WIEDZA OBRONNA 2024, Vol. 289 No. 4
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2024-4-7

AGNIESZKA BRZOSTEK*
Akademia Sztuki Wojennej, Warszawa, Polska

MINISTER OBRONY NARODOWEJ JAKO ORGAN WŁAŚCIWY W ZAKRESIE CYBERBEZPIECZEŃSTWA

MINISTER OF NATIONAL DEFENSE AS THE COMPETENT AUTHORITY FOR CYBERSECURITY

ABSTRAKT: Cyberbezpieczeństwo, jak i ochrona cyberprzestrzeni odgrywa współcześnie podstawową funkcję w sferze publicznej, jak i prywatnej. Rozwój ten jest ściśle związany z funkcjonowaniem państwa, zarówno w sferze wewnętrznej jak i międzynarodowej. Narastające ataki hybrydowe na infrastrukturę państwa wskazują na potrzebę wzmacniania roli i pozycji Ministra Obrony Narodowej w zakresie przeciwdziałania zagrożeniom cybernetycznym. Rekomendowanym rozwiązaniem byłaby ściślejsza współpraca pomiędzy ministrem obrony a właściwym ministrem cyfryzacji.

SŁOWA KLUCZOWE: Minister obrony narodowej, cyberbezpieczeństwo, administracja rządowa

ABSTRACT: Cybersecurity and cyberspace protection currently play a fundamental function in the public and private spheres. This development is closely related to the functioning of the state, both in the internal and international sphere. Increasing hybrid attacks on state infrastructure indicate the need to strengthen the role and position of the Minister of National Defense in the field of countering cyber threats. The recommended solution would be closer cooperation between the Minister of National Defense and the competent Minister of Digital Affairs.

KEY WORDS: Minister of National Defense, Cybersecurity, Government Administration

WPROWADZENIE

Od wielu lat wzrasta liczba zagrożeń i incydentów bezpieczeństwa w cyberprzestrzeni. Takie incydenty to ryzyko naruszenia bezpieczeństwa obywateli – przejęcia danych osobowych, naruszenia prywatności, utraty pieniędzy, a nierzadko też zdrowia. Cyberbezpieczeństwo to odporność systemów informacyjnych na działania, które naruszają poufność, integralność,

* dr Agnieszka Brzostek, War Study University, Warsaw, Poland
https://orcid.org/0000-0002-7444-0186 a.brzostek@akademia.mil.pl
Copyright (c) 2024 Agnieszka Brzostek. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

dostępność i autentyczność przetwarzanych danych i związanych z nimi usług oferowanych przez te systemy[1]. Tak zdefiniowane pojęcie cyberbezpieczeństwa miało stanowić odpowiednik użytego w dyrektywie NIS[2] terminu bezpieczeństwo sieci i systemów teleinformatycznych, który w art. 4 pkt 2 wskazano, jako odporność sieci i systemów informatycznych przy danym poziomie zaufania na wszelkie działania naruszające dostępność, autentyczność, integralność oraz poufność przechowywania, przekazywania lub przetwarzania danych[3]. Z kolei definicja legalna cyberprzestrzeni została umieszczona w art. 2 ust. 1b ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[4]. Poprzez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymian. Informacji tworzonych przez systemy teleinformatyczne wraz z powiązanymi pomiędzy nimi oraz realizacjami z użytkownikami. Konieczność przeciwdziałania zagrożeniom w sferze cyberprzestrzeni stało się ściśle związane z funkcjonowaniem państwa, zarówno w sferze wewnętrznej jak i międzynarodowej. Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Jednak na pojęcie bezpieczeństwa w sieci czy cyberbezpieczeństwa składa się ochrona zasobów – danych, informacji, a ogólnie treści cyfrowych, ochrona sieci teleinformatycznych, urządzeń czyli komputerów, a także ochrona przesyłu treści za pomocą sieci, a więc samego procesu komunikowania. K. Chałubińska-Jentkiewicz podkreślała jeszcze czynnik ludzki, czyli ochronę użytkownika sieci i komputerów. Wciąż kluczem do działań stwarzających wszelkiego typu zagrożenia w cyberprzestrzeni jest

[1] Art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2023, poz. 913 tj.
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 Lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U.UE.L.2016.194.1 z dnia 2016.07.19.

[3]Szerzej na temat definicji F. Radoniewicz, *Komentarz do art. 2*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 31-33.
[4] 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, Dz. U. 2017, 1932 tj.

kwestia wykorzystywania luk i błędów w narzędziach programistycznych, a istotnym elementem tego procesu wciąż pozostaje działanie człowieka[5].

Należy także zaznaczyć, że obok pojęcia cyberprzestrzeni i cyberbezpieczeństwa występuję pojęcie cyberzagrożenia. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) zdefiniowało cyberzagrożenie jako wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób. Podnoszenie poziomów odporności systemu informacyjnych administracji publicznej wraz ze zwiększeniem potencjału narodowego w zakresie technologii cyberbezpieczeństwa są jednym z celów wymienionych w Strategii Cyberbezpieczeństwa RP[6].

Państwo realizuje swoje zadnia za pośrednictwem organów władzy publicznej[7]. Stąd prawne uwarunkowania, które precyzują podstawę do działania organów administracji w tym zakresie. Zgodnie z postanowieniami ustawy o krajowym systemie cyberbezpieczeństwa organem właściwym w zakresie cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji. Budowanie zdolności obronnej w sferze cyberbezpieczeństwa stało się elementem polityki realizowanej przez ministra obrony narodowej. Stąd celem artykułu staję się ocena prawnych form działania ministra ze wskazaniem rekomendowanych rozwiązań, jakie minister obrony narodowej jako organ właściwy w zakresie cyberbezpieczeństwa może wdrożyć.

POZYCJA USTROJOWA MINISTRA OBRONY NARODOWEJ

Ustawa o urzędzie Ministra Obrony Narodowej umieszcza ten organ w strukturze organów administracji publicznej oraz wskazuje, że jest to organ, za pośrednictwem którego Prezydent RP sprawuje zwierzchni nadzór na Siłami Zbrojnymi[8]. Poczynając od drugiej części sformułowania wskazanego w ustawie, to zwierzchnictwo Prezydenta Rzeczypospolitej Polskiej

[5] K. Chałubińska – Jentkiewicz, Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2019, nr 2, s. 20.

[6] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, MP 2019, 1037.

[7] K. Chałubińska-Jentkiewicz, A. Brzostek, *Strategie cyberbezpieczeństwa we współczesnym świecie*, Warszawa 2021, s. 44.

[8] Art. 1 ust. 1 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej, Dz. U. 2019, poz. 196 t.j.

i rolę ministra w tym zakresie określa Konstytucja w art. 134 ust. 2[9]. Połączenie kompetencji Prezydenta i Ministra Obrony Narodowej jest oceniana w literaturze jako mało precyzyjne. Zauważono, że nie wskazano wprost na czym to zwierzchnictwo ma polegać[10]. Oznaczenie pośrednictwa ministra odnosi się do obowiązku współdziałania organów władzy wykonawczej w sferze obronności i szerzej w zakresie bezpieczeństwa państwa[11]. Celem tego przepisu było wykluczenie sytuacji, w której Prezydent wykonuje zwierzchnictwo nad Siłami Zbrojnymi bezpośrednio z pomięciem właściwego ministra. Ustrojowodawca wyróżnił rolę ministra obrony poprzez umieszczenie organu w Konstytucji, co daje także konieczność powołania urzędu przy tworzeniu rządu. Minister musi posiadać kompetencje w zakresie obronności, w tym kompetencje kierownicze wobec Sił Zbrojnych[12]. Stąd też powierzenie ministrowi rzeczywistego kierowania Siłami Zbrojnymi i dowodzenia za pośrednictwem wojskowych struktur dowodzenia nabiera szczególnego znaczenia biorąc pod uwagę normy wskazane w Konstytucji. W art. 5 Konstytucji jako funkcję państwa wskazano stanie na straży niepodległości i nienaruszalności terytorium państwa, powierzając w art. 26 ust. 1 realizację tych zadań Siłom Zbrojnym. W art. 146 ust. 4 wskazano, że tę funkcję powierzono Radzie Ministrów poprzez zapewnienie bezpieczeństwa zewnętrznego państwa oraz sprawowanie ogólnego kierownictwa w dziedzinie obronności kraju[13].

Jak wskazano wyżej, drugą funkcją przypisaną Ministrowi Obrony Narodowej jest kierowanie działem administracji rządowej jako organ administracji publicznej. Minister Obrony Narodowej kieruje działem administracji rządowej wskazane w art. 19 ustawy o działach administracji rządowej, w którym wskazano, że ten dział w czasie pokoju obejmuje między innymi sprawy obronę państwa oraz Sił Zbrojnych, cyberprzestrzeni w wymiarze militarnym oraz udział Rzeczypospolitej w wojskowych przedsięwzięciach organizacji międzynarodowych oraz w zakresie wywiązywania się z zobowiązań militarnych, wynikających z umów międzynarodowych[14]. Minister jest zobowiązany do inicjonowania i opracowania polityki Rady Ministrów w stosunku do działu, którym kieruje. Minister wykonuje w zakresie swego działu

[9] Konstytucja RP z 2 kwietnia 1997 r., Dz. U.
[10] P. Czarny, *Komentarz do art. 134* w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* wyd. II, 2023.
[11] M. Serowaniec, *Rola Ministra Obrony Narodowej w cywilnym modelu zwierzchnictwa nad Siłami zbrojnymi RP,* „Gdańskie Studia Prawnicze" 2018, tom XL, s. 566-567.
[12] Wyrok Trybunału Konstytucyjnego z dnia 27 czerwca 2008 r., K 52/07.
[13] J. Padzik, *Prawonoustrojowa pozycja Ministra Obrony Narodowej w systemie organów administracji rządowej,* „Bezpieczeństwo Narodowe" 20, IV-2011, s. 101-102.
[14] Art. 19 ustawy z dnia 4 września 1997 r. o działach administracji rządowej, Dz. U. 2019, poz. 945 tj.

politykę Rady Ministrów i koordynuje jej wykonywanie przez organy, urzędy i jednostki podległe[15]. Norma kompetencyjna, określają szeroki zakres spraw, jakie nadano Ministrowi Obrony Narodowej, poczynając od uczynienia go organem kierującym działalnością Sił Zbrojnych[16] w czasie pokoju, poprzez władzę wykonawczą, po sprawy kadrowe dotyczące wykonywania obronności państwa, poprzez realizację zobowiązań wynikających ze zobowiązań wojskowych podjętych przez Radę Ministrów do wykonywania zadań jako państwowa jednostka organizacyjna działająca w imieniu i na rzecz Skarbu Państwa[17].

Poza konstytucją, zadania Sił Zbrojnych zdefiniowane są w ustawie o Obronie Ojczyzny. Siły zbrojne stoją na straży suwerenności, niepodległości i bezpieczeństwa państwa. Mogą też brać udział m.in. w ochronie i obronie cyberprzestrzeni[18]. Poza ustawą o krajowym systemie cyberbezpieczeństwa, zadania w szerszym zakresie Sił Zbrojnych powiązane są z ustawą o zarządzaniu kryzysowym[19] i z ustawą o działaniach antyterrorystycznych[20]. Różnorodne zadania wymagają właściwej organizacji zapewniającej skuteczność działania Sił Zbrojnych[21].

Wraz z utworzeniem specjalistycznego komponentu Sił Zbrojnych nastąpiła zmiana w zakresie ochrony cyberprzestrzeni. Podjęcie decyzji o utworzeniu komponentu znaczyło, że cyberprzestrzeń w wymiarze militarnym stanowi jeden z głównych przedmiotów obrony przez zagrożeniami, a zadaniem Sił Zbrojnych jako najważniejszego elementu obronnego RP jest m.in. zapewnienie bezpieczeństwa tej cyberprzestrzeni[22]. Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni podlega Ministrowi Obrony narodowej do czasu mianowania Naczelnego Dowódcy Sił Zbrojnych. W art. 23 ust. 2 określono zadania dowódcy. Należą do nich w szczególności:

- Realizacja programu rozwoju sił zbrojnych;
- programowanie, planowanie, organizowanie, prowadzenie oraz nadzorowanie prowadzenia szkoleń będących we właściwości dowódcy komponentu na rzecz podległych jednostek wojskowych i związków organizacyjnych, komórek

[15] Z. Morawski, *Status prawny Ministra Obrony Narodowej i Szefa Sztabu Generalnego*, „Wojskowy Przegląd Prawniczy" 2011, nr 4, s. 82 i 83.
[16] J. Padzik, op. cit., s. 100.
[17] K. Wąsowski, *Tasks of the Minister of National Defense in the field of cybersecurity,* w: *Cybersecurity in Poland. Legal Aspects*, ed. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Springer 2022, s. 246.
[18] Szerzej zadania określone zostały w art. 11 ustawy z dnia 11 marca 2022 r. o Obronie Ojczyzny, Dz. U. 2022, 655.
[19] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2019, 1398 tj.
[20] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz. U. 2019, 796 tj.
[21] B. Kuś, *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne,* "Cybersecurity and Law" 2023, nr10, s. 37.
[22] B. Kuś, op. cit., s. 40.

organizacyjnych i jednostek organizacyjnych, a także instytucji, organów i podmiotów na podstawie zawartych porozumień;

- planowanie oraz organizowanie mobilizacyjnego i operacyjnego rozwinięcia oraz użycia wojsk obrony cyberprzestrzeni;
- budowa, utrzymanie oraz ochrona infrastruktury, a także ochrona informacji w cyberprzestrzeni;
- prowadzenie działań i operacji w cyberprzestrzeni;
- zapewnienie wsparcia operacji militarnych prowadzonych przez siły zbrojne oraz operacji w układzie sojuszniczym i koalicyjnym;
- współpraca z innymi organami i podmiotami w sprawach związanych z obronnością państwa;
- 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.

Dowództwo Komponentu prowadzi działalność naukowo-dydaktyczną, działalność badawczo-rozwojową, wdrożeniową i doradczą związaną z cyberbezpieczeństwem, a także Centrum Szkoleniowe *Expert Cyber Security,* które jest odpowiedzialne za kształtowanie kierunków rozwoju kształcenia zawodowego z zakresu cyberbezpieczeństwa, kryptologii i informatyki[23].

ZADANIA MINISTRA OBRONY NARODOWEJ W USTAWIE O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Ustawa o krajowym systemie cyberbezpieczeństwa wśród organów właściwych wymieniła Ministra Obrony Narodowej jako organ właściwy w stosunku do podmiotów określonych w art. 26 ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa dotyczy to już wskazanych wyżej podmiotów koordynowanych przez CSIRT MON, które są podległe ministrowi lub przez niego nadzorowanych, których systemy teleinformatyczne chodzą w skład infrastruktury krytycznej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym w stosunku do których organem orgaznizującym i nadzorującym wykonywania zadań na rzecz obronności jest właśnie Minister Obrony Narodowej. Ustawa wyróżnia uprawnienia jakie przysługują organom właściwym. Są to:

[23] M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, nr 1, s. 90.

- prowadzi bieżącą analizę podmiotów w danym sektorze pod kątem uznania ich za operatora usługi kluczowej
- wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej
- po wydaniu wskazanej wyżej decyzji, niezwłocznie przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu;
- składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;
- przygotowuje we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
- monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych;
- wzywa na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;
- prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych
- może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;
- przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;
- uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej[24].

Biorąc pod uwagę wskazane zadania, szczególną uwagę należy zwrócić na te zadania w kontekście uprawnień organu administracji publicznej, czyli kompetencji do wydania decyzji administracyjnej zgodnie z kodeksem postępowania nadzorcze, uprawnienia nadzorcze

[24] Art. 42 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.

i czynności materialno-techniczne. Wyodrębnienie ostatniego wskazanego zadania wskazuje na obligatoryjne uczestniczenie w ćwiczeniach z zakresu cyberbezpieczeństwa. Zdaniem K. Walczuka jest to wyraźne odniesienie do bezpieczeństwa regionalnego bez odniesienia do bezpieczeństwa globalnego, którego gwarantem jest Pakt Północnoatlantycki. Niemniej z art. 51 i 52 wyraźnie kształtuje się współpraca Sił Zbrojnych RP w obszarze obrony narodowej w zakresie cyberbezpieczeństwa z właściwymi organami UE, ale i także z NATO i innymi organizacjami międzynarodowymi. Odwołanie do ćwiczeń odbywanych tylko w UE związane jest z implementacją dyrektywy NIS, co nie powinno uzasadniać ograniczeń tylko na regionalny wymiar cyberbezpieczeństwa[25].

Zadania ministra obrony w zakresie cyberbezpieczeństwa formułuje ustawa o krajowym systemie cyberbezpieczeństwa. Określono zamknięty katalog w art. 51, w którym wskazane zadanie poza kierowaniem działaniami związanymi z obsługą incydentu krytycznego mają charakter nie władczy. Z tego katalogu można wyodrębnić następujący katalog zadań:

- współpracę Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa;
- zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych, a także poprzez organizację specjalistycznych przedsięwzięć szkoleniowych;
- pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej;
- kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego;
- ocenę wpływu incydentów na system obrony państwa i zagrożeń cyberbezpieczeństwa w czasie stanu wojennego;
- przedstawianie właściwym organom propozycji dotyczących działań obronnych;
- koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji

[25] K. Walczuk, *Komentarz do art. 43,* w: *Ustawa o krajowym systemie cyberbezpieczeństwa Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019,s. 272-273.

rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa.

Budowanie zdolności cyberbezpieczeństwa w Siłach Zbrojnych jako zadania określone w ramach pozyskiwania i rozwoju narzędzi służących budowaniu zdolność cyberbezpieczeństwa w SZ może zostać zakwalifikowane jako zadania władcze, które będzie miało podstawę do wykonywania zadań o charakterze cywilnoprawnym. Minister Obrony Narodowej wykonuje swoje zadania w czasie normalnego funkcjonowania państwa, jak i w czasie stanu wojennego. We wskazanych zadaniach minister realizuje zadania w ramach funkcji kierowniczej, jak i w ramach funkcji kontrolnej. Należy zwrócić uwagę na konieczność wyposażenia ministra w kompetencje, które umożliwią pozyskanie pełnej i kompleksowej informacji. Ostatnią funkcją wymienioną jest funkcja koordynacyjna ministra, która we wskazanych przepisach została ograniczona do czasu stanu wojennego, z czego można wywnioskować, że w czasie pokoju minister nie wykonuje takich zadań[26]. Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego[27].

Minister Obrony Narodowej powołał decyzją z 25 stycznia 2019 r. 28 pełnomocnika do spraw bezpieczeństwa cybernetycznego. Pełnomocnik, działając w imieniu Ministra Obrony Narodowej:

- wydaje wytyczne w sprawach bezpieczeństwa cyberprzestrzeni w odniesieniu do komórek i jednostek organizacyjnych resortu obrony narodowej, z wyłączeniem zadań zastrzeżonych dla pełnomocników do spraw ochrony informacji niejawnych,
- inicjuje oraz wspiera działania komórek i jednostek organizacyjnych resortu obrony narodowej w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;
- sprawuje nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;

[26] K. Wąsowski, *Komentarz do art. 51* w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s.
[27] Art. 52 ustawy o krajowym systemie cyberbezpieczeństwa.
[28] Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 25 stycznia 2019 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw bezpieczeństwa cyberprzestrzeni, Dz. Urz. MON 2019.19.

- współpracuje ze Służbą Kontrwywiadu Wojskowego w zakresie kreowania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni resortu obrony narodowej;
- reprezentuje resortu obrony narodowej w pracach kierowniczych gremiów (komitetów, zespołów, grup) Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej w zakresie bezpieczeństwa cyberprzestrzeni;
- przygotowuje do dnia 15 kwietnia każdego roku kalendarzowego, dla Ministra Obrony Narodowej, we współpracy z Szefem Sztabu Generalnego Wojska Polskiego, Szefem Służby Kontrwywiadu Wojskowego, Pełnomocnikiem Ministra Obrony Narodowej do spraw Ochrony Informacji Niejawnych - Dyrektorem Departamentu Ochrony Informacji Niejawnych oraz Dyrektorem Narodowego Centrum Kryptologii, roczny raport o stanie bezpieczeństwa cyberprzestrzeni w resorcie obrony narodowej.

Pełnomocnik Ministra Obrony Narodowej aby realizować wskazane zadania może żądać informacji, stanowisk i sprawozdań przygotowywanych resorcie MON, dokonywać ocen i formułować wnioski w zakresie realizacji zadań związanych z cyberbezpieczeństwem, a także zlecać w tym zakresie badania, analizy i ekspertyzy. Pełnomocnik Ministra Obrony Narodowej

może podejmować współpracę z organami administracji publicznej i organizacjami pozarządowymi oraz podmiotami krajowymi i międzynarodowymi wykonywanie zadań związanych z bezpieczeństwem cyberprzestrzeni[29]. Minister obrony Narodowej jako centralny organ administracji rządowej realizuje zadania poprzez przewidziane prawem formy działania. Poprzez tworzenie aktów normatywnych, zawieraniu umów z podmiotami realizującymi zadania z zakresu cyberbzpieczeństwa czy też wydawaniu jako organ właściwy decyzji administracyjnej.

CSIRT MON

Implementacja dyrektywy NIS w drodze ustawy o krajowym systemie cyberbezpieczeństwa wprowadziła system obsługi incydentów, wyróżniając CISRT GOV, CISRT MON i CISRT NASK. Do zadań CSIRT MON należy koordynacją obsługi incydentów zgłaszanych przez podmioty podległe ministrowi obrony narodowej lub przez nie nadzorowane, w tym podmioty, których systemy teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, którą sporządził dyrektor rządowego centrum

[29] M. Karpiuk, *Tasks of the Minister of National Defense*..., s. 89.

bezpieczeństwa na podstawie ustawy o zarządzaniu kryzysowym[30]. Do zadania CSIRT MON należy także koordynacja obsługi incydentów zgłoszonych przez przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej. W tym zakresie za bezpieczeństwo komputerowe odpowiada Minister Obrony Narodowej. Zespoły Reagowania na Incydenty działającą na szczeblu krajowym stanowią część krajowego systemu cyberbezpieczeństwa. Celem tego systemu jest zapewnienie bezpieczeństwa państwa, w tym nieprzerwanego świadczenia usług kluczowych i usług cyfrowych, poprzez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów wykorzystywanych od dostarczania usług i zapewnienia obsługi incydentów[31]. Stąd właśnie zespół CSIRT MON (obok CSIRT GOV i CSIRT NASK) jest kompetentny w zakresie incydentów do zdarzeń o charakterze terrorystycznym zagrażających bezpieczeństwu obronności państwa potencjału, Sił Zbrojnych RP i organizacji jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Podstawą prawną działania pozostaje art. 27 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa[32]. Zespoły reagowania CSIRT współpracują ze sobą opracowując główne elementy procedur postępowania w przypadku incydentu, którego koordynacja wymaga współpracy. Określają we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu. Jednocześnie zespoły CSIRT w drodze porozumienia mogą powierzać sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów. Z ustawy o krajowym systemie cyberbezpieczeństwa w zakresie cyberbezpieczeństwa wynika możliwość wykonywania przez zespoły CSIRT badań urządzeń lub oprogramowania w celu identyfikacji podatności, które wykorzystywane mogą być w celu zagrożenia integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Na podstawie tych badań CSIRT mogą składać rekomendacje w celu usunięcia podatności urządzeń lub oprogramowania stosowane przez podmioty krajowego systemu cyberbezpieczeństwa.

PODSUMOWANIE

[30] M. Nowikowska, *Komentarz do art. 26*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa*…, s. 198.
[31] Art. 3 ustawy o krajowym systemie cyberbezpieczeństwa.
[32] M. Karpiuk, op. cit., s. 91.

Zapewnienie bezpieczeństwa, w tym bezpieczeństwa cyfrowego jest podstawowym zadaniem władzy publicznej. Minister Obrony Narodowej jako centralny organ administracji rządowej kierujący działem administracji rządowej realizuje swoje zadania ustawowe poprzez realizację konkretnych form działania. Zakres działania Ministra obejmuje w czasie pokoju wszystkimi działaniami Sił Zbrojnych, w tym zapobieganie zagrożeniom cyberbezpieczeństwa wymagającym podjęcia środków obronnych w celu rozwijania zdolności i zapewnienia bezpieczeństwa cybernetycznego Sił Zbrojnych RP. Szczególnie ważne, w celu podnoszenia poziomu bezpieczeństwa cybernetycznego jest badanie rodzajów zagrożeń, monitorowanie ich nasilania i systemowe zwalczanie. W tym zakresie należy szczególną uwagę skupić na rozbudowywaniu specjalistycznego komponentu Sił Zbrojnych Wojsk Obrony Cyberprzestrzeni. Ustawodawca powinien wyposażyć także Ministra Obrony Narodowej w szersze kompetencje w zakresie koordynowania i kontrolowania wykonywania zadań wynikających z zakresu ustawy o krajowym systemie cyberbezpieczeństwa. Nie do przecenienia pozostaje także edukacja i to edukacja w podwójnym wymiarze. Można określić, że powszechna edukacja społeczna, w której w ramach zrozumiałych komunikatów zarówno organy właściwe, jak inne podmioty takie jak CISIRT będą prowadziły kampanie jak walczyć z zagrożeniami w sieci i z dezinformacją. Organy właściwe mają doświadczenie w tym zakresie, prowadziły już podobne kampanie. Niemniej jednak zagrożenia stają się powszechne i przybierają bardziej agresywne formy, tym bardziej organy właściwe i CSIRT, zachowując oczywiście informację związane z zagrożeniem bezpieczeństwa państwa, informować i edukować. Stąd nie do przecenienia pozostaje aktywność, w ramach kompetencji ustawowych, rola ministra obrony narodowej. Opracowanie i wdrażanie polityki cyberbezpieczeństwa, poprzez realizację przepisów UE, ustaw i celów Strategii Cyberbezpieczństwa, koncentrują się na budowaniu wspólnych zdolności reagowania na cyberatak i zapewnienia cyberbezpieczństwa.

BIBLIOGRAFIA
REFERENCES LIST

Chałubińska – Jentkiewicz K., Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2019, nr 2, s. 20.

Chałubińska-Jentkiewicz K., Brzostek A., *Strategie cyberbezpieczeństwa we współczesnym świecie*, Warszawa 2021.

Czarny P., *Komentarz do art. 134* w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* wyd. II, 2023.

Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity,* „Cybersecurity and Law" 2022, nr 1.

Kuś B., *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadeniania organizacyjno-prawne*, "Cybersecurity and Law" 2023, nr10.

Morawski Z., *Status prawny Ministra Obrony Narodowej i Szefa Sztabu Generalnego,* „Wojskowy Przegląd Prawniczy" 2011, nr 4.

Nowikowska M., *Komentarz do art. 26,* w: *Ustawa o krajowym systemie cyberbezpieczeństwa,* red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Padzik J., *Prawonoustrojowa pozycja ministra obrony narodowej w systemie organów administracji rządowej*, „Bezpieczeństwo Narodowe" 20, IV-2011.

Radoniewicz F., *Komentarz do art. 2,* w: *Ustawa o krajowym systemie cyberbezpieczeństwa*. *Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 31-33.

Serowaniec M., Rola ministra obrony narodowej w cywilnym modelu zwierzchnictwa nad Siłami zbrojnymi RP, „Gdańskie Studia Prawnicze" 2018, tom XL.

Wąsowski K., Komentarz do art. 51 w: U*stawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Wąsowski K., *Tasks of the Minister of National Defense in the field of cybersecurity,* w: *Cybersecurity in Poland. Legal Aspects*, ed. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Springer 2022.

Walczuk K., *Komentarz do art. 43,* w: *Ustawa o krajowym systemie cyberbezpieczeństwa Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

ŹRÓDŁA

SOURCES

Wyrok Trybunału Konstytucyjnego z dnia 27 czerwca 2008 r., K 52/07.