 2025 r. poz. 355).

Rozporządzenie Rady Ministrów z dnia 31 sierpnia 2023 r. w sprawie współdziałania Straży Granicznej oraz oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej (DzU z 2023 r. poz. 1767).

Rozporządzenie Rady Ministrów z dnia 20 lutego 2023 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu (DzU z 2023 r. nr 41 poz. 347).

Rozporządzenie Rady Ministrów z dnia 21 kwietnia 2022 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej ochrony (DzU z 2022 r. poz. 880).

Rozporządzenie Rady Ministrów z dnia 21 lipca 2016 r. w sprawie użycia oddziałów i pododdziałów policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego (DzU z 2016 r. poz. 1090).

Rozporządzenie Rady Ministrów z dnia 21 lipca 2016 r. w sprawie szczegółowych warunków i sposobu organizacji współdziałania oddziałów i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych Rzeczypospolitej Polskiej w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego (DzU z 2016 r. poz. 1087).

Rozporządzenie Rady Ministrów z dnia 20 grudnia 2013 r. w sprawie szczegółowych zasad użycia oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej w czasie stanu wyjątkowego (DzU z 2013 r. poz. 1733).

Zarządzenie nr 7/MON Ministra Obrony Narodowej z dnia 28 kwietnia 2023 r. w sprawie wprowadzenia do użytku „Regulaminu ogólnego żołnierza Wojska Polskiego" (Dz. Urz. MON z 2023 r. poz. 49).

Decyzja nr Z-4/MON Ministra Obrony Narodowej z dnia 6 maja 2022 r. w sprawie Systemu Zarządzania Kryzysowego resortu obrony narodowej.

Decyzja Nr 82/DWOT MON z dnia 18 marca 2022 r. w sprawie wsparcia wojewodów w związku z podejmowanymi działaniami wobec uchodźców z Ukrainy w ramach operacji pk. „NIEZAWODNA POMOC".

Inne dokumenty

Plan użycia Wojsk Obrony Terytorialnej w sytuacjach kryzysowych (dokument wewnętrzny).

SZK 3 Podkarpackiej Brygady Obrony Terytorialnej.

Wojska Obrony Terytorialnej w operacji, DD-3.40, Warszawa 2018.

Ppłk Janusz Leżoń

Zastępca dowódcy 3 Podkarpackiej Brygady Obrony Terytorialnej oraz absolwent Wyższej Szkoły Oficerskiej im. Stefana Czarnieckiego w Poznaniu. Specjalizuje się w zagadnieniach związanych z Wojskami Obrony Terytorialnej, w szczególności obszarem zarządzania kryzysowego oraz prowadzeniem działań niekinetycznych.

Kontakt: agajanuszlezon@interia.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 71–90
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.023.24172

ARTYKUŁ

Bezpieczeństwo wewnętrzne w erze cyfrowej – wyzwania i kierunki rozwoju

Internal security in the digital age – challenges and development areas

MICHAŁ ANTONIUK

Autor niezależny

https://orcid.org/0009-0006-7710-0685

Abstrakt

Celem artykułu jest przedstawienie oraz usystematyzowanie współczesnych kierunków rozwoju bezpieczeństwa wewnętrznego w warunkach postępującej cyfryzacji. Przedmiotem opracowania jest wpływ technologii cyfrowych na specyfikę zagrożeń wewnętrznych oraz funkcjonowanie instytucji odpowiedzialnych za zapewnienie bezpieczeństwa państwa. Artykuł ma charakter przeglądowo-analityczny. W badaniu zastosowano analizę literatury przedmiotu, aktów prawnych i dokumentów strategicznych. Autor porównał rozwiązania dotyczące stosowania technologii cyfrowych w zakresie bezpieczeństwa przyjęte w różnych państwach i organizacjach międzynarodowych. Przeprowadzona analiza wykazała, że rozwój tych technologii prowadzi do zasadniczej transformacji systemów bezpieczeństwa wewnętrznego, wymuszając zmianę modeli zarządzania, rozwój współpracy międzyinstytucjonalnej oraz dostosowanie regulacji prawnych do nowych zagrożeń. We wnioskach autor wskazuje, że skuteczne zapewnienie bezpieczeństwa wewnętrznego w erze cyfrowej wymaga zintegrowanego podejścia łączącego rozwiązania technologiczne, odpowiednie ramy prawne, rozwój kompetencji instytucjonalnych oraz współpracę międzynarodową.

Słowa kluczowe bezpieczeństwo wewnętrzne, cyfryzacja, cyberbezpieczeństwo, zagrożenia cyfrowe, transformacja cyfrowa

Abstract The aim of this article is to present and systematize contemporary directions in the development of internal security in the context of advancing digital transformation. The subject of the study is the impact of digital technologies on the nature of internal threats and on the functioning of institutions responsible for ensuring state security. The article has a review-analytical character. The study employs a review of the relevant literature, an analysis of legal acts and strategic documents. The author compared the solutions for application of digital technologies in the field of security adopted in different countries and international organisations. The conducted analysis demonstrates that the development of these technologies has fundamentally transformed internal security systems, requiring changes in management models, the development of interinstitutional cooperation, and the adaptation of legal frameworks to emerging threats. In the conclusions, the author indicates that effective internal security in the digital age requires an integrated approach combining technological solutions, appropriate legal frameworks, development of institutional capacities, and international cooperation.

Keywords internal security, digitalisation, cybersecurity, digital threats, digital transformation

Wprowadzenie

Bezpieczeństwo wewnętrzne stanowi jeden z filarów funkcjonowania państwa. Obejmuje ono ochronę porządku publicznego, bezpieczeństwa obywateli, infrastruktury krytycznej oraz stabilności instytucji państwowych. Rozwój technologii cyfrowych spowodował zasadniczą zmianę środowiska bezpieczeństwa. Współczesne zagrożenia coraz częściej mają charakter transgraniczny, są realizowane w cyberprzestrzeni i oddziałują jednocześnie na wiele sektorów funkcjonowania państwa[1].

[1] B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, London 1998, s. 21–35; M.D. Cavelty, *Cyber-Security and Threat Politics. US efforts to secure the information age*, London––New York 2009, s. 78–95.

W literaturze przedmiotu podkreśla się, że cyfryzacja nie tylko zwiększa efektywność funkcjonowania administracji publicznej i służb odpowiedzialnych za bezpieczeństwo, lecz także tworzy nowe obszary podatności. Autorzy tacy jak Barry Buzan, Myriam Dunn Cavelty czy Richard Clarke i Robert Knake, wskazują, że bezpieczeństwo wewnętrzne wymaga współcześnie odejścia od wyłącznie terytorialnego sposobu postrzegania zagrożeń na rzecz podejścia uwzględniającego cyberprzestrzeń, odporność infrastruktury krytycznej oraz bezpieczeństwo informacyjne. Z kolei dane z raportów Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (The European Union Agency for Cybersecurity, ENISA) oraz Organizacji Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation and Development, OECD) wskazują, że rosnąca liczba incydentów cybernetycznych wymusza zmianę sposobu organizacji instytucji odpowiedzialnych za bezpieczeństwo oraz rozwój współpracy publiczno-prywatnej[2].

Pytania badawcze niniejszego opracowania to: w jaki sposób postępująca cyfryzacja wpływa na funkcjonowanie systemu bezpieczeństwa wewnętrznego oraz jakie kierunki jego rozwoju wskazują współczesna literatura naukowa i dokumenty strategiczne?

Celem artykułu jest usystematyzowanie aktualnego stanu wiedzy dotyczącego wpływu transformacji cyfrowej na bezpieczeństwo wewnętrzne oraz identyfikacja najważniejszych wyzwań, kierunków rozwoju i rozwiązań z tym związanych, stosowanych w wybranych państwach oraz organizacjach międzynarodowych.

Artykuł ma charakter przeglądowo-analityczny. W badaniu wykorzystano analizę literatury przedmiotu, aktów prawnych i dokumentów strategicznych oraz metodę porównawczą. Zastosowanie tych metod dało możliwość zestawienia poglądów prezentowanych w literaturze, porównania rozwiązań instytucjonalnych i regulacyjnych oraz sformułowanie syntetycznych wniosków dotyczących kierunków rozwoju bezpieczeństwa wewnętrznego w erze cyfrowej.

Przekształcenie pojęcia bezpieczeństwa wewnętrznego w środowisku cyfrowym

Rozwój technologii cyfrowych doprowadził do zasadniczej zmiany sposobu postrzegania bezpieczeństwa wewnętrznego. Pojęcie to, wcześniej utożsamiane przede

[2] Zob. np. *ENISA Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [dostęp: 11 VIII 2026]; OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf?, s. 34–37 [dostęp: 11 VIII 2026].

wszystkim z ochroną porządku publicznego, zwalczaniem przestępczości oraz zapewnieniem stabilności funkcjonowania państwa w granicach jego terytorium, zostało rozszerzone o zwalczanie zagrożeń występujących w cyberprzestrzeni, których charakter wykracza poza klasyczne ujęcie bezpieczeństwa państwa[3].

Barry Buzan, Ole Wæver i Jaap de Wilde wskazują, że bezpieczeństwo należy rozpatrywać wielowymiarowo, obejmując zarówno aspekty militarne, jak i polityczne, gospodarcze, społeczne i technologiczne. W ich ujęciu rozwój technologii informacyjnych zmienia sposób identyfikacji zagrożeń oraz mechanizmy reagowania państwa, prowadząc do rozszerzenia zakresu odpowiedzialności instytucji bezpieczeństwa. Oznacza to, że bezpieczeństwo wewnętrzne powinno obejmować nie tylko ochronę obywateli przed zagrożeniami fizycznymi, lecz także zapewnienie odporności infrastruktury cyfrowej oraz bezpieczeństwa informacji[4].

Podobne stanowisko prezentuje Cavelty, która podkreśla, że cyfryzacja doprowadziła do powstania nowego środowiska bezpieczeństwa, w którym zagrożenia mają charakter dynamiczny, trudny do przewidzenia oraz często transgraniczny. Autorka zwraca uwagę, że cyberprzestrzeń stała się obszarem, w którym działania przestępcze, operacje wywiadowcze oraz kampanie dezinformacyjne mogą być prowadzone równocześnie wobec wielu państw, bez konieczności fizycznej obecności sprawców na ich terytorium. W rezultacie tradycyjne instrumenty ochrony bezpieczeństwa wewnętrznego okazują się niewystarczające, jeżeli nie są uzupełnione rozwiązaniami organizacyjnymi i technologicznymi dostosowanymi do specyfiki środowiska cyfrowego[5].

Znaczenie tej transformacji potwierdza również ENISA. W raporcie tej organizacji za rok 2023 wskazano, że liczba ataków wymierzonych w administrację publiczną, sektor ochrony zdrowia oraz operatorów infrastruktury krytycznej systematycznie rośnie. Jednocześnie zwiększa się stopień złożoności wykorzystywanych metod, obejmujących m.in. ataki ransomware, kampanie phishingowe oraz działania prowadzone przez grupy sponsorowane przez państwa. Oznacza to, że bezpieczeństwo wewnętrzne coraz silniej zależy od zdolności państwa do ochrony infrastruktury cyfrowej oraz szybkiego reagowania na incydenty cybernetyczne[6].

Analiza porównawcza rozwiązań przyjętych w wybranych państwach wskazuje, że proces dostosowania instytucji bezpieczeństwa przebiega w różnym tempie. Państwa członkowskie Unii Europejskiej rozwijają swoje systemy przede

[3] B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework*…, s. 27–29.

[4] Tamże, s. 31–33.

[5] M.D. Cavelty, *Cyber-Security and Threat Politics*…, s. 78–81.

[6] *ENISA Threat Landscape 2023*…, s. 45–46.

wszystkim na podstawie wspólnych regulacji prawnych, takich jak dyrektywa NIS 2[7], oraz współpracę w ramach ENISA.

Z kolei Stany Zjednoczone opierają rozwój cyberbezpieczeństwa na modelu zarządzania ryzykiem opracowanym przez National Institute of Standards and Technology (NIST), w którym szczególną rolę odgrywa współpraca administracji publicznej z sektorem prywatnym[8].

Oba modele zmierzają do zwiększenia odporności państwa, jednak różnią się zakresem centralizacji oraz sposobem podziału odpowiedzialności między instytucje publiczne i podmioty prywatne.

Istotną konsekwencją transformacji cyfrowej jest również zmiana charakteru zagrożeń. Clarke i Knake wskazują, że cyberataki mogą oddziaływać jednocześnie na wiele sektorów państwa i prowadzić do zakłócenia pracy administracji, systemów finansowych, energetyki czy transportu. Nie wymagają przy tym użycia siły militarnej ani fizycznej obecności sprawcy, a ich skutki mogą obejmować zarówno straty ekonomiczne, jak i destabilizację społeczną oraz utratę zaufania obywateli do instytucji publicznych[9].

Przegląd literatury przedmiotu prowadzi do wniosku, że bezpieczeństwo wewnętrzne w erze cyfrowej należy postrzegać przede wszystkim jako zdolność państwa do zapewnienia ciągłości funkcjonowania jego podstawowych struktur, ochrony infrastruktury krytycznej oraz skutecznego reagowania na zagrożenia powstające w cyberprzestrzeni. Oznacza to odejście od modelu skoncentrowanego na reagowaniu na incydenty na rzecz podejścia opartego na budowaniu odporności organizacyjnej, zarządzaniu ryzykiem oraz współpracy krajowej i międzynarodowej[10].

Zagrożenia cyfrowe i ich wpływ na bezpieczeństwo wewnętrzne

Rozwój technologii cyfrowych doprowadził do zmiany charakteru zagrożeń oddziałujących na bezpieczeństwo wewnętrzne państwa. W przeciwieństwie do zagrożeń

---

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

[8] *The NIST Cybersecurity Framework (CSF) 2.0*, February 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, s. 21–23 [dostęp: 17 VIII 2026].

[9] R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010, s. 12–14.

[10] M.D. Cavelty, *Cyber-Security and Threat Politics*…, s. 90–95; OECD, *Digital Security and Resilience*…, s. 34–37.

w wymiarze fizycznym, zagrożenia cyfrowe częściej mają charakter transgraniczny, są trudniejsze do identyfikacji, a ich skutki mogą obejmować jednocześnie wiele sektorów funkcjonowania państwa. Jak zauważa David S. Wall, cyberprzestępczość przestała być zjawiskiem ograniczonym do pojedynczych przestępstw komputerowych. Stała się złożonym systemem działalności przestępczej wykorzystującej globalne sieci teleinformatyczne. Obejmuje zarówno oszustwa finansowe, kradzieże tożsamości, jak i ataki na administrację publiczną, przedsiębiorstwa oraz infrastrukturę krytyczną[11].

Clarke i Knake wskazują, że cyberataki coraz częściej są ukierunkowane nie na pojedyncze systemy informatyczne, lecz na zakłócenie funkcjonowania całych sektorów gospodarki i administracji publicznej. Przykładem są ataki typu ransomware na szpitale, przedsiębiorstwa energetyczne oraz jednostki administracji samorządowej, których skutkiem jest nie tylko utrata danych, lecz także czasowe ograniczenie świadczenia usług publicznych. Autorzy podkreślają, że skuteczność takich działań wynika przede wszystkim z wysokiego stopnia cyfryzacji współczesnych państw oraz zależności między systemami teleinformatycznymi[12].

Odrębną kategorię zagrożeń stanowią kampanie dezinformacyjne prowadzone z wykorzystaniem mediów społecznościowych i platform internetowych. Lucas Kello zwraca uwagę, że współczesne konflikty coraz częściej obejmują działania informacyjne, których celem jest wpływanie na procesy polityczne, osłabianie zaufania obywateli do instytucji publicznych oraz pogłębianie podziałów społecznych. W przeciwieństwie do klasycznych cyberataków działania te nie prowadzą bezpośrednio do zniszczenia infrastruktury, lecz oddziałują na procesy decyzyjne oraz bezpieczeństwo społeczne, co czyni je jednym z najtrudniejszych wyzwań dla współczesnych systemów bezpieczeństwa wewnętrznego[13].

Znaczenie zagrożeń informacyjnych potwierdzają również raporty ENISA oraz OECD. Wynika z nich, że od 2022 r. jest obserwowany wzrost liczby skoordynowanych kampanii dezinformacyjnych towarzyszących konfliktom międzynarodowym oraz procesom wyborczym. Jednocześnie wskazuje się, że skuteczność przeciwdziałania tego rodzaju zagrożeniom zależy od rozwiązań technologicznych, poziomu edukacji społeczeństwa, odporności informacyjnej obywateli oraz sprawnego systemu komunikacji instytucji publicznych[14].

---

[11] D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007, s. 55–57.

[12] R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat*…, s. 24–28.

[13] L. Kello, *The virtual weapon and international order*, New Haven–London 2017, s. 59–62.

[14] *ENISA Threat Landscape 2023*…, s. 27–29; OECD, *Digital Security and Resilience*…, s. 56–58.

Analiza porównawcza doświadczeń państw Unii Europejskiej i Stanów Zjednoczonych wskazuje na odmienne modele reagowania na zagrożenia cyfrowe. W państwach UE położono nacisk na rozwój wspólnych standardów bezpieczeństwa, obowiązki zgłaszania incydentów oraz ochronę infrastruktury krytycznej wynikające z dyrektywy NIS 2. W Stanach Zjednoczonych podstawę stanowi *The NIST Cybersecurity Framework (CSF) 2.0*. Jest to model zarządzania ryzykiem koncentrujący się na identyfikacji zagrożeń, ochronie zasobów, wykrywaniu incydentów, reagowaniu oraz odbudowie zdolności operacyjnych po zakończeniu ataku.

W literaturze zwraca się uwagę również na asymetryczny charakter zagrożeń cyfrowych. Martin Libicki wskazuje, że relatywnie niewielkie grupy przestępcze lub podmioty sponsorowane przez państwa są w stanie osiągać skutki porównywalne z klasycznymi działaniami militarnymi, wykorzystując luki w zabezpieczeniach systemów teleinformatycznych. Oznacza to, że skuteczność działań nie zależy wyłącznie od potencjału ekonomicznego czy militarnego państwa, lecz także od poziomu jego odporności cyfrowej, przygotowania instytucji publicznych oraz jakości współpracy z operatorami infrastruktury krytycznej[15].

Przegląd literatury prowadzi do wniosku, że zagrożenia cyfrowe obejmują cyberprzestępczość, cyberterroryzm, działania hybrydowe, operacje dezinformacyjne oraz ataki na infrastrukturę krytyczną, których wspólną cechą jest możliwość jednoczesnego oddziaływania na bezpieczeństwo państwa, gospodarkę i społeczeństwo. Z tego względu współczesne bezpieczeństwo wewnętrzne powinno być postrzegane jako system zarządzania ryzykiem cyfrowym, który integruje rozwiązania technologiczne, organizacyjne i prawne, a nie jako jedynie działania podejmowane po wystąpieniu incydentu[16].

Stanowiska przedstawione w literaturze wskazują również, że skuteczność ochrony przed zagrożeniami cyfrowymi zależy od zdolności państwa do przewidywania nowych form ryzyka oraz ciągłego doskonalenia procedur bezpieczeństwa. W praktyce oznacza to konieczność regularnej aktualizacji krajowych strategii cyberbezpieczeństwa, rozwoju specjalistycznych kompetencji administracji publicznej oraz pogłębiania współpracy międzynarodowej w zakresie wymiany informacji o zagrożeniach i wspólnego reagowania na incydenty. Analiza porównawcza doświadczeń państw europejskich i Stanów Zjednoczonych potwierdza,

[15] M.C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007, s. 102–118.

[16] D.S. Wall, *Cybercrime: The Transformation of Crime*…, s. 55–70; S.W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012, s. 47–50.

że działania oparte na prewencji, budowaniu odporności oraz współpracy międzyinstytucjonalnej przynoszą lepsze rezultaty niż model koncentrujący się na reagowaniu po wystąpieniu ataku[17].

Wyzwania związane z dostosowaniem instytucjonalnym i zarządzaniem

Postępująca cyfryzacja wymusza zmianę sposobu funkcjonowania instytucji odpowiedzialnych za bezpieczeństwo wewnętrzne. Tradycyjne modele organizacyjne, oparte na hierarchicznym podziale kompetencji oraz reagowaniu na zdarzenia po ich wystąpieniu, okazują się niewystarczające wobec zagrożeń charakteryzujących się dużą dynamiką, transgranicznością i wysokim stopniem złożoności. W literaturze podkreśla się, że skuteczność współczesnego systemu bezpieczeństwa wewnętrznego zależy od dostępnych technologii, ale przede wszystkim od zdolności instytucji do szybkiej adaptacji organizacyjnej oraz efektywnej współpracy międzysektorowej[18].

Cavelty wskazuje, że jednym z najistotniejszych problemów współczesnych systemów bezpieczeństwa jest rozproszenie odpowiedzialności za cyberbezpieczeństwo. W wielu państwach kompetencje dotyczące ochrony infrastruktury krytycznej, przeciwdziałania cyberprzestępczości, ochrony danych osobowych oraz reagowania na incydenty są podzielone między administrację rządową, służby specjalne, organy ścigania i wyspecjalizowane zespoły reagowania na incydenty komputerowe (ang. *computer security incident response team*, CSIRT). Taki model zwiększa ryzyko dublowania zadań, wydłuża proces decyzyjny oraz utrudnia sprawną wymianę informacji[19].

Podobne wnioski przedstawiono w raporcie OECD *Digital Security and Resilience in Critical Infrastructure and Essential Services*. Wskazano w nim, że państwa osiągające najwyższy poziom odporności cyfrowej tworzą zintegrowane systemy zarządzania bezpieczeństwem, w których odpowiedzialność poszczególnych instytucji jest jasno określona, a współpraca między nimi opiera się na wspólnych procedurach oraz regularnej wymianie informacji. Podkreślono również znaczenie strategicznego planowania oraz ciągłego doskonalenia procedur reagowania na incydenty[20].

Przeprowadzona analiza porównawcza pokazuje wyraźne różnice między modelami zarządzania bezpieczeństwem cyfrowym w UE i USA. W państwach

[17] OECD, *Digital Security and Resilience*…, s. 34–37; *The NIST Cybersecurity Framework*…

[18] M.D. Cavelty, *Cyber-Security and Threat Politics*…, s. 78–82; OECD, *Digital Security and Resilience*…, s. 39–42.

[19] M.D. Cavelty, *Cyber-Security and Threat Politics*…, s. 91–95.

[20] OECD, *Digital Security and Resilience*…, s. 55–57.

członkowskich UE rozwój systemów cyberbezpieczeństwa opiera się przede wszystkim na harmonizacji przepisów prawa oraz współpracy prowadzonej w ramach ENISA i realizacji dyrektywy NIS 2. Państwa zobowiązano do wyznaczenia właściwych organów odpowiedzialnych za cyberbezpieczeństwo, utworzenia krajowych zespołów reagowania na incydenty oraz opracowania krajowych strategii bezpieczeństwa cyfrowego[21].

Model amerykański opiera się na zarządzaniu ryzykiem oraz partnerstwie administracji publicznej z sektorem prywatnym. Ramy zarządzania cyberbezpieczeństwem opracowane przez NIST obejmują pięć podstawowych etapów: identyfikację zagrożeń, ochronę zasobów, wykrywanie incydentów, reagowanie oraz odbudowę zdolności operacyjnych. Rozwiązanie to jest szeroko wykorzystywane zarówno przez administrację federalną, jak i przedsiębiorstwa zarządzające infrastrukturą krytyczną[22].

Istotnym elementem transformacji instytucjonalnej pozostaje rozwój kompetencji pracowników odpowiedzialnych za bezpieczeństwo. Henock Mulugeta Melaku zwraca uwagę, że skuteczność systemów cyberbezpieczeństwa zależy w równym stopniu od stosowanych technologii i od poziomu specjalistycznej wiedzy personelu. W praktyce oznacza to konieczność prowadzenia systematycznych szkoleń, rozwijania umiejętności z zakresu analizy danych, informatyki śledczej oraz zarządzania incydentami bezpieczeństwa. Niedobór wysoko wykwalifikowanych specjalistów stanowi obecnie jedno z najczęściej wskazywanych ograniczeń rozwoju krajowych systemów cyberbezpieczeństwa[23].

Coraz większego znaczenia nabiera również współpraca między administracją publiczną a sektorem prywatnym. Znaczna część infrastruktury krytycznej, obejmująca systemy energetyczne, telekomunikacyjne, finansowe oraz transportowe, pozostaje własnością prywatnych przedsiębiorstw. Ochrona tych zasobów wymaga zatem stworzenia mechanizmów umożliwiających bieżącą wymianę informacji o zagrożeniach, prowadzenie wspólnych ćwiczeń oraz opracowywania jednolitych procedur reagowania. Doświadczenia państw skandynawskich oraz Holandii pokazują, że dzięki rozwiniętym partnerstwom publiczno-prywatnym można szybciej identyfikować zagrożenia i skuteczniej ograniczać skutki incydentów cybernetycznych[24].

---

[21] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa*…

[22] *The NIST Cybersecurity Framework*…

[23] H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*, „Journal of Cybersecurity and Privacy" 2023, t. 3, nr 3, s. 347–350. https://doi.org/10.3390/jcp3030017.

[24] OECD, *Digital Security and Resilience*…, s. 51–53.

Przegląd literatury wskazuje również, że transformacja instytucjonalna nie może ograniczać się do wdrażania nowych technologii. Równie istotne jest budowanie kultury organizacyjnej sprzyjającej współpracy, wymianie wiedzy oraz ciągłemu doskonaleniu procedur bezpieczeństwa. Organizacje charakteryzujące się wysokim poziomem elastyczności organizacyjnej skuteczniej adaptują się do zmieniającego się środowiska zagrożeń niż instytucje funkcjonujące według sztywnych, hierarchicznych modeli zarządzania[25].

Podsumowując, można stwierdzić, że rozwój bezpieczeństwa wewnętrznego wymaga kompleksowej modernizacji instytucji publicznych. Obejmuje ona inwestycje w nowoczesne technologie, reformę struktur organizacyjnych, rozwój kompetencji pracowników, budowę trwałych mechanizmów współpracy z sektorem prywatnym oraz systematyczne doskonalenie procedur zarządzania ryzykiem. Analiza porównawcza doświadczeń państw UE i Stanów Zjednoczonych wskazuje, że najwyższą skuteczność osiągają systemy bezpieczeństwa łączące nowoczesne rozwiązania technologiczne z efektywnym zarządzaniem instytucjonalnym oraz jasno określonym podziałem odpowiedzialności[26].

Prawne i etyczne aspekty bezpieczeństwa wewnętrznego w erze cyfrowej

Transformacja cyfrowa spowodowała konieczność dostosowania obowiązujących regulacji prawnych dotyczących bezpieczeństwa wewnętrznego do zagrożeń w cyberprzestrzeni. Rozwój technologii informacyjnych umożliwił instytucjom publicznym wykorzystywanie narzędzi opartych na analizie dużych zbiorów danych, monitorowaniu sieci teleinformatycznych oraz automatyzacji procesów decyzyjnych. Jednocześnie rozwiązania te wywołały dyskusję dotyczącą granic ingerencji państwa w prawa i wolności jednostki. W literaturze przedmiotu podkreśla się, że skuteczność działań podejmowanych na rzecz bezpieczeństwa wewnętrznego powinna pozostawać w zgodzie z zasadą państwa prawa oraz standardami ochrony praw człowieka[27].

---

[25] Tamże.

[26] OECD, *Digital Security and Resilience*…, s. 55–58; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*…, s. 341–344; *The NIST Cybersecurity Framework*…

[27] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*; *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)*; M.D. Cavelty, *Cyber-Security and Threat Politics*…

Podstawowym aktem prawnym regulującym ochronę danych osobowych w państwach UE jest *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)* (dalej: rozporządzenie RODO). Regulacja ta ustanawia zasady legalności, przejrzystości, minimalizacji danych oraz ograniczenia celu ich przetwarzania. Z perspektywy bezpieczeństwa wewnętrznego oznacza to, że organy publiczne mogą wykorzystywać dane osobowe wyłącznie w zakresie niezbędnym do realizacji ustawowych zadań oraz z zachowaniem zasady proporcjonalności. Rozporządzenie RODO nie ogranicza możliwości prowadzenia działań związanych z bezpieczeństwem państwa, jednak nakłada obowiązek zapewnienia odpowiednich zabezpieczeń technicznych i organizacyjnych chroniących prawa obywateli.

Drugim istotnym elementem europejskiego systemu prawnego jest dyrektywa NIS 2. W porównaniu z wcześniejszą dyrektywą NIS1[28] rozszerzono katalog podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa oraz zaostrzono wymagania dotyczące zarządzania ryzykiem, zgłaszania incydentów oraz odpowiedzialności kierownictwa organizacji. Rozwiązania te odzwierciedlają zmianę podejścia – od reagowania na incydenty do systemowego budowania odporności państwa i infrastruktury krytycznej[29].

Istotne znaczenie dla współpracy międzynarodowej ma również konwencja Rady Europy o cyberprzestępczości zwana konwencją budapesztańską[30]. Dokument ten ujednolicił podstawowe definicje przestępstw komputerowych oraz stworzył ramy współpracy między organami ścigania różnych państw. Jak wskazuje Susan Brenner, skuteczne zwalczanie cyberprzestępczości wymaga harmonizacji regulacji prawnych, ponieważ sprawcy często wykorzystują różnice między krajowymi systemami prawnymi. Konwencja budapesztańska pozostaje podstawowym instrumentem współpracy międzynarodowej w zakresie ścigania przestępstw popełnianych z wykorzystaniem technologii informacyjnych.

W Polsce podstawę systemu cyberbezpieczeństwa stanowi ustawa o krajowym systemie cyberbezpieczeństwa[31] implementująca rozwiązania przyjęte

---

[28] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*.

[29] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa…*

[30] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.*; S.W. Brenner, *Cybercrime and the Law…*, s. 48–50.

[31] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*.

na poziomie UE. Ustawa określa kompetencje administracji publicznej, operatorów usług kluczowych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT MON, CSIRT NASK oraz CSIRT GOV). Jej celem jest zapewnienie sprawnego wykrywania incydentów, koordynacji działań naprawczych oraz wymiany informacji między instytucjami odpowiedzialnymi za bezpieczeństwo państwa.

Coraz większe znaczenie zyskują również regulacje dotyczące wykorzystania sztucznej inteligencji. Przyjęty przez Unię Europejską AI Act[32] wprowadza klasyfikację systemów sztucznej inteligencji według poziomu ryzyka oraz określa obowiązki podmiotów wdrażających rozwiązania o wysokim stopniu oddziaływania społecznego. W kontekście bezpieczeństwa wewnętrznego oznacza to konieczność zapewnienia przejrzystości działania algorytmów wykorzystywanych m.in. do analizy zagrożeń, monitorowania przestrzeni publicznej czy wspomagania procesów decyzyjnych służb odpowiedzialnych za bezpieczeństwo.

Aspekty prawne są ściśle związane z problematyką etyczną. Rozwój systemów monitoringu, analityki predykcyjnej oraz sztucznej inteligencji zwiększa możliwości zapobiegania zagrożeniom, ale jednocześnie rodzi ryzyko naruszenia prawa do prywatności oraz wystąpienia dyskryminacji algorytmicznej. Cavelty podkreśla, że przyzwolenie społeczne na wykorzystywanie nowoczesnych technologii w celu zapewnienia bezpieczeństwa zależy od przejrzystości procedur, możliwości kontroli działań administracji oraz skutecznych mechanizmów odwoławczych. Obywatele są bardziej skłonni akceptować zwiększony zakres działań państwa, jeżeli mają pewność, że ingerencja odbywa się na podstawie prawa i podlega niezależnemu nadzorowi[33].

Analiza porównawcza wskazuje wyraźne różnice między podejściem europejskim i amerykańskim. W UE pierwszeństwo przyznaje się ochronie praw podstawowych, prywatności oraz kontroli przetwarzania danych osobowych. W USA większy nacisk położono na efektywność działań operacyjnych służb odpowiedzialnych za bezpieczeństwo narodowe, pozostawiając przy tym szerszy zakres kompetencji instytucjom zajmującym się przeciwdziałaniem zagrożeniom. Różnice te wynikają z odmiennych tradycji prawnych i konstytucyjnych. Oba modele zmierzają jednak do zachowania równowagi między skutecznością działań w zakresie bezpieczeństwa a ochroną praw obywatelskich[34].

---

[32] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*.

[33] M.D. Cavelty, *Cyber-Security and Threat Politics*…, s. 91–93.

[34] Tamże, s. 91–95.

Przegląd literatury oraz obowiązujących regulacji prowadzi do wniosku, że rozwój bezpieczeństwa wewnętrznego w erze cyfrowej wymaga równoczesnego doskonalenia instrumentów prawnych i standardów etycznych. Nowoczesne technologie mogą znacznie zwiększać skuteczność instytucji odpowiedzialnych za bezpieczeństwo, jednak ich wykorzystanie powinno odbywać się w granicach wyznaczonych przez zasadę proporcjonalności, legalności i odpowiedzialności. Tylko zachowanie równowagi pomiędzy ochroną bezpieczeństwa państwa a poszanowaniem praw jednostki pozwala budować trwałe zaufanie społeczne i zapewnić skuteczność systemu bezpieczeństwa wewnętrznego[35].

Technologia jako narzędzie bezpieczeństwa wewnętrznego

Rozwój technologii cyfrowych istotnie zmienił sposób realizacji zadań związanych z zapewnieniem bezpieczeństwa wewnętrznego. Nowoczesne rozwiązania informatyczne nie pełnią już funkcji wyłącznie wspomagającej działalność instytucji publicznych, lecz stały się jednym z podstawowych elementów planowania, monitorowania zagrożeń i reagowania na nie. Jak podkreślają Clarke i Knake, współczesne bezpieczeństwo państwa w coraz większym stopniu jest uzależnione od zdolności do skutecznego wykorzystania technologii informacyjnych zarówno w działaniach prewencyjnych, jak i operacyjnych[36].

Jednym z najważniejszych kierunków rozwoju pozostaje wykorzystanie analizy danych oraz sztucznej inteligencji. Współczesne systemy bezpieczeństwa przetwarzają ogromne ilości informacji pochodzących z monitoringu, sieci teleinformatycznych, rejestrów administracyjnych oraz otwartych źródeł informacji (ang. *open-source intelligence*, OSINT). Zastosowanie algorytmów uczenia maszynowego umożliwia identyfikację nietypowych zachowań, przewidywanie potencjalnych zagrożeń oraz wspomaganie procesów decyzyjnych. Melaku wskazuje, że rozwiązania oparte na sztucznej inteligencji zwiększają skuteczność zarządzania cyberbezpieczeństwem pod warunkiem, że funkcjonują w ramach odpowiednio zaprojektowanego systemu zarządzania ryzykiem oraz podlegają stałemu nadzorowi ekspertów[37].

---

[35] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.…*; *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych…*; *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji…*

[36] R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat…*, s. 12–28.

[37] H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework…*, s. 348–350.

Istotną rolę odgrywają również technologie wspierające monitorowanie infrastruktury krytycznej. Systemy automatycznej detekcji zagrożeń pozwalają na bieżące analizowanie funkcjonowania sieci energetycznych, transportowych, telekomunikacyjnych oraz finansowych. Raport *ENISA Threat Landscape 2023* wskazuje, że szybkie wykrywanie nieprawidłowości znacznie ogranicza skutki ataków ransomware oraz innych incydentów wymierzonych w infrastrukturę państwa. Z tego względu coraz większy nacisk kładzie się na rozwój systemów wczesnego ostrzegania oraz automatyzację procedur reagowania[38].

Przykładem praktycznego wykorzystania technologii są krajowe i sektorowe centra operacji bezpieczeństwa (ang. *security operations centres*), których zadaniem jest całodobowe monitorowanie sieci teleinformatycznych oraz analiza pojawiających się zagrożeń. Funkcjonowanie takich jednostek umożliwia skrócenie czasu wykrywania incydentów oraz szybszą koordynację działań naprawczych.

Unia Europejska i Stany Zjednoczone mają odmienne podejście do wykorzystania technologii. Państwa unijne równolegle rozwijają technologię i system regulacyjny, akcentując ochronę danych osobowych oraz bezpieczeństwo infrastruktury krytycznej. W USA większy nacisk położono na współpracę administracji federalnej z sektorem prywatnym oraz rozwój innowacyjnych technologii opracowywanych przez przedsiębiorstwa technologiczne. Model amerykański sprzyja szybkiemu wdrażaniu nowych rozwiązań, europejski natomiast zapewnia silniejsze mechanizmy nadzoru prawnego nad ich stosowaniem[39].

Postępująca automatyzacja procesów bezpieczeństwa przynosi jednak również nowe wyzwania. Coraz większe uzależnienie administracji publicznej od systemów informatycznych powoduje, że awaria lub skuteczny cyberatak mogą prowadzić do zakłócenia funkcjonowania wielu sektorów jednocześnie. Libicki podkreśla, że wzrost poziomu cyfryzacji zwiększa zarówno efektywność działania instytucji publicznych, jak i skalę potencjalnych konsekwencji wynikających z naruszenia bezpieczeństwa systemów informatycznych. Oznacza to konieczność projektowania rozwiązań zapewniających odporność, redundancję oraz możliwość szybkiego odtworzenia funkcji krytycznych po wystąpieniu incydentu[40].

W literaturze zwraca się również uwagę na znaczenie współpracy między środowiskiem naukowym, administracją publiczną oraz sektorem prywatnym. Dynamiczny rozwój technologii powoduje, że instytucje odpowiedzialne za bezpieczeństwo nie są w stanie samodzielnie opracowywać wszystkich innowacyjnych

[38] *ENISA Threat Landscape 2023*…, s. 47–51.

[39] Tamże; *The NIST Cybersecurity Framework*…; *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych*…

[40] M.C. Libicki, *Conquest in Cyberspace*…, s. 102–106.

rozwiązań. OECD wskazuje, że partnerstwa obejmujące uczelnie, instytuty badawcze oraz przedsiębiorstwa technologiczne sprzyjają szybszemu wdrażaniu nowych narzędzi analitycznych, poprawiają jakość zarządzania ryzykiem oraz zwiększają poziom odporności cyfrowej państwa[41].

Przegląd literatury prowadzi do wniosku, że technologia stanowi obecnie jeden z najważniejszych instrumentów zapewnienia bezpieczeństwa wewnętrznego. Jej skuteczność zależy jednak od sposobu integracji z rozwiązaniami organizacyjnymi, prawnymi i kadrowymi. Samo wdrażanie nowych systemów informatycznych nie gwarantuje zwiększenia poziomu bezpieczeństwa. Decydujące znaczenie ma stworzenie spójnego modelu zarządzania, w którym rozwiązania technologiczne wspierają proces podejmowania decyzji, pozostając jednocześnie pod kontrolą odpowiednich procedur prawnych i kompetentnego personelu. Analiza doświadczeń państw UE i Stanów Zjednoczonych potwierdza, że najwyższą skuteczność osiągają systemy łączące rozwój technologii z inwestycjami w kapitał ludzki, współpracę międzyinstytucjonalną oraz systematyczną ocenę ryzyka[42].

Kontekst międzynarodowy i perspektywa porównawcza

Współczesne bezpieczeństwo wewnętrzne nie może być analizowane wyłącznie z perspektywy pojedynczego państwa. Rozwój technologii cyfrowych spowodował, że zagrożenia coraz częściej mają charakter transgraniczny, a ich skutki wykraczają poza granice jurysdykcji krajowych. Cyberprzestępczość, kampanie dezinformacyjne czy ataki na infrastrukturę krytyczną są prowadzone z wykorzystaniem globalnych sieci teleinformatycznych, co powoduje, że skuteczne przeciwdziałanie wymaga ścisłej współpracy międzynarodowej. Jak zauważa Kello, cyberprzestrzeń stała się nowym środowiskiem rywalizacji strategicznej, w którym granice między bezpieczeństwem wewnętrznym i zewnętrznym stopniowo się zacierają[43].

Pomimo różnic organizacyjnych systemy europejski i amerykański opierają się na podobnych założeniach strategicznych. W obu przypadkach kluczowe znaczenie mają: rozwój krajowych strategii cyberbezpieczeństwa, budowanie odporności infrastruktury krytycznej, doskonalenie systemów wymiany informacji oraz rozwój kompetencji specjalistycznych. Różnice dotyczą natomiast sposobu realizacji tych celów. W państwach UE większy nacisk położono na harmonizację

[41] OECD, *Digital Security and Resilience*…, s. 34–39.

[42] Tamże; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*…, s. 327–331; *The NIST Cybersecurity Framework*…

[43] L. Kello, *The virtual weapon and international order*…, s. 45–62.

przepisów prawa i ochronę praw podstawowych, a w USA na elastyczność organizacyjną oraz partnerstwo publiczno-prywatne[44].

Znaczącą rolę w międzynarodowym systemie bezpieczeństwa odgrywa również Organizacja Traktatu Północnoatlantyckiego (NATO). Po uznaniu cyberprzestrzeni za domenę działań operacyjnych NATO rozwija wspólne zdolności w zakresie przeciwdziałania zagrożeniom cybernetycznym, prowadzi ćwiczenia z udziałem państw członkowskich oraz wspiera wymianę doświadczeń dotyczących ochrony infrastruktury krytycznej. Rozwiązania te zwiększają zdolność państw do reagowania na incydenty o charakterze transgranicznym oraz sprzyjają ujednolicaniu procedur bezpieczeństwa[45].

Coraz większe znaczenie mają również działania prowadzone przez Organizację Narodów Zjednoczonych oraz Radę Europy. Konwencja budapesztańska stworzyła podstawy współpracy organów ścigania w zakresie zwalczania cyberprzestępczości, a eksperckie grupy ONZ opracowują rekomendacje dotyczące odpowiedzialnego zachowania państw w cyberprzestrzeni[46]. Chociaż dokumenty te nie eliminują wszystkich różnic między krajowymi systemami prawnymi, to przyczyniają się do stopniowej harmonizacji standardów międzynarodowych oraz ułatwiają współpracę w zakresie ścigania sprawców przestępstw komputerowych.

Analiza porównawcza dokumentów prowadzi do wniosku, że skuteczność systemów bezpieczeństwa wewnętrznego zależy nie od przyjęcia jednego uniwersalnego modelu organizacyjnego, lecz od umiejętnego dostosowania rozwiązań do uwarunkowań krajowych przy jednoczesnym wykorzystaniu doświadczeń międzynarodowych. Wspólnym elementem wszystkich analizowanych modeli, czyli unijnego i amerykańskiego, pozostaje rozwój współpracy międzyinstytucjonalnej, budowanie odporności infrastruktury krytycznej, systematyczna wymiana informacji o zagrożeniach oraz ciągłe doskonalenie kompetencji specjalistycznych. Przegląd literatury potwierdza, że państwa aktywnie uczestniczące w międzynarodowych sieciach współpracy osiągają wyższy poziom odporności na zagrożenia cyfrowe oraz skuteczniej reagują na incydenty o charakterze transgranicznym[47].

---

[44] OECD, *Digital Security and Resilience*…, s. 34–58; *ENISA Threat Landscape 2023*…; *The NIST Cybersecurity Framework*…

[45] A. Kozłowski, *Operacje NATO w cyberprzestrzeni*, CyberDefence24, 3 VI 2019 r., https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [dostęp: 11 IX 2026].

[46] *Konwencja Rady Europy o cyberprzestępczości*…; United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,* A/76/135, 14 July 2021, s. 57–59.

[47] OECD, *Digital Security and Resilience*…, s. 51–54; *ENISA Threat Landscape 2023*…; *The NIST Cybersecurity Framework*…

Podsumowanie i wnioski

Przeprowadzona analiza literatury przedmiotu, aktów prawnych oraz dokumentów strategicznych potwierdza, że postępująca cyfryzacja prowadzi do zasadniczej zmiany sposobu postrzegania bezpieczeństwa wewnętrznego. Współczesne zagrożenia coraz rzadziej mają charakter wyłącznie lokalny lub fizyczny, a coraz częściej obejmują cyberprzestrzeń, infrastrukturę krytyczną oraz środowisko informacyjne. W konsekwencji bezpieczeństwo wewnętrzne należy rozumieć jako system zdolny do identyfikowania, ograniczania i neutralizowania zagrożeń istniejących równocześnie w wymiarze technologicznym, organizacyjnym, prawnym i społecznym.

Analiza dorobku naukowego Barry'ego Buzana, Myriam Dunn Cavelty, Richarda Clarke'a, Roberta Knake'a, Lucasa Kello oraz Davida S. Walla i innych badaczy wskazuje, że rozwój technologii cyfrowych doprowadził do rozszerzenia zakresu odpowiedzialności instytucji bezpieczeństwa. Ochrona porządku publicznego obejmuje obecnie również zapewnienie bezpieczeństwa infrastruktury cyfrowej, ochronę danych, przeciwdziałanie dezinformacji oraz budowanie odporności społeczeństwa na zagrożenia informacyjne. Oznacza to odejście od tradycyjnego modelu bezpieczeństwa skoncentrowanego na reagowaniu po wystąpieniu zagrożenia na rzecz modelu opartego na zarządzaniu ryzykiem i wzmacnianiu odporności.

Przegląd literatury pozwala również stwierdzić, że skuteczność systemu bezpieczeństwa wewnętrznego zależy od stopnia integracji działań prowadzonych przez administrację publiczną, sektor prywatny oraz środowisko naukowe. Szczególne znaczenie ma ochrona infrastruktury krytycznej, która w większości państw pozostaje w znacznej części własnością podmiotów prywatnych. Doświadczenia państw europejskich oraz Stanów Zjednoczonych pokazują, że rozwinięte partnerstwa publiczno-prywatne umożliwiają skuteczniejszą wymianę informacji o zagrożeniach, szybsze reagowanie na incydenty oraz bardziej efektywne zarządzanie ryzykiem.

Państwa UE i Stany Zjednoczone realizują odmienne modele organizacji bezpieczeństwa cyfrowego. Model europejski koncentruje się na harmonizacji regulacji prawnych, ochronie praw podstawowych oraz budowaniu wspólnych standardów cyberbezpieczeństwa. Model amerykański większy nacisk kładzie na zarządzanie ryzykiem, elastyczność organizacyjną oraz współpracę administracji z sektorem prywatnym.

Analiza aktów prawnych wskazuje, że rozwój bezpieczeństwa wewnętrznego wymaga równoczesnego doskonalenia regulacji dotyczących ochrony danych osobowych, cyberbezpieczeństwa oraz wykorzystania sztucznej inteligencji. Unijne rozporządzenie RODO, dyrektywa NIS 2, konwencja budapesztańska oraz AI Act tworzą komplementarne ramy prawne umożliwiające prowadzenie działań na rzecz bezpieczeństwa przy jednoczesnym poszanowaniu praw i wolności obywatelskich.

Oznacza to konieczność zachowania równowagi między skutecznością działań służb odpowiedzialnych za bezpieczeństwo a ochroną prywatności, przejrzystością działania administracji oraz odpowiedzialnością za podejmowane decyzje.

Na podstawie przeprowadzonej analizy można sformułować następujące wnioski:

1. Cyfryzacja trwale zmieniła charakter bezpieczeństwa wewnętrznego, rozszerzając jego zakres o ochronę cyberprzestrzeni, w tym systemów obsługujących infrastrukturę krytyczną oraz bezpieczeństwa informacyjnego.
2. Największym wyzwaniem dla współczesnych systemów bezpieczeństwa pozostaje zdolność instytucji do szybkiego dostosowywania struktur organizacyjnych i procedur do dynamicznie zmieniającego się środowiska zagrożeń.
3. Skuteczność ochrony bezpieczeństwa wewnętrznego zależy od współpracy administracji publicznej, sektora prywatnego oraz środowiska naukowego, szczególnie w zakresie ochrony infrastruktury krytycznej i wymiany informacji o zagrożeniach.
4. Nowoczesne technologie, w tym sztuczna inteligencja, analiza dużych zbiorów danych oraz automatyzacja procesów bezpieczeństwa, zwiększają możliwości instytucji odpowiedzialnych za bezpieczeństwo, jednak wykorzystanie tych technologii wymaga odpowiednich gwarancji prawnych i etycznych.
5. Najwyższą skuteczność osiągają systemy łączące rozwój technologiczny z efektywnym zarządzaniem, jasnym podziałem kompetencji oraz rozbudowaną współpracą międzynarodową.

Bezpieczeństwo wewnętrzne w erze cyfrowej wymaga podejścia interdyscyplinarnego, łączącego wiedzę z zakresu nauk o bezpieczeństwie, prawa, nauk o zarządzaniu oraz technologii informacyjnych. Dalszy rozwój systemów bezpieczeństwa będzie uzależniony od zdolności państw do wdrażania innowacyjnych rozwiązań technologicznych przy jednoczesnym zachowaniu standardów demokratycznego państwa prawa i ochrony praw człowieka.

Na podstawie przeprowadzonej analizy autor zauważa również kierunki dalszych badań dotyczących wpływu sztucznej inteligencji na funkcjonowanie instytucji bezpieczeństwa, oceny skuteczności wdrażania dyrektywy NIS 2 w państwach UE oraz porównania krajowych modeli budowania odporności cyfrowej. Wiedza na ten temat może dostarczyć istotnych rekomendacji dla praktyki funkcjonowania administracji publicznej oraz dalszego doskonalenia krajowych systemów bezpieczeństwa wewnętrznego.

Bibliografia

Brenner S.W., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012.

Buzan B., Wæver O., Wilde J. de, *Security: A New Framework for Analysis*, London 1998.

Cavelty M.D., *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009.

Clarke R.A., Knake R.K., *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.

Kello L., *The virtual weapon and international order*, New Haven–London 2017.

Libicki M.C., *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007.

Melaku H.M., *A Dynamic and Adaptive Cybersecurity Governance Framework*, „Journal of Cybersecurity and Privacy" 2023, t. 3, nr 3, s. 327–350. https://doi.org/10.3390/jcp3030017.

United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021.

Wall D.S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007.

Źródła internetowe

ENISA Threat Landscape 2023, European Union Agency for Cybersecurity, October 2023, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [dostęp: 11 VIII 2026].

Kozłowski A., *Operacje NATO w cyberprzestrzeni*, CyberDefence24, 3 VI 2019 r., https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [dostęp: 11 IX 2026].

OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf? [dostęp: 11 VIII 2026].

The NIST Cybersecurity Framework (CSF) 2.0, February 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [dostęp: 17 VIII 2026].

Akty prawne

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

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27 XII 2022 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19 VII 2016 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) – (Dz. Urz. UE L 2024/1689 z 12 VII 2024 r.).

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.).

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (DzU z 2015 r. poz. 728).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2018 r. poz. 1560, ze zm.).

Michał Antoniuk

Ukończył studia na Uniwersytecie Warszawskim oraz podyplomowe studia w Akademii Sztuki Wojennej. Zawodowo związany z administracją publiczną, obecnie pełni służbę w Ministerstwie Obrony Narodowej, gdzie realizuje zadania z obszaru bezpieczeństwa. Jego zainteresowania naukowe i zawodowe obejmują geopolitykę oraz zarządzanie projektami.

Kontakt: antonek@o2.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 91–111
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.024.24173

ARTYKUŁ

Erozja odporności państwa jako wyzwanie dla bezpieczeństwa wewnętrznego – propozycja ramy analitycznej umożliwiającej wczesne rozpoznawanie zagrożeń społecznych i instytucjonalnych

Erosion of state resilience as a challenge to internal security – propsal for analytical framework enabling the early identification of social and institutional threats

RADOSŁAW KORDA

Autor niezależny

https://orcid.org/0009-0007-6609-5742

Abstrakt

Celem artykułu jest przedstawienie erozji odporności państwa jako użytecznej kategorii analitycznej w badaniu bezpieczeństwa wewnętrznego oraz zaproponowanie trójpoziomowej ramy analitycznej umożliwiającej obserwację symptomów osłabienia odporności państwa przed wystąpieniem jawnego kryzysu. Artykuł opiera się na analizie literatury przedmiotu, analizie porównawczej oraz syntezie modelowej (ang. *conceptual/model synthesis*). Punktem wyjścia jest założenie, że współczesne państwa są relatywnie dobrze przygotowane do reagowania na incydenty kryzysowe, gorzej natomiast identyfikują procesy długotrwałej erozji obejmujące sfery społeczną, instytucjonalną i informacyjną. Wniosek końcowy wskazuje, że bezpieczeństwo wewnętrzne wymaga nie tylko

zdolności do reagowania, lecz także rozwiniętej zdolności do rozpoznawania procesów erozyjnych o znaczeniu strategicznym.

Słowa kluczowe odporność państwa, kapitał społeczny, zaufanie instytucjonalne, analiza strategiczna, dezinformacja

Abstract The aim of the article is to present the erosion of state resilience as a useful analytical category in the study of internal security and a proposal for a three-level analytical framework for monitoring signs of a weakening of the state's resilience before an overt crisis arises. The article is based on the analysis of the relevant literature, comparative analysis and model synthesis. The starting point is the assumption that modern states are relatively well-prepared to respond to crisis incidents, yet are less adept at identifying processes of long-term erosion affecting social, institutional and informational spheres. The final conclusion indicates that internal security requires not only the ability to react but also a developed capacity to recognise erosional processes of strategic importance.

Keywords state resilience, social capital, institutional trust, strategic analysis, disinformation

Wprowadzenie

Współczesne państwa rozwijają rozbudowane procedury reagowania na zdarzenia gwałtowne – ataki terrorystyczne, katastrofy, awarie infrastruktury krytycznej, pandemie lub zakłócenia o charakterze hybrydowym. W ujęciu instytucjonalnym oznacza to wzrost znaczenia zarządzania kryzysowego, planów ciągłości działania oraz instrumentów koordynacji międzyresortowej. Tego rodzaju przygotowanie nie oznacza jednak pełnej zdolności do rozpoznawania procesów, które nie są jednorazowymi incydentami, lecz rozwijają się stopniowo, osłabiając relacje między społeczeństwem, instytucjami publicznymi i systemem informacyjnym państwa[1]. W praktyce bezpieczeństwa wewnętrznego szczególne znaczenie mają więc nie tylko nagłe zagrożenia, lecz także długotrwałe procesy erozyjne, które obniżają

[1] OECD, *Boosting Resilience through Innovative Risk Governance*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/05/boosting-resilience-through-innovative-risk-governance_g1g3fd76/9789264209114-en.pdf, s. 15–23 [dostęp: 26 III 2026].

zdolność państwa do absorpcji wstrząsów (np. przeciążenie systemu ochrony zdrowia, nagły spadek zaufania instytucjonalnego, zakłócenie komunikacji między władzą a społeczeństwem) oraz adaptacji do zmieniających się warunków i odbudowy sprawności[2].

Przedmiotem badań jest erozja odporności państwa ujmowana jako problem bezpieczeństwa wewnętrznego. Pojęcie to odnosi się do stopniowego osłabiania zdolności państwa do utrzymywania porządku instytucjonalnego, koordynowania reakcji publicznej oraz podtrzymywania zaufania społecznego niezbędnego dla skutecznego działania organów władzy. W takim ujęciu odporność nie jest wyłącznie cechą infrastruktury lub procedur kryzysowych, lecz obejmuje także czynniki społeczne, w tym poziom zaufania instytucjonalnego, spójność wspólnotową, legitymizację instytucji oraz jakość komunikacji między władzą a społeczeństwem[3]. Bezpieczeństwo wewnętrzne nie może być zatem rozumiane wyłącznie jako zdolność do neutralizacji zagrożenia po jego ujawnieniu, lecz także jako zdolność do wczesnego rozpoznawania sygnałów osłabienia struktur państwowych.

Problem badawczy można sformułować następująco: jakie symptomy i wskaźniki pozwalają rozpoznawać proces erozji odporności państwa, zanim przybierze on postać jawnego kryzysu bezpieczeństwa wewnętrznego? Pytanie to wynika z widocznej w literaturze dysproporcji między rozwiniętymi analizami reakcji kryzysowej a skromniejszym dorobkiem dotyczącym wczesnego identyfikowania procesów osłabiających zdolność państwa do skutecznego działania[4]. Z perspektywy analitycznej chodzi zatem o uchwycenie takich zjawisk jak spadek zaufania do instytucji, przeciążenie systemów publicznych, zaburzenia koordynacji między podmiotami publicznymi oraz narastanie chaosu informacyjnego.

Celem artykułu jest przedstawienie erozji odporności państwa jako użytecznej kategorii analitycznej w badaniu bezpieczeństwa wewnętrznego oraz zaproponowanie ramy analitycznej służącej rozpoznawaniu wczesnych symptomów erozji odporności państwa w tym obszarze. Rama ta łączy perspektywy: społeczną, instytucjonalną i informacyjną, przy założeniu, że osłabienie państwa rzadko jest jednowymiarowe. W artykule zastosowano analizę literatury przedmiotu, analizę porównawczą doświadczeń dwóch europejskich państw oraz syntezę modelową (ang. *conceptual/model synthesis*) prowadzącą do uporządkowania proponowanych

[2] C.S. Holling, *Resilience and Stability of Ecological Systems*, „Annual Review of Ecology and Systematics" 1973, nr 4, s. 14–18. http://dx.doi.org/10.1146/annurev.es.04.110173.000245.

[3] R.D. Putnam, *Bowling Alone. The Collapse and Revival of American Community*, New York 2000, s. 19–28; F. Fukuyama, *Trust. The Social Virtues and the Creation of Prosperity*, New York 1995, s. 26–35.

[4] A. Boin i in., *The Politics of Crisis Management. Public Leadership under Pressure*, Cambridge 2017, s. 3–12. https://doi.org/10.1017/9781316339756.

wskaźników. Takie podejście pozwala połączyć dorobek różnych dziedzin nauk społecznych, w tym studiów nad bezpieczeństwem, badań nad zarządzaniem (ang. *governance*) i odpornością instytucjonalną[5].

W artykule przyjęto hipotezę, zgodnie z którą erozja odporności państwa jest możliwa do rozpoznania przed wystąpieniem jawnego kryzysu, o ile analiza bezpieczeństwa wewnętrznego obejmuje nie tylko zdarzenia incydentalne, lecz także kumulację osłabienia na poziomach społecznym, instytucjonalnym i informacyjnym.

Odporność państwa jako kategoria analityczna – od reakcji kryzysowej do zdolności adaptacyjnej

Pojęcie odporności (ang. *resilience*) weszło do współczesnego języka analizy bezpieczeństwa dopiero na przełomie XX i XXI w., choć jego geneza jest wcześniejsza i wywodzi się z badań nad stabilnością złożonych systemów. W klasycznym ujęciu Crawforda S. Hollinga odporność nie oznacza po prostu powrotu do stanu pierwotnego, lecz zdolność systemu do absorpcji zakłóceń bez utraty podstawowych funkcji i struktury[6]. Zastosowanie tej definicji w odniesieniu do nauk o bezpieczeństwie pozwoliło na odejście od rozumienia kryzysu jako jednorazowego zakłócenia i skierowanie uwagi badaczy ku pytaniu o to, dlaczego jedne systemy ulegają destabilizacji szybciej niż inne.

W kolejnych dekadach termin *resilience* zaczęto stosować w odniesieniu do organizacji, infrastruktury, administracji publicznej i wspólnot politycznych. W tym ujęciu odporność przestała być kategorią opisującą wyłącznie trwałość systemu, a zaczęła odnosić się do jego zdolności do adaptacji, odbudowy i koordynacji[7]. Miało to szczególne znaczenie dla analizy państwa jako podmiotu bezpieczeństwa, ponieważ klasyczne modele bezpieczeństwa opierały się przede wszystkim na kategoriach ochrony, kontroli i reagowania. Państwo było traktowane jako podmiot mający neutralizować zagrożenie po jego rozpoznaniu, a nie jako system, którego zdolność do utrzymywania sprawności może się stopniowo zmniejszać. Tymczasem współczesne środowisko

[5] D.D. Woods, *Four Concepts for Resilience and the Implications for the Future of Resilience Engineering*, „Reliability Engineering & System Safety" 2015, t. 141, s. 5–9. https://doi.org/10.1016/j.ress.2015.03.018.

[6] C.S. Holling, *Resilience and Stability of Ecological Systems*…, s. 1–23.

[7] B. Walker, D. Salt, *Resilience Thinking. Sustaining Ecosystems and People in a Changing World*, Washington 2006, s. 1–17.

bezpieczeństwa coraz częściej obejmuje zagrożenia rozproszone, długotrwałe i niejednoznaczne, a nie takie, które przybierają postać pojedynczego incydentu[8].

Włączenie pojęcia odporności do analizy państwa oznacza więc istotną zmianę perspektywy. Nie chodzi już wyłącznie o pytanie, czy instytucje potrafią zareagować na zagrożenie, lecz także o to, czy mogą utrzymać zdolność działania w warunkach długotrwałej presji, przeciążenia lub utraty zaufania społecznego. W tym sensie odporność państwa można rozumieć jako zdolność struktur publicznych oraz otaczającego je środowiska społecznego do absorpcji wstrząsów, adaptacji do zmieniających się warunków oraz przywracania równowagi funkcjonalnej bez trwałej utraty sterowności[9]. Tak rozumiana odporność ma znaczenie nie tylko dla zarządzania kryzysowego, lecz także dla bezpieczeństwa wewnętrznego jako całości, ponieważ dotyczy zarówno instytucji bezpieczeństwa, jak i szerzej – zdolności państwa do zachowania porządku konstytucyjnego, ciągłości usług publicznych i społecznej legitymizacji działań.

Pojęcia bezpieczeństwa i odporności nie są tożsame. Bezpieczeństwo odnosi się tradycyjnie do stanu ograniczenia zagrożeń lub zdolności ich neutralizacji, odporność natomiast opisuje zdolność funkcjonowania mimo zakłóceń. Oznacza to, że państwo może dysponować znaczącymi instrumentami bezpieczeństwa formalnego, a jednocześnie wykazywać niską odporność w sensie społecznym, wynikającą ze słabości więzi i zaufania, lub instytucjonalnym. Może również pozostawać relatywnie odporne mimo występowania zagrożeń, jeśli ma wysoką zdolność adaptacyjną i regeneracyjną[10]. Dla bezpieczeństwa wewnętrznego rozróżnienie bezpieczeństwa i odporności ma zasadnicze znaczenie, ponieważ pozwala uchwycić zjawiska, które nie mieszczą się w prostym modelu „zagrożenie – reakcja – neutralizacja", a które w praktyce decydują o tym, czy państwo pozostaje sprawne w warunkach napięcia.

Z tej perspektywy szczególnie widoczne stają się ograniczenia klasycznych modeli bezpieczeństwa. Sprawdzają się one dobrze w przypadku zagrożeń wyraźnie identyfikowalnych, punktowych i operacyjnie uchwytnych, np. aktów przemocy, takich jak zamach, awarie infrastruktury czy zakłócenia porządku publicznego. Znacznie gorzej radzą sobie jednak z procesami rozciągniętymi w czasie, takimi jak spadek zaufania do instytucji, przeciążenie systemów publicznych, fragmentacja komunikacyjna (podział wspólnej przestrzeni informacyjnej na wiele kanałów przekazywania informacji i wiele grup odbiorców) czy zmniejszenie zdolności administracji publicznej w zakresie koordynacji działań. To właśnie tego rodzaju

[8] OECD, *Boosting Resilience*…, s. 9–18; RAND Corporation, *Building Resilience to Systemic Risks. A Review of the Literature*, Santa Monica 2021, s. 5–11.

[9] D.D. Woods, *Four Concepts for Resilience*…

[10] A. Wildavsky, *Searching for Safety*, New Brunswick–Oxford 1988, s. 77–91.

zjawiska mogą tworzyć środowisko sprzyjające kryzysowi, zanim ten uwidoczni się w formie jawnego incydentu[11].

Odporność państwa nie powinna być zatem traktowana jako pojęcie zastępujące bezpieczeństwo, lecz jako jego uzupełniająca i pogłębiająca kategoria analityczna. Pozwala ona dostrzec zarówno to, jak państwo reaguje na kryzys, jak i to, w jakim stanie wchodzi ono w sytuację napięcia i czy dysponuje wystarczającym potencjałem adaptacyjnym, aby utrzymać sterowność i zaufanie społeczne[12].

Erozja odporności państwa jako proces trudniejszy do rozpoznania, lecz istotny strategicznie

W analizie bezpieczeństwa wewnętrznego pojęcie kryzysu zazwyczaj odnosi się do zdarzenia rozpoznawalnego, wyraźnie odbiegającego od normy i wymagającego nadzwyczajnej reakcji instytucjonalnej. Kryzys ma zatem zwykle charakter punktowy – ujawnia się w określonym czasie, bywa nazywany sytuacją przełomową i uruchamia widoczne mechanizmy zarządzania. Inny charakter ma natomiast proces erozyjny, który nie musi oznaczać natychmiastowego zakłócenia porządku publicznego ani jednoznacznych symptomów operacyjnych, które wskazywałyby na konieczność reakcji, lecz stopniowo obniża zdolność państwa do skutecznego działania[13]. Nie jest więc to kryzys sam w sobie, lecz stan narastającej podatności, który może poprzedzać kryzys, pogłębiać jego skutki lub utrudniać odbudowę sprawności po jego wystąpieniu.

Różnica między kryzysem a procesem erozyjnym ma znaczenie analityczne i praktyczne. Kryzys skupia uwagę decydentów, ponieważ jest widoczny i może mieć jednoznaczne konsekwencje polityczne. Proces erozyjny przebiega natomiast poniżej progu natychmiastowej reakcji. Jego dynamika opiera się na kumulacji słabości, które z osobna wydają się mieć ograniczony wpływ, ale występujące razem zmieniają warunki funkcjonowania państwa[14]. Państwo nie przestaje działać nagle – zaczyna działać mniej spójnie, mniej przewidywalnie i mniej wiarygodnie. Przeciążenie instytucji administracyjnych może obniżać jakość podejmowanych przez nie decyzji i wydłużać czas reakcji, co z kolei wpływa na percepcję skuteczności działań państwa przez społeczeństwo. To utrudnia realizację działań wymagających legitymizacji i społecznej dyscypliny. Równolegle zakłócenia

[11] A. Boin i in., *The Politics of Crisis Management*…, s. 3–14; OECD, *Boosting Resilience*…, s. 21–24.

[12] *Designing Resilience. Preparing for Extreme Events*, L. Comfort, A. Boin, C.C. Demchak (red.), Pittsburgh 2010, s. 1–12.

[13] A. Boin i in., *The Politics of Crisis Management*…, s. 3–18.

[14] OECD, *Boosting Resilience*…, s. 21–30.

w sferze informacyjnej mogą osłabiać zdolność państwa do komunikowania intencji i wyjaśniania własnych działań[15].

Na poziomie społecznym erozja odporności przejawia się przede wszystkim w spadku zaufania społeczeństwa do instytucji państwa, przewidywalności działań z ich strony i gotowości do współdziałania. W stabilnych warunkach państwo może funkcjonować skutecznie także przy umiarkowanym poziomie napięć społecznych. Gdy jednak dochodzi do zakłócenia, znaczenia nabiera to, czy obywatele uznają działania instytucji za uzasadnione i adekwatne. Długotrwały spadek zaufania do instytucji publicznych, wzrost atomizacji społecznej oraz nasilenie polaryzacji osłabiają zdolność systemu do mobilizacji i koordynacji działań zbiorowych[16]. Oznacza to, że bezpieczeństwo wewnętrzne zależy nie tylko od formalnego potencjału aparatu państwowego, lecz także od jakości więzi społecznych i poziomu legitymizacji instytucjonalnej.

Na poziomie instytucjonalnym proces erozji staje się widoczny przede wszystkim przez przeciążenie struktur, spadek koordynacji i narastanie rozproszenia odpowiedzialności. Instytucje mogą formalnie zachowywać pełnię kompetencji, a jednocześnie stopniowo tracić zdolność do przekrojowego, szybkiego i konsekwentnego działania. W praktyce oznacza to wzrost liczby działań reaktywnych kosztem działań wyprzedzających, ograniczenie zdolności planistycznych oraz osłabienie współpracy między podmiotami odpowiedzialnymi za bezpieczeństwo, administrację i komunikację między władzą a społeczeństwem[17]. Erozja instytucjonalna często przybiera postać pozornej sprawności – system działa, ale coraz bardziej fragmentarycznie i z malejącą odpornością na zakłócenia.

Trzecim wymiarem procesu erozyjnego jest poziom informacyjny. Współczesne państwo funkcjonuje w środowisku, w którym zdolność do utrzymania porządku w zakresie komunikacji między władzą a społeczeństwem staje się elementem bezpieczeństwa wewnętrznego. Erozja odporności informacyjnej polega zarówno na obecności dezinformacji, jak i – szerzej – na narastaniu chaosu interpretacyjnego, spadku wiarygodności przekazu publicznego oraz utracie wspólnej płaszczyzny porozumienia, na której opierają się decyzje społeczne i instytucjonalne[18]. W takich warunkach nawet poprawne działania państwa mogą być odbierane jako niespójne lub arbitralne, a to zwiększa ryzyko wtórnej destabilizacji.

---

15 D.D. Woods, *Four Concepts for Resilience*…

16 R.D. Putnam, *Bowling Alone*…, s. 22–28; F. Fukuyama, *Trust. The Social Virtues*…, s. 26–37.

17 *Designing Resilience*…, s. 7–15.

18 RAND Corporation, *Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica 2018, s. 1–13.

Erozja odporności nie musi być utożsamiana z „upadkiem" państwa ani z dramatycznym załamaniem porządku. Jest raczej stanem stopniowego obniżania zdolności adaptacyjnych, który zmniejsza margines bezpieczeństwa instytucjonalnego i społecznego. Im wcześniej taki proces zostanie rozpoznany, tym większa pozostaje możliwość odbudowy sprawności[19]. Z tego względu analiza bezpieczeństwa wewnętrznego oprócz identyfikacji zdarzeń i incydentów powinna obejmować symptomy długotrwałego osłabienia, które – choć mniej widowiskowe – mają często większe znaczenie strategiczne.

W tym sensie erozja odporności państwa stanowi kategorię szczególnie użyteczną dla analizy bezpieczeństwa wewnętrznego. Pozwala bowiem uchwycić zjawiska, które nie są jeszcze kryzysem, ale przestają być neutralne dla funkcjonowania państwa. Jeżeli bezpieczeństwo ma być rozumiane jako zdolność nie tylko do reakcji, lecz także utrzymania sprawności pod presją, to procesy erozyjne należy włączyć do centralnego pola obserwacji analitycznej.

Kapitał społeczny i sprawność instytucjonalna – fundamenty odporności państwa

W ocenie odporności państwa nie należy polegać wyłącznie na zagadnieniach organizacyjnych czy infrastrukturalnych. Państwo jest systemem osadzonym w relacjach społecznych, normach zaufania i wzorcach współpracy. Kapitał społeczny i efektywność instytucjonalna to dwa splecione fundamenty jego odporności. Pierwszy odnosi się do jakości relacji społecznych i zasobów zaufania; drugi dotyczy zdolności instytucji do działania w sposób przewidywalny, skuteczny i skoordynowany. W odniesieniu do bezpieczeństwa wewnętrznego oba te wymiary, choć niezależne pod względem analitycznym, w praktyce warunkują się nawzajem[20].

W klasycznych ujęciach kapitał społeczny był rozumiany jako zasób tkwiący w relacjach społecznych, normach wzajemności i wzorach współpracy. Robert D. Putnam często wiązał go z poziomem uczestnictwa i zaangażowania obywatelskiego, zaufania i zdolności wspólnot do działania zbiorowego, wskazując, że jego osłabienie prowadzi do obniżenia jakości instytucji demokratycznych oraz skuteczności życia publicznego[21]. Francis Fukuyama podkreślał z kolei, że zaufanie społeczne

[19] OECD, *Boosting Resilience*…, s. 31–34; A. Boin i in., *The Politics of Crisis Management*…, s. 25–29.

[20] OECD, *Government at a Glance 2023*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/government-at-a-glance-2023_da193b0d/3d5c5d31-en.pdf, s. 17–24 [dostęp: 26 III 2026].

[21] Przez skuteczność życia publicznego w ujęciu Putnama należy rozumieć zdolność wspólnoty do rozwiązywania problemów zbiorowych i koordynowania działania zbiorowego oraz responsywność instytucji wobec potrzeb obywateli. Zob. R.D. Putnam, *Bowling Alone*…, s. 19–28.

stanowi podstawę efektywnej koordynacji w złożonych strukturach organizacyjnych i politycznych, ponieważ obniża koszty transakcyjne[22], zwiększa przewidywalność zachowań wszystkich stron relacji i wzmacnia gotowość do współpracy poza kontaktami stricte formalnymi[23]. W kontekście bezpieczeństwa państwa zaufanie nie jest kategorią wyłącznie normatywną czy moralną, lecz zasobem strategicznym wpływającym na zdolność systemu do reagowania i adaptacji.

Zaufanie społeczne ma szczególne znaczenie w sytuacjach napięcia, niepewności i przeciążenia instytucji. W stabilnych warunkach państwo może opierać swoje działanie w większym stopniu na procedurze i rutynie. W warunkach kryzysowych lub podwyższonej presji wzrasta natomiast znaczenie społecznej akceptacji decyzji publicznych, podporządkowania się komunikatom instytucjonalnym oraz współdziałania z organami państwa. Tam, gdzie zaufanie do instytucji jest trwale osłabione, nawet formalnie poprawne działania mogą być odbierane jako arbitralne, nieprzejrzyste lub nieskuteczne[24]. W konsekwencji obniża się zarówno efektywność zarządzania kryzysowego, jak i ogólna odporność państwa na zakłócenia społeczne, informacyjne i organizacyjne.

Równie istotna jak zaufanie jest spójność społeczna rozumiana jako zdolność społeczeństwa do utrzymywania minimalnego poziomu integracji normatywnej i systemowej (w rozumieniu klasycznego rozróżnienia D. Lockwooda między integracją społeczną a integracją systemową) mimo różnic interesów, poglądów czy doświadczeń[25]. Państwo może bowiem skutecznie funkcjonować nawet przy obecności konfliktów społecznych, o ile zostają zachowane podstawowe warunki współistnienia i wspólne zasady postępowania. Gdy jednak dochodzi do trwałego osłabienia więzi pionowych i poziomych – między obywatelami a instytucjami oraz wewnątrz samego społeczeństwa – maleje zdolność systemu do skoordynowanego reagowania na zakłócenia[26]. Z perspektywy bezpieczeństwa wewnętrznego oznacza to wzrost podatności na chaos komunikacyjny, polaryzację i wtórne konflikty wokół działań podejmowanych przez państwo.

Niemniej ważnym wymiarem odporności pozostaje sprawność instytucjonalna. Nawet wysoki kapitał społeczny nie kompensuje trwałej nieskuteczności

---

[22] Efekt obniżenia kosztów transakcyjnych przejawia się np. w mniejszej potrzebie szczegółowej kontroli i weryfikacji kontrahentów, krótszym czasie negocjacji, mniejszej liczbie sporów prawnych oraz ograniczonej konieczności stosowania zabezpieczeń formalnych (poręczeń, rozbudowanych umów).

[23] F. Fukuyama, *Trust. The Social Virtues*…, s. 26–37.

[24] M. Levi, L. Stoker, *Political Trust and Trustworthiness*, „Annual Review of Political Science" 2000, nr 3, s. 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475.

[25] D. Lockwood, *Social Integration and System Integration*, w: *Explorations in Social Change*, G.K. Zollschan, W. Hirsch, Houghton Mifflin (red.), Boston 1964, s. 244–257.

[26] J. Chan, *Social Cohesion and the Governance of Public Order*, w: *Social Capital and Public Policy*, D. Halpern (red.), Cambridge 2005, s. 145–162.

administracji, niespójności działań publicznych lub przeciążenia struktur odpowiedzialnych za koordynację działań. Sprawność instytucjonalna nie powinna być utożsamiana wyłącznie z efektywnością biurokratyczną. W kontekście bezpieczeństwa państwa obejmuje ona również zdolność do szybkiego rozpoznawania problemów, wymiany informacji, współpracy międzyinstytucjonalnej oraz utrzymania ciągłości działania pod presją[27]. Instytucje odporne są przede wszystkim zdolne do elastycznego, przewidywalnego i wiarygodnego działania.

Relacja między kapitałem społecznym a sprawnością instytucjonalną ma charakter sprzężenia zwrotnego. Instytucje działające w sposób przewidywalny i kompetentny wzmacniają zaufanie społeczne, podczas gdy niski poziom zaufania utrudnia realizację polityki publicznej i zwiększa koszty zarządzania. Z kolei osłabienie zdolności instytucjonalnych może przyspieszać erozję więzi społecznych, ponieważ obywatele zaczynają postrzegać państwo jako podmiot niezdolny do ochrony interesu publicznego lub zapewnienia elementarnej przewidywalności[28]. Z tego względu odporność państwa nie może być analizowana wyłącznie przez pryzmat zasobów materialnych, formalnych kompetencji czy rozwiązań organizacyjnych. O jej realnym poziomie współdecyduje także jakość relacji państwo–społeczeństwo.

Włączenie kapitału społecznego do analizy bezpieczeństwa państwa ma zatem znaczenie teoretyczne i operacyjne. Pozwala uchwycić te czynniki, które nie zawsze są bezpośrednio uwzględniane w klasycznych wskaźnikach bezpieczeństwa, a które w praktyce przesądzają o zdolności państwa do utrzymania sprawności w warunkach presji. Państwo odporne to państwo zarówno zdolne do reakcji, jak i zachowujące legitymizację, przewidywalność i zdolność współdziałania ze społeczeństwem[29]. Z perspektywy bezpieczeństwa wewnętrznego oznacza to konieczność traktowania zaufania społecznego, spójności wspólnotowej i sprawności instytucjonalnej jako elementów jednego, wspólnego układu odporności.

Autorska rama analityczna – model wczesnego rozpoznawania erozji odporności państwa

Wcześniejsze rozważania wyjaśniają, dlaczego do analizy bezpieczeństwa wewnętrznego jest potrzebne narzędzie, które uwidacznia nie tylko w pełni rozwinięte

[27] *Designing Resilience*…, s. 7–18.

[28] OECD, *Trust and Public Policy. How Better Governance Can Help Rebuild Public Trust*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/03/trust-and-public-policy_g1g74ea6/9789264268920-en.pdf, s. 31–46 [dostęp: 26 III 2026].

[29] R.D. Putnam, *Bowling Alone*…, s. 349–363; OECD, *Trust and Public Policy*…, s. 47–53.

kryzysy, lecz także zachowania stopniowo osłabiające zdolność państwa do reagowania. W tym celu sugeruje się podejście analityczne, które pomoże we wczesnej identyfikacji erozji odporności państwa. Nie ma ono na celu zastąpienia istniejących procesów oceny ryzyka ani stworzenia uniwersalnego narzędzia operacyjnego, lecz koordynację obserwacji dotyczących zjawisk – często niespójnych i pozornie niepowiązanych – których równoczesne wystąpienie może oznaczać zmniejszenie zdolności państwa do adaptacji do zmieniających się warunków[30]. Model ma charakter pomocniczy i interpretacyjny. Służy raczej do identyfikacji trendów oraz wzajemnych zależności niż do generowania prostych prognoz lub automatycznych ocen.

Punkt wyjścia modelu to założenie, że odporność państwa nie jest stanem binarnym – nie można jej opisywać wyłącznie jako „obecnej" lub „nieobecnej". Jest ona dynamiczna (zmienia się w czasie), relacyjna (zależy od kontekstu i interakcji między poziomami) i wielowymiarowa (obejmuje wymiary społeczny, instytucjonalny i informacyjny). Może stopniowo słabnąć, nie wywołując natychmiastowego kryzysu, ale jednocześnie powodować znaczne obniżenie zdolności państwa do reagowania na zakłócenia[31]. Drugie założenie dotyczy natury samej erozji: to efekt nakładania się procesów w wymiarach społecznym, instytucjonalnym i informacyjnym. Trzecie założenie ma charakter metodologiczny: wczesne rozpoznawanie powinno opierać się na obserwacji współwystępowania i trwałości sygnałów ostrzegawczych, a nie na pojedynczym wskaźniku[32].

Na tej podstawie proponowana rama analityczna obejmuje trzy poziomy obserwacji: społeczny, instytucjonalny i informacyjny. Nie są one niezależne od siebie – model zakłada, że rzeczywista wartość analityczna pojawia się dopiero wówczas, gdy zjawiska identyfikowane na poszczególnych poziomach zaczynają tworzyć układ, w którym wzajemnie się wzmacniają.

Pierwszy poziom – społeczny – obejmuje relacje zaufania, spójności i gotowości do współdziałania. W tej sferze do sygnałów ostrzegawczych można zaliczyć przede wszystkim trwały spadek zaufania do instytucji publicznych, osłabienie legitymizacji decyzji państwowych, wzrost percepcji niesprawiedliwości proceduralnej, nasilenie polaryzacji społecznej oraz obniżenie gotowości obywateli do respektowania norm wspólnego działania[33]. Nie chodzi przy tym o chwilowe napięcia lub typowe dla systemów demokratycznych konflikty polityczne, lecz o procesy utrwalające niski poziom przewidywalności społecznej i ograniczające zdolność państwa do mobilizowania współpracy. Z perspektywy bezpieczeństwa wewnętrznego poziom

[30] OECD, *Boosting Resilience*…, s. 21–34.

[31] D.D. Woods, *Four Concepts for Resilience*…, s. 5–9.

[32] *Designing Resilience*…, s. 1–18.

[33] R.D. Putnam, *Bowling Alone*…, s. 349–363; OECD, *Trust and Public Policy*…, s. 31–53.

społeczny ma podstawowe znaczenie, ponieważ to właśnie on decyduje o tym, czy państwo w sytuacji zakłócenia może liczyć na minimalną zgodność normatywną i akceptację działań przez społeczeństwo.

Drugi poziom dotyczy wymiaru instytucjonalnego, a więc zdolności państwa do działania skoordynowanego, przewidywalnego i adekwatnego do skali wyzwań. W tej sferze sygnały ostrzegawcze są zwykle mniej wyraźne, ale wiążą się bezpośrednio ze sprawnością państwa. Można do nich zaliczyć: narastające przeciążenie organizacyjne, wydłużanie czasu reakcji instytucjonalnej, rozproszenie odpowiedzialności, obniżenie zdolności koordynacyjnej między podmiotami publicznymi, wzrost liczby działań doraźnych kosztem działań wyprzedzających oraz pogarszającą się zdolność utrzymywania ciągłości funkcji publicznych[34]. Trudno uchwycić te zjawiska w sposób prosty i jednowymiarowy, jednak ich systematyczne występowanie może świadczyć o tym, że państwo formalnie zachowuje sterowność, lecz traci odporność rozumianą jako zdolność działania pod presją.

Trzeci poziom obejmuje wymiar informacyjny, którego znaczenie dla bezpieczeństwa wewnętrznego wyraźnie wzrosło w warunkach wysokiej fragmentacji komunikacyjnej i środowiska nasyconego dezinformacją. W proponowanym modelu poziom ten oprócz obecności fałszywych treści obejmuje szerzej: osłabienie wiarygodności komunikacji, wzrost rozbieżności interpretacyjnych dotyczących podstawowych faktów, narastanie chaosu narracyjnego, ograniczenie zdolności instytucji do utrzymania wspólnej płaszczyzny komunikacyjnej oraz zwiększoną podatność opinii publicznej na destabilizujące przekazy[35]. Z punktu widzenia odporności państwa problemem nie jest samo istnienie konkurencyjnych narracji – jest nim raczej sytuacja, w której państwo traci zdolność do skutecznego komunikowania sensu własnych działań oraz do utrzymywania minimalnej płaszczyzny porozumienia niezbędnej dla odpowiedniego poziomu koordynacji społecznej.

Wartość proponowanej ramy polega na próbie integracji trzech wskazanych katalogów zjawisk. Zgodnie z logiką modelu pojedynczy sygnał ostrzegawczy nie powinien być interpretowany jako wystarczający dowód erozji odporności państwa. Znaczenie analityczne zyskuje dopiero układ, w którym symptomy z różnych poziomów występują równolegle, utrzymują się w czasie i zaczynają się wzajemnie wzmacniać[36]. Przykładowo: spadek zaufania społecznego może nie mieć jeszcze istotnych skutków systemowych, jeśli instytucje zachowują wysoką sprawność i zdolność komunikacyjną. Gdy jednak towarzyszy mu przeciążenie organizacyjne oraz narastający chaos informacyjny, wzrasta

[34] A. Boin i in., *The Politics of Crisis Management*…, s. 25–42.

[35] RAND Corporation, *Truth Decay*…, s. 1–18.

[36] OECD, *Boosting Resilience*…, s. 35–39.

prawdopodobieństwo wejścia państwa w fazę obniżonej odporności. Model jest zatem relacyjny i sekwencyjny – służy do obserwacji konfiguracji, nie zaś do punktowania zjawisk.

Z metodologicznego punktu widzenia oznacza to potrzebę traktowania wskaźników jako elementów układu wczesnego rozpoznawania. Proponowana rama może być wykorzystywana zarówno do analizy porównawczej, jak i do interpretacji procesów zachodzących wewnątrz jednego państwa w dłuższej perspektywie czasowej[37]. Jej przydatność polega przede wszystkim na tym, że porządkuje obserwację zjawisk, które często są analizowane oddzielnie – zaufania społecznego, sprawności instytucjonalnej i komunikacji między władzą a społeczeństwem – mimo że w praktyce pozostają one współzależne.

Należy przy tym zaznaczyć ograniczenia modelu. Po pierwsze, nie jest on narzędziem prognostycznym w sensie ścisłym i nie pozwala przewidywać konkretnych zdarzeń. Po drugie, jego zastosowanie wymaga ostrożności przy interpretacji, ponieważ na część wskaźników mogą wpływać konteksty polityczny, kulturowy i sytuacyjny[38]. Po trzecie, model nie ma charakteru wdrożeniowego ani operacyjnego. Nie stanowi propozycji systemu dla służb, lecz próbę stworzenia uporządkowanej ramy badawczej, która może wspierać bardziej wnikliwe i wielowymiarowe rozpoznawanie procesów osłabiających odporność państwa.

Zadaniem proponowanej ramy analitycznej jest uzupełnienie istniejących instrumentów analitycznych o perspektywę, która pozwala traktować bezpieczeństwo wewnętrzne jako zdolność nie tylko do reagowania na kryzys, lecz także do rozpoznawania tego, że państwo zaczyna słabnąć, zanim stanie się to wyraźnie dostrzegalne.

Wielka Brytania i Polska jako dwa środowiska testowe

W odniesieniu do ram teoretycznych dodatkową zaletą proponowanego modelu analitycznego jest to, że można go postrzegać zarówno jako koncepcję, jak i proces interpretacji stosowany w rzeczywistych kontekstach państwowych. Można to zrobić przez porównanie dwóch przypadków: Wielkiej Brytanii i Polski. Oba kraje są członkami tego samego kręgu instytucjonalnego Zachodu, mają wysoką ekspozycję na zakłócenia informacyjne i geopolityczne, a jednocześnie mają różne wzorce/układy relacji między społeczeństwem, państwem a strukturami administracyjnymi. To zestawienie nie jest pełnym badaniem porównawczym – służy ilustracji działania modelu.

[37] A. Wildavsky, *Searching for Safety*…, s. 77–91.

[38] *Designing Resilience*…, s. 15–18; RAND Corporation, *Truth Decay*…, s. 45–51.

W przypadku Wielkiej Brytanii szczególnie widoczne są symptomy erozji odporności rozłożone na wszystkich trzech poziomach analizy. W wymiarze społecznym na znaczeniu zyskały długotrwałe skutki napięć związanych z brexitem, które utrwaliły wysoki stopień polaryzacji i osłabiły część mechanizmów integracyjnych[39]. Dodatkowym czynnikiem obciążającym była pandemia COVID-19, która wystawiła na próbę zarówno zdolność instytucji publicznych do koordynacji, jak i poziom społecznego zaufania do podejmowanych przez nie decyzji[40]. Dane z ostatnich lat wskazują, że zaufanie do rządu i części instytucji pozostaje niestabilne, a system ochrony zdrowia, samorządy i niektóre usługi publiczne funkcjonują pod znaczną presją organizacyjną[41]. W proponowanym modelu oznacza to współwystępowanie sygnałów na poziomach społecznym i instytucjonalnym: nie tyle jawny kryzys, ile obniżony poziom odporności wynikający z kumulacji napięć.

Na poziomie informacyjnym Wielka Brytania to państwo o wysokim stopniu pluralizmu komunikacyjnego, który w warunkach silnej fragmentacji komunikacyjnej może utrudniać spójną interpretację działań państwa przez społeczeństwo. Nie chodzi tu o samo istnienie sporu publicznego, lecz o trwałe osłabienie zdolności komunikacji instytucjonalnej do porządkowania sytuacji kryzysowej i redukowania niepewności. Z perspektywy proponowanej ramy analitycznej Wielka Brytania ilustruje zatem model erozji odporności o charakterze rozproszonym: państwo formalnie zachowuje wysoką funkcjonalność, lecz jednocześnie wykazuje symptomy przeciążenia, spadku przewidywalności i ograniczonej zdolności do reintegracji społecznej po okresach napięcia[42].

Polska prezentuje odmienny wzorzec, ale równie interesujący pod względem analitycznym. Na poziomie społecznym widoczna jest relatywnie wysoka zdolność do mobilizacji zbiorowej w sytuacjach granicznych, czego przykładami były reakcje społeczne na kryzys pandemiczny, wzrost liczby Ukraińców przybywających do Polski czy lokalne formy samoorganizacji w obrębie wspólnot[43]. Ten komponent mobilizacyjny należy uznać za istotny zasób odporności państwa[44]. Jednocześnie jednak dane

[39] S.B. Hobolt, T.J. Leeper, J. Tilley, *Divided by the Vote: Affective Polarization in the Wake of the Brexit Referendum*, „British Journal of Political Science" 2021, t. 51, nr 4, s. 1476–1493.

[40] UK Parliament, House of Commons, *Coronavirus: Lessons Learned to Date*, https://committees.parliament.uk/publications/7496/documents/78687/default/, s. 7–18 [dostęp: 26 III 2026].

[41] OECD, *Government at a Glance 2023*…, s. 145–152; *Public opinions and social trends, Great Britain*, Office for National Statistics, 20 IX 2024 r., https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/publicopinionsandsocialtrendsgreatbritain/august2024 [dostęp: 26 III 2026].

[42] Institute for Government, *Performance Tracker 2024*, London 2024, s. 9–22.

[43] J. Domaradzki i in., *Volunteering in the Front Line of the Ukrainian Refugee Crisis: A Brief Report from Poland*, „Frontiers in Public Health" 2022, t. 10, s. 1–11. https://doi.org/10.3389/fpubh.2022.979751.

[44] OECD, *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex*

dotyczące zaufania do instytucji publicznych oraz jakość debaty publicznej wskazują na obecność napięć, które w dłuższej perspektywie mogą ograniczać trwałość tego zasobu. W proponowanym modelu oznacza to sytuację, w której zdolność do mobilizacji nie zawsze idzie w parze z wysokim poziomem zaufania instytucjonalnego.

Na poziomie instytucjonalnym Polska wykazuje cechy systemu zdolnego do relatywnie szybkiej reakcji w warunkach presji, ale zarazem narażonego na przeciążenia w zakresie koordynacji działań i ich ograniczoną przewidywalność między różnymi segmentami administracji publicznej[45]. Z punktu widzenia odporności oznacza to, że system może być skuteczny w trybie reakcji, lecz mniej stabilny w wymiarze rozciągniętej w czasie adaptacji. W odniesieniu do bezpieczeństwa wewnętrznego ma to zasadnicze znaczenie, ponieważ państwo odporne powinno zarówno odpowiadać na zagrożenie, jak i utrzymywać spójność działania i społeczną legitymizację w okresach zwiększonego napięcia.

Także wymiar informacyjny wskazuje na odmienny niż brytyjski, lecz równie istotny wzorzec podatności. Polska przestrzeń komunikacyjna cechuje się wysoką dynamiką konfliktu interpretacyjnego oraz silnym wpływem przekazów tożsamościowych i polaryzacyjnych[46]. Z punktu widzenia proponowanej ramy analitycznej nie oznacza to automatycznie niskiej odporności, ale zwiększa ryzyko sytuacji, w której nawet racjonalne i poprawne działania państwa mogą być odbierane w sposób silnie zróżnicowany, co ogranicza zdolność do budowania spójnej reakcji społecznej.

Wielka Brytania i Polska reprezentują dwa różne profile odporności. Wielka Brytania ujawnia symptomy erozji w postaci długotrwałego przeciążenia systemu i rozproszonej utraty spójności społecznej i instytucjonalnej. Polska wykazuje większą gotowość mobilizacyjną i zdolność reagowania sytuacyjnego, ale równocześnie pozostaje wrażliwa na napięcia związane z ograniczoną stabilnością zaufania instytucjonalnego i wysoką polaryzacją w komunikacji[47]. W obu przypadkach wartość proponowanej ramy analitycznej objawia się w tym, że pozwala uchwycić nie tyle ogólną „siłę" lub „słabość" państwa, ile konfigurację czynników, które mogą w dłuższej perspektywie wzmacniać lub osłabiać jego odporność.

Policy Environment, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf, s. 17–29 [dostęp: 26 III 2026].

[45] OECD, *Government at a Glance 2023*…, s. 153–158; OECD, *OECD Survey on Drivers of Trust*…, s. 31–41.

[46] *Dokument roboczy służb Komisji. Sprawozdanie na temat praworządności z 2024 r.*, SWD(2024) 821 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52024SC0821, s. 4–11 [dostęp: 26 III 2026].

[47] OECD, *Government at a Glance 2023*…, s. 145–158; Institute for Government, *Performance Tracker 2024*…, s. 23–29.

Implikacje dla systemu bezpieczeństwa wewnętrznego – znaczenie analizy wieloźródłowej i procesowej dla państwa

Przyjęcie perspektywy procesowej wobec odporności państwa prowadzi do istotnej zmiany sposobu myślenia o bezpieczeństwie wewnętrznym. Konwencjonalne pojęcie systemu bezpieczeństwa koncentruje się na wykrywaniu zagrożeń, które stały się zauważalne na poziomie operacyjnym (incydenty, akty przemocy, awarie lub inne wymagające reakcji). Jest to nadal kluczowe podejście, ale nie wystarcza dla procesów rozwijających się stopniowo i niekoniecznie natychmiastowo objawiających się w formie jawnego kryzysu. Na poziomie makro oznacza to, że państwo musi uzupełnić działania reaktywne długoterminowym nadzorem. Konieczne jest monitorowanie procesu w celu wykrycia trendów, które osłabiają zdolność do działania, zanim skutki takich działań będą bezpośrednio odczuwalne[48].

Znaczenie takiego podejścia wynika z samej natury współczesnych zagrożeń. Wiele z nich nie jest skutkiem pojedynczego zdarzenia, lecz rezultatem długotrwałego nakładania się czynników społecznych, organizacyjnych i informacyjnych. W takich warunkach analiza skoncentrowana wyłącznie na incydencie może trafnie opisać moment kryzysowy, ale nie zawsze pozwala uchwycić warunki, które ten kryzys umożliwiły lub pogłębiły. Monitorowanie długoterminowych procesów staje się zatem zasadniczym elementem dla rozpoznawania podatności systemowej[49]. W praktyce oznacza to większą wrażliwość analityczną na zjawiska rozproszone, o niskim natężeniu i pozornie nieistotne, które dopiero w konfiguracji nabierają znaczenia strategicznego.

Z tego względu szczególnie istotna staje się analiza wieloźródłowa. Procesy erozji odporności państwa nie są bowiem widoczne wyłącznie w jednym typie danych ani w obrębie jednego sektora administracyjnego. Ich rozpoznawanie wymaga łączenia informacji dotyczących nastrojów społecznych, zaufania do instytucji, wydolności organizacyjnej struktur publicznych, jakości komunikacji między władzą a społeczeństwem oraz dynamiki środowiska informacyjnego[50]. Istotą nie jest przy tym maksymalizacja ilości danych, lecz ich odpowiednie zestawianie i interpretowanie. Dopiero perspektywa integrująca pozwala odróżnić przejściowe zakłócenie od bardziej trwałego osłabienia odporności.

Tego rodzaju podejście ma również znaczenie dla planowania strategicznego. Jeżeli bezpieczeństwo wewnętrzne ma obejmować także zdolność do neutralizacji zagrożenia i utrzymania sprawności w warunkach napięcia, to planowanie nie może

[48] OECD, *Boosting Resilience*…, s. 21–34.

[49] A. Boin i in., *The Politics of Crisis Management*…, s. 25–42.

[50] OECD, *Government at a Glance 2023*…, s. 17–24.

ograniczać się do scenariuszy kryzysowych rozumianych jako reakcja na wydarzenie. Powinno obejmować również analizę warunków, w których państwo wchodzi w sytuację zakłócenia – a więc ocenę, czy dysponuje wystarczającym poziomem zaufania społecznego, koordynacji instytucjonalnej i zdolności komunikacyjnej[51]. W tym sensie analiza odporności nie konkuruje z klasycznym planowaniem bezpieczeństwa, lecz je pogłębia, przesuwając uwagę z samego „co się wydarzy?" na równie istotne pytanie: „w jakim stanie będzie państwo w momencie mierzenia się z wyzwaniami?".

Taka perspektywa procesowa ma ponadto znaczenie dla zarządzania odpornością instytucjonalną, ponieważ traktuje sprawność państwa jako zasób wymagający obserwacji, wzmacniania i okresowego korygowania. W obliczu współczesnych zagrożeń instytucje publiczne funkcjonują w środowisku permanentnej presji – informacyjnej, organizacyjnej, społecznej i geopolitycznej. W takich warunkach odporność instytucjonalna zależy zarówno od procedur i kompetencji formalnych, jak i od zdolności uczenia się, adaptacji i utrzymywania spójności działania w czasie[52]. Rozpoznawanie symptomów erozji może więc pełnić funkcję nie tyle alarmową, ile stabilizującą – umożliwiając wczesne dostrzeżenie obszarów wymagających skorygowania, zanim dojdzie do pełnej materializacji zagrożenia.

Zaproponowana w niniejszym artykule rama analityczna nie stanowi gotowego rozwiązania wdrożeniowego ani nie rości sobie prawa do zastąpienia istniejących instrumentów oceny ryzyka. Jej wartość polega na uporządkowaniu perspektywy obserwacyjnej oraz na wskazaniu, że bezpieczeństwo wewnętrzne państwa wymaga równoczesnego uwzględniania procesów społecznych, instytucjonalnych i informacyjnych. Dla systemu bezpieczeństwa oznacza to potrzebę rozwijania kultury analitycznej bardziej wrażliwej na zjawiska rozciągnięte w czasie, mniej widowiskowe, lecz często ważniejsze pod względem strategicznym niż pojedyncze incydenty[53]. W tym sensie analiza procesowa nie stanowi alternatywy dla klasycznego myślenia o bezpieczeństwie, lecz jego konieczne dopełnienie.

Podsumowanie i wnioski

Celem niniejszego artykułu było zaproponowanie ramy analitycznej umożliwiającej wczesne rozpoznawanie procesów erozji odporności państwa w kontekście bezpieczeństwa wewnętrznego. Założono, że współczesne państwa dysponują coraz bardziej rozwiniętymi instrumentami reagowania na zdarzenia gwałtowne, mniej

[51] *Designing Resilience*…, s. 7–18.

[52] D.D. Woods, *Four Concepts for Resilience*…, s. 5–9.

[53] OECD, *Boosting Resilience*…, s. 35–39.

zaawansowane natomiast pozostają narzędzia służące identyfikowaniu procesów stopniowo osłabiających zdolność państwa do działania. Przeprowadzona analiza pozwala uznać hipotezę roboczą za zasadną: erozja odporności państwa może być rozpoznawana przed wystąpieniem kryzysu jawnego, o ile analiza bezpieczeństwa uwzględnia nie tylko incydenty, lecz także symptomy skumulowanego osłabienia na poziomach społecznym, instytucjonalnym i informacyjnym.

Bezpieczeństwo wewnętrzne nie jest wyłącznie funkcją siły państwa w zakresie reagowania. O jego realnym poziomie współdecyduje również jakość relacji państwo–społeczeństwo, zdolność instytucji do działania pod presją oraz możliwość utrzymania podstawowej spójności w zakresie komunikacji i organizacji. W tym sensie erozja odporności państwa stanowi problem bezpieczeństwa wewnętrznego, ponieważ stopniowo zmniejsza margines bezpieczeństwa i ogranicza zdolność adaptacyjną państwa w obliczu zakłóceń[54].

Zaproponowana w artykule rama analityczna ma charakter pomocniczy i porządkujący. Jej podstawowa użyteczność zawiera się w możliwości uchwycenia konfiguracji zjawisk, które w klasycznych modelach bezpieczeństwa bywają analizowane oddzielnie. Ujęcie społeczne, instytucjonalne i informacyjne pozwala spojrzeć na odporność państwa jako na układ współzależnych zasobów i podatności, a nie jednowymiarową cechę podmiotu publicznego. Porównanie Wielkiej Brytanii i Polski pokazało, że model ten może być użyteczny również w odniesieniu do interpretacji różnych środowisk instytucjonalnych.

Ze względu na ograniczenia artykułu przedstawiona rama nie została poddana ścisłej walidacji empirycznej i nie stanowi modelu pomiarowego. Ponadto część zaproponowanych wskaźników ma charakter pośredni i kontekstowy, co oznacza, że ich interpretacja wymaga ostrożności oraz uwzględnienia specyfiki danego państwa i momentu historycznego. Poza tym autor świadomie nie wnika w poziomy operacyjny ani wdrożeniowy, ponieważ celem artykułu było sformułowanie propozycji analitycznej, a nie projektowanie konkretnego instrumentu instytucjonalnego[55].

Dalsze badania nad modelem powinny zmierzać w trzech kierunkach. Po pierwsze, zasadne wydaje się rozwinięcie bardziej precyzyjnego zestawu wskaźników, możliwych do obserwacji porównawczej w dłuższej perspektywie czasowej. Po drugie, celowe byłoby sprawdzenie przydatności zaproponowanej ramy w analizie wybranych kryzysów państwowych i sytuacji granicznych. Po trzecie, wartościowym kierunkiem pozostaje pogłębienie relacji między kapitałem społecznym, sprawnością instytucjonalną i odpornością bezpieczeństwa państwa jako wspólnego pola badawczego[56].

[54] OECD, *Boosting Resilience*…, s. 35–39.

[55] *Designing Resilience*…, s. 15–18.

[56] OECD, *Trust and Public Policy*…, s. 47–53.

Wnioskiem końcowym pozostaje zatem potrzeba przesunięcia części uwagi analitycznej z samej reakcji na kryzys ku wczesnemu rozpoznawaniu warunków, w których państwo staje się mniej odporne. To właśnie ta zmiana perspektywy – od incydentu do procesu – może być użytecznym uzupełnieniem współczesnej refleksji nad bezpieczeństwem wewnętrznym.

Bibliografia

Boin A., 't Hart P., Stern E., Sundelius B., *The Politics of Crisis Management. Public Leadership under Pressure*, Cambridge 2017. https://doi.org/10.1017/9781316339756.

Chan J., *Social Cohesion and the Governance of Public Order*, w: *Social Capital and Public Policy*, D. Halpern (red.), Cambridge 2005, s. 145–162.

Designing Resilience. Preparing for Extreme Events, L. Comfort, A. Boin, C.C. Demchak (red.), Pittsburgh 2010.

Domaradzki J., Walkowiak D., Bazan D., Baum E., *Volunteering in the Front Line of the Ukrainian Refugee Crisis: A Brief Report from Poland*, „Frontiers in Public Health" 2022, t. 10, s. 1–11. https://doi.org/10.3389/fpubh.2022.979751.

Fukuyama F., *Trust. The Social Virtues and the Creation of Prosperity*, New York 1995.

Hobolt S.B., Leeper T.J., Tilley J., *Divided by the Vote: Affective Polarization in the Wake of the Brexit Referendum*, „British Journal of Political Science" 2021, t. 51, nr 4, s. 1476–1493. https://doi.org/10.1017/S0007123420000125.

Holling C.S., *Resilience and Stability of Ecological Systems*, „Annual Review of Ecology and Systematics" 1973, nr 4, s. 1–23. http://dx.doi.org/10.1146/annurev.es.04.110173.000245.

Institute for Government, *Performance Tracker 2024*, London 2024.

Levi M., Stoker L., *Political Trust and Trustworthiness*, „Annual Review of Political Science" 2000, t. 3, s. 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475.

Lockwood D., *Social Integration and System Integration*, w: *Explorations in Social Change*, G.K. Zollschan, W. Hirsch, Houghton Mifflin (red.), Boston 1964, s. 244–257.

Putnam R.D., *Bowling Alone. The Collapse and Revival of American Community*, New York 2000.

Walker B., Salt D., *Resilience Thinking. Sustaining Ecosystems and People in a Changing World*, Washington 2006.

Wildavsky A., *Searching for Safety*, New Brunswick–Oxford 1988.

Woods D.D., *Four Concepts for Resilience and the Implications for the Future of Resilience Engineering*, „Reliability Engineering & System Safety" 2015, t. 141, s. 5–9. https://doi.org/10.1016/j.ress.2015.03.018.

Źródła internetowe

OECD, *Boosting Resilience through Innovative Risk Governance*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/05/boosting-resilience-through-innovative-risk-governance_g1g3fd76/9789264209114-en.pdf [dostęp: 26 III 2026].

OECD, *Government at a Glance 2023*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/government-at-a-glance-2023_da193b0d/3d5c5d31-en.pdf [dostęp: 26 III 2026].

OECD, *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [dostęp: 26 III 2026].

OECD, *Trust and Public Policy. How Better Governance Can Help Rebuild Public Trust*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/03/trust-and-public-policy_g1g74ea6/9789264268920-en.pdf [dostęp: 26 III 2026].

Public opinions and social trends, Great Britain, Office for National Statistics, 20 IX 2024 r., https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/publicopinionsandsocialtrendsgreatbritain/august2024 [dostęp: 26 III 2026].

RAND Corporation, *Building Resilience to Systemic Risks. A Review of the Literature*, Santa Monica 2021.

RAND Corporation, *Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica 2018.

UK Parliament, House of Commons, *Coronavirus: Lessons Learned to Date*, https://committees.parliament.uk/publications/7496/documents/78687/default/ [dostęp: 26 III 2026].

Inne dokumenty

Dokument roboczy służb Komisji. Sprawozdanie na temat praworządności z 2024 r., SWD(2024) 821 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52024SC0821 [dostęp: 26 III 2026].

Dr inż. Radosław Korda

Doktor nauk społecznych, inżynier, były oficer Wojska Polskiego oraz były funkcjonariusz Metropolitan Police w Londynie. Od wielu lat mieszka i pracuje w Wielkiej Brytanii, łącząc działalność zawodową z badaniami nad bezpieczeństwem państwa, odpornością instytucjonalną oraz procesami społecznymi zachodzącymi w Europie. Jego zainteresowania naukowe koncentrują się wokół bezpieczeństwa wewnętrznego, kapitału społecznego, zarządzania kryzysowego oraz relacji między społeczeństwem a instytucjami publicznymi. W swoich badaniach wykorzystuje również wieloletnie doświadczenia związane z funkcjonowaniem brytyjskiego środowiska polonijnego oraz procesami migracyjnymi. Autor publikacji naukowych poświęconych problematyce bezpieczeństwa, odporności państwa i problemów społecznych, w tym monografii dotyczących długoterminowych procesów społecznych i instytucjonalnych.

Kontakt: radek.korda@gmail.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 113–134
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.025.24174

ARTYKUŁ

Państwo Islamskie w Chorasanie a potencjalne zagrożenie dla bezpieczeństwa Polski

The Islamic State in Khorasan and a potential threat to Poland's security

ŁUKASZ CYMBALUK

Wyższa Szkoła Kształcenia Zawodowego
https://orcid.org/0000-0003-1868-3869

Abstrakt

W artykule przedstawiono zarys działalności Państwa Islamskiego w Chorasanie (ang. Islamic State in Khorasan, IS-K), a także opisano ideologię oraz cele tej organizacji. Autor podjął próbę identyfikacji potencjalnych zagrożeń, jakie może ona stwarzać dla bezpieczeństwa Rzeczypospolitej Polskiej. Mimo że Polska nie znajduje się w centrum zainteresowania IS-K, to w ramach dżihadystycznej ideologii tego ugrupowania jest klasyfikowana – z uwagi na przynależność do szeroko pojętego Zachodu – jako jeden z tzw. wrogów dalekich. Organizacja może podejmować działania przede wszystkim w takich obszarach, jak: tworzenie sieci operacyjnych, rekrutacja, rozbudowa bazy członkowskiej czy pozyskiwanie funduszy. Równocześnie nie można wykluczyć spontanicznych przypadków radykalizacji (a nawet ataków inspirowanych propagandą IS-K), które mogą wystąpić bez bezpośrednich powiązań z przedstawicielami grupy. Otwarte pozostaje również pytanie, w jakim stopniu bieżące procesy migracyjne mogą w istocie generować zagrożenie ze strony IS-K oraz w jaki sposób ugrupowanie może być wykorzystywane przez aktorów zewnętrznych do realizacji własnych celów politycznych.

Słowa kluczowe Państwo Islamskie w Chorasanie, IS-K, filie Państwa Islamskiego, bezpieczeństwo Polski, rewolucyjny salafizm, radykalizm islamski, terroryzm

Abstract The article describes an outline of the activities of the Islamic State in Khorasan (IS-K), as well as the ideology and objectives of the organisation. The author attempted to identify potential threats it might pose to Poland's security. Although Poland is not the focus of the IS-K's attention, within the framework of the group's jihadist ideology it is classified – by virtue of its affiliation with the West in the broadest sense – as one of the distant enemies. The organisation may take action primarily in areas such as: establishment of operational networks, recruitment, expanding the membership base and fundraising. At the same time, spontaneous cases of radicalisation (even attacks inspired by the IS-K propaganda), which may occur without any direct links to the representatives of the group, cannot be ruled out. It also remains to be seen to what extent the current migration processes might in fact pose a threat from the IS-K, and how the group might be exploited by the external actors to achieve its own political objectives.

Keywords Islamic State in Khorasan, IS-K, Islamic State affiliates, Poland's security, revolutionary Salafism, Islamic radicalism, terrorism

Wprowadzenie

Porażka militarna w Iraku i Syrii oraz utrata zdobyczy terytorialnych nie oznaczały końca istnienia Państwa Islamskiego[1]. Po śmierci Abu Bakr al-Baghdadiego

[1] W tekstach naukowych i publicystycznych często pojawia się określenie tzw. Państwo Islamskie. Ma to podkreślać, że organizacja nie powinna być traktowana jako pełnoprawny podmiot państwowy. Warto jednak zaznaczyć, że od momentu proklamacji kalifatu (29 czerwca 2014 r.) Państwo Islamskie to w istocie nazwa własna ugrupowania. Stosowanie takiego nazewnictwa nie oznacza, że ma ono odzwierciedlenie w rzeczywistości (Państwo Islamskie miało następujące elementy państwowości – suwerenną władzę, ludność oraz terytorium, nie spełniało natomiast kryterium w postaci zdobycia uznania międzynarodowego). Z kolei w odniesieniu do organizacji omawianej w niniejszym artykule właściwym nazewnictwem powinno być Państwo Islamskie w Chorasanie (ang. Islamic State in Khorasan – IS-K lub też Islamic State Khorasan Province, ISKP). Skrót ISIS-K odwołuje się

27 października 2019 r.[2] stanowisko kalifa przejmowali kolejni dżihadyści[3], organizacja zaś – choć niemal irrelewantna w wymiarze lokalnym – nie zniknęła całkowicie z krajobrazu syryjskiej wojny domowej. Ugrupowanie zmieniło strategię i kontynuowało działalność jako globalna sieć terrorystyczna[4].

Istotne jest to, że jeszcze w czasie funkcjonowania kalifatu, czyli struktury politycznej opartej na rygorystycznej interpretacji prawa szariackiego jako bytu o charakterze państwowym, swoje podporządkowanie wobec niego zadeklarowały liczne grupy dżihadystyczne z różnych rejonów świata[5]. W efekcie Państwo Islamskie powołało do życia komórki zewnętrzne oraz wilajaty, czyli prowincje, które dążyły do realizacji celów ideologicznych i strategicznych macierzystej organizacji. Filie kalifatu (tzw. lokalne franczyzy) powstały m.in. w: Libii, Algierii, Egipcie, Jemenie, Nigerii, Rosji (na Kaukazie), Strefie Gazy[6], Indiach (w Kaszmirze)[7] i choć część z nich straciła na znaczeniu lub została rozbita (przynajmniej według oficjalnych doniesień)[8], to niektóre nadal są aktywne. Większy zakres niezależności

do poprzedniej nazwy (de facto zniesionej w czerwcu 2014 r.) – Islamic State of Iraq and Syria (lub też Islamic State of Iraq and al-Sham, ISIS).

[2] Przywódca Państwa Islamskiego zginął podczas operacji amerykańskich sił specjalnych. Zob. M. Rubin, *Abu Bakr al-Baghdadi Is Dead (But His Legacy Lives on)*, The National Interest, 27 X 2019 r., https://nationalinterest.org/blog/middle-east-watch/abu-bakr-al-baghdadi-dead-his-legacy-lives-91536 [dostęp: 4 XII 2024].

[3] Obecnie (stan na 1 IX 2026 r.) organizacji przewodzi Abu Hafs al-Hashimi al-Qurashi, który 3 sierpnia 2023 r. został ogłoszony piątym kalifem. Zob. *ISIL confirms death of leader Abu Hussein al-Qurashi, names successor*, Al Jazeera, https://www.aljazeera.com/news/2023/8/3/isil-confirms-death-of-leader-abu-hussein-al-qurashi-names-successor [dostęp: 1 IX 2026].

[4] Państwo Islamskie wciąż jest uważane za najniebezpieczniejszą organizację terrorystyczną na świecie. Zob. *Global Terrorism Index 2026*, https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf, s. 4 [dostęp: 21 VIII 2026].

[5] Do końca 2015 r. wierność Państwu Islamskiemu zadeklarowało ponad 40 grup terrorystycznych. W kolejnym roku filie kalifatu znajdowały się w 28 różnych państwach. Zob. *Global Terrorism Index 2016*, Institute for Economics and Peace, https://www.reliefweb.int/report/world/global-terrorism-index-2016, s. 2 [dostęp: 4 XII 2024]. W 2019 r. Państwo Islamskie zarządzało przynajmniej 19 komórkami.

[6] Na temat poszczególnych prowincji Państwa Islamskiego zob. szerzej: K. Leigh, J. French, J. Juan, *Islamic State and Its Affiliates*, The Wall Street Journal, http://graphics.wsj.com/islamic-state-and-its-affiliates [dostęp: 4 XII 2024]; B. Rahmani, A. Tanco, *ISIS's Growing Caliphate: Profiles of Affiliates*, Wilson Center, 19 II 2016 r., https://www.wilsoncenter.org/article/isiss-growing-caliphate-profiles-affiliates [dostęp: 4 XII 2024].

[7] *ISIL claims 'province' in India, officials call it 'propaganda'*, Al Jazeera, 12 V 2019 r., https://www.aljazeera.com/news/2019/5/12/isil-claims-province-in-india-officials-call-it-propaganda [dostęp: 4 XII 2024].

[8] Jako przykład pokonanych i rozbitych prowincji można wskazać filie Państwa Islamskiego w Libii.

prowincji po śmierci al-Baghdadiego oznacza bardziej rozproszony, sieciowy i niejawny charakter działań organizacji wiernych koncepcji Państwa Islamskiego.

Celem artykułu jest wskazanie obszarów potencjalnych zagrożeń, jakie to ugrupowanie może stwarzać dla bezpieczeństwa Polski. Przeprowadzona przez autora analiza przejawów aktywności Państwa Islamskiego w Chorasanie (ang. Islamic State in Khorasan, IS-K) została dokonana na podstawie dostępnego piśmiennictwa, raportów, a także publikacji i źródeł internetowych. W objaśnianiu działań oraz specyfiki IS-K istotną rolę odgrywają analogie do aktywności macierzystej organizacji.

Państwo Islamskie w Chorasanie – zarys działalności

Jednym z wilajatów, który przetrwał i pomimo upadku kalifatu pozostaje aktywny, jest IS-K. Prowincja powstała w 2015 r. w efekcie konsolidacji głównie afgańskich i pakistańskich dżihadystów[9] rozczarowanych działaniami talibów[10]. Państwo Islamskie w Chorasanie prowadzi działalność przede wszystkim na obszarze wschodniego i północnego Afganistanu oraz północno-zachodniego Pakistanu, przy czym kontroluje bardzo niewielki obszar. Nazwa Chorasan[11] odnosi się do historycznego regionu w Azji Środkowej, obecnie rozciągającego się na niemal cały Afganistan, wschodni Iran oraz południowe części Turkmenistanu, Tadżykistanu i Uzbekistanu[12]. Należy dodać, że stosowanie takiego nazewnictwa podkreśla rewizjonistyczne dążenia organizacji, będące równocześnie wyrazem kontestacji zachodniej nomenklatury oraz granic państwowych narzuconych przez wrogów[13].

---

[9] Od początku istnienia prowincji istotną rolę w strukturach organizacji odgrywali walczący w Afganistanie Uzbecy (członkowie Islamskiego Ruchu Uzbekistanu i Islamskiej Unii Dżihadu), Ujgurzy, a później także Tadżycy i Beludżowie. Zob. K. Strachota, *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, Ośrodek Studiów Wschodnich, 29 III 2024 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu [dostęp: 20 XII 2024].

[10] Na temat procesu przyłączania się dżihadystów z poszczególnych ugrupowań zob. szerzej: D. Rassler, *Situating the Emergence of the Islamic State of Khorasan*, „CTC Sentinel" 2015, t. 8, nr 3, https://ctc.westpoint.edu/wp-content/uploads/2015/03/CTCSentinel-Vol8Issue317.pdf, s. 7–11 [dostęp: 20 XII 2024].

[11] Chorasan (arab. *Khorasan*) można tłumaczyć jako 'Kraj Wschodu' lub 'Tam, gdzie wschodzi słońce'. Zob. A. Taylor, *The strange story behind the 'Khorasan' group's name*, The Washington Post, 25 IX 2014 r., https://www.washingtonpost.com/news/worldviews/wp/2014/09/25/the-strange-story-behind-the-khorasan-groups-name [dostęp: 24 XII 2024].

[12] M.K. Sheikh, *Islamic State Enters Al-Qaeda's Old Hotbed: Afghanistan and Pakistan*, „Connections" 2017, t. 16, nr 1, s. 40. https://doi.org/10.11610/Connections.16.1.03. W niektórych opisach tego regionu historycznego uwzględnia się również część terytorium Pakistanu.

[13] IS-K kontynuuje praktykę unikania „zachodniego" nazewnictwa kojarzonego z kolonializmem

Państwo Islamskie w Chorasanie po raz pierwszy zyskało duży rozgłos za sprawą zamachu na lotnisku im. Hamida Karzaja w Kabulu. 26 sierpnia 2021 r. zamachowiec samobójca zdetonował ładunki wybuchowe podczas ewakuacji z Afganistanu ludności cywilnej i cudzoziemców, która nastąpiła po wyjściu z tego państwa amerykańskich sił i przejęcia władzy przez talibów[14]. Ugrupowanie przyznało się również do aktu terrorystycznego dokonanego 22 marca 2024 r. w Krasnogorsku w pobliżu Moskwy[15]. Grupa uzbrojonych napastników otworzyła ogień do publiczności zgromadzonej w hali koncertowej Crocus City Hall[16]. Był to pierwszy zamach przeprowadzony poza zasadniczym obszarem funkcjonowania IS-K, a zamachowcami byli głównie Tadżycy[17]. Wcześniejsza aktywność terrorystyczna wilajatu w Chorasanie koncentrowała się na terytorium Afganistanu (łączyła się z działaniami zbrojnymi wymierzonymi w talibów) i Pakistanu[18]. Ataki zasadniczo były wymierzone w cele cywilne i społeczność Hazarów wyznającą islam szyicki[19].

obecną w narracji i komunikatach Państwa Islamskiego, np. zamiast Arabia Saudyjska – Półwysep Arabski.

[14] W zamachu zginęło ponad 180 osób, w tym 13 amerykańskich żołnierzy i 28 członków Talibanu. Zob. *What we know about Islamic State in Khorasan Province (ISIS-K)*, Al Jazeera, 27 VIII 2021 r., https://www.aljazeera.com/news/2021/8/27/islamic-state-in-khorasan-iskp-aka-isil [dostęp: 3 I 2025]. IS-K przyznało się do zamachu w poście na Telegramie. Zob. *ISIL claims responsibility for deadly Kabul attack*, Al Jazeera, 3 IX 2024 r., https://www.aljazeera.com/news/2024/9/3/isil-claims-responsibility-for-deadly-kabul-attack [dostęp: 3 I 2025].

[15] IS-K przyznało się do zamachu za pośrednictwem swojego medium propagandowego Amaq Media Channel. Rosja współodpowiedzialnością za ten atak próbowała obarczyć Ukrainę. Zob. A.M. Dyner, *Zamach w Moskwie*, Polski Instytut Spraw Międzynarodowych, 25 III 2024 r., https://www.pism.pl/publikacje/zamach-w-moskwie [dostęp: 6 I 2025].

[16] Tamże. Był to największy zamach terrorystyczny w Rosji od czasu ataku na szkołę w Biesłanie w 2004 r. Warto wspomnieć, że Stany Zjednoczone informowały (za pośrednictwem ambasady w Moskwie) o możliwym ataku ze strony IS-K. Zob. G. Faulconbridge, *US embassy warns of imminent attack in Moscow by 'extremists'*, Reuters, 8 III 2024 r., https://www.reuters.com/world/us-embassy-warns-imminent-extremist-attack-moscow-2024-03-08 [dostęp: 6 I 2025]. Ostrzeżenie to zostało zignorowane przez Rosjan. W podobny sposób USA przekazały komunikat Iranowi przed innym atakiem IS-K – zamachem samobójczym w Kermanie, do którego doszło 3 stycznia 2024 r. podczas uroczystości upamiętniającej czwartą rocznicę śmierci generała Ghasema Solejmaniego (dowódcy sił specjalnych Korpusu Strażników Rewolucji Islamskiej). Zob. M.R. Gordon, V. Salama, W.P. Strobel, *U.S. Secretly Alerted Iran Ahead of Islamic State Terrorist Attack*, The Wall Street Journal, 26 I 2024 r., https://www.wsj.com/world/middle-east/u-s-secretly-alerted-iran-ahead-of-islamic-state-terrorist-attack-af77a19a [dostęp: 6 I 2025].

[17] M.L. de Miguel, *ISIS-K: A Reboot of Jihadist Terrorism?*, „Revista Seguridad y Poder Terrestre" 2024, t. 3, nr 2, s. 105. https://doi.org/10.56221/spt.v3i2.58.

[18] Ważniejsze ataki terrorystyczne ugrupowania krótko przedstawiono w: *Islamic State in Khorasan Province*, https://mappingmilitants.org/profiles/islamic-state-in-khorasan-province [dostęp: 21 VIII 2026].

[19] Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K) In Post Us Withdrawal Afghanistan*, „Journal

Dynamika działań operacyjnych grupy zmniejszyła się w drugiej połowie 2018 r. wraz z pierwszymi poważnymi porażkami w bezpośrednich starciach[20]. Do spadku ogólnego potencjału i liczby bojowników[21] organizacji, a także do utraty znacznej części kontrolowanych przez nią obszarów przyczyniły się intensywne operacje militarne prowadzone przez afgańskie siły, międzynarodową koalicję kierowaną przez Stany Zjednoczone[22] oraz talibów. W listopadzie 2019 r. ówczesny prezydent Afganistanu, Ashraf Ghani, ogłosił pokonanie IS-K w prowincji Nangarhar (w głównym bastionie ugrupowania)[23].

Państwo Islamskie w Chorasanie wznowiło swoje działania wraz z ponownym przejęciem władzy przez talibów w sierpniu 2021 r., jednak dalsze straty, narastające problemy z gromadzeniem funduszy[24] oraz destabilizacja na Bliskim Wschodzie w związku z rozpoczęciem konfliktu w Gazie spowodowały istotną zmianę w sposobie funkcjonowania grupy. Nowe podejście oznaczało rozpoczęcie

of Professional Research in Social Sciences" 2024, t. 11, nr 1, s. 234–237. https://doi.org/10.58932/MULA0028; *Afghanistan: ISIS Group Targets Religious Minorities*, Human Rights Watch, 6 IX 2022 r., https://www.hrw.org/news/2022/09/06/afghanistan-isis-group-targets-religious-minorities [dostęp: 8 I 2025].

[20] A. Giustozzi, *The Islamic State in Khorasan*, Italian Institute for International Political Studies, 27 VI 2019 r., https://www.ispionline.it/en/publication/islamic-state-khorasan-23406 [dostęp: 8 I 2025].

[21] Według niektórych szacunków IS-K w 2016 r. dysponowało 7000–8500 bojownikami. W drugiej połowie 2019 r. liczba rekrutów organizacji spadła do 5000. Zob. M.D. Mohammadi, *Islamic State in Khorasan Recruitment Tactics: Analysis of Push & Pull Factors*, Tarzi Research Foundation, April 2021, s. 9. https://doi.org/10.13140/RG.2.2.32271.71841. Na temat strat ponoszonych przez prowincję w Chorasanie zob. szerzej: A. Jadoon, A. Mines, *Taking Aim: Islamic State Khorasan's Leadership Losses*, „CTC Sentinel" 2019, t. 12, nr 8, https://ctc.westpoint.edu/wp-content/uploads/2019/09/CTC-SENTINEL-082019.pdf, s. 14–22 [dostęp: 8 I 2025].

[22] Jednym z bardziej znanych działań Stanów Zjednoczonych (choć raczej o znaczeniu symbolicznym) wymierzonych w IS-K był nalot z wykorzystaniem GBU-43/B MOAB (najpotężniejszej nieatomowej bomby w arsenale USA, tzw. matki wszystkich bomb) przeprowadzony w prowincji Nangarhar w kwietniu 2017 r. Było to pierwsze wykorzystanie tej broni w warunkach konfliktu zbrojnego. Zob. szerzej: *Afghanistan/US, 'Mother of all bombs'*, https://casebook.icrc.org/case-study/afghanistan-us-mother-all-bombs [dostęp: 9 I 2025].

[23] I. Ikram, A. Siddique, *Afghan President Declares IS Defeated In Eastern Stronghold*, Radio Free Europe/Radio Liberty, 19 XI 2019 r., https://gandhara.rferl.org/a/afghan-president-declares-is-defeated-in-eastern-stronghold/30280871.html [dostęp: 8 I 2025]. Warto dodać, że w obliczu porażki ponad 1400 bojowników IS-K poddało się afgańskim władzom. Zob. F. Bezhan, *The Taliban, The Government, And Islamic State: Who Controls What In Afghanistan?*, Radio Free Europe/Radio Liberty, 31 V 2020 r., https://www.rferl.org/a/taliban-government-islamic-state-who-controls-what-in-afghanistan-/30644646.html [dostęp: 8 I 2025].

[24] A. Giustozzi, *The Islamic State in Khorasan between Taliban counter-terrorism and resurgence prospects*, International Centre for Counter-Terrorism, 30 I 2024 r., https://www.icct.nl/publication/islamic-state-khorasan-between-taliban-counter-terrorism-and-resurgence-prospects [dostęp: 8 I 2025].

aktywności poza Afganistanem i próby przyciągnięcia sympatyków z pobliskich państw – Tadżykistanu, Uzbekistanu oraz Kirgistanu. W 2022 r. IS-K przeprowadziło dwa ataki rakietowe[25]. Pierwszy (z 18 kwietnia) był wymierzony w Uzbekistan, drugi (z 7 maja) – w Tadżykistan[26]. Poza wywołaniem napięć w regionie ataki miały na celu podważenie zdolności rządu talibów do utrzymania bezpieczeństwa oraz mobilizację ruchów dżihadystycznych obecnych w atakowanych państwach[27]. Jaskrawym przejawem strategii ukierunkowanej na operacje zewnętrzne był wspomniany już zamach w Krasnogorsku. Obranie za cel Rosji[28] nie było przypadkowe, gdyż w percepcji kalifatu (a co za tym idzie prowincji w Chorasanie) to państwo było jednym z ważniejszych adwersarzy organizacji. Wrogość Państwa Islamskiego wobec Rosji jest rezultatem zarówno okupacji Afganistanu w latach 80. XX w., interwencji w Czeczenii (postrzeganych jako przykłady prześladowania

[25] W obu przypadkach rakiety wystrzelono z terytorium Afganistanu.

[26] U. Botobekov, *New ISIS Strategy and the Resurgence of Islamic State Khorasan*, Modern Diplomacy, 17 V 2022 r., https://www.moderndiplomacy.eu/2022/05/17/new-isis-strategy-and-the-resurgence-of-islamic-state-khorasan [dostęp: 15 I 2025]; J.C.K. Daly, *Rocket Attacks on Tajikistan and Uzbekistan Undermine Taliban Security Claims*, Jamestown, 8 I 2022 r., https://jamestown.org/program/rocket-attacks-on-tajikistan-and-uzbekistan-undermine-taliban-security-claims [dostęp: 15 I 2025].

[27] Pojawienie się grup dżihadystycznych w Azji Centralnej (w Uzbekistanie, Tadżykistanie, Kirgistanie, Turkmenistanie oraz Kazachstanie) jest wynikiem pogorszenia się sytuacji ekonomicznej i poziomu edukacji po upadku Związku Radzieckiego, a także ogólnej korupcji i represji stosowanych przez reżimy autorytarne. Na temat genezy, specyfiki oraz przykładów organizacji salafickich z tego regionu zob. szerzej: U. Botobekov, *Think like Jihadist: Anatomy of Central Asian Salafi groups*, Modern Diplomacy, 29 V 2019 r., https://moderndiplomacy.eu/2019/05/29/think-like-jihadist-anatomy-of--central-asian-salafi-groups [dostęp: 17 I 2025]. Kluczowe znaczenie ma również zjawisko masowych migracji zarobkowych z państw regionu. Państwem docelowym jest głównie Rosja, gdzie alienacja społeczna, ułatwiony dostęp do treści radykalnych oraz wykluczenie i frustracje społeczne, a także przymuszanie do służby wojskowej sprawiają, że nasila się zjawisko radykalizacji wśród migrantów. Państwo Islamskie w Chorasanie wypracowało efektywne metody dotarcia do takich środowisk. Zob. szerzej: K. Strachota, *Państwo Islamskie Chorasanu…* Warto dodać, że według niektórych raportów to właśnie z Rosji (lub też byłych republik Związku Radzieckiego) pochodziło najwięcej zagranicznych bojowników (ang. *foreign fighters*), którzy zasilili szeregi Państwa Islamskiego w okresie funkcjonowania kalifatu. Zob. szerzej: R. Barrett, *Beyond The Caliphate: Foreign Fighters and the Threat of Returnees*, https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf, s. 10–11 [dostęp: 17 I 2025].

[28] Należy zaznaczyć, że atak terrorystyczny w Krasnogorsku nie był pierwszym zamachem IS-K wymierzonym w Rosję. We wrześniu 2022 r. IS-K dokonało zamachu na rosyjską ambasadę w Kabulu. Zob. *Afghanistan: Deadly suicide attack at Russian embassy in Kabul*, Al Jazeera, 5 IX 2022 r., https://www.aljazeera.com/news/2022/9/5/suicide-bomb-blast-near-russian-embassy-in-kabul-afghan-police [dostęp: 17 I 2025].

muzułmanów), jak i wspierania przez Moskwę innych przeciwników kalifatu – Iranu oraz reżimu Asada w Syrii[29].

Ideologia i cele Państwa Islamskiego w Chorasanie

Ideologia IS-K jest tożsama z ideologią Państwa Islamskiego – był to jeden z warunków sine qua non powołania nowej prowincji[30]. Ugrupowanie wpisuje się w ramy nurtu rewolucyjnego salafizmu (dżihadu salafickiego)[31], który postuluje powrót do pierwotnej formy islamu na drodze zbrojnej lub z wykorzystaniem przemocy w celu wyciągnięcia muzułmanów ze stanu ogólnego kryzysu – wtórnej dżahilijji. Odrzucenie przejawów „zepsucia" oraz ideologicznych „naleciałości", takich jak państwo świeckie, modernizm, nacjonalizm czy demokracja (traktowanych jako przejawy bałwochwalstwa – arab. *shirk*), ściśle łączy się z traktowaniem Koranu i Sunny jako wyłącznych źródeł prawa[32]. Należy przy tym podkreślić, że zarówno religia, jak i poszczególne jej elementy są w przypadku tej organizacji wykorzystywane instrumentalnie.

Istotne znaczenie w ideologii grupy[33] ma koncept kalifatu – bytu politycznego, w którym panuje powszechne prawo szariatu i materializują się wszelkie islamskie ideały. Taki stan rzeczy może być osiągnięty tylko za pomocą „metodologii prorockiej"[34], czyli dokładnego podążania za wzorcami wytyczonymi przez proroka. Dlatego też politycznym i społecznym punktem odniesienia, do którego zmierza

[29] S. Harmouch, A. Jadoon, *How Moscow terror attack fits ISIS-K strategy to widen agenda, take fight to its perceived enemies*, The Conversation, 24 III 2024 r., https://www.theconversation.com/how-moscow-terror-attack-fits-isis-k-strategy-to-widen-agenda-take-fight-to-its-perceived-enemies-226469 [dostęp: 17 I 2025].

[30] Państwo Islamskie określiło zakres kryteriów i wymagań, które musiała spełnić dana organizacja, aby móc utworzyć prowincję. Taka grupa – poza podzielaniem wizji ideologicznej kalifatu – musiała wyłonić ze swoich szeregów lidera, złożyć i udokumentować przysięgę wierności (arab. *bay'a*), a także przedstawić strategię dotyczącą kwestii militarnych i zarządzania kontrolowanymi obszarami. Zob. *Wilāyat Khurāsān And The Bay'āt From Qawqāz*, „Dabiq" 2015, nr 7, s. 35.

[31] Zob. szerzej: Q. Wiktorowicz, *Anatomy of the Salafi Movement*, „Studies in Conflict & Terrorism" 2006, t. 29, nr 3, s. 207–239. https://doi.org/10.1080/10576100500497004.

[32] Warto zaznaczyć, że poza salafizmem Państwo Islamskie w znacznym stopniu czerpało również z myśli wahabickiej. Przytoczone elementy ideowe wywodzą się w dużej mierze właśnie z wahabizmu – powstałego w XVIII w. nurtu w islamie sunnickim, który zakłada przede wszystkim rygorystyczne podejście do religii oraz dosłowną interpretację świętych tekstów.

[33] Ważniejsze komponenty ideologii IS-K zostały również krótko przedstawione w: Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K)*…, s. 218–219.

[34] G. Wood, *What ISIS Really Wants*, The Atlantic, March 2015, https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980 [dostęp: 27 I 2025].

Państwo Islamskie (oraz jego filie), jest twór państwowy założony przez Muhammada w VII w. n.e. wraz z obowiązującymi w nim zasadami. Dążenie do utworzenia kalifatu oznacza równocześnie rewizjonistyczny stosunek wobec obecnego porządku międzynarodowego.

Kolejnym kluczowym elementem ideologii IS-K jest dżihad rozumiany jednoznacznie jako walka zbrojna[35]. Ma on być narzędziem umożliwiającym ustanowienie kalifatu i osiągnięcie dominującej pozycji islamu w skali globalnej. Wymaga to zastosowania przemocy (w tym przeprowadzania zamachów terrorystycznych), traktowanej przez organizację jako działanie konieczne i uzasadnione religijnie. Równocześnie dżihad jest przedstawiany jako obowiązek, który powinien być realizowany zarówno przez jednostkę, jak i zbiorowość wiernych. Religijną powinnością każdego muzułmanina ma być podjęcie walki zbrojnej z wrogami kalifatu lub organizacja zamachów terrorystycznych w miejscu swojego zamieszkania.

Z dżihadem jako działaniem zbrojnym łączy się koncepcja koranicznej ekskomuniki (arab. *takfir*). Jest to wykluczanie ze wspólnoty religijnej jednostek lub grup, które dopuściły się ciężkiego grzechu. W zradykalizowanej interpretacji IS-K ekskomunika rozciąga się również na muzułmanów, którzy nie podzielają światopoglądu tej grupy[36]. W rezultacie organizacja legitymizuje stosowanie przemocy wobec szerokiej kategorii „odstępców" lub „apostatów" (arab. *murtadd*). Zaliczają się do nich członkowie innych odłamów religijnych (szczególnie przedstawiciele nurtu szyickiego), a także zwolennicy rządów w państwach muzułmańskich, w których nie obowiązuje „czyste" prawo szariatu.

Państwo Islamskie w Chorasanie przyjęło od organizacji centralnej również podział na tzw. wrogów dalekich i bliskich. Do wrogów dalekich należą wszelkie zewnętrzne siły, które zwalczają (w percepcji ugrupowania) islam czy też prowadzą opresyjną politykę wobec muzułmanów. Są to przede wszystkim: Stany Zjednoczone

[35] W swojej narracji Państwo Islamskie wyraźnie odrzucało inne niż walka i przemoc znaczenia dżihadu. Kalifat traktuje odejście od walki zbrojnej – a co za tym idzie również podział na dżihad większy (dżihad jako „wysiłek duchowy") i mniejszy (dżihad jako walka na rzecz obrony wspólnoty przed zagrożeniami zewnętrznymi) – jako rodzaj „reinterpretacji" tego pojęcia. Na ten temat zob. szerzej: *Islam Is The Religion Of The Sword Not Pacifism*, „Dabiq" 2015, nr 7, s. 20–24. Według Państwa Islamskiego włączenie się w dżihad jest obowiązkiem wiernych.

[36] Z praktyką *takfir* łączy się pojęcie *al-wala' wa-l-bara* – koncepcja rozgraniczenia dobra i zła (potocznie określana jako „miłość i nienawiść w imię Allaha"), w której religia jest elementem wyraźnie oddzielającym wspólnotę od niewierzących. Zob. A.N. Celso, *Islamic Regression, Jihadist Frustration and Takfirist Hyper Violence*, „Journal of Political Sciences & Public Affairs" 2016, t. 4, nr 2, https://www.longdom.org/open-access/islamic-regression-jihadist-frustration-and-takfirist-hyper-violence-2332-0761-1000200.pdf, s. 2 [dostęp: 27 I 2025]. https://doi.org/10.4172/2332-0761.1000200. W przypadku ideologii Państwa Islamskiego i jego komórek podział występuje pomiędzy wąsko określoną grupą „prawdziwych" wyznawców a licznymi wrogami islamu.

(oraz ich państwa sojusznicze), Izrael, Chiny, a także Rosja i Iran[37]. W grupie wrogów bliskich znajdują się państwa, których rządy – choć tworzone przez muzułmanów – są postrzegane z powodu swoich powiązań z Zachodem jako bezbożne, oraz mniejszości religijne.

Istotny jest również fakt, że IS-K jako wrogów bliskich postrzega obecną, tworzoną przez talibów władzę w Afganistanie oraz powiązaną z nią Al-Kaidę. Cele organizacji w skali lokalnej to przede wszystkim delegitymizacja i podważenie pozycji Talibanu, a w konsekwencji pozbawienie ich władzy oraz utworzenie własnego kalifatu na terytorium Afganistanu[38]. Państwo Islamskie w Chorasanie krytykuje talibów za zbyt liberalne podejście do wdrażania szariatu oraz za odejście od zasad dżihadu przez działania na rzecz zdobycia uznania międzynarodowego[39]. Tendencje o nacjonalistycznym charakterze oraz powiązania ze Stanami Zjednoczonymi[40] (chociażby wspólne zwalczanie sił IS-K) sprawiają, że ugrupowanie postrzega afgański rząd w kategorii „apostatów" czy też jako pionka Zachodu. Z kolei konflikt z Al-Kaidą ma podłoże historyczne, ideologiczno-doktrynalne, a nawet generacyjne[41]. Organizacje rywalizują bowiem nie tylko o wpływy lokalne czy zasoby

[37] W narracji Państwa Islamskiego (w nr. 15 magazynu „Dabiq") pojawił się komentarz dotyczący obszernej listy wrogów, która wraz z podmiotami walczącymi z kalifatem w sposób potajemny rozciąga się de facto na wszystkie państwa świata. Zob. szerzej: *From the Battles of Al-Ahzāb to the War of Coalitions*, „Dabiq" 2015, nr 11, s. 47–48. Można zatem założyć, że IS-K kontynuująca tradycje organizacji centralnej również przyjmuje taką perspektywę, co oznacza, że traktuje jako wroga także Polskę (przynajmniej deklaratywnie).

[38] S. Coppolecchia, *Unveiling ISIS-K: Origins, Goals And Possible Impact*, Instituto Analisi Relazioni Internazionali, 6 IV 2024 r., https://www.iari.site/2024/04/06/unveiling-isis-k-origins-goals-and-possible-impact [dostęp: 7 II 2025].

[39] A. Legieć, *Perspektywy rozwoju tzw. Państwa Islamskiego w Afganistanie*, Polski Instytut Spraw Międzynarodowych, 1 X 2021 r., https://www.pism.pl/publikacje/perspektywy-rozwoju-tzw-panstwa-islamskiego-w%25C2%25A0afganistanie [dostęp: 7 II 2025].

[40] C. Timofte, *Unlikely Friends: What role would the USA play in the fight between ISIS-K and the Taliban?*, Institute of New Europe, 29 XI 2021 r., https://www.ine.org.pl/en/unlikely-friends-what-role-would-the-usa-play-in-the-fight-between-isis-k-and-the-taliban [dostęp: 7 II 2025].

[41] Rozłam Państwa Islamskiego i Al-Kaidy jest wynikiem narastających napięć i różnic ideologicznych. Podstawowe rozbieżności dotyczyły przede wszystkim tego, kiedy i w jakich okolicznościach należy utworzyć kalifat, a także jaki rodzaj wroga (bliski czy daleki) powinien być traktowany priorytetowo. Relacje pomiędzy organizacjami zdefiniował spór dotyczący statusu Frontu Nusra (Jabhat an-Nusra formalnie była filią Al-Kaidy) – Państwo Islamskie w sposób jednostronny próbowało przejąć kontrolę nad grupą i włączyć ją do swoich struktur. Przywódca An-Nusry, Abu Muhammad al-Dżaulani, potwierdził wówczas swoją wierność wobec Al-Kaidy. W rezultacie również jego grupa stała się wrogiem kalifatu. Na temat genezy antagonizmów pomiędzy Państwem Islamskim a Al-Kaidą zob. szerzej: A.Y. Zelin, *The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement*, The Washington Institute for Near East Policy, 26 VII 2014 r., https://www.washingtoninstitute.org/policy-analysis/view/the-war-between-isis-and-al-qaeda-for-supremacy-of-the-global-jihadist [dostęp: 4 II 2025].

rekrutacyjne, lecz także o prymat w globalnym ruchu dżihadystycznym. Dlatego też konfrontacja Państwa Islamskiego i Al-Kaidy przejawia się zarówno na płaszczyznach doktrynalnej oraz propagandowej (np. wzajemne oskarżenia o herezję czy dyskredytacja), jak i w bezpośrednich starciach w różnych regionach świata. Walka pomiędzy tymi organizacjami często odbywała się za pośrednictwem ich lokalnych grup afiliowanych. Poza Afganistanem tego typu starcia można było zaobserwować w związku z wojną domową w Jemenie[42] oraz w Mali[43].

Należy również wspomnieć o szczególnym znaczeniu Syrii. Struktury pozostałe tam po Państwie Islamskim kontynuują tam działania wymierzone przeciwko Hay'at Tahrir al-Sham (HTS), czyli frakcji rebelianckiej, która w grudniu 2024 r. obaliła reżim Baszszara al-Asada, a następnie utworzyła rząd tymczasowy. Wrogość ta wynika z faktu, że przywódca HTS, Ahmed al-Sharaa (dawniej znany jako Abu Muhammad al-Dżaulani), w przeszłości był liderem An-Nusry, a także ma bardziej umiarkowane podejście do kwestii ideologicznych[44] oraz oficjalnie deklaruje poszanowanie praw różnych grup etnicznych i religijnych[45].

Państwo Islamskie w Chorasanie a kwestie bezpieczeństwa Polski

Z perspektywy IS-K Polska ze względu na przynależność do Zachodu (przez powiązania sojusznicze ze Stanami Zjednoczonymi) jest zaliczana do wrogów dalekich. Jednocześnie trudno traktować Polskę jako strategicznego lub priorytetowego przeciwnika ugrupowania, co oznacza, że ustępuje ona w hierarchii innym aktorom, bardziej zaangażowanym w procesy istotne z punktu widzenia IS-K. W tym kontekście większe znaczenie mają m.in. Stany Zjednoczone, Rosja, Iran oraz Chiny, które w przeszłości były uwikłane w walkę z kalifatem lub podejmowały kroki polityczne postrzegane

[42] E. Kendall, *ISIS in Yemen: Caught in a Regional Power Game*, New Lines Institute for Strategy and Policy, 21 VII 2020 r., https://www.newlinesinstitute.org/isis/isis-in-yemen-caught-in-a-regional-power-game-2 [dostęp: 12 II 2025].

[43] Na temat rywalizacji pomiędzy organizacjami na terytorium Mali zob. szerzej: E. Baldaro, Y.S. Diall, *The End of the Sahelian Exception: Al-Qaeda and Islamic State Clash in Central Mali*, „The International Spectator" 2020, t. 55, nr 4, s. 69–83. https://doi.org/10.1080/03932729.2020.1833566.

[44] Hay'at Tahrir al-Sham wykazuje bardziej pragmatyczne i nieco bardziej „miękkie" stanowisko (jak na standardy dżihadystów) w sprawach ideologicznych. Ahmed al-Sharaa formalnie zerwał więzi z Al-Kaidą, przy czym często zaznacza się, że w istocie jest to działanie pozorne i czysto wizerunkowe. Zob. M. Al-Lami, *From Syrian jihadist leader to rebel politician: How Abu Mohammed al-Jolani reinvented himself*, BBC, 9 XII 2024 r., https://www.bbc.com/news/articles/c0q0w1g8zqvo [dostęp: 12 II 2025].

[45] S. Kajjo, *Syrians welcome new rulers' pledge of moderation but are concerned about extremists in their midst*, VOA, 24 XII 2024 r., https://www.voanews.com/a/syrians-welcome-new-rulers-pledge-of-moderation-but-are-concerned-about-extremists-in-their-midst-/7912678.html [dostęp: 12 II 2025].

przez IS-K jako akty opresji wymierzone w społeczność wiernych. Mając na względzie kwestie ideologiczne, należy zaznaczyć, że do podstawowej kategorii przeciwników ugrupowania zaliczają się przede wszystkim wrogowie bliscy.

W Polsce odnotowano kilka incydentów powiązanych z Państwem Islamskim (z czego przynajmniej jeden mający związek z IS-K) z udziałem zarówno polskich obywateli, jak i cudzoziemców[46]. Incydenty te nie skutkowały ofiarami śmiertelnymi, a działania sprawców zostały udaremnione. Warto dodać, że w przeszłości kilkunastu polskich obywateli zasiliło szeregi Państwa Islamskiego i udało się na obszary walk[47]. Niemniej odsetek odnotowanych zwolenników czy też członków tej organizacji jest w przypadku Polski zdecydowanie niższy w porównaniu z państwami takimi jak Niemcy, Francja, Wielka Brytania czy Belgia. Wynika to po pierwsze z liczebności mniejszości muzułmańskiej[48], a po drugie z braku zaszłości kolonialnych (jak np. we Francji). Zaszłości te mają istotny związek z wykluczeniem społecznym, stwarzającym dogodny grunt dla działań mobilizacyjnych lub rekrutacyjnych organizacjom dżihadystycznym. Należy jednak pamiętać, że marginalna liczba ewentualnych sympatyków lub nawet założenie, że na terytorium Polski nie istnieje żadna komórka ugrupowania, nie wykluczają możliwości zaistnienia spontanicznych operacji pod szyldem Państwa Islamskiego. W tym kontekście kluczowe znaczenie może mieć zjawisko tzw. samotnych wilków (ang. *lone wolves*), czyli jednostek, które niekoniecznie mają bezpośrednie powiązania z organizacją terrorystyczną,

[46] Opisy incydentów zamieszczono na interaktywnej mapie aktywności Państwa Islamskiego. Zob. A.Y. Zelin, *The Islamic State. Select Worldwide Activity Map,* The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/1972 [dostęp: 4 III 2025].

[47] Choć trudno wskazać szczegóły, to szacuje się, że w szeregach kalifatu było ok. 20 Polaków. Zob. P. Mazur, *Polscy dżihadyści – analiza zagrożenia ze strony terrorystów islamistycznych polskiego pochodzenia*, „Historia i Polityka" 2022, nr 39(46), s. 91. Odnotowano też komentarze, że mogli oni ulec radykalizacji podczas emigracji w państwach Europy Zachodniej (w Niemczech i Norwegii). Zob. K. Rękawek, *Jednak nie Państwo Islamskie? Zagrożenie terroryzmem międzynarodowym dla Polski*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2015 r., https://www.pism.pl/publikacje/Jednak_nie_Pa_stwo_Islamskie__Zagro_enie_terroryzmem_mi_dzynarodowym_dla_Polski_ [dostęp: 4 III 2025]. Najbardziej znanym dżihadystą pochodzącym z Polski (z Sandomierza) był Abu Khattab (pseudonim), znany również jako Al-Bulandi. W marcu 2017 r. pojawiła się informacja, że miał on zginąć w Syrii w zamachu samobójczym. Zob. SITE Intelligence Group, wpis na portalu X, 1 III 2017 r., https://www.x.com/siteintelgroup/status/837007988779073537 [dostęp: 4 III 2025].

[48] W Polsce odsetek muzułmanów wynosi 0,13% populacji, podczas gdy w Niemczech jest to 5%, we Francji 9,6%, w Belgii 6%, a w Wielkiej Brytanii 4,6% (stan na 2024 r.). Zob. *Europe Muslim Population in 2024*, https://www.muslimpopulation.com/Europe [dostęp: 4 III 2025]. Wartości te mogą się nieznacznie różnić w zależności od szacunków (oraz czasu, w którym dokonywano badań), jednak prawidłowość dotycząca różnicy pomiędzy Polską a wspomnianymi państwami pozostaje wyraźna.

ale podejmują wysiłki (zazwyczaj na skutek oddziaływania propagandy) w celu przeprowadzenia ataków[49].

Państwo Islamskie w Chorasanie może próbować budować w Polsce (podobnie jak w innych państwach) sieci operacyjne, bazy członkowskie oraz pozyskiwać fundusze. Można przypuszczać, że źródła finansowania ugrupowania pochodzące z podatków i wymuszeń, a także dochody z eksploatacji surowców (przede wszystkim minerałów takich jak talk i lapis lazuli) czy handlu narkotykami[50] zostały znacznie ograniczone wraz z ofensywą talibów w Afganistanie. Wynikający ze strat terytorialnych strategiczny zwrot w stronę państw sąsiedzkich oraz zainicjowanie kolejnych ataków terrorystycznych mogły być również podyktowane chęcią pozyskiwania środków na działalność. Istotną metodą zbierania funduszy pozostają nadal wpłaty i darowizny dokonywane przez zwolenników ugrupowania za pośrednictwem kryptowalut lub nieformalnego systemu hawala[51]. Do gromadzenia środków w dużej mierze jest wykorzystywana aplikacja Telegram, która zapewnia wysoki poziom anonimowości użytkowników i ich komunikacji. Przez tworzenie zamkniętych kanałów i grup Telegram stwarza IS-K przestrzeń do organizowania i promowania kampanii crowdfundingowych, a także otwiera dostęp do publicznych grup oraz forów, na których zwolennicy mogą umieszczać określone treści. Aplikacja może być równocześnie narzędziem do pozyskiwania nowych sympatyków, przekazywania materiałów propagandowych oraz instrukcji dotyczących przeprowadzania ataków, a nawet służyć do bezpośredniej koordynacji działań terrorystycznych[52].

---

[49] Na temat strategii tzw. samotnych wilków zob. szerzej: B. Mendelsohn, *ISIS' Lone-Wolf Strategy and How the West Should Respond*, Foreign Affairs, 25 VIII 2016 r., https://www.foreignaffairs.com/isis-lone-wolf-strategy [dostęp: 4 III 2025].

[50] A. Zerden, *What Is Known About ISIS-K Funding in Afghanistan?*, Lawfare, 30 VIII 2021 r., https://www.lawfaremedia.org/article/what-known-about-isis-k-funding-afghanistan [dostęp: 12 III 2025]; Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K)*…, s. 220, 227. Do ważniejszych źródeł finansowania IS-K należy również wsparcie ze strony organizacji centralnej.

[51] A. Zerden, *What Is Known About ISIS-K Funding in Afghanistan*…

[52] Na temat sposobów wykorzystywania aplikacji Telegram przez Państwo Islamskie zob. szerzej: *Islamic State's Telegram Hustle: How a Terrorist Organization Raises Funds*, Cyfirma, 13 III 2024 r., https://www.cyfirma.com/research/islamic-states-telegram-hustle-how-a-terrorist-organization-raises-funds [dostęp: 13 III 2025]; B. Clifford, H. Powell, *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/EncryptedExtremism.pdf [dostęp: 13 III 2025]. Autorzy badania podkreślają, że Telegram stanowi istotny system strategii komunikacyjnej Państwa Islamskiego. Wskazuje się, że członkowie organizacji (w Syrii i Iraku) mieli utrzymywać za pomocą aplikacji bezpośredni kontakt z organizatorami ataków w Paryżu (listopad 2015 r.) i Berlinie (grudzień 2016 r.). Zob. B. Clifford, H. Powell, *Encrypted Extremism. Inside*…, s. 10.

W kontekście potencjalnych zagrożeń ze strony IS-K warto rozważyć również bieżące ruchy migracyjne, przede wszystkim z Bliskiego Wschodu. Po pierwsze, nie można wykluczyć, że wśród przybywających migrantów – pomimo działań zabezpieczających i kontrolnych ze strony państwa – nie będzie członków organizacji o charakterze terrorystycznym, w tym zwolenników (a nawet bojowników) Państwa Islamskiego lub jego filii. W przeszłości swoboda przemieszczania się osób w Unii Europejskiej oraz mechanizmy Schengen ułatwiły zamachowcom mobilność[53]. Przebywanie potencjalnych zamachowców na terytorium Polski może być jednym z etapów ich podróży do państw docelowych. Istotnym aspektem jest też migracja uchodźców przez wschodnią granicę Polski w związku z wojną w Ukrainie. Kluczowe w tym zakresie może być zjawisko inżynierii przymusowej migracji (istniejącej lub wywołanej celowo) jako element działań aktorów zewnętrznych (przede wszystkim Rosji)[54]. Wykorzystanie migracji – w tym również ewentualne próby umieszczenia (np. przez rosyjskie służby specjalne) wśród migrantów przestępców lub członków grup terrorystycznych – ma w założeniu wymusić większe zaangażowanie zasobowe i logistyczne, aby uszczelnić granicę polsko-białoruską oraz zapobiec próbom jej nielegalnego przekraczania. Konsekwencją ma być ograniczenie wsparcia udzielanego stronie ukraińskiej, co mogłoby ułatwić Rosji osiąganie celów militarnych i politycznych.

Państwo Islamskie w Chorasanie może stanowić również element szerszej strategii działań rosyjskich służb[55]. Szczególne znaczenie w tym kontekście może mieć proces radykalizacji migrantów z Tadżykistanu (dokonujący się właśnie w Rosji), których udział w szeregach ugrupowania znacznie wzrósł[56]. Tadżyccy

[53] Przykładem takiej sytuacji był przytoczony już zamach w Berlinie z 19 grudnia 2016 r. Po przeprowadzeniu ataku na jarmarku świątecznym sprawca zbiegł (przez Holandię, Belgię i Francję) do Włoch, gdzie został zastrzelony podczas próby aresztowania. Na temat zamachu zob. szerzej: *Berlin lorry attack: What we know*, BBC, 24 XII 2016 r., https://www.bbc.com/news/world-europe-38377428 [dostęp: 19 III 2025].

[54] Na temat inżynierii przymusowej migracji zob. szerzej: M. Wojnowski, *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 11–49. https://doi.org/10.4467/20801335PBW.21.034.15694.

[55] K. Strachota, *Państwo Islamskie Chorasanu*…, s. 5.

[56] M. Tadych, *From Dushanbe to Berlin: The emerging ISIS-K threat*, Atlantic Council, 10 X 2024 r., https://www.atlanticcouncil.org/blogs/menasource/europe-isis-k-tajikistan [dostęp: 21 III 2025]. O większym znaczeniu dżihadystów pochodzenia tadżyckiego w ramach IS-K może świadczyć fakt, że zdecydowana większość zatrzymanych powiązanych z atakiem w Crocus City Hall była przedstawicielami tej nacji. Tadżyków powiązanych z filią w Chorasanie aresztowano również m.in. w Stanach Zjednoczonych, a nawet w Polsce. Zob. R.J. Bunker, P. Ligouri Bunker, *Eight Tajiks Arrested by ICE in Los Angeles, New York, and Philadelphia: Islamic State Khorasan (ISK) Strike Team Concerns*, Cofutures, 17 VI 2024 r., https://www.cofutures.net/post/eight-tajiks-arrested-by-ice-in-los-angeles-new-york-and-philadelphia-islamic-state-khorasan-isk [dostęp: 19 III 2025]; *Bojownik Państwa Islamskiego*

radykałowie mogą być z jednej strony wykorzystywani w zewnętrznych naciskach politycznych[57], z drugiej zaś ich ewentualna relokacja poza granice rosyjskiej strefy wpływów zwiększa poziom bezpieczeństwa wewnętrznego w Rosji.

Podsumowanie

Podobnie jak w przypadku Państwa Islamskiego podstawowym założeniem ideologicznym filii w Chorasanie jest utworzenie kalifatu. Dążenie do osiągniecia rządów „czystego islamu" oznacza wykorzystanie wszelkich możliwych środków, wśród których istotną rolę odgrywa dżihad, czyli aktywne prowadzenie walki z użyciem przemocy czy przeprowadzaniem aktów terrorystycznych. Istotne znaczenie ma również definiowanie oponentów, których pokonanie ma być niezbędne do zmiany obecnego globalnego porządku. Warto zwrócić uwagę, że ugrupowanie kładzie ideologiczny akcent na konfrontację w pierwszej kolejności z wrogami bliskimi. Zmiany w strategii IS-K – prawdopodobnie wynikające z porażek w podstawowym obszarze funkcjonowania – doprowadziły do przekierowania uwagi organizacji na przeciwników zewnętrznych. Choć na liście wrogów dalekich znajduje się też Polska, to priorytetem dla IS-K zdają się pozostawać państwa uwikłane w „prześladowania muzułmanów", a atak w Krasnogorsku może być tego egzemplifikacją. Do potencjalnych zagrożeń dla Polski ze strony IS-K można zaliczyć m.in. działania operacyjne tej organizacji, w tym rozbudowę bazy członkowskiej, pozyskiwanie nowych zwolenników, gromadzenie funduszy (lub pośrednictwo w tym zakresie), a nawet spontaniczne próby przeprowadzania zamachów. Z kolei migracje oraz wojnę w Ukrainie można traktować jako procesy generujące dodatkowe ryzyko.

Otwarte pozostaje również pytanie o dalszą aktywność Państwa Islamskiego w kontekście dynamiki wydarzeń w Syrii. Obalenie rządów Asada i utworzenie rządu de facto przez HTS pod przywództwem Al-Shary oznacza nowy rozdział w historii tego państwa, przy czym nie ustały procesy mogące skutkować dalszą destabilizacją. Pomimo starań rządu HTS o nawiązanie relacji politycznych i gospodarczych z innymi aktorami międzynarodowymi napięta sytuacja wewnętrzna może prowadzić do rebelii zainicjowanej przez poszczególne frakcje, a nawet do wznowienia wojny

w Polsce. Został deportowany z kraju, Onet, 16 IV 2024 r., https://www.wiadomosci.onet.pl/kraj/bojownik-panstwa-islamskiego-w-polsce-abw-deportowalo-go-z-kraju/t8qdqz1 [dostęp: 19 III 2025].

[57] Kwestia tadżyckich radykałów jest również wykorzystywana przez Rosję w stosunkach z Tadżykistanem. Zob. J. Lang, *Tadżykistan: chroniczna stagnacja*, Ośrodek Studiów Wschodnich, 16 III 2016 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2016-03-16/tadzykistan-chroniczna-stagnacja [dostęp: 19 III 2025].

domowej lub bezpośredniego zaangażowania któregoś z aktorów zewnętrznych. Takie okoliczności byłyby korzystne dla Państwa Islamskiego, które mogłoby dążyć do relokacji dostępnych zasobów i mobilizacji sympatyków (co z kolei może wiązać się ze zwiększoną aktywnością terrorystyczną w państwach traktowanych przez tę grupę jako wrogie), aby aktywnie włączyć się do walki z „wrogiem najbliższym" (czyli Al-Sharaa oraz HTS). W takim scenariuszu organizacja może nawet ponownie podjąć próbę stworzenia struktury terytorialnej. Niezależnie od tego, jak będzie się kształtowała sytuacja w Syrii, Państwo Islamskie ciągle pozostaje częścią tamtejszego krajobrazu politycznego i usiłuje podważyć zasadność istnienia oponentów ideologicznych[58].

Bibliografia

Akram Q., Asif N., *Islamic State Khorasan (ISIS-K) In Post Us Withdrawal Afghanistan*, „Journal of Professional Research in Social Sciences" 2024, t. 11, nr 1, s. 211–238. https://doi.org/10.58932/MULA0028.

Baldaro E., Diall Y.S., *The End of the Sahelian Exception: Al-Qaeda and Islamic State Clash in Central Mali*, „The International Spectator" 2020, t. 55, nr 4, s. 69–83. https://doi.org/10.1080/03932729.2020.1833566.

From the Battles of Al-Ahzāb to the War of Coalitions, „Dabiq" 2015, nr 11, s. 46–54.

Islam Is The Religion Of The Sword Not Pacifism, „Dabiq" 2015, nr 7, s. 20–24.

Mazur P., *Polscy dżihadyści – analiza zagrożenia ze strony terrorystów islamistycznych polskiego pochodzenia*, „Historia i Polityka" 2022, nr 39(46), s. 81–95.

Miguel M.L. de, *ISIS-K: A Reboot of Jihadist Terrorism?*, „Revista Seguridad y Poder Terrestre" 2024, t. 3, nr 2, s. 101–108. https://doi.org/10.56221/spt.v3i2.58.

Mohammadi M.D., *Islamic State in Khorasan Recruitment Tactics: Analysis of Push & Pull Factors*, Tarzi Research Foundation, April 2021. https://doi.org/10.13140/RG.2.2.32271.71841.

Sheikh M.K., *Islamic State Enters Al-Qaeda's Old Hotbed: Afghanistan and Pakistan*, „Connections" 2017, t. 16, nr 1, s. 37–49. https://doi.org/10.11610/Connections.16.1.03.

[58] W styczniu 2025 r. został udaremniony zamach (a przynajmniej taką informację upublicznił rząd HTS), który Państwo Islamskie usiłowało zrealizować w Damaszku. Zob. *Syria thwarts planned Islamic State attack on Shiite shrine*, VOA, 11 I 2025 r., https://www.voanews.com/a/syria-thwarts-planned-islamic-state-attack-on-shiite-shrine/7933294.html [dostęp: 24 III 2025].

Wiktorowicz Q., *Anatomy of the Salafi Movement*, „Studies in Conflict & Terrorism" 2006, t. 29, nr 3, s. 207–239. https://doi.org/10.1080/10576100500497004.

Wilāyat Khurāsān And The Bay'āt From Qawqāz, „Dabiq" 2015, nr 7, s. 33–37.

Wojnowski M., *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 11–49. https://doi.org/10.4467/20801335PBW.21.034.15694.

Źródła internetowe

Afghanistan: Deadly suicide attack at Russian embassy in Kabul, Al Jazeera, 5 IX 2022 r., https://www.aljazeera.com/news/2022/9/5/suicide-bomb-blast-near-russian-embassy-in-kabul-afghan-police [dostęp: 17 I 2025].

Afghanistan: ISIS Group Targets Religious Minorities, Human Rights Watch, 6 IX 2022 r., https://www.hrw.org/news/2022/09/06/afghanistan-isis-group-targets-religious-minorities [dostęp: 8 I 2025].

Afghanistan/US, 'Mother of all bombs', https://casebook.icrc.org/case-study/afghanistan-us-mother-all-bombs [dostęp: 9 I 2025].

Al-Lami M., *From Syrian jihadist leader to rebel politician: How Abu Mohammed al-Jolani reinvented himself*, BBC, 9 XII 2024 r., https://www.bbc.com/news/articles/c0q0w1g8zqvo [dostęp: 12 II 2025].

Barrett R., *Beyond The Caliphate: Foreign Fighters and the Threat of Returnees*, https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf [dostęp: 17 I 2025].

Berlin lorry attack: What we know, BBC, 24 XII 2016 r., https://www.bbc.com/news/world-europe-38377428 [dostęp: 19 III 2025].

Bezhan F., *The Taliban, The Government, And Islamic State: Who Controls What In Afghanistan?*, Radio Free Europe/Radio Liberty, 31 V 2020 r., https://www.rferl.org/a/taliban-government-islamic-state-who-controls-what-in-afghanistan-/30644646.html [dostęp: 8 I 2025].

Bojownik Państwa Islamskiego w Polsce. Został deportowany z kraju, Onet, 16 IV 2024 r., https://www.wiadomosci.onet.pl/kraj/bojownik-panstwa-islamskiego-w-polsce-abw-deportowalo-go-z-kraju/t8qdqz1 [dostęp: 19 III 2025].

Botobekov U., *New ISIS Strategy and the Resurgence of Islamic State Khorasan*, Modern Diplomacy, 17 V 2022 r., https://www.moderndiplomacy.eu/2022/05/17/new-isis-strategy-and-the-resurgence-of-islamic-state-khorasan [dostęp: 15 I 2025].

Botobekov U., *Think like Jihadist: Anatomy of Central Asian Salafi groups*, Modern Diplomacy, 29 V 2019 r., https://moderndiplomacy.eu/2019/05/29/think-like-jihadist-anatomy-of-central-asian-salafi-groups [dostęp: 17 I 2025].

Bunker R.J., Ligouri Bunker P., *Eight Tajiks Arrested by ICE in Los Angeles, New York, and Philadelphia: Islamic State Khorasan (ISK) Strike Team Concerns*, Cofutures, 17 VI 2024 r., https://www.cofutures.net/post/eight-tajiks-arrested-by-ice-in-los-angeles-new-york-and-philadelphia-islamic-state-khorasan-isk [dostęp: 19 III 2025].

Celso A.N., *Islamic Regression, Jihadist Frustration and Takfirist Hyper Violence*, „Journal of Political Sciences & Public Affairs" 2016, t. 4, nr 2, https://www.longdom.org/open-access/islamic-regression-jihadist-frustration-and-takfirist-hyper-violence-2332-0761-1000200.pdf [dostęp: 27 I 2025]. https://doi.org/10.4172/2332-0761.1000200.

Clifford B., Powell H., *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/EncryptedExtremism.pdf [dostęp: 13 III 2025].

Coppolecchia S., *Unveiling ISIS-K: Origins, Goals And Possible Impact*, Instituto Analisi Relazioni Internazionali, 6 IV 2024 r., https://www.iari.site/2024/04/06/unveiling-isis-k-origins-goals-and-possible-impact [dostęp: 7 II 2025].

Daly J.C.K., *Rocket Attacks on Tajikistan and Uzbekistan Undermine Taliban Security Claims*, Jamestown, 8 I 2022 r., https://jamestown.org/program/rocket-attacks-on-tajikistan-and-uzbekistan-undermine-taliban-security-claims [dostęp: 15 I 2025].

Dyner A.M., *Zamach w Moskwie*, Polski Instytut Spraw Międzynarodowych, 25 III 2024 r., https://www.pism.pl/publikacje/zamach-w-moskwie [dostęp: 6 I 2025].

Europe Muslim Population in 2024, https://www.muslimpopulation.com/Europe [dostęp: 4 III 2025].

Faulconbridge G., *US embassy warns of imminent attack in Moscow by 'extremists'*, Reuters, 8 III 2024 r., https://www.reuters.com/world/us-embassy-warns-imminent-extremist-attack-moscow-2024-03-08 [dostęp: 6 I 2025].

Giustozzi A., *The Islamic State in Khorasan between Taliban counter-terrorism and resurgence prospects*, International Centre for Counter-Terrorism, 30 I 2024 r., https://www.icct.nl/publication/islamic-state-khorasan-between-taliban-counter-terrorism-and-resurgence-prospects [dostęp: 8 I 2025].

Giustozzi A., *The Islamic State in Khorasan*, Italian Institute for International Political Studies, 27 VI 2019 r., https://www.ispionline.it/en/publication/islamic-state-khorasan-23406 [dostęp: 8 I 2025].

Global Terrorism Index 2016, Institute for Economics and Peace, https://www.reliefweb.int/report/world/global-terrorism-index-2016 [dostęp: 4 XII 2024].

Global Terrorism Index 2026, https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf [dostęp: 21 VIII 2026].

Gordon M.R., Salama V., Strobel W.P., *U.S. Secretly Alerted Iran Ahead of Islamic State Terrorist Attack*, The Wall Street Journal, 26 I 2024 r., https://www.wsj.com/world/middle-east/us-secretly-alerted-iran-ahead-of-islamic-state-terrorist-attack-af77a19a [dostęp: 6 I 2025].

Harmouch S., Jadoon A., *How Moscow terror attack fits ISIS-K strategy to widen agenda, take fight to its perceived enemies*, The Conversation, 24 III 2024 r., https://www.theconversation.com/how-moscow-terror-attack-fits-isis-k-strategy-to-widen-agenda-take-fight-to-its-perceived-enemies-226469 [dostęp: 17 I 2025].

Ikram I., Siddique A., *Afghan President Declares IS Defeated In Eastern Stronghold*, Radio Free Europe/Radio Liberty, 19 XI 2019 r., https://gandhara.rferl.org/a/afghan-president-declares-is-defeated-in-eastern-stronghold/30280871.html [dostęp: 8 I 2025].

ISIL claims 'province' in India, officials call it 'propaganda', Al Jazeera, 12 V 2019 r., https://www.aljazeera.com/news/2019/5/12/isil-claims-province-in-india-officials-call-it-propaganda [dostęp: 4 XII 2024].

ISIL claims responsibility for deadly Kabul attack, Al Jazeera, 3 IX 2024 r., https://www.aljazeera.com/news/2024/9/3/isil-claims-responsibility-for-deadly-kabul-attack [dostęp: 3 I 2025].

ISIL confirms death of leader Abu Hussein al-Qurashi, names successor, Al Jazeera, https://www.aljazeera.com/news/2023/8/3/isil-confirms-death-of-leader-abu-hussein-al-qurashi-names-successor [dostęp: 1 IX 2026].

Islamic State in Khorasan Province, https://mappingmilitants.org/profiles/islamic-state-in-khorasan-province [dostęp: 21 VIII 2026].

Islamic State's Telegram Hustle: How a Terrorist Organization Raises Funds, Cyfirma, 13 III 2024 r., https://www.cyfirma.com/research/islamic-states-telegram-hustle-how-a-terrorist-organization-raises-funds [dostęp: 13 III 2025].

Jadoon A., Mines A., *Taking Aim: Islamic State Khorasan's Leadership Losses*, „CTC Sentinel" 2019, t. 12, nr 8, https://ctc.westpoint.edu/wp-content/uploads/2019/09/CTC-SENTINEL-082019.pdf, s. 14–22 [dostęp: 8 I 2025].

Kajjo S., *Syrians welcome new rulers' pledge of moderation but are concerned about extremists in their midst*, VOA, 24 XII 2024 r., https://www.voanews.com/a/syrians-welcome-new-rulers-pledge-of-moderation-but-are-concerned-about-extremists-in-their-midst-/7912678.html [dostęp: 12 II 2025].

Kendall E., *ISIS in Yemen: Caught in a Regional Power Game*, New Lines Institute for Strategy and Policy, 21 VII 2020 r., https://www.newlinesinstitute.org/isis/isis-in-yemen-caught-in-a-regional-power-game-2 [dostęp: 12 II 2025].

Lang J., *Tadżykistan: chroniczna stagnacja*, Ośrodek Studiów Wschodnich, 16 III 2016 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2016-03-16/tadzykistan-chroniczna-stagnacja [dostęp: 19 III 2025].

Legieć A., *Perspektywy rozwoju tzw. Państwa Islamskiego w Afganistanie*, Polski Instytut Spraw Międzynarodowych, 1 X 2021 r., https://www.pism.pl/publikacje/perspektywy-rozwoju-tzw-panstwa-islamskiego-w%25C2%25A0afganistanie [dostęp: 7 II 2025].

Leigh K., French J., Juan J., *Islamic State and Its Affiliates*, The Wall Street Journal, http://graphics.wsj.com/islamic-state-and-its-affiliates [dostęp: 4 XII 2024].

Mendelsohn B., *ISIS' Lone-Wolf Strategy and How the West Should Respond*, Foreign Affairs, 25 VIII 2016 r., https://www.foreignaffairs.com/isis-lone-wolf-strategy [dostęp: 4 III 2025].

Rahmani B., Tanco A., *ISIS's Growing Caliphate: Profiles of Affiliates*, Wilson Center, 19 II 2016 r., https://www.wilsoncenter.org/article/isiss-growing-caliphate-profiles-affiliates [dostęp: 4 XII 2024].

Rassler D., *Situating the Emergence of the Islamic State of Khorasan*, „CTC Sentinel" 2015, t. 8, nr 3, https://ctc.westpoint.edu/wp-content/uploads/2015/03/CTCSentinel-Vol8Issue317.pdf, s. 7–11 [dostęp: 20 XII 2024].

Rękawek K., *Jednak nie Państwo Islamskie? Zagrożenie terroryzmem międzynarodowym dla Polski*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2015 r., https://www.pism.pl/publikacje/Jednak_nie_Pa_stwo_Islamskie__Zagro_enie_terroryzmem_mi_dzynarodowym_dla_Polski_ [dostęp: 4 III 2025].

Rubin M., *Abu Bakr al-Baghdadi Is Dead (But His Legacy Lives on)*, The National Interest, 27 X 2019 r., https://nationalinterest.org/blog/middle-east-watch/abu-bakr-al-baghdadi-dead-his-legacy-lives-91536 [dostęp: 4 XII 2024].

SITE Intelligence Group, wpis na portalu X, 1 III 2017 r., https://www.x.com/siteintelgroup/status/837007988779073537 [dostęp: 4 III 2025].

Strachota K., *Państwo Islamskie Chorasanu – nowa odsłona światowego dżihadu*, Ośrodek Studiów Wschodnich, 29 III 2024 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-03-29/panstwo-islamskie-chorasanu-nowa-odslona-swiatowego-dzihadu [dostęp: 20 XII 2024].

Syria thwarts planned Islamic State attack on Shiite shrine, VOA, 11 I 2025 r., https://www.voanews.com/a/syria-thwarts-planned-islamic-state-attack-on-shiite-shrine/7933294.html [dostęp: 24 III 2025].

Tadych M., *From Dushanbe to Berlin: The emerging ISIS-K threat*, Atlantic Council, 10 X 2024 r., https://www.atlanticcouncil.org/blogs/menasource/europe-isis-k-tajikistan [dostęp: 21 III 2025].

Taylor A., *The strange story behind the 'Khorasan' group's name*, The Washington Post, 25 IX 2014 r., https://www.washingtonpost.com/news/worldviews/wp/2014/09/25/the-strange-story-behind-the-khorasan-groups-name [dostęp: 24 XII 2024].

Timofte C., *Unlikely Friends: What role would the USA play in the fight between ISIS-K and the Taliban?*, Institute of New Europe, 29 XI 2021 r., https://www.ine.org.pl/en/unlikely-friends-what-role-would-the-usa-play-in-the-fight-between-isis-k-and-the-taliban [dostęp: 7 II 2025].

What we know about Islamic State in Khorasan Province (ISIS-K), Al Jazeera, 27 VIII 2021 r., https://www.aljazeera.com/news/2021/8/27/islamic-state-in-khorasan-iskp-aka-isil [dostęp: 3 I 2025].

Wood G., *What ISIS Really Wants*, The Atlantic, March 2015, https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980 [dostęp: 27 I 2025].

Zelin A.Y., *The Islamic State. Select Worldwide Activity Map*, The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/1972 [dostęp: 4 III 2025].

Zelin A.Y., *The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement*, The Washington Institute for Near East Policy, 26 VII 2014 r., https://www.washingtoninstitute.org/policy-analysis/view/the-war-between-isis-and-al-qaeda-for-supremacy-of-the-global-jihadist [dostęp: 4 II 2025].

Zerden A., *What Is Known About ISIS-K Funding in Afghanistan?*, Lawfare, 30 VIII 2021 r., https://www.lawfaremedia.org/article/what-known-about-isis-k-funding-afghanistan [dostęp: 12 III 2025].

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO
2026, nr 35, s. 113–134

Dr Łukasz Cymbaluk

Doktor nauk o polityce i administracji. Stopień doktora uzyskał na Uniwersytecie Wrocławskim w 2023 r. na podstawie rozprawy pt. *Państwo Islamskie w środowisku międzynarodowym*. Jego zainteresowania naukowe obejmują geopolitykę, bezpieczeństwo międzynarodowe oraz współczesne procesy polityczne.

Kontakt: lukasz.cymbaluk@wskz.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 135–148
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.026.24175

ARTYKUŁ

Sposób postępowania funkcjonariuszy Służby Więziennej z osadzonymi należącymi do struktur przestępczości zorganizowanej – środki bezpieczeństwa i nadzoru

Prison Service officers' conduct with prisoners belonging to organised crime structures – security and supervision measures

PAWEŁ ŁUSZCZ

Zakład Karny w Wojkowicach

https://orcid.org/0000-0002-5308-2324

Abstrakt

Głównymi celami artykułu są analiza sposobu postępowania funkcjonariuszy Służby Więziennej (SW) wobec osadzonych należących do struktur przestępczości zorganizowanej oraz ocena środków bezpieczeństwa i nadzoru stosowanych wobec nich w jednostce penitencjarnej. Omówione zostały zagadnienia dotyczące bezpieczeństwa jednostki penitencjarnej, rozpoznania osadzonego podczas przyjęcia do jednostki i w trakcie pobytu, a także postępowania z nim. Autor wykazał, że wiedza o osadzonych oraz wymiana informacji pomiędzy komórkami SW mają kluczowe znaczenie dla sposobu postępowania funkcjonariuszy wobec osadzonych i skuteczności podejmowanych czynności profilaktycznych oraz dla zwiększenia poziomu bezpieczeństwa zarówno osadzonych, jak i funkcjonariuszy SW w trakcie realizacji zadań służbowych.

Słowa kluczowe

Służba Więzienna, bezpieczeństwo, przestępczość zorganizowana, zabezpieczenie osadzonego

Abstract

The main objectives of this article are to analyse the conduct of the Prison Service officers towards prisoners who are members of organised crime groups and to assess the security and supervision measures applied to them within the penitentiary unit. Issues relating to the security of the penitentiary unit, the assessment of inmates both on admission and during their stay, and the appropriate way to deal with them were discussed. The author demonstrated that knowledge of prisoners and the exchange of information between the Prison Service units are of crucial importance to the way officers treat prisoners and the effectiveness of preventive measures taken, as well as to enhancing the security of both prisoners and officers while carrying out their duties.

Keywords

Prison Service, security, organised crime, security measures for the inmate

Wprowadzenie

Przedmiotem badań jest sposób postępowania funkcjonariuszy Służby Więziennej (SW) wobec osadzonych należących do struktur przestępczości zorganizowanej. Autor podjął ten temat ze względu na swoje doświadczenie zawodowe oraz brak źródeł naukowych poruszających to zagadnienie.

Główny problem badawczy to próba odpowiedzi na pytanie, jak powinien wyglądać sposób postępowania funkcjonariuszy SW z osadzonymi należącymi do struktur przestępczości zorganizowanej. Autor przyjął założenie, że właściwe rozpoznanie osadzonego oraz wymiana informacji pomiędzy komórkami SW, a także innymi służbami mają kluczowe znaczenie dla prawidłowego sposobu postępowania funkcjonariuszy SW z takimi osadzonymi. Celem artykułu jest identyfikacja i opis odpowiednich zasad oraz procedur tego postępowania, co zwiększy bezpieczeństwo zarówno osadzonych, jak i funkcjonariuszy SW w trakcie realizacji zadań służbowych.

Pojęcie przestępczości zorganizowanej – problemy definicyjne

Należy podkreślić, że nie istnieje jedna definicja przestępczości zorganizowanej. Ustawodawca nie określił też przesłanek, które mają decydować o zakwalifikowaniu

pewnych zachowań pod kątem znamion z art. 258 § 1 Kodeksu karnego[1]. Piśmiennictwo prawnicze[2] i orzecznictwo w Polsce wypracowały następujące kryteria w tej materii.

Zorganizowaną grupę przestępczą tworzą co najmniej trzy osoby, których celem jest popełnianie określonych przestępstw (zarówno stałe, jak i zależnie od nadarzającej się okazji) lub też popełnianie przestępstw o luźnym związku[3], bez stałych ról[4]. Określenie „zorganizowana" oznacza posiadanie przez grupę trwałej struktury, czy to pionowej – z przywódcą kierującym działalnością, czy poziomej – z gronem uczestników koordynujących działalność według określonych reguł, którzy zakładają popełnienie możliwie wielu czynów zabronionych (zachowań przestępczych). Pojęcie przestępczości zorganizowanej wskazuje zatem na istnienie podstawowej wewnętrznej struktury organizacyjnej (choćby z niskim stopniem zorganizowania), jakiejś trwałości, jakichś więzów organizacyjnych w ramach wspólnego porozumienia, podziału ról, skoordynowanego sposobu działania, na planowanie przestępstw, akceptację celów, zaspokajanie potrzeb grupy, gromadzenie narzędzi do popełniania przestępstw, wyszukiwanie miejsc do przechowywania przedmiotów pochodzących z czynów zabronionych i rozprowadzanie tych przedmiotów[5].

Komenda Główna Policji posługuje się definicją przestępczości zorganizowanej, na którą składa się kilka elementów: sprawcy działają z chęci zysku lub żądzy władzy, działalność grupy trwa przez dłuższy czas, grupa tworzy zorganizowaną strukturę, w której występuje podział zadań między członkami. Obejmuje on m.in. sposób zarabiania pieniędzy. Grupa jest hermetyczna, zdyscyplinowana i poddana kontroli wewnętrznej. Używa przemocy lub innych środków zastraszania. Dąży do

---

1 *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*.

2 Zob. szerzej: M. Stawarz, *Podstawy odpowiedzialności za przestępczość zorganizowaną na przykładzie wybranych instrumentów części ogólnej kodeksu karnego*, „Studia Prawnicze" 2023, nr 1 (227), s. 101–129. https://www.doi.org/10.37232/sp.2023e.

3 To sytuacja, w której celem grupy nie jest popełnienie jednego konkretnego czynu, lecz planowanie i realizacja różnych przestępstw elastycznie ze sobą powiązanych.

4 Stała rola oznacza, że każda osoba w grupie przestępczej ma przypisaną określoną, niezmienną rolę. Rola ta musi cechować się większym stopniem konkretyzacji niż przy zwykłym współsprawstwie. Zob. P. Sienko, *Zarzut z 258 kk, czyli udział w zorganizowanej grupie przestępczej*, 1 XII 2024 r., https://sienkoipartnerzy.pl/prawo-karne/zarzut-z-258-kk-czyli-udzial-w-zorganizowanej-grupy-przestepczej/ [dostęp: 4 VIII 2026].

5 Zob. wyrok Sądu Apelacyjnego (dalej: SA) w Łodzi z 24 I 2001 r., sygn. II AKa 240/01, „Prokuratura i Prawo" 2004, nr 5, poz. 25; wyrok SA w Lublinie z 23 VII 2002 r., sygn. II AKa 148/01, „Prokuratura i Prawo" 2003, nr 4, poz. 20; wyrok SA w Łodzi z 16 I 2014 r., sygn. II AKa 260/13; wyrok Sądu Najwyższego (dalej: SN) z 24 III 2009 r., sygn. WA 9/09; wyrok SA w Warszawie z 15 I 2013 r., sygn. II AKa 352/12; wyrok SN z 13 XI 2013 r., sygn. II KK 170/13.

wywarcia wpływu na politykę, organy ścigania, sądy oraz media, często prowadzi działalność w skali międzynarodowej[6].

W zdefiniowaniu pojęcia przestępczości zorganizowanej mogą pomóc normy prawa międzynarodowego. Polska ratyfikowała Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej. Celem tej konwencji jest promowanie współpracy na rzecz skuteczniejszego zwalczania tego rodzaju przestępczości i zapobiegania jej. W art. 2 wskazano: *„zorganizowana grupa przestępcza" oznacza posiadającą strukturę grupę składającą się z trzech lub więcej osób, istniejącą przez pewien czas oraz działającą w porozumieniu w celu popełnienia jednego lub więcej poważnych przestępstw określonych na podstawie niniejszej konwencji, dla uzyskania, w sposób bezpośredni lub pośredni, korzyści finansowej lub innej korzyści materialnej*[7].

Jednostki penitencjarne w Polsce

Zgodnie z art. 1 ustawy o Służbie Więziennej jest ona: *umundurowaną i uzbrojoną formacją apolityczną podległą Ministrowi Sprawiedliwości, posiadającą własną strukturę organizacyjną*[8]. Służba Więzienna jest zaliczana do grup dyspozycyjnych o charakterze paramilitarnym[9]. Do podstawowych zadań nałożonych na funkcjonariuszy SW należy prowadzenie oddziaływań penitencjarnych i resocjalizacyjnych wobec osób skazanych na karę pozbawienia wolności, wykonywanie tymczasowego aresztowania w sposób zabezpieczający prawidłowy tok postępowania karnego, ochrona społeczeństwa przed sprawcami przestępstw, a także zapewnienie w zakładach karnych i aresztach śledczych porządku i bezpieczeństwa[10]. Struktura wewnętrzna SW obejmuje nie tylko jej organy (Dyrektor Generalny SW, Dyrektor Okręgowy SW[11]), lecz także jednostki organizacyjne (Centralny Zarząd Służby Więziennej, zakłady karne i areszty śledcze[12]).

---

[6] Hasło: przestępczość zorganizowana, Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/przestepczosc-zorganizowana;3963636.html [dostęp: 25 XI 2025].

[7] *Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r.*

[8] *Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej*.

[9] *Grupy dyspozycyjne w obliczu Wielkiej Zmiany. Kulturowe i społeczne aspekty funkcjonowania*, J. Maciejewski, M. Bodziany, K. Dojwa (red.), Wrocław 2010, s. 53.

[10] Art. 2 ust. 2 pkt 1, 2, 5, 6 ustawy o Służbie Więziennej.

[11] Tamże, art. 7 pkt 1, 3.

[12] Tamże, art. 8 pkt 1, 3.

W Polsce istnieją (stan na 31 grudnia 2025 r.) 173 jednostki penitencjarne, w tym: 39 aresztów śledczych, 64 zakłady karne, 68 oddziałów zewnętrznych, a także 2 oddziały tymczasowego zakwaterowania skazanych[13]. W 2024 r. (stan na 31 grudnia) pełniło w nich służbę 27 158 funkcjonariuszy, a pracownicy byli zatrudnieni na 1860,46 etatach[14]. Jednostki te różnią się nie tylko miejscem usytuowania[15], lecz także pojemnością (tabela 1) oraz typem lub rodzajem[16].

Tabela 1. Jednostki penitencjarne według pojemności – stan na 31 grudnia 2025 r.

Pojemność	Areszty śledcze	Zakłady karne	Oddziały zewnętrzne	Oddziały tymczasowego zakwaterowania skazanych*	Ogółem
do 49	0	0	1	2	**3**
50–99	0	0	14	0	**14**
100–199	1	1	21	0	**23**
200–299	7	6	15	0	**28**
300–399	9	5	5	0	**19**
400–499	6	6	2	0	**14**
500–599	1	3	2	0	**6**
600–699	6	7	7	0	**20**
700–799	1	6	1	0	**8**
800–899	0	7	0	0	**7**
900–999	2	4	0	0	**6**
1000–1099	4	9	0	0	**13**
1100–1199	0	0	0	0	**0**

[13] Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2025*, K. Kosmala (oprac.), sygn. BEW.0332.17.2025.KKO, Warszawa 2026, tabela 2, s. 3.

[14] Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2024*, K. Kosmala, K. Kachniarz (oprac.), sygn. BEW.0332.17.2024.KK, Warszawa 2025, tabela 73, s. 40.

[15] Wiele jednostek jest usytuowanych w centrum dużych miast, np. AŚ Katowice, i na przedmieściach małych miejscowości, np. ZK Trzebinia.

[16] Zob. szerzej: *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy* (dalej: k.k.w.).

Pojemność	Areszty śledcze	Zakłady karne	Oddziały zewnętrzne	Oddziały tymczasowego zakwaterowania skazanych*	Ogółem
1200–1299	1	3	0	0	**4**
1300–1499	0	6	0	0	**6**
1500–1800	1	1	0	0	**2**
Ogółem	**39**	**64**	**68**	**2**	**173**

*oddziały utworzone przez Dyrektora Okręgowego Służby Więziennej

Źródło: Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2025*, K. Kosmala (oprac.), sygn. BEW.0332.17.2025.KKO, Warszawa 2026, tabela 2, s. 3.

Pojemność normatywna we wszystkich tych jednostkach wynosi 88 402. Stan ewidencyjny na 30 czerwca 2026 r. to 70 585 osób osadzonych[17].

Wśród osadzonych byli również cudzoziemcy. Na koniec czerwca 2026 r. było to 3037 osób, m.in. obywatele Ukrainy (1708 osób), Gruzji (254 osoby), Białorusi (178 osób) i Mołdawii (140 osoby)[18]. W zakładach karnych i aresztach śledczych funkcjonariusze SW mają więc do czynienia ze zjawiskiem wielokulturowości, stanowiącym novum[19]. Wśród różnych problemów, do których rozwiązywania muszą być przygotowani, są zatem i te mogące mieć źródło w odmiennościach kulturowych[20].

Osadzeni związani z przestępczością zorganizowaną – statystyki i warunki pobytu w jednostkach penitencjarnych

W omówionej wcześniej ogólnej populacji osadzonych są zarówno osoby odbywające karę pozbawienia wolności, jak i te tymczasowo aresztowane, w tym osoby związane z przestępczością zorganizowaną.

[17] Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Miesięczna informacja statystyczna za czerwiec 2026*, sygn. BEW.0332.07.2026.MM, M. Milewska (oprac.), Warszawa 2026, tabela 3, s. 3.

[18] Tamże, tabela 18, s. 20.

[19] B. Orłowska, *Współczesne problemy wielokulturowości*, „Horyzonty Wychowania" 2012, t. 11, nr 22, s. 2.

[20] E. Wasilewski, *Ochrona interesów poszkodowanego w wypadku*, „Forum Służby Więziennej" 2020, nr 263, s. 38.

W odniesieniu do kategorii „przestępczość zorganizowana" orzeczenia wykonywane według rodzajów przestępstw (określonych w k.k. z 1997 r.) kształtowały się na 31 grudnia 2024 r. następująco:

- orzeczenia prawomocne – 678 osób,
- orzeczenia nieprawomocne – 49 osób,
- tymczasowe areszty – 836 osób,
- w związku z artykułem 65 k.k. lub 58a k.k. – 1256 osób[21],
- orzeczenia dotyczące kobiet – 64 osoby,
- orzeczenia dotyczące młodocianych – 9 osób[22].

Ogółem liczba takich osadzonych wyniosła 1563 osoby[23]. Nie jest to zatem mało.

Osadzeni związani z przestępczością zorganizowaną mogą przebywać na terenie jednostki organizacyjnej na dwóch zasadach, tj. na ogólnych warunkach dotyczących osadzonych bądź na statusie osadzonego niebezpiecznego (tzw. więźnia „N"). Decyzje w tym zakresie podejmuje komisja penitencjarna. Zgodnie z Kodeksem karnym wykonawczym (dalej: k.k.w.): *Za skazanego stwarzającego poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu można uznać skazanego, który* (…) *popełnił przestępstwo w zorganizowanej grupie albo związku mających na celu popełnianie przestępstw, zwłaszcza z uwagi na jego kierowniczą lub znaczącą rolę w grupie lub związku*[24]. Przy podejmowaniu i każdorazowej weryfikacji decyzji o uznaniu skazanego za stwarzającego poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu komisja penitencjarna uwzględnia nie tylko popełniony czyn, lecz także m.in.:

1) właściwości i warunki osobiste skazanego;
2) motywacje i sposób zachowania się przy popełnieniu przestępstwa oraz rodzaj i rozmiar następstw przestępstwa (…);
5) w wypadku skazanego za przestępstwo popełnione w zorganizowanej grupie albo związku mających na celu popełnianie przestępstw – zagrożenie dla porządku prawnego, które może wyniknąć z nawiązania przez skazanego bezprawnych kontaktów z innymi członkami grupy, w tym zwłaszcza zagrożenie dla życia lub zdrowia ludzkiego lub dla czynności mających na celu ujawnienie mienia stanowiącego korzyść z popełnienia

[21] Art. 65 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny*; art. 58a *Ustawy z dnia 19 kwietnia 1969 r. Kodeks karny*.

[22] Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2024*…, tabela 14, s. 11.

[23] Tamże.

[24] Art. 88a § 1 pkt 2 k.k.w.

przestępstwa, oraz fakt, że inni członkowie grupy lub związku przebywają na wolności[25].

W przypadku podjęcia decyzji o zakwalifikowaniu osadzonego jako skazanego stwarzającego poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu odbywa on karę w wyznaczonym oddziale lub celi zakładu karnego typu zamkniętego w warunkach zapewniających wzmożoną ochronę społeczeństwa i bezpieczeństwo tego zakładu[26]. Warunki te są następujące:

1) cele mieszkalne oraz miejsca i pomieszczenia wyznaczone do: pracy, nauki, przeprowadzania spacerów, widzeń, odprawiania nabożeństw, spotkań religijnych i nauczania religii oraz zajęć kulturalno-oświatowych, z zakresu kultury fizycznej i sportu wyposaża się w odpowiednie zabezpieczenia techniczno-ochronne;
2) cele mieszkalne pozostają zamknięte całą dobę i są częściej kontrolowane (…);
4) poruszanie się skazanych po terenie zakładu karnego odbywa się pod wzmocnionym dozorem i jest ograniczone tylko do niezbędnych potrzeb;
5) skazanych poddaje się kontroli osobistej przy każdorazowym wyjściu i powrocie do cel (…);
10) skazani nie mogą korzystać z własnej odzieży i obuwia[27].

Warunki pobytu takiego osadzonego są określone w obowiązujących przepisach i funkcjonariusze nie mają dowolności w tym zakresie. Co istotne, przysługujące osadzonemu prawa, nakładane na niego obowiązki czy zakazy nie mogą być ograniczone w porównaniu z innymi osadzonymi. Są to np.: sposób przeprowadzania widzeń[28], odpowiednie wyżywienie pozwalające na zachowanie zdrowia[29] czy też zakaz wykonywania tatuaży i zezwalania na ich wykonywanie na sobie, jak również nakłanianie do takich czynów lub pomoc w ich dokonywaniu[30].

Na koniec należy wspomnieć, że istnieją grupy osób niewpisujące się w definicje przestępczości zorganizowanej[31], ale mogące pozostawać w zainteresowaniu grup przestępczych. Zainteresowanie to może być spowodowane chęcią wpłynięcia na zachowania czy wypowiedzi tych osób, a także na ich przynależność – również

[25] Art. 88a § 2 pkt 1, 2, 5 k.k.w.

[26] Art. 88a § 3 k.k.w.

[27] Art. 88b § 1 pkt 1, 2, 4, 5, 10 k.k.w.

[28] Art. 88b § 1 pkt 8 k.k.w.

[29] Art. 102 pkt 1 k.k.w.

[30] Art. 116a pkt 6 k.k.w.

[31] Mowa o osobach należących do grup pseudokibicowskich, obywatelach innych państw (w głównej mierze z dawnego bloku wschodniego), liderach ruchów religijnych, sekt i związków wyznaniowych, celebrytach, influenserach, patostreamerach czy też osobach powiązanych ze środowiskiem politycznym.

na terytorium jednostki penitencjarnej – która będzie zgodna z potrzebami takiej grupy.

Wiedza o osadzonym – kluczowy element bezpieczeństwa w jednostkach penitencjarnych

Systematyczne gromadzenie i analizowanie informacji o osadzonych pozwala na wcześniejsze identyfikowanie zagrożeń i zwiększanie poziomu bezpieczeństwa w jednostkach penitencjarnych. Rozpoznanie powinno być prowadzone z poszanowaniem godności i praw osób pozbawionych wolności.

Rozpoznanie osadzonego – początek procesu izolacji

Każda osoba, która trafia do jednostki, jest zapoznawana z warunkami i zasadami pobytu w niej, a także odbywa rozmowę wstępną. Obejmuje ona pozyskanie informacji od osadzonego na temat jego statusu rodzinnego, finansowego, uczestnictwa w podkulturze przestępczej. Rozmowę przeprowadza także personel medyczny (m.in. na temat przebytych chorób, przewlekłych dolegliwości zdrowotnych). Analizowana jest również dokumentacja sądowa – rodzaj zarzutów, liczba wspólników, postawa prezentowana przed organami wymiaru sprawiedliwości[32]. Pozyskane informacje i dane mają istotny wpływ na miejsce rozmieszczenia osadzonego oraz dobór współosadzonych.

Rozpoznanie osadzonego – w trakcie izolacji

Funkcjonariusze i pracownicy zakładów karnych i aresztów śledczych wykonują czynności profilaktyczne, które:

> (…) zmierzają do rozpoznania środowiska skazanych i tymczasowo aresztowanych w celu ochrony społeczeństwa przed przestępczością lub zapewnienia porządku lub bezpieczeństwa zakładów karnych, aresztów śledczych lub konwoju, w szczególności przez:
> 1) obserwowanie zachowań i relacji w środowisku skazanych i tymczasowo aresztowanych;
> 2) rozpoznawanie struktur podkultury przestępczej;
> 3) rozpoznawanie atmosfery i nastrojów wśród skazanych i tymczasowo aresztowanych oraz ich zachowań, które mogą naruszyć porządek i bezpieczeństwo zakładów karnych, aresztów śledczych lub konwoju[33].

[32] Przyznanie się do zarzutów lub ich negowanie, rodzaj i charakter złożonych wyjaśnień, współpraca z organami ścigania, prokuratorem, sądem.

[33] Art. 19a ust. 2 ustawy o Służbie Więziennej.

Rozpoznanie obejmuje także analizę korespondencji otrzymywanej przez osadzonego[34], jego widzeń[35], składanych próśb i wniosków[36], otrzymanych nagród, a także wniosków o wymierzenie kary dyscyplinarnej. Nadzór nad rozmowami telefonicznymi może dostarczyć wiedzy o tym, z kim osadzony ma kontakt, jakie ma relacje oraz potrzeby kontaktu z osobami nieprzebywającymi w jednostce.

Istotnym elementem są kwestie finansowe – otrzymywana przez osadzonego formalna pomoc w postaci przelewów pieniężnych[37], paczek, wypiski[38].

Należy wziąć pod uwagę także rodzaj wyżywienia wybrany przez osadzonego, np. diety wynikającej z zasad wyznania, oraz jego praktyki religijne[39], w tym zmianę wyznania. Może to dostarczyć cennych informacji o jego nastawieniu do obecnej sytuacji.

Właściwe rozpoznanie obejmuje ponadto wiedzę o: chęci podjęcia przez osadzonego pracy[40], udziale w procesie resocjalizacji, np. przyjęciu programowego systemu odbywania kary pozbawienia wolności[41], udziale w zajęciach kulturalno-oświatowych[42], podjęciu nauki w systemie szkolnym na terenie jednostki penitencjarnej czy uczestnictwie w spacerach[43]. Istotne dla zapewnienia bezpieczeństwa jest zaobserwowanie, z kim osadzony ma kontakt w czasie tych aktywności. O jego

[34] Z treści listów można uzyskać wiedzę, na czym osadzonemu zależy, za czym tęskni, czego mu brakuje.

[35] Nadzór nad widzeniami dostarcza informacji nie tylko o tym, kto odwiedza osadzonego i o czym rozmawiają, lecz także o tym, kto przywiózł osobę odwiedzającą. Może to być cenna informacja dla innych służb.

[36] Z formalnej dokumentacji osadzonego można się dowiedzieć, czego potrzebuje, jakie ma oczekiwania.

[37] Można ustalić nie tylko to, jakie kwoty otrzymuje osadzony, lecz także częstotliwość wpłat oraz kto ich dokonuje. Ta ostatnia informacja może mieć znaczenie dla innych służb.

[38] Wypiska to określenie używane w codziennej komunikacji między osobami pozbawionymi wolności, oznaczające realizację przez skazanego „(…) zakupów artykułów żywnościowych i wyrobów tytoniowych oraz innych artykułów dopuszczonych do sprzedaży w zakładzie karnym, za środki pieniężne pozostające do jego dyspozycji w depozycie". Zob. art. 113a § 1 k.k.w.

[39] Obserwuje się, czy osadzony dąży do spotkań z konkretnymi przedstawicielami ruchów religijnych, aktywnie uczestniczy w spotkaniach religijnych, np. mszach, oraz – co ważne – czy wynika to z potrzeby duchowej czy np. z chęci spotkania się z innym osadzonym.

[40] Dotyczy to również pracy nieodpłatnej. Osadzony może zabiegać o konkretny rodzaj pracy, np. w kuchni, a jego głównym motywem może być kontakt z innymi osadzonymi, aby móc prowadzić nielegalną działalność.

[41] Jednym z nałożonych zadań może być np. nawiązanie współpracy z kuratorem.

[42] W wielu jednostkach penitencjarnych funkcjonują np. sale muzyczne i są prowadzone zajęcia nauki gry na instrumentach.

[43] Administracja może modyfikować liczbę osób, które przebywają na spacerze. W tym czasie można obserwować zachowanie innych osadzonych względem danej osoby. Znaczenie ma też to, czy uczestniczy ona w spacerach czy unika wyjścia z celi mieszkalnej.

statusie czy pozycji w grupie może świadczyć to, że pod mury jednostki przybywają osoby, np. członkowie grup pseudokibicowskich, które go wspierają.

Cenna jest również wiedza na temat tego, czy dokonuje on samookaleczeń, zachowuje się w sposób instrumentalny[44], ma tatuaże[45], posługuje się pseudonimem.

Ostatnim elementem, który nie tylko spaja posiadane wiadomości, lecz także daje możliwość ich weryfikacji, są informacje pozyskane od innych osadzonych w ramach czynności profilaktycznych[46]. Przy powierzchownej ocenie mogą one wydawać się błahe. Dlatego tak istotną rolę odgrywa w jednostce profilaktyk[47], czyli osoba wyznaczona do analizowania tych informacji[48]. Należy dodać, że wskazane wyżej dane o osadzonym są zawarte w Centralnej Bazie Danych Osób Pozbawionych Wolności[49].

Pod uwagę warto wziąć również materiały uzyskane z mediów społecznościowych[50] oraz podczas rozmów dyrekcji jednostki z członkami rodziny osadzonego[51]. Ważnym elementem są informacje pozyskane od służb zewnętrznych, ale nie zawsze są one udokumentowane czy sformalizowane[52].

Podsumowanie i wnioski

Całokształt wiedzy, w tym na temat osadzonego, ma wpływ na dwie płaszczyzny:

- wewnętrzną – tj. sposób funkcjonowania osadzonego wewnątrz jednostki, jego rozmieszczenie w niej i współosadzeni, z którymi ma kontakt. Przekłada

[44] Przykładem może być próba samobójcza, aby wymusić decyzję korzystną dla osadzonego.

[45] Tatuowanie nie jest już tak powszechne jak kiedyś. Posiadane tatuaże mogą jednak wiele powiedzieć np. o uczestnictwie w podkulturze, sposobie zachowania się.

[46] Obejmują one nasłuch z rozmów osadzonych, również tych nieformalnych pomiędzy celami, a także bezpośrednie rozmowy z osadzonymi prowadzone przez funkcjonariuszy.

[47] Zob. szerzej: art. 19b ust. 1 ustawy o Służbie Więziennej.

[48] Np. uzyskana z nasłuchu informacja „czarny wjechał na puchę, będzie wesoło" (cytat) pozornie niewiele wnosi. Jednak profilaktyk, który wie, że „czarny" to przywódca pseudokibiców klubu X, a w jednostce przebywają osadzeni przynależący do zwaśnionych grup, może ich izolować.

[49] Baza ta obejmuje szereg modułów, np. zdrowie, pseudonimy, samouszkodzenia. Do modułów tych mają dostęp poszczególne grupy funkcjonariuszy.

[50] W internecie mogą pojawić się informacje o roli osadzonego w grupie, słowa wsparcia czy hejtu i nienawiści kierowane pod jego adresem. Ta wiedza pozwala zapewnić osadzonemu bezpieczeństwo.

[51] Członkowie rodziny mogą mimowolnie przekazać ważną informację, np. że są nachodzeni w miejscu zamieszkania.

[52] Organy ścigania posiadają np. wiedzę, że dana osoba jest członkiem lub liderem grupy zorganizowanej, ale formalnie nie ma jeszcze postawionych zarzutów.

się to na liczbę funkcjonariuszy kierowanych do kontaktu z osadzonym, przy czym pod uwagę bierze się nie tylko ich doświadczenie zawodowe i predyspozycje psychofizyczne, lecz także przeszkolenie w zakresie przeciwdziałania zagrożeniom[53];

- zewnętrzną – to wymiana informacji o osadzonym z innymi podmiotami, m.in. Policją, Agencją Bezpieczeństwa Wewnętrznego, Centralnym Biurem Śledczym Policji. Powinna ona obejmować całokształt posiadanej wiedzy o osadzonym, gdyż to, co dla jednej strony jest oczywiste, dla drugiej nie musi takie być.

Podjęcie opisanych działań wpisuje się w definicję bezpieczeństwa jednostki penitencjarnej, oznaczającą znajomość aktualnych zagrożeń i przewidywanie tych, które mogą zaistnieć, oraz wiedzę na temat procedur (działań) neutralizujących ich wystąpienie lub minimalizujących ich skutki, jak również taki sposób funkcjonowania jednostki, który przekłada się na bezpieczeństwo ludzi w niej przebywających, z akceptowalnym poziomem ryzyka i zagrożeń[54]. Wdrożenie odpowiedniego postępowania nie tylko zwiększy poziom bezpieczeństwa osadzonych i funkcjonariuszy SW, lecz także może pozytywnie wpłynąć na oddziaływania prowadzone przez organy śledcze, a także na postępowania sądowe. Można więc przyjąć, że założony cel artykułu został osiągnięty.

Bibliografia

Grupy dyspozycyjne w obliczu Wielkiej Zmiany. Kulturowe i społeczne aspekty funkcjonowania, J. Maciejewski, M. Bodziany, K. Dojwa (red.), Wrocław 2010.

Łuszcz P., *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia*, Poznań 2025.

Orłowska B., *Współczesne problemy wielokulturowości*, „Horyzonty Wychowania" 2012, t. 11, nr 22, s. 205–223.

Stawarz M., *Podstawy odpowiedzialności za przestępczość zorganizowaną na przykładzie wybranych instrumentów części ogólnej kodeksu karnego*, „Studia Prawnicze" 2023, nr 1 (227), s. 101–129. https://www.doi.org/10.37232/sp.2023e.

Wasilewski E., *Ochrona interesów poszkodowanego w wypadku*, „Forum Służby Więziennej" 2020, nr 263, s. 38–39.

[53] Np. szkolenia dotyczące korupcji bądź postępowania w przypadku próby szantażu.

[54] P. Łuszcz, *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia*, Poznań 2025, s. 174.

Źródła internetowe

Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/przestepczosc-zorganizowana;3963636.html [dostęp: 25 XI 2025].

Sienko P., *Zarzut z 258 kk, czyli udział w zorganizowanej grupie przestępczej*, 1 XII 2024 r., https://sienkoipartnerzy.pl/prawo-karne/zarzut-z-258-kk-czyli-udzial-w-zorganizowanej--grupy-przestepczej/ [dostęp: 4 VIII 2026].

Akty prawne

Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r. (DzU z 2005 r. nr 18 poz. 158).

Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (t.j. DzU z 2025 r. poz. 1750, 1823, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2025 r. poz. 383, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (t.j. DzU z 2025 r. poz. 911, ze zm.).

Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny (DzU z 1969 r. nr 13 poz. 94).

Orzecznictwo

Wyrok Sądu Najwyższego z 13 XI 2013 r., sygn. II KK 170/13.

Wyrok Sądu Najwyższego z 24 III 2009 r., sygn. WA 9/09.

Wyrok Sądu Apelacyjnego w Łodzi z 16 I 2014 r., sygn. II AKa 260/13.

Wyrok Sądu Apelacyjnego w Warszawie z 15 I 2013 r., sygn. II AKa 352/12.

Wyrok Sądu Apelacyjnego w Lublinie z 23 VII 2002 r., sygn. II AKa 148/01, „Prokuratura i Prawo" 2003, nr 4, poz. 20.

Wyrok Sądu Apelacyjnego w Łodzi z 24 I 2001 r., sygn. II AKa 240/01, „Prokuratura i Prawo" 2004, nr 5, poz. 25.

Inne dokumenty

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2024*, K. Kosmala, K. Kachniarz (oprac.), sygn. BEW.0332.17.2024.KK, Warszawa 2025.

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Roczna informacja statystyczna za rok 2025*, K. Kosmala (oprac.), sygn. BEW.0332.17.2025.KKO, Warszawa 2026.

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej, *Miesięczna informacja statystyczna za czerwiec 2026*, M. Milewska (oprac.), sygn. BEW.0332.07.2026.MM, Warszawa 2026.

Ppłk dr Paweł Łuszcz

Funkcjonariusz Służby Więziennej od 2002 r. Obecnie pełni służbę w Zakładzie Karnym w Wojkowicach na stanowisku zastępcy dyrektora. Członek Komisji Unii Europejskiej – Radicalisations Awareness Network. Biegły sądowy przy Sądzie Okręgowym w Kielcach. Laureat konkursu na najlepszą rozprawę doktorską poświęconą problematyce wymiaru sprawiedliwości organizowanego w Szkole Wyższej Wymiaru Sprawiedliwości (obecnie Akademia Wymiaru Sprawiedliwości). Autor książki *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia* oraz wielu publikacji dotyczących funkcjonowania jednostek organizacyjnych Służby Więziennej. Odznaczony srebrną odznaką za zasługi dla pracy penitencjarnej.

Kontakt: pawelmarkus1@wp.pl

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 149–184
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.027.24176

ARTYKUŁ

Służby wywiadu i bezpieczeństwa Chińskiej Republiki Ludowej – struktura, reformy i nadzór nad służbami w erze Xi Jinpinga

Intelligence and Security Services of the People's Republic of China: Structure, reforms, and Oversight in the Xi Jinping Era

MARCIN HUBICKI

Uniwersytet Warszawski

https://orcid.org/0009-0001-1580-8200

Abstrakt

Celem artykułu jest zbadanie współczesnej struktury aparatu wywiadowczego i bezpieczeństwa Chińskiej Republiki Ludowej (ChRL), z uwzględnieniem roli kierowniczo-nadzorczej Komunistycznej Partii Chin (KPCh). Zastosowaną metodą badawczą jest analiza jakościowa danych zastanych. Dane zebrano z dokumentów, komunikatów, ekspertyz, publikacji naukowych i prasowych. W artykule podjęto problem określenia zbioru instytucji zaliczanych do służb wywiadu i bezpieczeństwa ChRL oraz uporządkowania dorobku najnowszej literatury dotyczącego ich zadań, struktury i logiki funkcjonowania w systemie partyjno-państwowym po reformach przeprowadzonych w latach 2013–2025, czyli w czasie rządów sekretarza generalnego KPCh Xi Jinpinga. Z uwagi na specyfikę przedmiotu analizy wyniki nie dostarczają pogłębionej wiedzy na temat aktywności operacyjnej chińskich służb. Jednocześnie badanie identyfikuje podstawowe mechanizmy ich biurokratycznego funkcjonowania i nadzoru nad nimi, umożliwiające zrozumienie roli tych instytucji w systemie bezpieczeństwa ChRL.

Słowa kluczowe służby wywiadowcze i bezpieczeństwa ChRL, Komunistyczna Partia Chin, Ministerstwo Bezpieczeństwa Państwowego, Ministerstwo Bezpieczeństwa Publicznego, studia nad wywiadem

Abstract The aim of the article is to examine the contemporary structure of the intelligence and security services of the People's Republic of China (PRC), with particular consideration given to the leadership and supervisory role of the Chinese Communist Party (CCP). The study is based on a qualitative analysis of secondary data. The data was collected from documents, statements, expert reports, academic publications, and press materials. The article addresses the problem of defining the group of institutions classified as the PRC's intelligence and security services, systematising the most recent literature on their tasks, structure, and the logic of their functioning within the party-state system following the reforms introduced under Xi Jinping as General Secretary of the CCP in the years 2013–2025. Due to the specific nature of the subject under analysis, the findings do not provide in-depth knowledge of operational activities of the Chinese services. At the same time, the study identifies the key mechanisms of their bureaucratic functioning and supervision over them, enabling understanding the role of these institutions within the security system of the PRC.

Keywords PRC intelligence and security services, Chinese Communist Party (CCP), Ministry of State Security (MSS), Ministry of Public Security (MPS), intelligence studies

Wprowadzenie

W ostatnich dekadach wzrost potęgi Chińskiej Republiki Ludowej (ChRL) wiązał się ze zwiększeniem jej aktywności międzynarodowej, w tym działań aparatu wywiadowczego i bezpieczeństwa. Jednocześnie instytucje związane z tym aparatem odgrywają istotną rolę w sprawach wewnętrznych państwa. Z tego powodu analiza obecnych służb ChRL, w tym ich nadzoru ze strony Komunistycznej Partii Chin (KPCh lub Partia), ma znaczenie dla rozumienia funkcjonowania dzisiejszych Chin.

Celem artykułu jest zbadanie współczesnej struktury służb wywiadowczych i bezpieczeństwa ChRL[1], z uwzględnieniem ich roli w systemie partyjno-państwowym po reformach przeprowadzonych w latach 2013–2025 za rządów sekretarza generalnego KPCh Xi Jinpinga[2]. Mimo rosnącej liczby publikacji naukowych i raportów eksperckich poświęconych chińskim służbom literatura przedmiotu pozostaje względnie rozproszona i często nie odzwierciedla ostatnich zmian instytucjonalnych. Brakuje również opracowań w języku polskim poświęconych tej problematyce. Artykuł podejmuje próbę wypełnienia tej luki przez uporządkowanie współczesnego obrazu aparatu wywiadowczego i bezpieczeństwa ChRL. Zagadnienia dotyczące modus operandi chińskich służb oraz problematyki analizy informacji wywiadowczej w ChRL, oba niezwykle trudne jako przedmioty badań, nie stanowią głównego celu rozważań i zostały miejscami jedynie zasygnalizowane.

Zastosowaną metodą badawczą jest analiza jakościowa danych zastanych. Dane pozyskano z analizy dokumentów, komunikatów, ekspertyz, publikacji naukowych i prasowych. Artykuł odpowiada na pytania, jaki jest zakres instytucjonalny służb wywiadowczych i bezpieczeństwa ChRL oraz w jaki sposób reformy przeprowadzone w czasie rządów Xi Jinpinga wpłynęły na współczesną strukturę tych służb oraz system nadzoru nad nimi ze strony KPCh.

W artykule przyjęto strategię badawczą opartą na podejściu partyjnocentrycznym. Perspektywa ta jest ugruntowana wśród badaczy zajmujących się komunistycznymi Chinami[3], w tym również wśród ekspertów z think tanków i rządowych ośrodków analitycznych. Autorytarny system polityczny ChRL i wynikające z niego ograniczenia w dostępie do źródeł sprawiają, że jej przyjęcie jest metodologicznie zasadne. To odmienne podejście od strategii niejednokrotnie obieranych przez ekspertów doraźnie zajmujących się Chinami i często nieznających w dostatecznym stopniu logiki funkcjonowania KPCh. W ich publikacjach chińskie instytucje są opisywane przez pryzmat formalnoprawnych kompetencji lub porównywane z odpowiednikami w państwach demokratycznych. Nierzadko prowadzi to do

[1] W artykule celowo nie zastosowano polskiego terminu „służby specjalne", wprowadzono natomiast termin „służby wywiadowcze i bezpieczeństwa". Lepiej oddaje on charakter aparatu ChRL oraz przedmiot badań, który nie koncentruje się wyłącznie na klasycznym wywiadzie. W kilku przypadkach zastosowano anglojęzyczny zapis nazw skrótów, co wynika z ich dominacji w literaturze przedmiotu i problemu podobieństwa do polskich akronimów. Zgodnie z polską tradycją dla tłumaczeń nazw ministerstw użyto formy przymiotnikowej, chociaż czasem w polskich analizach można napotkać wariant rzeczownikowy. Tłumaczenia w artykule pochodzą od autora.

[2] Xi Jinping swoją najważniejszą funkcję z perspektywy systemu ChRL, czyli sekretarza generalnego KPCh, objął w listopadzie 2012 r. Jego reformy w sferze bezpieczeństwa rozpoczęły się w 2013 r.

[3] Badacze zajmujący się ChRL to m.in.: Joseph Fewsmith, Joseph Torigian, Neil Thomas, Li Ling, Victor Shih, Li Cheng, Adrian Brona.

uproszczeń, redukujących analizę do opisu instytucjonalnych fasad, które w systemie ChRL są drugorzędne wobec mechanizmów partyjnych. Brak dyscypliny w podejściu partyjnocentrycznym może prowadzić do tzw. pekinologii[4], jednak przy zachowaniu rygoru metodologicznego oraz rezygnacji z formułowania pogłębionych wniosków na podstawie fragmentarycznych przesłanek pozostaje ono użytecznym sposobem analizy ChRL, w tym jej struktur bezpieczeństwa.

Stan badań

Wzrost potęgi i aktywności polityczno-gospodarczej ChRL wpłynęły na zainteresowanie badawcze poświęcone jej służbom – o charakterze zarówno naukowym, jak i eksperckim. Widoczny jest trend publikowania tekstów dotyczących tej problematyki przez byłych analityków i oficerów wywiadów państw Zachodu[5], a także rozwój badań już wcześniej aktywnych w ramach studiów regionalnych i studiów nad wywiadem (ang. *intelligence studies*)[6]. Wśród najważniejszych pozycji ostatnich lat szczególne miejsce zajmuje praca Petera Mattisa i Matthew Brazzila pt. *Chinese Communist Espionage: An Intelligence Primer*[7]. Książka ta stanowi bardzo dobre wprowadzenie do tematyki, gdyż oferuje uporządkowaną bazę podstawowych informacji dotyczących historii, kadr oraz współczesnej struktury chińskich służb (choć w tym zakresie już częściowo się zdezaktualizowała). Zawiera też syntetyczne opisy przypadków operacji – zarówno historycznych, jak i współczesnych z pierwszej oraz drugiej dekady XXI w. Dodatkowym walorem książki jest doświadczenie autorów, którzy poza obecną działalnością ekspercką byli zawodowo związani ze strukturami amerykańskiej wspólnoty wywiadowczej i pracowali na kierunku

[4] Jak wskazują Michał Bogusz i Jakub Jakóbowski, w przypadku ChRL odpowiednikiem kremlinologii powinna być raczej zhongnanhaiologia, odnosząca się do Zhongnanhai, czyli siedziby kierownictwa KPCh. Zob. M. Bogusz, J. Jakóbowski, *Zerkając za „bambusową kurtynę": analizowanie Chińskiej Republiki Ludowej*, w: *Uporządkować rzeczywistość. Poradnik analityczny Ośrodka Studiów Wschodnich*, W. Konończuk, M. Menkiszak (red.), Warszawa 2025, s. 380.

[5] Są to m.in.: Nigel Inkster, David R. Shedd, Andrew Badger, Peter Mattis, Nicholas Eftimiades, Matthew Brazil.

[6] Wyniki tych badań są publikowane w czasopismach naukowych, m.in.: „The China Quarterly", „The China Journal", „Intelligence and National Security", „International Journal of Intelligence and Counterintelligence", „Studies in Intelligence", a także w pracach zbiorowych, m.in.: J. Mulvenon, *"Secret Line, Open Line": Inside China's Ministry of State Security*, w: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (red.), Oxford 2025. https://doi.org/10.1093/oxfordhb/9780197783160.013.0046.

[7] P. Mattis, M. Brazil, *Chinese Communist Espionage: An Intelligence Primer*, Annapolis 2019.

chińskim[8]. Należy wyróżnić również starsze publikacje – *Chinese Intelligence Operations* Nicolasa Eftimiadesa oraz *China's Intelligence and Internal Security Forces (Jane's Special Reports*) Howarda DeVore'a[9]. Warto też wskazać książkę Guo Xuezhiego pt. *China's Security State* na temat ewolucji wewnętrznego aparatu bezpieczeństwa[10] oraz publikację Joela Wuthnowa pt. *China's Other Army: The People's Armed Police in an Era of Reform* poświęconą reformie Zbrojnej Policji Ludowej (People's Armed Police, PAP)[11]. Istnieją też opracowania dotyczące specyficznego sektora wywiadu naukowo-technicznego, szpiegostwa przemysłowego i pozyskania na cele badawczo-rozwojowe informacji ze źródeł otwartych[12]. Równolegle ukazują się prace koncentrujące się na historii, a także publikacje popularnonaukowe[13], które upowszechniają informacje o służbach ChRL, choć często – o tym należy pamiętać – zawierają uproszczenia[14]. Tematyka pojawia się także w publikacjach poświęconych strategicznej rywalizacji ChRL z USA, przy czym wątki działań służb są elementami szerszych rozważań odnośnie do stanu relacji obu państw[15]. Dostępne są również publikacje dotyczące systemu inwigilacji i roli służb w jego funkcjonowaniu[16].

Zakres chińskich publikacji na temat współczesnych służb ChRL pozostaje ograniczony z uwagi na cenzurę w tym kraju. Mimo to powstawały wspomnienia i biografie byłych funkcjonariuszy oraz pozycje historyczne, a także wewnątrzresortowe

---

[8] Mattis był m.in. analitykiem ds. kontrwywiadu w Centralnej Agencji Wywiadowczej (Central Intelligence Agency, CIA), Brazil natomiast był m.in. oficerem struktur wywiadowczych podległych Departamentowi Obrony oraz dyplomatą oddelegowanym do Ambasady Stanów Zjednoczonych w Pekinie. Zob. *Chinese Communist Espionage. About the Author*, U.S. Naval Institute, https://www.usni.org/press/books/chinese-communist-espionage#author [dostęp: 5 IX 2026].

[9] N. Eftimiades, *Chinese Intelligence Operations*, Annapolis 1994; H. DeVore, *China's Intelligence and Internal Security Forces (Jane's Special Reports)*, Coulsdon 1999. Nowszą publikacją porównującą studia przypadków operacji jest: N. Eftimiades, *Chinese Espionage. Operations and Tactics*, [bmw] 2020.

[10] X. Guo, *China's Security State: Philosophy, Evolution, and Politics*, Cambridge 2012.

[11] J. Wuthnow, *China's Other Army: The People's Armed Police in an Era of Reform*, Washington 2019.

[12] *China's Quest for Foreign Technology. Beyond Espionage*, W.C. Hannas, D.K. Tatlow (red.), New York 2021; W.C. Hannas, J.C. Mulvenon, A. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, New York 2013. https://doi.org/10.4324/9780203630174.

[13] M. Schoenhals, *Spying for the People: Mao's Secret Agents, 1949–1967*, Cambridge 2013; R. Faligot, *Chinese Spies: From Chairman Mao to Xi Jinping*, London 2019.

[14] I. Smith, N. West, *Historical Dictionary of Chinese Intelligence*, Lanham 2012; D. Wise, *Tiger Trap: America's Secret Spy War with China*, Boston 2011.

[15] Np. *Cold Rivals: The New Era of US-China Strategic Competition*, E.S. Medeiros (red.), Washington 2023.

[16] Np. M. Pei, *The Sentinel State. Surveillance and the Survival of Dictatorship in China*, Cambridge 2024.

opracowania[17]. Istnieją też pozycje tematyczne, w tym opublikowane w chińskich czasopismach branżowych, ale dostęp do nich jest ograniczony[18].

W Polsce ukazały się artykuły m.in. Dariusza Pożaroszczyka, Marcina Adamczyka i Kamila Baraniuka[19]. Część z nich niestety się zdezaktualizowała, zwłaszcza w zakresie opisu organizacji aparatu wojskowego. Z kolei w publikacji Adamczyka i Baraniuka pt. *Wywiad Chińskiej Republiki Ludowej – zarys struktur i metod działalności* wykorzystano „metaforę plaży"[20] jako sposób ujęcia modus operandi wywiadu ChRL. Współcześnie metafora ta bywa krytykowana (np. przez Mattisa i Joskego)[21], choć w dyskursie nadal są obecni jej zwolennicy (np. Eftimades). W Polsce ukazują się też prace dotyczące Chińskiej Armii Ludowo-Wyzwoleńczej (ChALW), jednak tematyka rozpoznania i wywiadu wojskowego jest w nich drugorzędna[22].

Źródłami informacji na temat służb ChRL są także otwarte raporty służb kontrwywiadowczych i wywiadowczych[23], komisji rządowych, parlamentarnych

---

17 D.I. Chambers, *The Past and Present State of Chinese Intelligence Historiography*, „Studies in Intelligence" 2012, t. 56, nr 3, s. 31–46; Ch. Andrew, *The Secret World: A History of Intelligence*, London 2018, s. 752–753.

18 Np. „Guojia Anquan Tongxun" (pol. Biuletyn Bezpieczeństwa Państwowego) – miesięcznik Ministerstwa Bezpieczeństwa Państwowego ChRL o obiegu wewnętrznym/półotwartym.

19 D. Pożaroszczyk, *Wywiad Chińskiej Republiki Ludowej – charakterystyka działalności i zagrożenia dla Polski*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 98–113; M. Adamczyk, K. Baraniuk, *Wywiad Chińskiej Republiki Ludowej – zarys struktur i metod działalności*, „Studia Orientalne" 2017, nr 2, s. 34–58; M. Adamczyk, K. Baraniuk, *Wywiad jako instrument chińskiej polityki zagranicznej – przyczynek do badań*, „Studia Orientalne" 2017, nr 1, s. 41–72. https://doi.org/10.15804/so2017103.

20 „Metafora plaży" (znana także jako „tysiąc ziaren piasku") opisuje pogląd, zgodnie z którym chiński wywiad pozyskuje informacje, masowo wykorzystując szerokie spektrum podmiotów, m.in. studentów, naukowców, przedsiębiorców i przedstawicieli diaspory. Choć służby ChRL rzeczywiście wykorzystują przedstawicieli tych środowisk, to część badaczy uznaje tę metaforę za mylącą. Ich zdaniem błędnie sugeruje ona, że działalność wywiadowcza Chin opiera się na masowym gromadzeniu przez amatorów rozproszonych informacji, przy ograniczonej roli kadrowych oficerów i bez wyraźnego ukierunkowania na priorytetowe cele.

21 P. Mattis, *Assessing Western Perspectives on Chinese Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2012, t. 25, nr 4, s. 680–682. https://doi.org/10.1080/08850607.2012.678745; A. Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, Melbourne 2022, s. 4–5.

22 R. Kwieciński, *W cieniu niepewności. Siła militarna Chin w erze Xi Jinpinga*, Kraków 2023; W. Dziak, M. Pawiński, *Chińska Armia Ludowo-Wyzwoleńcza*, Warszawa 2014.

23 Np. Agencja Bezpieczeństwa Wewnętrznego, *Wybrane aktywności 2024–2025*, Warszawa 2026, s. 15–16; Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2024*, 2025, s. 34.

i śledczych innych państw[24]. Przy tego rodzaju źródłach należy jednak uwzględnić rolę tych podmiotów i kontekst relacji politycznych.

Uzupełniającą bazę stanowią dokumenty i komunikaty sądowe oraz doniesienia w mediach. Zazwyczaj dostarczają one fragmentarycznych informacji, np. odnoszących się do ujawnionych operacji, i nie pozwalają na rekonstrukcję szerszego obrazu działalności. Mogą jednak pełnić funkcję źródeł sygnalizujących aktywność oraz dostarczać podstawowych informacji na temat modus operandi funkcjonariuszy służb ChRL i ich agentury.

W ostatnich latach intensyfikacja prac poświęconych chińskim służbom jest widoczna wśród ekspertów z think tanków i rządowych ośrodków analitycznych. Szczególnie dotyczy to anglosaskich ośrodków, ale i innych[25]. W Polsce brakuje raportów skoncentrowanych na służbach ChRL. Jednocześnie powstają opracowania polskich analityków wprowadzające do zagadnienia funkcjonowania KPCh (m.in. Michała Bogusza, Jakuba Jakóbowskiego, Grzegorza Steca), które przekładają się także na większą zdolność analizy spraw sektora bezpieczeństwa w Chinach.

Dostępnych jest coraz więcej publikacji na temat tzw. operacji wpływu lub obcej ingerencji i w części z nich analizuje się rolę służb ChRL[26]. Wiele ma jednak szerszy zakres badawczy, w którym są uwzględniane aktywności licznych podmiotów partyjno-państwowych ChRL, a nie tylko służb wywiadowczych i bezpieczeństwa. Oprócz tego typu prac istnieją także ekspertyzy i śledztwa dziennikarskie, które nagłaśniają tematykę oddziaływania ChRL na sprawy wewnętrzne innych państw[27].

Reformy przeprowadzone w czasie rządów Xi Jinpinga a struktura służb wywiadowczych i bezpieczeństwa ChRL

W latach 2012–2013 w ChRL doszło do przyspieszenia reform w sektorze bezpieczeństwa, których oficjalnym celem była budowa państwa zorientowanego

[24] Np. US-China Economic & Security Review Commission, Public Inquiry into Foreign Interference (Kanada).

[25] M.in. Jamestown Foundation, Hoover Institution, Australian Strategic Pacific Institute, Center for Strategic and International Studies, Royal United Services Institute. Przykładowa analiza nieanglosaskiego ośrodka: P. Charon, J.-B. Jeangène Vilmer, *Les opérations d'influence chinoises*, Paris 2021.

[26] Np. A. Joske, *Spies and Lies…*, 2022; C. Hamilton, M. Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World*, London 2021.

[27] M.in. J. Manthorpe, *Claws of the Panda: Beijing's Campaign of Influence and Intimidation in Canada*, Toronto 2019; S. Czubkowska, *Chińczycy trzymają nas mocno. Pierwsze śledztwo o tym, jak Chiny kolonizują Europę, w tym Polskę*, Kraków 2022.

na bezpieczeństwo narodowe[28]. Przez ponad dekadę toczenia się tego procesu definicja bezpieczeństwa narodowego rozszerzała się i w 2022 r. obejmowała 16[29], a na koniec 2025 r. 20 obszarów[30]. Fundamentem pozostaje obszar bezpieczeństwa politycznego, będący gwarantem władzy KPCh[31]. Reformy znalazły odzwierciedlenie w tworzeniu i nowelizacji praw, w tym wpływających na aparat wywiadowczy i bezpieczeństwa. Z tego względu zasadne jest wskazanie katalogu ustaw oraz ich ogólny opis. Tabela 1 obrazuje proces rozbudowy ustaw w latach 2013–2025[32].

Tabela 1. Wybrane zmiany prawa ChRL w okresie reform Xi Jinpinga w obszarze bezpieczeństwa.

Sektor	Rok przyjęcia i nowelizacji	Akt prawny	Zakres regulacji	Znaczenie dla aparatu wywiadowczego i bezpieczeństwa
Wywiad, kontrwywiad, ochrona informacji niejawnych	**2015**	ustawa o bezpieczeństwie narodowym	ustawa ramowa dla sektora bezpieczeństwa	ideologiczno-prawna podstawa systemu bezpieczeństwa; ustawa parasolowa, która legitymizuje późniejsze poszerzenie pojęcia bezpieczeństwa narodowego

[28] W języku mandaryńskim „bezpieczeństwo narodowe" i „bezpieczeństwo państwa" są zapisywane tymi samymi znakami 国家安全 (*guojia anquan*), stąd tłumaczenie pozostaje przedmiotem debaty. W tym artykule termin „bezpieczeństwo narodowe" w odniesieniu do ChRL jest rozumiany jako bezpieczeństwo systemu partyjno-państwowego, tj. faktyczna ochrona ciągłości rządów KPCh. Zob. S. Chestnut Greitens, *How Does China Think about National Security?*, w: *The China Questions 2: Critical Insights into US–China Relations*, M. Carrai, J. Rudolph, M. Szonyi (red.), Cambridge 2022, s. 171–177.

[29] Zob. tabelę przygotowaną przez analityków Mercator Institute for China Studies (MERICS): K. Drinhausen, H. Legarda, *'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad*, Berlin 2022, s. 11.

[30] *Xin shidai de Zhongguo guojia anquan* (pol. Bezpieczeństwo narodowe Chin w nowej erze), The State Council Information Office of the People's Republic of China, 12 V 2025 r., http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html, sekcja II [dostęp: 9 II 2026].

[31] J. Nyman, *Towards a Global Security Studies: What Can Looking at China Tell Us About the Concept of Security?*, „European Journal of International Relations" 2023, t. 29, nr 3, s. 675. https://doi.org/10.1177/13540661231176990.

[32] Pełne nazwy ustaw zostały podane w bibliografii załącznikowej (przyp. red.).

Sektor	Rok przyjęcia i nowelizacji	Akt prawny	Zakres regulacji	Znaczenie dla aparatu wywiadowczego i bezpieczeństwa
Wywiad, kontrwywiad, ochrona informacji niejawnych	**2017**	ustawa o wywiadzie narodowym	ogólne ramy funkcjonowania struktur wywiadowczych ChRL	ustawa porządkująca prawo wywiadowcze, która legitymizuje i potwierdza obowiązek współpracy z organami wywiadu; ustawa określa typy organów prowadzących działalność wywiadowczą (organy bezpieczeństwa państwa, organy wywiadowcze bezpieczeństwa publicznego, wojskowe organy wywiadowcze – nie wymienia jednak enumeratywnie konkretnych służb ani nie określa szczegółowego podziału kompetencji między nimi), a także ogólne zasady kierownictwa i koordynacji ich działalności
	2014 (nowelizacja 2023)	ustawa o przeciwdziałaniu szpiegostwu	kontrwywiad	rozszerzenie definicji szpiegostwa i chronionych elementów; rozszerzenie kompetencji służb w zakresie kontrwywiadu, w tym – choć nie dosłownie – Ministerstwa Bezpieczeństwa Państwowego (Ministry of State Security)
	1988 (nowelizacje 2010 i 2024)	ustawa o ochronie tajemnicy państwowej	ochrona informacji niejawnych, kontrwywiad	wzmocnienie kontroli nad obiegiem informacji i odpowiedzialności za naruszenia; rozszerzenie zakresu informacji chronionych o kategorię „tajemnicy służbowej"; formalizacja roli organu KPCh w kształtowaniu polityki ochrony informacji niejawnych
Nadzór, antykorupcja	**2018 (nowelizacja 2024)**	ustawa o nadzorze	nadzór i dyscyplinowanie elit, działania antykorupcyjne	instytucjonalizacja uprawnień Centralnej Komisji Dyscyplinarnej KPCh w strukturach Państwowej Komisji Nadzoru

Sektor	Rok przyjęcia i nowelizacji	Akt prawny	Zakres regulacji	Znaczenie dla aparatu wywiadowczego i bezpieczeństwa
Aparat policyjny i bezpieczeństwa	**1995 (nowelizacja 2012)**	ustawa o Policji Ludowej	status i kompetencje Policji Ludowej	podstawowa regulacja dotycząca policji w ChRL; trwają prace nad nowelizacją, której projekt został opublikowany w styczniu 2026 r.
	2015	ustawa o zwalczaniu terroryzmu	zwalczanie terroryzmu i ekstremizmu	regulacja dotycząca zwalczania klasycznego terroryzmu; jednocześnie legalizacja szerokich działań prewencyjnych; rozszerzające definicje terroryzmu i ekstremizmu umożliwiające ich zastosowanie wobec np. opozycji politycznej, mniejszości
	2009 (nowelizacja 2020)	ustawa o Zbrojnej Policji Ludowej (People's Armed Police, PAP)	podporządkowanie i zadania PAP	ustawowe podporządkowanie PAP wyłącznie Centralnej Komisji Wojskowej i likwidacja podwójnego nadzoru; wcześniej to Ministerstwo Bezpieczeństwa Publicznego (Ministry of Public Security, MPS) sprawowało kontrolę operacyjną nad bieżącym wykorzystaniem PAP w obszarze bezpieczeństwa wewnętrznego
Cyberbezpieczeństwo, wpływy zewnętrzne	**2016**	ustawa o zarządzaniu działalnością zagranicznych organizacji pozarządowych (ang. *non-governmental organization*, NGO) na terytorium ChRL	nadzór nad NGO	de facto prawo przeciw zagranicznym NGO; rejestracja, nadzór i sankcje wobec tych organizacji pod kontrolą MPS; wcześniej pozostawało to w znacznym zakresie pod jurysdykcją Ministerstwa Spraw Cywilnych
	2020	ustawa o bezpieczeństwie narodowym Specjalnego Regionu Administracyjnego Hongkong	funkcjonowanie aparatu bezpieczeństwa w regionie autonomicznym	prawna neutralizacja znacznego zakresu autonomii Hongkongu; legalizacja obecności służb ChRL w Hongkongu; nowe przestępstwa wobec bezpieczeństwa państwa i możliwość przenoszenia spraw do jurysdykcji kontynentalnej

Sektor	Rok przyjęcia i nowelizacji	Akt prawny	Zakres regulacji	Znaczenie dla aparatu wywiadowczego i bezpieczeństwa
Cyberbezpieczeństwo, wpływy zewnętrzne	**2021**	ustawa o bezpieczeństwie danych	dane	dane jako element bezpieczeństwa narodowego; ułatwiony nadzór administracyjny i regulacyjny nad przetwarzaniem danych
	2016 (nowelizacja 2025)	ustawa o cyberbezpieczeństwie	sieci, systemy IT, infrastruktura krytyczna	formalne włączenie cyberprzestrzeni do systemu bezpieczeństwa narodowego; sformalizowanie obowiązków raportowania przez operatorów

Źródło: opracowanie własne.

W realiach systemu ChRL prawo pozostaje ostatecznie podporządkowane dyrektywom KPCh, jednak pełni też funkcję legitymizowania i porządkowania kluczowych mechanizmów funkcjonowania państwa oraz sygnalizuje wagę danej sfery. Przykładem jest ustawa o wywiadzie narodowym, która nie przyznaje kompetencji operacyjnych ani nie określa enumeratywnie katalogu służb, lecz odgrywa przede wszystkim rolę normatywno-ideologiczną. Warto zaznaczyć, że akt ten przewiduje obowiązek współpracy chińskich obywateli i podmiotów gospodarczych z wywiadem (art. 7), co wywołało niepokój części zachodnich ekspertów. Podobne zapisy występowały jednak już w innych ustawach, a w systemie autorytarnym egzekwowanie współpracy nie musi się opierać na przepisach prawa[33].

Akty prawne ChRL nie wskazują enumeratywnie pełnych nazw instytucji wywiadowczych, ograniczając się do wymiany ogólnych kategorii organów (bezpieczeństwa państwowego, publicznego i wywiadu wojskowego). Fakt ten, a także charakter pracy niektórych komórek KPCh sprzyjają temu, że w dyskursie nadmiernie szeroko interpretuje się zakres podmiotowy chińskich służb. Zasadne są zatem uwagi krytyczne wobec takiego podejścia, w ramach którego do „chińskiego wywiadu" bywają zaliczane struktury Komitetu Centralnego (KC) – Departament

[33] Obowiązki współpracy zostały wskazane już m.in. w ustawie o przeciwdziałaniu szpiegostwu (art. 8) i ustawie o zwalczaniu terroryzmu (art. 9). Zob. J. Daum, *What China's National Intelligence Law Says, And Why it Doesn't Matter*, China Law Translate, 22 II 2024 r., https://www.chinalawtranslate.com/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/ [dostęp: 9 II 2026].

Pracy Zjednoczonego Frontu[34] oraz Departament Międzynarodowy[35], który jest odpowiedzialny za współpracę z zagranicznymi ugrupowaniami politycznymi, zwłaszcza komunistycznymi i socjalistycznymi.

Wskazane komórki KC faktycznie współpracują z organami wywiadu i bezpieczeństwa ChRL oraz mogą pełnić funkcję instytucji przykrycia. Nie oznacza to jednak, że stanowią służby wywiadowcze ChRL w ścisłym znaczeniu. Po pierwsze, choć podmioty te odgrywają istotną rolę w rozszerzaniu wpływów politycznych ChRL i w niektórych przypadkach ingerencji wobec państw trzecich, to główne cele ich aktywności nie sprowadzają się do systematycznego pozyskiwania informacji, w tym niejawnych, czy do zwalczania „zagrożeń" z wykorzystaniem wyspecjalizowanej kadry i środków technicznych. Rozszerzanie wpływu, dyplomacja partyjna czy nawet lobbing w tzw. szarej strefie nie są równoznaczne z prowadzeniem działalności wywiadowczej. Po drugie, gromadzenie i analizowanie informacji nie jest wystarczającym kryterium uznania podmiotu za wywiad. Aktywności te są naturalne dla instytucji politycznych lub ich zaplecza, a rozszerzanie definicji wywiadu na wszystkie tego typu organy prowadziłoby do rozmycia znaczenia pojęcia i m.in. do utrudnienia badań.

Trudności pojawiają się także przy „totalnym" definiowaniu wywiadu ChRL, w ramach którego bywają zaliczane instytucje kultury, media, instytuty naukowe, przedsiębiorstwa oraz osoby fizyczne. Nie ma wątpliwości, że część ujawnionych przypadków wskazuje na współpracę tych podmiotów lub operacje z udziałem kadrowych funkcjonariuszy służb ChRL pod ich przykryciem[36]. Równocześnie jednak

---

[34] Departament Pracy Zjednoczonego Frontu KC kieruje tzw. systemem Zjednoczonego Frontu. W wymiarze zewnętrznym obejmuje on m.in. oddziaływanie na diasporę, organizacje, niektóre media, środowiska polityczne i przedsiębiorstwa; w wymiarze wewnętrznym nadzoruje m.in. partie koncesjonowane, kwestie religijne i etniczne oraz sprawy Tajwanu. Choć departament odgrywa wiodącą rolę i odpowiada za koordynację, to działania z zakresu Zjednoczonego Frontu realizują także inne instytucje. Zob. A. Joske, *The party speaks for you: Foreign interference and the Chinese Communist Party's united front system*, Policy brief. Report No 32/2020, Canberra 2020; K.K. Gershaneck, *Political warfare: Strategies for Combating China's Plan to "Win without Fighting"*, Quantico 2020, s. 52–55.

[35] Czeski kontrwywiad w jednym z raportów określił ten departament mianem służby wywiadowczej. Zob. Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2015*, 2016, s. 9.

[36] W kontekście oskarżeń pracowników przedsiębiorstw z ChRL o współpracę z chińskim wywiadem lub bycie kadrowym oficerem warto przywołać sprawę Weijinga W., który pracował w Konsulacie ChRL w Gdańsku, a następnie został dyrektorem w Huawei Polska. W styczniu 2019 r. został on zatrzymany pod zarzutem szpiegostwa na rzecz ChRL. Sprawa miała charakter precedensowy – uchodzi za pierwszy w państwie członkowskim NATO przypadek zatrzymania aktywnego etatowego pracownika Huawei pod zarzutem szpiegostwa. Zob. M. Mikowski, *Dyrektor z Huawei oskarżony o szpiegostwo ponownie zatrzymany*, PAP, 30 VII 2021 r., https://www.pap.pl/aktualnosci/news%2C920081%2Cdyrektor-z-huawei-oskarzony-o-szpiegostwo-ponownie-zatrzymany.html [dostęp:

część spraw w zakresie pozyskania technologii, korupcji lub nielegalnego lobbingu ma charakter oddolny (tj. niebezpośrednio zarządzany przez wywiad ChRL). Z tego powodu wymagane jest zachowanie analitycznego dystansu wobec automatycznego przypisywania każdego typu działań chińskim służbom wywiadowczym w klasycznym ujęciu pojęcia wywiadu[37].

W konsekwencji autor artykułu postuluje podejście łączące ramy prawne z praktyką aparatu Partii, co pozwala ograniczyć pojęcie wywiadu i służb bezpieczeństwa ChRL do instytucji faktycznie wykonujących zadania wywiadowcze, kontrwywiadowcze, policyjne (w tym policji politycznej), antykorupcyjne i nadzorczo-represyjne.

W tabeli 2 pogrupowano instytucje wchodzące w skład szeroko rozumianego aparatu wywiadowczego i bezpieczeństwa ChRL oraz wskazano ich podstawowe zadania i stosowane metody działania.

Tabela 2. Służby wywiadowcze i bezpieczeństwa ChRL – zadania i metody działania.

Kategoria	Instytucja	Zadania i metody działania
Cywilne służby wywiadowcze i bezpieczeństwa oraz policji (w tym policji politycznej)	Ministerstwo Bezpieczeństwa Państwowego (Ministry of State Security)	cywilny wywiad zagraniczny i kontrwywiad wewnętrzny; zadania z zakresu ochrony bezpieczeństwa politycznego, tj. zwalczanie opozycji i zagrożeń ideologicznych
	Ministerstwo Bezpieczeństwa Publicznego (Ministry of Public Security)	ochrona porządku publicznego i bezpieczeństwa wewnętrznego, w tym z zakresu policji politycznej; aktywność wewnątrz ChRL, ale czasami także poza granicami (np. kontrola diaspory); czasem wypełnianie lub wspomaganie zadań kontrwywiadowczych; nadzór nad migracją, zagranicznymi NGO, niektórymi cudzoziemcami i ich przedsiębiorstwami

9 II 2026]. Dla porównania, w Kanadzie w 2018 r. zatrzymano Meng Wanzhou, wiceprezes i córkę założyciela Huawei. Zarzuty dotyczyły jednak naruszenia sankcji. Zob. *The Meng Wanzhou Huawei saga: A timeline*, CBC News, 25 IX 2021 r., https://www.cbc.ca/news/meng-wanzhou-huawei-kovrig-spavor-1.6188472 [dostęp: 6 IX 2026].

[37] Analiza 595 ujawnionych spraw wskazuje, że ok. 22% przypadków (ok. 130 spraw) dotyczyło przedsiębiorstw lub osób działających wyłącznie dla korzyści komercyjnych. Zob. N. Eftimiades, *Chinese Espionage*…, s. 8.

Kategoria	Instytucja	Zadania i metody działania
Służby wywiadu i rozpoznania Chińskiej Armii Ludowo-Wyzwoleńczej (ChALW)	Biuro Wywiadu Połączonego Sztabu Centralnej Komisji Wojskowej	wywiad wojskowy; wykorzystywanie sieci attaché obrony; integracja informacji z różnych źródeł na potrzeby ChALW i kierownictwa KPCh
	jednostki wywiadu i rozpoznania technicznego ChALW (powstałe w wyniku rozwiązania Sił Wsparcia Strategicznego w 2024 r.) znajdujące się w ramach Sił Wsparcia Informacyjnego, Sił Cyberprzestrzeni, Sił Kosmicznych	rozpoznanie; wywiad techniczny (SIGINT, IMINT i in.), działania w cyberprzestrzeni, wsparcie informacyjne i elektroniczne
Siły bezpieczeństwa wewnętrznego	Zbrojna Policja Ludowa (żandarmeria, de facto wojska wewnętrzne i straż przybrzeżna)	działania prewencyjne; zwalczanie terroryzmu, tłumienie zamieszek, ochrona infrastruktury krytycznej; użycie siły paramilitarnej do zadań z zakresu bezpieczeństwa wewnętrznego
Służba antykorupcyjna i aparat nadzoru systemu partyjno-państwowego	Centralna Komisja Kontroli Dyscyplinarnej KPCh (Central Commission for Discipline Inspection, CCDI) / Państwowa Komisja Nadzoru (PKN)	zintegrowany aparat ds. kontroli, antykorupcji i de facto dyscyplinowania elit; nadzór nad Partią i całym sektorem publicznym, w tym przez postępowania dyscyplinarne i quasiśledcze (np. liuzhi); PKN jest tutaj państwowym organem instytucjonalizującym (zasada „jedna instytucja – dwie tabliczki") dla CCDI; oprócz zwalczania korupcji jest to faktyczne narzędzie represji wobec kadr sektora publicznego i podmiotów pozostających w relacjach z aparatem państwa (np. wykonawców przetargów)

Źródło: opracowanie własne.

Ministerstwo Bezpieczeństwa Państwowego (MSS), utworzone w 1983 r.[38], jest organem łączącym cywilny wywiad zagraniczny i kontrwywiad wewnętrzny. Oprócz dwóch podstawowych funkcji MSS realizuje zadania z zakresu zwalczania opozycji politycznej (w tym za granicą) i ochrony systemu politycznego[39]. Aktywność MSS w obszarze wywiadu zagranicznego do końca lat 90. XX w. pozostawała ograniczona. Wynikało to zarówno z konieczności budowy struktur (m.in. rezydentur w placówkach dyplomatycznych), jak i z dominującej roli wywiadu wojskowego, który był preferowany przez kluczowych decydentów KPCh (okresy Deng Xiaopinga, Jiang Zemina)[40]. Działania Jia Chunwanga, który był ministrem bezpieczeństwa państwowego w latach 1985–1998, umożliwiły natomiast rozwój roli wewnętrznej poprzez rozbudowę struktur terenowych MSS, obejmujących prowincje i miasta na prawach prowincji, a także miejscami niższe szczeble administracji[41].

Na początku XXI w. nastąpił wzrost aktywności MSS w wywiadzie zagranicznym. Proces ten objawiał się zwiększeniem liczby klasycznych operacji wywiadowczych przy jednoczesnym zmniejszeniu koncentracji na zwalczaniu opozycji za granicą. Towarzyszyło temu zniesienie części ograniczeń dotyczących obecności oficerów w niektórych ambasadach ChRL i rekrutacji źródeł osobowych[42]. Od lat 90. XX w. zaczęto tworzyć w ramach MSS wyspecjalizowane jednostki do działań w cyberprzestrzeni, funkcjonujące równolegle do wojskowych struktur cybernetycznych. W XXI w. odniosły one sukcesy operacyjne[43]. W okresie rządów Xi Jinpinga ma być dostrzegalne rozszerzanie obszaru kompetencji i operacji MSS, w tym sygnały dotyczące reorganizacji zarządzania strukturami terenowymi. Procesom tym towarzyszy „otwarcie wizerunkowe" MSS, obejmujące m.in. kampanie

[38] Do momentu jego utworzenia w 1983 r. cywilny wywiad zagraniczny działał w komórce partyjnej, tj. Centralnym Wydziale Śledczym KC. Zadania kontrwywiadowcze realizowało MPS.

[39] M. Pei, *Piercing the Veil of Secrecy: The Surveillance Role of China's MSS and MPS*, „China Leadership Monitor" 2024, nr 79, s. 1–3.

[40] P. Mattis, E. Kania, *Modernizing Military Intelligence: Playing Catchup (Part Two)*, „China Brief" 2016, t. 16, nr 19.

[41] P. Mattis, M. Brazil, *Chinese Communist Espionage…*, s. 54–55.

[42] P. Mattis, *The New Normal: China's Risky Intelligence Operations*, The National Interest, 6 VII 2015 r., https://nationalinterest.org/feature/the-new-normal-chinas-risky-intelligence-operations-13260 [dostęp: 27 II 2026].

[43] Przykładem są ataki na Federalne Biuro Zarządzania Kadrami (U.S. Office of Personnel Management, OPM), w wyniku których pozyskano dane milionów obecnych i byłych pracowników administracji USA. Informacje te miały następnie służyć typowaniu przez służby ChRL osób do werbunków. Zob. Ch. Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Federal Bureau of Investigation, 7 VII 2020 r., https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states [dostęp: 27 II 2026].

informacyjne i obchodzenie dnia edukacji w zakresie bezpieczeństwa, utworzenie kanałów w mediach społecznościowych oraz strony do raportowania zagrożeń[44].

Elementem działań MSS jest wykorzystywanie zaplecza w postaci uczelni i think tanków. Najbardziej znanym jest Chiński Instytut Współczesnych Stosunków Międzynarodowych (China Institutes of Contemporary International Relations, CICIR). Choć formalnie brakuje potwierdzenia podporządkowania CICIR, to analitycy wskazują ten ośrodek jako XI. departament centrali MSS[45]. Były szef MSS Geng Huichang, nim objął stanowisko ministra, był dyrektorem CICIR i jego analitykiem ds. USA. Inne ośrodki, np. Szanghajska Akademia Nauk Społecznych[46], mają być wykorzystywane przez funkcjonariuszy jako przykrycie w działaniach operacyjnych. Praktyka ta nie jest jednak specyficzna dla ChRL i istnieje również w państwach demokratycznych, w których podobne instytucje bywają miejscami ulokowania oficerów wywiadu.

Schemat organizacyjny centrali pozostaje niejawny, jednak na podstawie rozproszonych informacji część analityków podejmuje próby rekonstrukcji struktury organizacyjnej MSS[47]. Pod względem organizacyjnym MSS składa się z centrali w Pekinie i komórek terenowych, gdzie MSS obejmuje departamenty (delegatury) bezpieczeństwa państwowego na poziomie prowincji i biura w miastach na prawach prowincji[48], a także niższego szczebla biura w prefekturach oraz niektórych powiatach. W przeciwieństwie do powszechnej struktury terenowej policji system MSS jest bardziej skoncentrowany na poziomie prowincji i prefektur. Według części ekspertów niektóre regionalne delegatury MSS mają swoje specjalizacje zagraniczne[49].

---

[44] S. Chestnut Greitens, *Counter-Espionage and State Security: The Changing Role of China's Ministry of State Security*, „China Leadership Monitor" 2025, nr 83, s. 2.

[45] W. Zajączkowski, *Rozumieć politykę międzynarodową. Metody analizy źródeł otwartych*, Warszawa 2025, s. 101.

[46] *Virginia Man Arrested and Charged With Espionage*, U.S. Department of Justice, 22 VI 2017 r., https://www.justice.gov/opa/pr/virginia-man-arrested-and-charged-espionage [dostęp: 25 II 2026].

[47] Mattis i Brazil w swojej książce piszą o 18 komórkach wchodzących w skład MSS. Z kolei w analizie, której współautorem jest A. Joske, wskazano, że ok. 2018 r. centrala MSS przeszła reorganizację i obecnie obejmuje co najmniej 20 komórek. Zob. P. Mattis, M. Brazil, *Chinese Communist Espionage*…, s. 58; A. Joske, Y. Jeon, *Redesigning State Security: The 2018 Reorganisation of the Ministry of State Security*, „Deserepi: Studies in Chinese Communist Party External Work" 2025, nr 1, s. 1, 16–17.

[48] Na szczeblu prowincji mamy do czynienia z departamentami (*ting*). W miastach na prawach prowincji, mimo ich formalnie równorzędnego statusu, analogiczne jednostki określane są jako biura (*ju*), np. Szanghajskie Biuro Bezpieczeństwa Państwowego (*Shanghai shi guojia anquan ju*).

[49] P. Mattis, *Everything We Know about China's Secretive State Security Bureau*, The National Interest, 10 VII 2017 r., https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459 [dostęp: 25 II 2026].

Ministerstwo Bezpieczeństwa Publicznego (MPS) jest największym cywilnym organem bezpieczeństwa ChRL, realizującym swoje zadania za pośrednictwem rozbudowanej struktury policyjnej[50]. Zakres kompetencji MPS wykracza poza klasyczne zwalczanie przestępczości kryminalnej, obejmując ochronę decydentów, działania antyterrorystyczne i bezpieczeństwo polityczne. Z uwagi na uwarunkowania historyczne, operacyjne i techniczne MPS realizuje również część zadań kontrwywiadowczych, pełniąc funkcję pomocniczą wobec MSS[51]. W sferze zwalczania opozycji i kontrwywiadu kluczową rolę odgrywa Biuro Ochrony Bezpieczeństwa Politycznego (I. Biuro MPS).

MPS działa jako policja polityczna także poza granicami Chin. Są to zarówno jawne, jak i niejawne operacje mające na celu inwigilowanie oraz sprowadzanie do ChRL osób poszukiwanych przez organy bezpieczeństwa[52]. Działania te realizuje się zarówno w ramach oficjalnej współpracy policyjnej, jak i operacji pod przykryciem[53]. MPS reprezentuje również ChRL w Interpolu, co umożliwia mu inicjowanie procedur międzynarodowych, w tym wnioskowanie o wydanie czerwonych not, które mogą być wykorzystywane jako narzędzie do ekstradycji nie tylko pospolitych przestępców, lecz także chińskich dysydentów[54]. W literaturze przedmiotu i raportach wskazuje się na funkcjonowanie nielegalnych posterunków MPS, służących do nadzorowania oraz monitorowania diaspory, zwalczania opozycji i gromadzenia informacji poza terytorium Chin[55].

---

[50] E. Schwarck, *Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China*, „The China Journal" 2018, t. 80, s. 22. https://doi.org/10.1086/697089.

[51] P. Mattis, M. Brazil, *Chinese Communist Espionage…*, s. 40–41.

[52] Zob. M. Walden, *Operation Fox Hunt and China's international efforts to force 'fugitives' back*, ABC News, 18 I 2022 r., https://www.abc.net.au/news/2022-01-19/china-operations-to-force-fugitives-back/100747234 [dostęp: 12 III 2026].

[53] Np. *Nine Individuals Charged in Superseding Indictment with Conspiring to Act as Illegal Agents of the People's Republic of China*, U.S. Department of Justice, 22 VII 2021 r., https://www.justice.gov/archives/opa/pr/nine-individuals-charged-superseding-indictment-conspiring-act-illegal-agents-people-s [dostęp: 6 IX 2026].

[54] Jednym z głównych zadań chińskiego aparatu wywiadowczego i bezpieczeństwa jest zwalczanie działalności dysydentów oraz innych środowisk uznawanych za zagrożenie dla władzy KPCh, w szczególności tzw. Pięciu Trucizn, do których zalicza się: demokratyczną opozycję, ruch Falun Gong oraz ruchy niepodległościowe Tybetu, Tajwanu i Xinjiangu.

[55] *110 Overseas: Chinese Transnational Policing Gone Wild*, Safeguard Defenders, 29 X 2022 r., https://safeguarddefenders.com/en/publications/110-overseas [dostęp: 12 III 2026]; *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government*, U.S. Department of Justice, 17 IV 2023 r., https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government [dostęp: 5 III 2026].

MPS zarządza w Chinach infrastrukturą kontroli, obejmującą systemy CCTV (ang. *closed circuit television*), rejestry, bazy danych (w tym hoteli), nadzór nad cyberprzestrzenią i systemy identyfikacji ludności. MPS podlega Narodowa Administracja Imigracyjna, która odpowiada za kontrolę granic i monitorowanie przepływów ludności. W stosunku do liczby mieszkańców Chin MPS nie jest proporcjonalnie dużą strukturą, stąd od lat wdraża się model proaktywnych działań policyjnych opartych na systematycznej analizie informacji (ang. *intelligence-led policing*). W jego ramach integrowane są informacje pozyskiwane przez komórki MPS w celu prowadzenia działań nie tylko prewencyjnych, lecz także represyjnych[56].

Strukturalnie MPS – podobnie jak MSS – składa się z centrali w Pekinie i rozbudowanej sieci terenowych departamentów bezpieczeństwa publicznego na poziomie prowincji, biur bezpieczeństwa w miastach wydzielonych (równorzędnych prowincjom), a także niższych rangą biur na poziomie prefektur i powiatów, uzupełnianych przez komisariaty na najniższych szczeblach. Jednostki terenowe zachowują pewien stopień autonomii, ale pozostają zależne od lokalnych struktur Partii, a miejscowy szef policji często jest członkiem tych struktur. Z racji liczebności oraz zakresu realizowanych zadań MPS pozostaje znacznie bardziej widocznym elementem chińskiego aparatu bezpieczeństwa niż MSS[57].

Komponenty wywiadu wojskowego ChRL zostały zreorganizowane w wyniku reform Centralnej Komisji Wojskowej (CKW) i ChALW przeprowadzonych z inicjatywy Xi Jinpinga w latach 2015–2016 i kontynuowanych w 2024 r. Poprzednio struktury wywiadu wojskowego funkcjonowały jako zarządy Sztabu Generalnego[58]. W czasie reform zainicjowanych przez Xi Jinpinga Sztab Generalny został przekształcony w Połączony Sztab Generalny wszystkich rodzajów sił zbrojnych ChALW i funkcjonuje jako departament CKW. W jego ramach utworzono **Biuro Wywiadu Połączonego Sztabu**. Odpowiada ono za wojskowy wywiad strategiczny, integrując informacje z innych struktur ChALW, i samodzielnie pozyskuje informacje, w tym przez sieć attaché obrony. Wywiad wojskowy nadzoruje również ośrodki analityczne pełniące funkcje think tanków, instytucji kontaktów międzynarodowych,

[56] E. Schwarck, *Behind the Golden Shield: China Reforms Public Security Intelligence*, „China Brief" 2017, t. 17, nr 16. Więcej na temat *intelligence-led policing* zob. J.H. Ratcliffe, *Intelligence-Led Policing*, London 2016.

[57] Y. Ma, *The Police System in China*, w: *The Routledge Handbook of Chinese Criminology*, L. Cao, I.Y. Sun, B. Hebenton (red.), London–New York 2014, s. 64–67.

[58] Według podziału: II Zarząd (2PLA) odpowiadający za HUMINT, wywiad strategiczny i IMINT; III Zarząd (3PLA) realizujący zadania SIGINT i operacje w cyberprzestrzeni oraz IV Zarząd (4PLA) zajmujący się walką elektroniczną i działaniami informacyjnymi. Działania jednostek cyber miały się częściowo nakładać.

a niekiedy przykrycia[59]. Szczególnie znane są Chiński Instytut Międzynarodowych Studiów Strategicznych (China Institute for International Strategic Studies, CIISS) oraz Chińska Fundacja Międzynarodowych Studiów Strategicznych (China Foundation for International and Strategic Studies, CFISS)[60].

Wywiad i rozpoznanie techniczne wojska zostały w 2015 r. przeniesione do nowo utworzonego rodzaju sił zbrojnych ChALW – Sił Wsparcia Strategicznego (SWS)[61]. Siły te odpowiadały m.in. za SIGINT, działania w cyberprzestrzeni, walkę elektroniczną i wsparcie informacyjne, realizując zadania na potrzeby zarówno CKW, jak i dowództw regionalnych. W 2024 r. SWS zostały rozwiązane, a ich zadania rozdzielone pomiędzy: Siły Wsparcia Informacyjnego, Siły Cyberprzestrzeni i Siły Kosmiczne[62].

Zbrojna Policja Ludowa (PAP) stanowi żandarmerię i de facto wojska wewnętrzne ChRL. Do 2018 r. formacja była podporządkowana jednocześnie CKW i MPS, przy czym minister sprawował nad nią nadzór polityczno-partyjny oraz kierownictwo operacyjne w zakresie ochrony porządku publicznego[63]. Reformy z lat 2017–2018 zniosły dualne kierownictwo i podporządkowały PAP pod CKW, w której szczególną rolę odgrywa sekretarz generalny KPCh jako jej przewodniczący. W ramach PAP funkcjonują komórki rozpoznania i analiz realizujące zadania o charakterze policyjno-wojskowym, a nie strategiczny wywiad. Formacja koncentruje się na utrzymaniu porządku wewnętrznego, reagowaniu na masowe niepokoje, działaniach kontrterrorystycznych, wspomaganiu ChALW w wypadku konfliktu zbrojnego, wsparciu ochrony granic, a także ochrony wód terytorialnych po włączeniu w 2018 r. Straży Przybrzeżnej do jej struktur[64].

---

59 P. Mattis, M. Brazil, *Chinese Communist Espionage…*, s. 51–52.

60 Więcej na temat historii tych instytucji zob. B. Gill, J. Mulvenon, *Chinese Military-Related Think Tanks and Research Institutions*, „The China Quarterly" 2002, t. 171, nr 1, s. 617–624. https://doi.org/10.1017/S0009443902000384.

61 US–China Economic and Security Review Commission, *China's Intelligence Services and Espionage Threats to the US*, 2019, sekcja 3, s. 290.

62 J. Dahm, *A Disturbance in the Force: The Reorganization of PLA Command and Elimination of China's Strategic Support Force*, „China Brief" 2024, t. 24, nr 9.

63 J. Wuthnow, *China's Other Army…*, s. 6–10.

64 T.W. Carberry, *China's People's Armed Police Presents a Significant Force Multiplier During Armed Conflict*, U.S. Army Training and Doctrine Command, 2025, s. 1–3. W niniejszym artykule nie ujęto zwykłych oddziałów ChALW, która nie pełni głównej funkcji organu bezpieczeństwa wewnętrznego, choć stanowi „ostatnią linię" systemu KPCh w przypadku wystąpienia np. dużej skali zamieszek. Milicja Ludowa (*minbing*) odgrywa role zbliżone do gwardii narodowej, rezerw i role pomocnicze w obszarze bezpieczeństwa wewnętrznego. Z zestawienia wyłączono także Centralne Biuro Gwardii, podporządkowane Biuru Generalnemu KC. Centralne Biuro Gwardii jest odpowiedzialne za ochronę kierownictwa Partii.

Centralna Komisja Kontroli Dyscyplinarnej KPCh (CCDI) i jej państwowe rozszerzenie w postaci Państwowej Komisji Nadzoru (PKN) po reformie z 2018 r. pełni funkcje: 1) partyjno-państwowego instrumentu nadzoru, 2) głównego organu antykorupcyjnego, 3) narzędzia dyscyplinowania i realizatora czystek wobec chińskich elit. Choć w większości literatury CCDI nie jest klasyfikowana jako organ bezpieczeństwa wewnętrznego, to reformy przeprowadzone za rządów Xi Jinpinga uzasadniają takie ujęcie w sensie funkcjonalnym. Przemawiają za tym obecne uprawnienia, skala i sposób działania CCDI.

Proces przemiany CCDI w quasiorgan bezpieczeństwa wewnętrznego wpisywał się w szerszą tendencję ekspansji aparatu partyjnego ery Xi Jinpinga i instytucjonalnych reform kolejnych organów według zasady nazywanej „jedna instytucja – dwie tabliczki"[65], przy ograniczaniu znaczenia formalnie autonomicznych mechanizmów urzędniczych. Reforma z 2018 r. zmieniła rozproszony układ nadzoru i jednostek antykorupcyjnych w scentralizowany organ działający jako jedna struktura o dwóch nazwach – CCDI/PKN[66].

Kompetencje dyscyplinarne i dochodzeniowe, wcześniej rozdzielone między tryb partyjny i państwowy, zostały zunifikowane w jednym reżimie, który – w zależności od statusu osoby objętej postępowaniem – działa jako organ partyjny (CCDI) lub państwowy (PKN). Jurysdykcja obejmuje nie tylko członków KPCh (ponad 100 mln) i urzędników administracji, lecz także kierownictwo przedsiębiorstw państwowych i część sektora prywatnego spełniającą kryteria ustawowe (np. wykonawcy zamówień publicznych). W rezultacie aparat CCDI/PKN obejmuje potencjalnie setki milionów osób, a jego prerogatywy i skala działań w erze Xi Jinpinga wykraczają poza klasyczny organ audytu, czyniąc go instrumentem antykorupcyjnym, ale również narzędziem czystek w walkach frakcyjnych[67].

Za uznaniem CCDI jako elementu aparatu bezpieczeństwa wewnętrznego przemawia jej sposób działania. Instytucja dysponuje specjalnymi uprawnieniami quasiśledczymi, w tym procedurą *liuzhi*, która jest wykorzystywana w najcięższych sprawach, m.in. dotyczących przestępstw korupcyjnych lub niedopełnienia obowiązków służbowych[68]. *Liuzhi* umożliwia zatrzymanie osoby poza trybem sądowym,

---

[65] W tym przypadku zasada określana w dokumentach KPCh jako „jedna instytucja – dwie tabliczki" (*yi ge jigou liang kuai paizi*) oznacza, że partyjny organ (CCDI) i jego państwowy odpowiednik (PKN) są kadrowo i organizacyjnie zintegrowane, działając faktycznie jako jedna instytucja.

[66] W ramach reformy rozwiązano m.in. Ministerstwo Nadzoru odpowiadające za urzędników, a także przeniesiono do PKN niektóre komórki Prokuratury Ludowej ds. zwalczania korupcji.

[67] Ch. Carothers, *Xi's Anti-Corruption Campaign: An All-Purpose Governing Tool*, „China Leadership Monitor" 2021, nr 67, s. 1–3.

[68] Po 2018 r. procedura *liuzhi* zastąpiła wcześniejsze partyjne postępowanie dyscyplinarne *shuanggui* i państwowe *liangzhi*.

a następnie jej izolację do sześciu lub ośmiu miesięcy (z możliwością jednokrotnego zrestartowania procedury w przypadku pojawienia się nowych zarzutów). Osoba objęta tą procedurą pozostaje bez dostępu do obrońcy i kontaktu ze światem zewnętrznym[69]. Relacje byłych zatrzymanych w ramach *liuzhi* wskazują na przesłuchania wykraczające poza standardowe działania administracyjne[70]. Oficjalnie KPCh w odpowiedzi na doniesienia o „przekroczeniach uprawnień przez organy nadzoru (tj. CCDI/PKN)" wdrożyła normy nadzoru nad procesem, m.in. w ustawie o funkcjonariuszach organów nadzoru z 2021 r.[71] i w nowelizacji ustawy o nadzorze z 2024 r.[72] Zmiany faktycznie rozszerzyły katalog środków pozasądowych pozostających w dyspozycji CCDI/PKN, formalnie wprowadzając obok *liuzhi* dodatkowe tryby. Według doniesień medialnych w ostatnich latach CCDI rozbudowuje sieć ośrodków odosobnienia. Ośrodki te potencjalnie wzmacniają samodzielność działań CCDI, gdyż są poza jurysdykcją MPS i Ministerstwa Sprawiedliwości[73].

Według oficjalnych danych w latach 2013–2025 w ramach systemu kontroli dyscyplinarnej kierowanego przez CCDI sankcjami dyscyplinarnymi obejmowano średnio ok. 550 000 członków KPCh rocznie. Nie w każdej ze spraw zastosowano procedurę *liuzhi* (lub przed 2018 r. wyżej wymienione środki o zbliżonym charakterze) i nie każda dotyczyła przestępstw korupcyjnych lub kończyła się skierowaniem na tryb karny i wyrokiem. Znaczna część z nich miała finał w postaci sankcji dyscyplinarnych (upomnienie, nagana, degradacja, wydalenie z Partii). W latach 2020–2024 na tryb postępowania karnego przekazywano rocznie średnio 69 000 spraw. Liczba postępowań wobec wyższych przedstawicieli aparatu partyjno-państwowego wynosiła natomiast ok. 56 rocznie[74].

---

[69] *Supervision Law 2024 Revisions – Comparison of new vs. old*, China Law Translate, 26 XII 2024 r., https://www.chinalawtranslate.com/en/supervision-law-2025/ [dostęp: 10 III 2026].

[70] U.S. Department of State, *2024 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)*, https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/china/, sekcja 2c i 3a [dostęp: 6 IX 2026].

[71] Zob. ustawa ChRL o funkcjonariuszach organów nadzoru z 20 VIII 2021 r.

[72] J. Daum, *Keeping an Eye on the Watch Dog (2): Changes to the Supervision Law*, China Law Translate, 3 I 2025 r., https://www.chinalawtranslate.com/en/supervision-law-amendments-overview/ [dostęp: 9 II 2026].

[73] Y. Xiong, *China is building new detention centers all over the country as Xi Jinping widens corruption purge*, CNN, 28 XII 2024 r., https://edition.cnn.com/2024/12/28/china/china-liuzhi-detention-centers-dst-intl-hnk [dostęp: 15 II 2026].

[74] Y. Cao, *China's anti-graft efforts deepen in 2025, with 115 senior officials probed*, China Daily, 17 I 2026 r., https://www.chinadailyhk.com/hk/article/627253 [dostęp: 11 II 2026]; M. Pei, *From Purge to Control: A Recent Pivot in Xi Jinping's Anti-Corruption Crackdown*, „China Leadership Monitor" 2025, nr 83, s. 3–5.

Jeśli chodzi o zarządzanie aparatem, to na czele CCDI stoi członek Stałego Komitetu Biura Politycznego KC. Po reformach z 2018 r. pierwszy zastępca szefa CCDI pełni również funkcję dyrektora PKN, co pokazuje sprzężenie struktur. CCDI podlegają komisje dyscyplinarne struktur terenowych na poziomie prowincji, prefektur i powiatów. W innych jednostkach partyjno-państwowych także funkcjonują komórki dyscyplinarne. Są one wbudowane w te organy, lecz raportują i podlegają przede wszystkim CCDI. W ramach reform rozszerzono ich aktywność, a po 2013 r. stopniowo wzmacniano nadzór centrali CCDI nad siecią tych komórek przez ograniczenie ich podwójnego podporządkowania lokalnym komitetom KPCh. Zwiększono również aktywność specjalnych zespołów inspekcyjnych wysyłanych przez wyższe szczeble systemu organizacyjnego CCDI[75]. Finalizacją procesu była ustawa o nadzorze z 2018 r., która formalnie scentralizowała system[76]. W strukturach ChALW i Ludowej Policji Zbrojnej funkcjonuje autonomiczna Komisja ds. Inspekcji Dyscypliny (CMCCDI) przy CKW. Szef CMCCDI pełni jednocześnie funkcję zastępcy przewodniczącego CCDI. Ma on więc formalnie „podwójną odpowiedzialność". Oznacza to de iure włączenie wojskowego pionu w ogólny system kontroli KPCh, przy jednoczesnym zachowaniu autonomii[77].

W czasie rządów Xi Jinpinga występowały przepływy wyższych kadr kierowniczych pomiędzy CCDI a cywilnymi służbami wywiadowczymi i bezpieczeństwa. Przykładem jest były minister bezpieczeństwa państwowego Chen Wenqing, obecnie członek Biura Politycznego oraz jednocześnie szef komisji nadzorującej służby ChRL. Chen jeszcze przed objęciem teki ministerialnej pełnił funkcję zastępcy szefa CCDI[78]. Kolejnym przykładem jest Liu Jinguo, obecnie zastępca szefa CCDI i dyrektor PKN, który wcześniej był wiceministrem bezpieczeństwa publicznego i szefem komórki dyscyplinarnej wewnątrz tego resortu.

---

[75] C. Carothers, Z. Zhang, *From Corruption Control to Everything Control: The Widening Use of Inspections in Xi's China*, „Journal of Contemporary China" 2023, t. 32, nr 140, s. 225–242. https://doi.org/10.1080/10670564.2022.2071885.

[76] M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin i jej państwo*, Warszawa 2019, s. 89–91.

[77] Po kolejnych czystkach w kierownictwie Centralnej Komisji Wojskowej przeprowadzonych na przełomie 2025 i 2026 r. szczególną pozycję uzyskał gen. Zhang Shengmin – szef CMCCDI i wiceprzewodniczący CKW. Jest on jedynym obok Xi Jinpinga członkiem organu zarządzającego siłami zbrojnymi ChRL (stan na początek 2026 r.).

[78] Chen Wenqing początkowo był funkcjonariuszem policji w MPS, a następnie zajmował różne stanowiska w strukturach MSS.

Rola KPCh i jej zadania nadzorcze w erze Xi Jinpinga

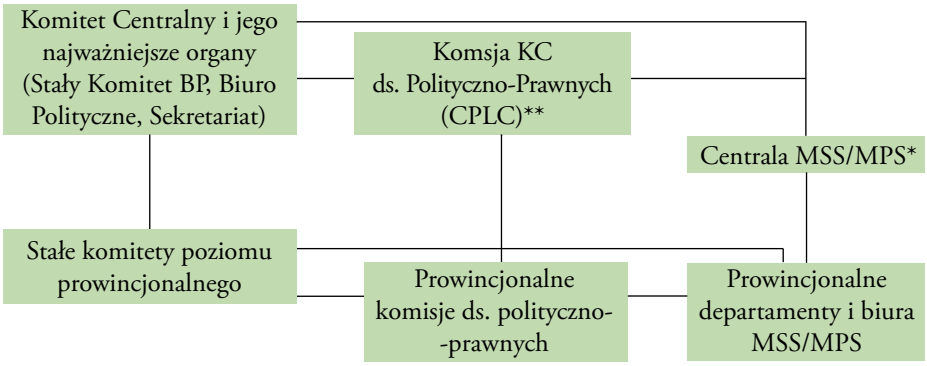
Zwierzchnictwo nad służbami pozostaje w rękach kierownictwa KPCh[79]. W ramach KC funkcjonują wyspecjalizowane departamenty, komisje partyjne i grupy kierownicze realizujące zadania nadzorcze oraz koordynacyjne wobec poszczególnych sektorów polityki państwa. Sektor wojskowy, w tym wywiad ChALW, znajduje się pod zwierzchnictwem CKW. Jeśli chodzi o aktywność zagraniczną, w tym wywiadowczą, znaczenie mają partyjne koordynacyjne grupy kierownicze i komisje (np. ds. zagranicznych, ds. Tajwanu). Z punktu widzenia ogólnego zarządzania i koordynacji nad cywilnymi służbami bezpieczeństwa kluczowe rolę odgrywają: Komisja KC ds. Polityczno-Prawnych (Central Political and Legal Affairs Commission, CPLC) i utworzona po 2013 r. – w wyniku reform Xi Jinpinga – Centralna Komisja Bezpieczeństwa Narodowego (Central National Security Commission, CNSC). CNSC przewodniczy sekretarz generalny KPCh i ma ona przede wszystkim charakter strategiczny, sprawuje nadzór partyjny i wyznacza ogólne kierunki polityki bezpieczeństwa. Jej działanie pozostaje w znacznej mierze niejawne[80]. W codziennym zarządzaniu cywilnym aparatem służb – zwłaszcza w sferze bezpieczeństwa wewnętrznego – większe znaczenie ma CPLC, która nadzoruje MPS, MSS, prokuraturę i sądownictwo[81].

Na rysunku 1 przedstawiono schemat kontroli KPCh nad MPS i MSS.

[79] Najwyższą pozycję w systemie politycznym ChRL zajmuje sekretarz generalny KPCh, będący jednocześnie przewodniczącym ChRL i przewodniczącym CKW. Następne w tym systemie są: Stały Komitet Biura Politycznego, Biuro Polityczne i Komitet Centralny KPCh. Istotną rolę pełnią także Sekretariat KC zajmujący się codziennymi operacjami KC i Biuro Generalne KC (swego rodzaju „kancelaria" kierownictwa). W ramach KC funkcjonują liczne wyspecjalizowane departamenty, grupy i komisje partyjne, realizujące zadania nadzorcze i koordynacyjne. Więcej o zarządzaniu KPCh zob. M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin*…, s. 18–22, 31.

[80] Z. Burdette i in., *Understanding China's National Security Decisionmaking*, Santa Monica 2026, s. 41; J. Wuthnow, *A New Chinese National Security Bureaucracy Emerges*, „China Brief" 2021, t. 21, nr 23.

[81] M. Pei, *The Sentinel State*…, s. 79–80.



* Ministerstwo Bezpieczeństwa Publicznego (MPS) i Ministerstwo Bezpieczeństwa Państwowego (MSS) formalnie podlegają Radzie Państwa ChRL (tj. rządowi).
** W schemacie pominięto Centralną Komisję Bezpieczeństwa Narodowego (CNSC) – ma ona charakter strategiczny, dokładne relacje zarządzania nie są publicznie znane.

Rysunek 1. Kontrola KPCh nad Ministerstwem Bezpieczeństwa Państwowego i Ministerstwem Bezpieczeństwa Publicznego – poziom centralny i prowincjonalny.

Źródło: opracowanie własne.

Bieżącą kontrolę KPCh sprawuje poprzez swoje struktury, system sekretarzy partyjnych oraz hierarchię instytucji aparatu. Na poziomie jednostek terytorialnych struktury władzy Partii odtwarzają model centralny, dlatego istotną pozycję zajmują lokalni sekretarze i komitety KPCh, którym podlegają właściwe dla danego szczebla komisje ds. polityczno-prawnych oraz komisje bezpieczeństwa narodowego. W otoczeniu tych organów działają miejscowe struktury aparatu bezpieczeństwa, które podlegają jednocześnie pionowo swoim centralom i poziomo lokalnym komitetom KPCh[82], co uwidacznia napięcie między zarządzaniem wertykalnym (hierarchią resortową i wyższą partyjną) a horyzontalnym (relacjami z lokalnym aparatem KPCh w prowincjach, miastach na prawach prowincji, prefekturach itd.)[83].

W ostatnich latach widoczne są sygnały centralizacji zarządzania aparatem MSS. Edward Schwarck stwierdza, że reformy z lat 2016–2017 doprowadziły do wzmocnienia „wertykalnego kierownictwa", w ramach którego aparat KC i centrala MSS przejęły większą kontrolę nad polityką kadrową, finansowaniem i nadzorem działalności operacyjnej delegatur terenowych MSS. W efekcie lokalne delegatury MSS w większym

[82] Na temat podziału administracyjnego ChRL i organizacji struktur terenowych KPCh zob. M. Bogusz, *Podział administracyjny ChRL*, Za Wielkim Murem, 18 I 2018 r., https://zawielkimmurem.net/2018/01/18/podzial-administracyjny-chrl/ [dostęp: 6 IX 2026].

[83] M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin…*, s. 38.

stopniu są podporządkowane priorytetom władz centralnych. Ze względu na wysoki poziom niejawności funkcjonowania MSS dostępne dane są ograniczone. To utrudnia pełne odtworzenie reform, przesłanki wskazują jednak na wzmocnienie nadzoru. Inaczej przedstawia się sytuacja terenowych struktur MPS, które jako mniej elitarne, bardziej powszechne i silniej zakorzenione w miejscowych układach są podatniejsze na oddziaływanie lokalnych komitetów KPCh[84].

Istotą zrozumienia systemu zarządzania partyjno-państwowego ChRL – pomijaną w opracowaniach analizujących relacje normatywne – jest rola sekretarzy KPCh i prymat stanowiska partyjnego nad administracyjnym. Z reguły ważniejszym decydentem w resortach pozostaje sekretarz komórki KPCh, stojący wyżej w hierarchii partyjnej niż minister, podczas gdy to na ministrze spoczywa bieżące administrowanie[85]. Natomiast w MSS i MPS stanowiska ministra i sekretarza resortowej komórki partyjnej są łączone i wydaje się, że w czasie rządów Xi Jinpinga ta praktyka jest utrzymywana. Dzięki temu resorty bezpieczeństwa unikają często występującego dwutorowego kierownictwa. W przypadku MSS – z wyjątkiem Chen Wenqinga, który objął funkcję sekretarza w 2015 r.[86], a tekę ministra w listopadzie 2016 r. – ministrowie od momentu utworzenia resortu w 1983 r. łączyli przez większość kadencji obie funkcje. Analogiczna praktyka utrwaliła się w MPS co najmniej od lat 90. XX w., z krótką przerwą w latach 2021–2022, gdy Wang Xiaohong najpierw objął kierownictwo partyjne resortu, a po siedmiu miesiącach stanowisko ministra[87]. Odmiennie zorganizowany jest natomiast system kontroli politycznej w ChALW i PAP. W obu formacjach istnieje system komitetów partyjnych jednostek oraz korpus komisarzy i oficerów politycznych. Komisarze polityczni funkcjonują na wyższych szczeblach struktur wojskowych (od pułku wzwyż, aż po sztaby i wyższe dowództwa), zajmują pozycję równorzędną do dowódców jednostek i odpowiadają za dyscyplinę oraz ideologiczną lojalność wobec KPCh. Na niższych szczeblach (tj. batalionu i kompanii) analogiczne zadania w zakresie pracy partyjno-politycznej realizują instruktorzy i oficerowie polityczni[88].

---

84 E. Schwarck, *The Power Vertical: Centralization in the PRC's State Security*, „China Brief" 2024, t. 24, nr 22.

85 Możliwe są rzadkie wyjątki, gdy minister pełni równocześnie wyższą funkcję w strukturach KPCh niż sekretarz partyjnej komórki w resorcie.

86 K. Lu Huang, *Graft-buster named as head of China's spy agency as anti-corruption watchdog extends its power*, South China Morning Post, 8 X 2015 r., https://www.scmp.com/news/china/policies-politics/article/1865395/graft-buster-named-head-chinas-spy-agency-anti [dostęp: 10 III 2025].

87 E. Xie, *China's Ministry of Public Security gets new party chief amid corruption drive targeting law enforcement*, South China Morning Post, 20 XI 2021 r., https://www.scmp.com/news/china/politics/article/3156802/chinas-ministry-public-security-gets-new-party-chief-amid [dostęp: 6 VI 2026].

88 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024. Annual Report to Congress*, Washington, D.C. 2024, s. 160–161.

Kampanie antykorupcyjne i czystki kadrowe ery Xi Jinpinga objęły również struktury bezpieczeństwa i wywiadu[89]. Symbolicznym przypadkiem jest sprawa z lat 2013–2015 dotycząca Zhou Yongkanga, byłego ministra bezpieczeństwa publicznego i szefa CPLC oraz członka Stałego Komitetu BP KC, który zyskał ogromne wpływy w cywilnych służbach, co jednak nie uchroniło go od utraty pozycji[90]. Początek większej fali czystek i działań antykorupcyjnych w cywilnych strukturach bezpieczeństwa datuje się na 2018 r.[91] Należy ponownie podkreślić, że kampanie dyscyplinarne i antykorupcyjne służą w ChRL nie tylko ograniczaniu nadużyć, lecz także są narzędziem neutralizacji rywali frakcyjnych oraz wzmacniania kontroli nad aparatem wywiadowczym i bezpieczeństwa. Działania antykorupcyjne objęły również struktury ChALW, w tym szefów lub nadzorców wywiadu. Przed erą Xi Jinpinga takim przypadkiem była sprawa gen. Ji Shengde, byłego szefa II Zarządu Sztabu Generalnego (wywiadu) skazanego w 2000 r. W okresie rządów Xi skala kampanii objęła najwyższych dowódców ChALW, w tym członków CKW, m.in. wiceprzewodniczącego gen. Zhang Youxia i szefa Połączonego Sztabu gen. Liu Zhenliego[92].

W zakresie kadry zarządzającej w erze Xi Jinpinga widoczny stał się po XX Zjeździe KPCh wzrost liczby awansów funkcjonariuszy wywodzących się z cywilnych służb lub członków aparatu KPCh specjalizujących się w tym sektorze. Chen Wenqing awansował z funkcji ministra bezpieczeństwa państwowego na sekretarza CPLC, członka Biura Politycznego i członka Sekretariatu KC i stał się pierwszym w historii byłym szefem MSS, który objął tak wysokie stanowiska. Chen Yixin, wieloletni współpracownik Xi Jinpinga i wcześniej członek CPLC, objął stanowisko szefa MSS. Wang Xiaohong, współpracownik Xi Jinpinga w mieście Fuzhou jeszcze z lat 90. XX w., otrzymał najpierw stanowisko sekretarza komitetu KPCh

[89] Np. były wiceminister MSS Ma Jian – dożywocie; były wiceminister MPS (i były prezydent Interpolu) Meng Hongwei – 13,5 roku pozbawienia wolności; były wiceminister MPS Sun Lijun – kara śmierci w zawieszeniu; były wiceminister MPS i minister sprawiedliwości Fu Zhenghua – kara śmierci w zawieszeniu; były szef szanghajskiego Biura Bezpieczeństwa Publicznego Gong Dao'an – dożywocie. Na temat sprawy Fu i Sun zob. G. Wu, *Xi Jinping's Purges Have Escalated. Here's Why They Are Unlikely to Stop*, Asia Society Policy Institute, 26 II 2025 r., https://asiasociety.org/policy-institute/xi-jinpings-purges-have-escalated-heres-why-they-are-unlikely-stop [dostęp: 10 III 2026].

[90] Jego upadek był elementem walki frakcyjnej obejmującej również byłego członka Biura Politycznego KC Bo Xilaia. Reportaż dotyczący tej sprawy zob. P. Ho, W. Huang, *Uderzenie w czerń*, Wołowiec 2015. Analityczny opis zob. M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin…*, s. 70.

[91] M. Pei, *The CCP's Domestic Security Taskmaster: The Central Political and Legal Affairs Commission*, „China Leadership Monitor" 2021, nr 69, s. 5.

[92] Na temat analizy obrazującej skalę czystek i kampanii antykorupcyjnej wewnątrz ChALW i PAP zob. B. Lin i in., *The Purges Within China's Military Are Even Deeper Than You Think*, Center for Strategic and International Studies, 24 II 2026 r., https://chinapower.csis.org/china-pla-military-purges/ [dostęp: 9 III 2026].

w MPS (2021 r.), a następnie tekę ministra bezpieczeństwa publicznego (2022 r.). Po XX Zjeździe KPCh został on również członkiem Sekretariatu KC. W rezultacie kierownictwo MSS, MPS i CPLC zostało obsadzone przez osoby ściśle powiązane z Xi Jinpingiem. Warto przy tym zauważyć, że lider tej grupy, Chen Wenqing, w 2027 r. nadal będzie poniżej nieformalnego progu wieku emerytalnego dla członków najwyższego kierownictwa Partii (tj. 68 lat). Choć w erze Xi zasada ta jest przestrzegana mniej konsekwentnie niż wcześniej, to wiek Chen Wenqinga nadal może stanowić atut w kontekście potencjalnego awansu podczas XXI Zjazdu KPCh[93].

Wnioski

W odpowiedzi na pytania badawcze należy przyjąć, że określenie zakresu instytucji zaliczanych do służb wywiadowczych i bezpieczeństwa ChRL wymaga oparcia się na kryterium partyjno-funkcjonalnym. Po reformach Xi Jinpinga zasadne jest to szersze – nadal zawężone w porównaniu z „totalnym" – ujęcie, obejmujące nie tylko klasyczne organy wywiadu i kontrwywiadu (MSS), wywiadu wojskowego, policji politycznej (MSS, MPS) i bezpieczeństwa publicznego (MPS, PAP), lecz także aparat antykorupcyjny oraz nadzoru w postaci CCDI/PKN, który w okresie rządów Xi Jinpinga ukształtował się jako instytucja o potencjale represyjno-dyscyplinującym.

Reformy z lat 2013–2025 są dowodem koncentracji obecnego kierownictwa KPCh na sprawach bezpieczeństwa, w tym wywiadu i służb. W obszarze wojskowym widoczne są kolejne reorganizacje w postaci utworzenia Biura Wywiadu Połączonego Sztabu, jak również jednostek wywiadu i rozpoznania technicznego po stworzeniu, a następnie rozwiązaniu SWS w 2024 r. Równocześnie cywilne służby (MSS i MPS) zachowują względną stabilność instytucjonalną, choć ich kierownictwo również objęły kampanie antykorupcyjne. PAP została natomiast podporządkowana CKW, z wyłączeniem operacyjnego nadzoru MPS, i stała się podmiotem podlegającym bezpośredniej kontroli sekretarza generalnego KPCh jako przewodniczącego CKW. Można zatem wskazać cztery obszary reform:

1) rozbudowa i porządkowanie ram prawnych, reformy struktur aparatu wywiadowczego i bezpieczeństwa, zwiększenie działań propagandowych w sprawach bezpieczeństwa,
2) sygnały o centralizacji zarządzania MSS i wzmocnieniu modelu „wektorowego", opartego na pionowej kontroli nad delegaturami,

[93] S. Chestnut Greitens, *New Leaders in "National" Security after China's 20th Party Congress*, „China Leadership Monitor" 2023, nr 78, s. 2–16.

3) rozszerzenie kompetencji organu partyjnego CCDI, w tym przez utworzenie jego państwowego przedłużenia (PKN),
4) potencjalny wzrost znaczenia kadr wywodzących się z cywilnego aparatu bezpieczeństwa i nadzoru w Partii.

Istotnym punktem odniesienia dla ostatecznej oceny tych procesów będzie XXI Zjazd KPCh w październiku 2027 r. Szczególnie warty obserwacji jest Chen Wenqing, którego awans oznaczałby pierwszy przypadek wejścia byłego szefa MSS do Stałego Komitetu Biura Politycznego KC.

W odniesieniu do badań nad służbami ChRL należy podkreślić truizm, że jest to obszar stwarzający badaczom duże trudności. Wynikają one zarówno z niejawności sektora, jak i z ograniczeń źródłowych oraz językowych. Mimo to, ze względu na rosnące znaczenie i aktywność ChRL, zasadne jest podejmowanie prób analiz, m.in. porównawczych polegających na zestawianiu chińskich struktur z analogicznymi instytucjami innych państw o zbliżonych systemach (np. porównanie Chin i Wietnamu).

W pewnym zakresie może to być także obszar dla polskich badaczy, którzy dysponują umiejętnościami analizy historycznych struktur bezpieczeństwa państw komunistycznych. Doświadczenia te ułatwiają zrozumienie logiki funkcjonowania systemu partyjnego także w wypadku ChRL. Celowe jest również rozwijanie analiz ujawnionych przypadków operacji i modus operandi chińskich służb wywiadowczych. W Polsce pojawiały się kazusy związane z aktywnością wywiadowczą ChRL lub podejrzenia tej aktywności – m.in. wspomniana już sprawa Weijinga W. czy sprawa, która w wyniku współpracy Agencji Bezpieczeństwa Wewnętrznego z jej szwedzkim odpowiednikiem zakończyła się w 2018 r. skazaniem w Szwecji agenta działającego na rzecz chińskiego wywiadu. Jego oficerem prowadzącym był funkcjonariusz MSS działający pod przykryciem dyplomatycznym w Ambasadzie ChRL w Warszawie, który został wydalony z Polski[94]. Połączenie tych czynników, tj. doświadczenia rodzimych badaczy, aktywności chińskich służb i rosnącej roli ChRL w systemie międzynarodowym, powinno stanowić dla polskiego środowiska naukowego impuls do dalszych badań.

[94] *Stanisław Żaryn: polskie służby przyczyniły się do skazania chińskiego szpiega*, Polskie Radio 24, 30 X 2019 r., https://polskieradio24.pl/artykul/2394461,stanislaw-zaryn-polskie-sluzby-przyczynily-sie-do-skazania-chinskiego-szpiega [dostęp: 6 IX 2026]; *Stanisław Żaryn: W marcu wydalono wicekonsula Rosji w Poznaniu*, Interia, 4 XI 2019 r., https://wydarzenia.interia.pl/kraj/news-stanislaw-zaryn-w-marcu-wydalono-wicekonsula-rosji-w-poznani,nId,3316751 [dostęp: 6 IX 2026].

Bibliografia

Adamczyk M., Baraniuk K., *Wywiad Chińskiej Republiki Ludowej – zarys struktur i metod działalności*, „Studia Orientalne" 2017, nr 2, s. 34–58.

Adamczyk M., Baraniuk K., *Wywiad jako instrument chińskiej polityki zagranicznej – przyczynek do badań*, „Studia Orientalne" 2017, nr 1, s. 41–72. https://doi.org/10.15804/so2017103.

Andrew Ch., *The Secret World: A History of Intelligence*, London 2018.

Bogusz M., Jakóbowski J., *Komunistyczna Partia Chin i jej państwo*, Warszawa 2019.

Bogusz M., Jakóbowski J., *Zerkając za „bambusową kurtynę": analizowanie ChRL*, w: *Uporządkować rzeczywistość. Poradnik analityczny Ośrodka Studiów Wschodnich*, W. Konończuk, M. Menkiszak (red.), Warszawa 2025.

Burdette Z., Mei S., Bujwid E., Burns McCaslin I., Weaver L., Beauchamp-Mustafaga N., Gunness K., *Understanding China's National Security Decisionmaking*, Santa Monica 2026.

Carberry T.W., *China's People's Armed Police Presents a Significant Force Multiplier During* Armed Conflict, U.S. Army Training and Doctrine Command, 2025.

Carothers Ch., *Xi's Anti-Corruption Campaign: An All-Purpose Governing Tool*, „China Leadership Monitor" 2021, nr 67.

Carothers C., Zhang Z., *From Corruption Control to Everything Control: The Widening Use of Inspections in Xi's China*, „Journal of Contemporary China" 2023, t. 32, nr 140, s. 225–242. https://doi.org/10.1080/10670564.2022.2071885.

Chambers D.I., *The Past and Present State of Chinese Intelligence Historiography*, „Studies in Intelligence" 2012, t. 56, nr 3, s. 31–46.

Charon P., Jeangène Vilmer J.B., *Les opérations d'influence chinoises*, Paris 2021.

Chestnut Greitens S., *Counter-Espionage and State Security: The Changing Role of China's Ministry of State Security*, „China Leadership Monitor" 2025, nr 83.

Chestnut Greitens S., *How Does China Think about National Security?*, w: *The China Questions 2: Critical Insights into US–China Relations*, M. Carrai, J. Rudolph, M. Szonyi (red.), Cambridge 2022.

Chestnut Greitens S., *New Leaders in "National" Security after China's 20th Party Congress*, „China Leadership Monitor" 2023, nr 78.

China's Quest for Foreign Technology. Beyond Espionage, W.C. Hannas, D.K. Tatlow (red.), New York 2021.

Cold Rivals: The New Era of US-China Strategic Competition, E.S. Medeiros (red.), Washington 2023.

Czubkowska S., *Chińczycy trzymają nas mocno. Pierwsze śledztwo o tym, jak Chiny kolonizują Europę, w tym Polskę*, Kraków 2022.

Dahm J., *A Disturbance in the Force: The Reorganization of PLA and Elimination of China's Strategic Support Force*, „China Brief" 2024, t. 24, nr 9.

DeVore H., *China's Intelligence and Internal Security Forces (Jane's Special Reports)*, Coulsdon 1999.

Drinhausen K., Legarda H., *'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad*, Berlin 2022.

Dziak W., Pawiński M., *Chińska Armia Ludowo-Wyzwoleńcza*, Warszawa 2014.

Eftimiades N., *Chinese Espionage. Operations and Tactics*, [bmw] 2020.

Eftimiades N., *Chinese Intelligence Operations*, Annapolis 1994.

Faligot R., *Chinese Spies: From Chairman Mao to Xi Jinping*, London 2019.

Gershaneck K.K., *Political Warfare: Strategies for Combating China's Plan to "Win without Fighting"*, Quantico 2020.

Gill B., Mulvenon J., *Chinese Military-Related Think Tanks and Research Institutions*, „The China Quarterly" 2002, t. 171, nr 1, s. 617–624. https://doi.org/10.1017/S0009443902000384.

Guo X., *China's Security State: Philosophy, Evolution, and Politics*, Cambridge 2012.

Hamilton C., Ohlberg M., *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World*, London 2021.

Hannas W.C., Mulvenon J.C., Puglisi A., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, New York 2013. https://doi.org/10.4324/9780203630174.

Ho P., Huang W., *Uderzenie w czerń*, Wołowiec 2015.

Joske A., *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, Melbourne 2022.

Joske A., *The party speaks for you: Foreign interference and the Chinese Communist Party's united front system*, Policy brief. Report No 32/2020, Canberra 2020.

Joske A., Jeon Y., *Redesigning State Security: The 2018 Reorganisation of the Ministry of State Security*, „Deserepi: Studies in Chinese Communist Party External Work" 2025, nr 1, s. 1–19.

Kwieciński R., *W cieniu niepewności. Siła militarna Chin w erze Xi Jinpinga*, Kraków 2023.

Ma Y., *The Police System in China*, w: *The Routledge Handbook of Chinese Criminology*, L. Cao, I.Y. Sun, B. Hebenton (red.), London–New York 2014, s. 64–67.

Manthorpe J., *Claws of the Panda: Beijing's Campaign of Influence and Intimidation in Canada*, Toronto 2019.

Mattis P., *Assessing Western Perspectives on Chinese Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2012, t. 25, nr 4, s. 678–699. https://doi.org/10.1080/08850607.2012.678745.

Mattis P., Brazil M., *Chinese Communist Espionage: An Intelligence Primer*, Annapolis 2019.

Mattis P., Kania E., *Modernizing Military Intelligence: Playing Catchup (Part Two)*, „China Brief" 2016, t. 16, nr 19.

Mulvenon J., *"Secret Line, Open Line": Inside China's Ministry of State Security*, w: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (red.), Oxford 2025, s. 634–651. https://doi.org/10.1093/oxfordhb/9780197783160.013.0046.

Nyman J., *Towards a Global Security Studies: What Can Looking at China Tell Us About the Concept of Security?*, „European Journal of International Relations" 2023, t. 29, nr 3, s. 673–697. https://doi.org/10.1177/13540661231176990.

Pei M., *From Purge to Control: A Recent Pivot in Xi Jinping's Anti-Corruption Crackdown*, „China Leadership Monitor" 2025, nr 83.

Pei M., *Piercing the Veil of Secrecy: The Surveillance Role of China's MSS and MPS*, „China Leadership Monitor" 2024, nr 79.

Pei M., *The CCP's Domestic Security Taskmaster: The Central Political and Legal Affairs Commission*, „China Leadership Monitor" 2021, nr 69.

Pei M., *The Sentinel State. Surveillance and the Survival of Dictatorship in China*, Cambridge 2024.

Pożaroszczyk D., *Wywiad Chińskiej Republiki Ludowej – charakterystyka działalności i zagrożenia dla Polski*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 98–113.

Ratcliffe J.H., *Intelligence-Led Policing*, London 2016.

Schoenhals M., *Spying for the People: Mao's Secret Agents*, 1949–1967, Cambridge 2013.

Schwarck E., *Behind the Golden Shield: China Reforms Public Security Intelligence*, „China Brief" 2017, t. 17, nr 16.

Schwarck E., *Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China*, „The China Journal" 2018, t. 80, s. 1–23. https://doi.org/10.1086/697089.

Schwarck E., *The Power Vertical: Centralization in the PRC's State Security System*, „China Brief" 2024, t. 24, nr 22.

Smith I., West N., *Historical Dictionary of Chinese Intelligence*, Lanham 2012.

Wise D., *Tiger Trap: America's Secret Spy War with China*, Boston 2011.

Wuthnow J., *A New Chinese National Security Bureaucracy Emerges*, „China Brief" 2021, t. 21, nr 23.

Wuthnow J., *China's Other Army: The People's Armed Police in an Era of Reform*, Washington 2019.

Zajączkowski W., *Rozumieć politykę międzynarodową. Metody analizy źródeł otwartych*, Warszawa 2025.

Źródła internetowe

Bogusz M., *Podział administracyjny ChRL*, Za Wielkim Murem, 18 I 2018 r., https://zawielkimmurem.net/2018/01/18/podzial-administracyjny-chrl/ [dostęp: 6 IX 2026].

Cao Y., *China's Anti-Graft Efforts Deepen in 2025, with 115 Senior Officials Probed*, „China Daily", 17 I 2026 r., https://www.chinadailyhk.com/hk/article/627253 [dostęp: 11 II 2026].

Chinese Communist Espionage. About the Author, U.S. Naval Institute, https://www.usni.org/press/books/chinese-communist-espionage#author [dostęp: 5 IX 2026].

Daum J., *Keeping an Eye on the Watch Dog (2): Changes to the Supervision Law*, China Law Translate, 3 I 2025 r., https://www.chinalawtranslate.com/en/supervision-law-amendments-overview/ [dostęp: 9 II 2026].

Daum J., *What China's National Intelligence Law Says, And Why it Doesn't Matter*, China Law Translate, 22 II 2024 r., https://www.chinalawtranslate.com/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/ [dostęp: 9 II 2026].

Lin B., Hart B., Li L., Desai S., Tinsley T., Yang L., Hung F., Chang T.-H., *The Purges Within China's Military Are Even Deeper Than You Think*, Center for Strategic and International Studies, 24 II 2026 r., https://chinapower.csis.org/china-pla-military-purges/ [dostęp: 9 III 2026].

Lu Huang K., *Graft-buster named as head of China's spy agency as anti-corruption watchdog extends its power*, South China Morning Post, 8 X 2015 r., https://www.scmp.com/news/china/policies-politics/article/1865395/graft-buster-named-head-chinas-spy-agency-anti [dostęp: 10 III 2025].

Mattis P., *Everything We Know about China's Secretive State Security Bureau*, The National Interest, 10 VII 2017 r., https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459 [dostęp: 25 II 2026].

Mattis P., *The New Normal: China's Risky Intelligence Operations*, The National Interest, 6 VII 2015 r., https://nationalinterest.org/feature/the-new-normal-chinas-risky-intelligence-operations-13260 [dostęp: 27 II 2026].

Mikowski M., *Dyrektor z Huawei oskarżony o szpiegostwo ponownie zatrzymany*, PAP, 30 VII 2021 r., https://www.pap.pl/aktualnosci/news%2C920081%2Cdyrektor-z-huawei-oskarzony-o-szpiegostwo-ponownie-zatrzymany.html [dostęp: 9 II 2026].

Nine Individuals Charged in Superseding Indictment with Conspiring to Act as Illegal Agents of the People's Republic of China, U.S. Department of Justice, 22 VII 2021 r., https://www.justice.gov/usao-edny/pr/nine-individuals-charged-superseding-indictment-conspiring-act-illegal-agents-people-s [dostęp: 6 IX 2026].

110 Overseas: Chinese Transnational Policing Gone Wild, Safeguard Defenders, 29 X 2022 r., https://safeguarddefenders.com/en/publications/110-overseas [dostęp: 12 III 2026].

Stanisław Żaryn: polskie służby przyczyniły się do skazania chińskiego szpiega, Polskie Radio 24, 30 X 2019 r., https://polskieradio24.pl/artykul/2394461,stanislaw-zaryn-polskie-sluzby--przyczynily-sie-do-skazania-chinskiego-szpiega [dostęp: 6 IX 2026].

Stanisław Żaryn: W marcu wydalono wicekonsula Rosji w Poznaniu, Interia, 4 XI 2019 r., https://wydarzenia.interia.pl/kraj/news-stanislaw-zaryn-w-marcu-wydalono-wicekonsula--rosji-w-poznani,nId,3316751 [dostęp: 6 IX 2026].

Supervision Law 2024 Revisions – Comparison of new vs. old, China Law Translate, 26 XII 2024 r., https://www.chinalawtranslate.com/en/supervision-law-2025/ [dostęp: 10 III 2026].

The Meng Wanzhou Huawei saga: A timeline, CBC News, 25 IX 2021 r., https://www.cbc.ca/news/meng-wanzhou-huawei-kovrig-spavor-1.6188472 [dostęp: 6 IX 2026].

Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government, U.S. Department of Justice, 17 IV 2023 r., https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government [dostęp: 5 III 2026].

Virginia Man Arrested and Charged With Espionage, U.S. Department of Justice, 22 VI 2017 r., https://www.justice.gov/opa/pr/virginia-man-arrested-and-charged-espionage [dostęp: 25 II 2026].

Walden M., *Operation Fox Hunt and China's international efforts to force 'fugitives' back*, ABC News, 18 I 2022 r., https://www.abc.net.au/news/2022-01-19/china-operations-to-force-fugitives-back/100747234 [dostęp: 12 III 2026].

Wray Ch., *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the US*, Federal Bureau of Investigation, 7 VII 2020 r., https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states [dostęp: 27 II 2026].

Wu G., *Xi Jinping's Purges Have Escalated. Here's Why They Are Unlikely to Stop*, Asia Society Policy Institute, 25 II 2025 r., https://asiasociety.org/policy-institute/xi-jinpings-purges-have-escalated-heres-why-they-are-unlikely-stop [dostęp: 10 III 2026].

Xie E., *China's Ministry of Public Security gets new party chief amid corruption drive targeting law enforcement*, South China Morning Post, 20 XI 2021 r., https://www.scmp.com/news/china/politics/article/3156802/chinas-ministry-public-security-gets-new-party-chief-amid [dostęp: 6 VI 2026].

Xiong Y., *China is building new detention centers all over the country as Xi Jinping widens corruption purge*, CNN, 28 XII 2024 r., https://edition.cnn.com/2024/12/28/china/china-liuzhi-detention-centers-dst-intl-hnk [dostęp: 15 II 2026].

Akty prawne

Ustawa ChRL o Policji Ludowej (*Zhonghua Renmin Gongheguo Renmin Jingcha Fa*), 28 II 1995 r.; nowelizacja 26 XII 2012 r.

Ustawa ChRL o bezpieczeństwie narodowym (*Zhonghua Renmin Gongheguo Guojia Anquan Fa*), 1 VII 2015 r.

Ustawa ChRL o zwalczaniu terroryzmu (*Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa*), 27 XII 2015 r.

Ustawa ChRL o zarządzaniu działalnością zagranicznych organizacji pozarządowych na terytorium Chin (*Zhonghua Renmin Gongheguo Jingwai Fei Zhengfu Zuzhi Jingnei Huodong Guanli Fa*), 28 IV 2016 r.

Ustawa ChRL o wywiadzie narodowym (*Zhonghua Renmin Gongheguo Guojia Qingbao Fa*), 27 VI 2017 r.

Ustawa ChRL o Zbrojnej Policji Ludowej (*Zhonghua Renmin Gongheguo Renmin Wuzhuang Jingcha Fa*), 27 VIII 2009 r.; nowelizacja 20 VI 2020 r.

Ustawa ChRL o ochronie bezpieczeństwa narodowego w Specjalnym Regionie Administracyjnym Hongkong (*Zhonghua Renmin Gongheguo Xianggang Tebie Xingzhengqu Weihu Guojia Anquan Fa*), 30 VI 2020 r.

Ustawa ChRL o bezpieczeństwie danych (*Zhonghua Renmin Gongheguo Shuju Anquan Fa*), 10 VI 2021 r.

Ustawa ChRL o funkcjonariuszach organów nadzoru (*Zhonghua Renmin Gongheguo Jiandu Renyuan Fa*), 20 VIII 2021 r.

Ustawa ChRL o przeciwdziałaniu szpiegostwu (*Zhonghua Renmin Gongheguo Fan Jiandie Fa*), 1 XI 2014 r.; nowelizacja 26 IV 2023 r.

Ustawa ChRL o ochronie tajemnicy państwowej (*Zhonghua Renmin Gongheguo Baoshou Guojia Mimi Fa*), 5 IX 1988 r., nowelizacja 27 II 2024 r.

Ustawa ChRL o nadzorze (*Zhonghua Renmin Gongheguo Jiancha Fa*), 20 III 2018 r.; nowelizacja 25 XII 2024 r.

Ustawa ChRL o cyberbezpieczeństwie (*Zhonghua Renmin Gongheguo Wangluo Anquan Fa*), 7 XI 2016 r.; nowelizacja 28 X 2025 r.

Inne dokumenty

Agencja Bezpieczeństwa Wewnętrznego, *Wybrane aktywności 2024–2025*, Warszawa 2026.

Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2015*, 2016.

Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2024*, 2025.

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024. Annual Report to Congress*, Washington, D.C. 2024.

U.S. Department of State, *2024 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)*, https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/china/ [dostęp: 6 IX 2026].

US–China Economic and Security Review Commission, *China's Intelligence Services and Espionage Threats to the United States*, 2019.

Xin shidai de Zhongguo guojia anquan, The State Council Information Office of the People's Republic of China, 12 V 2025 r., http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html [dostęp: 9 II 2026].

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO
2026, nr 35, s. 149-184

Marcin Hubicki

Absolwent Uniwersytetu Jagiellońskiego i Krajowej Szkoły Administracji Publicznej. Doktorant w Szkole Doktorskiej Nauk Społecznych Uniwersytetu Warszawskiego.

Kontakt: m.hubicki@uw.edu.pl

ARTYKUŁY RECENZYJNE / RECENZJE

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 187–197
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.028.24177

RECENZJA

Bezpieczeństwo miasta wobec współczesnych wyzwań, Natalia Moch[1]

IWONA OSŁOWSKA

Autorka niezależna

https://orcid.org/0000-0002-8625-0072



Według Bena Wilsona miasta (…) *mimo swoich ogromnych sukcesów, są brutalnym, bezlitosnym środowiskiem. Oferują perspektywy edukacji i wyższych zarobków, ale mogą skazić dusze i umysł, zatruć płuca. Trzeba nauczyć się w nich żyć, znosić hałas, smog i denerwującą ciasnotę*[2]. Mimo to liczba ich mieszkańców stale rośnie, co potwierdzają dane statystyczne[3].

Tym, co od zawsze przyciągało ludzi do miast, była możliwość przynależności do kultury miejskiej, a obecnie jest to także dostęp do wielu inteligentnych systemów, infrastruktury medycznej i wszystkiego, co ma przełożenie na wysoką

[1] N. Moch, *Bezpieczeństwo miasta wobec współczesnych wyzwań*, Warszawa 2025, Difin, 465 s.

[2] B. Wilson, *Metropolis. Największy wynalazek ludzkości*, Warszawa 2022, s. 15–16.

[3] United Nations. Departament of Economic and Social Affairs, *World Urbanization Prospects 2025. Summary of Results*, New York 2025, https://population.un.org/wup/assets/Publications/undesa_pd_2025_wup2025_summary_of_results_final.pdf [dostęp: 3 VIII 2026].

jakość życia jednostki. W efekcie w ostatnich latach notuje się wzrost zainteresowania przebiegiem i dynamiką procesów urbanizacyjnych, co znajduje odbicie zarówno w dyskusji publicznej, jak i w dyskursie naukowym[4]. Badacze i publicyści omawiają różne aspekty miejskiego uniwersum. Miasto wymaga od nich prowadzenia kompleksowych analiz i wskazywania nowoczesnych rozwiązań, ponieważ stale ewoluuje, a kierunek zachodzących w nim zmian jest dynamiczny.

Wnikliwej oceny jednego z jego elementów, tj. bezpieczeństwa, podjęła się Natalia Moch, której działalność dydaktyczna skupia się wokół zagadnień związanych z systemem bezpieczeństwa narodowego, zarządzaniem kryzysowym oraz bezpieczeństwem miast. W 2025 r. nakładem wydawnictwa Difin ukazała się jej publikacja pt. *Bezpieczeństwo miasta wobec współczesnych wyzwań*. Autorka wskazuje, że dotychczasowe regulacje prawne, dokumenty strategiczne czy plany zarządzania kryzysowego nie ułatwiają kompleksowej oceny i opracowania właściwej polityki w tym zakresie. Jej zdaniem w obecnej narracji brakuje holistycznego podejścia do tego problemu. Przeprowadzone przez nią badania i wyciągnięte na ich podstawie wnioski mogą w przyszłości posłużyć władzom miast do przygotowania rozwiązań poprawiających poziom bezpieczeństwa.

Autorka wyznaczyła sobie pięć celów szczegółowych i postawiła następujące pytania:

1. Jakie są uwarunkowania badań nad bezpieczeństwem miasta?
2. Jak potrzeba bezpieczeństwa wpływała na powstanie i rozwój miast?
3. Jakie są wyzwania dla bezpieczeństwa współczesnych miast we wszystkich sferach ich funkcjonowania?
4. Jak problematyka dotycząca bezpieczeństwa miasta jest przedstawiona w międzynarodowym i krajowym dorobku prawnym i doktrynalnym?
5. Za pomocą jakich narzędzi jest możliwa ocena bezpieczeństwa, a w jej wyniku formułowanie polityki bezpieczeństwa miasta?[5]

Zastosowanie przez autorkę triangulacji metod badawczych w prowadzonej analizie umożliwiło uzyskanie wyników o wysokiej jakości. Dokonany przegląd i ocena bezpieczeństwa miasta pozwoliły odpowiedzieć na główny problem badawczy odnoszący się do zapewnienia bezpieczeństwa w obliczu możliwych do zidentyfikowania zagrożeń. Z kart monografii przebija przeświadczenie, że w ten

[4] Zob. także: C. Moreno, *15-minutowe miasto. Jak uratować nasz czas i planetę*, Kraków 2024; D. Szymańska, *Inteligentne miasta*, Warszawa 2023; S. Gzell, *Urbanistyka XXI wieku*, Warszawa 2020; A. Majer, *Miasto według socjologii. Wybrane tematy*, Łódź 2020; D. Wantuch-Matla, *Przestrzeń publiczna 2.0. Miasto u progu XXI wieku*, Łódź 2016; W. Graham, *Miasta wyśnione. Siedem wizji urbanistycznych, które kształtują nasz świat*, Kraków 2016; J. Kowalczyk, *Bezpieczeństwo przestrzeni współczesnych miast. Przykład Wielkiej Brytanii*, Warszawa 2020.

[5] N. Moch, *Bezpieczeństwo miasta*…, s. 16–17.

proces powinni się włączyć wszyscy interesariusze, tj. mieszkańcy, władze miejskie oraz podmioty publiczne i prywatne. Tylko ich wspólne działania mogą zapewnić komfort funkcjonowania miasta w różnych jego sferach i wpłynąć na poziom bezpieczeństwa.

Pierwszy rozdział monografii jest odpowiedzią na pytanie o uwarunkowania badań nad bezpieczeństwem miasta. Autorka rozpoczyna tę część od opisania ewolucji miasta i jego wpływu na jednostkę. Podkreśla, że badaczom nie udało się jak dotąd wypracować jednej definicji, która w pełni oddawałaby jego istotę, co wymusza sięgnięcie po opracowania z różnych dyscyplin nauki[6]. W związku z tym przywołuje opinie filozofów, socjologów, geografów i urbanistów, którzy w swoich badaniach zajmowali się tą problematyką. Moch wskazuje, że ośrodki miejskie od zawsze różniły się wielkością, położeniem, liczbą mieszkańców i funkcjami. W dalszej kolejności wymienia cechy opisujące współczesne miasto oraz kryteria ich wyodrębnienia. W monografii wyjaśnia fenomen dynamicznego rozwoju współczesnych ośrodków miejskich. Spojrzenie autorki z punktu widzenia jej własnej dyscypliny naukowej stanowi uzupełnienie dotychczasowych badań prowadzonych przez naukowców reprezentujących inne gałęzie nauki. Zaproponowany przez nią interdyscyplinarny wgląd w charakter współczesnego miasta ułatwia zrozumienie zarówno jego, jak i zachodzących w nim procesów, które sprawiają, że jest ono specyficznym systemem współtworzonym przez różne grupy interesariuszy. Na ten system składają się infrastruktura, środowisko, zasoby oraz przepisy prawa miejscowego. Jej zdaniem miasto jako przedmiot badań ma charakter heterogeniczny i można je rozpatrywać w aspektach: empirycznym, humanistycznym, przyrodniczym i społecznym oraz w sferach realnej i konceptualnej.

Moch zwraca uwagę, że podobnie jak w przypadku określenia, czym jest miasto, trudno zdefiniować bezpieczeństwo ośrodków miejskich. Współcześnie nie ogranicza się ono do zapewnienia ochrony przed przestępczością i działań o charakterze stricte policyjnym, lecz obejmuje wiele aspektów miejskiego życia. Wynika to z faktu, że dla jednostki bezpieczeństwo jest drugą najważniejszą potrzebą z piramidy Maslowa[7]. Zwracał na to uwagę także Zygmunt Bauman, który twierdził, że (…) *człowiek cywilizowany rezygnuje częściowo z szansy na szczęście w imię powiększenia szansy bezpieczeństwa*[8]. W naukach o bezpieczeństwie miasta są zarówno podmiotem, jak i przedmiotem. Według współczesnych badaczy pozostają istotnym elementem bezpieczeństwa światowego. Zachodzi w nich wiele problematycznych

[6] Zob. także przegląd definicji zamieszczony w: S. Baraniewicz-Kotasińska, *Smart City. Kto rządzi w inteligentnych miastach?*, Warszawa 2023, s. 21–28.

[7] A. Maslow, *Motywacja i osobowość*, Warszawa 2009, s. 65–66.

[8] Z. Bauman, *Ponowoczesność jako źródło cierpień*, Warszawa 2000, s. 7.

sytuacji współczesnego świata wynikających ze wzrostu przestępczości zorganizowanej, zagrożenia terroryzmem i cyberatakami oraz zmianami klimatycznymi, migracjami, kryzysami ekonomicznymi i energetycznymi, a także z tego, że coraz częściej stają się polem działań wojennych[9]. Dlatego ośrodki miejskie powinny być odporne na zagrożenia i zdolne do reagowania na zmiany. Autorka uważa, że wówczas spełnią pokładane w nich nadzieje odnośnie do bezpieczeństwa. W jej opinii pomocne w osiągnięciu tego stanu będzie zarówno włączenie w prowadzone działania wszystkich grup interesariuszy z danego obszaru, jak i wykorzystanie innowacyjnych oraz tradycyjnych narzędzi.

Po omówieniu zagadnień odnoszących się do miasta jako obiektu badań nauk o bezpieczeństwie oraz jako podmiotu i gwaranta bezpieczeństwa Moch w rozdziale drugim opisuje historię powstania samego miasta. Ujęcie od czasów starożytnych aż do współczesności pozwala przyjrzeć się miastom, które od wieków są (…) *motorami zmian społecznych i kulturowych, postępu technologicznego oraz wymiany dóbr, ludzi i idei*[10]. Autorka scharakteryzowała także czynniki miastotwórcze, w tym: przyrodniczy, gospodarczy, obronny, komunikacyjny, obyczajowo-prawny oraz kompozycji urbanistycznej. Dodatkowo analizuje zmieniające się na przestrzeni wieków koncepcje bezpieczeństwa miasta, a rozważania kończy na czasach współczesnych, kiedy pojęcie bezpieczeństwa zaczęto rozpatrywać w kontekście bezpieczeństwa publicznego, społecznego oraz socjalnego. Omawia kluczowe teorie, w tym m.in. przestrzeni obronnej Oscara Newmana z 1972 r.[11], a także koncepcję dotyczącą zapobiegania przestępczości przez odpowiednie projektowanie przestrzeni (ang. *crime prevention through environmental design*, CPTED) Clarence'a Raya Jeffery'ego[12]. Moch zamieszcza ich krótką charakterystykę, która pozwala lepiej zrozumieć postrzeganie przez tych badaczy spraw związanych z bezpieczeństwem miasta. Następnie omawia nowe spojrzenia zawarte w koncepcji CPTED II autorstwa Gregory'ego Saville'a i Gerry'ego Clevelanda[13] oraz koncepcję CPTED III, której autorami są Mateja Mihinjac i Gregory Saville[14]. Moch wskazuje, że ta ostatnia jest najbliższa koncepcji miasta zrównoważonego, rozwijającego się w kierunku

[9] S. Graham, *Cities as Battlespace: The New Military Urbanism*, „City" 2009, t. 13, nr 4, s. 383–402. https://doi.org/10.1080/13604810903298425.

[10] N. Moch, *Bezpieczeństwo miasta*…, s. 67.

[11] O. Newman, *Defensible Space: Crime Prevention Through Urban Design*, New York 1972.

[12] C.R. Jeffery, *Crime Prevention Through Environmental Design*, Beverly Hills 1971.

[13] G. Cleveland, G. Saville, *Introduction to 2nd Generation to CPTED, pt. 2 – continued from the last issue of CPTED perspective*, „CPTED Perspective: The International CPTED Association Newsletter" 2003, t. 6, nr 2, s. 4–7.

[14] M. Mihinjac, G. Saville, *Third-Generation Crime Prevention Through Environmental Design (CPTED)*, „Social Sciences" 2019, nr 6, s. 1–20. https://doi.org/10.3390/socsci8060182.

inteligentnego miasta (ang. *smart city*). W dalszej kolejności zapoznaje czytelnika z inicjatywą Secured by Design wdrożoną przez ACPO (ang. Association of Chief Officers, obecnie NPCC – National Police Chiefs' Council), wprowadzającą system akredytacji dla produktów wykorzystywanych w przestrzeni publicznej (np. drzwi, okna, zamki, systemy ścian). Jej podstawowe założenie to poprawa bezpieczeństwa budynków i otoczenia przez wdrażanie odpowiednich standardów. Jest to szczególnie istotne w miastach dążących do bycia *smart*, w których także architektura buduje poczucie bezpieczeństwa. W monografii kilkukrotnie odnosi się również do samego pojęcia *smart city* wprowadzonego do dyskursu naukowego w 1992 r., które do tej pory nie doczekało się jednoznacznej definicji[15]. Moch wskazuje, że bezpieczeństwo w miastach ma charakter dynamiczny, a działania zmierzające do jego zapewnienia wykorzystują nowe technologie, co pozwala m.in. monitorować w czasie rzeczywistym stan infrastruktury krytycznej, planować konserwację urządzeń bądź szybko podejmować działania w sytuacjach kryzysowych. Obecnie poczucie bezpieczeństwa w przestrzeni publicznej budują m.in. inteligentne systemy oświetlenia, monitoring miejski, systemy transportowe oraz rozwiązania z zakresu cyberbezpieczeństwa, zwłaszcza dotyczące zabezpieczenia danych. Autorka zwraca ponadto uwagę na wzrost znaczenia i liczbę różnego rodzaju aplikacji wykorzystywanych przez nowoczesne ośrodki, umożliwiających np. mapowanie przestępczości w czasie rzeczywistym, inteligentny nadzór wizyjny, wczesne ostrzeganie o katastrofach czy alarmowanie z wykorzystaniem smartfonów. Opisane w tym rozdziale koncepcje i rozwiązania technologiczne pokazują, że kwestia bezpieczeństwa miasta od dawna pozostawała w zainteresowaniu badaczy i władz. Współcześnie w obliczu globalnych kryzysów potrzeba bezpiecznego miasta jeszcze wzrosła.

W trakcie wielowątkowych rozważań autorka często powraca do zalecenia, by w budowanie bezpiecznego miasta włączyć wszystkich interesariuszy korzystających z przestrzeni miejskiej, ponieważ to oni zmagają się z codziennymi wyzwaniami i zagrożeniami w jej poszczególnych sferach. Zdaniem Moch prowadzenie badań w tym zakresie jest niezbędne przede wszystkim z powodu zmian, jakim podlegają miasta, ich złożoności, niepewności i dynamiczności. Dodatkowo procesy urbanizacyjne mogą powodować wśród mieszkańców poczucie niepewności, a nawet zagrożenia. Badaczka wskazuje na konieczność podejmowania przez władze miast decyzji zmierzających do wcześniejszej identyfikacji potencjalnych niebezpieczeństw. Dowodzi, że wnioski ze zdarzeń mogą być pomocne przy opracowaniu strategii działania miasta. Tej tematyce poświęca trzeci rozdział monografii,

[15] B. Tundys, K.H. Bachanek, E. Puzio, *Smart city. Modele, generacje, pomiar i kierunki rozwoju*, Kraków–Legionowo 2022, s. 67–127; A. Korenik, *Smart Cities. Inteligentne miasta w Europie i Azji*, Warszawa 2019, s. 20–21.

w którym nie tylko opisuje konkretne sfery i podaje przykłady zagrożeń, lecz także wymienia narzędzia pozwalające zapewnić bezpieczeństwo.

Jako pierwszą omawia sferę urbanizacyjno-przestrzenną, w której problemy wynikają z zachodzących procesów urbanizacyjnych. Ich niekontrolowany przebieg może prowadzić do trudności gospodarczych, środowiskowych, organizacyjno-politycznych oraz wymusić nowe spojrzenie na zarządzanie miastem, w tym jego bezpieczeństwem.

Z kolei zjawiska takie jak eksurbanizacja i dzika urbanizacja mogą skutkować trudnościami w kolejnej sferze – gospodarczej i infrastrukturalnej. Przejawiają się one niedostatecznym zapleczem mieszkaniowym, niedostosowaniem usług komunalnych i publicznych do potrzeb mieszkańców, słabą infrastrukturą transportową, energetyczną, telekomunikacyjną, wodną i sanitarną. W kontekście bezpieczeństwa miasta szczególnie istotne w tej sferze jest zapewnienie ciągłości działania infrastruktury krytycznej.

Rozrastające się miasta generują także problemy w sferze społeczno-kulturalnej. Miasto zamieszkują osoby o różnym statusie społecznym, wywodzące się z odmiennych kręgów kulturowych. Skutkiem tego dużego zróżnicowania mogą być konflikty społeczne i podziały, z którymi muszą się zmagać władze miejskie. Dodatkowo współczesne miasta mierzą się ze zjawiskiem ubóstwa miejskiego wynikającego z braku miejsc pracy, z kradzieżami, rozbojami, włamaniami, wandalizmem, chuligaństwem czy obawą przed terroryzmem. Przedmieścia, które miały być synonimem bezpieczeństwa, stwarzają coraz więcej zagrożeń, związanych m.in. ze złym stylem życia prowadzącym do chorób cywilizacyjnych i alienacji społecznej[16]. Autorka szczegółowo omawia problemy odnoszące się do tej sfery i wskazuje, że ze względu na duży obszar i dużą gęstość zaludnienia zapobieganie im stanowi wyzwanie dla miejskiego systemu bezpieczeństwa.

Te dwa elementy oddziałują także na sposób projektowania bezpieczeństwa w odniesieniu do sfery środowiskowo-przyrodniczej. Przeprowadzone przez badaczy analizy potwierdzają, że działania zapobiegające negatywnym zjawiskom bądź usuwającym ich skutki wymagają na obszarze miejskim dużego nakładu sił i środków, ponieważ (…) *miasta funkcjonują na przecięciu dynamicznych systemów naturalnych, ekonomicznych, metabolicznych, społecznych i kulturowych*[17]. Omawiając zagrożenia w tej sferze, autorka nie ogranicza się tylko do opisania możliwości ich wystąpienia w polskich miastach, lecz także podaje przykłady rozwiązań pomocnych w ich neutralizowaniu. W jej opinii współczesne miasta, by sprostać tym

[16] Ch. Montgomery, *Miasto szczęśliwe. Jak zmienić nasze życie, zmieniając nasze miasta*, Kraków 2024, s. 136–137.

[17] J.F.P. Rose, *Dobrze nastrojone miasto. Współczesna nauka, starożytne cywilizacje i ludzka natura: czego mogą nas nauczyć o przyszłości życia w miastach*, Kraków 2019, s. 242.

wyzwaniom, powinny zbudować system wytrzymały na zagrożenia, pozwalający na odbudowanie się w razie konieczności.

Kolejne kwestie dotyczą sfery techniczno-technologicznej i wiążą się z zagrożeniem cyberatakiem. Obecnie miasta gromadzą wiele danych ułatwiających codzienne funkcjonowanie. W niepożądanych rękach te informacje mogą stwarzać zagrożenie. Autorka sygnalizuje konieczność zapewnienia ochrony przed tego typu atakami, ponieważ paraliżują one pracę urzędów i usług świadczonych przez miasta. Moch poleca stosowanie takich narzędzi, jak: sztuczne sieci neuronowe, systemy ekspertowe (specjalistyczne oprogramowanie) czy bezzałogowe statki powietrzne, które mogą zostać wykorzystane m.in. do prognozowania i modelowania procesów miejskich czy diagnozowania ryzyka. Jednocześnie rekomenduje zachowanie ostrożności przy ich stosowaniu i każdorazowe rozważenie potencjalnych korzyści i ewentualnych szkód z tym związanych.

W dalszej części zaleca współpracę władz cywilnych i wojskowych oraz wspólne ćwiczenia w celu zapobiegania zagrożeniom występującym w sferze militarnej i ich eliminowania. Miasta od wieków odgrywały istotną rolę w działaniach wojennych, co pokazują podane przez autorkę przykłady m.in. z okresu II wojny światowej czy czasów współczesnych, jak: Grozny (1995–2000), Mosul (2016–2017), Marawi (2017 r.). Obecnie zwarta zabudowa miast sprzyja prowadzeniu działań obronnych, ogranicza możliwość natarcia i umożliwia prowadzenie walki na różnych poziomach. Jednocześnie ich infrastruktura jest w przeważającej mierze niegotowa do pełnienia funkcji ochronnej dla ludności cywilnej. Dodatkowo realizowanie konkretnych działań obronnych i ochronnych może być utrudnione z powodu niedostatecznego przygotowania lokalnych społeczności na możliwość wystąpienia sytuacji zagrożenia życia. Powszechna w takich przypadkach dezinformacja wywołuje panikę i może prowadzić do wielu szkód na różnych polach. Dlatego Moch wskazuje, że współczesne miasto to (…) *najtrudniejsze i najbardziej złożone pole bitwy*[18], a sfera militarna jest bardzo istotna w kontekście jego bezpieczeństwa.

Właściwe funkcjonowanie każdej z powyższych sfer wpływa na ocenę miasta i, na co zwraca uwagę autorka, jest konieczne do zapewnienia mu bezpieczeństwa. Pomocne w tym zakresie może być opracowanie polityki bezpieczeństwa miasta opartej na identyfikacji, analizie, ewaluacji przy jednoczesnym uwzględnieniu zmieniających się uwarunkowań, tak by systemy miejskie stały się bardziej zintegrowane, odporne i elastyczne.

Jane Jacobs pisała, że (…) *miasta wszystkim mają coś do zaoferowania, pod warunkiem, że wszyscy je współtworzą*[19]. Dlatego działania na ich rzecz prowadzą

[18] N. Moch, *Bezpieczeństwo miasta*…, s. 211.

[19] J. Jacobs, *Śmierć i życie wielkich miast Ameryki*, Warszawa 2014, s. 249.

m.in. Organizacja Narodów Zjednoczonych, Bank Światowy, Organizacja Współpracy Gospodarczej i Rozwoju (Organisation for Economic Cooperation and Development, OECD) oraz Unia Europejska. Procesy zachodzące w miastach, które obecnie obserwujemy, ze względu na dużą liczbę i szybkie tempo sprawiają, że jednostka może czuć się zagubiona. W takiej sytuacji konieczne jest zbudowanie parasola ochronnego, na który w rozwiniętych ośrodkach składają się: kultura, komunikacja, spójność, wspólnota i współodpowiedzialność[20].

Moch poświęciła tym zagadnieniom przedostatni rozdział publikacji, w którym przeanalizowała międzynarodowy i krajowy dorobek prawny pod kątem bezpieczeństwa miasta. Przegląd rozpoczęła od opisu inicjatyw realizowanych przez agencje ONZ, tj. Program Narodów Zjednoczonych ds. Osiedli Ludzkich (United Nations Human Settlements Programme, UN-Habitat), Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (United Nations Office on Drugs and Crime, UNODC) oraz Biuro Narodów Zjednoczonych ds. Ograniczania Ryzyka i Katastrof (United Nations Office for Disaster Risk Reduction, UNDRR). Koncepcje realizowane przez te wyspecjalizowane jednostki mają m.in. uczynić miasta obszarami zrównoważonymi i sprzyjającymi włączeniu społecznemu, przy zaangażowaniu w te działania lokalnych społeczności oraz dzięki prowadzonym szkoleniom, programom i wymianie doświadczeń. Poza tym te agendy wspierają państwa w walce z narkotykami, korupcją, terroryzmem i przestępczością. Złe zarządzanie miastami, w których jest utrudniony dostęp do usług społecznych oraz w których dominują przemoc i strach, wpływa negatywnie nie tylko na ich obraz i codzienność mieszkańców, lecz także na wizerunek danego kraju. Autorka szerzej analizuje elementy zarządzania bezpieczeństwem miasta wskazane przez UNODC, a także zalecenia UNDRR dotyczące budowania jego odporności w kontekście wystąpienia klęsk żywiołowych. Podsumowując działania organizacji, zwraca uwagę czytelnika, że mimo dużego zaangażowania ze strony ONZ problem bezpieczeństwa miasta pozostaje nierozwiązany.

Inicjatywy podejmowane przez Bank Światowy odnoszą się głównie do poprawy systemu planowania i lokalnych możliwości miast, wzmocnienia systemów fiskalnych i finansowych, promowania rozwoju terytorialnego i przestrzennego, budowania odporności klimatycznej i miejskiej, inwestowania w społeczności miejskie, które mają niskie dochody i są marginalizowane. Autorka opisuje je szczegółowo, podobnie jak narzędzia oraz usługi analityczne mające pomóc w sprostaniu wymaganiom urbanizacji. Podkreśla, że Bank Światowy dla podniesienia poziomu bezpieczeństwa miasta stawia na budowanie partnerstw publiczno-prawnych, angażowanie lokalnych społeczności, tworzenie baz wiedzy służących wymianie

[20] J.F.P. Rose, *Dobrze nastrojone miasto*…, s. 28.

doświadczeń oraz oferuje różne metody finansowania i wspiera przekształcanie ośrodków w *smart city*.

W dalszej części rozdziału autorka przedstawia także strategię działania OECD na rzecz budowy bezpiecznego miasta. Wskazuje, że ta instytucja dokonuje przeglądów krajowych polityk miejskich, opracowuje ich standardy i zasady oraz – w ramach forów dialogu – służy wymianie informacji i doświadczeń. Przedstawia narzędzia, które pomagają miastom w osiągnięciu zrównoważonego rozwoju. Szeroko opisuje współpracę OECD z UN-Habitat i Cities Alliance oraz program Krajowa Polityka Miejska (National Urban Policy), pozwalający na monitorowanie polityk miejskich i wypracowanie wspólnego stanowiska odnośnie do rozwoju tych obszarów[21]. Analizy przeprowadzone przez autorkę potwierdzają, że bezpieczeństwo miejskie nie jest kluczową kwestią w programach realizowanych przez OECD. Współczesne miasta pomimo różnorodnych problemów, z którymi zmagają się na co dzień, mają jednak zasoby umożliwiające odbudowę po kryzysie oraz narzędzia pozwalające na zapobieganie im w przyszłości.

Ostatnią przedstawioną w książce organizacją międzynarodową, która angażuje się w budowanie bezpiecznego miasta, jest Unia Europejska. Autorka w nawiązaniu do kluczowych unijnych dokumentów dotyczących tej kwestii omawia proponowane w nich możliwości osiągnięcia przez miasta satysfakcjonującego poziomu bezpieczeństwa, będącego jedną z podstawowych cech miast przyszłości. Wskazuje, że istotną rolę w tym procesie odgrywają urbaniści formułujący politykę przestrzenną oraz osoby i instytucje bezpośrednio zaangażowane w te działania. Ważne w jego przebiegu są też implementacja zaawansowanych technologii informacyjno-komunikacyjnych oraz prowadzenie polityki integracji społecznej zapobiegającej nierównościom i wykluczeniu. Przywołane w monografii dokumenty, m.in.: *Nowa Karta Ateńska – Wizja miast XXI wieku* (2003 r.), *Karta Lipska na rzecz zrównoważonego rozwoju miast europejskich* (2007 r.), *Deklaracja z Toledo* (2010 r.), *Miasta przyszłości. Wyzwania, wizje, perspektywy* (2011 r.), *Agenda Miejska Unii Europejskiej* (2016 r.), *Plan działania na rzecz wspierania ochrony przestrzeni publicznej* (2017 r.), *Plan działania – Partnerstwo agendy miejskiej. Bezpieczeństwo w przestrzeni publicznej* (2020 r.), czy *Agenda terytorialna Unii Europejskiej 2030* (2020 r.), potwierdzają konieczność zapewnienia ochrony przestrzeni publicznej przez podmioty nią zarządzające. Po przeanalizowaniu tych dokumentów autorka stwierdza, że wykorzystanie różnych narzędzi do budowania bezpiecznego miasta i zaangażowanie w ten proces interesariuszy na szczeblu zarówno krajowym, jak i lokalnym przyniesie pozytywne efekty oraz wpłynie na miejską odporność.

[21] Zob. także: *What is National Urban Policy?*, https://unhabitat.org/programme/national-urban-policy [dostęp: 3 VIII 2026].

W tej części omawia również działania instytucji standaryzacyjnych oraz osób prywatnych, które w ramach świadczonych usług, opierając się na stworzonych normach, budują bezpieczne miasta. Rozważania kończy analizą dokumentów o charakterze politycznym i strategicznym dostępnych w polskim dorobku doktrynalnym i prawnym, które odnoszą się do tej kwestii. Dokonany przez nią przegląd działań wymienionych organizacji oraz regulacji prawnych wskazuje na brak dokumentów i metodyk odnoszących się w sposób całościowy do omawianego zagadnienia. Jej zdaniem ich rozproszenie utrudnia władzom miast reagowanie na wyzwania i zagrożenia, zarówno te bieżące, jak i te, które pojawią się w przyszłości.

W ostatniej części Moch rekomenduje narzędzia przydatne do oceny bezpieczeństwa i opracowania polityki bezpieczeństwa. Proponuje, by opierać ją na danych obiektywnych i subiektywnych, co umożliwi zbudowanie całościowej koncepcji, będącej częścią strategii rozwoju miasta. Jej zdaniem decydenci powinni zwrócić uwagę na to, że ośrodki miejskie są wielofunkcyjną społeczno-przestrzenno-gospodarczo-kulturową całością, o specyficznej historii budującej ich tożsamość i uniwersalnych prawidłowościach przestrzenno-funkcjonalnych. Warto przy tym pamiętać, że we współczesnych miastach zachodzi wiele procesów, co utrudnia ścisłe określenie ich przyszłości i kierunku rozwoju. Dodatkowo rosnąca liczba ludności powoduje, że budowanie ich bezpieczeństwa wymaga wielu działań i zaangażowania wszystkich interesariuszy. Autorka zaleca więc, by uwaga rządzących koncentrowała się na redukcji niepewności oraz występujących zagrożeń. W planowaniu, przygotowaniu i koordynacji działań widzi możliwość zwiększenia odporności miasta na rozpoznane i przyszłe kryzysy. Uważa, że na bezpieczeństwo takich ośrodków należy patrzeć w kontekście analizy sytuacji codziennej, jak wydarzenia cykliczne, oraz sytuacji sporadycznej, jak wydarzenia incydentalne. Proponuje przeprowadzanie jego corocznej oceny, co ma ułatwić opracowanie właściwej polityki i strategii bezpieczeństwa miejskiego oraz monitorowanie zmian. Załączony do publikacji przykładowy kwestionariusz badania ankietowego odnoszący się do zagadnień, na które należy zwrócić uwagę w przygotowaniu takiej polityki, może ułatwić jej realizację, monitorowanie oraz eliminowanie słabych stron.

Według Moch na bezpieczeństwo miasta należy patrzeć całościowo, ograniczenie się bowiem do jednego aspektu może prowadzić do fragmentaryzacji zarządzania i braku spójności, a w efekcie to, co wcześniej było wyzwaniem, może stać się zagrożeniem. Proponuje, by politykę bezpieczeństwa opracowywać w 5-letniej perspektywie. Powinna się ona cechować przekrojowym charakterem, holistycznym podejściem i odnosić się do różnych sfer funkcjonowania miasta w kontekście bezpieczeństwa. Podane przykłady konkretnych polityk oraz szczegółowy opis ich przygotowania mogą być pomocne, gdy władze miast robią to po raz pierwszy. Obecnie niewiele z nich decyduje się na taki krok, mimo że jako pierwsze mierzą się

z zagrożeniami. Podjęcie tego trudu będzie opłacalne dla miast, ponieważ są one przyszłością cywilizacji, a liczba ludności w nich już w 2007 r. przewyższyła liczbę mieszkańców wsi i do 2030 r. prawdopodobnie przekroczy 60% w skali globalnej[22]. Na naszej planecie dominują miasta, w których krystalizują się i rozprzestrzeniają nowe idee, a zachodzące procesy urbanizacyjne są jednym z przejawów współczesnej cywilizacji.

Recenzowaną książkę wyróżnia interdyscyplinarne, holistyczne podejście do omawianej materii. Wzbogacają ją wykresy i tabele, a także załączniki dotyczące definiowania pojęcia miasta w różnych krajach świata, obliczania wskaźników do pomiaru bezpieczeństwa w mieście oraz badania poczucia bezpieczeństwa wśród mieszkańców. Te dodatkowe materiały ułatwiają czytelnikowi zrozumienie omawianego zagadnienia, a władzom miast opracowanie stosownych dokumentów, w tym polityki bezpieczeństwa. Autorka przywołuje przykłady odnoszące się zarówno do polskich, jak i zagranicznych miast, w przystępny sposób prezentuje tę złożoną problematykę. Przeprowadzone badania nie tylko stanowią istotny wkład do dorobku nauk o bezpieczeństwie, lecz także pozwalają na identyfikację luk w dokumentach, metodykach i politykach oraz ułatwiają wypracowanie jednolitych standardów oceny poziomu bezpieczeństwa, co może wpłynąć na skuteczność stosowanych rozwiązań. Publikacja może spełniać także funkcję podręcznika akademickiego. Analiza bezpieczeństwa miasta i współczesnych wyzwań z tym związanych została dokonana z wykorzystaniem bogatego aparatu naukowego, co może pomóc w dalszych badaniach tego zjawiska, a osobom po raz pierwszy spotykającym się z tym zagadnieniem ułatwiać poruszanie się po tej skomplikowanej materii. Prowadzenie nad nią dalszych studiów będzie konieczne – miasta przyszłości wciąż się bowiem zmieniają. Badania przeprowadzone przez Natalię Moch służą budowaniu przyjaznej przestrzeni miejskiej i poczucia bezpieczeństwa wśród mieszkańców, którzy w obecnym czasie mogą się obawiać różnego rodzaju zagrożeń wpływających na ich życie i codzienność.

Dr Iwona Osłowska

Kontakt: i.oslowska@wp.pl

[22] M. Degórski, *Suburbanizacja a środowisko – kontekst dobrostanu człowieka*, w: *Suburbanizacja. Człowiek – zmiana – przestrzeń*, M. Grochowski (red. nauk.), Warszawa 2023, s. 98.

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 199–224
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.029.24178

RECENZJA

Szkic do studium przypadku – *Śpiące psy*... Marka Świerczka[1]

WOJCIECH DYLEWSKI

Autor niezależny



W 2025 r. Wydawnictwo LTW opublikowało książkę ppłk. dr. Marka Świerczka pt. *Śpiące psy. Rosyjskie gry agenturalne wobec Urzędu Ochrony Państwa początkiem lat 90. XX w*. Jest ona poświęcona analizie sprawy aresztowania w 1993 r. i następnie skazania w 1994 r. za szpiegostwo na rzecz ZSRR/Rosji byłego funkcjonariusza Służby Bezpieczeństwa PRL Marka Zielińskiego.

Autor książki jest byłym funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego. W latach 2023–2024 pełnił funkcję redaktora naczelnego „Przeglądu Bezpieczeństwa Wewnętrznego". W 2017 r. obronił rozprawę doktorską, której tematem była sowiecka dezinformacja w okresie międzywojennym, ze szczególnym uwzględnieniem operacji „Trust". Jak wynika z informacji na okładce, w dorobku ma również kilkadziesiąt artykułów naukowych i cztery monografie, a także cztery powieści „będące

[1] M. Świerczek, *Śpiące psy. Rosyjskie gry agenturalne wobec Urzędu Ochrony Państwa początkiem lat 90. XX w.*, Łomianki 2025, Wydawnictwo LTW, 318 s.

hybrydami literatury historycznej i grozy" oraz kilkanaście opowiadań fantastycznych.

Książka ma dwóch recenzentów: prof. dr. hab. Grzegorza Łukomskiego, który z wykształcenia jest historykiem, oraz dr. hab. Dominika Smyrgałę, eksperta ds. bezpieczeństwa związanego ze Służbą Kontrwywiadu Wojskowego (w 2007 r.), głównego analityka w Ośrodku Monitorowania i Analiz Ministerstwa Obrony Narodowej (2016–2017), szefa Gabinetu Politycznego Ministra Obrony Narodowej Antoniego Macierewicza (2017 r.), podsekretarza stanu w MON (2017–2018).

Już na wstępie chciałbym zaznaczyć, że nie podzielam opinii autora *Śpiących psów*… co do sprawy Zielińskiego oraz kreowanego przez niego obrazu organizacji, pracy, wyposażenia, potencjału operacyjnego oraz efektywności Urzędu Ochrony Państwa (UOP) na początku lat 90. XX w. W książce został wykreowany obraz naiwnych Polaków, po raz kolejny wodzonych za nos i zmanipulowanych przez Rosjan w celu ochrony rosyjskiej agentury uplasowanej gdzieś wysoko w strukturach służb specjalnych lub nawet w strukturach państwa.

Uważam, że w dobie coraz bardziej agresywnych działań służb specjalnych Federacji Rosyjskiej w ramach prowadzonej także przeciwko Polsce wojny hybrydowej przedstawiony w książce de facto zniesławiający obraz UOP oraz ocena sprawy Zielińskiego jako przegranej przez Polskę gry wywiadowczej są nie tylko nieprawdziwe, lecz także szkodliwe. Mogą podważać zaufanie społeczeństwa do państwa i skuteczności działań jego służb, jak również mogą mieć negatywny wpływ na motywację funkcjonariuszy.

W trosce o prawdę historyczną, obiektywną ocenę faktów i procesów publikacja ta wymaga reakcji, aby umożliwić czytelnikowi krytyczne spojrzenie na opisywaną w książce rzeczywistość na początku lat 90. XX w. Moim zdaniem jest to szczególnie ważne dla funkcjonariuszy będących aktualnie w służbie czynnej, gdyż wielu z nich zna okres budowy demokratycznego państwa po wyborach w 1989 r. jedynie z różnych, przeważnie subiektywnych relacji. Różnice wynikające z kontekstu historycznego, odmienność otoczenia oraz wyjątkowość sytuacji, gdy zmieniał się ustrój państwa i cały kontekst geopolityczny, utrudniają dziś, często w znacznym stopniu, ocenę ówczesnych decyzji, wyciąganych wniosków oraz sposobów i metod pracy operacyjnej. Bez dokładnej znajomości tła historycznego pełne zrozumienie zdarzeń będzie niemożliwe, a ich ocena – nieprawdziwa.

Autor *Śpiących psów*… deklaruje, że jego książka to publikacja naukowa. Nie sposób się z tym zgodzić. Marek Świerczek formułuje trzy hipotezy badawcze i uznaje za prawdziwą jedną z nich na podstawie uznania za fałszywe dwóch pozostałych. Nie jest to metoda naukowa, również z uwagi na to, że trzy hipotezy autora książki nie są jedynymi, które można postawić w analizowanej sytuacji. Na dodatek

dowody na fałszywość dwóch hipotez przedstawione przez autora książki nie są przekonujące oraz dopuścił się on wielu przeinaczeń, mieszając fakty z fikcją. Postaram się to wykazać w niniejszej recenzji.

Problem źródeł

Analizę sprawy Zielińskiego autor książki oparł na aktach sądowo-prokuratorskich, które opisują jedynie częściowo i w specyficznie sformalizowany sposób fragment rzeczywistości badany w czasie procesu. Warto zauważyć, że praktycy przygotowujący materiał operacyjny do postępowania dowodowego uznają, że sądowo można wykorzystać przeważnie 20–25% takiego materiału. Oczywiście zdarzają się wyjątki, chociaż większość spraw wskazuje raczej na mniejszy zakres wykorzystania[2]. Problematyka tzw. uprocesowienia materiałów operacyjnych stwarza trudności wszystkim służbom na świecie, nawet mimo lokalnych ułatwień prawno-procesowych.

Autor książki informuje, że kontaktował się z Markiem Zielińskim, ale odmówił on współpracy (s. 7). Trudno zrozumieć, dlaczego nie skontaktował się z oficerami UOP biorącymi udział w sprawie, zarówno na jej operacyjnym, jak i procesowym etapie. To grono kilkunastu osób, do których Marek Świerczek nie dotarł.

Autor miał dostęp, jak wskazuje, do zeznań złożonych podczas procesu Zielińskiego, zawartych w odtajnionych materiałach Instytutu Pamięci Narodowej (sygn. IPN BU 3790/1-5), i to one stanowią podstawę wywodu (s. 7). Wcześniej akta sądowe dotyczące tej sprawy były przechowywane w archiwum Sądu Okręgowego w Warszawie (sygnatura SO 84/94).

W 2017 r., gdy ukazywała się książka Tomasza Piątka pt. *Macierewicz i jego tajemnice*[3], opisująca powiązania jednej z osób z otoczenia ministra Antoniego Macierewicza ze Służbą Bezpieczeństwa, ówczesny minister obrony narodowej zaczął przeglądać teczki spraw sądowych szpiegów złapanych przez UOP ćwierć wieku wcześniej[4].

Akta sądowe sprawy Zielińskiego zostały udostępnione także Annie Gielewskiej i Marcinowi Dzierżanowskiemu, autorom książki *Antoni Macierewicz. Biografia nieautoryzowana*, wydanej w 2018 r. Dopiero z tej publikacji opinia publiczna

[2] Źródłem tego stwierdzenia jest osobista obserwacja autora recenzji spraw prowadzonych przez Zarząd Śledczy Urzędu Ochrony Państwa lub dostępnych w ramach współpracy z partnerskimi służbami.

[3] T. Piątek, *Macierewicz i jego tajemnice*, Warszawa 2017.

[4] R. Gruca, *Pilna wizyta Macierewicza w IPN? Co stało się z teczkami agentów?*, Fakt, 25 VI 2018 r., https://www.fakt.pl/polityka/pilna-wizyta-macierewicza-w-ipn-co-stalo-sie-z-teczkami-agentow/hx509dh [dostęp: 26 VIII 2026].

dowiedziała się, że Antoni Macierewicz jako minister spraw wewnętrznych nakazał w 1992 r. zaprzestania operacji kontrwywiadu przeciwko rezydenturze GRU w Warszawie i jej szefowi Władimirowi Iwanowiczowi Łomakinowi.

Polecenie zakończenia gry polskiego kontrwywiadu z Rosjanami minister Antoni Macierewicz przekazał ustnie dyrektorowi Zarządu Kontrwywiadu UOP płk. Konstantemu Miodowiczowi. Według relacji Miodowicza otrzymał on ten rozkaz w gabinecie ministra spraw wewnętrznych w obecności ówczesnego szefa UOP Piotra Naimskiego[5].

Wykorzystanie tylko jednego i to specyficznego źródła oznacza pominięcie przez autora *Śpiących psów*… całości materiałów operacyjnych w sprawie Zieliński/Łomakin – opinii i analiz powstałych w Zarządzie Śledczym UOP, które nie zostały dołączone do materiałów przesłanych wraz z aktem oskarżenia, zapisów przesłuchań, materiałów dotyczących ustaleń obserwacji i treści utrwalonych przez środki techniki operacyjnej. Informacje te są prezentowane w sądzie jako dowód z przesłuchania. Oczywiście to sąd decyduje, kto jest przesłuchiwany. Nie są włączane do materiału prokuratorsko-sądowego informacje, których nie można przekształcić w dowód procesowy ze względu na dominujący interes operacyjny lub gdy nie istnieje sposób ich prezentacji bez szkody dla prowadzonych innych spraw lub osób zaangażowanych w nie i czynności objętych tajemnicą państwową. Nie oznacza to, że nie będą one wykorzystane w innych sprawach i prezentowane w sposób bezpieczny dla dóbr prawnie chronionych.

Jak postrzegam cele opublikowania *Śpiących psów*…

Autor książki deklaruje i podkreśla (wytłuszcza), że: *Jej* [tj. omawianej książki – dop. aut. recenzji] *cel jest jedynie naukowy, z nadzieją na praktyczne zastosowanie* (s. 7). Dalej oświadcza: *Autor ma nadzieję, że analiza zostanie odebrana zgodnie z jego zamierzeniem, tj. jako zastosowanie metodologii naukowej oraz praktyki pracy operacyjnej do przeanalizowania metod i form pracy rosyjskich służb specjalnych* (s. 7).

Trudno oprzeć się wrażeniu, że prawdziwe cele tej książki były inne, a przymiot naukowości jej nie przysługuje.

Aby zrozumieć prawdziwe intencje autora *Śpiących psów*…, warto pochylić się nad *Wstępem*. Marek Świerczek stwierdza w nim, że sprawa Zielińskiego była „z prawdopodobieństwem graniczącym z pewnością" grą rosyjskich służb przeciw UOP (s. 17). Zieliński był ofiarą tej gry, mającej osłonić siatki agenturalne Komitetu Bezpieczeństwa Państwowego ZSRR (KGB) i GRU, zbudowane w czasach PRL i –

[5] Źródłem tego stwierdzenia jest wiedza własna autora recenzji.

jak wydaje się sugerować w książce – funkcjonujące do chwili obecnej. Zdaniem Marka Świerczka ta „operacja decepcyjna" (sic!): (…) *następnie stała się kanwą mitu politycznego, dzięki któremu można było w dalszym ciągu osłabiać międzynarodową pozycję Polski, kształtując obraz polskiego świata politycznego jako przeżartego rosyjską agenturą* (s. 17 i 18).

Dalej autor książki pisze: *Rzeczpospolita tak długo nie będzie gwarantem interesów narodowych, jak długo będzie ofiarą procesów decepcyjno-mitotwórczych kształtujących postawy obywateli i elit rządzących* (s. 19). *Mistyfikowanie rzeczywistości społeczno-politycznej w Polsce nie pozwoliło w początkowych latach III RP na przeprowadzenie gruntownych reform, choćby w postaci przecięcia splotu niejawnych wpływów na aparat państwowy dzięki dekomunizacji i lustracji* (s. 18).

Przytoczone powyżej stwierdzenia autora nie wynikają ani z treści omawianej książki, ani z żadnej znanej publicznie, obiektywnej pracy naukowej, są bowiem sensu stricto polityczną oceną propagowaną przez niektóre środowiska, z którą autor książki się zgadza.

Marek Świerczek nie przedstawia żadnych dowodów na poparcie tych tez. Nie wyjaśnia, jaki mit ma na myśli. Tymczasem to właśnie *Śpiące psy*… próbują wytworzyć mit potężnych rosyjskich służb, które na początku lat 90. XX w. prowadziły skuteczne gry z niedoświadczonym kontrwywiadem UOP.

Oprócz niezwykle kategorycznych stwierdzeń autora dotyczących sprawy Zielińskiego, w książce pojawia się też próba wprowadzenia do dyskusji terminu „operacja decepcyjno-mitotwórcza". Pojęcie to wywodzi się z psychologii i nauk pokrewnych, ale nie zostało ostatecznie zdefiniowane.

Książka zawiera również szereg opinii autora o wydźwięku politycznym (s. 17–19 i inne).

Po *Wstępie* (ideologicznym) autor przechodzi do rozdziału zatytułowanego *Sprawa Marka Zielińskiego*, w którym dość pobieżnie prezentuje sylwetkę bohatera. Najwięcej uwagi poświęca atakom medialnym na ministra Antoniego Macierewicza, któremu zarzucano bardzo bliskie relacje z wieloma osobami podejrzanymi o pracę „na rzecz" lub tylko o sympatię do Rosji. Marek Świerczek pisze: (…) *sprawa Marka Zielińskiego uległa pełnej polityzacji, stając się ważnym ogniwem łańcucha dowodowego, mającego wykazać rzekome związki Macierewicza i jego środowiska z wywiadem wojskowym Federacji Rosyjskiej* (s. 48).

Nasuwa się pytanie, czy to nie autor *Śpiących psów*… próbuje przeprowadzić polityzację sprawy Zielińskiego, stwierdzając, że ataki na Antoniego Macierewicza uderzają w polską rację stanu, gdyż powodują, że Polska jest postrzegana jako państwo postsowieckie, a nie wiarygodny członek NATO i Unii Europejskiej? Jego zdaniem: *Problem* (…) *polega na tym, że* (…) *sprawa Marka Zielińskiego w rzeczywistości wyglądał*a *zupełnie inaczej, niż się powszechnie przyjmuje, a sam Marek*

Zieliński odegrał w niej zupełnie inną rolę, niż mu to przypisał sąd na podstawie ustaleń prokuratury wojskowej (s. 48).

Można zatem sądzić, że autor książki, bazując na tych samych materiałach co sąd, podważa wydany przez niego wyrok.

W moim przekonaniu autor ujawnia tu jeden (być może najważniejszy) z prawdziwych celów napisania tej książki: podważenie zasadności ataków na Antoniego Macierewicza przez zanegowanie znaczenia sprawy Zielińskiego/Łomakina, która to sprawa jest jakoby powiązana z tymi atakami (s. 48). Tymczasem w okresie, kiedy rozgrywała się ta sprawa, takich ataków nie było.

Patrząc pobieżnie, można odnieść wrażenie, że spojrzenie Marka Świerczka na sprawę Zielińskiego/Łomakina jest po prostu kontynuacją jego dotychczasowych zainteresowań naukowych i doktoratu dotyczącego operacji „Trust". Niezależnie od tego książka *Śpiące psy*… jest również obroną decyzji ministra Antoniego Macierewicza, który zakazał UOP rozpracowywania szefa rezydentury GRU w ambasadzie Rosji w Warszawie.

Drugim celem *Śpiących psów*… jest zdezawuowanie osób kierujących UOP na początku lat 90. przez obwinianie ich o niekompetencję i uleganie rosyjskiej manipulacji.

Trzecim celem jest wzmocnienie mitu „opcji zerowej", czyli zbudowania służb specjalnych RP bez udziału byłych funkcjonariuszy służb PRL. Autor sugeruje takie rozwiązanie w wielu miejscach w książce, nie nazywając go literalnie „opcją zerową". Nie przedstawia żadnych argumentów za takim rozwiązaniem, milcząco uznając, że byłoby to rozwiązanie znacznie lepsze dla Rzeczpospolitej. Przykład Republiki Czeskiej, gdzie pomimo „opcji zerowej" pojawiła się największa w krajach byłego obozu socjalistycznego (z wyjątkiem Federacji Rosyjskiej) liczba oligarchów uwłaszczonych na majątku państwowym, wskazuje, że jest wręcz przeciwnie[6]. Jednocześnie zauważmy, że w ostatnich 35 latach tempo wzrostu gospodarczego w Polsce, w której nie wprowadzono „opcji zerowej", było znacznie szybsze niż w Czechach, gdzie zaistniała[7].

Mity i rzeczywistość

Marek Świerczek w swojej książce buduje, o czym już wspomniałem, mit potęgi rosyjskich służb specjalnych. Już we *Wstępie* przedstawia przykłady ich sukcesów, poczynając od stworzenia fałszywego polskiego Rządu Narodowego po upadku

[6] D. Tramba, *The Unstoppable Rise of Czech Oligarchs*, Aspen Institute Central Europe, 16 XI 2019 r., https://www.aspeninstitutece.org/article/2019/unstoppable-rise-czech-oligarchs/ [dostęp: 14 VI 2026].

[7] J. Borowski, K. Jaworski, J. Olipra, *Jak mierzyć „cud gospodarczy" w Polsce?*, Bank.pl, 23 VI 2025 r., https://bank.pl/jak-mierzyc-cud-gospodarczy-w-polsce/ [dostęp: 3 X 2026].

powstania styczniowego, przez wykreowanie fałszywej organizacji kontrrewolucyjnej „Trust" w latach 20. XX w., aż do rozbicia podziemia w Polsce, Pribałtyce i Ukrainie po II wojnie światowej (s. 15–17). Zastanawiający jest brak przykładów porażek radzieckich/rosyjskich służb. Kierując się naukowym obiektywizmem, autor książki powinien przynajmniej o nich wspomnieć. Radzieckie służby nie przewidziały np. ataku III Rzeszy na ZSRR w 1941 r., a w 2022 r. rosyjskie służby nie doceniły zdolności obronnych Ukrainy.

Autor książki stara się przedstawić radzieckie, a później rosyjskie służby jako organizacje skuteczne i sprawne. W odróżnieniu od służb PRL, które według niego charakteryzowały: pijaństwo, nepotyzm, kumoterstwo, ideologiczne zaślepienie, niska inteligencja kadry kierowniczej, służalstwo niższej kadry, biurokracja i działania pozorne. Uważa, że te cechy przeniosły się „początkiem lat 90." do UOP (s. 214–224). Nie zauważa natomiast, że podobne problemy mogły mieć radzieckie, a później rosyjskie służby[8].

Zdaniem autora książki przykładem sukcesu rosyjskich służb jest także sprawa Zielińskiego, który w 1993 r., tuż po wycofaniu rosyjskich wojsk z Polski, został aresztowany przez funkcjonariuszy UOP, a następnie skazany na dziewięć lat więzienia za szpiegostwo na rzecz ZSRR i Federacji Rosyjskiej. Aby to uwiarygodnić, wysnuwa bardzo daleko idące wnioski, przypominające typową teorię spiskową[9].

Według opisu Marka Świerczka sprawa Zielińskiego była prosta. Jej „bohater" to były funkcjonariusz Służby Bezpieczeństwa PRL. Specjalizował się w pisaniu analiz na temat opozycji demokratyczno-solidarnościowej. W 1987 r. podczas kontroli zawartości szaf służbowych wykryto, że nielegalnie kopiuje i gromadzi wiele dokumentów niejawnych. Ukarano go naganą i przesunięto do działań operacyjnych. W kierownictwie SB podobno byli tacy, którzy mieli mu za złe, że oprócz oficjalnych, służbowych kontaktów z przedstawicielami KGB w Warszawie utrzymuje też stosunki towarzyskie z attaché wojskowym ZSRR. Wkrótce Zieliński został jednak przywrócony do pracy analitycznej i dołączył do zespołu bezpośrednio wspierającego ministra spraw wewnętrznych Czesława Kiszczaka, dla którego pisał przemówienia, zwłaszcza w okresie Okrągłego Stołu (s. 49–50, 98–99).

Niechęć Zielińskiego do Solidarności była tak silna, że po jej zwycięstwie nie poddał się weryfikacji, tylko odszedł na emeryturę i zajął działalnością w dynamicznie wówczas rozwijającej się branży ochroniarskiej (s. 101). Jego firma „Dakota" próbowała zdobywać kontrakty na kierunku wschodnim, a on utrzymywał liczne kontakty z osobami z byłego MSW PRL i funkcjonariuszami PZPR (s. 53–58).

[8] A. Grajewski, *Tarcza i miecz. Rosyjskie służby specjalne 1991–1998*, Warszawa 1998, s. 20.

[9] P. Łukowski, *Sens wyrażenia „teoria spiskowa", czyli jak odróżnić teorię spiskową od niespiskowej*, „Hybris" 2016, nr 33, s. 101–124.

Aby pomóc czytelnikowi recenzji w zrozumieniu sensu czynności podejmowanych w sprawie Zielińskiego oraz ich kontekstu historycznego, zamieszczam skrót kalendarium wydarzeń zawartego w książce Marka Świerczka. Uzupełniłem je o znane wydarzenia ze sceny politycznej, które z dużym prawdopodobieństwem miały wpływ na przebieg sprawy, a autor o nich nie wspomniał.

- 26 czerwca 1991 r. – Andrzej Anklewicz, kierownik Zespołu Analiz i Obsługi Ministra Spraw Wewnętrznych, poinformował kontrwywiad UOP i ministra spraw wewnętrznych, że jego kolega z czasów służby w SB Marek Zieliński próbował namówić go na współpracę z „dziennikarzem rosyjskiej agencji prasowej TASS", co było oczywistą próbą werbunku do pracy na rzecz wywiadu ZSRR. Kontrwywiad UOP polecił Anklewiczowi podjęcie gry.
- Lipiec 1991 r. – odbyło się kilka spotkań Zielińskiego z Anklewiczem, podczas których ten drugi przekazał swoje żądania finansowe (kilkanaście tysięcy dolarów za samą zgodę na współpracę) oraz zażądał osobistego spotkania z „dziennikarzem".
- 19–21 sierpnia 1991 r. – w Moskwie doszło do nieudanego puczu Janajewa. W rezultacie 22 sierpnia obalono pomnik Feliksa Dzierżyńskiego na Łubiance; 24 sierpnia Ukraina, a 25 sierpnia Białoruś ogłosiły niepodległość; 29 sierpnia zlikwidowano Komunistyczną Partię Związku Radzieckiego (uzupełnienie autora recenzji).
- 28 sierpnia 1991 r. – podczas spotkania w restauracji Zieliński dowiedział się, że jego nowym oficerem prowadzącym będzie kmdr Władimir Łomakin.
- 27 września 1991 r. – Anklewicz przekazał materiały dla Rosjan przygotowane przez kontrwywiad UOP.
- 2 października 1991 r. – Łomakin odwiedził Zielińskiego w jego firmie „Dakota". Ocenił materiały przekazane przez Anklewicza jako mało interesujące.
- 12 listopada 1991 r. – Łomakin spotkał się z Zielińskim w restauracji. Nie zachowywali się konspiracyjnie. Łomakin dał 800 dolarów, w tym 500 dolarów dla Anklewicza.
- 15 listopada 1991 r. – Zieliński podał Anklewiczowi datę (29 listopada) i miejsce (przy Teatrze Powszechnym) spotkania z oficerem GRU, a także znak rozpoznawczy (reklamówkę) oraz hasło i odzew. Przekazał mu także mapę Warszawy z zaznaczonym miejscem spotkania i 500 dolarów za poprzednie materiały.
- 29 listopada 1991 r. – spotkanie Anklewicza z Łomakinem, który przedstawił system skrytej łączności, obiecał dać aparat do zdjęć szpiegowskich, zapowiedział, że wynagrodzenia za następne pakiety dokumentów będą

wynosić od 1000 do 1500 dolarów. W odpowiedzi na pytanie Anklewicza określił też zainteresowania GRU: zamiary USA, Wielkiej Brytanii i Niemiec wobec Rosji, działania kontrwywiadowcze UOP wobec Rosjan w Polsce oraz oceny sytuacji w Rosji przesyłane z Ambasady RP w Moskwie. W sprawie informacji na temat obronności i ochrony granic Łomakin stwierdził „My to mamy". Zalecił także zerwanie kontaktu z Zielińskim, bo „on nie jest przydatny dla GRU". Następne spotkanie zostało ustalone na 17 grudnia 1991 r.

- 17 grudnia 1991 r. – podczas spotkania Łomakin przekazał Anklewiczowi, że jego materiały były tylko częściowo interesujące. Nie potrzebował materiałów z Ministerstwa Spraw Wewnętrznych i Ministerstwa Spraw Zagranicznych, chciał tylko depesze z Ambasady RP w Moskwie i informacje na temat obszarów zainteresowania kontrwywiadu UOP. Kolejne spotkanie ustalono na 14 lutego 1992 r. Łomakin miał wtedy wręczyć 1500 dolarów za poprzednio otrzymane materiały i dać aparat fotograficzny oraz radiotelefon.
- Nowy minister spraw wewnętrznych Antoni Macierewicz (funkcję objął 23 grudnia 1991 r.) kategorycznie nakazał zaprzestania gry z Łomakinem. Zezwolił tylko na spotkanie kończące współpracę. Decyzja ta uniemożliwiła pozyskanie dowodów w postaci środków łączności tajnej (uzupełnienie autora recenzji).
- Koniec stycznia 1992 r. – Zieliński złożył propozycję pracy dla Rosjan Dariuszowi C. Ten nie potraktował jej poważnie, gdyż na spotkaniu Zieliński nadużywał alkoholu.
- 20 lutego 1992 r. – w terminie rezerwowym odbyło się spotkanie Łomakina z Anklewiczem, który zgodnie z instrukcją UOP powiedział, że boi się współpracować i nie będzie się więcej spotykać. Anklewicz nagrał tę rozmowę.
- 20 maja 1992 r. – Łomakin wyraził zgodę na werbunek Feliksa B., który jako konsultant przygotowywał komentarz do Instrukcji Operacyjnej UOP.
- 11 listopada 1992 r. – Zieliński ponownie zaproponował Feliksowi B. sprzedaż dokumentów UOP za cenę od 50 do 1000 dolarów. Po kilku dniach Feliks B. przez telefon odmówił Zielińskiemu, ale nie poinformował o tej propozycji kontrwywiadu UOP.
- 18 listopada 1992 r. – Zieliński podczas spotkania z Łomakinem poprosił o przerwę we współpracy, gdyż bał się, że Feliks B. może go zdradzić. Łomakin się na to zgodził.
- 16 grudnia 1992 r. – oficer UOP Jan S. poinformował kontrwywiad UOP, że otrzymał (kiedyś) od Zielińskiego propozycję współpracy z „rosyjskim dziennikarzem". Kontrwywiad UOP po raz drugi podjął grę, zakładając zarówno pulę celów, jak i kierunki postępowania procesowego.

- 31 maja 1993 r. – Łomakin po raz kolejny spotkał się z Zielińskim w restauracji i nie zachował konspiracji. Ponaglał go o werbunki.
- 19 czerwca 1993 r. – Zieliński przedstawił Janowi S. różne propozycje współpracy biznesowej w ramach firmy „Dakota" i wspomniał o możliwości sprzedawania dokumentów UOP za od 1000 do 3000 dolarów. Zgodnie z instrukcją kontrwywiadu UOP Jan S. nie odmówił, ale i nie wyraził zgody.
- 21 czerwca 1993 r. – Zieliński spotkał się w restauracji z Łomakinem i poinformował go o rozmowie z Janem S. Łomakin nalegał na szybki werbunek Jana S. Informację o wynikach rozmowy werbunkowej Zieliński miał wsunąć w nocy pod drzwi mieszkania Łomakina.
- 30 sierpnia 1993 r. – podczas spotkania Zieliński podał Janowi S. cennik za przekazywane dokumenty. Dokumenty resortowe: 200–500 dolarów, tajne: 500–1000 dolarów, tajne spec. znaczenia: 1000–5000 dolarów. Zaproponował też wyjazd na weekend poza Warszawę. Jak później zeznał Zieliński, Łomakin nie wykluczał udziału w tym spotkaniu. Do spotkania wyjazdowego jednak nie doszło.
- 17 września 1993 r. – ostatnia jednostka armii rosyjskiej opuściła terytorium Polski (uzupełnienie autora recenzji).
- 18 września 1993 r. – podczas spotkania w restauracji Jan S. przekazał Zielińskiemu przygotowane przez kontrwywiad UOP materiały dla Łomakina – do zwrotu następnego dnia.
- 27 września 1993 r. – podczas spotkania w restauracji Jan S. przekazał Zielińskiemu m.in. *Raport o stanie bezpieczeństwa państwa*.
- 28 września 1993 r. – Zieliński napisał dla Łomakina charakterystykę Jana S. i później spotkał się z nim w restauracji. Było zbyt tłoczno, aby przekazać mu *Raport o stanie bezpieczeństwa państwa*, więc umówili się na spotkanie w siedzibie „Dakoty". Łomakin wyszedł, a UOP zatrzymał Zielińskiego oraz (uzupełnienie autora recenzji) Łomakina.
- Zieliński został aresztowany, a Łomakin niezwłocznie wydalony z Polski.

Marek Świerczek przedstawia tę sprawę jako przykład gry operacyjnej określanej jako gambit pionka, gdy poświęca się nieistotnego współpracownika, aby chronić ważniejsze aktywa. W tym przypadku GRU miało poświęcić Zielińskiego, aby po pierwsze odwrócić uwagę UOP od innych, ważniejszych szpiegów pracujących dla radzieckich/rosyjskich służb, a po drugie uwiarygodnić oficerów UOP pochodzących z SB jako wiernych nowemu państwu (jedni z nich informują o próbach werbunku, a inni skutecznie łapią szpiega), a tym samym zapobiec „opcji zerowej" (s. 283–287).

Konkluzja ta opiera się na rzekomym wykazaniu, że inne alternatywne sposoby wyjaśnienia przebiegu sprawy Zielińskiego są nieprawdopodobne.

U podstaw tego rozumowania autora książki leży opinia, że działania Łomakina w relacji z Zielińskim, zarówno co do sposobu kontaktowania się, jak i stawiania mu zadań, były skrajnie sprzeczne z zasadami obowiązującymi w radzieckim/rosyjskim wywiadzie. Po pierwsze, Łomakin nie starał się zachować tych kontaktów w tajemnicy, a po drugie, nalegał na werbunek osób z MSW i UOP, bez zwracania uwagi na możliwości tych kandydatów w zakresie pozyskiwania informacji cennych dla radzieckich/rosyjskich służb (s. 137–142).

Marek Świerczek przedstawia dwie hipotezy mogące wyjaśnić to, jego zdaniem, nieprofesjonalne zachowanie Łomakina. Hipoteza pierwsza: Łomakin był nieudolny i nie umiał bezpiecznie prowadzić działalności wywiadowczej. Hipoteza druga: Łomakin był pod presją, aby bardzo szybko pozyskać źródła informacji w UOP i MSW, gdyż w tym czasie radzieckie/rosyjskie służby ich zupełnie nie miały (s. 143–147).

Zdaniem autora książki hipoteza pierwsza nie może być prawdziwa, gdyż Łomakin wykazał swoją sprawność i profesjonalizm, gdy przez sześć lat przebywał na placówce w USA i nie został z niej wydalony za szpiegostwo. Hipoteza druga również jest fałszywa, gdyż radzieckie służby miały w MSW PRL bardzo wiele źródeł, więc jest mało prawdopodobne, aby żadne z tych źródeł nie trafiło do UOP lub nowego MSW. Marek Świerczek stwierdza, że ponieważ obie te hipotezy są fałszywe, to prawdziwa musi być hipoteza trzecia: radzieckie/rosyjskie służby świadomie chciały poświęcić Zielińskiego (s. 252). Łomakin celowo tak prowadził Zielińskiego, aby UOP wykrył jego działalność agenturalną. Miało to na celu ochronę znacznie ważniejszych aktywów GRU. Zieliński jest więc kozłem ofiarnym przykrywającym dalej działającą agenturę.

Nie sposób uznać tego rozumowania za poprawne.

Łomakin rzeczywiście przez sześć lat pracował w rezydenturze w USA, jednak następstwem tego były kolejne odmowy udzielenia mu „Agrément" w kolejnych krajach europejskich. Tak więc z tego, że Łomakin przez te sześć lat nie został wydalony z USA, nie musi wynikać, że był sprawny w szpiegowskim rzemiośle. Może był tak mało sprawny, że FBI w pełni kontrolowała jego aktywność i źródła, więc nie chciała jego wydalenia, aby następca nie okazał się trudniejszym przeciwnikiem. Nie można zatem uznać, że Marek Świerczek dowiódł fałszywości tej hipotezy.

Również uznanie przez niego, że hipoteza druga jest fałszywa, nie ma logicznych podstaw, gdyż nawet przy założeniu, że radzieckie służby (KGB/GRU) miały w 1990 r. w strukturach MSW RP siatkę funkcjonariuszy SB zwerbowanych w latach 80., co nie znajduje jednak żadnego potwierdzenia ani wtedy, kiedy sprawa Zielińskiego się rozgrywała, ani w perspektywie następnych lat i kolejnych zdarzeń, to jest bardzo prawdopodobne, że niewielu z nich nadal chciało i mogło współpracować

w nowej sytuacji politycznej. Nie sposób więc uznać, że Marek Świerczek wykazał fałszywość hipotezy drugiej.

Jeszcze poważniejszy problem z poprawnością rozumowania autora książki polega na tym, że możliwa i bardzo prawdopodobna jest hipoteza czwarta: Łomakin chciał pozyskać nowe źródła, aby wykazać swoją przydatność i pozostać na placówce w Warszawie. W okresie, kiedy rozgrywała się sprawa Zielińskiego/Łomakina, rozpadał się ZSRR, więc dyplomaci i szpiedzy nie mogli czuć się pewnie na swoich placówkach. Nawet gdyby GRU miało dobre źródła, to nie były one sukcesem Łomakina, tylko jego poprzedników. On zaś potrzebował własnego sukcesu, aby mieć większe szanse na pozostanie za granicą, na stanowisku dyplomatycznym.

Na koniec trzeba zauważyć, że błędna jest też podstawa całego tego rozumowania, czyli dokonana przez autora książki ocena, że sposób zadaniowania i kontaktowania się Łomakina z Zielińskim był sprzeczny z zasadami działania wywiadu. Nie było sprzeczne z tymi zasadami to, że nie ukrywali oni swojej znajomości, a tylko starali się utrudnić UOP ustalenie częstotliwości spotkań, starannie unikając przy tym sprawienia wrażenia, że mają one charakter konspiracyjny. Dlatego siadali w restauracjach na środku sali, a nie w ukrytym kącie i nie unikali przypadkowo spotykanych znajomych. Była to taktyka całkiem skuteczna. Rutynowa obserwacja UOP zarejestrowała kilka spotkań Łomakina z Zielińskim, jednak nie wzbudziło to większego zainteresowania aż do momentu, gdy Anklewicz zawiadomił kontrwywiad UOP, że Zieliński chce go zwerbować. Powyższe stwierdzenia to kontrwywiadowcze abecadło.

Zaproponowana przez Marka Świerczka koncepcja sprawy Zielińskiego jako gambitu pionka jest też nielogiczna, gdyż poświęcenie Zielińskiego w żaden sposób nie mogło zabezpieczyć interesów radzieckich/rosyjskich służb. Wręcz przeciwnie, przyniosło same straty.

1. Aresztowanie, a następnie surowy wyrok dla Zielińskiego musiały zniechęcać zarówno ówczesnych współpracowników rosyjskich służb, jak i ewentualnych kandydatów do werbunku. Zobaczyli, że UOP potrafi skutecznie działać, a sądy nie mają litości.
2. Wydalenie Łomakina ze względu na jego działalność szpiegowską osłabiało pozycję Rosji jako państwa szukającego dobrych relacji z Zachodem i prowadzącego przyjazną politykę wobec państw Europy Środkowej i Wschodniej, a na takim postrzeganiu zależało Federacji Rosyjskiej pod rządami Borysa Jelcyna[10].
3. Wydalenie Łomakina utrudniło działanie rezydentury KGB/GRU, a zwłaszcza jego sieci źródeł (jeśli takie istniały).

[10] A. Grajewski, *Tarcza i miecz…*, s. 197.

4. Dowód, że UOP potrafi dostarczać spreparowane materiały zawierające dezinformację, musiał doprowadzić do wzrostu niepewności co do wartości dokumentów i informacji dostarczanych rosyjskim służbom przez agenturę (jeśli wówczas istniała).
5. Operacja wobec Zielińskiego nie należała do szczególnie dynamicznie prowadzonych i wymagających specjalnych środków kontroli operacyjnej, stosowanych wobec licznej grupy osób. W związku z tym absolutnie nie wyczerpywała zasobów kontrwywiadu UOP i nie mogła stanowić przeszkody dla innych działań kontrwywiadowczych, w tym wykrywania rosyjskich agentów.

Jeżeli poświęcenie Zielińskiego miało zapobiec „opcji zerowej", to nie byłoby to w interesie ZSRR/Rosji, gdyż to właśnie ta opcja na wiele lat sparaliżowałaby działania polskich służb specjalnych, osłabiałaby Polskę i ośmielała potencjalnych zdrajców ojczyzny do podjęcia współpracy z obcymi wywiadami, w tym radzieckim/rosyjskim. Nie dawałaby natomiast pewności, że agenci Rosji nie przeniknęli do nowych służb, gdyż – jak zauważa też Marek Świerczek – radzieckie służby mogły werbować współpracowników również w środowiskach opozycyjnych (s. 190). O tych werbunkach nie było wszak zapisów w rejestrach polskich służb, nie mogły więc zostać wykryte w toku lustracji.

Byli funkcjonariusze SB uwiarygadniali się wobec nowego kierownictwa UOP przez działania (np. operacja „Samum/Przyjazny Saddam" – wyprowadzenie amerykańskich agentów z Iraku). Uwiarygadniała ich codzienna praca z obserwującymi ich z bliska ludźmi z tzw. solidarnościowego naboru, którzy na koniec 1990 r. stanowili już pokaźną grupę.

Sprawę Zielińskiego/Łomakina nadzorował dyrektor Zarządu Kontrwywiadu, a etap procesowy był pod nadzorem zastępcy dyrektora Zarządu Śledczego – obaj byli z nowego naboru.

Podsumowując, teza Marka Świerczka, jakoby sprawa Zielińskiego była gambitem pionka ze strony rosyjskich służb wobec UOP, nie ma podstaw.

Kontekst sprawy Zielińskiego

Jak przebiegała współpraca Zielińskiego z radzieckimi służbami w latach 80.?

Zieliński był w tym czasie wzorcowym przykładem funkcjonariusza SB PRL usiłującego przypodobać się przedstawicielom radzieckich służb, aby zaskarbić sobie w ten sposób uwagę i sympatię przełożonych. W tych latach bezpośrednie spotkania funkcjonariuszy SB z funkcjonariuszami KGB i GRU nie stanowiły problemu. Zieliński uniknął też poważniejszych kłopotów, gdy okazał się „kolekcjonerem"

kopiującym materiały niejawne. Niebawem został nawet powołany do zespołu doradców ministra spraw wewnętrznych Czesława Kiszczaka, tzw. zespołu Iwanciowa.

Jak wyglądała sytuacja radzieckich służb w Polsce na przełomie lat 80. i 90.? Pod koniec lat 80. radzieckie służby nie wiedziały, jak zachowają się Polacy, jeśli dojdzie do przełomu – nie tylko opozycja, lecz także partyjni decydenci. Rozwiązanie SB i przeprowadzenie weryfikacji wprowadziło olbrzymi zamęt w ich sieci informacyjne, o ile nadal one istniały. Przedstawiciele radzieckich służb rozpoczęli prowadzone wielotorowo rozmowy dotyczące charakteru przyszłych relacji polsko-radzieckich. Wystarczy wspomnieć blisko roczny cykl spotkań i rozmów Jarosława Kaczyńskiego z domniemanym radzieckim dyplomatą na temat „finlandyzacji" Polski[11].

Postępujący upadek ZSRR sprawił, że w radzieckich służbach nastał czas „ratowania się", „urządzania się", „wykorzystywania możliwości". Od obaw o własny los i miejsce w kształtującej się nowej rzeczywistości wewnątrz służb nie byli wolni oficerowie KGB i GRU. Po rozpadzie ZSRR w grudniu 1991 r. trzeba było czasu dla okrzepnięcia nowych, już rosyjskich służb i wyważenia relacji między nimi, zarówno na arenie wewnętrznej, jak i poza granicami.

Po 1 sierpnia 1990 r. sytuacja radzieckich służb w Warszawie stała się dużo trudniejsza. Rosyjscy funkcjonariusze stracili możliwość wejść na teren budynków rządowych, w tym MSW. Przestały działać ich bezpośrednie telefony (kilka z czystej ciekawości zostawiono), musieli błyskawicznie zwijać instalacje techniczne i tajne bazy w śródmiejskich dzielnicach i obiektach. W dodatku zaczęła się weryfikacja byłych funkcjonariuszy SB i nikt z nowego UOP i MSW nie chciał z przedstawicielami radzieckich służb rozmawiać. W rosyjskich ambasadach w Europie co chwila zmieniały się obsady i dotyczyło to także personelu rezydentur. Warszawa została obsadzona przez ambasadora Jurija Kaszlewa, pułkownika KGB, będącego jednocześnie rezydentem. Podlegali mu także pracownicy rezydentury GRU, choć w porównaniu z kolegami z KGB byli zapewne w mniej uprzywilejowanej sytuacji.

W takim rozgardiaszu rozpoczyna się sprawa Zielińskiego, który do pracy dla nowych służb się nie zgłosi, ale zna wielu takich, którzy chcą do nich pójść. Może z nimi rozmawiać i namówić ich do współpracy z radzieckimi służbami.

Początkiem czynności kontrwywiadu UOP w sprawie Zielińskiego staje się jego oferta złożona Anklewiczowi, który kieruje zespołem analityczno-obsługowym ministra spraw wewnętrznych. Dla radzieckich służb jest on potencjalnie cennym źródłem. Wie, kto, gdzie się znalazł w nowej rzeczywistości, ma dostęp do kalendarza, w którym znajdują się bezcenne notatki dotyczące na przykład spotkań ministra i jego zastępców oraz szefa UOP. Anklewicz lojalnie informuje

[11] T. Piątek, *Kaczyński i jego pajęczyna. Tkanie sieci 1949–1995*, Warszawa 2022, s. 257.

kontrwywiad UOP i za zgodą ministra wchodzi w pierwszy etap gry. Od początku wiadomo, że trzeba dojść do rezydentury, dlatego Zieliński jest naciskany na bezpośredni kontakt z oficerem prowadzącym i dążenie do ustalenia technicznych kanałów łączności. Taki rezultat byłby ogromnym sukcesem kontrwywiadowczym, rzadkim we wspólnocie, do której Polacy wtedy dopiero aspirowali.

Każda tego typu sprawa trwa, mijają dni i tygodnie, czasem intencjonalnie, a czasem przez przypadek. Nawiązanej nici dialogu nie wolno przerwać. W końcu wszystko jest gotowe. I wtedy zmienia się minister spraw wewnętrznych, szef oraz niektórzy dyrektorzy w UOP. W dojrzałych służbach okrzepłego państwa nie ma to znaczenia, ale w młodej III RP…

Gdy Anklewicz na rozkaz ministra Antoniego Macierewicza rezygnuje z usług na rzecz GRU, Zieliński nie zaprzestaje działalności werbunkowo-informacyjnej, ale kieruje ją na następnego z kolegów z przeszłości – Jana S. O propozycji werbunkowej Zielińskiego Jan S. melduje w trybie służbowym. Sytuacja zaczyna się budować nie tyle już w grę[12] (w zaistniałej sytuacji nie sposób do niej wrócić), ile w kombinację mającą jednak swoje ważne cele. Przy czym UOP zaczyna intensywniej dążyć do eliminacji Łomakina. Funkcjonariusze operacyjni wprowadzają w sprawę śledczych, co oznacza dążenie do procesowej realizacji sprawy. Decyzja o realizacji zapada z uwzględnieniem wielu zmiennych, także tych z zakresu polityki zagranicznej.

Małe i duże błędy autora książki

Największym błędem autora jest próba przekonania czytelnika, że sprawa Zielińskiego, oceniana dotąd jako niewątpliwy sukces UOP, była w istocie rosyjską grą, którą określa jako gambit pionka. Twierdzi on, że świadomie poświęcając mało istotnego agenta, jakim był Zieliński, rosyjskie służby osiągnęły znacznie ważniejsze dla nich cele. Nie określa, jakie mogłyby to być cele, warte nie tylko utraty agenta skazanego na długoletnie więzienie, lecz także wydalenia jego oficera prowadzącego, kmdr. Łomakina. Nie analizuje, jak takie wydarzenia mogły wpłynąć na innych agentów lub osoby, które rosyjskie służby chciałyby pozyskać do współpracy. Ignoruje też fakt, że realizacja sprawy Zieliński/Łomakin chwilę po wyjściu rosyjskiej Północnej Grupy Wojsk stanowiła czytelny sygnał przekazany Moskwie – nie akceptujemy waszego szpiegostwa i będziemy je zwalczać. Warto przypomnieć, że mówimy o 1993 r.

[12] A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, s. 21.

Analizując tekst *Śpiących psów*…, dostrzegam, że autor książki popełnił również wiele innych dyskwalifikujących błędów.

Błąd pierwszy to ahistoryczność i brak oceny wpływu rozpadu ZSRR na wydarzenia opisane w książce oraz zmian organizacyjnych w strukturach służb, a także brak charakterystyki czynników zewnętrznych.

Błąd drugi to brak odniesień do warsztatu pracy kontrwywiadowczej, zarówno indywidualnego oficera, jak i szerszych struktur, zwłaszcza w zakresie budowania obszarów zainteresowań, budowy map ryzyka, wektorów rozpoznawczych i przeciwdziałania, prewencji i działań wyprzedzających.

Błąd trzeci to brak zrozumienia elementu odpowiedzialności prawnej w pracy operacyjnej z figurantami prowadzonej przez oficerów.

Błąd czwarty to fałszywe założenie, że fakty zawarte w sądowo-prokuratorskich aktach sprawy oddają cały jej obraz. Sąd, zgodnie ze swoją rolą, dokonywał oceny pod kątem wypełnienia znamion przestępstwa przez osoby o nie oskarżone. Sąd nie badał zatem, jakie korzyści operacyjne uzyskał UOP w związku z tą sprawą.

Błąd piąty to brak obiektywizmu. Nie można do niego aspirować, jeśli w analizie zamieszcza się tezy ściśle ideologiczne.

Problem z recenzowaną książką polega też na tym, że jest w niej duża liczba błędnych osądów, przekłamań i efektów niewiedzy. Poniżej przedstawiam najbardziej jaskrawe przykłady dostrzeżonych błędów. Cytaty z książki zostały wyróżnione kursywą.

S. 60, przypis 7: *Oznacza to, że Anklewicz doskonale zdawał sobie sprawę z tego, że podjęcie współpracy z obcym wywiadem oznacza brak możliwości bezproblemowego wyjścia z niej. Tym bardziej zaskakująca jest przeprowadzona przez niego rozmowa kończąca kontakt z GRU*.

Trudno powiedzieć, czego dotyczy wątpliwość Marka Świerczka. To, co mówi Anklewicz, jest wynikiem jego współpracy z kontrwywiadem UOP, niezależnie od tego, czy zaczyna czy kończy pozorowaną współpracę z Łomakinem. Łomakin, żegnając się z Anklewiczem, może uważać, że do wzajemnych relacji będzie mógł powrócić w dogodnym czasie. Autor książki dowodzi, że jego wiedza dotycząca zarówno etapu werbunku, jak i współpracy jest niewielka.

S. 62, przypis 15: *Choć jest to wbrew najbardziej elementarnym zasadom współpracy z agenturą,* Łomakin *faktycznie dał Zielińskiemu nie tylko własną wizytówkę, ale też swojego zastępcy* (…).

Rozdawanie wizytówek przez dyplomatów, w tym pracowników ataszatów wojskowych, jest powszechną praktyką, bez związku z ich działaniami szpiegowskimi.

S. 75: (…) *rezultat pozyskania Jana S. (który jako naczelnik wydziału UOP zajmującego się gospodarką nie miał żadnego istotnego znaczenia dla GRU)* (…).

Z racji zajmowanego stanowiska Jan S. posiadał informacje o UOP i funkcjonariuszach. W okresie pokoju GRU było zainteresowane sytuacją gospodarczą RP. Jan S. pracował w nowo utworzonej jednostce, o której rosyjskie służby mogły nie mieć żadnych informacji.

S. 75, przypis 75: (…) *zgodnie z ówczesną metodyką pracy UOP, obserwacja kończyła pracę o 22:00.*

Autor książki nie podaje źródła tej informacji. Jest ona niezgodna z prawdą. Ani taka metodyka, ani taka praktyka nigdy nie miały miejsca.

S. 78, przypis 95: *Nietrudno zauważyć, że pomysł przyjazdu Łomakina był absurdem operacyjnym. Po pierwsze, po co było zlecać werbunek Zielińskiemu, skoro GRU było gotowe w nim uczestniczyć? Po drugie, w razie dekonspiracji, Łomakin zostałby aresztowany na gorącym uczynku z agentami i tajnymi dokumentami UOP, co redukowałoby do zera możliwość dyplomatycznych zaprzeczeń.*

Po pierwsze, Łomakin nie znał Jana S., więc nie miał jak go werbować bez udziału Zielińskiego. Można się domyślać, że Łomakin dołączyłby do Jana S. i Zielińskiego tylko w przypadku, gdyby Jan S. wyraził zgodę na werbunek. Obecność Łomakina spełniałaby wymóg autentyczności werbunku. Warunek osobistego spotkania z oficerem prowadzącym wyraził wcześniej Anklewicz. Nie był to więc absurdalny pomysł.

Po drugie, gdyby wkroczył UOP, Łomakin mógłby łatwo zaprzeczyć swojemu wykroczeniu poza status dyplomaty, wskazując, że padł ofiarą prowokacji. Powiedziałby, że jego znajomy Zieliński zaprosił go na spotkanie towarzyskie, które okazało się pułapką zastawioną przez UOP. On nikogo nie chciał werbować, a to Jan S. przyniósł materiały i chciał za nie pieniądze. Kolejny raz autor książki dowodzi, że nie rozumie specyfiki pracy operacyjnej.

S. 80: *Dopiero 28 września 1993 r. Zieliński zaczął pisać charakterystykę Jana S. dla Łomakina* (…). **Przypis 109**: *Czyli charakterystyka kandydata* (…) *zaczęła być pisana przez Zielińskiego już po (rzekomym) pozyskaniu Jana S.*

Wcześniej Zieliński przekazał ustnie charakterystykę Jana S. Łomakin wiedział, że kandydat jako naczelnik w UOP jest wartościowym źródłem informacji. Patrz uwaga o autorze powyżej.

S. 81: *Gdy Zieliński wsiadł do swojego samochodu, został zatrzymany przez UOP, który z nieznanych przyczyn nie zdecydował się na zatrzymanie Łomakina w trakcie szpiegowskiego rendez-vous w restauracji* (…).

Łomakin został zatrzymany kilka minut później. Spotkanie było pod pełną kontrolą UOP. Decyzja o oddzielnym zatrzymaniu obu podejrzanych miała uzasadnienie operacyjne.

S. 94, przypis 17: *Nigdzie w wyjaśnieniach Zielińskiego nie pojawiła się refleksja, do czego właściwie GRU go potrzebowało* [w latach 80. – dop. aut. recenzji], *skoro miało oficjalny dostęp do całości informacji MSW PRL.*

Radzieckie służby otrzymywały od MSW PRL jedynie pisemne informacje w odpowiedzi na składane o nie wnioski. Zieliński przekazywał inne dokumenty mogące zainteresować te służby oraz doprecyzowywał je w czasie spotkań.

S. 96, przypis 27: (…) *oficerowie KGB mieli stały, codzienny kontakt z MSW i to zarówno z kierownictwem najwyższego szczebla, jak i z szeregowymi pracownikami.*

Sposób postępowania polegał na złożeniu przez oficerów radzieckich służb zapotrzebowania i potem zgłoszeniu się po informację. O realizacji zapotrzebowania decydował naczelnik, z wyjątkiem spraw zastrzeżonych dla dyrektora. Zapytania były rejestrowane w ewidencji wydziałowej. Oficjalny sposób kontaktu polegał na wskazaniu miejsca oraz osoby, która w obrębie problematyki danego wydziału mogła udzielić informacji. Oczywiście to teoria – praktyka zdecydowanie upraszczała cały proces. Innym sposobem kontaktu była oficjalna korespondencja (pełna dekretacji i decyzji). Tak więc oficerowie KGB mieli kontakt tylko z kierownictwem departamentów i wyznaczonymi pracownikami. Często były to zespoły dwuosobowe. Pozostałych funkcjonariuszy obowiązywał zakaz kontaktów z KGB.

S. 114: (…) *Zieliński najwyraźniej nie był formalnie pozyskany i nie podpisał zobowiązania.*

Bardzo często osoby współpracujące z obcymi służbami nie podpisywały zobowiązań. Nie można wykluczyć, że zgoda była ustna i udokumentowana nagraniem.

S. 154: *Grupa Operacyjna „Wisła" w Moskwie.*

Autor książki nie podaje, że jego wiedza jest oparta na publikacji *Współpraca SB MSW PRL z KGB ZSRR w latach 1970–1990. Próba bilansu*[13]. Na polecenie szefa ABW gen. Krzysztofa Bondaryka stworzył ją zespół funkcjonariuszy ABW po ponadrocznej kwerendzie w zbiorze zastrzeżonym IPN i zebraniu ponad 30 relacji byłych funkcjonariuszy SB. Zespołem kierował ppłk dr Zbigniew Nawrocki[14].

S. 154: [Grupa operacyjna „Wisła" – dop. aut. recenzji] *była uprawniona do prowadzenia pracy operacyjnej wobec Polaków (w tym do werbowania tajnych współpracowników), jednakże tylko w ścisłej współpracy z KGB.*

S. 155: *Rosjanie* (…) *musieli wiedzieć o sporej grupie pozyskanych do współpracy obywateli PRL, którzy po pracy w ZSRR wracali do kraju.*

---

[13] *Współpraca SB MSW PRL z KGB ZSRR w latach 1970–1990. Próba bilansu*, Z. Nawrocki (red.), seria: Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego, Emów 2013.

[14] Zbigniew Nawrocki (1959–2017) – były funkcjonariusz UOP. W latach 2006–2010 dyrektor pionu archiwalnego IPN, a w latach 2010–2015 dyrektor Centralnego Ośrodka Szkolenia ABW w Emowie oraz redaktor naczelny „Przeglądu Bezpieczeństwa Wewnętrznego".

Stwierdzenie pozbawione podstaw. Kandydaci do pozyskania byli zgłaszani do Departamentu II MSW, który podejmował decyzję o pozyskaniu. O wynikach nie informowano KGB.

S. 172, przypis 135: *Dostęp do informacji o związkach byłych opozycjonistów z SB był w UOP praktycznie nielimitowany, gdyż listy sprawdzeń kandydatów do Sejmu i Senatu w wyborach 1991 r. były przechowywane na powszechnie dostępnych komputerach wydziałowo-sekretarskich w UOP.*

Autor *Śpiących psów*… podaje tę informację za Michałem Grockim[15]. W rzeczywistości dane dotyczące kandydatów do parlamentu były zbiorem dokładnie zabezpieczonym w Biurze Ewidencji i Archiwów UOP o ściśle reglamentowanym dostępie, gdzie wówczas nie było komputerów. Nie było ich również w sekretariatach wydziałów.

S. 195–196: *Administracja Reagana kontynuowała prace nad implementacją pocisków balistycznych MX, Pershing II, Cruise oraz bombowców B-1, uzyskując po raz pierwszy w historii zimnej wojny możliwość przeprowadzenia wyprzedzającego uderzenia na ZSRS* (…).

Autor książki myli zdolności do jądrowego uderzenia strategicznego (z USA na ZSRR i odwrotnie) ze zdolnościami średniego zasięgu (z Europy Zachodniej na Wschodnią i odwrotnie). W latach 70. ZSRR miał przewagę w rakietach jądrowych średniego zasięgu rozmieszczonych w Niemieckiej Republice Demokratycznej i Czechosłowacji. Mógł planować atak na Europę Zachodnią z użyciem broni jądrowej, licząc, że USA nie odpowiedzą swoim systemem rakiet międzykontynentalnych, gdyż wtedy ZSRR mógłby odpowiedzieć swoimi rakietami strategicznymi rozmieszczonymi na Syberii. Wprowadzenie amerykańskich rakiet Pershing i Tomahawk zdolnych do przenoszenia głowic jądrowych doprowadziło do równowagi sił nuklearnych w Europie. ZSRR nie mógł już liczyć na „bezkarne" użycie swoich pocisków nuklearnych w Europie, co unieważniło plany ataku na Europę Zachodnią. Rakiety średniego zasięgu rozmieszczone w Europie nie mogły dosięgnąć wyrzutni rakiet międzykontynentalnych rozmieszczonych na Syberii, więc ZSRR zachował zdolność do zniszczenia USA[16]. To, co mogło (w dalekiej przyszłości) zachwiać tą zdolnością, to SDI (Strategic Defense Initiative) ogłoszona przez prezydenta Ronalda Reagana w marcu 1983 r.

Radzieckie służby po raz kolejny okazały swoją typową słabość polegającą na przedstawianiu kierownictwu państwa obrazu sytuacji zgodnego z oczekiwaniami tych władz, a nie z rzeczywistością. Nie potrafiły dostarczyć przekonujących argumentów

[15] M. Grocki, *Konfidenci są wśród nas*, Warszawa [brw].

[16] *Koniec traktatu INF o zakazie posiadania rakiet średniego zasięgu?*, Stowarzyszenie Euro-Atlantyckie, https://sea.org.pl/koniec-traktatu-inf-o-zakazie-posiadania-rakiet-sredniego-zasiegu-.html [dostęp: 26 VIII 2026].

za tym, że SDI to głównie operacja psychologiczna. Ewentualny rzeczywisty rozwój tego systemu musiałby zająć wiele lat, a rezultat był dalece niepewny. Zamiast rozwiewać obawy swoich władz, radzieckie służby podjęły absurdalną operację „Rajan" mającą monitorować przygotowania NATO do ataku jądrowego na ZSRR. Takich przygotowań nie było, ale wielu oficerów radzieckich służb przyjemnie spędzało czas w Europie Zachodniej.

S. 209: (…) *radzieckie służby wywiadowcze (z prawdopodobieństwem graniczącym z absolutną pewnością) budowały sieci agenturalne w PRL najpóźniej od 1976 r.*

Autor książki stwierdza, że miały niemniej niż 15 lat na ich zbudowanie. Nie zauważa jednak, że w ciągu tych 15 lat sytuacja zasadniczo się zmieniała. Do 1980 r. główny wysiłek był skierowany na kontrolowanie władz PRL, a zwłaszcza resortów siłowych i „instytucji frontu ideologicznego". Dopiero od 1980 r. można się spodziewać, że jakaś część uwagi została poświęcona infiltracji Solidarności i opozycji, w celu ewentualnego prowadzenia gier z władzami PRL, a zwłaszcza wymuszania na nich ostrzejszego kursu. Można przyjąć, że zasadniczy wysiłek radzieckich służb również po 1980 r. był skierowany na środowiska związane z władzą lub opozycyjne wobec niej, ale z pozycji ortodoksyjnego komunizmu i więzi z ZSRR.

S. 210: *Przypomnijmy, że w 1991 r. Łomakin był gotów płacić jednorazowo 1500 $ za dokumenty UOP pozyskiwane przez Anklewicza. W schyłkowym PRL-u, gdzie średnia pensja w przeliczeniu na dolary wynosiła 15–20 $, oznaczało to, że w zamian za współpracę z Rosjanami można było jednorazowo otrzymać równowartość 75 do 100 średnich pensji.*

Propozycja dla Anklewicza to był już 1991 r., gdy średnia pensja wynosiła ok. 190 dolarów. Oferta Łomakina odpowiadała zatem ok. 8 średnim pensjom. Wysocy oficerowie MSW mający dostęp do dokumentów ściśle tajnych nie zarabiali średnich pensji, tylko znacznie więcej. Nie były to więc dla nich aż tak oszałamiające kwoty.

S. 224: (…) *nie da się znaleźć jakiejkolwiek racjonalnej przyczyny, dla której GRU zmuszało Zielińskiego do jak najszybszych werbunków, nie zwracając przy tym uwagi na elementarne reguły konspiracji.*

Po pierwsze, Zieliński nie werbował bardzo szybko. To były tylko cztery próby, w tym dwie poważne, w ciągu ponad dwóch lat. Po drugie, ta zwerbowana już agentura (o ile była) nie została zwerbowana przez Łomakina.

S. 229: *Dlaczego zatem Łomakin kazał Zielińskiemu pisać charakterystykę Anklewicza, jakby był on postacią kompletnie nieznaną Rosjanom?*

Autor książki zdaje się nie zauważać, jak wiele zmieniło się od pobytu Anklewicza w ZSRR w latach 80. i jak zmieniła się pozycja Anklewicza. Jest to także element formalny procedury werbunku.

S. 229, przypis 8: *Kto trzeźwo rozumujący podjąłby się werbunku człowieka, wiedząc, że ten ma najwyraźniej bardzo silną motywację, by zachować pracę w UOP.*

Bez sensu byłoby werbowanie kogoś, kto chciałby niebawem odejść z UOP.

S. 230: (…) *dlaczego GRU pchało Zielińskiego do pozyskania Anklewicza, który był naczelnikiem Gabinetu Ministra Spraw Wewnętrznych, rezygnując z prób werbunku naczelnika Biura Techniki UOP oraz oficera Zarządu Kontrwywiadu UOP, o których informował Zieliński?*

Autor książki stwierdza, że w odróżnieniu od tych oficerów Anklewicz mógł mieć tylko bardzo ograniczony kontakt z materiałami operacyjnymi UOP. Nie zauważa, że przez gabinet ministra nie tylko przechodziły dokumenty o charakterze strategicznym, lecz istotne mogły być także informacje o kontaktach ministra z poszczególnymi osobami z kierownictwa. Anklewicz miał też bezpośrednie kontakty z tymi osobami. Można przyjąć, że Anklewicz byłby dla GRU o wiele cenniejszym źródłem niż większość oficerów UOP.

S. 231: *17 grudnia 1991 r., w czasie kolejnego spotkania, Łomakin przekazał Anklewiczowi, że nie chce już więcej materiałów z MSW i MSZ, gdyż – jak powiedział – mają tam szerokie kontakty, znają ludzi i nie mają problemu z uzyskaniem materiałów (a więc powtórnie zdradził posiadane przez GRU zasoby agenturalne). Cenne miały być dla niego jedynie szyfrówki z Moskwy z ocenami sytuacji w Federacji Rosyjskiej dokonywanymi przez ambasadę polską, antyrosyjskie uzgodnienia między RP i USA, a nade wszystko aktywne zainteresowania kontrwywiadu UOP.*

Marek Świerczek błędnie uważa, że zadania stawiane Anklewiczowi przez Łomakina były pozbawione sensu, gdyż nie mógł on mieć dostępu do tych materiałów. W istocie Anklewicz nie miał dostępu do informacji o aktywnych zainteresowaniach kontrwywiadu UOP, ale miał do pozostałych. W sytuacji gdy rozpadał się ZSRR, a RP przeżywała poważny kryzys ekonomiczny, informacje na temat obronności miały mniejsze znaczenie. Zwłaszcza że ZSRR miał bardzo dokładne dane na temat stanu obronności PRL. Natomiast bardzo istotne dla władz w Moskwie były informacje na temat planów mocarstw zachodnich wobec powstającej Federacji Rosyjskiej. Jest też zupełnie zrozumiałe, że Łomakina szczególnie interesowały depesze z ambasady RP w Moskwie. Po pierwsze, osobiście potrzebował informacji na temat zawirowań w polityce wewnętrznej Rosji, aby odpowiednio kierować swoją dalszą karierą. Po drugie, takie depesze, jeśli były przechwytywane przez Rosjan, jak sugeruje Marek Świerczek, mogły stanowić znakomity test wiarygodności materiałów dostarczanych przez Anklewicza. Potwierdziłoby to wartość pozyskanego agenta i podniosło pozycję Łomakina w Moskwie.

S. 236: (…) *nawet szeregowy oficer kontrwywiadu UOP mógł zdobywać informacje na temat spraw operacyjnych prowadzonych przez kolegów, w związku z ówczesnym zwyczajem pozostawiania dokumentów dla pracowników wydziałów w otwartych plastikowych kuwetach w sekretariatach.*

W dodatku Wydział Wschodni Zarządu Kontrwywiadu UOP w tamtym okresie miał jeden tylko telefon z wyjściem na miasto, umiejscowiony w sekretariacie (…).

Opisana sytuacja nie jest zgodna z prawdą. Dokumenty w kuwetach, po dekretacji przełożonych, były w zamkniętych kopertach. Pracownik po otrzymaniu i otwarciu koperty przekazywał sekretarce numer i czego dotyczy (tylko kryptonim lub inicjały osoby) korespondencja. Sekretarka nie miała wglądu w dokumentację.

Wydział Wschodni, w początkowym okresie pracy (przez kilka tygodni), dysponował jedną jednostką telefoniczną z numerem miejskim. Dodatkowe numery miejskie zostały przydzielone jeszcze w tym samym roku. Należy nadmienić, że od początku istnienia tego wydziału wszystkie numery wewnętrzne miały uprawnienia wyjścia na miasto.

Nawet, co bardzo wątpliwe, jeśli w tym wydziale nie przestrzegano zasad poufności pracy operacyjnej, to Łomakin nie mógł o tym wiedzieć. Natomiast w oczach przełożonych Łomakina zwerbowanie przez niego szeregowego oficera byłoby o wiele mniejszym sukcesem niż pozyskanie dyrektora gabinetu ministra spraw wewnętrznych.

S. 236: (…) *przekazywał dopiero co zwerbowanemu szpiegowi* [chodzi o Anklewicza – dop. aut. recenzji] *wskazówki nt. posiadanych (?) zasobach agenturalnych w MSW, MON i MSZ*.

Autor książki nie dopuszcza myśli, że Łomakin się chwalił i nie mówił prawdy? Nie podawał przecież, co oczywiste, żadnych dowodów na dostęp do tych zasobów. Być może testował agenta? Gdyby niebawem wszczęto w tych resortach działania zmierzające do wykrycia przecieków, to byłby dowód, że Anklewicz jest podstawiony przez UOP.

S. 237: (…) *strategiczne decyzje gospodarcze w III RP podejmowano w oparciu o opinie pana po maturze oraz leśnika, który – z nieznanych przyczyn – trafił do służb specjalnych*.

Opinie, o których mowa, nigdy nie były autorstwa pojedynczych osób. Autor książki zapomina też, że Bill Gates i Steve Jobs, a w Polsce Tadeusz Mazowiecki, Lech Wałęsa oraz wielu innych działaczy i polityków również nie ukończyło studiów wyższych.

S. 238: *Będący w powijakach pion gospodarczy UOP nie był w stanie sporządzać choćby quasi-profesjonalnych raportów na temat ówczesnych procesów gospodarczych* (…). *W związku z tym wartość źródła ulokowanego w tym pionie dla GRU była bardzo niewielka (a może nawet zerowa, zważywszy specyfikę zainteresowań wywiadu wojskowego)*.

Po pierwsze, pion pracował (lepiej lub gorzej), ale nie mając tam źródła, Łomakin nie wiedział, jaka jest wartość opracowań tego pionu. Po drugie, nie tylko w okresie takich zmian jak w początku lat 90. sytuacja ekonomiczna państwa jest

kluczowa dla jego zdolności obronnych. Strukturalnie sytuacją gospodarczą zajmowały się trzy jednostki organizacyjne UOP.

S. 240: *Niemniej, z punktu widzenia oficera GRU prowadzącego Zielińskiego, akceptacja obu opisanych wyżej prób werbunkowych* [Feliksa B. i Dariusza C. – dop. aut. recenzji] *stanowiła operacyjny nonsens, powiązany przy tym z monstrualnym ryzykiem dekonspiracji werbownika* (…).

Jednak nie zameldowali oni kontrwywiadowi UOP o tych próbach, czyli ryzyko nie było większe niż w innych przypadkach. Ogólnie werbowanie szpiegów najczęściej jest obarczone ryzykiem.

S. 248: *Czyli, w pewnym uproszczeniu, wraz z początkiem lat dziewięćdziesiątych XX w. doszło do pogłębienia anomii powstałej w służbach specjalnych w dekadzie lat osiemdziesiątych.* (…) *Gdybyśmy przedstawili graficznie sytuację kontrwywiadowczą w ostatniej dekadzie SB i początkach UOP,* (…) *to byłaby to stale opadająca krzywa, która osiągnęła dolne poziomy w latach 1987–1997. Natomiast wykres ilustrujący poziom zaangażowania służb radzieckich (rosyjskich) w Polsce ukazywałby stale wznoszącą się krzywą*.

Autor *Śpiących psów*… nie dostrzega wpływu otoczenia politycznego i zmian organizacyjnych w samych służbach, zarówno radzieckich/rosyjskich, jak i polskich.

Polskie służby, zwłaszcza cywilne, przeszły wstrząs związany z upadkiem PRL, rozwiązaniem SB, weryfikacją jej funkcjonariuszy i utworzeniem UOP. Można założyć, że funkcjonariusze przyjęci do UOP czuli satysfakcję i w większości identyfikowali się z nową służbą i nowym państwem. UOP został też na samym początku zasilony nieliczną, ale energiczną kadrą wywodzącą się z opozycji demokratycznej i dbającą o budowę postaw patriotycznych i propaństwowych wśród funkcjonariuszy wywodzących się z SB. Zasadnie można założyć, że najniższy punkt morale polskich służb cywilnych przypadł na pierwszą połowę 1990 r., gdy została rozwiązana SB i pracowała Sejmowa Komisja Nadzwyczajna do Zbadania Działalności MSW (tzw. komisja Rokity). Później morale rosło, chociaż nie obyło się bez kryzysów.

Radzieckie służby wchodziły w drugiej połowie lat 80. w kryzys wynikający z rezygnacji państwa radzieckiego z masowego terroru i totalnej kontroli nad społeczeństwem. Skutkowało to pojawieniem się ruchów narodowych w republikach radzieckich, gigantycznym rozwojem struktur przestępczych i powstaniem ruchu demokratycznego w samej Rosji. W połowie 1991 r., gdy zaczyna się sprawa Zielińskiego, ZSRR wyraźnie chylił się ku upadkowi, co musiało bardzo obniżać morale służb. W sierpniu 1991 r. pucz Janajewa gwałtownie przyspieszył ten proces. Zainteresowanie oficerów służb specjalnych z konieczności musiało skoncentrować się na zachowaniu osobistej pozycji lub opuszczeniu służb i rozwijaniu kariery poza nimi (patrz Putin). Minimum morale radzieckich/rosyjskich służb przypadło więc na drugą połowę 1991 r. i początek 1992 r. Zainteresowania rosyjskich służb zwróciły się na byłe republiki radzieckie (bliska zagranica) i najważniejsze państwa

Zachodu, zwłaszcza USA. Państwa byłego obozu socjalistycznego miały znaczenie drugorzędne. Bez większych oporów wycofano z nich jednostki rosyjskiej armii. Poważny kryzys ekonomiczny i strukturalny Federacji Rosyjskiej nie pozwalał służbom na zaangażowanie znacznych środków na drugorzędnych kierunkach. Nie były w stanie przeciwdziałać rozszerzeniu NATO. Dopiero poczynając od 2000 r., następuje konsolidacja i podjęcie agresywnych działań. Tak więc można przyjąć, że autor książki błędnie przedstawił zmienność w czasie sytuacji kontrwywiadowczej UOP oraz zaangażowania wywiadowczego radzieckich/rosyjskich służb w Polsce.
S. 281: *Przy obsadzie stanowisk kierowniczych* [w UOP – dop. aut. recenzji] (…) *nie organizowano konkursów mogących wyłonić najlepszych kandydatów* (…).

Stwierdzenie autora książki jest nieprawdziwe. Takich praktyk nie stosowano i nie stosuje się w żadnych służbach specjalnych.
S. 282, przypis 27: *W UOP, a później w ABW chyba jedynym polem awansu poziomego były tzw. dodatki językowe (…). Ta możliwość została zablokowana w ABW przez K. Bondaryka, który – w sprzeczności z konstytucyjną zasadą praw nabytych – „wygasił" bezterminowo przyznane dodatki językowe, a jednocześnie zrobił bardzo wiele, by ściśle powiązać stopnie oraz tzw. grupy zaszeregowania ze stanowiskami. Dzięki temu polska służba specjalna* (…) *miała być tworem na kształt urzędów carskich, w których wyżsi urzędnicy zarabiali krocie, zaś urzędnicza drobnica żyła „od pierwszego do pierwszego", spłacając kredyty zaciągnięte w czasach gdy – dzięki dodatkom – posiadano wyższe świadczenia. Był to potężny cios w morale kadry ABW* (…).

Ten fragment zdaje się stanowić wyjaśnienie takich, a nie innych poglądów autora wyrażonych w tej książce.

W tym okresie w ABW wprowadzono motywacyjny system nagradzania funkcjonariuszy ruchomym dodatkiem służbowym, przyznawanym na czas określony (z reguły na kwartał i przedłużany bądź nie) na wniosek przełożonego, za wyniki osiągane w służbie. Wynagrodzenie funkcjonariusza składało się z wynagrodzenia podstawowego wraz z należnym dodatkiem stałym (z reguły niskim) i wysokim dodatkiem motywacyjnym. Dodatek językowy pozostał w Gabinecie Szefa (sprawy zagraniczne, tłumacze, łącznicy) oraz w Centrum Antyterrorystycznym.

Niezależnie od powyższego dbano o znajomość języków obcych. Przykładowo w 2011 r. sfinansowano udział 1244 funkcjonariuszy ABW w kilkumiesięcznym kursie specjalistycznym pogłębiającym znajomość języka angielskiego[17].
S. 283: (…) *sprawa Zielińskiego była idealnym uwiarygodnieniem dla wszystkich byłych funkcjonariuszy SB, podejmujących służbę w UOP.*

Dwie sprawy (Zieliński, Łomakin) zostały zrealizowane nie dla uwiarygodnienia, lecz z uwagi na bezpieczeństwo RP. Uwiarygodniły zaangażowanych w nie

[17] *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2011 r.*

funkcjonariuszy, ale to nie znaczy, że wszystkich. Inni musieli uwiarygadniać się przez rezultaty własnej pracy.

Tytułem zakończenia

W mojej ocenie intencja autora książki, o czym już wspomniałem, jest jasna – podważyć dobre imię polskiego kontrwywiadu i usprawiedliwić z pozycji „profesjonalnej" decyzję ministra Antoniego Macierewicza nakazującą zaprzestania rozpracowywania rosyjskiej agentury w Polsce.

Trudno mi również oprzeć się wrażeniu, że prowadząc badania historyczne, Marek Świerczek zatrzymał się na rozpoznaniu rosyjskich, a w zasadzie radzieckich, służb specjalnych i na ich działaniu w pierwszej połowie XX w. O obecnych rosyjskich służbach wie niewiele.

Promując książkę w mediach społecznościowych, jej autor znajduje także w sprawach aktualnych, jak np. zatrzymanie za szpiegostwo pracownika cywilnego Ministerstwa Obrony Narodowej, kolejne przykłady gambitu pionka, czyli sposobu zwodzenia służb specjalnych w celu ochrony wyżej plasowanej agentury. Zastanawia mnie głęboko, czemu mogą służyć takie zabiegi autora książki. Niepokojąco przypominają one radziecką i rosyjską dezinformację mającą na celu obezwładnienie woli oporu przeciwnika i spowodowanie jego bierności[18].

Lektura *Śpiących psów*… po raz kolejny skłoniła mnie do refleksji, że zasadne jest podjęcie kompleksowych, interdyscyplinarnych badań nad sytuacją kontrwywiadowczą w Polsce na początku lat 90. oraz historią UOP. Celem powinno być stworzenie opartego na źródłach, możliwie obiektywnego i rzetelnego obrazu funkcjonowania ówczesnych służb, z uwzględnieniem uwarunkowań ich działalności w okresie transformacji ustrojowej oraz wyraźnym rozróżnieniem między ustaleniami źródłowymi a późniejszymi interpretacjami i ocenami.

Recenzja wyraża poglądy autora i nie reprezentuje stanowiska Agencji Bezpieczeństwa Wewnętrznego.

[18] *Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024. Raport Zespołu ds. Dezinformacji*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich, s. 19 [dostęp: 17 X 2026].

Płk Wojciech Dylewski

Absolwent Uniwersytetu Warszawskiego, prawnik, nauczyciel akademicki, funkcjonariusz Urzędu Ochrony Państwa od początku jego istnienia. W 1992 r. zastępca dyrektora Biura Kadr i Szkolenia UOP, a w latach 1993–1996 zastępca dyrektora Zarządu Śledczego UOP nadzorujący wszystkie postępowania o szpiegostwo. W 1996 r. został zwolniony z UOP w związku ze sprawą „Olina". W latach 1997–2001 pełnił funkcje zastępcy Komendanta Głównego Straży Granicznej, podsekretarza stanu w Ministerstwie Spraw Wewnętrznych i Administracji oraz pełnomocnika rządu ds. reformy administracyjnej w województwie dolnośląskim.

PRACE KONKURSOWE

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 227–253
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.030.24179

ARTYKUŁ

Rola oraz możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej[1]

The role and potential applications of open-source intelligence in ensuring the security of the Republic of Poland

ANNA NASTUŁA

Autorka niezależna

https://orcid.org/0000-0002-2061-5067

Abstrakt

Celem artykułu jest określenie znaczenia oraz możliwości wykorzystania wywiadu jawnoźródłowego (*open source intelligence*, OSINT) w zapewnianiu bezpieczeństwa państwa. W opracowaniu omówiono zagadnienia teoretyczne związane z charakterystyką OSINT, w tym jego metody i środki oraz prawne i pozaprawne aspekty jego wykorzystania. Przedstawiono również rozwój OSINT w Stanach Zjednoczonych, Wielkiej Brytanii oraz Izraelu. Następnie zaprezentowano wyniki badań empirycznych zrealizowanych w latach 2023–2024 z zastosowaniem metody indywidualnych wywiadów pogłębionych przeprowadzonych z 12 ekspertami z zakresu bezpieczeństwa oraz wywiadu jawnoźródłowego. Na podstawie dokonanej

[1] Artykuł powstał na podstawie rozprawy doktorskiej pt. *Znaczenie wywiadu jawnoźródłowego w bezpieczeństwie państwa* obronionej na Wojskowej Akademii Technicznej. Praca została nagrodzona w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

analizy oraz wyników badań sformułowano wnioski i rekomendacje dotyczące możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej.

Słowa kluczowe wywiad jawnoźródłowy, OSINT, bezpieczeństwo, informacje jawnoźródłowe, otwarte źródła informacji, cyberbezpieczeństwo

Abstract The aim of this article is to determine the significance and potential applications of open-source intelligence in ensuring state security. The paper discusses theoretical issues related to the characteristics of open-source intelligence, including its methods and means, as well as the legal and non-legal aspects of its use. It also presents the development of open-source intelligence in the United States, the United Kingdom, and Israel. Subsequently, the results of empirical research conducted in 2023–2024 are presented. The study employed the method of individual in-depth interviews carried out with twelve experts in the fields of security and OSINT. Based on the findings of the empirical research and the theoretical analysis undertaken, conclusions and recommendations were formulated regarding the possibilities of using open-source intelligence in ensuring the security of the Republic of Poland.

Keywords open-source intelligence, OSINT, security, open-source information, open sources, cybersecurity

Wprowadzenie

Rola i skala wykorzystania otwartych źródeł informacji systematycznie wzrastają. Wynika to z postępującej rewolucji w dziedzinie technologii informacyjnych, zwiększającej się transparentności procesów politycznych charakterystycznych dla państw demokratycznych oraz z procesów globalizacyjnych. Tym zjawiskom towarzyszy znaczny przyrost ilości informacji ze źródeł otwartych, ich zróżnicowanie oraz problem z ich analizą. W obliczu tych wyzwań zasadne staje się pytanie o rolę i znaczenie wywiadu jawnoźródłowego (*open source intelligence*, OSINT)[2], perspektywy jego rozwoju, a także – co najistotniejsze – możliwości zastosowania w celu zapewnienia bezpieczeństwa państwa.

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

Istotnym warunkiem bezpieczeństwa państwa jest dostęp do rzetelnych i aktualnych informacji, które stanowią jeden z jego strategicznych zasobów. Zmiany społeczno-komunikacyjne przyczyniły się do wzrostu znaczenia mediów społecznościowych jako przestrzeni wymiany informacji, kształtowania opinii publicznej oraz prowadzenia dyskursu politycznego. W konsekwencji decyzje w obszarze bezpieczeństwa państwa coraz częściej opierają się na informacjach pozyskiwanych ze źródeł otwartych, stanowiących podstawę OSINT. Wywiad jawnoźródłowy to zaplanowane i zorganizowane pozyskiwanie oraz przetwarzanie informacji, a następnie dystrybucja produktu analitycznego do określonej grupy odbiorców (decydentów) w ustalonej formie, zgodnie ze sprecyzowanym zapotrzebowaniem informacyjnym. Źródła OSINT są legalne oraz powszechnie dostępne, ale dostęp do niektórych może wymagać poniesienia nakładów.

Celem artykułu jest określenie znaczenia oraz możliwości wykorzystania wywiadu jawnoźródłowego w zapewnianiu bezpieczeństwa Rzeczypospolitej Polskiej. Przedstawione rozważania oparto na wynikach badań przeprowadzonych przez autorkę w ramach rozprawy doktorskiej pt. *Znaczenie wywiadu jawnoźródłowego w bezpieczeństwie państwa*.

Charakterystyka wywiadu jawnoźródłowego

W tradycyjnym ujęciu ukształtowanym w amerykańskiej terminologii wojskowo-wywiadowczej ze względu na rodzaj źródeł pozyskiwania informacji wyróżnia się pięć podstawowych dyscyplin wywiadowczych:

1) HUMINT (*human intelligence*) – wywiad osobowy (źródła osobowe),
2) SIGINT (*signals intelligence*) – wywiad elektromagnetyczny (źródła elektromagnetyczne),
3) IMINT (*imagery intelligence*) – wywiad obrazowy (źródła obrazowe),
4) MASINT (*measurement and signature intelligence*) – wywiad pomiarowo-badawczy (źródła badawczo-pomiarowe),
5) OSINT (*open source intelligence*) – wywiad jawnoźródłowy (otwarte źródła informacji).

Rozpoczęcie rozpoznania od eksploracji źródeł otwartych jest praktycznie zawsze uzasadnione oraz zazwyczaj prowadzi do obniżenia kosztów związanych z innymi kategoriami działalności wywiadowczej[3]. Eksperci bezpieczeństwa oceniają, że to właśnie informacje jawnoźródłowe pozyskiwane ze wszystkich możliwych ogólnie dostępnych źródeł składają się obecnie na ostateczny materiał

[3] J. Konieczny, *Kryminalistyczny leksykon śledztwa*, Opole 2020, s. 336.

wywiadowczy[4]. Z tego względu zasadne jest postrzeganie wymienionych dyscyplin wywiadowczych jako nakładających się na siebie, a wywiadu jawnoźródłowego jako integralnej części wszystkich działań wywiadowczych[5].

Wywiad jawnoźródłowy dostarcza kontekstu prowadzonego rozpoznania przez zapewnienie ogólnej wiedzy, która stanowi punkt wyjścia do określenia dalszych kierunków rozpoznania. Użyteczność OSINT wynika z możliwości szybkiego pozyskiwania informacji o rozległej tematyce. Istotną zaletą jest także to, że można weryfikować i uzupełniać informacje o te uzyskiwane ze źródeł zamkniętych. Powszechny dostęp do źródeł otwartych umożliwia szybką reakcję na zdarzenia i skraca czas podejmowania decyzji na rzecz bezpieczeństwa. Wywiad jawnoźródłowy może dostarczać skondensowanych i precyzyjnych informacji, które pozwalają zweryfikować przyjęte założenia oraz stanowią wystarczającą podstawę do formułowania nowych hipotez analitycznych. Dodatkowym atutem takiego wywiadu jest łatwość wymiany i rozpowszechniania uzyskanej wiedzy między podmiotami odpowiedzialnymi za bezpieczeństwo. Ponadto pozwala on na prowadzenie analiz na bieżąco, co ma szczególne znaczenie w dynamicznie zmieniającym się środowisku bezpieczeństwa[6].

Rozwój globalnej sieci wpłynął na ewolucję wywiadu jawnoźródłowego. Wyodrębnienie kolejnych generacji OSINT jest powiązane z etapami rozwoju World Wide Web – Sieć 1.0, Sieć 2.0 i Sieć 3.0[7]. Każda z nich odzwierciedla zarówno postęp technologiczny, jak i zmieniające się potrzeby w zakresie pozyskiwania informacji jawnoźródłowych. Rysunek 1 przedstawia najważniejsze cechy kolejnych generacji OSINT.

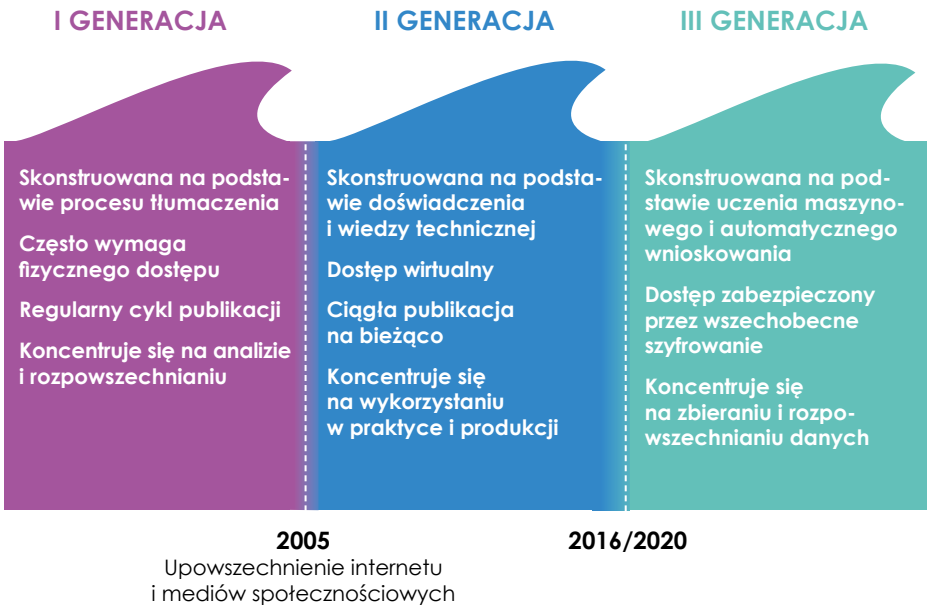
---

[4] W opracowaniu NATO wskazano, że ponad 80% informacji zawartych w końcowym materiale wywiadowczym może pochodzić ze źródeł otwartych. Jeden z przywołanych szacunków dotyczył wsparcia wywiadowczego w zakresie przeciwdziałania proliferacji. Zob. NATO, *Open Source Intelligence Reader*, February 2002, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf, s. 17, 73 [dostęp: 27 III 2025]. W 2005 r. emerytowany wysoki rangą funkcjonariusz CIA William M. Nolte stwierdził, że 95–98% wszystkich informacji przetwarzanych przez społeczność wywiadowczą USA pochodzi ze źródeł otwartych. Zob. S.D. Gibson, *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content, s. 93 [dostęp: 25 VI 2026].

[5] M.M. Lowenthal, *OSINT the State of Art, The Artless State*, „Studies in Intelligence" 2001, t. 45, nr 3, s. 63.

[6] S.D. Gibson, *Open Source Intelligence*, w: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (red.), London 2014, s. 127.

[7] H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, s. 39 [dostęp: 27 III 2025].



Rysunek 1. Generacje wywiadu jawnoźródłowego.

Źródło: opracowanie własne na podstawie: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, s. 40 [dostęp: 27 III 2025].

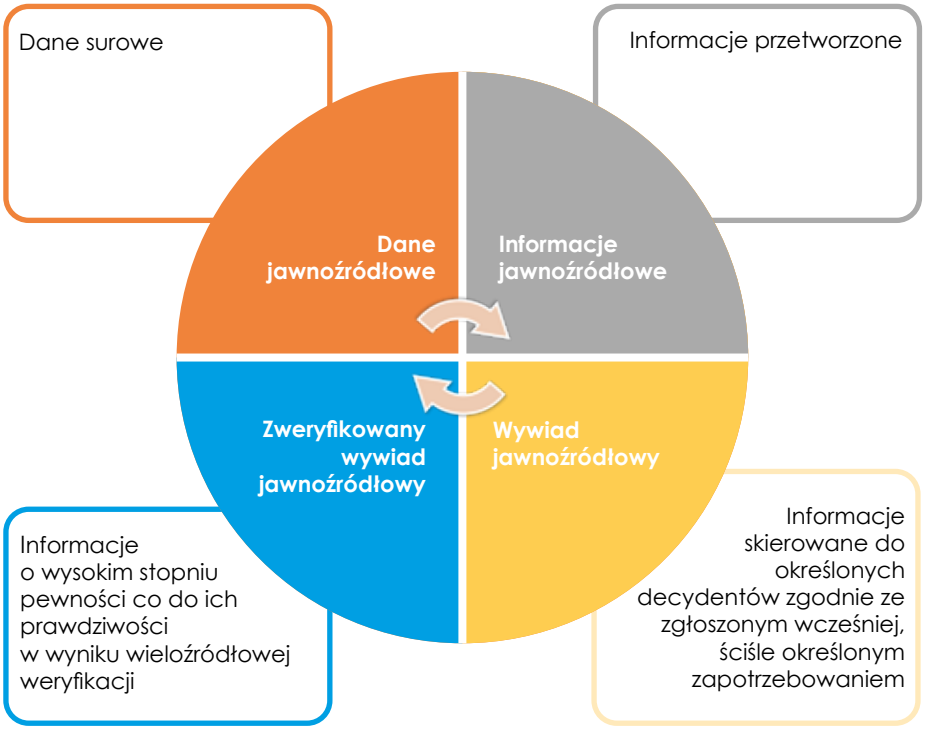
Pierwsza generacja OSINT była związana z rozwojem Sieci 1.0 w latach 90. XX w. Charakteryzowała się brakiem interaktywności oraz prostą, jednokierunkową komunikacją, której model można przyrównać do triady klasycznych mediów, tj. prasy, radia i telewizji. W tym okresie działalność wywiadowcza opierała się na gromadzeniu, monitorowaniu, analizie i rozpowszechnianiu informacji oraz tłumaczeniu materiałów zagranicznych.

Przejście do drugiej generacji OSINT nastąpiło wraz z rozwojem Sieci 2.0 i zmianą modelu komunikacji między właścicielami serwisów internetowych a ich użytkownikami. Wzrost interaktywności komunikacji oraz udziału użytkowników w tworzeniu treści sprzyjał dynamicznemu rozwojowi mediów społecznościowych i niemal ciągłej publikacji informacji. W rezultacie zwiększył się udział informacji jawnoźródłowych w prowadzonych działaniach wywiadowczych.

Trzecia generacja wywiadu jawnoźródłowego jest związana z rozwojem Sieci 3.0. Sieć ta, określana mianem semantycznej, umożliwia uczenie maszynowe i automatyczne wnioskowanie. Na tym etapie rozwoju OSINT szczególnego znaczenia nabierają również rozszerzona rzeczywistość (*augmented reality*) i psychometria,

a jednym z głównych wyzwań staje się upowszechnienie szyfrowania ograniczającego dostęp do informacji[8].

Podstawowe pojęcia, takie jak dane jawnoźródłowe, informacje jawnoźródłowe, wywiad jawnoźródłowy oraz zweryfikowany wywiad jawnoźródłowy, oraz założenia dotyczące OSINT zostały opracowane przez amerykańskie służby specjalne i ekspertów zajmujących się działalnością rozpoznawczą współpracujących w ramach NATO. Proces przekształcania danych jawnoźródłowych w produkt wywiadowczy został przedstawiony na rysunku 2.



Rysunek 2. Proces przekształcania danych jawnoźródłowych w produkt wywiadowczy.

Źródło: opracowanie własne.

Dane jawnoźródłowe (*open source data*, OSD) to surowe dane pochodzące ze źródeł pierwotnych. Występują w formie drukowanej, przekazu radiowego i telewizyjnego, ustnych wypowiedzi publicznych lub w innych postaciach, m.in. fotografii,

[8] Tamże, s. 40.

nagrań dźwiękowych i audiowizualnych, komercyjnych zobrazowań, prywatnej korespondencji. Dane te można klasyfikować ze względu na format na: ustrukturyzowane, częściowo ustrukturyzowane i nieustrukturyzowane.

Informacje jawnoźródłowe to dane pozyskane w pierwszym etapie, poddane odpowiedniemu przetworzeniu obejmującemu, w zależności od charakteru OSD, translację, transkrypcję, konwersję formatu, a także filtrowanie, korelację, grupowanie oraz interpretację. W wyniku integracji, oceny i analizy informacji, dokonywanych w celu odpowiedzi na konkretne zapytania, powstaje produkt wywiadowczy. Dodatkowym etapem jest wieloźródłowa weryfikacja produktu wywiadowczego przez funkcjonariuszy mających dostęp do informacji niejawnych, która pozwala ocenić stopień wiarygodności tego produktu. Wysoki poziom wiarygodności można osiągnąć również w przypadku informacji pochodzących z jawnego źródła, którego prawdziwość nie budzi wątpliwości. W ten sposób powstaje zweryfikowany produkt wywiadu jawnoźródłowego.

Źródła otwarte można klasyfikować według kanału przekazywania publicznie dostępnych informacji na: treści pozyskane z obserwacji, dokumenty i materiały drukowane, treści transmitowane przez media nadawcze oraz treści cyfrowe[9].

Gromadzenie informacji przez obserwację polega na ich bezpośrednim pozyskiwaniu od osób fizycznych, grup osób lub podczas publicznych wydarzeń, oficjalnych kontaktów oraz obserwacji otoczenia. Umożliwia to uzyskanie aktualnych informacji niewystępujących jeszcze w sformalizowanych źródłach.

Dokumenty i materiały drukowane, obejmujące m.in. prasę, książki, raporty, dokumenty urzędowe oraz szarą literaturę, stanowią podstawowe źródło wiedzy faktograficznej i specjalistycznej, pozwalające na weryfikację oraz pogłębioną analizę informacji.

Media nadawcze, takie jak radio, telewizja oraz inne nieinternetowe publicznie dostępne transmisje, dostarczają informacji o charakterze społeczno-politycznym, gospodarczym i z dziedziny bezpieczeństwa, umożliwiając monitorowanie bieżących wydarzeń.

Publicznie dostępne treści cyfrowe obejmują wszelkie dane, które można pobierać i przetwarzać za pomocą urządzeń cyfrowych, niezależnie od ich formatu. Do tej kategorii treści należą strony internetowe, blogi, media społecznościowe oraz inne zasoby internetowe dostępne we wszystkich warstwach sieci, również w darknecie.

[9] OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023 r., s. 2. Dokument jest dostępny na stronie: https://www.osintfoundation.com/osint/Standards.asp [dostęp: 25 VI 2026].

Skuteczność OSINT zależy od właściwej identyfikacji źródeł, doboru odpowiednich metod analizy oraz krytycznej oceny wiarygodności pozyskanych informacji. Dynamiczny rozwój źródeł otwartych prowadzi do stopniowego zacierania granic między informacjami jawnymi i niejawnymi[10]. Wymaga to zmiany podejścia do klasyfikacji źródeł informacji oraz metod ich analizy, a także uwzględnienia nowych wyzwań prawnych i organizacyjnych.

Metody i środki OSINT w cyberprzestrzeni

Rozwój nowoczesnych technologii znacznie zwiększył efektywność i precyzję pozyskiwania informacji ze źródeł otwartych. Przyjmując klasyfikację gromadzenia informacji opartą na czterech rodzajach wykorzystywanych źródeł otwartych (obserwacja, dokumenty drukowane, media nadawcze, treści cyfrowe) należy zaznaczyć, że obecnie wywiad jawnoźródłowy obejmuje zarówno tradycyjne metody pozyskiwania informacji, jak i zaawansowane rozwiązania oparte na automatyzacji, analizie dużych zbiorów danych oraz sztucznej inteligencji. We współczesnym wywiadzie jawnoźródłowym dominującą rolę odgrywają źródła internetowe.

Pozyskiwanie informacji z internetu może być realizowane zarówno manualnie, jak i automatycznie z użyciem specjalistycznych narzędzi i skryptów. Do charakterystycznych metod cyfrowego OSINT należą: monitorowanie, wyszukiwanie, techniczny footprinting, analiza mediów społecznościowych oraz web scraping.

Monitorowanie polega na ustrukturyzowanym i systematycznym śledzeniu w określonym czasie zmieniających się treści generowanych przez stałe źródło.

Wyszukiwanie obejmuje posłużenie się wyspecjalizowanym oprogramowaniem lub stronami internetowymi do eksploracji internetu w celu pozyskania informacji odpowiadających określonym potrzebom informacyjnym.

Techniczny footprinting, inaczej odtwarzanie śladów cyfrowych, jest procesem gromadzenia dostępnych informacji na temat systemów komputerowych, infrastruktury sieciowej, technologii, usług oraz podmiotów, do których należą. Dzięki technicznemu footprintingowi można odtworzyć techniczny i organizacyjny obraz badanego podmiotu, zidentyfikować jego zasoby cyfrowe oraz rozpoznać potencjalne podatności informacyjne na podstawie źródeł otwartych.

Analiza mediów społecznościowych pozwala na identyfikację treści, relacji, nastrojów, wzorców zachowań oraz dynamiki komunikacji w środowisku cyfrowym. Ten rodzaj analizy odgrywa istotną rolę w zarządzaniu sytuacjami kryzysowymi, ponieważ umożliwia monitorowanie procesów radykalizacji, identyfikację zagrożeń oraz

[10] H.J. Williams, I. Blum, *Defining Second Generation*…, s. 37.

prognozowanie trendów wpływających na bezpieczeństwo. Informacje pozyskane z mediów społecznościowych są wykorzystywane do zwalczania przestępczości i terroryzmu – wspierają profilowanie kryminalne, w tym pośrednie szacowanie osobowości, opracowanie taktyki przesłuchania oraz typowanie kandydatów do roli agenta[11].

Web scraping polega na automatycznym pozyskiwaniu danych z zasobów internetowych i zapisywaniu ich w systemie plików lub bazie danych w celu późniejszego wyszukiwania, przetwarzania i analizy.

Metody pozyskiwania informacji można podzielić ze względu na poziom interakcji z obiektem rozpoznania na pasywne, półpasywne i aktywne[12]. Wybór właściwej metody zależy od podmiotu prowadzącego rozpoznanie, celu i charakteru działań, rodzaju pozyskiwanych informacji oraz wymagań bezpieczeństwa operacyjnego (*operations security*) i powinien zostać określony już na etapie planowania. Metody półpasywne i aktywne wymagają interakcji z badanym obiektem lub jego infrastrukturą, dlatego wykraczają poza klasyczną definicję wywiadu jawnoźródłowego opartego na pozyskiwaniu informacji bez ingerencji w obiekt rozpoznania[13]. Rekonesans pasywny stanowi podstawową metodę prowadzenia wywiadu jawnoźródłowego, z uwagi na cel gromadzenia informacji wyłącznie ze źródeł otwartych oraz konieczność zachowania wysokich standardów etycznych i bezpieczeństwa prowadzonych działań.

Informacje jawnoźródłowe mogą być również kupowane od podmiotów komercyjnych lub ich pozyskanie może być zlecone w ramach outsourcingu. Często używa się do tego programów agentowych i botów. Rozwiązania te wymagają jednak zachowania odpowiednich standardów etycznych oraz zgodności z obowiązującymi przepisami.

Ze względu na metody pozyskiwania i przetwarzania informacji jawnoźródłowych można wyróżnić cztery główne kategorie narzędzi:

1) językowe i tekstowe (lingwistyczne),
2) geoprzestrzenne,
3) oparte na teorii sieci (sieciowe),
4) wykorzystujące kryminalistykę wizualną[14].

Narzędzia lingwistyczne umożliwiają analizę dużych zbiorów danych tekstowych pochodzących z wielu źródeł i języków. Są one wykorzystywane do identyfikacji

[11] Zob. szerzej: J. Konieczny, *Kryminalistyczny leksykon*…, s. 145, 202–203.

[12] N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018, s. 14.

[13] W Izraelu, ze względu na różnice w normach prawnych oraz uwarunkowania społeczno-historyczne, część metod półpasywnych i aktywnych jest uznawana za element wywiadu jawnoźródłowego.

[14] H. Akın Ünver, *Digital Open Source Intelligence and International Security: A Primer*, „Cyber Governance and Digital Democracy" 2018, nr 8, s. 8. https://doi.org/10.13140/RG.2.2.16242.56000.

słów kluczowych, analizy częstotliwości ich występowania oraz wnioskowania o cechach demograficznych, poglądach i zachowaniach autorów. Analiza sentymentu oraz analiza stanowiska pozwalają określić emocjonalny wydźwięk wypowiedzi, postawy oraz intencje badanych podmiotów. Coraz większą rolę odgrywa przetwarzanie języka naturalnego (*natural language processing*) oraz uczenie maszynowe, zapewniające automatyczną analizę wielojęzycznych i nieustrukturyzowanych zbiorów danych oraz identyfikację wzorców językowych.

Narzędzia geoprzestrzenne służą do pozyskiwania i analizy informacji lokalizujących osoby, obiekty i zdarzenia w przestrzeni geograficznej, wspierając rozpoznanie sytuacji politycznej, militarnej i kryzysowej. Podstawowe metody analizy geoprzestrzennej obejmują geotagowanie, geolokację, geownioskowanie oraz georeferencjonowanie[15]. Pozwalają one określać położenie obiektów, odtwarzać ich przemieszczanie oraz identyfikować zależności przestrzenne. W analizach są wykorzystywane systemy informacji geograficznej, dane GPS, zobrazowania satelitarne i lotnicze, LIDAR oraz informacje publikowane w mediach społecznościowych. Integracja danych geoprzestrzennych z innymi źródłami OSINT umożliwia monitorowanie konfliktów zbrojnych, migracji ludności, sytuacji kryzysowych oraz infrastruktury krytycznej, co zwiększa świadomość sytuacyjną oraz wspiera procesy decyzyjne w obszarze bezpieczeństwa państwa.

Narzędzia sieciowe opierają się na metodach analizy relacji między osobami, organizacjami, miejscami i innymi podmiotami. Umożliwia to identyfikację struktur społecznych oraz zależności występujących w badanych sieciach. W wywiadzie jawnoźródłowym są używane przede wszystkim do analizy mediów społecznościowych przez wyszukiwanie, mapowanie i ocenę relacji między użytkownikami z wykorzystaniem metod obliczeniowej analizy sieci oraz sztucznej inteligencji. Narzędzia sieciowe znajdują zastosowanie m.in. w identyfikacji sieci terrorystycznych i przestępczych, analizie kampanii dezinformacyjnych oraz rozpoznawaniu mechanizmów oddziaływania na grupy społeczne.

Narzędzia wykorzystujące kryminalistykę wizualną służą do ekstrakcji danych z plików graficznych i wideo, umożliwiają wykrywanie zmanipulowanych obrazów oraz przeprowadzenie analizy fotogrametrycznej. Ich znaczenie wzrosło wraz z rozwojem mediów społecznościowych i ewolucją komunikacji z tekstowej na opartą na mediach. W analizie materiałów wizualnych stosuje się m.in. analizę artefaktów, fotogrametrię, analizę metadanych, porównanie fotograficzne oraz analizę cyfrową, wspieraną danymi geoprzestrzennymi, zobrazowaniami satelitarnymi i materiałami z dronów. Metody te umożliwiają weryfikację autentyczności obrazów i nagrań, wykrywanie manipulacji, geolokalizację zdarzeń oraz rekonstrukcję ich przebiegu,

[15] H.J. Williams, I. Blum, *Defining Second Generation*…, s. 33.

dostarczając materiału o wartości dowodowej. Rozwiązania z zakresu kryminalistyki wizualnej są szeroko wykorzystywane w działaniach wywiadowczych, dochodzeniowych oraz dokumentowaniu naruszeń praw człowieka i konfliktów zbrojnych.

Rozwój technologii informacyjnych, automatyzacji i sztucznej inteligencji znacznie zwiększył efektywność oraz precyzję wywiadu jawnoźródłowego. Umożliwił gromadzenie i automatyczną analizę ogromnych zbiorów danych, skrócił czas opracowania produktów wywiadowczych oraz podniósł ich wartość analityczną. Zintegrowane wykorzystanie różnych narzędzi OSINT ułatwia wzajemne uzupełnianie i weryfikację pozyskanych informacji, dzięki czemu można otrzymać pełniejszy i bardziej wiarygodny obraz analizowanego zjawiska. Efektywność ich użycia zależy jednak nie tylko od możliwości technologicznych, lecz także od wiedzy i praktycznych umiejętności analityka oraz właściwego doboru metod i narzędzi.

Prawne i pozaprawne aspekty wywiadu jawnoźródłowego

Wywiad jawnoźródłowy funkcjonuje w środowisku prawnym, które nie zostało dotychczas kompleksowo uregulowane ani na szczeblu krajowym, ani międzynarodowym. Brak jednoznacznych regulacji prowadzi do rozbieżności interpretacyjnych oraz zróżnicowanych praktyk stosowania OSINT. Może to ograniczać jego skuteczność i jednocześnie zwiększać ryzyko zagrożeń dla bezpieczeństwa państwa. Choć istotą OSINT jest wykorzystywanie informacji pochodzących z publicznie dostępnych źródeł, to ich agregacja za pomocą nowoczesnych narzędzi może prowadzić do identyfikacji osób fizycznych, tzw. efekt mozaiki. Powoduje to wyzwania w zakresie ochrony prywatności i danych osobowych. Aspekty prawne dotyczą również ochrony praw autorskich oraz baz danych, które mogą obejmować wykorzystywane materiały jawnoźródłowe. Dodatkowe aspekty wynikają z rosnącej roli prywatnych podmiotów prowadzących działalność OSINT, których aktywność wpływa na dotychczasowy model zarządzania informacją wywiadowczą. Kolejnym zagadnieniem jest pozyskiwanie informacji wykraczających poza zakres postawionego zapytania, co może prowadzić do naruszenia przepisów prawa oraz norm etycznych dotyczących ochrony prywatności i godności jednostki.

Rozproszenie regulacji prawnych sprawia, że normy etyczne pełnią funkcję uzupełniającą wobec prawa, wyznaczając granice pozyskiwania i analizy informacji. Automatyzacja procesów gromadzenia i analizy dużych zbiorów danych (Big Data) zwiększa znaczenie tych standardów, jednak ich dobrowolny charakter nie zapewnia skutecznego ograniczania powstających zagrożeń. Zarówno w praktyce, jak i w literaturze przedmiotu jest akcentowana pilna potrzeba opracowania spójnych

ram etycznych dla prowadzenia wywiadu jawnoźródłowego przez podmioty państwowe i prywatne[16].

Inne pozaprawne czynniki, które wpływają na OSINT, to uwarunkowania metodologiczne oraz techniczne. Obejmują one m.in. zakłócenia cyklu wywiadowczego, błędy poznawcze analityków, problemy językowe oraz ograniczenia infrastruktury technicznej i bezpieczeństwa operacyjnego.

Informacje jawnoźródłowe, ze względu na swoją dostępność oraz łatwość rozpowszechniania, są szczególnie podatne na manipulacje. Najpoważniejsze zagrożenia dla wywiadu jawnoźródłowego stanowią dezinformacja i propaganda, których celem jest świadome zniekształcanie rzeczywistości, kształtowanie postaw odbiorców oraz wpływanie na procesy decyzyjne. Rozwój mediów cyfrowych oraz technologii informacyjnych znacznie zwiększył skuteczność tych działań, umożliwiając szybkie rozpowszechnianie fałszywych narracji oraz ich dostosowywanie do określonych grup odbiorców. Propaganda pełni obecnie funkcję nie tylko perswazyjną, lecz także mobilizacyjną oraz służy kształtowaniu narracji społeczno-politycznych. Dezinformacja stała się jednym z podstawowych elementów wrogich operacji informacyjnych prowadzonych zarówno przez państwa, jak i podmioty niepaństwowe. Jej celem jest destabilizacja sytuacji politycznej, społecznej i gospodarczej oraz osłabianie zaufania do instytucji państwa. Współczesne technologie, w tym sztuczna inteligencja, umożliwiają tworzenie zaawansowanych form manipulacji, takich jak fake newsy i deepfaki, których wykrywanie staje się coraz większym wyzwaniem analitycznym.

Jednocześnie wywiad jawnoźródłowy odgrywa istotną rolę w wykrywaniu i analizie kampanii dezinformacyjnych oraz propagandowych. Skuteczne przeciwdziałanie manipulacjom informacyjnym wymaga jednak posłużenia się nowoczesnymi technologiami wspierającymi analizę OSINT oraz podnoszenia kompetencji analityków i odporności społeczeństwa na dezinformację.

Rozwój wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii i Izraelu

Analiza doświadczeń Stanów Zjednoczonych, Wielkiej Brytanii oraz Izraela w zakresie wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa państwa pozwala zidentyfikować dotychczasowe kierunki rozwoju OSINT w państwach

[16] Etycznym aspektom wywiadu jawnoźródłowego były poświęcone międzynarodowe projekty badawcze, np. The Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation (VIRTUOSO, 2010–2013), The Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime (CAPER, 2011–2014), The Maritime Integrated Surveillance Awareness (MARISA, 2017–2020).

demokratycznych o wysoko rozwiniętych instytucjach bezpieczeństwa oraz wieloletniej praktyce w posługiwaniu się informacjami jawnoźródłowymi.

Początki zinstytucjonalizowanego wywiadu jawnoźródłowego w USA sięgają okresu II wojny światowej, kiedy utworzono Służbę Monitoringu Nadawców Zagranicznych (Foreign Broadcast Monitoring Service), którą 26 lipca 1942 r. przekształcono w Federalną Służbę Informacji Radiowej (Federal Broadcast Information Service). Instytucja ta odpowiadała za monitorowanie, tłumaczenie i analizę zagranicznych informacji pochodzących ze źródeł otwartych. W kolejnych latach rozwój OSINT wspierały m.in. Wydział Dokumentacji Zagranicznej (Foreign Documents Division) oraz Federalny Wydział Badawczy Biblioteki Kongresu (Federal Research Division). Reformy przeprowadzone po zakończeniu zimnej wojny[17] oraz po zamachach z 11 września 2001 r.[18] miały przełomowe znaczenie i doprowadziły do utworzenia Open Source Center, a następnie Open Source Enterprise funkcjonującego w strukturach Centralnej Agencji Wywiadowczej (Central Intelligence Agency).

W marcu 2024 r. opublikowano Strategię OSINT Wspólnoty Wywiadowczej Stanów Zjednoczonych na lata 2024–2026[19], określającą kompleksową wizję, priorytety i kierunki dalszego rozwoju wywiadu jawnoźródłowego oraz działania ukierunkowane na wzmocnienie jego roli w systemie wywiadowczym. Cele strategii ujęto w czterech kluczowych obszarach:

1. Koordynacja pozyskiwania danych ze źródeł otwartych oraz rozszerzenie ich udostępniania.
2. Ustanowienie zintegrowanego zarządzania zasobami informacji jawnoźródłowych.

[17] Raport Komisji do spraw Ról i Możliwości Wspólnoty Wywiadowczej Stanów Zjednoczonych (Commission on the Roles and Capabilities of the United States Intelligence Community, potocznie: komisja Aspina-Browna) z 1996 r. zawierał rekomendacje dotyczące reformy amerykańskiej Wspólnoty Wywiadowczej. Autorzy raportu podkreślili znaczenie informacji jawnoźródłowych oraz konieczność dostosowania działalności wywiadowczej do złożonych i wielowymiarowych zagrożeń. Zob. szerzej: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, „American Intelligence Journal" 1995, t. 16, nr 2/3, s. 11–17.

[18] Na potrzebę reformy struktury wywiadowczej Stanów Zjednoczonych, w tym utworzenia podmiotu odpowiedzialnego za wywiad jawnoźródłowy, wskazywała Narodowa Komisja ds. Ataków Terrorystycznych na Stany Zjednoczone (The National Commission on Terrorist Attacks Upon the United States, potocznie: komisja 9/11) w swoim raporcie opublikowanym w 2004 r. Zob. *The 9/11 Commission Report*, https://www.9-11commission.gov/report/911Report.pdf [dostęp: 15 VI 2026].

[19] United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT*, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [dostęp: 15 VI 2026].

3. Rozwój innowacji w zakresie OSINT w celu tworzenia nowych zdolności analitycznych i operacyjnych.
4. Kształcenie specjalistów oraz doskonalenie metodologii wywiadu jawnoźródłowego[20].

Strategia stanowi istotny etap instytucjonalizacji OSINT, wzmacniając jego integrację z działalnością Wspólnoty Wywiadowczej Stanów Zjednoczonych (United States Intelligence Community) oraz potwierdzając jego znaczenie dla procesów analitycznych i decyzyjnych.

Ewolucja wywiadu jawnoźródłowego w USA doprowadziła do jego formalizacji i profesjonalizacji oraz ugruntowania jego roli w działalności wywiadowczej.

Rozwój wywiadu jawnoźródłowego w Wielkiej Brytanii ma najdłuższą udokumentowaną historię spośród analizowanych państw. Istotną rolę w jego rozwoju odegrała działalność utworzonego w 1939 r. BBC Monitoring, odpowiedzialnego za monitorowanie, tłumaczenie i analizę zagranicznych źródeł informacji. Po zakończeniu II wojny światowej elementem brytyjskiego systemu bezpieczeństwa stała się współpraca międzynarodowa realizowana w ramach sojuszu Five Eyes[21], umożliwiająca wymianę informacji jawnoźródłowych oraz koordynację działań wywiadowczych. Wywiad jawnoźródłowy znajduje zastosowanie również w działalności brytyjskiej policji oraz służb specjalnych, takich jak Służba Bezpieczeństwa (Security Service, MI5) i Tajna Służba Wywiadowcza (Secret Intelligence Service, MI6). Wspiera zapobieganie terroryzmowi, zwalczanie przestępczości oraz przeciwdziałanie zagrożeniom hybrydowym.

Zasady wykorzystywania informacji jawnoźródłowych przez organy ścigania w Wielkiej Brytanii określiła Krajowa Rada Szefów Policji (National Police Chiefs' Council). W swoich wytycznych wskazuje ona m.in. na konieczność przestrzegania przepisów prawa, proporcjonalność działań oraz poszanowanie prawa do prywatności i ochrony danych osobowych[22]. Z kolei brytyjskie Ministerstwo Obrony (Ministry of Defence) ujęło OSINT w doktrynie działalności wywiadowczej, definiując go jako informacje wywiadowcze pochodzące z informacji

[20] Tamże, s. 1.

[21] Five Eye (Sojusz Pięciorga Oczu) – partnerstwo wywiadowcze Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii, którego podstawę stanowiło brytyjsko-amerykańskie porozumienie zawarte 5 marca 1946 r. Współpraca obejmuje wymianę informacji pozyskiwanych w ramach różnych dyscyplin wywiadowczych, w tym wywiadu jawnoźródłowego.

[22] J. Housego, *NPCC Guidance on Open Source Investigation/Research*, April 2015, https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf, s. 4–5 [dostęp: 14 VIII 2026].

publicznie dostępnych oraz innych informacji jawnych o ograniczonym dostępie lub rozpowszechnianiu[23].

Współpraca z sektorem prywatnym i środowiskiem akademickim, realizowana m.in. za pośrednictwem OSINT Hub działającego w ramach CENTRIC[24], sprzyja rozwojowi nowoczesnych narzędzi, kompetencji oraz innowacyjnych metod pozyskiwania i analizy informacji jawnoźródłowych. Uzupełnieniem tego modelu jest działalność wyspecjalizowanych organizacji pozarządowych i podmiotów prywatnych, takich jak Association of British Investigators oraz UK OSINT Community, promujących rozwój kompetencji, standardów oraz dobrych praktyk w zakresie OSINT. Z kolei osiągnięcia Bellingcat i BBC potwierdziły znaczenie wywiadu jawnoźródłowego w dokumentowaniu konfliktów zbrojnych, naruszeń praw człowieka oraz przeciwdziałaniu dezinformacji, m.in. w związku z agresją Rosji na Ukrainę[25].

Brytyjski model wywiadu jawnoźródłowego wyróżnia się podejściem łączącym rozwój aspektów organizacyjnych i legislacyjnych, współpracę międzynarodową oraz wykorzystanie potencjału sektora prywatnego i środowiska akademickiego.

Działalność wywiadowcza Izraela jest uznawana za jedną z najskuteczniejszych na świecie. Jednocześnie analiza izraelskiego modelu wykorzystania OSINT stanowi wyzwanie badawcze ze względu na ograniczoną dostępność oficjalnych informacji. To ograniczenie wynika z geopolitycznych i historycznych uwarunkowań państwa, a także możliwości celowego kształtowania przekazu oraz zniekształcania w ramach działań dezinformacyjnych informacji dostępnych w źródłach otwartych.

Analiza programu szkoleniowego dla europejskich służb wywiadowczych uruchomionego przez Mossad w 2021 r. wskazuje, że wywiad jawnoźródłowy jest intensywnie wykorzystywany w działalności operacyjnej izraelskiego wywiadu[26]. Program podkreśla znaczenie integracji informacji jawnoźródłowych z danymi pochodzącymi z innych źródeł wywiadowczych, rozwoju nowoczesnych metod

[23] Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3, s. 2–12, pkt 227 [dostęp: 14 VIII 2026].

[24] *OSINT Hub. CENTRIC open cource intelligence hub*, CENTRIC, https://centric-research.co.uk/projects/osint-hub [dostęp: 15 VI 2026].

[25] A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, s. 11 [dostęp: 25 VI 2026].

[26] *Mossad trains European intel agents in open source spy tools analysis*, Intelligence Online, 20 VII 2022 r., https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra [dostęp: 18 VI 2026].

gromadzenia i analizy informacji oraz współpracy izraelskiego wywiadu z sektorem prywatnym.

Zarówno Shin Bet odpowiedzialna za bezpieczeństwo wewnętrzne, jak i Aman, czyli wywiad wojskowy, traktują OSINT jako uzupełnienie informacji pozyskiwanych z innych źródeł wywiadowczych. Przykładem skutecznego zastosowania analizy komunikacji prowadzonej za pośrednictwem mediów społecznościowych i komunikatorów internetowych było udaremnienie zamachów planowanych przez Al-Kaidę na ambasadę USA w Tel Awiwie oraz na Międzynarodowe Centrum Konferencyjne w Jerozolimie[27].

W ramach Amanu funkcjonuje jednostka 8200, która specjalizuje się w SIGINT. W jej strukturach utworzono komórkę Hatzav odpowiedzialną za wywiad jawnoźródłowy. Ewolucja mediów społecznościowych doprowadziła do rozszerzenia działalności Hatzav z monitorowania tradycyjnych mediów arabskich na analizę informacji publikowanych w czasie rzeczywistym w serwisach internetowych. Miało to znaczenie zarówno taktyczne, ponieważ umożliwiało monitorowanie informacji dotyczących konkretnych operacji, jak i strategiczne, gdyż pozwalało na analizę nastrojów społecznych. Hatzav rozwijał specjalistyczne narzędzia analityczne oraz model szkolenia oparty na kompetencjach językowych, znajomości mediów społecznościowych i umiejętnościach informatycznych. W 2021 r. Hatzav został zlikwidowany, a jego zadania rozproszone. Przeciwnicy tej decyzji krytykowali nadmierne poleganie na technicznych metodach pozyskiwania informacji kosztem analiz prowadzonych przez wyspecjalizowanych analityków OSINT.

Doświadczenia związane z wojną, która rozpoczęła się 7 października 2023 r., doprowadziły do odtworzenia Hatzav oraz odbudowy zdolności służb w zakresie wywiadu jawnoźródłowego. Decyzja o reaktywacji jednostki potwierdziła, że OSINT stanowi odrębną i komplementarną wobec pozostałych dyscyplin wywiadowczych formę rozpoznania. Nie są w stanie jej zastąpić zaawansowane rozwiązania technologiczne i sztuczna inteligencja, które nie uchwycą np. niuansów językowych i kulturowych, takich jak kontekst polityczny, uwarunkowania społeczne czy pamięć instytucjonalna[28].

Z analizy porównawczej rozwoju i wykorzystania wywiadu jawnoźródłowego w Stanach Zjednoczonych, Wielkiej Brytanii i Izraelu wynika, że wszystkie te państwa dostrzegają rosnące znaczenie informacji pochodzących ze źródeł otwartych

[27] M. Ginsburg, T. Staff, *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014 r., https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/ [dostęp: 25 IV 2024].

[28] A. Bohbot, *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025 r., https://www.jpost.com/israel-news/defense-news/article-858491 [dostęp: 25 VI 2026].

oraz ich istotny wpływ na bezpieczeństwo. Różnice są widoczne zarówno na płaszczyźnie definicyjnej, jak i w sposobie postrzegania wywiadu jawnoźródłowego. Stany Zjednoczone i Wielka Brytania koncentrują się na równoległym rozwoju jego aspektów organizacyjnych i legislacyjnych, podczas gdy w Izraelu OSINT pełni funkcję jedynie wspomagającą, jako element naprowadzający do podejmowania złożonych działań operacyjnych.

Jednocześnie we wszystkich analizowanych państwach obserwuje się intensywny rozwój i wykorzystanie nowoczesnych technologii, w tym sztucznej inteligencji i Big Data, co wiąże się z koniecznością dalszych inwestycji w infrastrukturę technologiczną oraz rozwój metod analitycznych. Technologie te znajdują zastosowanie odpowiednio w rozwoju narzędzi OSINT w Stanach Zjednoczonych, działaniach policyjnych i monitorowaniu zagrożeń wewnętrznych w Wielkiej Brytanii oraz integracji wywiadu jawnoźródłowego z operacjami cyberbezpieczeństwa w Izraelu.

Kolejną wspólną cechą jest rozproszenie działań i odpowiedzialności w zakresie wywiadu jawnoźródłowego między podmioty publiczne. Prowadzi to do ograniczonej współpracy między instytucjami, niedostatecznego finansowania potrzeb operacyjnych oraz zróżnicowania poziomu dostępu i metod gromadzenia danych.

Istotnym obszarem wymagającym dalszego rozwoju pozostają kompetencje w zakresie wywiadu jawnoźródłowego, przy czym w Stanach Zjednoczonych i Wielkiej Brytanii nadal są dostrzegane braki w analizie, selekcji, integracji i dystrybucji informacji jawnoźródłowych w całym cyklu wywiadowczym. Izrael rozwija te kompetencje we współpracy z sektorem prywatnym, obejmującej transfer wiedzy, technologii oraz działalność szkoleniową.

We wszystkich omówionych państwach jako kierunek rozwoju jest wskazywane wzmacnianie współpracy międzynarodowej zarówno w ramach sojuszy takich jak Five Eyes, jak i partnerstw z sektorem prywatnym, które służą wymianie informacji, koordynacji działań, rozwojowi nowoczesnych technologii oraz poprawie zdolności wywiadowczych i cyberbezpieczeństwa.

Przeprowadzona analiza wskazuje, że Stany Zjednoczone, Wielka Brytania oraz Izrael systematycznie zwiększają wykorzystanie wywiadu jawnoźródłowego, wzmacniając tym samym swoje zdolności w zakresie działań zarówno defensywnych, jak i ofensywnych.

Wykorzystanie OSINT a możliwości państwa w zakresie przeciwdziałania zagrożeniom. Wyniki badań

Celem badań przeprowadzonych przez autorkę w ramach przygotowywania rozprawy doktorskiej było pozyskanie jakościowych informacji umożliwiających

identyfikację zależności między wykorzystaniem wywiadu jawnoźródłowego a możliwościami państwa w zakresie przeciwdziałania zagrożeniom wewnętrznym i zewnętrznym. Zamierzeniem było również uzyskanie prognoz dotyczących kierunków rozwoju metod oraz środków technicznych stosowanych do pozyskiwania i analizy informacji jawnoźródłowych w celu zapewniania bezpieczeństwa państwa.

Badanie było realizowane od grudnia 2023 r. do kwietnia 2024 r., co pozwoliło na zachowanie względnie stałych warunków badawczych w odniesieniu do zarówno prawnych i pozaprawnych aspektów wykorzystania wywiadu jawnoźródłowego, uwarunkowań geopolitycznych, jak i stosowanych metod oraz środków technicznych używanych w rozpoznaniu prowadzonym z wykorzystaniem źródeł otwartych. Zastosowano metodę indywidualnych wywiadów pogłębionych (*in-depth interviews*). Do udziału w badaniu zaproszono 12 ekspertów wybranych według określonych kryteriów. Były to osoby mające specjalistyczną wiedzę oraz bogate doświadczenie zawodowe w obszarze bezpieczeństwa i OSINT. Część z nich uczestniczyła po 1990 r. w tworzeniu komórek organizacyjnych zajmujących się wywiadem jawnoźródłowym w Polsce. Wśród respondentów znaleźli się byli oraz czynni zawodowo funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Jednostki Wojskowej GROM, Wojsk Obrony Terytorialnej oraz Wojsk Obrony Cyberprzestrzeni, przedstawiciel administracji rządowej zatrudniony w Departamencie Cyberbezpieczeństwa Ministerstwa Cyfryzacji, naukowiec zajmujący się problematyką wywiadu i bezpieczeństwa państwa, detektyw oraz dziennikarz śledczy pełniący wcześniej funkcję dyrektora w biurze analiz i informacji. Narzędziem badawczym był *Scenariusz wywiadu z ekspertami wykorzystującymi wywiad jawnoźródłowy w swojej pracy zawodowej*, obejmujący 11 pytań dotyczących doświadczeń respondentów związanych z wykorzystaniem OSINT oraz oceny jego znaczenia dla bezpieczeństwa państwa.

Eksperci konsekwentnie akcentowali, że wywiad jawnoźródłowy odgrywa istotną rolę w zapewnianiu bezpieczeństwa państwa, wspierając procesy decyzyjne na wszystkich poziomach zarządzania, od lokalnego po międzynarodowy. Integracja informacji jawnoźródłowych z informacjami operacyjnymi na wczesnym etapie analizy zwiększa zrozumienie problemu oraz skuteczność planowania działań. Respondenci podkreślali również, że rozwój technologii informacyjnych oraz zmieniające się środowisko bezpieczeństwa systematycznie podnoszą znaczenie OSINT, przy czym jego potencjał nie jest w pełni wykorzystywany, zwłaszcza w obszarze wspierania rozwoju gospodarczego i strategicznego państwa.

Uczestnicy badania przewidują, że zastosowanie nowoczesnych technologii, w tym sztucznej inteligencji oraz zaawansowanych narzędzi Big Data, doprowadzi do dalszego rozwoju i poprawy efektywności wykorzystania wywiadu jawnoźródłowego w sektorze bezpieczeństwa. Automatyzacja procesów pozyskiwania i analizy

informacji jawnoźródłowych, wspierana przez algorytmy uczenia maszynowego, pozwala na szersze, a przede wszystkim ciągłe monitorowanie źródeł otwartych. Tym samym możliwe się staje skrócenie czasu niezbędnego do przetwarzania informacji, co podnosi zdolność identyfikacji i oceny zagrożeń oraz przyczynia się do szybszego reagowania na nie. Narzędzia oparte na sztucznej inteligencji usprawniają analizę tekstu, obrazu, dźwięku oraz innych treści multimedialnych, identyfikację wzorców, zależności i trendów, a także analizę mediów społecznościowych. Eksperci podkreślili, że w zakresie metod wykorzystywanych w OSINT szczególnego znaczenia nabierają analiza predykcyjna, analiza semantyczna oraz analiza sieci społecznościowych. Jednocześnie integracja metod i narzędzi OSINT umożliwia prowadzenie wieloaspektowej analizy informacji pochodzących z różnych źródeł i zwiększa możliwości identyfikacji zależności, wykrywania zagrożeń oraz wspierania procesów decyzyjnych w obszarze bezpieczeństwa państwa.

Analiza tych wypowiedzi wskazuje, że prawne i pozaprawne uwarunkowania prowadzenia wywiadu jawnoźródłowego mają istotny wpływ na jego skuteczność, przy czym największym wyzwaniem pozostaje manipulacja informacją, w tym działania dezinformacyjne, propaganda, fake newsy oraz smog informacyjny. Agregacja i przetwarzanie informacji jawnoźródłowych, mimo ich legalnego pozyskania, mogą prowadzić do identyfikacji osób fizycznych, co rodzi istotne wyzwania prawne i etyczne w obszarze ochrony prywatności i danych osobowych. Na efektywność wykorzystania OSINT wpływają ponadto czynniki technologiczne, ekonomiczne i organizacyjne, w szczególności ograniczony dostęp do specjalistycznych narzędzi, wysokie koszty ich wdrażania oraz niewystarczająca współpraca między instytucjami. Istotną barierę stanowi również niedostateczny poziom kompetencji analitycznych, brak doświadczenia, predyspozycji psychologicznych oraz specjalistycznych szkoleń funkcjonariuszy.

Na podstawie przeprowadzonych wywiadów można stwierdzić, że jednym z głównych kierunków rozwoju wywiadu jawnoźródłowego w państwach demokratycznych jest wzmacnianie międzynarodowej współpracy oraz wymiany informacji z państwami sojuszniczymi. Kooperacja międzynarodowa przyczynia się do zwiększenia zdolności państw do identyfikowania i oceny globalnych zagrożeń, takich jak terroryzm, cyberataki czy dezinformacja, przez co wspiera procesy decyzyjne w obszarze bezpieczeństwa. Skuteczność tej współpracy wymaga stosowania jednolitych standardów bezpieczeństwa, przestrzegania zasad etycznych oraz obowiązujących regulacji prawnych. Jednocześnie eksperci podkreślali, że współpraca międzynarodowa wymaga zachowania szczególnej ostrożności oraz starannej selekcji udostępnianych materiałów, aby nie ujawniać sojusznikom informacji mogących wskazywać na słabe strony państwa, zwłaszcza w sytuacji

zmieniających się uwarunkowań geopolitycznych i zróżnicowanych priorytetów poszczególnych sojuszników.

Wnioski i rekomendacje dla Rzeczypospolitej Polskiej

Coraz większa liczba informacji jawnoźródłowych oraz dynamiczny rozwój technologii informacyjnych powodują systematyczny wzrost znaczenia wywiadu jawnoźródłowego jako integralnego elementu procesów wywiadowczych. Zastosowanie nowoczesnych technologii zwiększa wydajność pozyskiwania, przetwarzania i analizy informacji jawnoźródłowych, jednocześnie skracając czas reakcji na zagrożenia.

Uwarunkowania prawne i pozaprawne wpływają na skuteczność OSINT. Jednym z największych wyzwań w tym obszarze pozostaje dezinformacja, której efektywne przeciwdziałanie wymaga zintegrowania działań technologicznych, organizacyjnych, prawnych oraz edukacyjnych. Brak jednolitych regulacji oraz niejednoznaczność podstawowych pojęć mogą prowadzić do niepewności prawnej i rozbieżności interpretacyjnych, co zmniejsza skuteczność wywiadu jawnoźródłowego. Warunkiem jego optymalnego wykorzystania jest więc wdrożenie rozwiązań prawnych, organizacyjnych i technicznych, które zapewnią spójność działań podmiotów odpowiedzialnych za bezpieczeństwo państwa.

Wywiad jawnoźródłowy odgrywa istotną rolę we wspieraniu procesów decyzyjnych w obszarze bezpieczeństwa państwa przez identyfikację i ocenę zagrożeń oraz budowanie świadomości sytuacyjnej. Jednocześnie współpraca i wymiana informacji z państwami sojuszniczymi, sektorem prywatnym oraz środowiskiem akademickim może prowadzić do sprawniejszego monitorowania globalnych zagrożeń, standaryzacji metod analitycznych oraz poprawy jakości produktów wywiadowczych.

Na podstawie wniosków z analizy teoretycznej oraz badań empirycznych autorka sformułowała rekomendacje dotyczące usprawnienia wykorzystania wywiadu jawnoźródłowego na rzecz bezpieczeństwa RP. Ich wdrożenie mogłoby poprawić współpracę między podmiotami odpowiedzialnymi za bezpieczeństwo państwa, zwiększyć efektywność zarządzania informacjami jawnoźródłowymi oraz ograniczyć ryzyko błędów wynikających z ich interpretacji. W konsekwencji byłoby możliwe zwiększenie zdolności państwa do wczesnego wykrywania i oceny zagrożeń, skuteczniejsze planowanie działań w obszarze bezpieczeństwa oraz lepsze wykorzystanie informacji jawnoźródłowych w procesach decyzyjnych. Rekomendacje, które mogłyby stanowić również element dalszej modernizacji struktur bezpieczeństwa, obejmują cztery obszary.

1. Uporządkowanie w polskim systemie prawnym pojęć związanych z wywiadem jawnoźródłowym

Zdefiniowanie podstawowych pojęć związanych z wywiadem jawnoźródłowym pozwoli na ograniczenie rozbieżności interpretacyjnych oraz precyzyjne określenie zakresu pozyskiwania i analizy informacji jawnoźródłowych. W konsekwencji zmniejszy się ryzyko naruszenia przepisów dotyczących ochrony danych osobowych, prawa do prywatności, praw autorskich oraz innych regulacji sektorowych. Wprowadzenie odpowiednich regulacji prawnych zapewni przejrzystość funkcjonowania wywiadu jawnoźródłowego oraz stworzy podstawy do opracowania jednolitych procedur, standardów i dobrych praktyk w zakresie prowadzenia działań OSINT, co przyczyni się do jego standaryzacji i profesjonalizacji. Spójne ramy prawne zwiększą zaufanie do wyników analiz OSINT oraz możliwości ich wykorzystania w procesach decyzyjnych. Stworzą również warunki do bezpiecznego wdrażania narzędzi bazujących na nowoczesnych technologiach, w tym sztucznej inteligencji, w analizie informacji jawnoźródłowych. Dostosowanie regulacji do norm międzynarodowych usprawni również współpracę międzynarodową w omawianym obszarze.

Ta rekomendacja jest zgodna z kierunkami rozwoju wywiadu jawnoźródłowego w Stanach Zjednoczonych oraz Wielkiej Brytanii, gdzie równolegle doskonali się aspekty organizacyjne oraz legislacyjne.

2. Stworzenie Zespołu Koordynacyjnego ds. Wywiadu Jawnoźródłowego

Zespół podlegający bezpośrednio Prezesowi Rady Ministrów i skupiający przedstawicieli służb specjalnych oraz agencji rządowych zapewniałby koordynację działań państwa w obszarze wywiadu jawnoźródłowego. Jego funkcjonowanie przyczyniłoby się do przyspieszenia procesów pozyskiwania i analizy informacji jawnoźródłowych, wyeliminowania dublowania działań, poprawy ekonomiki operacji oraz optymalizacji wykorzystania zasobów. Opracowywanie spójnych produktów analitycznych, opartych na informacjach jawnoźródłowych pozyskiwanych przez różne podmioty, zwiększyłoby kompleksowość analiz oraz zdolność państwa do identyfikowania działań dezinformacyjnych i przeciwdziałania im.

Do zadań zespołu należałoby inicjowanie, koordynowanie oraz monitorowanie działań podejmowanych przez organy administracji rządowej w zakresie wywiadu jawnoźródłowego. Zespół realizowałby zadania związane z opracowywaniem i przekazywaniem danych wyjściowych oraz analiz jawnoźródłowych służbom specjalnym, podmiotom odpowiedzialnym za bezpieczeństwo państwa, w tym Prezydentowi Rzeczypospolitej Polskiej, Prezesowi Rady Ministrów, marszałkom Sejmu i Senatu, Radzie Ministrów według rozdzielnika, ministrowi koordynującemu służby specjalne, szefom poszczególnych służb, a także społeczeństwu. Zespół

przygotowywałby również przeznaczone dla społeczeństwa analizy jawnoźródłowe w formie komunikatów, raportów lub cyklicznych opracowań analitycznych, udostępniane z uwzględnieniem wymogów bezpieczeństwa państwa. W ten sposób wspierałby przeciwdziałanie dezinformacji.

Istotnym obszarem jego działalności byłaby organizacja współpracy międzynarodowej w zakresie wywiadu jawnoźródłowego oraz przygotowywanie zbiorczych analiz związanych z zagrożeniami dla Polski i państw sojuszniczych. Do kompetencji tej grupy należałoby również opracowywanie projektów standardów etycznych, procedur prowadzenia OSINT oraz wytycznych dotyczących narzędzi wykorzystywanych do pozyskiwania i analizy informacji. Ponadto zespół przygotowywałby propozycje usprawnienia metod i narzędzi stosowanych przez podmioty publiczne oraz monitorował kierunki działań dezinformacyjnych i źródła otwarte wykorzystywane do ich generowania i rozpowszechniania.

Przedstawiona rekomendacja koresponduje z rozwiązaniami przyjętymi w *Strategii OSINT Wspólnoty Wywiadowczej Stanów Zjednoczonych na lata 2024–2026*[29], w której podkreślono znaczenie centralnej koordynacji, wspólnych standardów oraz integracji działań w obszarze wywiadu jawnoźródłowego.

3. Stworzenie rządowej platformy wymiany informacji jawnoźródłowych jako wspólnej przestrzeni do wyszukiwania, łączenia i promowania materiałów jawnoźródłowych

Utworzenie scentralizowanej rządowej platformy OSINT zapewni wszystkim podmiotom odpowiedzialnym za bezpieczeństwo państwa dostęp do wspólnej przestrzeni pozyskiwania, integracji i udostępniania informacji jawnoźródłowych. Zwiększy to efektywność wymiany tych informacji między podmiotami odpowiedzialnymi za bezpieczeństwo państwa, usprawni ich współpracę i wymianę dobrych praktyk. Krótszy czas identyfikacji zagrożeń i opracowywania materiałów analitycznych poprawi z kolei efektywność procesów decyzyjnych oraz zracjonalizuje wykorzystanie zasobów kadrowych, technicznych i finansowych. Zintegrowana platforma OSINT umożliwi ponadto prowadzenie kompleksowych analiz z uwzględnieniem szerszego kontekstu zagrożeń oraz zależności między nimi, wykraczających poza zakres zadań realizowanych przez poszczególne służby.

Rekomendacja ta znajduje potwierdzenie w rozwiązaniach wdrażanych w Stanach Zjednoczonych i Wielkiej Brytanii. Zarówno amerykańska koncepcja wspólnych platform OSINT powiązanych ze scentralizowanym, wielodomenowym katalogiem informacji dostępnych publicznie i komercyjnie[30], jak i brytyjska platforma

[29] United States Intelligence Community, *IC OSINT Strategy 2024–2026*…

[30] Tamże, s. 3.

INDEX[31] opierają się na centralizacji zasobów, zapewnieniu interoperacyjności systemów oraz stworzeniu wspólnej przestrzeni do gromadzenia i wymiany informacji jawnoźródłowych, raportów oraz narzędzi OSINT. Rozwiązania te zmierzają do wyeliminowania dublowania działań prowadzonych przez poszczególne instytucje, ujednolicenia standardów analitycznych oraz zintensyfikowania wykorzystania nowoczesnych technologii, takich jak uczenie maszynowe i zaawansowane metody analityczne, w procesach analizy informacji. Ich implementacja stanowi ważny punkt odniesienia przy projektowaniu polskich rozwiązań systemowych w zakresie wywiadu jawnoźródłowego.

4. Utworzenie Inkubatora Innowacji Wywiadu Jawnoźródłowego

Celem inicjatywy jest rozwój współpracy między administracją publiczną, sektorem prywatnym, środowiskiem akademickim oraz społeczeństwem obywatelskim w zakresie wywiadu jawnoźródłowego. Jej efektem byłaby wymiana wiedzy i doświadczeń, rozwój innowacyjnych metod i narzędzi OSINT oraz budowanie trwałych relacji wspierających bezpieczeństwo RP.

Model ten umożliwiałby wykorzystanie wiedzy i doświadczenia byłych funkcjonariuszy służb z praktyką operacyjną oraz ekspertów z zakresu nowoczesnych technologii, którzy tworzyliby kadrę inkubatora. Synergia ich kompetencji sprzyjałaby rozwojowi innowacyjnych rozwiązań w obszarze wywiadu jawnoźródłowego.

Współpraca z sektorem prywatnym otwierałaby drogę do pozyskiwania nowoczesnych technologii oraz bezpiecznego outsourcingu wybranych procesów związanych z pozyskiwaniem i analizą informacji, przy jednoczesnej optymalizacji kosztów dzięki współfinansowaniu badań, rozwoju technologii i innowacyjnych projektów.

Do podstawowych zadań Inkubatora Innowacji Wywiadu Jawnoźródłowego należałoby tworzenie nowych technologii i narzędzi oraz rozwijanie metod wykorzystywanych w wywiadzie jawnoźródłowym, w tym rozwój algorytmów wspierających analizę informacji jawnoźródłowych. Istotnym obszarem jego działalności, wynikającym z interdyscyplinarności OSINT, powinno być również pozyskiwanie kadr o zróżnicowanych kompetencjach zawodowych i doświadczeniach. Inkubator odpowiadałby również za organizację szkoleń i działań edukacyjnych skierowanych zarówno do funkcjonariuszy służb specjalnych i pracowników jednostek sektora finansów publicznych, jak i do społeczeństwa. Ponadto jego zadaniem byłaby organizacja konferencji i sympozjów na szczeblu rządowym i samorządowym oraz rozwijanie współpracy

[31] J. Hugill, *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021 r., https://www.public.io/blog-post/introducing-index-a-cross-government-digital-information-and-data-exchange [dostęp: 25 VI 2026].

z sektorem prywatnym, ośrodkami akademickimi i instytucjami badawczymi w celu wspólnego opracowywania innowacyjnych rozwiązań w obszarze OSINT.

Zasadność utworzenia takiego inkubatora potwierdzają doświadczenia Izraela, gdzie powołano CyberSpark Innovation Arena. Jest to wspólne przedsięwzięcie izraelskiej administracji publicznej, środowiska akademickiego oraz sektora przemysłowego ukierunkowane na rozwój innowacji i współpracy w obszarze cyberbezpieczeństwa[32]. Inicjatywa ta pokazuje, że integracja potencjału administracji, nauki i przemysłu sprzyja rozwojowi kapitału ludzkiego, transferowi wiedzy i technologii oraz wzmacnianiu zdolności państwa w zakresie pozyskiwania i analizy informacji jawnoźródłowych.

Podsumowanie

Procesy wywiadowcze są ściśle związane z informacją, technologią oraz zmieniającym się środowiskiem bezpieczeństwa. Rosnąca liczba źródeł otwartych, dostępnych niejednokrotnie w czasie rzeczywistym, umożliwia szybsze reagowanie i dostarczanie odpowiedzi na bieżące potrzeby informacyjne decydentów. Współcześnie czas podejmowania decyzji jest jednym z podstawowych czynników warunkujących poziom bezpieczeństwa oraz zachowanie ciągłości działania. Informacje zdobyte w wyniku działań wywiadu jawnoźródłowego nie tylko uzupełniają informacje pozyskane drogą operacyjną, lecz także przyczyniają się do skrócenia czasu koniecznego do podjęcia decyzji. Zwiększa to skuteczność działań państwa w wymiarach defensywnym i ofensywnym.

Przedstawione uwarunkowania wskazują na potrzebę zmiany sposobu postrzegania roli OSINT przez podmioty odpowiedzialne za bezpieczeństwo państwa oraz modelu współpracy w zakresie wymiany informacji jawnoźródłowych między służbami i organami administracji publicznej. Wdrożenie kompleksowych rozwiązań systemowych umożliwiających dobrą integrację, analizę i wykorzystanie informacji pochodzących ze źródeł otwartych może się przyczynić do poprawy skuteczności prowadzonych działań i ich ekonomicznej efektywności przez ograniczenie kosztów pozyskiwania informacji.

Znaczenie wywiadu jawnoźródłowego będzie systematycznie wzrastać wraz z postępującą cyfryzacją życia oraz wzrostem ilości danych w źródłach otwartych.

[32] *Prime Minister Announces National Cyber Hub*, Americans for Ben-Gurion University, 28 I 2014 r., https://americansforbgu.org/prime-minister-announces-national-cyber-hub/ [dostęp: 27 VI 2026]; *Cyberspark*, World Economic Forum, https://www.weforum.org/organizations/cyberspark/ [dostęp: 27 VI 2026].

W obliczu coraz bardziej złożonych zagrożeń dla bezpieczeństwa Polski zapotrzebowanie na wiarygodne i zweryfikowane informacje nigdy nie było większe. Dlatego wyzwaniem staje się pełne wykorzystanie potencjału wywiadu jawnoźródłowego dla obrony RP oraz jej strategicznych interesów.

Bibliografia

Akın Ünver H., *Digital Open-Source Intelligence and International Security: A Primer*, „Cyber Governance and Digital Democracy" 2018, nr 8. https://doi.org/10.13140/RG.2.2.16242.56000.

Gibson S.D., *Open Source Intelligence*, w: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (red.), London 2014.

Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018.

Konieczny J., *Kryminalistyczny leksykon śledztwa*, Opole 2020.

Lowenthal M.M., *OSINT the State of Art, The Artless State*, „Studies in Intelligence" 2001, t. 45, nr 3, s. 61–66.

Preparing for the 21st Century. An Appraisal of U.S. Intelligence. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, „American Intelligence Journal" 1995, t. 16, nr 2/3, s. 11–17.

Źródła internetowe

Bohbot A., *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025 r., https://www.jpost.com/israel-news/defense-news/article-858491 [dostęp: 25 VI 2026].

Cyberspark, World Economic Forum, https://www.weforum.org/organizations/cyberspark/ [dostęp: 27 VI 2026].

Gibson S.D., *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content [dostęp: 25 VI 2026].

Ginsburg M., Staff T., *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014 r., https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/ [dostęp: 25 IV 2024].

Hugill J., *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021 r., https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/ [dostęp: 25 VI 2026].

Janjeva A., Harris A., Byrne J., *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf [dostęp: 25 VI 2026].

Mossad trains European intel agents in open-source spy tools analysis, Intelligence Online, 20 VII 2022 r., https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra [dostęp: 18 VI 2026].

OSINT Hub CENTRIC open cource intelligence hub, CENTRIC, https://centric-research.co.uk/projects/osint-hub [dostęp: 15 VI 2026].

Prime Minister Announces National Cyber Hub, Americans for Ben-Gurion University, 28 I 2014 r., https://americansforbgu.org/prime-minister-announces-national-cyber-hub/ [dostęp: 27 VI 2026].

The 9/11 Commission Report, https://www.9-11commission.gov/report/911Report.pdf [dostęp: 15 VI 2026].

Williams H.J., Blum I., *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf [dostęp: 27 III 2025].

Inne dokumenty

Housego J., *NPCC Guidance on Open Source Investigation/Research*, April 2015, https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf [dostęp: 14 VIII 2026].

Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3 [dostęp: 14 VIII 2026].

NATO, *Open Source Intelligence Reader*, February 2002, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf [dostęp: 27 III 2025].

OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023 r. Dokument jest dostępny na stronie: https://www.osintfoundation.com/osint/Standards.asp [dostęp: 25 VI 2026].

United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT.* https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [dostęp:15 VI 2026].

Dr Anna Nastuła

Doktor nauk o bezpieczeństwie (Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie), prawnik, certyfikowany audytor wiodący ISO/IEC 27001 oraz AQAP 2110:2016 i ISO 9001:2015. Inspektor ochrony danych, obsługuje podmioty publiczne i prywatne. Prowadzi szkolenia i warsztaty na temat ochrony danych osobowych i cyberbezpieczeństwa. Prelegentka podczas konferencji krajowych i międzynarodowych. Autorka publikacji naukowych z zakresu prawa i cyberbezpieczeństwa.

Kontakt: anna.nastula@arkadiapolska.com

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 255–284
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.031.24180

ARTYKUŁ

Kryminalistyczne aspekty pobierania próbek węgla kamiennego dla celów postępowania karnego[1]

Forensic Aspects of Hard Coal Sampling in Criminal Proceedings

KAMIL LEŚNIEWSKI

Autor niezależny

https://orcid.org/0000-0003-2988-0024

Abstrakt

Praktyka pokazuje, że skuteczne zwalczanie przestępczości związanej z górnictwem węgla kamiennego niejednokrotnie jest zadaniem trudnym do zrealizowania – poczynając od etapu wykrywczego, a na procesie dowodzenia kończąc. Trudności mogą wynikać z różnych przyczyn, w tym ze specyfiki rozważanych przestępstw oraz ich powiązania z technicznymi uwarunkowaniami działalności górniczej, a w przypadku czynów, których przedmiotem jest węgiel, również z właściwości fizykochemicznych tego surowca. W konsekwencji efektywne prowadzenie postępowań karnych w rozpatrywanym obszarze wymaga często posiadania specjalistycznej wiedzy. W artykule omówiono jedno z wyzwań –

[1] Artykuł powstał na podstawie rozprawy doktorskiej pt. *Kryminalistyczno-prawna problematyka przestępczości gospodarczej na szkodę spółek węglowych na przykładzie Polskiej Grupy Górniczej S.A.* obronionej na Uniwersytecie Jagiellońskim. Autor wykorzystał głównie fragmenty rozdziału 3.4.2. *Ustalenie jakości węgla będącego przedmiotem czynności wykonawczej danego przestępstwa*. Rozprawa zdobyła I miejsce w kategorii „prace doktorskie" w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

problematykę pobierania na potrzeby postępowania karnego próbek węgla kamiennego z naczepy pojazdu ciężarowego. Przeanalizowano ją przez pryzmat zasad taktyki kryminalistycznej oraz wymogów procedury karnej.

Słowa kluczowe górnictwo węgla kamiennego, zwalczanie przestępczości, taktyka kryminalistyczna, trudności dowodowe, pobieranie próbek węgla

Abstract The investigation and prosecution of criminal activities associated with the hard coal mining industry in Poland pose substantial challenges for law enforcement authorities. These difficulties may arise from various factors, including the specific nature of the offences and their close relationship with the technical characteristics of the mining sector. Consequently, many investigations require specialised knowledge, which may significantly complicate the detection of offences as well as the collection and securing of forensically sound evidence. This article discusses one of the challenges encountered in this field, namely the collection of coal samples from vehicles intercepted in connection with coal quality fraud or coal theft, through the lens of forensic principles and evidentiary requirements applicable in criminal proceedings.

Keywords hard coal mining, criminal investigation, investigative techniques and tactics, evidentiary difficulties, coal sampling

Wprowadzenie

W literaturze górnictwo jest przedstawiane jako najstarsza forma działalności technicznej człowieka, której korzenie sięgają czasów prehistorycznych. Badania historyczno-archeologiczne dowodzą, że już w tym okresie górnictwo było obecne na terenach stanowiących obszar współczesnej Polski. Sposobami górniczymi miano początkowo pozyskiwać krzemień, a z biegiem czasu także inne surowce, w tym rudy żelaza[2]. Na przestrzeni wieków na tych terenach wydobywano również m.in. bursztyn, sól, rudy złota, srebra, ołowiu i miedzi, a także węgiel brunatny oraz

[2] P. Strzałkowski, *Zarys rozwoju technologii górnictwa podziemnego*, Gliwice 2011, s. 19.

kamienny. Przyjmuje się, że ostatni z wymienionych surowców zaczęto wydobywać na skalę przemysłową w XVIII w.[3]

Węgiel kamienny występuje w Polsce w trzech złożach – Dolnośląskim Zagłębiu Węglowym, Lubelskim Zagłębiu Węglowym oraz Górnośląskim Zagłębiu Węglowym, przy czym aktualnie wydobycie jest prowadzone wyłącznie w dwóch ostatnich. W piśmiennictwie teza, że w XX w. górnictwo węgla kamiennego odegrało istotną rolę w rozwoju Polski, wydaje się nie wzbudzać kontrowersji. Zauważa się równocześnie, że chociaż rola tego sektora – jako strategicznego elementu polskiej gospodarki – maleje, to przez najbliższe dekady w dalszym ciągu będzie on mieć istotne znaczenie dla funkcjonowania i rozwoju kraju. Pomimo spadającego udziału węgla w krajowym miksie energetycznym zasoby węgla kamiennego posiadane przez Polskę nadal są określane jako stabilizator bezpieczeństwa energetycznego kraju[4].

Z teoretycznego punktu widzenia rozważania nauk prawnych w zakresie górnictwa węgla kamiennego mogą dotyczyć czterech zasadniczych aspektów: 1) prawnomiędzynarodowego (np. problematyka kopalń jako dopuszczalnego celu wojskowego), 2) administracyjnoprawnego (np. problematyka koncesji na wydobywanie kopalin), 3) cywilnoprawnego (np. problematyka odszkodowań za szkody wyrządzone ruchem zakładów górniczych) oraz 4) prawnokarnego, w tym kryminalistycznego (np. problematyka wypadków i katastrof w podziemnych wyrobiskach, problematyka metodyk śledczych w sprawach przestępstw popełnianych na szkodę spółek górniczych, a związanych bezpośrednio z ich działalnością gospodarczą).

Artykuł poświęcono metodyce pobierania na potrzeby postępowania karnego próbek węgla kamiennego znajdującego się w naczepie pojazdu ciężarowego, w związku z zatrzymaniem in flagranti osób podejrzewanych o jego przestępczy wywóz. Zagadnienie to wpisuje się w szerszą problematykę wskazaną w końcowej części poprzedniego akapitu, stanowiąc jedną z jej szczegółowych kwestii. Opracowując tę metodykę, dokonano przeglądu specjalistycznej literatury z zakresu nauk technicznych i zaadaptowano zawarte w niej wytyczne do realiów czynności kryminalistyczno-procesowych.

---

[3] Tamże, s. 20–30.

[4] A. Kielerz, M. Porzerzyńska-Antonik, *Węgiel w energetyce zawodowej i ciepłownictwie – stan obecny i perspektywy*, „Zeszyty Naukowe Instytutu Gospodarki Surowcami Mineralnymi i Energią PAN" 2019, nr 108, s. 40, 42. https://www.doi.org/10.24425/znigsme.2019.128676; A. Rybak, *Rola i przyszłość węgla w zapewnieniu bezpieczeństwa energetycznego Polski*, Gliwice 2020, s. 29–31, 157. Zob. także: Ministerstwo Aktywów Państwowych, *Program dla sektora górnictwa węgla kamiennego w Polsce* (wersja uwzględniająca korekty z 2022 r.), https://www.gov.pl/web/energia/programu-dla-sektora-gornictwa-wegla-kamiennego-w-polsce [dostęp: 1 VI 2024].

Metodyka opróbowywania na potrzeby postępowania karnego węgla kamiennego przewożonego pojazdami ciężarowymi

Jednym ze znanych praktyce organów ścigania mechanizmów przestępczego działania na szkodę zakładów górniczych jest wywóz z kopalni węgla innego sortymentu lub klasy niż wynikające z dokumentów sprzedaży (tzw. jakościówka lub klasówka). Mechanizm ten bazuje na różnicach cenowych pomiędzy różnymi rodzajami węgla oferowanego do sprzedaży (sortymenty[5]/klasy[6]) oraz na trudnościach ze stwierdzeniem bez odpowiednich przyrządów ewentualnych różnic pomiędzy towarem zakupionym a faktycznie wywożonym transportem kołowym (samochodowym) lub szynowym[7]. Osoby dopuszczające się tego procederu mogą przy tym podejmować działania maskujące, które mają na celu utrudnienie wykrycia niezgodności między dokumentami zakupowymi a rzeczywistym załadunkiem (np. przykrywanie lepszego sortymentu warstwą sortymentu gorszego). Rozróżnienie klas węgla bez przeprowadzenia odpowiednich badań jest zasadniczo niewykonalne. W konsekwencji jest możliwe wywiezienie z kopalni węgla o wyższej wartości rynkowej niż węgiel opłacony. Następnie „lepszy" węgiel jest odsprzedawany dalszym podmiotom po cenach właściwych dla jego rzeczywistego sortymentu/klasy, co generuje wymierne zyski dla osób kierujących taką działalnością.

W tych okolicznościach nie powinno budzić wątpliwości, że w przypadku opisanego mechanizmu kluczowe znaczenie z perspektywy śledczej ma ustalenie jakości węgla, który stał się przedmiotem czynności wykonawczej danego przestępstwa (tj. faktycznej klasy i/lub sortymentu wywiezionego surowca, a w konsekwencji

[5] Podstawą podziału węgla kamiennego na sortymenty jest wielkość uziarnienia (tj. wielkość pojedynczej bryłki węgla). W zależności od wielkości ziaren wyróżnia się m.in. następujące sortymenty węgla: kęsy, kostkę, orzech, groszek, miał oraz muł. Zob. szerzej: PN-82/G-97001 *Węgiel kamienny. Sortymenty.*

[6] Podstawą podziału węgla kamiennego na klasy są jego wartość opałowa (kaloryczność), zawartość popiołu oraz siarki. Zob. szerzej: PN-82/G-97003 *Węgiel kamienny do celów energetycznych.* Poszczególne klasy węgla są oznaczane za pomocą trzyczłonowego symbolu. Np. oznaczenie „28/05/08" wskazuje, że wartość opałowa węgla wynosi 28 MJ/kg (28 000 kJ/kg), zawartość popiołu nie przekracza 5%, a zawartość siarki – 0,8%. Klasa węgla przekłada się bezpośrednio na jego wartość rynkową – im wyższa klasa, tym wyższa cena surowca. W praktyce handlowej klasyfikacja ta często bywa upraszczana i sprowadzana do wartości opałowej. Warto zauważyć, że od wartości opałowej wywodzi się powszechnie stosowane określanie danej partii węgla mianem węgla danej klasy. Np. węgiel o wartości opałowej 24 MJ/kg określa się jako „węgiel klasy 24".

[7] Orientacyjnie można przyjąć, że duży zestaw ciężarowy z naczepą-wywrotką w typowej sytuacji może przewieźć ok. 24–27 ton węgla, w zależności od parametrów pojazdu. Ładowność jednej węglarki to ok. 55 ton, przy czym w skład pociągu wchodzi często ok. 25 węglarek (a zatem łącznie 1375 ton).

także wartości szkody). Na płaszczyźnie wykrywczo-dowodowej[8] ta okoliczność przekłada się na podstawowy problem, jaki może pojawić się w tego rodzaju sprawach, tj. jak prawidłowo pobrać, zabezpieczyć i poddać badaniu próbkę analizowanego surowca, aby uzyskany wynik był miarodajny oraz spełniał wymogi procedury karnej.



A B C D

Zdjęcie 1. Wybrane sortymenty węgla kamiennego – zdjęcia poglądowe: kostka (A), orzech (B), groszek (C), miał II (D).

Źródło: materiały własne (dzięki uprzejmości PGG S.A.).

Do pobierania próbek węgla kamiennego na potrzeby postępowania karnego może dojść w różnych okolicznościach. W tym artykule rozważania ograniczono do jednego przypadku, uznanego przez autora za najbardziej odpowiedni do prezentacji postulowanej metodologii opróbowywania, tj. do procesowego zatrzymania in flagranti domniemanych sprawców wywożących pojazdem kołowym

[8] Pod pojęciem wykrywania, zgodnie z definicją zaproponowaną przez Tadeusza Hanauska, autor rozumie: „ogół działań (poszukiwanie, ujawnienie, stwierdzanie) organów ścigania nastawionych na ujawnienie zdarzenia określanego na danym etapie postępowania jako przestępstwo oraz na uzyskanie informacji pozwalających postawić hipotezę dotyczącą osoby pozostającej w prawnie relewantnej relacji przyczynowej z tym zdarzeniem, a następnie ustalenie danych dotyczących tej osoby (…) i w rezultacie tego jej zabezpieczenie i zebranie wstępnych materiałów uprawdopodobniających hipotezę sprawstwa tej osoby w stopniu uzasadniającym rozpoczęcie udawadniania". Zob. T. Hanausek, *Zarys kryminalistycznej teorii wykrywania. Część I. Pojęcie i przedmiot wykrywania sprawców przestępstw*, Warszawa 1978, s. 45. Pod pojęciem udawadniania należy z kolei rozumieć, co do zasady, kontynuację czynności zapoczątkowanych na etapie wykrywczym, z zastrzeżeniem, że czynności dowodowe powinny dodatkowo spełniać wymogi obowiązującej ustawy procesowej (m.in. uwzględniać zakazy dowodowe). W piśmiennictwie zasadnie wskazuje się, że „udawadnianie najogólniej można określić jako uzasadnianie pewnej hipotezy, którą najczęściej jest hipoteza, że określona osoba jest sprawcą przestępstwa. (…) Skutkiem przeprowadzenia takich czynności jest gromadzenie materiału mającego walory dowodowe, a więc takiego, który pozwala m.in. na uzasadnienie twierdzeń dotyczących: faktu popełnienia danego przestępstwa i jego okoliczności, sposobu działania i motywacji sprawcy, danych odnoszących się do sprawcy". Zob. *Kryminalistyka. Przewodnik*, D. Wilk (red.), Toruń 2013, s. 28.

węgiel z kopalni węgla kamiennego (dalej: KWK), jeszcze przed opuszczeniem jej terenu (np. zatrzymania stanowiącego kulminację rozpracowania operacyjnego)[9]. Zastosowanie w tego typu sytuacjach znajduje instytucja tzw. postępowania w niezbędnym zakresie (o ile dotychczas w sprawie nie wszczęto śledztwa/dochodzenia), o której mowa w art. 308 § 1 Kodeksu postępowania karnego (dalej: k.p.k.)[10]. Spełniona jest bowiem jej podstawowa przesłanka w postaci realnej obawy utraty dowodów przestępstwa. Pobieranie próbek węgla w takich okolicznościach to nic innego jak część oględzin (por. art. 207 § 2 k.p.k.), a więc czynności expressis verbis dopuszczalnej na gruncie przywołanego art. 308 § 1 k.p.k. Oględziny, podczas których planuje się opróbowanie danej partii (transportu) węgla, mogą – jak każde inne oględziny – przybrać formę tzw. oględzin prostych (bez udziału biegłego) lub tzw. oględzin złożonych[11] (z udziałem biegłego[12]), przy czym udział biegłego nie wydaje się w tym przypadku uzasadniony i nie jest konieczny do pobrania próbki węgla[13]. W świetle obowiązujących przepisów brakuje normy, która stałaby na przeszkodzie, aby opróbowania dokonał organ prowadzący czynności, tzn. funkcjonariusz lub prokurator kierujący czynnościami. Organ powinien się jednak wzbraniać od samodzielnego opróbowywania węgla, jeśli nie ma w tym zakresie stosownego

[9] Należy podkreślić znaczenie wczesnego pobrania próbek węgla, tj. jeszcze na terenie KWK, bezpośrednio po opuszczeniu jej terenu przez pojazd transportujący węgiel lub – w przypadku niejawnego nadzorowania trasy przewozu – tak długo, jak utrzymywany jest stały nadzór nad ładunkiem. Jeżeli węgiel nie zostanie opróbowany na etapie zapewniającym możliwość wykazania, że badany materiał pozostaje tożsamy z surowcem wydanym w ramach konkretnej transakcji (tj. m.in. bez ryzyka jego wymieszania z węglem innego pochodzenia lub podmiany), to wartość dowodowa badań laboratoryjnych próbki pobranej w późniejszym czasie się zmniejsza.

[10] *Ustawa z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego*.

[11] *Kryminalistyka. Przewodnik…*, s. 107.

[12] Analiza list biegłych z lokalnych sądów okręgowych (tj. SO Katowice, SO Gliwice, SO Rybnik – stan na 31 XII 2023 r.) podaje w wątpliwość, czy biegli wskazani tam pod hasłami „górnictwo" (i zbliżonymi) mają wiadomości specjalne w zakresie istotnym dla opróbowywania węgla kamiennego. Można to porównać do następującej sytuacji na gruncie nauk prawnych: nie każdy prawnik w sposób szczególny zna się na zagadnieniach związanych z międzynarodowym prawem humanitarnym konfliktów zbrojnych. Doświadczenie życiowe wskazuje, że jest to stosunkowo niszowa wiedza wśród prawników, zwłaszcza w porównaniu z takimi dziedzinami prawa jak proces karny i cywilny. W przypadku chęci skorzystania z pomocy biegłego przy pobieraniu próbek węgla celowe wydaje się zatem uprzednie ustalenie (np. telefoniczne), czy biegły ma wiadomości specjalne także w tym zakresie. Na uwagę zasługuje również rozważenie zastosowania w takiej sytuacji instytucji biegłego ad hoc, spośród osób, które naukowo zajmują się problematyką przeróbki węgla kamiennego, np. w ramach Głównego Instytutu Górnictwa – Państwowego Instytutu Badawczego w Katowicach.

[13] Do analogicznych wniosków judykatura doszła na kanwie śladów osmologicznych. Por. np. wyrok Sądu Najwyższego (dalej: SN) z 5 XI 1999 r., sygn. V KKN 440/99, LEX nr 38328.

przeszkolenia, i oddać tę czynność w ręce odpowiednio dobranych specjalistów[14]. Trafnie zauważa się bowiem w literaturze, że należy jednoznacznie odróżnić pojęcie wiedzy specjalnej w rozumieniu art. 193 § 1 k.p.k. od wiedzy stricte technicznej, pomocnej przy prawidłowym wykonywaniu konkretnych czynności dowodowych[15]. Judykatura słusznie podkreśla, że na gruncie k.p.k. specjalista jest w istocie pomocnikiem organu procesowego – umiejętności i techniczne know-how specjalisty pozwalają na rzetelną realizację czynności leżących w gestii samego organu[16]. Analiza charakteru opróbowywania prowadzi z kolei do konkluzji, że jest to czynność techniczna, którą można porównać do pobierania wymazówką śladów krwi z przedmiotu znalezionego na miejscu zabójstwa czy też zabezpieczania śladów linii papilarnych ujawnionych na miejscu kradzieży. Tak jak dopiero ekspertyza genetyczna czy ekspertyza daktyloskopijna (a nie pobieranie i zabezpieczenie śladów do tych badań) stanowią przedmiot opinii biegłego, tak dopiero badanie laboratoryjne pobranej próbki węgla stanowi czynność pozostającą w gestii biegłego. Szczególnie istotne jest, aby specjalista dokonujący opróbowania – jeśli ma być ono miarodajne – był dobrze zaznajomiony z metodyką ręcznego pobierania próbek węgla kamiennego. Nie może budzić wątpliwości teza, że modelowo taka osoba powinna mieć zarówno przeszkolenie teoretyczne w tym zakresie (np. ukończony „Kurs dla próbobiorców w zakresie obowiązujących norm technicznych PN i ISO" organizowany przez Główny Instytut Górnictwa – Państwowy Instytut Badawczy w Katowicach[17]), jak i doświadczenie praktyczne. Tym samym standardowy technik kryminalistyki nie wydaje się właściwą osobą do pobierania takich próbek. W związku z tym, jeśli organ nie dysponuje osobami odpowiednio przeszkolonymi w omawianym zakresie, warto rozważyć wezwanie ad hoc uprzednio ustalonej osoby do wykonania tych czynności (art. 15 § 3 k.p.k. w związku z art. 205 § 1 k.p.k.).

W dalszej części artykułu zostanie przedstawiona postulowana metodyka ręcznego pobierania na potrzeby śledcze próbek węgla kamiennego przewożonego

---

[14] Formalnie brak takiego wymogu (art. 205 § 1 k.p.k. nie obliguje organu do skorzystania z pomocy specjalistów). Należy jednak unikać pobierania próbek węgla przez osoby nieposiadające przeszkolenia w tym zakresie, gdyż w przeciwnym wypadku wartość dowodowa wyników badań laboratoryjnych uzyskanych z tak pobranych próbek węgla może budzić uzasadnione wątpliwości.

[15] Por. m.in. J. Kasprzak, *Biegły i specjalista przed sądem – wybrane aspekty taktyczne*, Warszawa 2001, s. 15; *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2023, komentarz do art. 205 k.p.k.; *Kodeks postępowania karnego. Tom II: Komentarz do art. 167–296*, R.A. Stefański, S. Zabłocki (red.), Warszawa 2019, s. 627 i nast.

[16] Zob. wyrok SN z 3 XI 2021 r., sygn. V KK 460/20, LEX nr 3342210.

[17] Kurs obejmuje sześć godzin wykładowych i kosztuje 890 zł (stan na 31 XII 2023 r.). Zob. *Kurs dla próbobiorców w zakresie obowiązujących norm technicznych PN i ISO*, Główny Instytut Górnictwa – Centrum Rozwoju Kompetencji, http://szkolenia.gig.eu/wydarzenie/kurs-dla-probobiorcow-w-zakresie-obowiazujacych-norm-technicznych-pn-i-iso/ [dostęp: 31 XII 2023].

transportem samochodowym. Na początek – jako swoisty lejtmotyw – warto przywołać trafne spostrzeżenie Juty Olszówki oraz Bronisława Paula:

> (…) w przypadku węgla, który stanowi materiał o dużym stopniu niejednorodności, wyrażającym się różnorodnością cech fizykochemicznych i petrograficznych, zmiennością składu ziarnowego oraz zawartością substancji mineralnej i wilgoci – właściwe pobierane próbek i ich przygotowanie jest zadaniem trudnym i odpowiedzialnym. Pobrana z określonej partii węgla próbka powinna swoimi własnościami [właściwościami – przypis K. L.] odpowiadać średnim własnościom badanej partii. Próbka nieprzedstawiająca średnich własności badanej partii w granicach dozwolonego błędu daje wyniki niewłaściwe, prowadzące do błędnych wniosków. Dlatego też próbki powinny być pobierane według pewnych zasad, z dużą starannością, tym bardziej, że na ogół pobierane są jednorazowo bez możliwości ich powtórzenia (…). Dokładność i miarodajność pobranych próbek zależą od tego, czy wszystkie czynności zostały wykonane zgodnie z opracowaną przez Polskie Normy metodyką pracy oraz od sumienności, staranności i kwalifikacji osób zatrudnionych przy pobieraniu i przygotowywaniu próbek[18].

Szacuje się, że wpływ etapu pobierania próbek na całkowity błąd analizy (ang. *total error*)[19] może wynosić nawet 80%[20]. Pobieranie próbek węgla powinno odbywać się zatem z najwyższą starannością. Węgiel określa się przy tym jako jeden z materiałów najtrudniejszych do opróbowania, a pobranie próbki węgla stanowiącej idealne odwzorowanie badanej partii uznaje się de facto za niemożliwe. Stosując się jednak ściśle do metodologii opracowanej przez nauki techniczne, można zminimalizować do akceptowalnego poziomu ryzyko pobrania niereprezentatywnych próbek[21]. Innymi słowy, opróbowanie nie ma na celu precyzyjnego ustalenia parametrów danej partii, lecz ich wiarygodne oszacowanie[22] (ustalenie precyzyjnych

[18] J. Olszówka, B. Paul, *Zasady kontroli jakości węgla*, Katowice 1972, s. 68.

[19] Przez błąd całkowity należy rozumieć sumę błędów losowych i systematycznych, poczynając od etapu pobierania próbki, przez jej przygotowanie, kończąc na jej ostatecznej analizie w laboratorium. Wyniki nawet najbardziej starannego opróbowania mogą na każdym z tych etapów zostać obarczone błędem. Zob. W.B. Membrey, *Coal samping*, w: *The Coal Handbook. Volume 1: Towards Cleaner Coal Supply Chains*, D. Osborne (red.), San Diego 2023, s. 108; *Metodyka dokumentowania złóż kopalin stałych. Część III: Opróbowanie złóż kopalin*, M. Nieć (red.), Kraków 2012, tabela 7.1., s. 91.

[20] Z. Qian, *Coal sampling and analysis standards*, London 2014, s. 18, 46; M. Mastelarz, *Dlaczego kluczowym etapem analizy paliwa jest odpowiednie pobranie próbek?*, Instytut Technologii Paliw i Energii, www.itpe.pl/blog/2021/09/08/dlaczego-kluczowym-etapem-analizy-paliwa-jest-odpowiednie-pobranie-probek/ [dostęp: 31 XII 2023]. Aktualnie strona nie jest dostępna (dop. red.).

[21] Z. Qian, *Coal sampling…*, s. 18.

[22] W.B. Membrey, *Coal sampling…*, s. 107.

parametrów danej partii byłoby możliwe wyłącznie po jej całościowym przebadaniu, co z przyczyn techniczno-ekonomicznych nie jest praktykowane).

Przeprowadzona przez autora analiza dostępnych baz danych[23] nie wykazała, aby istniała opublikowana, ściśle kryminalistyczna metodologia pobierania i zabezpieczania próbek węgla kamiennego opracowana na potrzeby procesu karnego. Nie jest to zaskakujące ze względu na niszowy charakter omawianej problematyki. Tym samym zasadne wydaje się wykorzystanie ogólnej metodologii opróbowywania węgla kamiennego wypracowanej w naukach technicznych, z uwzględnieniem dodatkowych wymogów wynikających ze specyfiki postępowania karnego.

Kluczowymi dokumentami regulującymi metodologię pobierania próbek węgla kamiennego w Polsce są dwie Polskie Normy[24]: PN-ISO 18283:2008 *Węgiel kamienny i koks. Ręczne pobieranie próbek*[25] oraz PN-G-04502:2014-11 *Węgiel kamienny i brunatny. Pobieranie i przygotowanie próbek do badań laboratoryjnych. Metody podstawowe*. Bazowanie na tych normach jest zalecane, gdyż harmonizuje z nimi metodologia pracy akredytowanych[26] laboratoriów analitycznych działających w Polsce. Normy te opracowano na podstawie teorii statystycznej kontroli jakości, rachunku prawdopodobieństwa oraz teorii błędów[27]. Z punktu widzenia praktyki druga z wymienionych norm wydaje się istotniejsza, ponieważ stanowi uszczegółowienie pierwszej i krok po kroku opisuje postulowaną metodologię pobierania próbek węgla z poszczególnych lokalizacji (m.in. z przenośnika taśmowego, zwału, wagonu kolejowego oraz samochodu ciężarowego)[28].

---

[23] Google, Google Scholar, Google Books, EBSCO Discovery Service (w ramach dostępu Biblioteki Jagiellońskiej). Hasła wyszukiwania były podawane w języku polskim, angielskim, niemieckim, rosyjskim oraz ukraińskim.

[24] Polskie Normy to dokumenty przyjęte na zasadzie konsensu, ustalające zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzające do uzyskania optymalnego stopnia uporządkowania w określonym zakresie. Za ich przygotowanie odpowiada Polski Komitet Normalizacyjny. Poszczególne normy oznacza się skrótem PN i dalszą częścią wskazującą na konkretną normę i rok jej wprowadzenia. Zob. *Co to jest PN?*, Polski Komitet Normalizacyjny, http://www.pkn.pl/polskie-normy/informacje-o-pn/co-jest-pn [dostęp: 31 XII 2023]; *Ustawa z dnia 12 września 2002 r. o normalizacji*.

[25] Norma ta jest ścisłym tłumaczeniem anglojęzycznej Normy Międzynarodowej ISO 18283:2006. Aktualna wersja międzynarodowa ISO 18283:2022 jest z 2022 r. (na 31 XII 2023 r. PN-ISO 18283:2008 nie została zaktualizowana).

[26] Jedynym organem akredytacyjnym w Polsce jest Polskie Centrum Akredytacji. Działa ono na podstawie przepisów *Ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku*.

[27] J. Olszówka, B. Paul, *Zasady kontroli jakości*…, s. 69; W.B. Membrey, *Coal sampling*…, s. 107–109.

[28] Normy te są ze sobą spójne. Na temat relacji tych norm zob. szerzej: M. Mastelarz, *Polskie normy dotyczące ręcznego pobierania próbek węgla kamiennego*, Instytut Technologii Paliw i Energii, 9 X 2023 r., https://itpe.pl/polskie-normy-dotyczace-recznego-pobierania-probek-wegla-kamiennego/ [dostęp: 31 XII 2023].

Analiza przywołanych norm, przeprowadzona w świetle ogólnych reguł kryminalistyki, pozwala na sformułowanie następujących podstawowych wytycznych[29] w zakresie prawidłowego opróbowywania dla potrzeb śledczych węgla kamiennego załadowanego na samochód ciężarowy:

- zatrzymany samochód powinien, co do zasady, zostać rozładowany, tj. należy unikać pobierania próbek węgla z załadowanego samochodu. Podstawowe założenie teorii opróbowywania stanowi, że pobranie każdego ziarna opróbowywanej partii jest równie prawdopodobne. W przypadku ręcznego opróbowywania węgla, zwłaszcza znajdującego się w naczepie samochodu ciężarowego, praktycznej realizacji rzeczonego założenia daleko do ideału[30]. Trudno bowiem uznać, że prawdopodobieństwo pobrania ziarna z dna naczepy o głębokości ok. 2 m jest takie samo jak ziaren znajdujących się bliżej powierzchni, przy znacznie ograniczonym dostępie do dna. W takich okolicznościach ryzyko pobrania niereprezentatywnej próbki jest dodatkowo potęgowane przez zjawisko segregacji ziaren wynikające z praw fizyki[31] oraz przez ewentualne oddziaływania atmosferyczne podczas transportu. Aby temu przeciwdziałać, teoria opróbowywania zaleca rozładowanie samochodu i pobranie próbek z powstałej pryzmy. W takich okolicznościach nadal istnieje ryzyko pobrania niereprezentatywnej próbki, ale zostaje ono zminimalizowane[32]. Co więcej, mechanizm przestępczego działania może polegać

[29] Autor tego artykułu nie rości sobie prawa do szczegółowego omówienia prawidłowej metodologii opróbowywania węgla kamiennego, gdyż kwestia ta wymaga odpowiedniego wykształcenia w zakresie nauk technicznych. Autor, z wykształcenia prawnik, stoi na stanowisku, że celem kryminalistycznego kształcenia prawników nie jest przekształcenie ich w quasilekarzy, quasichemików czy quasifizyków – co zasadniczo wymagałoby gruntownego wykształcenia kierunkowego, aby ograniczyć ryzyko formułowania twierdzeń pseudonaukowych – lecz stworzenie swoistego pomostu, który umożliwia praktykowi prawa (sędziemu, prokuratorowi, adwokatowi, radcy prawnemu czy policjantowi) zarówno nawiązywanie rzeczowego dialogu z biegłymi w danej dziedzinie, w tym zadawanie im odpowiednio merytorycznych pytań oraz kontrolowanie udzielanych odpowiedzi, jak i prowadzenie czynności procesowych w sposób ograniczający ryzyko popełnienia błędów niemożliwych do naprawienia (ten aspekt dotyczy głównie organów procesowych, adwokaci oraz radcy prawni powinni natomiast być przygotowani do identyfikowania potencjalnych uchybień w sposobie procedowania organów procesowych i do reagowania na te uchybienia).

[30] W literaturze przyjmuje się, że należy unikać ręcznego pobierania próbek. Aby zminimalizować ryzyko błędów, w tym ludzkich, zaleca się – jeśli to możliwe – stosowanie mechanicznego opróbowywania węgla, najlepiej na taśmociągu za pomocą automatycznego próbobiornika. W przypadkach rozważanych w tym artykule opróbowywanie mechaniczne nie jest jednak praktykowane z uwagi na ich specyfikę. Zob. Z. Qian, *Coal sampling*…, s. 29.

[31] W. Wawrzynkiewicz, L. Róg, K. Hamala, *Dokładność pobierania próbek paliw stałych za pomocą urządzeń mechanicznych*, „Przegląd Górniczy" 2005, t. 61, nr 11, s. 25.

[32] PN-ISO 18283:2008, s. 35.

na tym, że „lepszy" węgiel zostanie przykryty „gorszym". W tym przypadku rozładowanie pojazdu prowadzi do choć częściowego ich wymieszania. Z praktycznego punktu widzenia warto nadto zauważyć, że zgodnie z § 105 ust. 1 *Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy* pracą na wysokości jest praca wykonywana na powierzchni znajdującej się na wysokości co najmniej 1 m nad poziomem ziemi. Wysokość załadowanej naczepy/skrzyni ładunkowej wywrotki przekracza tę wysokość, co oznacza, że pobieranie próbek węgla bezpośrednio z załadowanego samochodu stanowiłoby pracę na wysokości w rozumieniu przywołanych przepisów i wymagałoby stosownego zabezpieczenia.

Jeśli analizowane czynności są przeprowadzane na terenie KWK, to prowadzący je powinien, co do zasady, skonsultować z przedstawicielem kopalni miejsce rozładunku. Miejsce to powinno być pustą, utwardzoną powierzchnią płaską, która uniemożliwia mieszanie się rozładowanego węgla z podłożem. Celowe wydaje się sporządzenie stosownej dokumentacji fotograficznej pojazdu przed jego rozładowaniem, miejsca wybranego na rozładunek (przed jego dokonaniem) oraz pryzmy węgla powstałej w wyniku rozładunku. Dokumentacja ta może mieć istotne znaczenie na etapie sądowym sprawy, m.in. w przypadku przyjęcia linii obrony polegającej na kwestionowaniu prawidłowości opróbowania. Przed rozładowaniem pojazd powinien zostać kontrolnie zważony, przy czym ważenie kontrolne – jeśli to możliwe – należy przeprowadzić na innej wadze niż ta, na której dokonano pierwotnego ważenia (skoro następuje rozładunek, to jest to ostatni moment na pomiar masy zakwestionowanego pojazdu w dokładnie takim stanie, w jakim opuścił on teren kopalni). Ważenie na innej wadze ma na celu wykluczenie ewentualnego błędu pomiaru spowodowanego uszkodzeniem wagi lub nieuprawnioną ingerencją w jej odczyty;

- na pryzmie węgla powstałej w wyniku rozładowania samochodu należy wyznaczyć równomiernie 32 punkty pobrań, a następnie pobrać z nich 32 tzw. próbki pierwotne. Jeśli to możliwe, miejsca pobrań należy oznaczyć za pomocą znaczników i sfotografować. Próbki należy pobierać szuflą lub łopatą (narzędzia te powinny mieć szerokość co najmniej trzy razy większą od wymiaru największego ziarna w opróbowywanej partii[33]) z dołków pionowo wykopanych w wyznaczonych punktach. Istotne jest, aby dołki miały

[33] PN-ISO 18283:2008, s. 32. Wielkość największego ziarna należy ustalić na podstawie deklarowanego sortymentu, a w razie wątpliwości przyjąć wymiary odpowiednio większe. Minimalna szerokość to 30 mm.

różną głębokość – jednak niemniej niż 0,4 m. Minimalna masa pojedynczej próbki pierwotnej jest związana z wielkością największego ziarna węgla w opróbowywanej partii. Masę próbki pierwotnej (m) oblicza się według następującego wzoru: m = 0,06 × D, gdzie „D" to wielkość największego ziarna w badanej partii wyrażona w milimetrach. Jako wielkość największego ziarna w badanej partii należy przyjąć wielkość największego ziarna dla danego sortymentu według normy PN-82/G-97001 *Węgiel kamienny. Sortymenty*. Masa próbki pierwotnej nie może być jednak mniejsza niż 0,5 kg[34] (tabela 1).

Tabela 1. Minimalna masa próbki pierwotnej.

Wielkość największego ziarna w opróbowywanej partii (mm)	Minimalna masa próbki pierwotnej (kg)
200,0	12,0
125,0	7,5
80,0	4,8
50,0	3,0
31,5	1,9
20,0	1,2
10,0	0,6

Źródło: opracowanie własne na podstawie: PN-G-04502:2014-11 *Węgiel kamienny i brunatny. Pobieranie i przygotowanie próbek do badań laboratoryjnych. Metody podstawowe*.

Przykładowo, jeśli opróbowywaniu podlega partia znajdującego się w ofercie Polskiej Grupy Górniczej S.A. miału o nazwie handlowej GreenPal Miał Plus, tj. produktu o uziarnieniu 3–20 mm, to każda z 32 próbek pierwotnych powinna mieć masę minimum 1,2 kg. Należy zauważyć, że jest to masa minimalna, a nie maksymalna – istotne jest, aby każda z 32 próbek pierwotnych miała taką samą (lub jak najbardziej zbliżoną) masę. W praktyce przemysłowej próbobiorcy, co do zasady, nie prowadzą szczegółowego ważenia próbek pierwotnych i pobierają je orientacyjnie, np. posiłkując się objętością pobieranych próbek. Dla opróbowywania na cele procesowe, z daleko posuniętej ostrożności, należy zalecić zważenie co najmniej jednej z próbek pierwotnych, aby ustalić jej masę – tj. jeśli próbki pierwotne

[34] PN-G-04502:2014-11, s. 11.

pobiera się za pomocą miary szufli/łopaty (jedna szufla/łopata = jedna próbka pierwotna), to należałoby przynajmniej jedną taką próbkę zważyć, aby chociaż szacunkowo znać masę pobranych próbek pierwotnych;

- pobrane próbki pierwotne należy następnie połączyć – w ten sposób powstaje tzw. próbka ogólna. Zgodnie z metodologią opisaną w przywołanych Polskich Normach próbka ta podlega dalszym zabiegom, w wyniku których otrzymuje się próbkę laboratoryjną, a z niej – próbkę analityczną. Norma PN-G-04502:2014-11 stanowi, że próbkę laboratoryjną należy przygotować w miarę możliwości bezpośrednio po pobraniu próbki ogólnej[35]. Wydaje się jednak, że w przypadku opróbowywania partii węgla na potrzeby procesu karnego wskazane jest zakończenie prac zespołu oględzinowego na etapie sporządzenia próbki ogólnej, a następnie jej odpowiednie zabezpieczenie i przesłanie do laboratorium w celu przeprowadzenia stosownych badań w ramach opinii biegłego. W ten sposób zmniejsza się ryzyko ewentualnych błędów podczas czynności koniecznych do przygotowania próbek laboratoryjnych lub analitycznych (tzw. pomniejszanie oraz rozdrabianie[36]), co jawi się jako szczególnie istotne, skoro zabezpieczony materiał może stanowić newralgiczny dowód w sprawie. Postulowane zakończenie prac na etapie otrzymania próbki ogólnej nie wydaje się przy tym nadmiernie uciążliwe z perspektywy logistycznej. W przypadku miału próbka ogólna powinna ważyć ok. 38,4 kg (1,2 kg × 32 = 38,4 kg), a w przypadku groszku – ok. 60,8 kg (1,9 kg × 32 = 60,8 kg). Przekłada się to odpowiednio na dwa oraz trzy worki węgla[37]. Dla sortymentów grubych (kostka oraz orzech) podejście to wydaje się o tyle trudne do zrealizowania, że próbka ogólna ma zauważalnie większą masę (ok. 153,6 kg w przypadku orzecha oraz ok. 384 kg w przypadku kostki). W takich sytuacjach celowe wydaje się pomniejszenie próbki ogólnej bezpośrednio po jej przygotowaniu. Pomniejszanie to może odbywać się za pomocą specjalnego urządzenia (tzw. rozdzielaczem próbek typu Jones) lub ręcznie (tzw. kwartowanie). Kwartowanie polega na: a) usypaniu stożka węgla (z próbki ogólnej) – węgiel należy sypać na wierzch stożka, aby ziarna zsypywały się równomiernie po jego zboczu

[35] Tamże.

[36] Norma PN-ISO 18283:2008 stosuje ścisłe rozróżnienie terminologiczne pomiędzy podziałem próbki (zgodnie z punktem 3.24 ww. normy jest to „jeden z procesów przygotowywania próbki polegający na jej podziale na reprezentatywne oddzielne porcje") a rozdrabnianiem próbki (zgodnie z punktem 3.26 ww. normy jest to „jeden z procesów przygotowywania próbki, podczas którego wielkość ziaren jest zmniejszana poprzez kruszenie lub mielenie").

[37] Standardowy worek, w którym w PGG S.A. jest sprzedawany konfekcjonowany węgiel, np. Ekogroszek Karlik, ma pojemność 20 kg.

i aby wierzchołek nie przesuwał się na boki; b) rozpłaszczeniu stożka; c) podzieleniu rozpłaszczonego stożka na cztery równe części; d) połączeniu ze sobą dwóch przeciwległych ćwiartek; e) odrzuceniu jednej z otrzymanych w ten sposób mas – druga stanowi masę docelową. Gdy jest to konieczne, procedura kwartowania powinna zostać powtórzona, aż do uzyskania pożądanej masy próbki. Zalecaną metodą pomniejszania jest metoda mechaniczna, gdyż ogranicza ryzyko błędów ludzkich[38]. Z perspektywy problematyki niniejszego artykułu należy ponownie zalecić zakończenie prac zespołu oględzinowego na etapie pomniejszania, a przed etapem rozdrabiania i przekazanie próbki w takim stanie do badań (laboratorium rozdrobni węgiel we własnym zakresie). Jeśli prowadzący czynności uzna jednak, że zasadne jest rozdrobnienie próbki na miejscu, to za pomocą specjalnego urządzenia, tzw. kruszarki, należy ją rozdrobnić do ziaren o frakcji 3 mm[39]. Uzyskana masa może podlegać dalszemu pomniejszaniu według opisanych powyżej zasad, przy czym próbka przekazana do laboratorium powinna mieć masę minimum 2 kg[40]. Na tym etapie prac zespołu oględzinowego należy ponadto rozważyć przeprowadzenie tzw. analizy sitowej, która wydaje się niezbędna w dwóch przypadkach: po pierwsze, gdy podejrzewa się wywóz innego sortymentu niż deklarowany, a po drugie, gdy brak jest w ogóle informacji co do sortymentu zakwestionowanej partii (np. wykryto nielegalny wywóz węgla z terenu KWK X i należy ustalić zarówno klasę, jak i sortyment węgla, który był przedmiotem takiego wywozu). Do celów analizy sitowej można wykorzystać odrzuconą część próbki ogólnej. Analiza ta polega na przesiewaniu badanej partii węgla przez sita o różnych otworach (np. 5 mm, 10 mm, 20 mm, 30 mm, 40 mm itd.), co pozwala na ustalenie klasy ziarnowej badanej próbki, tj. jej sortymentu[41];

- przygotowana próbka powinna następnie zostać zabezpieczona w plastikowym pojemniku lub worku. Jeśli planowane jest przeprowadzanie badań w zakresie wilgoci (w przypadku prowadzenia czynności w kierunku ewentualnego oszustwa klasowego jest to konieczne), to opakowanie powinno być szczelne i wykonane z materiału nieulegającego korozji oraz niezmieniającego właściwości próbki[42]. Do tak pobranej i zabezpieczonej próbki należy

[38] PN-G-04502:2014-11, s. 12–13.

[39] Można również rozdrabianiać ręcznie, za pomocą ubijaków. Nie jest to jednak zalecane.

[40] PN-G-04502:2014-11, s. 13.

[41] Analizie sitowej jest poświęcona odrębna Polska Norma – PN-ISO 1953:1999 *Węgiel kamienny. Analiza ziarnowa metodą przesiewania.*

[42] PN-G-04502:2014-11, s. 13–14.

dołączyć metryczkę, na której powinny się znaleźć co najmniej: data pobrania próbki, dane próbobiorcy, masa próbki, typ i sortyment węgla, masa partii, z której pobrano próbkę, a także standardowe dane wpisywane na metryczkę podczas zabezpieczania śladów, tj. oznaczenie organu dokonującego oględzin, przedmiotu oględzin, ich miejsca, numeru śladu oraz podpisy próbobiorcy i przedstawiciela organu prowadzącego czynności[43].


A B C

Zdjęcie 2. Opróbowywanie węgla kamiennego – zdjęcia poglądowe: pobieranie próbek pierwotnych (A), kwartowanie (B), zestaw sit do analizy sitowej (C).

Źródło: materiały własne (dzięki uprzejmości PGG S.A.).

Pobranie i następujące po nim zabezpieczenie pobranej próbki węgla powinno zostać szczegółowo opisane w protokole oględzin. Należy zalecić jak najbardziej szczegółowy opis przeprowadzonych czynności, aby biegły opiniujący w sprawie mógł ex post dokonać kontroli prawidłowości przebiegu opróbowywania. Ze względu na wagę ww. czynności i ich niepowtarzalny charakter należy postulować ponadto pełną rejestrację ich przebiegu za pomocą urządzenia rejestrującego obraz (vide art. 147 § 1 k.p.k.). Jeśli taka rejestracja z przyczyn technicznych nie jest możliwa, to należy zapewnić co najmniej dokumentację fotograficzną miejsc pobrania próbek. Czynność ta nie wymaga nadmiernego wysiłku, a w sposób istotny może zarówno chronić prawidłowe opróbowanie przed ewentualnymi późniejszymi zarzutami jego tendencyjności, jak i pozwolić na wykrycie nieprawidłowości na rozpatrywanym etapie, w tym tzw. błędów grubych[44]. Niezależnie od powyższego

[43] J. Kasprzak, *Oględziny osoby, miejsca i rzeczy*, w: *System Prawa Karnego Procesowego. Tom VIII. Dowody. Cz. 4*, P. Hofmański (red.), Warszawa 2019, s. 5154.

[44] Błąd gruby zachodzi, gdy różnica pomiędzy wynikiem pomiaru a wartością rzeczywistą jest znaczna. Błędy tego typu są związane, co do zasady, z czynnikiem ludzkim (brak wymaganych umiejętności u dokonującego pomiaru, błędy przy zapisywaniu wyników itd.). Błąd ten można określić mianem błędu rażącego.

należy zadbać, aby w protokole zostały zawarte informacje dotyczące stanu (wyglądu) załadunku samochodu przed jego rozładowaniem (tj. czy widoczna powierzchnia załadowanego węgla była mokra, czy samochód przeciekał itp.), warunków atmosferycznych panujących podczas przeprowadzania oględzin, a także wizualnego stanu rozładowanego surowca. Kwestie te mogą zostać precyzyjnie opisane po zasięgnięciu opinii próbobiorców, którzy z założenia powinni posługiwać się fachową terminologią. Zapewnia ona – jak słusznie zauważa Józef Gurgul – komunikatywność protokołu, która jawi się jako szczególnie ważna m.in. dla biegłego mogącego opiniować w sprawie na dalszym etapie[45]. W szczególności warto zauważyć, że informacje zawarte w protokole mogą się okazać istotne dla ewentualnych wyliczeń biegłego ukierunkowanych na ustalenie, czy dana partia węgla mogła zmienić swoje właściwości podczas transportu (dotyczy to głównie sytuacji, gdy transport węgla został zatrzymany po upływie pewnego czasu od jego załadunku, jednak należy liczyć się z możliwością, że taki zarzut pojawi się również w przypadku pobrania próbek niedługo po załadowaniu, tj. jeszcze na terenie danej KWK)[46]. Zgodnie z wymaganiami art. 205 § 3 k.p.k. w protokole należy obligatoryjnie zawrzeć także dane osobowe próbobiorców. Jeśli było ich co najmniej dwóch lub jeśli próbobiorcy pomagał specjalista-funkcjonariusz organu ścigania (lub sam kierujący czynnościami organ, np. prokurator, czego nie można wykluczyć), to w protokole powinno znaleźć się szczegółowe opisanie podziału ról tych osób w czynnościach związanych z poborem próbek (np. X – pobór próbek pierwotnych nr 1–16; Y – pobór próbek pierwotnych nr 16–32; Z – przytrzymywanie worka podczas zabezpieczania próbki ogólnej). Dane te, jak słusznie zauważa się w piśmiennictwie, mogą następnie posłużyć do dotarcia do osób, które w razie wątpliwości co do prawidłowości dokonanego opróbowania mogą zostać przesłuchane w charakterze świadków (vide art. 205 § 3 k.p.k.)[47]. O ile doświadczenie życiowe oraz wiedza o ludzkiej pamięci[48] uczą,

[45] J. Gurgul, *Instytucja specjalisty w procesie karnym*, „Prokuratura i Prawo" 1998, nr 11–12, s. 121. Warto również zwrócić uwagę na trafne zapatrywanie Sądu Apelacyjnego w Lublinie odnośnie do znaczenia należytego pobrania i odpowiedniego zabezpieczenia materiału dowodowego w perspektywie jakości późniejszej opinii biegłego. Zostało ono wyrażone w wyroku tego sądu z 29 IX 1998 r., sygn. II AKa 142/97, LEX nr 37066 (rozważania przedmiotowego orzeczenia dotyczą bezpośrednio ekspertyzy osmologicznej, ale należy stanąć na stanowisku, że w analizowanym zakresie zachodzi pełna analogia).

[46] Tego rodzaju ustalenia wymagają każdorazowo szczegółowej analizy m.in. trasy danego transportu oraz warunków atmosferycznych panujących w jego trakcie i w sposób ścisły należą do kompetencji biegłych.

[47] *Kodeks postępowania karnego. Komentarz. Tom I: Art. 1–424*, D. Świecki (red.), Warszawa 2024, s. 753.

[48] Błędy pamięci dotyczące danych wspomnień – ogólnie rzecz ujmując – z biegiem czasu wzrastają. Są one wpisane w naturę ludzkiego postrzegania i pamięci, która – jak wskazują liczne badania – stopniowo staje się coraz bardziej podatna na różne zakłamania. Pod wpływem czasu pewna część materiału ulega zapomnieniu, a pojawiające się luki są często niejako automatycznie i nieświadomie uzupełniane bądź

że osoby te po upływie pewnego czasu od rozpatrywanych czynności mogą nie pamiętać ich szczegółów (co więcej – jeżeli twierdzą, że szczegóły te pamiętają, to do tego rodzaju zeznań należy podejść z dużą dozą ostrożności), o tyle podczas przesłuchania powinno się dążyć co najmniej do ustalenia, czy osoby te były zaznajomione z prawidłową metodyką opróbowywania. Wydaje się to – jak już wskazano – podstawowym zabezpieczeniem prawidłowego przebiegu tej czynności[49].

Równocześnie należy uznać, że w świetle aktualnego stanu prawnego naruszenie właściwej metodologii opróbowywania węgla nie skutkuje pozbawieniem wartości dowodowej tak pobranej próbki (i jej następczej analizy laboratoryjnej) per se. Innymi słowy, brak jest automatyzmu pomiędzy wadliwym pobraniem próbek a wykluczeniem uzyskanych w jej następstwie wyników badań laboratoryjnych z materiału dowodowego zgromadzonego w danej sprawie. Wszelkie uchybienia wykryte w przebiegu opróbowywania powinny zostać – w świetle dyrektyw art. 7 k.p.k. – każdorazowo wnikliwie przeanalizowane przez organ prowadzący daną sprawę oraz uwzględnione przy ocenie wartości dowodowej wyników końcowego badania laboratoryjnego węgla. W tym zakresie zasadne wydaje się zasięgnięcie opinii biegłego w celu weryfikacji prawidłowości przebiegu pobierania próbek, skali ewentualnych uchybień wówczas popełnionych oraz ich potencjalnego wpływu na otrzymany wynik badań laboratoryjnych[50]. Warto zauważyć, że analogiczne poglądy judykatura wyrażała dotychczas w kwestii skutków uchybień, które zaistniały podczas czynności procesowej okazania[51], a brak jest uzasadnionych podstaw do różnicowania tych sytuacji.

---

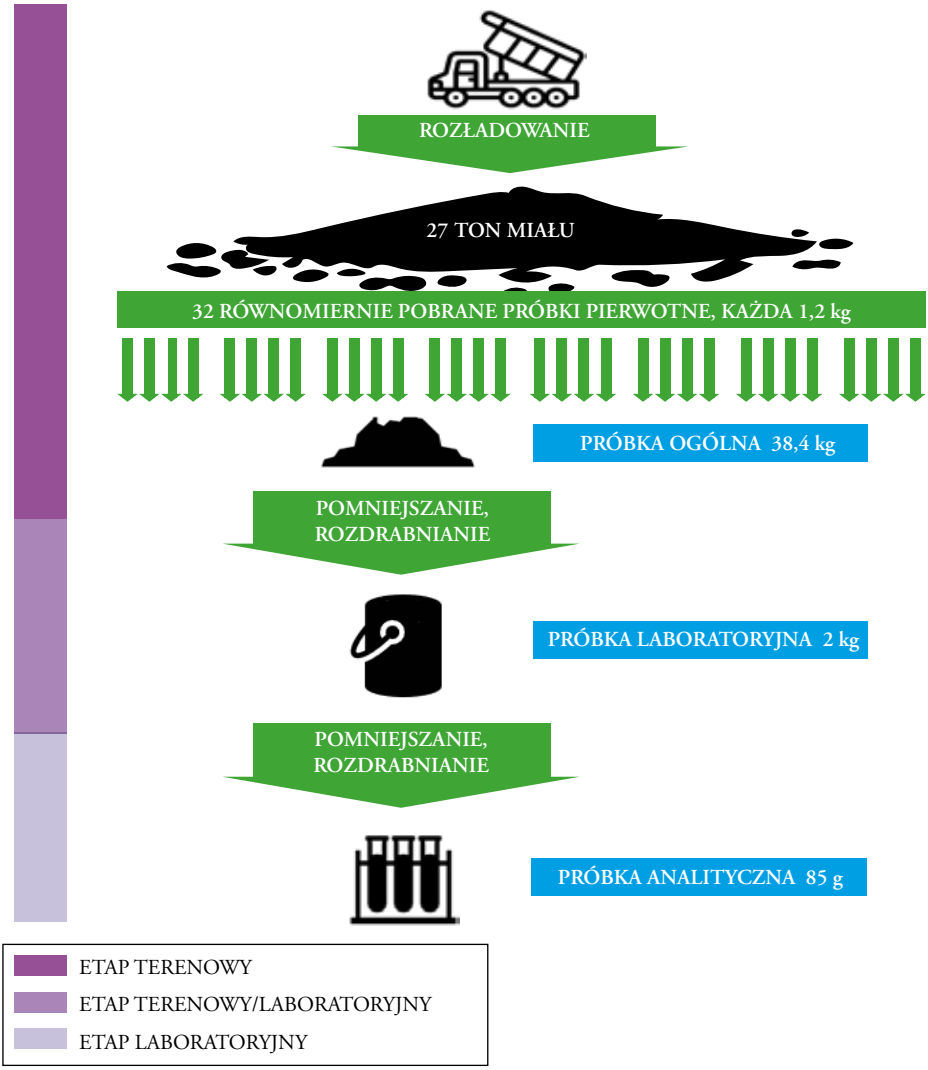
reinterpretowane poprzez połączenie „starych" wspomnień z informacjami zaczerpniętymi w okresie późniejszym, z mediów lub od organu procesowego (ang. *post-event information effect*), z oczekiwaniami czy też z tym, co z biegiem czasu wydaje się danej osobie spójne, logiczne i racjonalne. Zob. K. Leśniewski, M. Zubańska, *O rozpoznaniu przez świadka naocznego raz jeszcze. Studium przypadku niedoszłej pomyłki sądowej*, „Studia Prawnoustrojowe" 2022, nr 57, s. 386. https://doi.org/10.31648/sp.7895.

[49] Kluczowe jest ustalenie – na tyle, na ile to możliwe – czy osoby te znały omawianą metodykę już w czasie pobierania próbek, a nie w chwili przesłuchania. Nie można bowiem wykluczyć, że dana osoba dopiero przed przesłuchaniem przeszła szkolenie w tym zakresie. Podczas przesłuchania należy zatem zadać pytania m.in. odnośnie do kwestii takich jak: gdzie, kiedy oraz w jakich okolicznościach przesłuchiwana osoba nabyła tę wiedzę.

[50] Analogiczna opinia może zostać zasięgnięta w przypadku wątpliwości co do prawidłowości przechowywania pobranych próbek lub przestrzegania prawidłowej metodologii podczas badań laboratoryjnych. W przypadku uzasadnionych wątpliwości co do rzetelności pracy laboratorium wykonującego badania pierwszeństwo powinno mieć jednak przeprowadzenie niezależnych badań w innej jednostce – oczywiście pod warunkiem, że część materiału dowodowego będzie nadal zachowana w formie zdatnej do takich badań.

[51] Przykładowo, Sąd Najwyższy wskazał, że „brak spełnienia wszystkich warunków, jakie powinny zostać zapewnione przy okazaniu, nie musi prowadzić do dyskwalifikacji wartości dowodowej tej czynności procesowej". Zob. wyrok SN z 18 VII 2013 r., sygn. III KK 92/13, OSNKW 2013, nr 11, poz. 98, wraz z glosą J. Wójcikiewicza, *Glosa do wyroku Sądu Najwyższego z 9 lipca 2019 r.,*

Etapy badania jakości węgla na potrzeby śledcze zostały przedstawione na rysunku 1.



Rysunek 1. Proces badania jakości węgla – etapy (przez etap terenowy należy rozumieć fazę oględzin).

Źródło: opracowanie własne.

III KK 92/13 [tytuł przywołanej glosy zawiera omyłkę pisarską – prawidłowa data wydania orzeczenia to 18 lipca 2013 r. – dop. K. L.], „Palestra" 2014, nr 3–4, s. 204–208. Zob. także: wyrok Sądu Apelacyjnego (dalej: SA) w Katowicach z 26 X 2012 r., sygn. II AKa 415/12, LEX nr 1285048 oraz wyrok SA we Wrocławiu z 30 XII 2014 r., sygn. II AKa 399/14, LEX nr 1657128.

Jak już wskazano, odpowiednio pobrana i zabezpieczona próbka węgla powinna bez zbędnej zwłoki zostać skierowana do wybranego laboratorium w celu przeprowadzenia interesujących organ badań. Podstawowymi parametrami, które należy ustalić w przypadku podejrzenia oszustwa klasowego, są: zawartość wilgoci (symbol „W_t^r" – wilgoć całkowita w stanie roboczym), zawartość popiołu (symbol „A^r" – popiół w stanie roboczym), zawartość siarki (symbol „S_t^r" – siarka całkowita w stanie roboczym), a także wartość opałowa (symbol „Q_i^r" – wartość opałowa w stanie roboczym; wartość ta stanowi kluczowy parametr w analizowanym kontekście i może być wyznaczana na podstawie wyników analizy pozostałych parametrów węgla oraz odpowiednich zależności obliczeniowych)[52]. Badanie próbek węgla należy bezspornie do wiadomości specjalnych, a zatem – zgodnie z treścią art. 193 § 1 k.p.k. – wymaga zasięgnięcia opinii biegłego. Celowe wydaje się przy tym zasięganie nie tyle opinii biegłego, ile stosownego instytutu czy laboratorium (vide art. 193 § 2 k.p.k.), gdyż przeprowadzenie takich badań wymaga posiadania specjalistycznej aparatury. Należy zalecić korzystanie, jeśli tylko to możliwe, z podmiotów mających akredytację Polskiego Centrum Akredytacji do wykonywania określonego typu badań[53]. Jednostkami mającymi akredytację do

[52] Warto zaznaczyć, że norma PN-G-04502:2014-11 zakłada niepewność pobierania próbek do badań laboratoryjnych do ± 2% (dla popiołu). Oznacza to, że dla konkretnej partii węgla wynik oznaczenia zawartości popiołu może mieścić się w przedziale szerokości 4% i jest to spowodowane wyłącznie naturalną niejednorodnością rozważanego surowca. Ze znanych autorowi wyników badań przeprowadzonych w Głównym Instytucie Górnictwa – Państwowym Instytucie Badawczym w Katowicach wynika, że na 1% zawartości popiołu w węglu energetycznym przypada ok. 300 kJ/kg wartości opałowej. W konsekwencji można przyjąć, że wynik oznaczenia wartości opałowej dla próbki pobranej z konkretnej partii węgla może mieścić się w przedziale o szerokości 1200 kJ/kg. Okoliczność ta ma istotne przełożenie na rozważania zawarte w niniejszym artykule. Oznacza bowiem, że różnica pomiędzy klasą węgla (wartością opałową) „na fakturze" a wartością ustaloną w wyniku badań laboratoryjnych próbki pobranej z tej partii węgla musi być większa niż wskazane powyżej wartości, aby w ogóle zasadnie rozważać ewentualne oszustwo jakościowe. Należy zatem uznać, że różnica rzędu np. 900 kJ/kg (tj. < 1000 kJ/kg) powinna prowadzić do umorzenia lub niewszczynania postępowania (vide art. 5 § 2 k.p.k.). Z kolei przy różnicach mniejszych niż dwie klasy (lecz większych niż 1000 kJ/kg, tj. 1001–2000 kJ/kg) przed podjęciem ostatecznej decyzji odnośnie do dalszego losu postępowania celowe wydaje się zasięgnięcie szczegółowej opinii biegłego oraz wnikliwe przeanalizowanie in concreto pozostałych dowodów zgromadzonych w sprawie.

[53] Zob. D. Wilk, *Nowoczesne metody fizykochemii kryminalistycznej w procesie karnym. Zagadnienia wybrane*, Kraków 2018, s. 212–213. Zob. także: wyrok SA w Warszawie z 22 V 2023 r., sygn. II AKa 92/23, LEX nr 3581607. Trafnie stwierdzono w nim, że „specjalistyczną jest taka instytucja, w której profilu działalności mieści się wykonywanie ekspertyz, co zostało potwierdzone przez właściwe organy państwowe i jest przez nie na bieżąco nadzorowane. Pozwala to zaliczyć do instytucji specjalistycznych także prywatne podmioty gospodarcze, o ile posiadają własną wyspecjalizowaną kadrę o potwierdzonych przez organy państwowe kompetencjach, wykonują badania we własnych laboratoriach, które zostały poddane procedurze certyfikacji, a kierownik jednostki ma przygotowanie w zakresie nauk sądowych, aby wyznaczyć do wykonania opinii kompetentną osobę".

przeprowadzania badań w zakresie wartości opałowej węgla są np. Główny Instytut Górnictwa – Państwowy Instytut Badawczy w Katowicach, Instytut Technologii Paliw i Energii w Zabrzu oraz Centralne Laboratorium Pomiarowo-Badawcze Sp. z o.o. w Jastrzębiu-Zdroju.

Finalnie należy wskazać, że nawet najbardziej modelowo przeprowadzone opróbowanie danego transportu węgla pozwala jedynie na uzyskanie materiału dowodowego odnoszącego się bezpośrednio do tego konkretnego transportu. Z kolei analizowane mechanizmy działania przestępczego, co do zasady, nie są zachowaniami jednorazowymi, lecz są wielokrotnie powtarzane. Dotychczasowa praktyka śledcza wskazuje, że przypisanie przestępstwa w szerszym zakresie niż tylko wywóz, w trakcie którego doszło do zatrzymania, wymaga wzmożonej aktywności organu prowadzącego postępowanie (szeroko zakrojone, a zarazem sprawne zabezpieczanie potencjalnego materiału dowodowego, m.in. dokumentów handlowych, listów przewozowych, bilingów), a ponadto gotowości do skrupulatnej, opartej na zasadach logiki formalnej analizy materiału dowodowego zgromadzonego w sprawie. Przykładem tego typu rozumowania może być fragment uzasadnienia zawarty w wyroku Sądu Okręgowego w Gliwicach, Ośrodek Zamiejscowy w Rybniku z 9 sierpnia 2016 r.:

> (…) Oficjalnie KWK (…) w okresie objętym zarzutami w swojej ofercie posiadała miał węglowy w klasie „19" zatem o wartości energetycznej od 19.000 do 19.999 kJ/kg. Nie posiadała w ofercie miałów w klasie „22" oraz „23" zatem oficjalnie nie mogła takiego miału ani produkować, ani sprzedawać. Z wiarygodnych – zdaniem sądu – zeznań przesłuchanych na tę okoliczność przedstawicieli (…) – K. oraz Z. G. (2), wynika, że na skutek dostarczenia spółce (…) miałów w klasie energetycznej „22" i „23" zamiast miału o parametrach wynikających ze złożonych zamówień, (…) poniosła wymierną szkodę, wyliczoną w sposób opisany na stronie 9 uzasadnienia. Oskarżony wiedział, jakie parametry winien posiadać miał węglowy, odsprzedawany spółce (…), a następnie sprzedawany przez (…) poszczególnym elektrociepłowniom[54]. Przecież to oskarżony w imieniu spółki (…) zawarł umowę nr (…) z dnia 10.01.2003 r. o współpracy obu tych podmiotów (…). Jak wskazano wyżej, ustalenia dotyczące parametrów węgla, który miał być dostarczany przez (…) dla konkretnych elektrociepłowni – zgodnie z § 2 umowy określały tzw. warunki szczegółowe. Chcąc więc wywiązać się z tych ustaleń, oskarżony musiał zadbać o to, by każdorazowo węgiel sprzedawany spółce (…) i dalej odsprzedawany

[54] W odniesieniu do powyższego warto zaznaczyć, że piece stosowane w energetyce zawodowej i ciepłownictwie są, co do zasady, przystosowane do określonych parametrów jakościowych węgla. Nawet jeżeli piec nie ulegnie awarii, spalanie węgla niespełniającego parametrów wymaganych dla danego urządzenia może skutkować obniżeniem jego wydajności.

przez (…) konkretnej elektrociepłowni posiadał parametry wymagane przez daną elektrociepłownię, będącą końcowym odbiorcą węgla. Normalnie, aby uczynić zadość wymaganiom konkretnej elektrociepłowni, a tym samym ustaleniom owych warunków szczegółowych oskarżony winien złożyć zamówienie sam lub nakazać to podległym sobie pracownikom w tej kopalni, która w swojej ofercie posiadała węgiel o wymaganych przez odbiorcę końcowego parametrach. Nasuwa się pytanie, dlaczego tak nie postąpił, nie wyszukał kopalni, która taki węgiel miała w swojej ofercie, lecz zamówienia na węgiel o parametrach dużo niższych od wymaganych przez poszczególne elektrociepłownie nakazał złożyć w KWK (…), która w owym czasie oficjalnie węgla o takich parametrach nie posiadała. Jest oczywiste, że kupując węgiel energetyczny w klasie „19" zatem dużo gorszy niż określony dla poszczególnych elektrociepłowni ryzykował zerwaniem współpracy przez spółkę (…). Dlaczego mimo to polecił składać zamówienia na oferowany przez KWK (…) węgiel w klasie „19"? Odpowiedź może być tylko jedna. Otóż musiał wiedzieć, że zamawiając węgiel w klasie energetycznej „19" otrzyma węgiel znacznie lepszej jakości, taki który będzie odpowiadać ustaleniom zawartym w warunkach szczegółowych. Mało tego, zamawiając oferowany przez KWK (…) węgiel w klasie „19" płacił cenę zgodną z cennikiem przewidzianym dla tej klasy węgla, mimo iż faktycznie otrzymywał węgiel o znacznie lepszych parametrach, za który normalnie musiałby zapłacić wyższą cenę. O tym, że oskarżony wiedział, że w następstwie realizacji zamówień na węgiel o parametrach 19/25/08, na kopalni (…) załadowany na wagony zostanie węgiel o znacznie lepszych parametrach wynika zresztą z jego własnych wyjaśnień, gdzie przyznał, że wiedział, iż zamawiany miał węglowy w klasie „19" faktycznie będzie w klasie wyższej (…). Jakkolwiek sąd w przypadku transakcji ujętych w a/o ostatecznie wykluczył dosypywanie flotokoncentratu do przerostu w celu podwyższenia jego kaloryczności, niemniej zeznania ww. świadków potwierdzają przyjęte założenie, iż dlatego składano zamówienia na węgiel w klasie „19" bo wiadomo było, że faktyczne parametry dostarczonego przez KWK (…) węgla dla spółki (…) będą dużo lepsze. Żeby móc się dowiedzieć, o ile dokładnie lepsze, pracownicy spółki otrzymywali przygotowane dla nich na tej kopalni zaplombowane próbki węgla, które zawozili do badań laboratoryjnych, co wykazano wcześniej. Za niedorzeczne sąd uznał twierdzenie oskarżonego, że wiedział, iż otrzymany węgiel będzie w klasie wyższej niż zamówiony, bo… wszystkim taki węgiel był sprzedawany. Gdyby tak było, ów proceder wyszedłby na jaw znacznie wcześniej[55].

[55] Wyrok SO w Gliwicach Ośrodka Zamiejscowego w Rybniku z 9 VIII 2016 r., sygn. V K 12/15, LEX nr 2322408.

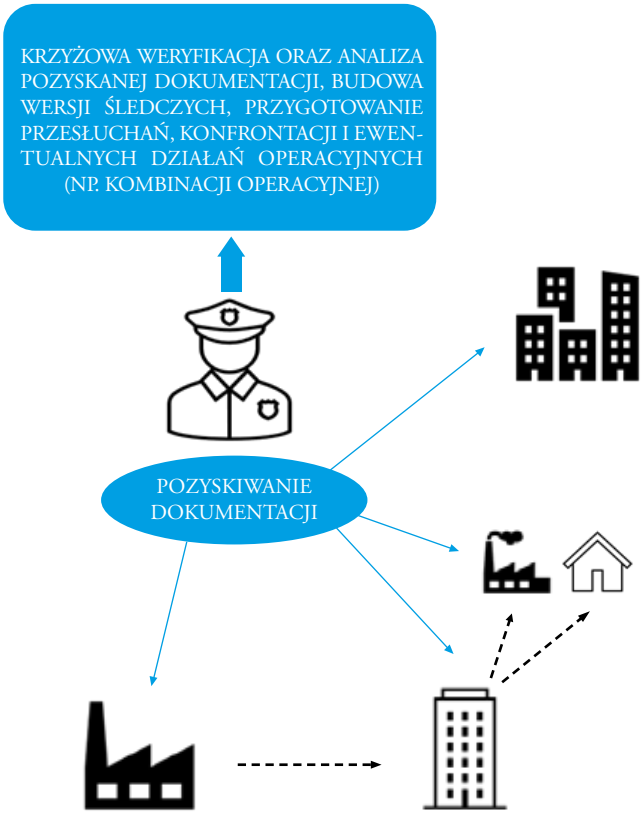
Warto zapoznać się także z argumentacją Sądu Apelacyjnego w Katowicach zawartą w wyroku z 13 czerwca 2013 r.:

> Głównym odbiorcą węgla od oskarżonego była (…) Sp. z o.o., która z kolei odsprzedawała go Przedsiębiorstwu (…) w K. Realizacja dostaw miału węglowego zamawianego przez oskarżonego w praktyce sprowadzała się do tego, że węgiel ten był ładowany na wagony i koleją dostarczany bezpośrednio z kopalni do K. Kolejne podmioty gospodarcze wystawiały natomiast faktury dokumentujące sprzedaż węgla, tj. KWK (…) na rzecz A. C., oskarżony na rzecz (…) Sp. z o.o., a ta ostatnia spółka na rzecz (…) w K. Charakterystyczne było to, że w fakturach otrzymywanych przez oskarżonego była wykazywana kaloryczność zakupywanego miału węglowego (19 - 21 kJ/kg) [omyłka w oryginale, powinno być MJ/kg – dop. K. L.], ale już w wystawianych przez niego na rzecz (…) takiej informacji już nie było. Z uwagi na przeznaczenie miału (…) był zainteresowany nabywaniem miału węglowego o wyższej kaloryczności, tj. rzędu 23 - 25 MJ/kg. Węgiel o gorszych parametrach powodował awarie w systemie grzewczym, a także nie dawał odpowiedniego ciepła. Z tego też powodu w zawartej pomiędzy (…) Składy (…) w K. a (…) Sp. z o.o. umowie określona została odpowiednia kaloryczność węgla, który miał być przedmiotem dostaw (umowa stanowi dowód w tej sprawie). Przesłuchany w toku postępowania prezes spółki z o.o. (…) Składy (…) w K. M. W. potwierdził, że jego firma była zainteresowana wyłącznie nabywaniem węgla o wyższej kaloryczności. Z kolei pracownicy spółki (…), tj. S. W. i S. B. zeznali, iż w celu właściwej realizacji umowy z (…) w K. zmuszeni byli kupować miał węglowy o kaloryczności minimum 23 MJ/kg. Potwierdzali też, że z tego powodu ze swoimi dostawcami m.in. firmą (…), którą prowadził oskarżony, uzgadniali dostawy węgla o takich właśnie parametrach. Zatem oczywistym wydaje się być, że (…) sp. z o. o. nie była zainteresowana nabywaniem węgla o kaloryczności 19 MJ/kg lub 21 MJ/kg. Jednocześnie bezsporne w przedmiotowej sprawie było to, że w KWK (…) został zorganizowany przestępczy proceder wyłudzania miału węglowego. Grupa osób z kierownictwa kopalni (skazanych prawomocnym wyrokiem) weszła w porozumienie z niektórymi kontrahentami. Umożliwiała im składanie zamówień na zakup miału węgla o niższej jakości, za który płacili cenę zgodnie z taryfikatorem, ale w zamian za korzyść majątkową, przekazywała im węgiel o wyższych parametrach (…). W oparciu o całokształt przytoczonych wyżej faktów sąd pierwszej instancji wyciągnął wnioski, którym nie sposób odmówić logiki. Skoro A. C. mógł odsprzedawać swoim odbiorcom węgiel jedynie o lepszych parametrach to taki właśnie powinien był otrzymywać z kopalni. Jeżeli zatem realizował dostawy do (…) to zgodnie z umową dostarczał miał węglowy o parametrach nie mniejszych niż 23 MJ/kg. Zatem logika podpowiada, że taki właśnie węgiel otrzymywał od swojego dostawcy,

> mimo składania formalnych zamówień i zapłaty za węgiel o kaloryczności 19 - 21 MJ/kg. Było to możliwe, gdyż uczestniczył w realizacji przestępczego procederu, o którym wspomniano wcześniej. Dokonując ustaleń w taki sposób nie trzeba było wykazywać, że próbki pobierane do badań laboratoryjnych (…) w K. nie były podmieniane, na co wskazywał skarżący. W wyniku tych badań nie zakwestionowano jakości dostarczonego węgla, co tylko dodatkowo uwiarygadnia inne dowody obciążające oskarżonego. Inaczej byłoby, gdyby testy laboratoryjne wskazały na niższą jakość węgla dostarczanego przez oskarżonego. Wówczas byłby to istotny dowód przeczący winie oskarżonego, ale taka sytuacja w okresie od 27 lipca 2005 roku nie miała miejsca. Ta okoliczność tłumaczy jednocześnie przyjęty w akcie oskarżenia czasokres, który pozwala przyjąć, że od tej daty oskarżony z całą pewnością dostarczał węgiel o wyższych parametrach niż sam zamawiał na kopalni (…). Argumenty zawarte w apelacji obrońcy nie są w stanie tego łańcucha poszlak obalić, gdyż tworzy on spójną, zwartą i logiczną całość, wykluczającą inną wersję wydarzeń. Z całą pewnością nie są nimi twierdzenia, że oskarżony nie był obecny przy załadunku węgla na wagony, jak również nie otrzymywał wyników badań jego próbek z kopalnianego laboratorium, a w związku z tym nie mógł wiedzieć co ostatecznie kopalnia sprzedała[56].

Podejście śledcze odzwierciedlone w przytoczonych fragmentach orzeczeń przedstawiono schematycznie na rysunku 2.

[56] Wyrok SA w Katowicach z 13 VI 2013 r., sygn. II AKa 150/13, LEX nr 1349896.



Podmioty trzecie mogące posiadać informacje istotne dla sprawy (np. zewnętrzne laboratoria badające węgiel, operatorzy telekomunikacyjni):

- dokumentacja badań fizykochemicznych danej partii węgla (jeśli zlecała je kopalnia lub podejrzewany podmiot);
- dane telekomunikacyjne (wykazy połączeń, dane lokalizacyjne z logowań do BTS);
- dokumentacja transportowa (np. listy przewozowe)

Odbiorcy końcowi nabywający węgiel od podmiotu podejrzewanego o udział w procederze (odbiorcy indywidualni lub podmioty gospodarcze):

- dokumentacja handlowa (od kogo, kiedy i jaki węgiel nabywali);
- dokumentacja związana z badaniami węgla – jeśli dany odbiorca zlecał własne badania (czynią tak, co do zasady, np. elektrownie i elektrociepłownie);
- dokumentacja techniczna posiadanych pieców (dot. podmiotów z zakresu ciepłownictwa lub energetyki zawodowej)

Kopalnia:

- dokumentacja wewnętrzna związana ze sprzedażą i/lub produkcją węgla, a także dokumentacja pracownicza (zapisy rejestru czasu pracy osób odpowiedzialnych za załadunek węgla lub jego ważenie w danym okresie itp.)

Podmiot podejrzewany o udział w procederze:

- dokumentacja handlowa (komu, kiedy i jaki węgiel zbywał; od kogo, kiedy i jaki węgiel nabywał; jaki węgiel posiadał w ofercie);
- dokumentacja dotycząca posiadanej infrastruktury technicznej (czy podejrzewany podmiot dysponował własnymi magazynami oraz zapleczem technicznym umożliwiającym mieszanie lub wzbogacanie węgla itp.)

Rysunek 2. Przykładowy schemat wybranych czynności śledczych dla mechanizmu „jakościowego" w przypadku nieujęcia sprawców in flagranti lub podejrzenia, że ujawnione zdarzenie stanowi jedynie część szerszego procederu. Należy zaznaczyć, że dokumentacja będąca w posiadaniu podejrzewanego podmiotu powinna, co do zasady, zostać zabezpieczona w trybie art. 217 oraz art. 219–220 k.p.k. (tj. wezwanie do wydania rzeczy połączone z następującym

po nim przeszukaniem). Istotne jest przy tym, aby bezpośrednio po tych czynnościach (lub równolegle do nich) zabezpieczyć także dokumentację będącą w posiadaniu pozostałych podmiotów wskazanych na rysunku 2 w celu zminimalizowania ryzyka potencjalnego matactwa. Dokumentację pochodzącą z różnych źródeł należy następnie poddać krzyżowej analizie poprzez wzajemne zestawienie i weryfikację poszczególnych informacji. Podana kolejność pozyskiwania dokumentacji ma charakter poglądowy, a rzeczywista sekwencja powinna być uzależniona od okoliczności konkretnej sprawy.

Źródło: opracowanie własne.

Podsumowanie i wnioski

Sprawne prowadzenie czynności wykrywczo-dowodowych w sprawach dotyczących przestępczości na szkodę spółek węglowych, w tym przestępczości dotyczącej bezpośrednio węgla kamiennego, wymaga, co do zasady, posiadania przez osoby, które są za te czynności odpowiedzialne, należytego rozeznania w szeroko pojętej specyfice górniczej. Takie rozeznanie – będące w istocie specjalizacją branżową funkcjonariusza według terminologii zaproponowanej przez Tadeusza Hanauska[57] – jawi się jako szczególnie pomocne zarówno w typowaniu źródeł informacji o potencjalnej istotności dla danej sprawy, jak i w należytym obcowaniu z nimi. Jak bowiem zasadnie podnoszą Mariusz Kulicki, Violetta Kwiatkowska-Wójcikiewicz oraz Leszek Stępka: (…) *aby nie przeoczyć śladu, rozumieć jego wymowę i umieć dowodzić na podstawie śladów, trzeba orientować się, jakie ślady powstają w związku z określonymi działaniami, gdzie mogą one występować, na jakie działania wskazują*

[57] Hanausek pisał o celowości wyspecjalizowania procesów wykrywczych, wskazując, że rozwój pracy wykrywczej musi uwzględniać także potrzebę wyspecjalizowania tej pracy. Słusznie podkreślał, że specjalizacja powoduje zwiększenie efektywności danych działań. W swoich rozważaniach wyróżnił kryterium obiektowe, które opisywał jako polegające na: „(…) selektywnym zacieśnianiu działalności wykrywczej do określonego obiektu bądź obiektów przeznaczenia społecznego, np. fabryk, zakładów. Ponieważ prócz oczywistego wyróżnika terenowego (obiekt wszak znajduje się na określonym terenie) występuje tu ponadto także pewne zacieśnienie środowiskowe związane z faktem, iż w określonym obiekcie z reguły występuje względnie stałe środowisko, kryterium to bardzo ogranicza działalność wykrywczą (…). Z uwagi na liczebność kadr organów wykrywczych (…), w typowej pracy wykrywczej pionu kryminalnego kryterium to nie bywa stosowane. Wykazuje ono jednak szereg zalet i zasługuje na bliższą uwagę". Komentując powyższe, należy wskazać na celowość nie tyle specjalizacji obiektowej „całego" organu, ile konkretnych funkcjonariuszy. Hanausek wyróżnił również kryterium branżowe, o którym pisał: „(…) zastosowanie kryterium branżowego w ramach specjalizacji wykrywczej polega na zacieśnianiu procesu wykrywczego do określonej sfery działalności społecznej, przede wszystkim wytwórczej lub usługowej. Od kryterium obiektowego i terenowego różni je ukierunkowanie specjalizacji na merytorycznie bliskie sobie obiekty działalności społecznej usytuowane równorzędnie bądź w hierarchicznym podporządkowaniu". Zob. T. Hanausek, *Zarys kryminalistycznej teorii wykrywania. Część II. Proces wykrywczy*, Warszawa 1987, s. 40–44.

określone ślady i jakie dalsze ślady mogą towarzyszyć śladom już ujawnionym[58]. Odpowiednie rozeznanie w tym zakresie niewątpliwie minimalizuje również ryzyko ewentualnych przeoczeń lub uchybień podczas wykonywania poszczególnych czynności procesowych (np. niewłaściwe opróbowanie – w ramach oględzin – zatrzymanego transportu węgla może skutkować niemiarodajnością otrzymanych następnie wyników badań laboratoryjnych, a tym samym ich wątpliwą wartością dowodową). Wydaje się ono także nie do przecenienia w kontekście dokonywania oceny zeznań (wyjaśnień) czy też identyfikacji okoliczności uzasadniających zasięgnięcie opinii biegłego, a także określenia przedmiotu i zakresu zlecanej ekspertyzy[59]. Mając powyższe na uwadze, należy postulować, aby komórki organów ścigania, które obejmują swą właściwością zakłady górnicze, dysponowały funkcjonariuszami odpowiednio zaznajomionymi z rozpatrywaną problematyką, tj. z jej podstawowymi zagadnieniami. Od przedstawicieli organów ścigania nie można wymagać, co oczywiste, przygotowania merytorycznego na poziomie właściwym dla osób mających wykształcenie branżowe czy też biegłych danej specjalności, trzeba jednak dążyć do tego, aby funkcjonariusz odpowiedzialny za „sprawy górnicze" miał wiedzę pozwalającą mu na efektywną interakcję z tymi osobami. Wiedzę taką może on nabyć m.in. dzięki stosownej praktyce lub udziałowi w odpowiednich szkoleniach. Wydaje się, że nie jest to postulat nad wyraz wygórowany, zwłaszcza jeśli się zważy, że PGG S.A. jest największym podmiotem gospodarczym – pod względem liczby zatrudnianych pracowników – na obszarze województwa śląskiego, a poszczególne kopalnie wchodzące w skład spółki stanowią newralgiczne zakłady przemysłowe w miejscowościach, na których terenie są ulokowane[60].

---

[58] M. Kulicki, V. Kwiatkowska-Wójcikiewicz, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2009, s. 365.

[59] Jak słusznie zauważa Tadeusz Widła, „(…) podjęcie decyzji o zasięgnięciu opinii biegłego łączy się z koniecznością rozstrzygnięcia wielu dylematów, które najogólniej podzielić można na dwie grupy [jest to raczej błąd redakcyjny i należy przyjąć, że Widła miał na myśli trzy grupy – przypis K. L.]: dotyczące zasadności przeprowadzenia tej czynności, dotyczące wyboru wykonawcy ekspertyzy, dotyczące realizacji tej czynności". Zob. T. Widła, *Aprioryczna ocena dowodu z opinii biegłych*, w: *Nauka wobec prawdy sądowej: księga pamiątkowa ku czci profesora Zdzisława Kegla*, R. Jaworski, M. Szostak (red.), Wrocław 2005, s. 605.

[60] Zob. J. Frankowski, J. Mazurkiewicz, *Województwo śląskie w punkcie zwrotnym transformacji*, IBS Research Report 02/2020, Instytut Badań Strukturalnych, http://ibs.org.pl/app/uploads/2021/02/IBS_Research_Report_02_2020.pdf [dostęp: 1 VIII 2024]. Rozprawa doktorska, na której został oparty niniejszy artykuł, dotyczy bezpośrednio przestępczości na szkodę PGG S.A. Analogiczną prawidłowość można jednak dostrzec również w odniesieniu do kopalń należących do innych podmiotów, a w konsekwencji sformułować podobne wnioski.

Bibliografia

Gurgul J., *Instytucja specjalisty w procesie karnym*, „Prokuratura i Prawo" 1998, nr 11–12, s. 113–126.

Hanausek T., *Zarys kryminalistycznej teorii wykrywania. Część I. Pojęcie i przedmiot wykrywania sprawców przestępstw*, Warszawa 1978.

Hanausek T., *Zarys kryminalistycznej teorii wykrywania. Część II. Proces wykrywczy*, Warszawa 1987.

Kasprzak J., *Biegły i specjalista przed sądem – wybrane aspekty taktyczne*, Warszawa 2001.

Kasprzak J., *Oględziny osoby, miejsca i rzeczy*, w: *System Prawa Karnego Procesowego. Tom VIII. Dowody. Cz. 4*, P. Hofmański (red.), Warszawa 2019.

Kielerz A., Porzerzyńska-Antonik M., *Węgiel w energetyce zawodowej i ciepłownictwie – stan obecny i perspektywy*, „Zeszyty Naukowe Instytutu Gospodarki Surowcami Mineralnymi i Energią PAN" 2019, nr 108, s. 39–50. https://www.doi.org/10.24425/znigsme.2019.128676.

Kodeks postępowania karnego. Komentarz, J. Skorupka (red.), Warszawa 2023.

Kodeks postępowania karnego. Komentarz. Tom I: Art. 1–424, D. Świecki (red.), Warszawa 2024.

Kodeks postępowania karnego. Tom II: Komentarz do art. 167–296, R.A. Stefański, S. Zabłocki (red.), Warszawa 2019.

Kryminalistyka. Przewodnik, D. Wilk (red.), Toruń 2013.

Kulicki M., Kwiatkowska-Wójcikiewicz V., Stępka L., *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2009.

Leśniewski K., Zubańska M., *O rozpoznaniu przez świadka naocznego raz jeszcze. Studium przypadku niedoszłej pomyłki sądowej*, „Studia Prawnoustrojowe" 2022, nr 57, s. 375–390. https://doi.org/10.31648/sp.7895.

Membrey W.B., *Coal sampling*, w: *The Coal Handbook. Volume 1: Towards Cleaner Coal Supply Chains*, D. Osborne (red.), San Diego 2023.

Metodyka dokumentowania złóż kopalin stałych. Część III: Opróbowanie złóż kopalin, M. Nieć (red.), Kraków 2012.

Olszówka J., Paul B., *Zasady kontroli jakości węgla*, Katowice 1972.

Rybak A., *Rola i przyszłość węgla w zapewnieniu bezpieczeństwa energetycznego Polski*, Gliwice 2020.

Strzałkowski P., *Zarys rozwoju technologii górnictwa podziemnego*, Gliwice 2011.

Qian Z., *Coal sampling and analysis standards*, London 2014.

Wawrzynkiewicz W., Róg L., Hamala K., *Dokładność pobierania próbek paliw stałych za pomocą urządzeń mechanicznych*, „Przegląd Górniczy" 2005, t. 61, nr 11, s. 24–29.

Widła T., *Aprioryczna ocena dowodu z opinii biegłych*, w: *Nauka wobec prawdy sądowej: księga pamiątkowa ku czci profesora Zdzisława Kegla*, R. Jaworski, M. Szostak (red.), Wrocław 2005.

Wilk D., *Nowoczesne metody fizykochemii kryminalistycznej w procesie karnym. Zagadnienia wybrane*, Kraków 2018.

Wójcikiewicz J., *Glosa do wyroku Sądu Najwyższego z 9 lipca 2019 r., III KK 92/13*, „Palestra" 2014, nr 3–4, s. 204–208.

Źródła internetowe

Co to jest PN?, Polski Komitet Normalizacyjny, http://www.pkn.pl/polskie-normy/informacje-o-pn/co-jest-pn [dostęp: 31 XII 2023].

Frankowski J., Mazurkiewicz J., *Województwo śląskie w punkcie zwrotnym transformacji*, IBS Research Report 02/2020, Instytut Badań Strukturalnych, http://ibs.org.pl/app/uploads/2021/02/IBS_Research_Report_02_2020.pdf [dostęp: 1 VIII 2024].

Kurs dla próbobiorców w zakresie obowiązujących norm technicznych PN i ISO, Główny Instytut Górnictwa – Centrum Rozwoju Kompetencji, http://szkolenia.gig.eu/wydarzenie/kurs-dla-probobiorcow-w-zakresie-obowiazujacych-norm-technicznych-pn-i-iso/ [dostęp: 31 XII 2023].

Mastelarz M., *Dlaczego kluczowym etapem analizy paliwa jest odpowiednie pobranie próbek?*, Instytut Technologii Paliw i Energii, www.itpe.pl/blog/2021/09/08/dlaczego-kluczowym-etapem-analizy-paliwa-jest-odpowiednie-pobranie-probek/ [dostęp: 31 XII 2023].

Mastelarz M., *Polskie normy dotyczące ręcznego pobierania próbek węgla kamiennego*, Instytut Technologii Paliw i Energii, 9 X 2023 r., https://itpe.pl/polskie-normy-dotyczace-recznego-pobierania-probek-wegla-kamiennego/ [dostęp: 31 XII 2023].

Ministerstwo Aktywów Państwowych, *Program dla sektora górnictwa węgla kamiennego w Polsce* (wersja uwzględniająca korekty z 2022 r.), https://www.gov.pl/web/energia/programu-dla-sektora-gornictwa-wegla-kamiennego-w-polsce [dostęp: 1 VI 2024].

Akty prawne

Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. DzU z 2022 r. poz. 1854).

Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. DzU z 2015 r. poz. 1483).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. DzU z 2024 r. poz. 37, ze zm.).

Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (t.j. DzU z 2003 r. nr 169 poz. 1650, ze zm.).

Orzecznictwo

Wyrok Sądu Najwyższego z 3 XI 2021 r., sygn. V KK 460/20, LEX nr 3342210.

Wyrok Sądu Najwyższego z 18 VII 2013 r., sygn. III KK 92/13, OSNKW 2013, nr 11, poz. 98.

Wyrok Sądu Najwyższego z 5 XI 1999 r., sygn. V KKN 440/99, LEX nr 38328.

Wyrok Sądu Apelacyjnego w Warszawie z 22 V 2023 r., sygn. II AKa 92/23, LEX nr 3581607.

Wyrok Sądu Apelacyjnego we Wrocławiu z 30 XII 2014 r., sygn. II AKa 399/14, LEX nr 1657128.

Wyrok Sądu Apelacyjnego w Katowicach z 13 VI 2013 r., sygn. II AKa 150/13, LEX nr 1349896.

Wyrok Sądu Apelacyjnego w Katowicach z 26 X 2012 r., sygn. II AKa 415/12, LEX nr 1285048.

Wyrok Sądu Apelacyjnego w Lublinie z 29 IX 1998 r., sygn. II AKa 142/97, LEX nr 37066.

Wyrok Sądu Okręgowego w Gliwicach Ośrodka Zamiejscowego w Rybniku z 9 VIII 2016 r., sygn. V K 12/15, LEX nr 2322408.

Inne dokumenty

PN-82/G-97001 *Węgiel kamienny. Sortymenty*.

PN-82/G-97003 *Węgiel kamienny do celów energetycznych*.

PN-ISO 1953:1999 *Węgiel kamienny. Analiza ziarnowa metodą przesiewania*.

PN-ISO 18283:2008 *Węgiel kamienny i koks. Ręczne pobieranie próbek*.

PN-G-04502:2014-11 *Węgiel kamienny i brunatny. Pobieranie i przygotowanie próbek do badań laboratoryjnych. Metody podstawowe*.

Dr Kamil Leśniewski

Doktor nauk prawnych, sędzia sądu rejonowego, autor publikacji z zakresu kryminalistyki, postępowania karnego oraz międzynarodowego prawa humanitarnego konfliktów zbrojnych.

Kontakt: k.lesniewski@alumni.uj.edu.pl.

VARIA

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 287–298
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.032.24181

VARIA

Mikrobiologia w służbie ochrony dziedzictwa kulturowego



Zarówno prawo międzynarodowe, w tym konwencja haska z 1954 r., jak i przepisy krajowe o ochronie zabytków zobowiązują Polskę do zabezpieczania znajdujących się na jej terenie dóbr kultury przed skutkami konfliktów zbrojnych. Kluczem do sukcesu są działania podejmowane w czasie pokoju, w tym ochrona tych dóbr nie tylko przed ogniem, wodą czy toksycznymi substancjami chemicznymi, lecz także szkodliwymi mikroorganizmami.

Jak skutecznie chronić zbiory muzealne, archiwalne i biblioteczne przed grzybami i bakteriami, nie szkodząc jednocześnie cennym eksponatom? Rozmawiamy o tym z **dr Magdaleną Dydą**, specjalistką z wieloletnim doświadczeniem, która w pracy zawodowej łączy badania naukowe z zakresu mikrobiologii z ich praktycznym zastosowaniem na rzecz ochrony dziedzictwa kulturowego.

Daria Olender: W ostatnim czasie wiele uwagi poświęca się zagadnieniom związanym z ochroną ludności i obroną cywilną. Obejmuje to również problematykę zabezpieczenia dóbr materialnych, w tym dziedzictwa kulturowego. Porozmawiajmy o mniej oczywistych zagrożeniach czyhających na zabytki i muzealia. Odwołując się do Pani wykształcenia i praktyki zawodowej, zapytam: po co muzeom i archiwom biolodzy?

Dr Magdalena Dyda: Biolodzy i mikrobiolodzy wspomagają muzea, archiwa i biblioteki w prewencji konserwatorskiej, która w głównej mierze wiąże się z monitorowaniem szkodliwych czynników biologicznych. Do najbardziej niszczycielskich, po człowieku, organizmów żywych w kontekście ochrony dóbr kultury przechowywanych w budynkach zaliczamy gryzonie, owady i mikroorganizmy. Wsparcie biologów i mikrobiologów pozwala na działania interwencyjne np. po zalaniu, ale również na zaplanowanie monitoringu zgodnie z Polską Normą dotyczącą konserwacji dziedzictwa kulturowego[1]. Cykliczny monitoring mikrobiologiczny i entomologiczny przestrzeni ekspozycyjnych czy magazynowych pozwala wykryć zagrożenie oraz określić ryzyko, jakie niesie ze sobą obecność danego owada lub mikroorganizmu. Dzięki temu działania interwencyjne, np. dezynfekcja, będąca działaniem nieobojętnym dla materiałów zabytkowych, są przeprowadzane tylko i wyłącznie dla tych obiektów, dla których ma to uzasadnienie. Przyjmujemy tutaj regułę mniejszego zła. Wiemy, że dezynfekcja jest szkodliwa, ale w przypadku potwierdzonej aktywności mikrobiologicznej robimy ją, ponieważ niekorzystne zmiany, jakie spowoduje aktywność mikrobiologiczna, będą większe. Co ważne, dezynfekcja nie pozwala na całkowitą eliminację mikroorganizmów i ich form przetrwalnych, ponieważ nie jest to sterylizacja. Często jeden zabieg nie wystarcza i trzeba go powtórzyć. Tu również pomocne są analizy czystości mikrobiologicznej, które umożliwiają zweryfikowanie skuteczności tej procedury.

Analizy mikrobiologiczne wykonuje się również podczas przekazywania zbiorów do innej instytucji, gdy wracają z wypożyczenia czy przed ich relokacją do nowego budynku. Dzięki przeglądom mikrobiologicznym całych kolekcji muzealnych, zasobu archiwalnego czy bibliotecznego możemy ocenić, które zbiory są skażone i wymagają dezynfekcji, które są zanieczyszczone zarodnikami pleśni i trzeba je mechanicznie oczyścić,

[1] PN-EN 16790:2016-08 *Konserwacja dziedzictwa kulturowego. Kompleksowa metodyka postępowania ze skażeniami i zanieczyszczeniami biologicznymi (IPM) na potrzeby ochrony dziedzictwa kulturowego*.

a które można bezpiecznie przenieść do nowej lokalizacji. Ponadto dzięki identyfikacji wyizolowanych mikroorganizmów możemy ocenić narażenie pracowników na szkodliwe czynniki biologiczne w miejscu pracy. Często wykonujemy badania w pomieszczeniach, w których stwierdzono uciążliwy, nieprzyjemny czy piwniczny zapach. Dobrze zaplanowane badania pozwalają zidentyfikować jego przyczynę. Najczęściej jest nią aktywność mikrobiologiczna w miejscach o ograniczonej cyrkulacji, np. za meblami, lub w pobliżu nieszczelności z instalacji wodno-kanalizacyjnej.

Mikrobiolodzy monitorują również jakość powietrza, czyli warunki, w jakich zbiory są przechowywane. Analizą mikroorganizmów i ich przetrwalników unoszących się w powietrzu zajmuje się rozwijająca się dynamicznie, m.in. dzięki wykorzystaniu metod genetycznych, dziedzina wiedzy zwana aeromikrobiologią. Analizy jakości powietrza pozwalają ustalić, czy problem skażenia powietrza w budynku występuje, a jeżeli tak, to w których pomieszczeniach i jaka jest jego przyczyna. Pozwolę sobie w tym miejscu na dygresję. Pandemia COVID-19 uświadomiła ludziom występowanie ryzyka mikrobiologicznego, które nie jest widoczne. To przełożyło się na wzrost zainteresowania jakością powietrza i liczby zapytań o takie badania, zwłaszcza po powrocie do pracy w biurach.

W pomieszczeniach przeprowadza się także pomiary składu chemicznego powietrza, czyli analizy stężenia wybranych związków chemicznych, realizowane przy użyciu specjalistycznych urządzeń. Obecność w powietrzu związków silnie utleniających i reaktywnych, takich jak tlenki siarki, azotu, ozon, kwas octowy czy formaldehyd, znacznie przyspiesza starzenie się materiałów zabytkowych. Z tego względu np. w normie ISO:11799[2] czy wytycznych Kanadyjskiego Instytutu Konserwacji[3] zawarto informacje o maksymalnych dopuszczalnych stężeniach tych substancji w powietrzu. Zapewnienie jakości powietrza zgodnie z tymi wytycznymi ma wpływ na bezpieczne długotrwałe przechowywanie zbiorów.

Wykonujemy ponadto przeglądy entomologiczne zbiorów. Pozwalają one oszacować, czy w pomieszczeniach występują stawonogi, jak molowate czy skórnikowate, których obecność może zagrażać zbiorom.

[2] PN-ISO 11799:2024 *Informacja i dokumentacja. Wymagania dotyczące warunków przechowywania materiałów archiwalnych i bibliotecznych*.

[3] *Preventive conservation guidelines for collections*, Canadian Conservation Institute, https://www.canada.ca/en/conservation-institute/services/preventive-conservation/guidelines-collections.html [dostęp: 26 VIII 2026].

W monitoringu entomologicznym pomocne są pułapki lepowe i feromonowe oraz bezpośrednie odławianie okazów.

W kontekście ochrony zbiorów istotna jest cykliczność badań mikrobiologicznych i przeglądów entomologicznych. Wskazane jest ich prowadzenie w różnych porach roku, przy różnym natężeniu ruchu turystycznego, w pomieszczeniach o różnym przeznaczeniu, z różnym typem wentylacji i na różnych kondygnacjach. Dobrym przykładem jest monitoring, jaki prowadziliśmy w Zamku Królewskim na Wawelu, którego wyniki zostały opublikowane[4]. Niestety nie wszystkie instytucje kultury chcą dzielić się wynikami takich badań, przez co nie mamy pełnej wiedzy o skali problemu.

Dobrą praktyką jest wydzielenie działu zajmującego się prewencją konserwatorską. Obecnie takie działy istnieją tylko w nielicznych instytucjach muzealnych.

A co biolodzy biorą pod uwagę, oceniając stan budynku?

Oceną stanu budynku zajmują się mykolodzy budowlani. Pełne ekspertyzy mykologiczno-budowlane obejmują analizy zawilgocenia przegród budowlanych, rodzaju wysolenia (chlorki, azotany, siarczany) z analizą stężenia soli, ocenę stopnia degradacji elementów drewnianych i murów, a także stopnia zagrzybienia przegród budowlanych wraz z identyfikacją czynników mikrobiologicznych czy owadów. Zwracamy uwagę, czy występują mostki cieplne i co jest przyczyną korozji biologicznej i skażenia przegród budowlanych. Z doświadczenia wiemy, że największe zagrożenia związane z działaniem wody dotyczą najwyższej i najniższej kondygnacji. Potwierdza to m.in. Biblioteka Narodowa – 90% zbiorów papierowych, które trafiają do nich do osuszenia po zalaniu, to zbiory przechowywane albo w piwnicach, albo na poddaszach. Główne przyczyny aktywności

[4] *Prewencja jako niezbędny element opieki nad zbiorami Zamku Królewskiego na Wawelu. Konserwacja prewencyjna kolekcji Lanckorońskich*, E. Wiłkojć, J. Winiewicz (red.), Kraków 2019; *Konserwacja i prewencja jako niezbędny element opieki nad zbiorami w Zamku Pieskowa Skała*, E. Wiłkojć (red.), Kraków 2023; M. Dyda, A. Pyzik, P. Drabik, Ł. Istel, E. Wiłkojć, O. Buchwald-Zięcina, A. Bogdanowicz-Prus, A. Skłodowska, *Monitoring of Bio-Aerosols, Gaseous and Particulate Matter (PM) Pollution of Wawel Royal Castle in Krakow, Poland*, „CEST2019 Proceedings" 2019. https://doi.org/10.30955/gnc2019.00887; A. Pyzik, M. Dyda, E. Wiłkojć, J. Winiewicz-Wolska, *Microbiological Diversity and Microbial Related Risks at Wawel Royal Castle in Krakow, Poland*, „CEST2019 Proceedings" 2019. https://doi.org/10.30955/gnc2019.00339.

wody w materiałach oraz pojawienia się w rezultacie jej działania mikroorganizmów to przecieki z dachu i instalacji wodno-kanalizacyjnych oraz podciąganie kapilarne wód gruntowych czy zalania z urządzeń regulujących mikroklimat, takich jak nawilżacze i osuszacze.

Warto przypomnieć, że ekspertyza mykologiczno-budowlana to obowiązek w obiektach zarówno współczesnych, jak i zabytkowych, zwłaszcza przed planowaną przebudową, rozbudową, modernizacją lub zmianą przeznaczenia budynku oraz w wypadku stwierdzenia występowania zawilgocenia i oznak korozji biologicznej. Wynika to z rozporządzenia ministra infrastruktury w sprawie warunków technicznych budynków[5].

Jak wyglądają działania prewencyjne w przypadku archiwów?

Archiwa Państwowe mogą kierować się normą ISO 11799, o której już wspomniałam. Określa ona zasady bezpiecznego długoterminowego przechowywania zbiorów archiwalnych i bibliotecznych, czyli w głównej mierze obiektów wykonanych na podłożu papierowym. To jednak norma, która – jak większość – nie jest obligatoryjna. Część archiwów wprowadziła zasadę, że każdy zasób, który z racji ustawy trafia do nich na wieczyste przechowywanie, musi mieć wynik badania mikrobiologicznego potwierdzający brak skażenia. Wymóg ten wynika ze wskazanej normy ISO[6]. W zależności od ilości przekazywanych akt archiwum ustala, jaka liczba badań mikrobiologicznych jest niezbędna.

Jeśli chodzi o przechowywanie zbiorów archiwalnych, to głównym zanieczyszczeniem mikrobiologicznym są zarodniki, które osadzają się na powierzchniach w drodze sedymentacji. Aby ograniczyć ten proces, zalecane jest stosowanie oczyszczaczy powietrza, w których regularnie wymienia się filtry, a także zapewnienie odpowiedniej wentylacji i częste sprzątanie powierzchni użytkowych oraz mebli – przecieranie ich środkami dezynfekującymi bezpiecznymi dla papieru, mechaniczne oczyszczanie opakowań obiektów archiwalnych. To podstawa. Pamiętajmy przy tym, że nawet najnowocześniejsze urządzenia mające zapewnić

[5] *Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie* (t.j. DzU z 2022 r. poz. 1225, ze zm.).

[6] „Obiekty przechowywane w magazynie powinny być biologicznie czyste. Zaleca się dezynfekcję wszystkich obiektów, co do których zachodzi podejrzenie, że są zakażone przez mikroorganizmy, lub że gnieżdżą się w nich owady. Podobnie, zalecana jest dezynfekcja regałów oraz półek, na których odkryto obecność mikroorganizmów".

dokumentom ochronę nie spełnią swojej funkcji, jeśli nie będzie się ich stale kontrolować. W tym roku mieliśmy przypadek zalania z szafy klimatyzacyjnej zamontowanej w magazynie najcenniejszych i najbardziej wrażliwych zbiorów, tj. obrazów, obiektów papierowych i fotografii. Na skutek przecieku doszło do rozwoju pleśni na ścianach i obiektach. Ten przykład pokazuje, że instalacja zaawansowanych rozwiązań technicznych nie zastąpi cyklicznego sprawdzania przez personel stanu pomieszczeń.

Tu warto ponownie wspomnieć o dezynfekcji. W przypadku zbiorów wykonanych na podłożu papierowym najbardziej bezpieczną i powszechnie stosowaną w bibliotekach i archiwach jest dezynfekcja tlenkiem etylenu[7] metodą fumigacji w specjalistycznych komorach. Dla zbiorów po zalaniu sugeruję, by taką dezynfekcję prowadzić z wydłużonym czasem fumigacji, aby zwiększyć oddziaływanie związku biobójczego na mikroorganizmy. Takie podejście pozwala ograniczyć koszty – unikamy kolejnej fumigacji, która jest związana z powtórnym transportem zbiorów.

W czerwcu 2026 r. pożar będący skutkiem rosyjskiego ataku strawił w Kijowie zabytkowy kompleks Ławry Peczerskiej wpisany na listę światowego dziedzictwa UNESCO. To tylko jeden z wielu przykładów ogromnych strat związanych z wojną w Ukrainie. Czy Pani zdaniem pod wpływem doświadczeń za wschodnią granicą podmioty w naszym kraju zaczęły lepiej dbać o ochronę zabytków? Chodzi mi głównie o szukanie pomieszczeń, które mogłyby posłużyć za schronienie na wypadek sytuacji kryzysowej.

Pomieszczenia w instytucjach muzealnych są przygotowywane przede wszystkim pod kątem ewakuacji zbiorów, nie ludzi. Jako pierwsi muszą się wypowiedzieć konstruktorzy. To oni wskazują najbezpieczniejsze miejsce w danym budynku, badają, czy wytrzyma uderzenie, a strop udźwignie gruz, który może na nim spocząć. Zbiory trzeba zabezpieczyć odpowiednio wcześniej, gdyż w czasie działań wojennych jest to w zasadzie niemożliwe. Eksplozje nie muszą doprowadzić do zawalenia budynku, ale mogą uszkodzić okna. To naraża eksponaty na działanie czynników środowiskowych takich jak deszcz, temperatura i w efekcie na aktywność wody w materiałach, co sprzyja rozwojowi grzybów nie tylko pleśniowych, lecz także wielkoowocnikowych. I tutaj w sukurs przychodzą niekonwencjonalne rozwiązania takie jak środki z nanocząsteczkami

[7] Nazwa handlowa – Rotanox.

srebra, które działają zdecydowanie dłużej niż tradycyjne biocydy oparte na alkoholach. Nie są one dopuszczone do stosowania w obiektach zabytkowych, ale wojna to sytuacja wyjątkowa. Polska przekazała Ukrainie preparaty oparte na nanocząsteczkach srebra. Spryskiwano nimi księgozbiory w pomieszczeniach pozbawionych okien, aby do czasu ewakuacji zabezpieczyć je przed rozwojem grzybów mogących całkowicie zniszczyć papier. Dobrą praktyką w ramach ochrony zbiorów na wypadek działań zbrojnych jest ich umieszczanie z dala od przeszkleń.

W Polsce z podobną sytuacją mieliśmy do czynienia po pożarze Archiwum Urzędu Miasta Krakowa[8]. Doszło do niego w lutym, ale ze względu na ryzyko katastrofy budowlanej i działania śledczych dokumenty można było wydobyć dopiero w kwietniu. Po dwóch miesiącach od gaszenia pożaru, co wiązało się z wpompowaniem do budynku ok. 60 000 m^3 wody, dokumenty były już tak zainfekowane i przerośnięte grzybnią, że większości zasobu nie dało się uratować. W przypadku Krakowa straty są porównywalne do tych związanych ze spaleniem Biblioteki Ordynacji Krasińskich[9], czyli zbiorów obecnej Biblioteki Narodowej w Warszawie. Takie sytuacje skłaniają do refleksji, że powinniśmy inwestować w powstawanie cyfrowych bliźniaków obiektów zgromadzonych w instytucjach kultury. Podobnie należy działać w celu zabezpieczenia zabytkowych budynków. Inwentaryzacja 3D w bardzo dobrej rozdzielczości, ze szczegółową fotogrametrią, z uwzględnieniem detali architektonicznych, pozwoli je odtworzyć w razie potrzeby. Wiem, że w naszym kraju podejmuje się takie działania. W Narodowym Instytucie Dziedzictwa powołano mobilne laboratorium mające zinwentaryzować budynki zabytkowe.

Co jeszcze możemy zrobić, aby skuteczniej działać w sytuacjach kryzysowych?

Za bezcenne uważam szkolenia praktyczne, których – muszę to stwierdzić z przykrością – organizujemy zbyt mało. Kilkanaście lat temu sieć Archiwów Państwowych prowadziła szkolenia, podczas których uczestnicy wchodzili do zalanego magazynu i musieli ewakuować zbiory. Grupy

[8] Pożar wybuchł w lutym 2021 r. i całkowicie strawił archiwum. Zniszczeniu uległo ok. 150–200 mln dokumentów. Z 20 km akt uratowano niespełna 1 km i były one w bardzo złym stanie.

[9] Biblioteka Ordynacji Krasińskich spaliła się we wrześniu 1944 r. z powodu bombardowań dokonywanych przez Niemców.

były międzynarodowe, więc dodatkowe wyzwanie stanowiła bariera językowa. To doświadczenie uwrażliwiało na wiele aspektów i uczyło pokory. Moim zdaniem powinniśmy wrócić do takich praktyk. Cieszę się, że ten postulat pojawia się coraz częściej na spotkaniach związanych z opieką nad zabytkami. Wybrzmiał chociażby podczas ostatniej konferencji Polskiego Stowarzyszenia Inwentaryzatorów Muzealnych, podczas której podkreślono, że proste szkolenie z użycia gaśnicy jest bardziej skuteczne niż instrukcja czy procedura PPOŻ. A to pracownicy będą reagować jako pierwsi w przypadku realnego zagrożenia.

W ramach III Kongresu Bezpieczeństwa Dziedzictwa KOBED w 2025 r. miałam okazję obserwować ćwiczenia ratowniczo-gaśnicze dla pożaru, który „wybuchł" w lesie obok Zamku Pieskowa Skała. Pierwsze wozy Straży Pożarnej przyjechały po ok. 30 minutach od zgłoszenia. Nie wspominam o tym po to, by wytykać strażakom opieszałość. Absolutnie nie! Chcę tylko przypomnieć, że dojazd służb jest warunkowany specyfiką terenu. To pokazuje, z jakimi problemami muszą się mierzyć muzea i inne instytucje kultury usytuowane daleko poza centrami miast. Dlatego uważam, że jeśli chodzi o ochronę dóbr kultury na wypadek katastrof i działań wojennych, powinniśmy kłaść duży nacisk na szkolenia praktyczne, uwzględniające różne scenariusze zagrożeń. Szkolenia z gaszenia pożaru prowadzi np. Instytut Bezpieczeństwa Dziedzictwa. Dodam, że jest on organizatorem wspomnianego kongresu KOBED, podczas którego są omawiane zagadnienia związane z ochroną dóbr kultury w obliczu współczesnych kryzysów[10].

> **Wspomnijmy o kolejnym aspekcie Pani pracy. Badania mikrobiologiczne służą także ochronie zdrowia pracowników muzeów czy archiwów.**

Przypadek, o którym opowiem, akurat nie dotyczy budynków muzealnych, ale dobrze ilustruje problem. Wykonywaliśmy w tym roku analizy czystości mikrobiologicznej powietrza w pomieszczeniach mieszczących się w 10-letnim biurowcu w Gdańsku. Wyniki okazały się katastrofalne. Ilość zarodników pleśni w powietrzu była porównywalna do tych, jakie stwierdziliśmy w zawilgoconych kryptach katedry. Do krypt wchodzimy

[10] W 2026 r. odbyła się czwarta edycja tego wydarzenia. Zob. *IV Kongres Bezpieczeństwa Dziedzictwa Kobed'26. Zabezpieczenie i Ochrona Dóbr Kultury*, https://ibd.org.pl/kobed26/ [dostęp: 26 VIII 2026].

wyposażeni w maski i kombinezony, a w tych biurach ludzie pracowali przez osiem godzin bez żadnych środków ochrony. Okazało się, że w drugiej części budynku doszło do zalania, a podniesiona konstrukcja podłogi pozwoliła na przemieszczanie się wody do innych pomieszczeń, zawilgocenie na całej kondygnacji ścian działowych wykonanych z płyt kartonowo-gipsowych i wzrost grzybów pleśniowych na ich powierzchni. Zarodniki pleśni unosiły się w powietrzu, choć nie było widać aktywności mikrobiologicznej nad podłogą. Głównym powodem wykonania analiz jakości powietrza był nieprzyjemny zapach i objawy alergiczne u pracowników. Mówiąc o tym, chcę podkreślić, że często infekcja mikrobiologiczna nie jest widoczna, a niesie ze sobą poważne konsekwencje zdrowotne. Grzyby pleśniowe w trakcie wzrostu wydzielają kilkadziesiąt różnych związków chemicznych, w tym szkodliwe mykotoksyny, z których część jest rakotwórcza. Warto mieć świadomość, że takie zdarzenia coraz częściej dotyczą nowych budynków. To nie tylko kwestia gorszej jakości materiałów, z jakich są wykonywane instalacje wodno-kanalizacyjne, lecz także skutek nieodpowiedniego serwisowania systemu wentylacji i klimatyzacji w budynku. Obserwujemy również niebezpieczne praktyki administratorów budynków polegające na zmniejszaniu ilości wymian powietrza, co ma ograniczyć koszty eksploatacyjne. Takie działanie skutkuje niebezpiecznymi dla zdrowia stężeniami czynników szkodliwych w powietrzu – dwutlenku węgla, formaldehydu oraz bioaerozoli. Powoduje to u ludzi zmniejszenie poziomu koncentracji i wydajności pracy, a w przypadku długotrwałego narażenia może wywoływać alergie i schorzenia układu oddechowego.

Przy tej okazji chcę zwrócić uwagę, że popularne ozonowanie w przypadku grzybów pleśniowych często jest nieskuteczne. Ozon działa biobójczo na wirusy i bakterie, jednak zarodniki grzybów pleśniowych często pozostają całkowicie oporne na jego działanie, co potwierdza jedna z wojewódzkich stacji sanitarno-epidemiologicznych. Ponadto aby osiągnąć biobójcze stężenie ozonu i zagwarantować bezpieczeństwo tej procedury, należy zapewnić bardzo szczelne warunki. Ozon jest niebezpiecznym gazem, gdyż szybciej niż tlen łączy się z naszymi krwinkami. W trakcie ozonowania drastycznie wzrasta też stężenie formaldehydu wydzielanego podczas utleniania przez ozon tworzyw sztucznych: klejów, lakierów i farb np. z powierzchni mebli. Znam przypadki zatrucia formaldehydem osób, które przebywały w pomieszczeniu sąsiadującym z tym ozonowanym.

Jak zatem sprawdzić, czy powietrze w miejscu, gdzie pracujemy, jest czyste?

To niestety nie jest proste. Administratorzy budynków robią przeglądy, ale problem polega na tym, że nie ma wymogu wykonywania badań mikrobiologicznych powietrza. Jeżeli takie badanie jest wykonywane na prośbę wynajmującego przestrzeń biurową, ale zleceniodawcą jest administrator budynku, to w dniu, kiedy ma się odbyć, zapewnia on nienaganne warunki. Pamiętam sytuację, gdy robiąc pomiary na zlecenie instytucji, która wynajmowała pomieszczenia biurowe, zostałam wyprowadzona z budynku przez ochronę pod pretekstem, że administracji wcześniej nie poinformowano o badaniach. Jestem zwolenniczką tego, by administratorów zachęcać do dbałości o dobry stan powietrza w pomieszczeniach, a nie karać. Coraz więcej czasu spędzamy w zamkniętych przestrzeniach, zatem znaczenie jakości powietrza w nich także rośnie. I ciekawostka. W Japonii przy naborze do pracy podkreśla się, że jakość powietrza w pomieszczeniu biurowym jest na bieżąco monitorowana, a wyniki są ogólnodostępne. Traktuje się to jako zachętę i benefit dla pracownika.

Pracuje Pani w Research and Development for Life Sciences – pierwszej spółce spin-off, która powstała na Uniwersytecie Warszawskim, oferującej m.in. badania mikrobiologiczne dla muzeów i archiwów. Jakie były początki tej inicjatywy i jak ona się rozwinęła?

Początki przedsięwzięcia to działalność naukowa prof. Aleksandry Skłodowskiej[11], która m.in. prowadziła przewody doktorskie z zakresu ochrony dzieł sztuki. Spółka RDLS powstała w 2014 r. z jej inicjatywy, a także dr. Łukasza Drewniaka, dziś profesora na UW, oraz Łukasza Rodka, obecnie pełniącego funkcję jej prezesa. Naszą siedzibą jest Wydział Biologii UW i zajmujemy się działaniami związanymi z mikrobiologią. W rozmowie skupiłyśmy się na zagrożeniach mikrobiologicznych dla muzeów i archiwów, ale nie zapominajmy, że mikroorganizmy mają również pozytywny wpływ na otaczające nas środowisko. Drugą „nogą" działalności RDLS jest projektowanie i budowa naturalnych oczyszczalni ścieków,

[11] Prof. dr hab. Aleksandra Danuta Skłodowska (1953–2024) – wybitna specjalistka w dziedzinie mikrobiologii i biotechnologii środowiskowej, inicjatorka Pracowni Analizy Skażeń Środowiska na Wydziale Biologii Uniwersytetu Warszawskiego, którą kierowała przez 16 lat.

które są łatwe i tanie w obsłudze. Ze względu na relatywnie duży rozmiar najlepiej sprawdzają się na terenach wiejskich. Za wdrożenie tej technologii otrzymaliśmy w 2025 r. tytuł Innowatora Mazowsza. Do tej pory wybudowaliśmy pięć takich oczyszczalni.



Zdjęcie 1. Nauka w służbie dziedzictwa kulturowego – dr Magdalena Dyda podczas badania arrasów wawelskich.

Źródło: archiwum M. Dydy.

Jeżeli chodzi o współpracę w zakresie badań mikrobiologicznych i mikologicznych, to w ciągu ostatnich 12 lat wykonaliśmy tysiące analiz dla krajowych ośrodków naukowych, instytucji muzealnych, archiwalnych, bibliotecznych oraz administracji państwowej. Badaliśmy na przykład tak cenne eksponaty jak arrasy na Wawelu, Statuty Łaskiego i Konstytucję 3 Maja ze zbiorów Archiwum Głównego Akt Dawnych czy Biblię Gutenberga w Muzeum Diecezjalnym w Pelplinie.

Od lat prowadzimy również szkolenia i warsztaty w instytucjach kultury, w tym wspólnie z Narodowym Instytutem Muzeów. Owocem wieloletniej współpracy z NIM jest poradnik dotyczący bezpieczeństwa mikrobiologicznego kolekcji, dostępny bezpłatnie w formie elektronicznej na stronach Instytutu[12].

W swojej działalności koncentrujemy się na badaniach wykonywanych dla instytucji krajowych, ale ma ona również wymiar transgraniczny. Realizowaliśmy projekty m.in. wspólnie z Biblioteką Narodową w Pradze, Archiwami Państwowymi w Budapeszcie oraz Słowacką Biblioteką Narodową.

[12] M. Dyda, *Zagrożenia mikrobiologiczne zbiorów muzealnych*, Warszawa 2020, https://nim.gov.pl/wydawnictwa/abc-zagrozenia-mikrobiologiczne-zbiorow-muzealnych [dostęp: 25 VIII 2026].

Dla osób zajmujących się zbiorami opracowaliśmy praktyczny przewodnik na wypadek niepożądanych zdarzeń[13]. Zaprezentowaliśmy w nim podstawowy zakres działań, jakie instytucja może wdrożyć, aby przygotować się na takie sytuacje. Nie uwzględniliśmy niestety warunków wojennych, gdyż publikacja powstała przed pełnoskalową inwazją Rosji na Ukrainę.

Rozmawiała: Daria Olender

Dr Magdalena Dyda

Doktor nauk biologicznych, specjalizuje się w mikrobiologii konserwatorskiej i prewencji zbiorów muzealnych, archiwalnych i bibliotecznych. Pracuje w RDLS – spółce spin-off Uniwersytetu Warszawskiego.

Autorka publikacji naukowych i popularyzatorskich. Współorganizatorka konferencji oraz warsztatów i wykładów skoncentrowanych na praktycznych metodach prewencji biologicznej i bezpieczeństwie zbiorów. Prowadzi badania, doradztwo i szkolenia z zakresu zagrożeń biologicznych, bezpieczeństwa zbiorów oraz prewencji konserwatorskiej dla instytucji opiekujących się zbiorami. Zajmuje się analizą różnorodności i aktywności mikroorganizmów zasiedlających budynki oraz ruchome obiekty zabytkowe wykonane z różnych materiałów, a także monitoringiem czynników fizykochemicznych i zanieczyszczenia mikrobiologicznego powietrza w budynkach.

Od ponad 10 lat współpracuje z instytucjami kultury w Polsce, m.in. Zamkiem Królewskim na Wawelu, Muzeum Łazienki Królewskie, Archiwami Państwowymi, Narodowym Instytutem Muzeów. Realizowała badania m.in. w ramach projektów „Wawel – dziedzictwo dla przyszłości", „Wielokulturowa Rzeczpospolita, Zamek Pieskowa Skała" oraz „Ratujemy Pelplińską Biblię Gutenberga". Od 2017 r. prowadzi szkolenia i warsztaty mikrobiologiczne w ramach współpracy z NIM.

[13] B.F. Zerek, *Guidelines for preparing an emergency protocol for libraries and archives*, https://bparchiv.hu/wp-content/uploads/2024/02/v4_emergency_protocol_guidelines_0.pdf [dostęp: 25 VIII 2026].

Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 35, s. 299–304
CC BY-NC-SA 4.0
https://doi.org/10.4467/20801335PBW.26.033.24182

VARIA

O bezpieczeństwie w zmieniającym się świecie

Przekrój zagadnień, o których dyskutowali uczestnicy III Międzynarodowej Konferencji Naukowej z cyklu „Współczesne bezpieczeństwo. Wyzwania. Szanse. Zagrożenia", sfinansowanej ze środków Ministerstwa Nauki i Szkolnictwa Wyższego w ramach programu „Wektory Nauki", był naprawdę szeroki. Od wniosków płynących z doświadczeń wojny rosyjsko-ukraińskiej, przez wojnę hybrydową, operacje w cyberprzestrzeni, znaczenie proxy wars dla stabilności świata, rolę obrony cywilnej we współczesnym konflikcie zbrojnym, po niekontrolowaną ekspansję sztucznej inteligencji i zagrożenia klimatyczne. Ideę tak wielowymiarowego ujęcia problematyki bezpieczeństwa wyjaśnia **dr hab. inż. Marian Żuber, prof. ANS**, przewodniczący Komitetu Organizacyjnego. Zwraca uwagę, że dynamiczny rozwój technologii, przemiany geopolityczne i społeczne oraz nasilające się kryzysy ekologiczne sprawiają, że tradycyjne, wąskie rozumienie obronności państwa nie odpowiada już aktualnym wyzwaniom.



III Międzynarodowa Konferencja Naukowa

„Współczesne bezpieczeństwo. Wyzwania. Szanse. Zagrożenia"

Nowy Sącz, 26–28 maja 2026 r.

TEMATYKA

Współczesne konflikty zbrojne i ich wpływ na bezpieczeństwo globalne i regionalne

- wojna Rosja–Ukraina i jej znaczenie dla bezpieczeństwa europejskiego – różne perspektywy,
- wojna Rosja–Ukraina – wojna dronów,
- konflikty zastępcze w polityce mocarstw globalnych,
- wojna hybrydowa i jej znaczenie we współczesnej polityce,
- wojny w cyberprzestrzeni i budowanie odporności na zagrożenia.

Ochrona ludności i bezpieczeństwo człowieka

- ochrona ludności w obliczu zagrożeń naturalnych,
- obrona cywilna i jej rola w czasie konfliktu zbrojnego,
- budowa systemu ochrony ludności i obrony cywilnej,
- system indywidualnej i zbiorowej ochrony ludności,
- ochrona ludności przed bronią niekonwencjonalną (CBRN),
- Unijny Mechanizm Ochrony Ludności.

Inne zagadnienia z obszaru współczesnego bezpieczeństwa

- globalne ocieplenie i możliwości adaptacji do zmian klimatycznych,
- odnawialne źródła energii i ich rola w walce ze zmianami klimatu,
- problemy bezpieczeństwa środowiskowego,
- sztuczna inteligencja (AI) i zagrożenia płynące z jej niekontrolowanej ekspansji,
- bezpieczeństwo personalne i ergonomia człowieka.

Daria Olender: Dlaczego Akademia Nauk Stosowanych zdecydowała się na organizację cyklu konferencji naukowych poświęconych tak szeroko rozumianym problemom bezpieczeństwa?

Dr hab. inż. Marian Żuber, prof. ANS: W obliczu dynamicznego rozwoju technologii i zmian geopolitycznych tradycyjne podejście do obronności państwa już nie wystarcza. Współczesne bezpieczeństwo obejmuje problematykę nie tylko konfliktów zbrojnych, lecz także kryzysów ekologicznych, globalnego ocieplenia, transformacji energetycznej czy masowych migracji. Wymaga to interdyscyplinarnego spojrzenia, łączącego dorobek nauk o bezpieczeństwie z naukami przyrodniczymi i technicznymi. Dziś mamy do czynienia z wojną hybrydową, cyberzagrożeniami, dronami oraz wykorzystaniem sztucznej inteligencji w działaniach destabilizacyjnych. Brakowało również – naszym zdaniem – platformy, która tak mocno łączyłaby świat teorii naukowych z doświadczeniem praktyków z wojskowości, obrony cywilnej i służb wewnętrznych. Naszymi celami były też edukacja przyszłych kadr oraz poszerzanie świadomości społecznej w zakresie ochrony ludności. Konferencja miała stać się bodźcem do wypracowania nowych procedur i modeli teoretycznych, które pomogą budować odporność państwa na poziomie jednostkowym, narodowym i ponadpaństwowym. W tym miejscu chcę podkreślić możliwości, jakie dał nam udział w projekcie finansowanym przez Ministra Nauki i Szkolnictwa Wyższego w ramach programu „Wektory Nauki". Przyznany grant pozwolił nadać temu przedsięwzięciu zdecydowanie większy prestiż.

Chciałbym również zwrócić uwagę, że konferencja jest wydarzeniem o dużej wartości dla lokalnej społeczności. Dzięki niej wzrasta znaczenie Nowego Sącza jako ośrodka nauki i zwiększają się szanse na rozwój lokalnych inicjatyw badawczych. Uczestnicy spotkania zostali zachęceni do współpracy z regionalnymi przedsiębiorstwami, co może zaowocować nowymi inwestycjami.

Na jakich zagadnieniach skupiono się podczas tegorocznej edycji?

Dyskusje podzieliliśmy na trzy obszary tematyczne. W pierwszym z nich, zatytułowanym „Współczesne konflikty zbrojne i ich wpływ na bezpieczeństwo globalne i regionalne", skupiliśmy się na analizie doświadczeń płynących z wojny rosyjsko-ukraińskiej, ze szczególnym uwzględnieniem

masowego użycia bezzałogowców, oraz na mechanizmach wojny hybrydowej, operacjach w cyberprzestrzeni i znaczeniu konfliktów zastępczych, tzw. proxy wars, dla stabilności Europy i świata. Z kolei panel pt. „Ochrona ludności i bezpieczeństwo człowieka" przeniósł ciężar dyskusji na poziom operacyjny i formalnoprawny. Prelegenci podjęli próbę zdefiniowania na nowo roli obrony cywilnej w czasie konfliktu zbrojnego. Przeanalizowano architekturę systemów ochrony zbiorowej, procedury reagowania na zagrożenia asymetryczne, wykorzystanie broni niekonwencjonalnej, a także efektywność operacyjną Unijnego Mechanizmu Ochrony Ludności. W ramach trzeciego bloku, zbiorczo określonego jako „Inne zagadnienia z obszaru współczesnego bezpieczeństwa", poruszyliśmy kwestie, które nie wynikają wprost z działań wojennych, ale mają bezpośredni wpływ na życie ludzkie. Kluczowym punktem była debata nad zagrożeniami związanymi z niekontrolowaną ekspansją sztucznej inteligencji. Istotne miejsce zajęła także analiza bezpieczeństwa środowiskowego, roli odnawialnych źródeł energii oraz strategii adaptacji do zmian klimatycznych i globalnego ocieplenia, skutkujących rosnącymi temperaturami, powodziami i suszami, które dotykają również nasz region. Proponując taki podział, staraliśmy się uwzględnić cały łańcuch zależności współczesnego bezpieczeństwa: od przyczyn, przez mechanizmy obronne, po globalne determinanty środowiskowe. Uczestnicy konferencji mogli wysłuchać ponad 60 referatów wygłoszonych przez ekspertów z Polski i zagranicy. Efektem tegorocznych obrad było nakreślenie kierunków dalszych badań naukowych oraz zaprezentowanie innowacyjnych rozwiązań organizacyjno-technicznych podnoszących poziom bezpieczeństwa w różnych sferach.

Czy obecność wybitnych ekspertów ze świata to rezultat współpracy Akademii Nauk Stosowanych z ośrodkami z zagranicy?

Tak. Stoją za tym lata osobistych kontaktów członków komitetu naukowego naszej konferencji z naukowcami ze świata, realizacji przez uczelnię wspólnych przedsięwzięć z ośrodkami zagranicznymi, a także wymian akademickich. Dużą rolę odegrała także renoma naszych tegorocznych współorganizatorów: Wojskowej Akademii Technicznej w Warszawie, Akademii Wojsk Lądowych we Wrocławiu oraz Uniwersytetu Przyrodniczego we Wrocławiu. Te instytucje mają potężną sieć globalnych powiązań naukowych. Taka współpraca gwarantuje wysoką jakość

merytoryczną oraz praktyczną wartość wyników prac naukowych. Ponadto znaczenie miała aktualność i uniwersalność poruszanej tematyki – wojna hybrydowa, cyberzagrożenia, ochrona ludności to palące tematy, które interesują specjalistów na całym świecie. W tym roku gościliśmy ekspertów m.in. z Norwegii, Litwy, Estonii, Ukrainy, Rumunii, Chorwacji, Słowacji oraz Stanów Zjednoczonych. Współpraca z zagranicą pozwala na lepsze zrozumienie wspólnych zagrożeń, a także otwiera drzwi do realizacji w Polsce międzynarodowych projektów badawczych.

Warto podkreślić, że w obradach wzięli udział również młodzi naukowcy z innych kręgów kulturowych – doktorant Politechniki Wrocławskiej pochodzący z Nigerii oraz student Uniwersytetu Wrocławskiego pochodzący z Indii. W tym miejscu chciałbym wyrazić uznanie dla pracy tłumaczy symultanicznych. Dzięki ich profesjonalizmowi i zaangażowaniu uczestnicy mogli lepiej przyswoić specjalistyczne, nierzadko ściśle branżowe, treści.

Uczestnicząc w konferencji, zauważyłam, jak wiele uwagi poświęca Pan Profesor młodym ludziom i jak dobry kontakt ma ze studentami.

Cieszę się, że to jest dostrzegalne! Dydaktyka to moja pasja. W studentach staram się zaszczepić ciekawość świata i pokazywać im, że nauki o bezpieczeństwie to nie tylko sucha teoria, lecz także realne życie. Uważam, że dobry dydaktyk to ten, który inspiruje i potrafi słuchać. Staram się więc skracać dystans, budować atmosferę wzajemnego zaufania i udowadniać młodym ludziom, że ich głos ma znaczenie – także w poważnych, międzynarodowych projektach. Relacja oparta na takich filarach pozwala stworzyć bezpieczną przestrzeń, w której studenci nie boją się zadawać trudnych pytań i chętnie się angażują w inicjatywy wykraczające poza standardowy program studiów. To działa zresztą w obie strony. Energia i zaangażowanie studentów dają mi napęd do działania.

Tradycją naszej konferencji stał się Dzień Studencki, podczas którego młodzi badacze mogą zaprezentować wyniki prac realizowanych w ramach kół naukowych. W tym roku najliczniejszą grupę stanowili członkowie Studenckiego Koła Naukowego „Bezpiecznik", działającego na Wydziale Inżynierii Kształtowania Środowiska i Geodezji Uniwersytetu Przyrodniczego we Wrocławiu. Obecność studentów na konferencji

oraz ich śmiałe interakcje z ekspertami to najlepszy dowód na to, że są oni integralną częścią społeczności akademickiej.

Czy organizatorzy planują wydanie publikacji pokonferencyjnych?

Pisemne utrwalenie dorobku naukowego wydarzenia to jeden z kluczowych wskaźników ewaluacji całego projektu, na co zwraca uwagę również Ministerstwo Nauki i Szkolnictwa Wyższego w programie Wektory Nauki. Przed konferencją wydaliśmy *Księgę abstraktów*, w której zgromadziliśmy syntetyczne opisy zaprezentowanych wyników badań. Publikację można bezpłatnie pobrać ze strony internetowej naszej uczelni, w zakładce wydawnictwa naukowego, oraz z witryny konferencji[1]. Autorom najlepszych wystąpień stworzyliśmy możliwość opublikowania pełnych wersji artykułów w recenzowanej monografii zbiorowej, która ukaże się w ciągu najbliższych miesięcy. Podobnie jak *Księga abstraktów* będzie ona dostępna w sieci. Zachęcam do śledzenia strony naszej uczelni!

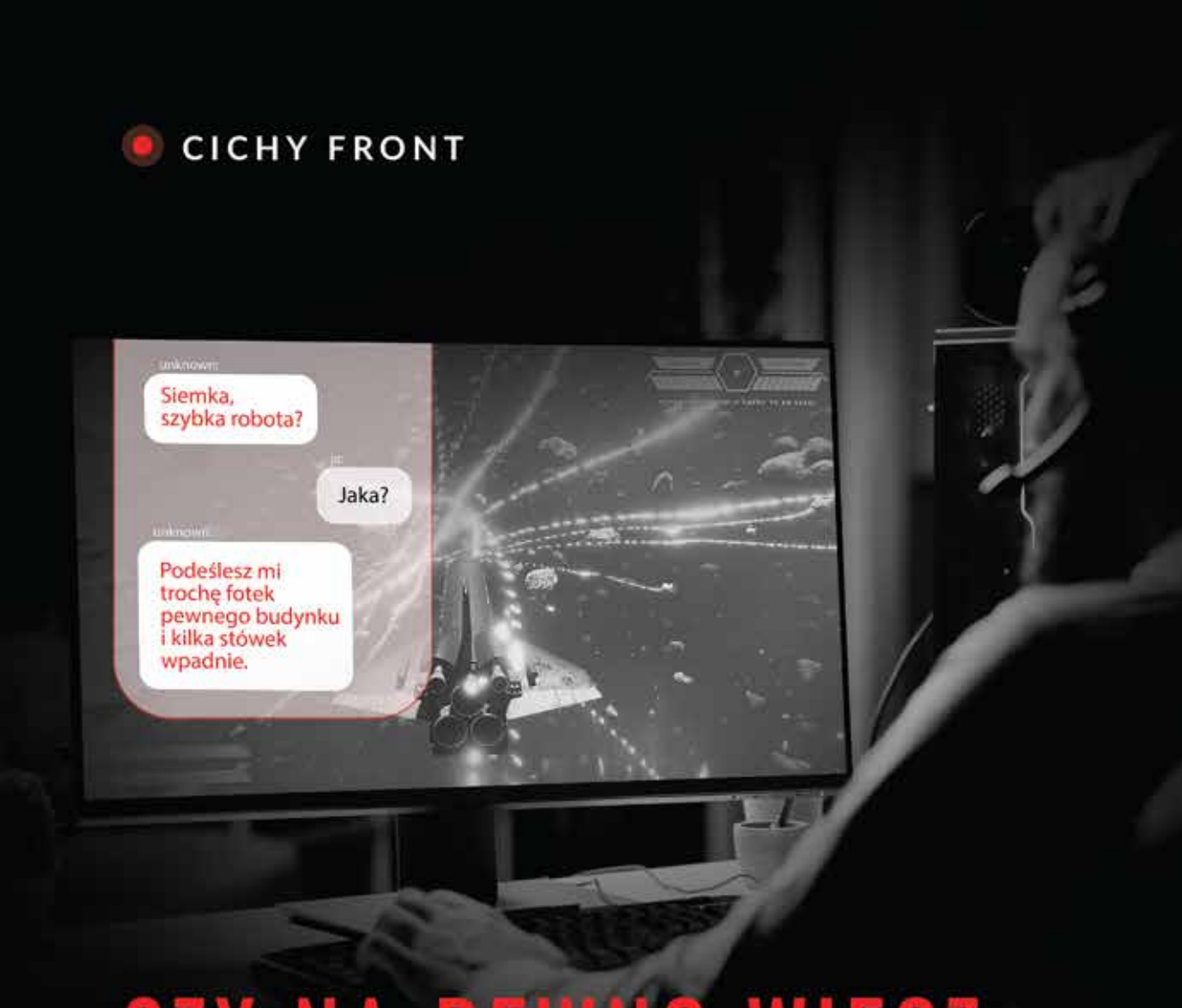
Rozmawiała: Daria Olender

Dr hab. inż. Marian Żuber, prof. ANS i UPWr

Doktor habilitowany w dziedzinie nauk społecznych w dyscyplinie nauki o bezpieczeństwie. Pracował w Wyższej Szkole Oficerskiej Wojsk Lądowych, a następnie Akademii Wojsk Lądowych we Wrocławiu, gdzie pełnił funkcje prodziekana Wydziału Nauk o Bezpieczeństwie i Wydziału Zarządzania. Obecnie wykłada na Uniwersytecie Przyrodniczym we Wrocławiu oraz w Akademii Nauk Stosowanych w Nowym Sączu. Autor wielu monografii, podręczników i artykułów z zakresu bezpieczeństwa narodowego i międzynarodowego. Organizator licznych konferencji naukowych w obszarze bezpieczeństwa (m.in. cyklu „Katastrofy naturalne i cywilizacyjne"). Jego zainteresowania badawcze obejmują: bezpieczeństwo narodowe i międzynarodowe, ochronę środowiska, terroryzm, broń masowego rażenia oraz bezpieczeństwo infrastruktury krytycznej.

[1] https://wydawnictwo.ans-ns.edu.pl; https://wspolczesnebezpieczenstwo.edu.pl/.

CICHY FRONT



CZY NA PEWNO WIESZ, DLA KOGO PRACUJESZ?

Nie zawsze zagrożenie wygląda jak w filmach.
Częściej zaczyna się od wiadomości.
Komentarza. Jednej decyzji.

Bądź czujny! Nie daj się wykorzystać!

www.cichyfront.gov.pl

Kampania społeczna „Cichy Front"
wspólna inicjatywa **Agencji Bezpieczeństwa Wewnętrznego i Telewizji Polskiej**
dotycząca zagrożeń hybrydowych ze strony służb specjalnych państw wrogich Polsce