Bartosz Kuś*

Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne

Streszczenie

Współcześnie istotną rolę zarówno w państwie, jak i w społeczeństwie odgrywają systemy teleinformatyczne. Bezpieczeństwo państwa militarne i pozamilitarne, zewnętrzne i wewnętrzne zyskało dodatkowy wymiar w postaci cyberprzestrzeni. Jednym z podstawowych celów Rzeczypospolitej Polskiej jest zapewnienie bezpieczeństwa obywatelom. Ochrona niepodległości państwa i niepodzielności jego terytorium oraz zapewnienie bezpieczeństwa i nienaruszalności jego granic są konstytucyjnymi zadaniami organów władzy publicznej. Podstawowym elementem systemu obronnego państwa uczestniczącym w realizacji polityk bezpieczeństwa i obronnej są Siły Zbrojne Rzeczypospolitej Polskiej. Ustawowym zadaniem tej formacji jest m.in. ochrona i obrona cyberprzestrzeni. Specjalistycznym komponentem Sił Zbrojnych RP są wojska obrony cyberprzestrzeni. Proces tworzenia tej kategorii wojsk nie został jeszcze zakończony.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, siły zbrojne, ochrona i obrona cyberprzestrzeni

* Dr Bartosz Kuś, adiunkt, Katedra Prawa Administracyjnego, Wydział Prawa, Prawa Kanonicznego i Administracji, Katolicki Uniwersytet Lubelski Jana Pawła II.

Wstęp

Bezpieczeństwo to uniwersalna wartość dotycząca nieskończonej liczby podmiotów. Równie rozległe są kategorie (rodzaje) bezpieczeństwa możliwe do wyróżnienia w zależności od sfery aktywności danego podmiotu. Największe przypisuje się bezpieczeństwu jednostki, grupy społecznej i państwa. Od zarania dziejów ludzkości bezpieczeństwo jednostki wiązało się z procesami państwowotwórczymi. Tworzenie przez ludzi większych organizacji (społeczności sąsiedzkiej, rodu, plemienia, a ostatecznie państwa) powinno być rozpatrywane w głównej mierze z punktu widzenia działań mających na celu zapewnienie bezpieczeństwa[1].

W literaturze zauważono, że natura bezpieczeństwa międzynarodowego i konfliktów pozostaje niezmienna. Poszczególne państwa permanentnie uwikłane są w rywalizację militarną i gospodarczą, konflikty zbrojne wciąż wydają się nieuniknione, dylematy bezpieczeństwa pojawiają się nieustannie i dlatego konieczne jest balansowanie między nimi. Zmienił się sposób działania, konflikty toczą się w nowy, innowacyjny i radykalnie odmienny sposób[2].

W ostatnich latach na znaczeniu zyskała koncepcja wojny hybrydowej spopularyzowana przez Franka Hoffmana, który stwierdził, że: „[...] zagrożeniem hybrydowym jest, gdy jakikolwiek adwersarz używający kombinacji broni konwencjonalnej, nieregularnej taktyki, terroryzmu i przestępczości, w tym samym czasie i na tym samym polu bitwy, celem osiągnięcia celów politycznych”[3]. Tego rodzaju konflikty mogą być prowadzone zarówno przez podmioty państwowe, jak i pozapaństwowe, przez pojedyncze oddziały, a także złożone formacje. Walka prowadzona jest z wykorzystaniem taktyk partyzanckich połączonych z nowoczesnymi technologiami wojskowymi[4].

Termin „wojna hybrydowa” jest pojęciem spornym i nie istnieje jej powszechnie przyjęta definicja. Krytykowany jest za brak klarowności pojęciowej,

1 M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016, s. 17.

2 A. Bilal, *Wojna hybrydowa – nowe zagrożenia, złożoność i „zaufanie” jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html [dostęp: 10.05.2023].

3 Cyt. za: J. Hajduk, T. Stępniewski, *Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty*, „Studia Europejskie” 2015, nr 4, s. 135 i nast.

4 S. Gardocki, J. Wrona, *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji” 2020, nr 2, s. 33 i nast.

bycie jedynie chwytliwym zwrotem lub słowem wytrychem i niewnoszenie niczego wyraźnie nowego do debat politycznych. Niemniej jednak koncepcja ta pozwala na dokonanie kluczowych spostrzeżeń na temat współczesnych i przyszłych wyzwań w dziedzinie bezpieczeństwa i obrony. W prostym ujęciu wojna hybrydowa polega na współdziałaniu lub połączeniu konwencjonalnych i niekonwencjonalnych instrumentów siłowych i dywersyjnych. Wspomniane instrumenty lub narzędzia są łączone w zsynchronizowany sposób, żeby wykorzystać słabe punkty przeciwnika i osiągnąć efekt synergii. Charakteryzując wojnę hybrydową, wskazuje się umiejętność wykorzystania nowoczesnych technologii w działaniach taktycznych i strategicznych, niejednokrotnie wykorzystywana jest również walka informacyjna obejmująca działania mające na celu wpłynięcie na przeciwnika, jego zasoby informacyjne, systemy informatyczne i sieci komputerowe[5].

Systemy teleinformatyczne odgrywają współcześnie istotną rolę zarówno w państwie, jak i w społeczeństwie, służą nie tylko do komunikowania się, lecz także do realizacji zadań publicznych czy prowadzenia działalności gospodarczej. Ochrona cyberbezpieczeństwa postrzeganego jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy jest zarówno zadaniem, jak i wyzwaniem[6].

Powyższe oznacza, że współcześnie bezpieczeństwo państwa militarne i pozamilitarne, zewnętrzne i wewnętrzne zyskało dodatkowy wymiar, oprócz lądu, wody, powietrza i przestrzeni kosmicznej – cyberprzestrzeń. Stanowi ona pole konfliktu z innymi państwami czy wrogimi organizacjami (grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi)[7]. Obejmuje przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne[8] wraz z powiązaniami między nimi

5 Ibidem.

6 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, s. 13.

7 *Doktryna bezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 4, 7; Konstytucja RP z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483, z późn. zm., art. 5.

8 Systemy teleinformatyczne to zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci – zob. *Doktryna bezpieczeństwa Rzeczypospolitej...*, s. 7.

oraz relacjami z użytkownikami[9]. Cyberprzestrzeń Rzeczypospolitej Polskiej to terytorium państwa polskiego oraz miejsca, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią Polski podlegające polskiej jurysdykcji)[10]. W dobie społeczeństwa informacyjnego zapewnienie bezpieczeństwa w cyberprzestrzeni, w tym świadczenia usług cyfrowych czy też korzystania ze środków komunikacji elektronicznej, należy do podstawowych obowiązków państwa. Zagwarantowanie cyberbezpieczeństwa wymaga podejścia holistycznego wykorzystującego narzędzia nie tylko tej konkretnej dziedziny. Zadania ukierunkowane na osiągnięcie strategicznego celu, tj. zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym[11].

Zapewnienie bezpieczeństwa obywatelom zostało wskazane przez ustawodawcę konstytucyjnego jako jeden z podstawowych celów Rzeczypospolitej[12]. Cele te zostały sformułowane w postaci zasad o charakterze programowym. Wskazują kierunki działania państwa, nie określają jednak środków i sposobów ich realizacji. Bezpieczeństwo należy rozumieć jako stan dający poczucie pewności i stabilności oraz ochrony. W zakres tego pojęcia wchodzi m.in. bezpieczeństwo polityczne, militarne, socjalne i ekologiczne. Państwo ma w pierwszej kolejności zapewnić bezpieczeństwo własnym obywatelom. Jednakże jego zakres jest większy. Jeżeli zapewnienie bezpieczeństwa polega na ochronie praw konstytucyjnych przysługujących każdej osobie, niezależnie od

9 Zob. 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., Dz.U. 2022, poz. 2091, z późn. zm., art. 2, ust. 1b; Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, t.j., ibidem 2017, poz. 1928, z późn. zm., art. 2, ust. 1a; Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, t.j., ibidem, poz. 1897, z późn. zm., art. 3, ust. 1, pkt 4. Cyberprzestrzeń jest przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych. Pozwala jej użytkownikom na komunikację w sieci i nawiązywanie relacji w czasie rzeczywistym. Cyberprzestrzeń jest środowiskiem wymiany informacji za pomocą sieci i systemów komputerowych. Cyberprzestrzeń jest wymiarem aktywności, w którym wszelkie działania odbiegają charakterem od środowiska fizycznego – zob. M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 1–2, s. 59.

10 *Doktryna bezpieczeństwa Rzeczypospolitej Polskiej...*, s. 7.

11 Ibidem, s. 14.

12 Konstytucja RP z dnia 2 kwietnia 1997..., art. 5.

obywatelstwa, to trudno wyobrazić sobie realizację tego obowiązku wyłącznie wobec obywateli polskich[13].

Ochrona niepodległości państwa i niepodzielności jego terytorium oraz zapewnienie bezpieczeństwa i nienaruszalności jego granic są konstytucyjnymi zadaniami Prezydenta RP, Rady Ministrów oraz innych organów władzy publicznej[14]. Realizacja zadań z dziedziny obronności państwa należy do wszystkich organów władzy i administracji rządowej oraz innych organów i instytucji państwowych, organów samorządu terytorialnego, przedsiębiorców, organizacji pozarządowych i innych podmiotów, a także do każdego obywatela[15]. Podstawowym elementem systemu obronnego RP uczestniczącym w realizacji polityk bezpieczeństwa i obronnej są siły zbrojne. Formacja ta realizuje zadania w zakresie ochrony niepodległości państwa, niepodzielności jego terytorium oraz zapewnienia bezpieczeństwa i nienaruszalności jego granic[16]. Właściwie funkcjonujące siły zbrojne stanowią jeden z filarów bezpieczeństwa każdego państwa, w tym bezpieczeństwa informacyjnego. Osiągnięciu takiego stanu rzeczy powinny służyć m.in. stosowne rozwiązania prawne. Na gruncie sformułowanych uwag jest aktualne zagadnienie zależności pomiędzy funkcjonowaniem Sił Zbrojnych RP a zapewnieniem cyberbezpieczeństwa. Wagę podjętej tematyki uzasadnia też niedawna zmiana stanu prawnego polegająca na uchwaleniu nowej, fundamentalnej regulacji prawnej – ustawy o obronie Ojczyzny, stanowiącej niepoddany jeszcze w wystarczającym stopniu badaniom obszar.

Struktura organizacyjna Sił Zbrojnych RP a cyberbezpieczeństwo

Wykorzystanie wojska do wsparcia władz publicznych w utrzymaniu lub do przywrócenia pożądanego poziomu bezpieczeństwa publicznego ma dosyć długą tradycję, także w Polsce. Dzieje się tak, pomimo że żołnierze poza formacjami żandarmerii nie są szkoleni do wykonywania tego typu zadań, a sprzęt

13 P. Tuleja [w:] P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziewicz, P. Tuleja, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. 2, LEX/el. 2021, art. 5.

14 M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3, s. 17–18.

15 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. 2022, poz. 2305, art. 7.

16 Ibidem, art. 11, ust. 4.

użytkowany przez siły zbrojne jest przeznaczony do sprawnego wykonywania zadań o charakterze militarnym. Z punktu widzenia władz publicznych wojsko to poważna organizacja o charakterze instytucjonalnym, do tego zorganizowana hierarchicznie, zdyscyplinowana i w znacznej mierze dyspozycyjna. Siły zbrojne są wyposażone w wyspecjalizowane środki techniczne oraz różnorodne uzbrojenie, którego zazwyczaj nie mają inne funkcjonujące w państwie formacje zmilitaryzowane. Możliwość użycia tego sprzętu może pozwolić na reakcję na występujące w obecnych czasach zagrożenia bezpieczeństwa wewnętrznego, którym nie byłby w stanie przeciwstawić się inny podmiot organizacyjny[17].

Cyberbezpieczeństwo jako jeden z celów strategicznych w obszarze bezpieczeństwa naszego państwa służy zapewnieniu ochrony głównym sektorom gospodarki, obywatelom oraz przedsiębiorcom. Jest to obszar wymagający stałego rozwoju i rozbudowy. Andrzej Nowak zauważa, że współcześnie trudno nie zgodzić się z tezą, że bezpieczeństwo informacyjne jest jednym z wielu elementów potencjału obronnego państwa, a co za tym idzie, jednym z podsystemów operacyjnych wsparcia bezpieczeństwa narodowego. Jeżeli głównym elementem tego systemu są siły zbrojne, to komponent bezpieczeństwa informacyjnego jest jednym z najważniejszych czynników kształtowania tego systemu[18].

Siły zbrojne są zhierarchizowaną, umundurowaną formacją zbrojną, stanowiącą wyodrębnioną organizacyjnie część systemu obronnego RP. Mogą brać udział w wielu działaniach o charakterze ochronnym, ratowniczym, poszukiwawczym czy służącym neutralizacji określonych zagrożeń, wśród których ustawodawca wskazał wprost ochronę i obronę cyberprzestrzeni[19]. Zadania wojska są powiązane z ustawami: o zarządzaniu kryzysowym, o działaniach antyterrorystycznych i o krajowym systemie cyberbezpieczeństwa.

Różnorodne zadania do wykonania wymagają właściwej organizacji zapewniającej skuteczność działania sił zbrojnych. Ich trzon stanowią wojska lądowe, których zadaniem jest zapewnienie obrony przed atakiem lądowo-powietrznym w dowolnym rejonie kraju wobec każdej formy zagrożenia militarnego. Wojska lądowe składają się z następujących rodzajów wojsk: pancernych i zmechanizowanych, aeromobilnych, rakietowych i artylerii, obrony

17 H. Królikowski [w:] J. Bulira, A. Jagnieża, E. Krempeć, F. Seredyński, H. Królikowski, *Obrona ojczyzny. Komentarz*, Warszawa 2023, art. 11.

18 A. Nowak, *Instytucjonalne podmioty ochrony militarnej cyberbezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2016, nr 2, s. 136.

19 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 11, ust. 2, 3.

przeciwlotniczej, inżynieryjnych, chemicznych, łączności i informatyki, a także oddziałów i pododdziałów rozpoznania i walki elektronicznej oraz logistycznych. Są one przystosowane do wykonywania zadań w niesprzyjających warunkach pogodowych i bojowych oraz wielopłaszczyznowego współdziałania z siłami powietrznymi i marynarką wojenną. W strukturze wojsk lądowych wyróżnia się związki taktyczne, oddziały i pododdziały.

Siły powietrzne zapewniają obronę przestrzeni powietrznej kraju. Są także przygotowane do prowadzenia operacji mających na celu utrzymanie przewagi w powietrzu oraz wspierania innych rodzajów wojsk w operacjach połączonych. Siły powietrzne tworzą trzy główne rodzaje wojsk: lotnicze, obrony przeciwlotniczej oraz radiotechniczne. Są zorganizowane w skrzydła (oddziały wojsk lotniczych) oraz brygady. W skład sił powietrznych wchodzą dwa skrzydła lotnictwa taktycznego, skrzydło lotnictwa transportowego, skrzydło lotnictwa szkolnego, brygada rakietowej obrony powietrznej, brygada radiotechniczna oraz jednostki zabezpieczenia.

Marynarka wojenna broni interesów państwa na polskich obszarach morskich. Powierzono jej także morską obronę wybrzeża. Jest formacją przygotowaną do udziału w lądowej obronie wybrzeża we współdziałaniu z innymi rodzajami sił zbrojnych w ramach strategicznej operacji obronnej. Podstawowym zadaniem marynarki wojennej w czasie kryzysu i wojny jest obrona oraz utrzymanie morskich linii komunikacyjnych, a także niedopuszczenie do blokady morskiej. Zgodnie ze zobowiązaniami międzynarodowymi utrzymuje także zdolność do realizacji zadań związanych z zapewnieniem bezpieczeństwa zarówno w obszarze Morza Bałtyckiego, jak i poza nim. W czasie pokoju marynarka wojenna współdziała ze Strażą Graniczną na obszarze morskich wód terytorialnych i wyłącznej strefy ekonomicznej w celu jak najskuteczniejszej ochrony granicy państwowej. Marynarkę wojenną tworzą: flotylla okrętów, brygada lotnictwa marynarki wojennej, a także brzegowe jednostki wsparcia i zabezpieczenia działań oraz ośrodki szkolne.

Wojska specjalne są przeznaczone do prowadzenia operacji specjalnych zarówno w kraju, jak i poza jego granicami w czasie pokoju, kryzysu i wojny. Zadania przez nie wykonywane (prowadzone samodzielnie lub we współdziałaniu z innymi siłami) mogą mieć znaczenie strategiczne lub operacyjne. Ten rodzaj sił zbrojnych tworzą samodzielne oddziały i pododdziały, w których skład wchodzą specjalnie wyselekcjonowani, wyszkoleni i wyposażeni żołnierze, przygotowani do realizacji działań w warunkach najwyższego ryzyka. Każda z jednostek wojsk specjalnych ma unikalną specyfikę i jest stale gotowa do realizacji wyznaczonych zadań. Wojska specjalne są przygotowane do

prowadzenia wielu różnorodnych operacji specjalnych w razie zaistnienia zdarzeń w sytuacjach nadzwyczajnych. Innym ważnym zadaniem wojsk specjalnych jest utrzymywanie w gotowości sił i środków do wsparcia policji w zwalczaniu terroryzmu na terenie państwa[20].

Wojska obrony terytorialnej tworzą żołnierze pełniący terytorialną służbę wojskową, na co dzień pracujący zawodowo w swoich profesjach. Pełnią oni służbę w rejonie swojego zamieszkania. Oprócz nich służą także żołnierze zawodowi. Ich zadaniem jest obrona i wspieranie lokalnych społeczności. W czasie pokoju to m.in. przeciwdziałanie skutkom klęsk żywiołowych i zwalczanie ich oraz prowadzenie działań ratowniczych w sytuacjach kryzysowych. W czasie wojny będą wsparciem wojsk operacyjnych w strefie działań bezpośrednich.

Działania wywiadowcze na rzecz wojska wykonuje Służba Wywiadu Wojskowego (SWW). Jest to służba specjalna chroniąca przed zagrożeniami zewnętrznymi, która ponadto strzeże bezpieczeństwa i zdolności bojowej SZ RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej.

Zadania o charakterze kontrwywiadowczym na rzecz SZ RP wykonuje Służba Kontrwywiadu Wojskowego (SKW). Jest to służba specjalna właściwa w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej[21]. W przypadku ogłoszenia powszechnej lub częściowej mobilizacji oraz w czasie wojny Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego stają się z mocy prawa częścią sił zbrojnych[22].

Dowódcami rodzajów sił zbrojnych są: dowódca generalny Rodzajów Sił Zbrojnych, dowódca operacyjny Rodzajów Sił Zbrojnych oraz dowódca Wojsk Obrony Terytorialnej[23]. Siły zbrojne składają się z jednostek wojskowych i związków organizacyjnych. Jednostka wojskowa stanowi jednostkę organizacyjną sił zbrojnych, funkcjonuje na podstawie nadanego przez Ministra

20 Obecnie w strukturze wojsk specjalnych funkcjonują: Dowództwo Wojsk Specjalnych (Kraków), Jednostka Wojskowa GROM (Warszawa), Jednostka Wojskowa Komandosów (Lubliniec), Jednostka Wojskowa Formoza (Gdynia), Jednostka Wojskowa Agat (Gliwice), Jednostka Wojskowa Nil (Kraków).

21 Zob. *Struktura i organizacja Sił Zbrojnych RP*, https://zpe.gov.pl/a/struktura-i-organizacja-sil-zbrojnych-rp/D11sA9IBV [dostęp: 20.06.2023]; *Siły Zbrojne RP*, https://www.wojsko-polskie.pl/ [dostęp: 1.06.2023].

22 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 15, ust. 5.

23 Ibidem, art. 15, ust. 3.

Obrony Narodowej etatu oraz posługuje się pieczęcią urzędową z godłem Rzeczypospolitej Polskiej i nazwą (numerem) jednostki. Związki organizacyjne to jednostki wojskowe zorganizowane przez Ministra Obrony Narodowej w określoną strukturę, w szczególności w korpus, dywizję lub brygadę funkcjonującą samodzielnie albo w składzie rodzaju sił zbrojnych, na podstawie nadanych etatów[24]. Jednostki wojskowe i ich związki organizacyjne są rozmieszczone w garnizonach. Garnizon to określenie grupy wojsk stacjonujących w określonym miejscu, dawniej w celu pilnowania i obrony tego miejsca, obecnie używania go jako bazy. Garnizon obejmuje żołnierzy (oddziały wojskowe), pracowników wojska oraz infrastrukturę w jednej lub kilku miejscowościach[25].

W skład sił zbrojnych wchodzi również Żandarmeria Wojskowa jako ich wyodrębniona i wyspecjalizowana służba wykonująca zadania polegające na wsparciu policyjnym dowódców sił zbrojnych, udziale w ochronie wojsk, współdziałaniu z zagranicznymi i krajowymi formacjami w sprawach bezpieczeństwa i porządku publicznego[26].

Specjalistycznym komponentem Sił Zbrojnych RP są wojska obrony cyberprzestrzeni (WOC)[27]. Podjęcie decyzji o utworzeniu tej kategorii wojsk oznacza że cyberprzestrzeń w wymiarze militarnym stanowi jeden z głównych przedmiotów obrony przez zagrożeniami, a zadaniem sił zbrojnych RP jako najważniejszego elementu systemu obronnego RP jest m.in. zapewnienie bezpieczeństwa tej przestrzeni (cyberbezpieczeństwa).

Geneza cyberwojsk w Polsce

Od 2 czerwca do 5 grudnia 2014 roku Najwyższa Izba Kontroli prowadziła ocenę struktur państwowych funkcjonujących w obszarze cyberbezpieczeństwa.

24 Ibidem, art. 2, pkt 12, 38.

25 H. Królikowski [w:] J. Bulira, A. Jagnieża, E. Krempeć, F. Seredyński, H. Królikowski, op. cit., art. 16. W aktualnym stanie prawnym funkcjonuje 106 garnizonów utworzonych na podstawie rozporządzenia Ministra Obrony Narodowej z 10 sierpnia 2022 r. w sprawie utworzenia, przekształcenia i zniesienia garnizonów oraz określenia zadań, siedzib i terytorialnego zasięgu właściwości ich dowódców, Dz.U. 2022, poz. 1868.

26 Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j., ibidem 2021, poz. 1214, art. 3, ust. 1; J. Stelmach, *Żandarmeria Wojskowa w narodowym systemie przeciwdziałania zagrożeniu terroryzmem*, „Zeszyty Naukowe WSOWL" 2013, nr 3, s. 47–63. Więcej zob. B. Kuś, *Żandarmeria Wojskowa i wojskowe organy porządkowe* [w:] *Prawo wojskowe*, red. M. Czuryk, M. Karpiuk, Warszawa 2015, s. 167–178.

27 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 15, ust. 4, pkt 2.

Kontrola miała na celu zweryfikowanie istnienia systemu, z którego pomocą państwo jest gotowe ochraniać zasoby oraz swoich obywateli przed zagrożeniami występującymi w cyberprzestrzeni. Badaniem objęto okres od początku 2008 roku do dnia zakończenia czynności kontrolnych. Celami cząstkowymi kontroli było uzyskanie odpowiedzi na następujące pytania: 1. Czy został opracowany spójny system działania organów administracji państwowej mający na celu monitorowanie zagrożeń występujących w cyberprzestrzeni RP, przeciwdziałanie im oraz minimalizowanie skutków incydentów? W szczególności: czy określono ramy prawne tego systemu, dokonano podziału uprawnień między jego uczestnikami, przydzielono im niezbędne zasoby, określono mechanizmy koordynacji i wymiany informacji oraz sformułowano krajowy zbiór dobrych praktyk? 2. Czy funkcjonujące w Polsce rozwiązania instytucjonalno-prawne zapewniają skuteczne szacowanie ryzyk związanych z zagrożeniami występującymi w cyberprzestrzeni? 3. Czy obowiązujące obecnie regulacje prawne oraz działania realizowane przez podmioty państwowe na rzecz bezpieczeństwa systemów teleinformatycznych są spójne, kompletne oraz odwołują się do uznanych międzynarodowych wzorów dobrych praktyk?[28].

W opublikowanej informacji o wynikach kontroli NIK negatywnie ocenił realizację zadań podmiotów państwowych z ochrony cyberprzestrzeni RP. Administracja państwowa nie podjęła niezbędnych działań mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski. Pomimo że coraz większa część usług publicznych oraz istotnych aspektów życia społecznego i gospodarczego jest realizowana obecnie w sieci internet lub z wykorzystaniem systemów teleinformatycznych, bezpieczeństwo Polski w dalszym ciągu jest postrzegane jedynie w sposób konwencjonalny (jako działania na rzecz zapobiegania i reagowania na tradycyjne zagrożenia takie, jak np.: powodzie, pożary, akty terroru z wykorzystaniem przemocy fizycznej, tradycyjne konflikty zbrojne). Nie dostrzeżono, że powstała nowa kategoria zagrożeń, wymagająca pilnej reakcji państwa. Kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem

28 Kontrolą objęto osiem podmiotów państwowych, którym przypisano kluczowe zadania związane z bezpieczeństwem teleinformatycznym państwa, tj.: Ministerstwo Administracji i Cyfryzacji, Agencję Bezpieczeństwa Wewnętrznego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych, Naukową i Akademicką Sieć Komputerową, Urząd Komunikacji Elektronicznej, Rządowe Centrum Bezpieczeństwa oraz Komendę Główną Policji – zob. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP. Informacja o wynikach kontroli*, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf [dostęp: 2.06.2023].

cyberprzestrzeni oraz wynikających z tego nowych zadań administracji państwowej. Działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzenia oraz biernego oczekiwania na rozwiązania, które w tym obszarze zaproponuje Unia Europejska. Głównym czynnikiem paraliżującym aktywność państwa w tym zakresie był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych[29].

Podczas szczytu NATO w Warszawie w 2016 roku potwierdzono, że obrona cyberprzestrzeni należy do podstawowych zadań kolektywnej obrony Sojuszu. Cyberprzestrzeń została uznana za obszar działań militarnych. W odpowiedzi na wyzwania i zagrożenia związane z rozwojem nowych technologii Ministerstwo Obrony Narodowej zadeklarowało konsolidację potencjału i zasobów jednostek realizujących zadania na rzecz zapewnienia bezpieczeństwa w cyberprzestrzeni[30].

W związku z powyższym 9 października 2017 roku podczas III Europejskiego Forum Cyberbezpieczeństwa CYBERSEC w Krakowie poinformowano o planach sformowania kolejnego rodzaju sił zbrojnych. Minister Obrony Narodowej wskazał wówczas, że będzie liczył on co najmniej 1000 żołnierzy, a koszty jego sformowania wyniosą 2 mld zł. Podczas święta Dowództwa Generalnego Rodzajów Sił Zbrojnych 21 czerwca 2018 roku przekazano informację o pracach nad projektem sformowania wojsk obrony cyberprzestrzeni. W strukturze Ministerstwa Obrony Narodowej został utworzony zespół analizujący działania wykonywane przez różne instytucje związanych z informatyką, teleinformatyką i cyberbezpieczeństwem. Jego zadaniem było wypracowanie rekomendacji dotyczących wzmocnienia potencjału i usprawnienia procesów w tych obszarach. Jednocześnie prowadzono pogłębione audyty bezpieczeństwa teleinformatycznego i testy[31].

W lutym 2019 roku w ramach programu CYBER.MIL.PL, którego celem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni, resort obrony narodowej przedstawił koncepcję formowania wojsk obrony cyberprzestrzeni oraz pakiet działań związanych z rozwojem zdolności resortu

29 Ibidem.

30 *Wojska Obrony Cyberprzestrzeni*, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni [dostęp: 15.06.2023].

31 R. Muczyński, *Koncepcja Wojsk Obrony Cyberprzestrzeni*, https://milmag.pl/koncepcja-wojsk-obrony-cyberprzestrzeni/ [dostęp: 12.06.2013].

obrony narodowej w zakresie cyberbezpieczeństwa[32]. Podjęto decyzję o powołaniu Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC) na bazie Narodowego Centrum Kryptologii i Inspektoratu Informatyki. Skonsolidowano zasoby i kompetencje całego resortu obrony narodowej w dziedzinach cyber, krypto i IT w jednej instytucji. 5 lutego 2019 roku powołano pełnomocnika ministra obrony narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni, który jednocześnie objął stanowisko dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni[33]. Tym samym był on odpowiedzialny za dwa najważniejsze procesy konsolidacji oraz rozwoju zdolności Sił Zbrojnych RP. Do zadań pełnomocnika należało: zweryfikowanie dotychczasowego stanu prawnego w celu określenia niezbędnych zmian związanych z uznaniem cyberprzestrzeni za domenę działań operacyjnych, koordynacja działań zmierzających do utworzenia wojsk obrony cyberprzestrzeni oraz nadzór nad prawidłową realizacją zadań związanych z osiągnięciem przez te wojska gotowości operacyjnej[34].

Pełnomocnik ds. utworzenia wojsk obrony cyberprzestrzeni został zobowiązany do przedstawienia do 30 czerwca 2019 roku Ministrowi Obrony Narodowej koncepcji organizacji i funkcjonowania tych wojsk[35]. Została ona zatwierdzona we wrześniu 2019 roku. Dwa miesiące później weszła w życie decyzja Ministra ON w sprawie organizacji i funkcjonowania systemu cyberbezpieczeństwa w resorcie obrony narodowej (decyzja 396/NCBC/MON). W lutym 2020 roku została utworzona grupa ds. sformowania dowództwa wojsk obrony cyberprzestrzeni, a w marcu powstał Nieetatowy Zespół ds. Wdrożenia kolejnych etapów tworzenia WOC oraz wdrażania cyberprzestrzeni jako środowiska działań operacyjnych w Siłach Zbrojnych RP. Projekt utworzenia cyberwojsk dostał kolejne wsparcie w kwietniu 2020 roku, kiedy to został powołany pełnomocnik ministra obrony narodowej ds. bezpieczeństwa cyberprzestrzeni[36].

32 CYBER.MIL.PL to program Ministerstwa Obrony Narodowej obejmujący cztery strategiczne obszary: konsolidacja i budowa struktur cyberbezpieczeństwa; edukacja, szkolenie i treningi; współpraca i budowa silnej pozycji międzynarodowej; podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów. Więcej zob. *Kim jesteśmy?*, https://www.cyber.mil.pl/kim-jestesmy/ [dostęp: 12.06.2023].

33 Zob. Decyzja Ministra Obrony Narodowej z dnia 5 lutego 2019 r. nr 17/MON w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni, Dz. Urz. MON 2019, poz. 23, par. 1, 2.

34 Ibidem, par. 3.

35 Ibidem, par. 4.

36 *Wojska Obrony Cyberprzestrzeni*...

W latach 2019–2022 pod zwierzchnictwem NCBC nastąpiła konsolidacja instytucji i jednostek odpowiedzialnych za cyberbezpieczeństwo i informatykę w siłach zbrojnych i resorcie obrony narodowej. W ministerstwie w 2021 roku utworzono Departament Cyberbezpieczeństwa. Kolejnym etapem formowania WOC było utworzenie Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, które powstawało przy NCBC. Założono, że obie struktury, tj. NCBC i WOC, funkcjonują, wspierając swoje działania. Jest to rozwiązanie na wzór amerykański, gdzie dowódca US Cyber Command jest równocześnie dyrektorem NSA[37].

Następny etap programu, czyli CYBER.MIL.PL 2.0, ma obejmować zadania związane z budową i rozwojem kompetencji, co ma w efekcie doprowadzić także do osiągnięcia przez WOC pełnej zdolności do działania jako specjalistyczny komponent sił zbrojnych[38]. Warto wspomnieć, że w wojskach obrony terytorialnej powstałych na początku 2017 roku jest rozwijany komponent „cyber" pod nazwą Zespół Działań Cyberprzestrzennych (ZDC), który w zamierzeniu ma stanowić kuźnię kadr dla WOC. Docelowo w Zespole tym ma służyć 100 żołnierzy. Planuje się, że tylko dziesięciu z nich to będą żołnierze zawodowi. Nie jest to struktura ostateczna, ponieważ wojska obrony terytorialnej planują dalszy rozwój zdolności w obszarze cyberbezpieczeństwa. Docelowy cyberkomponent WOT będzie posiadał w swej strukturze autonomiczne elementy zdolne do samodzielnego wykonywania zadań[39].

Organizacja i zadania cyberwojsk – stan aktualny

Wojska obrony cyberprzestrzeni formalnie zostały sformowane 1 stycznia 2022 roku, struktury komponentu są w początkowej fazie formowania i obecnie nie stanowią rodzaju sił zbrojnych. Struktura oparta jest na samodzielnych jednostkach wojskowych podporządkowanych Dowództwu Komponentu WOC. Pełnią w niej służbę specjalnie wyselekcjonowani i wyszkoleni żołnierze.

37 P. Jaszczuk, *Wojska Obrony Cyberprzestrzeni – rodzaj sił zbrojnych, rodzaj wojsk czy specjalistyczny komponent?*, https://cyberdefence24.pl/armia-i-sluzby/wojska-obrony-cyberprzestrzeni-rodzaj-sil-zbrojnych-rodzaj-wojsk-czy-specjalistyczny-komponent [dostęp; 9.06.2023]. NSA – National Security Agency – amerykańska wewnętrzna agencja wywiadowcza koordynująca m.in. zadania wywiadu elektronicznego.

38 Ibidem.

39 *Wojska Obrony Terytorialnej*, https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20t--wojska-obrony-terytorialnej/ [dostęp: 15.06.2023]; *Cyberkomponent*, https://terytorialsi.wp.mil.pl/cyberkomponent [dostęp: 15.06.2023].

Według przyjętej w resorcie obrony narodowej koncepcji polskie cyberwojska do czasu powołania Naczelnego Dowódcy Sił Zbrojnych będą podlegały Ministrowi Obrony Narodowej[40].

Proces tworzenia WOC nie został jeszcze zakończony. Formacja ta uzyska status specjalistycznego komponentu dopiero z chwilą osiągnięcia pełnej gotowości do działania. Według deklaracji, które pojawiały się w przestrzeni publicznej, będzie to miało miejsce na przełomie 2024 i 2025 roku. Z chwilą osiągnięcia stosownego poziomu gotowości do działania WOC stanie się specjalistycznym komponentem sił zbrojnych, usytuowanym w czasie pokoju w sposób podobny do Żandarmerii Wojskowej (bezpośrednio szefowi resortu obrony narodowej), a z chwilą ogłoszenia mobilizacji lub wojny podporządkowanym wskazanemu przez Prezydenta RP Naczelnemu Dowódcy Sił Zbrojnych[41].

Ustawowa regulacja dotyczy przede wszystkim zakresu działania dowódcy komponentu WOC, właściwemu w zakresie dowodzenia jednostkami wojskowymi i związkami organizacyjnymi WOC. Ustawodawca sformułował otwarty katalog zadań dowódcy komponentu WOC, w tym:

1) realizacja programu rozwoju sił zbrojnych;

2) programowanie, planowanie, organizowanie, prowadzenie oraz nadzorowanie prowadzenia szkoleń będących we właściwości dowódcy komponentu WOC na rzecz podległych jednostek wojskowych i związków organizacyjnych, komórek organizacyjnych i jednostek organizacyjnych, a także instytucji, organów i podmiotów na podstawie zawartych porozumień;

3) planowanie oraz organizowanie mobilizacyjnego i operacyjnego rozwinięcia oraz użycia WOC;

4) budowa, utrzymanie oraz ochrona infrastruktury, a także ochrona informacji w cyberprzestrzeni;

5) prowadzenie działań i operacji w cyberprzestrzeni;

6) zapewnienie wsparcia operacji militarnych prowadzonych przez siły zbrojne oraz operacji w układzie sojuszniczym i koalicyjnym;

7) współpraca z innymi organami i podmiotami w sprawach związanych z obronnością państwa;

40 P. Jaszczuk, *Wojska Obrony Cyberprzestrzeni. Kto może trafić do polskiego cyberwojska?*, https://cyberdefence24.pl/armia-i-sluzby/wojska-obrony-cyberprzestrzeni-kto-moze-trafic-do-polskiego-cyberwojska [dostęp: 12.06.2023].

41 Idem, *Wojska Obrony Cyberprzestrzeni – rodzaj sił zbrojnych*...

8) zarządzanie i przeprowadzanie kontroli podległych jednostek wojskowych i związków organizacyjnych na zasadach i w trybie określonych w ustawie z 15 lipca 2011 roku o kontroli w administracji rządowej[42].

Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni wykonuje swoje zadania z pomocą Dowództwa Komponentu WOC[43]. Strukturze tej są podporządkowane jednostki poziomu taktycznego. Ich prawidłowe funkcjonowanie zapewnia jednostka wsparcia działań. Dowództwo odpowiada również w resorcie obrony narodowej za obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT. Głównym zadaniem jednostki jest zapewnienie bezpieczeństwa teleinformatycznego całego resortu, prowadzenie badań, projektowanie, budowa, wdrażanie, użytkowanie i ochrona narodowych technologii kryptologicznych oraz wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych. Prowadzi też działalność naukowo-edukacyjną, wdrożeniową, badawczo-rozwojową i opiniodawczą. Eksperci DKWOC opracowują nowoczesne metody wykrywania incydentów w cyberprzestrzeni, projektują rozwiązania do ochrony i zabezpieczenia informacji, rozwijają też własne metody i urządzenia kryptograficzne. Zadaniem DKWOC jest też zapewnienie prawidłowego funkcjonowania zespołu CSIRT MON (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego), który monitoruje sieci resortu obrony narodowej w trybie 24 godziny/7 dni i tym samym realizuje obronę pasywną polskiej cyberprzestrzeni[44]. Ze względu na charakter działań prowadzonych przez nowo formowany komponent sił zbrojnych szczegółowy zakres działania, siedzibę i strukturę organizacyjną Dowództwa Wojsk Obrony Terytorialnej określa niepodlegające ogłoszeniu zarządzenie Ministra Obrony Narodowej[45].

Na podstawie ogólnodostępnych informacji wiadomo, że aktualnie w strukturach WOC służy i pracuje kilkuset żołnierzy oraz pracowników wojska, a proces rekrutacji nadal jest prowadzony. Dokładne dane liczbowe nie są dostępne publicznie. Podstawową część kadr WOC stanowią żołnierze i tylko oni są upoważnieni do prowadzania działań militarnych w cyberprzestrzeni. Resort obrony narodowej planuje w kolejnych latach dalszą rozbudowę

42 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 23, ust. 2.
43 Ibidem, art. 23, ust. 3.
44 https://www.cyber.mil.pl/ncbc-dkwoc/ [dostęp: 12.06.2023].
45 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 22, ust. 4.

komponentu. Aktualnie w strukturach NCBC – Dowództwa WOC służy i pracuje łącznie ponad 5 tys. żołnierzy i pracowników wojska[46].

Do służby w WOC, analogicznie jak w całych siłach zbrojnych RP, powołać można osobę, która spełnia określone ustawowo kryteria. Ustawodawca wyróżnił dwa rodzaje warunków powołania do czynnej służby wojskowej, tj. obligatoryjne i fakultatywne. Warunki obligatoryjne dotyczą powołania do każdego rodzaju czynnej służby wojskowej, a fakultatywne wiążą się z pełnieniem służby na określonych stanowiskach służbowych[47]. Do służby wojskowej może być powołana osoba, która spełnia następujące warunki:

1) posiada obywatelstwo polskie;
2) posiada nieposzlakowaną opinię;
3) posiada zdolność fizyczną i psychiczną do pełnienia służby wojskowej;
4) posiada wiek co najmniej 18 lat;
5) nie była karana za przestępstwo umyślne;
6) nie jest przeznaczona do służby zastępczej;
7) nie jest wyłączona od obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny;
8) nie posiada nadanego przydziału organizacyjno-mobilizacyjnego do służby w jednostce zmilitaryzowanej;
9) posiada wykształcenie:

a) co najmniej wyższe – w przypadku pełnienia służby na stanowisku służbowym w korpusie oficerów,

b) co najmniej średnie lub średnie branżowe – w przypadku pełnienia służby na stanowisku służbowym w korpusie podoficerów,

c) co najmniej podstawowe – w przypadku pełnienia służby na stanowisku służbowym w korpusie szeregowych – jeżeli występują potrzeby uzupełnieniowe sił zbrojnych[48].

Warunki fakultatywne to:

1) posiadanie przez kandydata na żołnierza kwalifikacji wymaganych do zajmowania stanowiska służbowego;
2) posiadanie orzeczenia o braku przeciwwskazań do pełnienia służby na stanowiskach wymagających szczególnych predyspozycji psychofizycznych;
3) złożenie ankiety bezpieczeństwa osobowego[49].

46 P. Jaszczuk, *Wojska Obrony Cyberprzestrzeni. Kto może trafić...*

47 J. Bulira [w:] J. Bulira, A. Jagnieża, E. Krempeć, F. Seredyński, H. Królikowski, op. cit., art. 83.

48 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny..., art. 83, ust. 1.

49 Ibidem, art. 83, ust. 2.

Ze względu na wysoce specjalistyczny charakter dużej części stanowisk służbowych w jednostkach poziomu taktycznego WOC przyjęto, że na wybrane specjalistyczne stanowiska można powołać wyłącznie osoby, które oprócz określonych wymagań posiadają:

1) specjalistyczną wiedzę z obszaru szeroko rozumianego cyberbezpieczeństwa i zaliczyły wymagany dla konkretnego stanowiska służbowego (na które dana osoba ma być wyznaczona) test kompetencyjny prowadzony przez NCBC;

2) orzeczenia o braku przeciwskazań do pełnienia służby na stanowiskach wymagających szczególnych predyspozycji psychofizycznych;

3) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub złożyły wniosek wraz z ankietą bezpieczeństwa o przeprowadzenie właściwego postępowania sprawdzającego na zasadach określonych w przepisach o ochronie informacji niejawnych[50].

W przypadku WOC poszukiwani są przede wszystkim specjaliści dysponujący wiedzą i umiejętnościami w dziedzinie informatyki, matematyki, teleinformatyki i cyberbezpieczeństwa, gotowi dołączyć do zespołu ekspertów Sił Zbrojnych RP i służyć swoim doświadczeniem państwu polskiemu[51].

Zakończenie

Współczesne konflikty często toczą się w innowacyjny sposób z wykorzystaniem nowoczesnych technologii. W działaniach taktycznych i strategicznych niejednokrotnie jest wykorzystywana także walka informacyjna obejmująca działania mające na celu wpłynięcie na przeciwnika, jego zasoby informacyjne, systemy informatyczne i sieci komputerowe.

Jednym z podstawowych celów Rzeczypospolitej Polskiej, wskazanym przez ustawodawcę konstytucyjnego, jest zapewnienie bezpieczeństwa obywatelom, w tym w cyberprzestrzeni. Obejmuje ona przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, co w odniesieniu do Rzeczypospolitej Polskiej oznacza terytorium państwa polskiego oraz miejsca, gdzie funkcjonują jej przedstawicielstwa. Cyberprzestrzeń została uznana za obszar działań militarnych. W dobie społeczeństwa informacyjnego zapewnienie bezpieczeństwa w cyberprzestrzeni, w tym

50 P. Jaszczuk, *Wojska Obrony Cyberprzestrzeni. Kto może trafić...*
51 https://www.cyber.mil.pl/kariera/ [dostęp: 16.06.2023].

świadczenia usług cyfrowych czy też korzystania ze środków komunikacji elektronicznej, należy do podstawowych obowiązków państwa. Zagwarantowanie cyberbezpieczeństwa wymaga podejścia holistycznego wykorzystującego narzędzia nie tylko z tej konkretnej dziedziny.

Przytoczone okoliczności wskazują, że zapewnienie cybebezpieczeństwa w wymiarze militarnym jest obecnie jednym z głównych zadań RP. Ich wykonaniu służy działalność polskiego ustawodawcy, który proponuje w tym celu konkretne rozwiązania prawne.

Podstawowy elementem systemu obronnego państwa polskiego są Siły Zbrojne Rzeczypospolitej Polskiej, a jednym z ustawowo wskazanych zadań tej formacji jest ochrona i obrona cyberprzestrzeni. Różnorodność powierzonych do wykonania zadań wymaga właściwej organizacji zapewniającej skuteczność działania sił zbrojnych. Pięć rodzajów Sił Zbrojnych RP dysponuje osobnym składem osobowym, uzbrojeniem oraz zakresem działania. Specjalistycznym komponentem SZ RP są wojska obrony cyberprzestrzeni. Podjęcie decyzji o ich utworzeniu oznacza, że cyberprzestrzeń w wymiarze militarnym stanowi jeden z głównych przedmiotów obrony przez zagrożeniami, a zadaniem sił zbrojnych jako najważniejszego elementu systemu obronnego RP jest m.in. zapewnienie bezpieczeństwa tej przestrzeni (cyberbezpieczeństwa).

Wojska obrony cyberprzestrzeni formalnie zostały sformowane 1 stycznia 2022 roku, struktury komponentu są w fazie formowania i obecnie nie są rodzajem sił zbrojnych.

Głównym zadaniem jednostki jest zapewnienie bezpieczeństwa teleinformatycznego całego resortu, prowadzenie badań, projektowanie, budowa, wdrażanie, użytkowanie oraz ochrona narodowych technologii kryptologicznych czy wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych. Aktualnie w strukturach WOC służy i pracuje kilkuset żołnierzy oraz pracowników wojska.

W wojskach obrony terytorialnej, powstałych na początku 2017 roku, jest rozwijany cyberkomponent ZDC, który w zamierzeniu ma stanowić kuźnię kadr dla WOC. Docelowo w ZDC ma służyć 100 żołnierzy. Planuje się, że tylko dziesięciu z nich będzie żołnierzami zawodowymi.

Działania polskiego ustawodawcy w zakresie ochrony cyberbezpieczeństwa w wymiarze militarnym są obecnie w toku. Osiągnięcie założonego stanu jest procesem wymagającym wielu rozłożonych w czasie różnorakich czynności. Działania podjęte dotychczas, które doprowadziły do utworzenia specjalistycznego komponentu Sił Zbrojnych RP, należy ocenić pozytywnie.

Bibliografia

Bilal A., *Wojna hybrydowa – nowe zagrożenia, złożoność i „zaufanie" jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html [dostęp: 10.05.2023].

Bulira J., Jagnieża A., Krempeć E., Seredyński F., Królikowski H., *Obrona ojczyzny. Komentarz*, Warszawa 2023.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.

Gardocki S., Wrona J., *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji" 2020, nr 2.

Hajduk J., Stępniewski T., *Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty*, „Studia Europejskie" 2015, nr 4.

Konstytucja Rzeczypospolitej Polskiej. Komentarz, wyd. 2, red. P. Tuleja, LEX/el. 2021.

Kuś B., *Żandarmeria Wojskowa i wojskowe organy porządkowe*, [w:] *Prawo wojskowe*, red. M. Czuryk, M. Karpiuk, Warszawa 2015.

Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 1–2.

Nowak A., *Instytucjonalne podmioty ochrony militarnej cyberbezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2016, nr 2.

Stelmach J., *Żandarmeria Wojskowa w narodowym systemie przeciwdziałania zagrożeniu terroryzmem*, „Zeszyty Naukowe WSOWL" 2013, nr 3.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

The Armed Forces of the Republic of Poland and cybersecurity. Organizational and legal issues

Abstract

Today, ICT systems play an important role in both the state and society. state security in the military and non-military dimensions, external and internal, has gained an additional dimension in the form of cyberspace. One of the primary goals of the Republic of Poland is to ensure the security of citizens. Protecting the independence of the state and the indivisibility of its territory and ensuring the security and inviolability of its borders are constitutional tasks of public authorities. The basic element of the defense system of the Republic of Poland participating in the implementation of security and defense policies is the Polish Armed Forces. The statutory task of this formation is, among other things, the protection and defense of cyberspace. A specialized component of the Polish Armed Forces is the Cyber Defense Forces. The process of creating this category of troops has not yet been completed.

Key words: cybersecurity, cyberspace, Armed Forces, defence of cyberspace