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

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

BUDOWA STRATEGICZNEGO BEZPIECZEŃSTWA CYBEROBRONY SIŁ ZBROJNYCH RP

BUILDING STRATEGIC CYBER DEFENCE CAPABILITIES FOR THE POLISH ARMED FORCES

Streszczenie

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

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

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

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

Abstract

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

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

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

Wstęp

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozwój cyberbezpieczeństwa w NATO i Siłach Zbrojnych RP

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

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

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

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

Europejska polityka w zakresie cyberobrony składa się z czterech filarów:

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

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

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

Program CYBER.MIL.PL tworzą:

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

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

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

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

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

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

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

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

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

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

Powstanie i rozwój Wojsk Obrony Cyberprzestrzeni

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

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

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

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

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

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

Pod DKWOC podlegają następujące jednostki:

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

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

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

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

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

Podsumowanie

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

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

Literatura

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

Akty prawne

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

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

Netografia

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

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