Zbigniew Ciekanowski[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska
Wiesława Załoga[2]
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Warszawa
Martyna Zaroślak[3]
Uniwersytet w Siedlcach

https://doi.org/10.29316/9788368103373_22

ROLA WOJSK OBRONY CYBERPRZESTRZENI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA WOBEC ZAGROŻEŃ HYBRYDOWYCH

THE ROLE OF CYBER DEFENCE FORCES IN THE NATIONAL SECURITY SYSTEM IN THE FACE OF HYBRID THREATS

Streszczenie

Celem rozdziału jest określenie rzeczywistej roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa oraz zbadanie, czy są one jedynie wyspecjalizowanym komponentem militarnym, czy też pełnią funkcję węzłową w krajowym ekosystemie odporności na zagrożenia hybrydowe. Problem badawczy dotyczy zagadnienia, w jakim stopniu Wojska Obrony Cyberprzestrzeni wzmacniają zdolność

[1] https://orcid.org/0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl
[2] https://orcid.org/0000-0001-7758-0187, e-mail: wieslawa.zaloga@wat.edu.pl
[3] https://orcid.org/0000-0001-7693-8327, e-mail: martynazaroslak@gmail.com

państwa do zapobiegania, wykrywania, neutralizowania oraz odtwarzania skutków złożonych kampanii hybrydowych, obejmujących działania w cyberprzestrzeni, manipulację informacyjną, presję na infrastrukturę krytyczną oraz operacje prowadzone poniżej progu wojny. Zastosowano jakościową analizę instytucjonalno-prawną, krytyczny przegląd literatury polsko- i anglojęzycznej, analizę wtórną danych statystycznych z raportów CERT Polska i CSIRT GOV za lata 2020-2024 oraz studium przypadku incydentu dezinformacyjno-cybernetycznego związanego z fałszywą depeszą PAP z 31 maja 2024 r. Analiza potwierdza, że skuteczność Wojsk Obrony Cyberprzestrzeni nie wynika wyłącznie z posiadania zdolności technicznych, lecz z ich integracji z całym systemem bezpieczeństwa państwa, w tym z krajowymi CSIRT-ami, administracją publiczną, infrastrukturą krytyczną, sektorem prywatnym i strukturami sojuszniczymi. Empirycznie widoczny wzrost liczby incydentów w polskiej cyberprzestrzeni oraz narastanie zagrożeń mieszanych wskazują, że Wojska Obrony Cyberprzestrzeni powinny być traktowane jako komponent obrony państwa, odporności systemowej i wsparcia operacji połączonych, a nie wyłącznie jako narzędzie ochrony sieci resortu obrony.

Słowa kluczowe: bezpieczeństwo państwa, cyberbezpieczeństwo, zagrożenia hybrydowe, Wojska Obrony Cyberprzestrzeni, odporność, CSIRT, infrastruktura krytyczna

Abstract

The aim of chapter is to define the actual role of the Cyberspace Defence Forces in the state security system and to verify whether they should be understood merely as a specialised military component or rather as a nodal actor in the national resilience ecosystem against hybrid threats. The research problem concerns the extent to which the Cyberspace Defence Forces enhance the state's ability to prevent, detect, neutralise, and recover from complex hybrid campaigns involving cyber operations, information manipulation, pressure on critical infrastructure, and activities conducted below the threshold of war. The study uses qualitative institutional and legal analysis, a critical review of Polish- and English-language literature, secondary statistical analysis based on CERT Polska and CSIRT GOV reports for 2020-2024, and a case study of the cyber-disinformation incident related to the false PAP mobilisation dispatch on 31 May 2024. Findings: The study shows that the effectiveness of the Cyberspace Defence Forces depends not only on their technical capabilities but above all on their integration with the broader state security architecture, including national CSIRTs, public administration, critical infrastructure operators, the private sector and allied structures.

Keywords: state security, cybersecurity, hybrid threats, Cyberspace Defence Forces, resilience, CSIRT, critical infrastructure

Wstęp

Współczesne środowisko bezpieczeństwa jest kształtowane przez zjawiska, które wymykają się klasycznemu podziałowi na pokój i wojnę. W praktyce rośnie znaczenie działań prowadzonych poniżej progu otwartego konfliktu zbrojnego, łączących presję polityczną, operacje informacyjne, sabotaż, wrogą aktywność w cyberprzestrzeni i uderzenia w infrastrukturę krytyczną. Unia Europejska definiuje zagrożenia hybrydowe jako skoordynowane działania wymierzone w państwo lub instytucję przy użyciu zróżnicowanych, często łączonych środków, takich jak manipulacja informacyjna, cyberataki, presja ekonomiczna czy groźba użycia siły. Z kolei NATO uznaje cyberobronę za element odstraszania i obrony zbiorowej, a od szczytu w Warszawie w 2016 r. traktuje cyberprzestrzeń jako domenę operacyjną, w której Sojusz musi bronić się równie skutecznie jak na lądzie, morzu i w powietrzu. W sensie strategicznym oznacza to, że państwo nie może już oddzielać bezpieczeństwa militarnego od cyfrowego i informacyjnego, przeciwnie, musi myśleć o nich jako o jednym polu współzależnych oddziaływań (Bachmann i in., 2023; Hoffman, 2007).

W przypadku Polski skala wyzwania jest wyraźnie widoczna w danych operacyjnych. Według rocznego sprawozdania o cyberbezpieczeństwie w 2024 r. krajowe zespoły CSIRT zarejestrowały łącznie 111 660 incydentów bezpieczeństwa teleinformatycznego; sam CSIRT NASK odnotował 103 449 przypadków, CSIRT GOV 3 991, a CSIRT MON 4 220 (Ministerstwo Cyfryzacji, 2025). Oznacza to dalszy wzrost presji na państwowy ekosystem bezpieczeństwa oraz pokazuje, że problem cyberzagrożeń nie ma już charakteru niszowego, lecz systemowego. W warunkach utrzymującego się podwyższonego poziomu zagrożenia w cyberprzestrzeni oraz obowiązywania stopnia alarmowego CHARLIE-CRP zdolności obronne muszą być rozpatrywane w kategoriach stałej gotowości, a nie wyłącznie doraźnej reakcji (Ministerstwo Cyfryzacji, 2025). W tym kontekście kluczowego znaczenia nabiera wyspecjalizowany komponent militarny odpowiedzialny za ochronę i działania w cyberprzestrzeni. Zgodnie z informacjami Ministerstwa Obrony Narodowej, Wojska Obrony Cyberprzestrzeni realizują zadania w kluczowych obszarach związanych z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów teleinformatycznych (Ministerstwo Obrony Narodowej, 2022; Ministerstwo Obrony Narodowej, b.d.). W ich strukturze

znajduje się 12 podporządkowanych jednostek wojskowych, w tym wyspecjalizowane jednostki działań w cyberprzestrzeni „A" i „B", od 2024 r. trwa również formowanie jednostki „C" we Wrocławiu. WOC odpowiadają także za świadczenie usług teleinformatycznych na rzecz Sił Zbrojnych RP oraz za zapewnienie prawidłowego funkcjonowania CSIRT MON, prowadzącego całodobowy monitoring sieci resortu obrony. Przyjęte rozwiązania instytucjonalne potwierdzają, że Wojska Obrony Cyberprzestrzeni nie są jedynie uzupełnieniem klasycznych rodzajów sił zbrojnych, lecz stanowią istotny filar ochrony cyfrowego wymiaru działań militarnych oraz cyfrowego zaplecza państwa (Kuś, 2023).

Celem niniejszego rozdziału jest zatem odpowiedź na pytanie, jaka jest rzeczywista rola Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa wobec zagrożeń hybrydowych. Przyjęto hipotezę, że skuteczność WOC zależy przede wszystkim od stopnia ich integracji z szerszym systemem bezpieczeństwa państwa, a nie wyłącznie od własnych zdolności technicznych. Weryfikacja tej hipotezy wymaga połączenia perspektywy prawno-instytucjonalnej, strategicznej i empirycznej, dlatego w dalszej części zestawiono ustalenia literatury z aktualnymi rozwiązaniami organizacyjnymi oraz danymi o zagrożeniach i incydentach.

Przegląd literatury

W literaturze przedmiotu pojęcie zagrożeń hybrydowych ujmowane jest szeroko, jednak jego wspólny rdzeń stanowi łączenie środków wojskowych i pozawojskowych, jawnych i ukrytych, a także kinetycznych i niekinetycznych. Frank G. Hoffman wskazywał, że wojny hybrydowe charakteryzują się równoczesnym wykorzystaniem zróżnicowanych instrumentów oddziaływania, przy czym ich skuteczność wzrasta wraz z umiejętnym zacieraniem granic między stanem wojny a stanem pokoju. Nowsze ujęcia tego zagadnienia akcentują znaczenie tzw. szarej strefy działań, rozumianej jako przestrzeń celowych operacji prowadzonych poniżej progu formalnej wojny, lecz zarazem dostatecznie intensywnych, aby wpływać na decyzje polityczne, odporność społeczną oraz ciągłość funkcjonowania państwa. W tym kontekście Dominika Dziwisz trafnie lokuje cyberprzestrzeń w centrum rosyjskiej perspektywy działań typu grey zone, wskazując, że operacje cyfrowe są szczególnie użyteczne w sytuacji, gdy państwo dąży do osiągania efektów

strategicznych bez uruchamiania pełnoskalowej eskalacji (Dziwisz, 2024; Hoffman, 2007).

Drugi istotny nurt badań koncentruje się na relacji między wojną hybrydową a cyberoperacjami. Alan Brill i John Bennett podkreślają, że współczesne zagrożenia w cyberprzestrzeni stają się coraz bardziej złożone, wielowarstwowe oraz maskujące swój rzeczywisty cel, co utrudnia zarówno ich atrybucję, jak i szybkie podjęcie adekwatnej reakcji. Z kolei analizy dotyczące wojny rosyjsko-ukraińskiej wskazują, że cyberoperacje rzadko stanowią autonomiczne narzędzie rozstrzygające konflikt, lecz regularnie pełnią funkcję wzmacniającą wobec innych instrumentów oddziaływania: wspierają rozpoznanie, wpływają na świadomość społeczną, zakłócają świadczenie usług, obciążają administrację publiczną oraz generują presję psychologiczną. Matthias Schulze, analizując użyteczność działań cybernetycznych na poziomie strategicznym, operacyjnym i taktycznym, dochodzi do wniosku, że ich największa skuteczność ujawnia się w ścisłym powiązaniu z innymi narzędziami polityki państwa. Podobny kierunek interpretacyjny odnaleźć można u Wróblewskiego i Wiśniewskiego, którzy wskazują, że konflikt w Ukrainie istotnie zwiększył ryzyko cyberataków, dezinformacji i agresji informacyjnej, oddziałujących również na sektor publiczny oraz społeczeństwo w Polsce (Brill, Bennett, 2022; Schulze, 2020; Wróblewski, Wiśniewski, 2024).

Trzeci obszar badań obejmuje problematykę odporności oraz współpracy cywilno-wojskowej. Raport Joint Research Centre Komisji Europejskiej wskazuje, że odporność na zagrożenia hybrydowe nie może być budowana w sposób punktowy, lecz powinna mieć charakter systemowy, uwzględniający zależności i współzależności między poszczególnymi segmentami państwa i społeczeństwa. W praktyce oznacza to konieczność integrowania komponentów militarnego, administracyjnego, infrastrukturalnego oraz prywatnego. Csaba Krasznay podkreśla natomiast, że wojna rosyjsko-ukraińska unaoczniła szczególną podatność infrastruktury krytycznej, której ochrona w wielu przypadkach opiera się na zdolnościach cywilnych podmiotów cyberbezpieczeństwa. W konsekwencji skuteczna obrona wymaga rozwiniętej wymiany informacji, wspólnych standardów oraz mechanizmów integrujących wojskowe i cywilne zdolności ochronne. Obserwacja ta ma szczególne znaczenie dla Wojsk Obrony Cyberprzestrzeni, ponieważ ich

efektywność zależy nie tylko od potencjału technicznego jednostek wojskowych, lecz także od jakości współdziałania z instytucjami cywilnymi oraz sektorem prywatnym (Jungwirth i in., 2023; Krasznay, 2024). W polskiej literaturze problematyka organizacyjno-prawnej roli sił zbrojnych w obszarze cyberbezpieczeństwa została wyraźnie zarysowana przez Bartosza Kusia, jednak nadal brakuje opracowań łączących perspektywę normatywną, instytucjonalną i empiryczną w odniesieniu do zmian po 2024 r., w szczególności po przyjęciu nowej Strategii Cyberbezpieczeństwa RP oraz nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa w 2026 r. W rezultacie pozostaje dostrzegalna luka badawcza pomiędzy klasycznym ujęciem Wojsk Obrony Cyberprzestrzeni jako wyspecjalizowanego komponentu Sił Zbrojnych a analizą ich rzeczywistej funkcji w państwowym systemie reagowania na zagrożenia hybrydowe. Niniejszy rozdział zmierza do wypełnienia tej luki poprzez zestawienie ustaleń literatury przedmiotu z aktualnymi dokumentami strategicznymi oraz danymi operacyjnymi (Kuś, 2023).

Część empiryczna

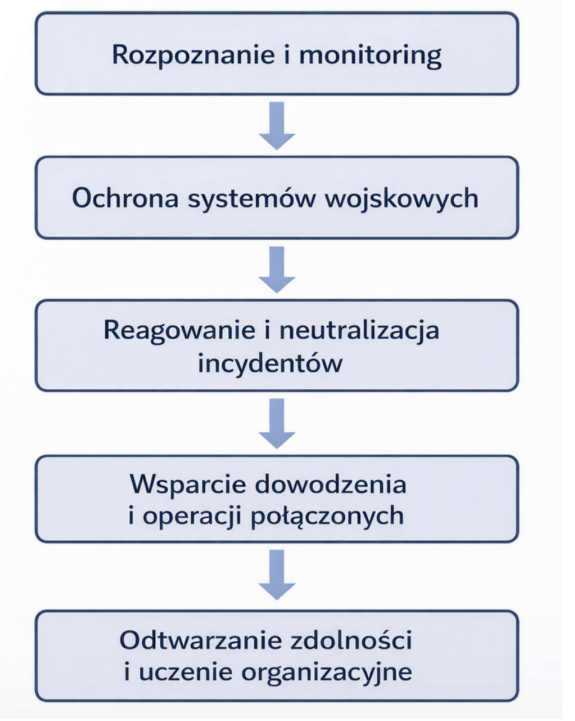
Część empiryczną oparto na triangulacji trzech typów materiału badawczego. Po pierwsze, przeprowadzono analizę instytucjonalno-prawną aktualnych dokumentów państwowych i sojuszniczych, obejmującą m.in. informacje dotyczące statusu Wojsk Obrony Cyberprzestrzeni, nowej Strategii Cyberbezpieczeństwa RP oraz zmian w krajowym systemie cyberbezpieczeństwa. Po drugie, wykorzystano wtórną analizę danych statystycznych zawartych w raportach CERT Polska i CSIRT GOV za lata 2020-2024. Po trzecie, zastosowano metodę studium przypadku, odnosząc ją do incydentu z 31 maja 2024 r., kiedy w oficjalnym serwisie PAP opublikowano fałszywą depeszę dotyczącą mobilizacji, zakwalifikowaną w oficjalnych materiałach jako cyberatak o istotnym wymiarze informacyjnym. Tak dobrany materiał badawczy pozwala ujmować Wojska Obrony Cyberprzestrzeni nie jako abstrakcyjny konstrukt organizacyjny, lecz jako podmiot funkcjonujący w konkretnym środowisku zagrożeń.

Punktem wyjścia analizy jest status formalnoprawny tej formacji. Ustawa o obronie Ojczyzny wskazuje Wojska Obrony Cyberprzestrzeni jako wyspecjalizowany komponent Sił Zbrojnych Rzeczypospolitej Polskiej, właściwy do realizacji pełnego spektrum działań w cyberprzestrzeni

(Rysunek 1). Na poziomie praktycznym oznacza to zdolność do prowadzenia działań obronnych, rozpoznawczych i ofensywnych, a zarazem odpowiedzialność za utrzymywanie oraz monitorowanie sieci i systemów teleinformatycznych Sił Zbrojnych RP, zarówno jawnych, jak i niejawnych. Dodatkowo, Wojska Obrony Cyberprzestrzeni zapewniają funkcjonowanie CSIRT MON, stanowiącego element krajowego systemu reagowania na incydenty odpowiedzialnego za obszar resortu obrony narodowej. Istotne znaczenie ma również logika programu CYBER.MIL 2.0, opartego na pięciu filarach: budowie struktur i infrastruktury, edukacji i szkoleniu, rekrutacji oraz aktywnej rezerwie, współpracy międzynarodowej, a także pozyskiwaniu narzędzi umożliwiających prowadzenie pełnego spektrum działań w cyberprzestrzeni. W ujęciu praktycznym wskazuje to, że Wojska Obrony Cyberprzestrzeni są projektowane jako formacja integrująca funkcje obronne, operacyjne, kadrowe i innowacyjne (Kuś, 2023).

W perspektywie systemowej rola Wojsk Obrony Cyberprzestrzeni wykracza poza ochronę wewnętrznych sieci wojskowych i obejmuje szerszy zakres funkcji istotnych z punktu widzenia bezpieczeństwa państwa. W tym kontekście można wyróżnić co najmniej cztery wzajemnie powiązane obszary ich oddziaływania. Po pierwsze, Wojska Obrony Cyberprzestrzeni zabezpieczają zdolność Sił Zbrojnych RP do zachowania ciągłości procesów dowodzenia, łączności, logistyki oraz zarządzania zasobami (Tabela 1). Po drugie, poprzez funkcjonowanie CSIRT MON stanowi istotny element krajowego systemu reagowania na incydenty cybernetyczne. Po trzecie, wzmacniają odporność państwa dzięki ochronie kluczowych technologii oraz rozwijaniu współpracy krajowej i międzynarodowej w obszarze cyberbezpieczeństwa. Po czwarte, pełnią funkcję odstraszającą, gdyż posiadanie wyspecjalizowanego komponentu cybernetycznego zwiększa koszt i ryzyko działań podejmowanych przez potencjalnego przeciwnika. Taki sposób ujmowania roli Wojsk Obrony Cyberprzestrzeni koresponduje z kierunkami wyznaczonymi w Strategii Cyberbezpieczeństwa RP z 10 marca 2026 r., przewidującej rozwój krajowej kryptografii i technologii kwantowych, rozwiązań chmurowych dla potrzeb cyberbezpieczeństwa, bezpieczeństwa łańcucha dostaw oraz centralnej ochrony przed atakami DDoS dla instytucji publicznych, w tym Sił Zbrojnych RP (Rada Ministrów, 2026; Ministerstwo Cyfryzacji, 2026). W konsekwencji, Wojska Obrony Cyberprzestrzeni

należy postrzegać jako istotny element szerszego programu budowy suwerenności technologicznej i cyberodporności państwa.



Rysunek 1. Model roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa

Źródło: opracowanie własne na podstawie Ministerstwo Cyfryzacji, 2025, 2026; Ministerstwo Obrony Narodowej, 2022, b.d.; NATO, 2016, 2024; Rada Unii Europejskiej, 2026.

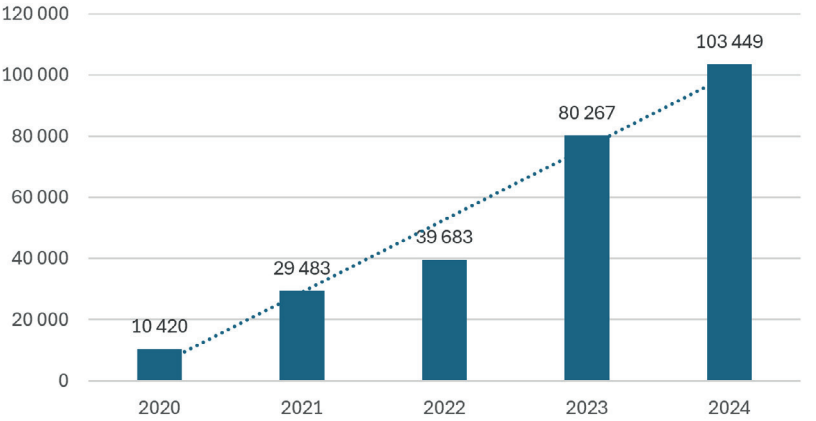
Tabela 1. Główne wymiary roli Wojsk Obrony Cyberprzestrzeni w systemie bezpieczeństwa państwa

Wymiar roli	Treść funkcji	Główni partnerzy instytucjonalni	Przykładowy efekt bezpieczeństwa
Strategiczny	budowa zdolności, planowanie, rozwój narzędzi, współpraca sojusznicza	MON, NATO, instytucje rządowe	wzrost odstraszania I odporności państwa
Operacyjny	monitorowanie, reagowanie, obsługa incydentów, wsparcie operacji połączonych	CSIRT MON, inne CSIRT-y poziomu krajowego, PCOC	skrócenie czasu wykrycia I reakcji

Wymiar roli	Treść funkcji	Główni partnerzy instytucjonalni	Przykładowy efekt bezpieczeństwa
Ochronny	ochrona sieci, systemów I łączności Sił Zbrojnych RP	jednostki wojskowe, logistyka, dowodzenie	utrzymanie ciągłości działania wojska
Systemowy	współpraca cywilno-wojskowa, wsparcie infrastruktury krytycznej, wymiana informacji	administracja publiczna, sektor prywatny, operatorzy IK	ograniczenie skutków kampanii hybrydowych
Kadrowo-rozwojowy	edukacja, szkolenia, aktywna rezerwa, rozwój kompetencji	uczelnie, partnerzy technologiczni, program CYBER.MIL	zwiększenie podaży specjalistów I zdolności adaptacyjnych

Źródło: opracowanie własne na podstawie Ministerstwo Cyfryzacji, 2025, 2026; Ministerstwo Obrony Narodowej, 2022, b.d.; NATO, 2016, 2024; Jungwirth i in., 2023; Krasznay, 2024.

Znaczenie Wojsk Obrony Cyberprzestrzeni staje się jeszcze bardziej widoczne, gdy zestawi się je z dynamiką incydentów odnotowywanych w polskiej cyberprzestrzeni. Dane CERT Polska wskazują na bardzo wyraźny wzrost liczby obsłużonych incydentów w latach 2020-2024: od 10 420 w 2020 r., przez 29 483 w 2021 r., 39 683 w 2022 r. i 80 267 w 2023 r., aż do 103 449 w 2024 r. Oznacza to, że w ciągu czterech lat liczba incydentów wzrosła niemal dziesięciokrotnie. Tendencji tej nie należy interpretować wyłącznie w kategoriach ilościowych. Tak wysokie tempo wzrostu świadczy o nasilającej się presji wywieranej na państwo przez aktywność wrogą, przestępczą oraz haktywistyczną, a więc przez zjawiska charakterystyczne dla współczesnego środowiska zagrożeń hybrydowych. W tej perspektywie Wojska Obrony Cyberprzestrzeni powinny być oceniane nie tylko przez pryzmat ich bezpośrednich działań operacyjnych, lecz również przez pryzmat zdolności do odciążania i wzmacniania całej architektury bezpieczeństwa cyfrowego państwa. Na Rysunku 2 przedstawiono dynamikę liczby incydentów obsłużonych przez CERT Polska w latach 2020-2024, ukazującą wyraźną tendencję wzrostową w analizowanym okresie.



Rysunek 2. Dynamika liczby incydentów obsłużonych przez CERT Polska w latach 2020-2024

Źródło: opracowanie własne na podstawie CERT Polska, 2025; Ministerstwo Cyfryzacji, 2025.

Na szczególną uwagę zasługuje sytuacja sektora publicznego. Z danych CERT Polska wynika, że w 2024 r. CSIRT NASK obsłużył 3 450 incydentów w podmiotach publicznych, co oznacza wzrost o 58% w porównaniu z rokiem poprzednim, przy czym najwyższą liczbę odnotowano w administracji publicznej – 1 911 przypadków. Z perspektywy nauk o bezpieczeństwie ustalenie to ma istotne znaczenie, ponieważ wskazuje, że ciężar zagrożeń nie koncentruje się wyłącznie w sektorze finansowym czy komercyjnym, lecz w coraz większym stopniu dotyczy struktur odpowiedzialnych za ciągłość funkcjonowania państwa. W konsekwencji wzrasta znaczenie komponentu militarnego zdolnego zarówno do współpracy z administracją publiczną, jak i do ochrony własnych systemów dowodzenia, zwłaszcza w sytuacji, gdy presja wywierana na sektor publiczny może stanowić element przygotowania pola pod szerszą operację hybrydową (Gaie, Karpiuk, Spaziani, 2025; Gaie, Karpiuk, Strizzolo, 2025). Szczególnie wymowne pozostaje studium przypadku fałszywej depeszy dotyczącej mobilizacji, opublikowanej 31 maja 2024 r. w oficjalnym serwisie PAP. W raporcie o stanie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej wskazano wprost, że doszło do dwukrotnego zamieszczenia fałszywej depeszy odnoszącej się do mobilizacji w Polsce. Znaczenie tego incydentu wykracza poza klasycznie rozumianą kategorię naruszenia systemu informatycznego, ponieważ jego potencjalnym skutkiem mogło być wywołanie paniki

informacyjnej, podważenie zaufania do oficjalnych kanałów komunikacji oraz wygenerowanie wtórnych efektów psychologicznych. Przypadek ten stanowi modelowy przykład splotu warstwy cybernetycznej i informacyjnej, a więc dokładnie tego rodzaju zjawiska, wobec którego niewystarczające byłyby zarówno wyłącznie techniczne zdolności typu SOC, jak i samodzielnie funkcjonujący aparat komunikacji strategicznej. Właśnie w takich sytuacjach niezbędny jest podmiot zdolny do równoczesnego rozumienia militarnego, technicznego i strategicznego wymiaru ataku.

Dopełnieniem tego obrazu jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa z 2026 r. Wprowadza ona Połączone Centrum Operacyjne Cyberbezpieczeństwa jako organ pomocniczy Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, rozszerza kompetencje krajowych CSIRT-ów, umożliwia tworzenie sektorowych CSIRT-ów oraz ustanawia krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Z punktu widzenia roli Wojsk Obrony Cyberprzestrzeni jest to zmiana szczególnie istotna, ponieważ wzmacnia mechanizmy koordynacji pomiędzy elementami systemu i przesuwa debatę z poziomu pytania o to, kto odpowiada za cyberbezpieczeństwo, na poziom pytania o sposób integrowania zdolności resortowych, sektorowych i narodowych w jeden spójny system działania. W tym sensie można stwierdzić, że otoczenie instytucjonalne dojrzewa do logiki, w jakiej Wojska Obrony Cyberprzestrzeni zostały powołane.

Dyskusja

Przeprowadzona analiza prowadzi do wniosku, że rola Wojsk Obrony Cyberprzestrzeni jest wyraźnie szersza niż tradycyjnie rozumiana ochrona wojskowych sieci teleinformatycznych. W ujęciu funkcjonalnym WOC pełnią co najmniej trzy równoległe role: podmiotu odpowiedzialnego za ochronę wojskowej ciągłości działania, komponentu państwowego systemu reagowania na incydenty oraz narzędzia wzmacniania odporności strategicznej państwa. Ujęcie to pozostaje zgodne z sojuszniczym rozumieniem cyberobrony, w którym cyberprzestrzeń traktowana jest jako domena operacyjna, a odpowiedź na zagrożenia powinna integrować poziomy polityczny, wojskowy i techniczny. Oznacza to, że w warunkach zagrożeń hybrydowych WOC nie powinny być sytuowane na obrzeżach państwowego systemu bezpieczeństwa, lecz w jego centrum, jako komponent integrujący wojskowe i pozawojskowe wektory odporności (NATO, 2024).

Jednocześnie materiał empiryczny wskazuje, że sama specjalizacja wojskowa nie jest wystarczająca. Współczesne cyberoperacje często dotyczą infrastruktury i usług, które formalnie pozostają poza resortem obrony, lecz mają zasadnicze znaczenie zarówno dla bezpieczeństwa państwa, jak i dla sprawności sił zbrojnych. Krasznay trafnie zauważa, że ochrona infrastruktury krytycznej bardzo często wymaga ścisłej koordynacji z cywilnymi dostawcami usług bezpieczeństwa oraz z sektorem prywatnym. Analogiczny kierunek wzmacnia dyrektywa NIS2, która rozszerza ramy ochrony na osiemnaście sektorów krytycznych i nakłada na państwa obowiązek budowy strategii, zdolności oraz mechanizmów współpracy i raportowania. W przypadku Polski oznacza to, że WOC muszą funkcjonować w środowisku gęstej sieci relacji z krajowymi CSIRT-ami, sektorowymi CSIRT-ami, administracją publiczną, operatorami usług kluczowych oraz partnerami prywatnymi. Im silniejsze są te relacje, tym większa jest skuteczność WOC, im słabsze, tym większe staje się ryzyko, że formacja pozostanie wprawdzie bardzo sprawna technicznie, lecz operacyjnie odizolowana (Krasznay, 2024).

Drugim istotnym problemem pozostają zasób kadrowy oraz transfer kompetencji. Program CYBER.MIL 2.0 już w 2022 r. eksponował rekrutację i aktywną rezerwę jako jeden z pięciu filarów rozwoju, co należy interpretować jako pośrednie przyznanie, że zdolności cybernetyczne nie mogą być budowane wyłącznie w klasycznej logice etatowej i koszarowej. Wysoko wykwalifikowani specjaliści funkcjonują bowiem na rynku cywilnym, w ośrodkach badawczych, firmach technologicznych i organizacjach eksperckich, a wojskowy komponent cyberbezpieczeństwa musi być zdolny do przyciągania, czasowego angażowania i utrzymywania tego zasobu. Z tej perspektywy WOC są nie tylko formacją operacyjną, lecz również platformą organizacyjną służącą łączeniu środowiska wojskowego, technologicznego i naukowego. W przeciwnym razie nawet najlepiej zaprojektowana struktura prawna nie przełoży się na rzeczywistą zdolność działania w warunkach gwałtownej ewolucji zagrożeń.

Trzecia kwestia dotyczy prawno-strategicznej logiki działań prowadzonych poniżej progu wojny. Definicje zagrożeń hybrydowych eksponują ich niejednoznaczność, trudność atrybucji oraz celowe utrzymywanie się poniżej progu, który wywoływałby jednoznaczną reakcję zbrojną. To właśnie sprawia, że WOC muszą działać w przestrzeni szczególnie wymagającej:

wystarczająco stanowczo, aby chronić państwo, a jednocześnie w zgodzie z krajowymi i międzynarodowymi ograniczeniami użycia siły oraz w ścisłej współpracy z władzami cywilnymi. NATO dopuszcza, że skumulowany efekt istotnych złośliwych działań cybernetycznych może w określonych okolicznościach zostać uznany za zbrojną napaść, jednak każdorazowo ocena ta ma charakter polityczno-strategiczny. Z perspektywy polskiej oznacza to potrzebę dalszego rozwijania doktryn, procedur decyzyjnych oraz zasad współdziałania WOC z innymi instytucjami państwa w sytuacjach niejednoznacznych, typowych dla presji hybrydowej (Dziwisz, 2024; NATO, 2024).

Czwarty wątek ma charakter rozwojowy i odnosi się do państwowej suwerenności technologicznej. Strategia Cyberbezpieczeństwa RP z 2026 r. akcentuje rozwój krajowej kryptografii, migrację do kryptografii postkwantowej, bezpieczeństwo łańcucha dostaw oraz rozwój rodzimych technologii. Z punktu widzenia WOC jest to zmiana o znaczeniu fundamentalnym. Formacja ta nie może być bowiem oceniana wyłącznie przez pryzmat bieżącego reagowania na incydenty, lecz również jako uczestniczka długofalowej polityki budowy narodowych kompetencji technologicznych. W warunkach rywalizacji geopolitycznej zależność od zewnętrznych rozwiązań, nieprzejrzystych łańcuchów dostaw czy obcych standardów kryptograficznych może sama w sobie stać się źródłem podatności. W tym sensie rozwój WOC oznacza jednocześnie rozwój wojskowych zdolności operacyjnych oraz wzmacnianie państwowej autonomii technologicznej.

Wyniki badania pozwalają zatem uznać hipotezę roboczą za potwierdzoną. O skuteczności WOC nie decyduje wyłącznie poziom militarnej specjalizacji ani liczba jednostek organizacyjnych, lecz zdolność do działania w logice sieciowej, obejmującej współpracę z administracją, krajowymi i sektorowymi CSIRT-ami, operatorami infrastruktury krytycznej, partnerami technologicznymi oraz strukturami sojuszniczymi. Innymi słowy, WOC są najskuteczniejsze wtedy, gdy pozostają jednocześnie formacją wojskową i instytucją systemową.

Wnioski

Przeprowadzona analiza prowadzi do kilku podstawowych wniosków. Wojska Obrony Cyberprzestrzeni należy traktować jako trwały i konieczny element systemu bezpieczeństwa państwa, a nie jedynie wyspecjalizowaną

strukturę ochrony teleinformatycznej resortu obrony. Ich rola ma charakter wielopoziomowy i obejmuje zarówno obronę infrastruktury wojskowej, wsparcie krajowego reagowania na incydenty, udział w budowie odporności państwa, jak i wzmacnianie odstraszania. Dynamika incydentów odnotowywanych w latach 2020-2024 dowodzi, że zagrożenia wobec Polski mają charakter systemowy i ciągły, co uzasadnia dalsze wzmacnianie wyspecjalizowanych zdolności wojskowych w cyberprzestrzeni. Przypadki takie jak fałszywa depesza PAP pokazują ponadto, że współczesne ataki coraz częściej łączą wymiar cybernetyczny i informacyjny, a skuteczna odpowiedź wymaga integracji zasobów militarnych, technicznych i komunikacyjnych. Przyszła skuteczność Wojsk Obrony Cyberprzestrzeni będzie natomiast zależała od jakości współpracy cywilno-wojskowej, rozwoju kadr, budowy krajowych technologii oraz efektywnego włączenia formacji w rozwijającą się architekturę krajowego systemu cyberbezpieczeństwa i Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (Kancelaria Sejmu, 2018; Rada Ministrów, 2026; Ministerstwo Cyfryzacji, 2026)

Z perspektywy praktycznej oznacza to potrzebę dalszego rozwoju wspólnych ćwiczeń z administracją publiczną i operatorami usług kluczowych, doprecyzowania zasad wymiany informacji między komponentami wojskowym i cywilnym, budowy mechanizmów szybkiego pozyskiwania kompetencji eksperckich oraz wdrożenia mierników oceny skuteczności WOC, wykraczających poza prostą statystykę incydentów. W naukach o bezpieczeństwie rozdział wzmacnia tezę, że cyberbezpieczeństwo państwa w epoce zagrożeń hybrydowych nie jest sumą odrębnych działań technicznych, lecz rezultatem zdolności do organizacyjnego integrowania narzędzi wojskowych, administracyjnych, prawnych i społecznych. To właśnie w tej przestrzeni Wojska Obrony Cyberprzestrzeni odgrywają rolę strategicznie pierwszoplanową.

Literatura

1. Bachmann, S.-D. D., Putter, D., Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy, 14*(5), 858-869. https://doi.org/10.1111/1758-5899.13257
2. Brill, A., Bennett, J. (2022). Understanding hybrid warfare in cyberspace: Building resilience through understanding. W: *Building cyber*

resilience against hybrid threats. *NATO Science for Peace and Security Series D: Information and Communication Security*. IOS Press. https://doi.org/10.3233/NICSP220016

3. CERT Polska. (2025). *Annual report 2024*. NASK – Państwowy Instytut Badawczy.
4. CSIRT GOV. (2025). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*. Agencja Bezpieczeństwa Wewnętrznego.
5. Dziwisz, D. (2024). Rethinking future conflicts: The cyber grey zone from the Russian perspective. *Politeja, 21*(5), 281-309. https://doi.org/10.12797/Politeja.21.2024.92.13
6. Gaie, C., Karpiuk, M., Spaziani, A. (2025). Cybersecurity in France, Poland and Italy. *Studia Iuridica Lublinensia, 34*(1), 73-95. https://doi.org/10.17951/sil.2025.34.1.73-95
7. Gaie, C., Karpiuk, M., Strizzolo, N. (2025). Cybersecurity of public sector institutions. *Prawo i Więź, 53*(6), 347-362. https://doi.org/10.36128/PRIW.VI53.1129
8. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
9. Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., Giannopoulos, G. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. Publications Office of the European Union. https://doi.org/10.2760/37899
10. Kancelaria Sejmu. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1560 z późn. zm.)
11. Krasznay, C. (2024). The role of civilian cybersecurity companies in military cyber operations. *Land Forces Academy Review, 29*(1), 1-10. https://doi.org/10.2478/raft-2024-0001
12. Kuś, B. (2023). Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo: Zagadnienia organizacyjno-prawne. *Cybersecurity and Law, 10*(2), 32-50. https://doi.org/10.35467/cal/174908
13. Ministerstwo Cyfryzacji. (2025). *Krajobraz cyberprzestrzeni: Roczne sprawozdanie o cyberbezpieczeństwie*. Pobrane z: https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie (dostęp: 12.02.2026).

14. Ministerstwo Cyfryzacji. (2026). *Nowa strategia cyberbezpieczeństwa: Polska wzmacnia ochronę przed cyberatakami*. Pobrane z: https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami (dostęp: 12.02.2026).
15. Ministerstwo Obrony Narodowej. (2022). *Wojska Obrony Cyberprzestrzeni rozpoczynają działalność*. Pobrane z: https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc (dostęp: 12.02.2026).
16. Ministerstwo Obrony Narodowej. (b.d.). *Wojska Obrony Cyberprzestrzeni*. Pobrane z: https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni (dostęp: 12.02.2026).
17. NATO. (2016). *Warsaw Summit Communiqué. North Atlantic Treaty Organization*. Pobrane z: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique (dostęp: 12.02.2026).
18. NATO. (2024). *Cyber defence. North Atlantic Treaty Organization*. Pobrane z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (dostęp: 12.02.2026).
19. Rada Ministrów. (2026). *Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Monitor Polski, poz. 309. Pobrane z: https://monitorpolski.gov.pl/MP/2026/309 (dostęp: 12.02.2026).
20. Rada Unii Europejskiej. (2026). *Hybrid threats*. Pobrane z: https://www.consilium.europa.eu/en/policies/hybrid-threats/ (dostęp: 12.02.2026).
21. Schulze, M. (2020). Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. W: *2020 12th International Conference on Cyber Conflict* (s. 183-197). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon49761.2020.9131733
22. Wróblewski, W., Wiśniewski, M. (2024). Cybersecurity in the context of hybrid warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. *Central European Journal of Security Studies, 1*(1), 48-60. https://doi.org/10.15804/CEJSS.2023105