WIEDZA OBRONNA
2022, Vol. 279 No. 2
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2022-j279

MARCIN KOŚKA *
Uniwersytet Jana Kochanowskiego, Piotrków Trybunalski, Polska

CYBERTERRORYZM - ZADANIA ANTYTERRORYSTYCZNE SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ W KONTEKŚCIE OBOWIĄZUJĄCYCH AKTÓW PRAWNYCH

CYBERTERRORISM - ANTITERRORIST TASKS OF THE POLISH ARMED FORCES IN THE CONTEXT OF APPLICABLE LEGAL ACTS

ABSTRAKT: Artykuł jest sprawozdaniem z badań dotyczących zadań Sił Zbrojnych Rzeczypospolitej Polskiej realizowanych celem przeciwstawienia się zagrożeniom o charakterze terrorystycznym w cyberprzestrzeni. Badaniami zostały objęte zasadnicze akty polskiego prawa regulujące powyższą tematykę. Przedstawiane przedsięwzięcia sił zbrojnych powiązane są z zadaniami realizowanymi w celu zapewnienia bezpieczeństwa w cyberprzestrzeni. Artykuł ponadto, przedstawia terminologię z zakresu cyberbezpieczeństwa obowiązującą zarówno Polsce, jak i w międzynarodowych organizacjach takich, jak Sojusz Północnoatlantycki oraz Unia Europejska.

SŁOWA KLUCZOWE: siły zbrojne, cyberterroryzm, cyberprzestrzeń, cyberbezpieczeństwo.

ABSTRACT: The article is a report on the research on the tasks of the Armed Forces of the Republic of Poland carried out in order to counter terrorist threats in cyberspace. The research covered the main acts of Polish law regulating the above-mentioned issues. The presented undertakings of the armed forces are related to the tasks performed to ensure security in cyberspace. In addition, the article presents the terminology in the field of

* dr Marcin Kośka, Jan Kochanowski University, Piotrków Trybunalski, Polska
https://orcid.org/0000-0003-0672-2330 email: marcin.koska@ujk.edu.pl

cybersecurity in force both in Poland and in international organizations such as the North Atlantic Alliance and the European Union.

KEYWORDS: armed forces, cyberterrorism, cyberspace, cyber security.

WPROWADZENIE

Terroryzm jest zagrożeniem, z którym ludzkość miała do czynienia już przed naszą erą. Przykładem było m.in. zabicie władcy Rzymu Juliusza Cezara. Rozkwit społeczeństw obejmujący ponad dwa tysiąclecia postępu, w tym nowe technologie, umożliwiły rozwój w różnych obszarach. Zmienił się również terroryzm. Jednym z jego stosunkowo nowych postaci jest cyberterroryzm, który określany jest m.in. jako użycie cyberprzestrzeni do celów terrorystycznych, zdefiniowanych przez prawo krajowe lub międzynarodowe[2]. Niestety, czasami może budzić trudność zaklasyfikowanie ataku w cyberprzestrzeni jako czynu o charakterze terrorystycznym. Przykładowo, skradzione informacje ze skrzynek pocztowych polityków mogą być wykorzystane zarówno do wymuszenia podjęcia określonych decyzji politycznych, jak i do szantażu w celu uzyskania korzyści majątkowych. Mając na uwadze fakt, że trudno jest jednoznacznie określić, z jakim zdarzeniem mamy do czynienia i jakie mogą być jego skutki, polski system bezpieczeństwa cyberprzestrzeni powinien wykrywać możliwie największą ilość incydentów. Szczególnie incydentów krytycznych, poważnych i incydentów w podmiocie publicznym. W związku z powyższym, zadania Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP) przeciwko zagrożeniom cyberterrorystycznym powinny być realizowane w ramach ogólnego systemu bezpieczeństwa cyberprzestrzeni.

Jak już wspomniano, zaklasyfikowanie incydentu jako terrorystyczny, może przysporzyć wiele trudności. Przykładowo, w 1997 r. w Worcester w Stanach Zjednoczonych Ameryki, napastnik odciął port lotniczy od sieci telefonicznej. Tym samym, w znacznym stopniu utrudnił wieży kontroli lotów świadczenie usług w zakresie bezpieczeństwa żeglugi powietrznej[3]. Inny przykład to zamach w 2000 r. w stanie Queensland w Australii, gdzie terrorysta korzystając z dostępu do Internetu, radia oraz wykradzionego oprogramowania spowodował spuszczenie

[2] J.B. Godwin II, A. Kulpin, K.F. Rauscher, V. Yaschenko, *Critical Terminology Foundations 2*, The EastWest Institute New York - Information Security Institute Moscow State University 2014, s. 30.

[3] https://mlodytechnik.pl/technika/28586-cyberterroryzm-rozkwita-ogniem-i-netem (dostęp: 12.01.2022).

miliona ścieków do rzeki i wód przybrzeżnych nadmorskiego miasta Maroochydore. Na skutek ataku, w wodach, gdzie znalazły się ścieki zamarło życie biologiczne. Mieszkańcy zamieszkujący obszary objęte wyciekiem zostali zmuszeni do opuszczenia miejsc zamieszkania na wiele tygodni ze względu na panujące warunki[4]. Atak w cyberprzestrzeni, który można określić jako terrorystyczny miał miejsce również w Polsce. W styczniu 2012 r., grupa Anonymus zablokowała strony rządowe m.in.: Sejmu, Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Ministerstwa Kultury i Dziedzictwa Narodowego, jak również Stowarzyszenia Autorów ZAIKS. Celem ataku było wywarcie presji na polski rząd, aby nie podpisywał międzynarodowego porozumienia Anti-Counterfeiting Trade Agreement (ACTA) dotyczącego ochrony praw własności intelektualnych[5].

Mając na uwadze fakt, że zagrożenia atakami terrorystycznymi są realne, polski ustawodawca przyjął akty prawne umożliwiające przeciwdziałanie tego typu zagrożeniom. Dokumentem, który w największym stopniu dotyczy bezpieczeństwa w cyberprzestrzeni jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Należy nadmienić, że SZ RP są częścią tego systemu. Oprócz już wymienionego aktu prawnego, drugim istotnym dokumentem dotyczącym cyberprzestrzeni, a dokładnie przedstawiającym zadania realizowane w przypadku wystąpienia zagrożeń terrorystycznych, jest ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Niniejszy artykuł przedstawia wyniki badań, które miały na celu identyfikację zadań antyterrorystycznych realizowanych przez SZ RP w cyberprzestrzeni na podstawie przepisów polskiego prawa. Realizowane badania miały swoje ograniczenia, a mianowicie analizowano akty prawne omawiające zadania wykonywane w czasie pokoju. Nie brano pod uwagę zadań realizowanych po wprowadzeniu stanów nadzwyczajnych[6] i w czasie wojny.

Opracowanie zostało podzielone na cztery części, a mianowicie: wstęp, aparat pojęciowy, zadania wynikające z aktów prawnych oraz podsumowanie. We wstępie przedstawiono zarys prowadzonych badań. W części nazwanej aparat pojęciowy, wyjaśniono znaczenia kluczowych

[4] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty naukowe Akademii Marynarki Wojennej rok XLVI Nr 1 (160)", Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2005, s. 179.

[5] M. Proszowski, J. Satora, *Atak za ACTA: Rządowe strony zablokowane,* Dziennik Rzeczypospolita https://www.rp.pl/kraj/art6300061-atak-za-acta-rzadowe-strony-zablokowane (dostęp: 12.01.2022).

[6] Należy nadmienić, że w przypadku zewnętrznego zagrożenia państwa, w tym zagrożenia w cyberprzestrzeni, Prezydent RP może wprowadzić stan wojenny na wniosek Rady Ministrów. 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. z 2017 r. poz. 1932), art. 2 ust. 1.

pojęć użytych w artykule. Z kolei zadania wynikające z aktów prawnych przedstawiają przedsięwzięcia SZ RP dotyczące działań antyterrorystycznych ujętych w przepisach ustawy o krajowym systemie cyberbezpieczeństwa, o działaniach antyterrorystycznych oraz w akcie w wykonawczym do tej ustawy. W podsumowaniu ujęto wnioski z prowadzonych badań.

APARAT POJĘCIOWY

Polska jest częścią Organizacji Traktatu Północnoatlantyckiego (ang. North Atlantic Treaty Organization - NATO) i mając na uwadze wspólne przeciwdziałanie zagrożeniom w cyberprzestrzeni, rozumienie terminów takich, jak cyberprzestrzeń, czy cyberbezpieczeństwo powinno być podobne w celu zapewnienia interoperacyjności. Zgodnie z doktryną NATO, cyberprzestrzeń jest globalną domeną, na którą składają się wszystkie połączone systemy komunikacyjne, informatyczne i inne systemy elektroniczne, sieci i ich dane, w tym te oddzielone lub niezależne, które przetwarzają, przechowują lub przesyłają dane[7]. W polskich aktach prawnych, cyberprzestrzeń określona jest jako przestrzeń przetwarzania i wymiany informacji, którą tworzą systemy teleinformatyczne[8] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[9].

Z kolei cyberbezpieczeństwo w NATO rozumiane jest jako stosowanie środków bezpieczeństwa w celu ochrony komunikacji, informacji i innych systemów elektronicznych oraz informacji przechowywanych, przetwarzanych lub przesyłanych w tych systemach w odniesieniu do poufności, integralności, dostępności, wiarygodności i niezaprzeczalności (autentyczności źródła pochodzenia)[10]. Zgodnie z polską ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, cyberbezpieczeństwo oznacza odporność systemów

[7] *Allied Joint Doctrine for Cyberspace Operations AJP-3.20*, NATO Standardization Office, Bruksela 2020 r., str. 24, tłum. własne. W oryginale, w języku angielskim: Cyberspace - the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.

[8] System teleinformatyczny rozumiany jest jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. z 2021 r. poz. 2070), art. 3 pkt 3.

[9] Dz.U. z 2017 r. poz. 1932, art. 2 ust. 1b.

[10] *Allied Joint Doctrine for Cyberspace Operations*…, dz. cyt., str. 24, tłum. własne. W oryginale, w języku angielskim: Cyber Security - the application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[11].

Oba terminy są podobnie rozumiane zarówno w Sojuszu jak i w Polsce, co wpływa pozytywnie na zapewnienie interoperacyjności. Należy także zauważyć, że Polska jest członkiem Unii Europejskiej (UE), gdzie cyberbezpieczeństwo oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników tych systemów oraz innych osób przed cyberzagrożeniami[12].

W UE sieci i systemy teleinformatyczne oznaczają:

- sieci łączności elektronicznej;
- wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub
- dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w poprzednich tiretach, w celu ich eksploatacji, użycia i utrzymania[13]

Bezpieczeństwo sieci i systemów informatycznych oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne[14].

Polska, jako członek UE, zobowiązana jest do stosowania dyrektyw Unijnych, co też widać przy porównaniu definicji. Niemiej jednak, bez względu na fakt czy mamy do czynienia z definicjami Polskimi, Sojuszniczymi czy Unijnymi, cyberbezpieczeństwo (bezpieczeństwo sieci i systemów informatycznych), czy cyberprzestrzeń rozumiane jest podobnie mimo użycia innych słów do ich zdefiniowania. Podobne postrzeganie bezpieczeństwa umożliwia współdziałanie ze

[11] Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 2020 r. poz. 1369), art. 2 pkt. 4.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. *w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)* (Dz.U. UE L 151/15 z 17.04.2019), art. 2 pkt 1.

[13] 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 194/1 z 6.07.2016) art. 4 pkt 1.

[14] Tamże, art. 4 pkt 2.

sobą elementów odpowiedzialnych za bezpieczeństwo zarówno w kraju jak i w ramach organizacji międzynarodowych, których Polska jest członkiem.

Oprócz dotychczas omówionych terminów, należy jeszcze wyjaśnić znaczenie pojęcia incydent, ponieważ jest ono istotne dla omawianych w niniejszym opracowaniu kwestii. Jego słownikowe znaczenie jest powszechnie znane jako niespodziewane i nieprzyjemnie w skutkach zdarzenie[15]. Jednakże ustawodawca, dla potrzeb jednakowego rozumienia przepisów dotyczących cyberprzestrzeni, incydentem nazwał zdarzenie mające niekorzystny wpływ na cyberbezpieczeństwo. Ponadto, dokonał typizacji incydentów na krytyczne, poważne, istotne oraz incydenty w podmiocie publicznym. Incydent krytyczny to taki, którego konsekwencje przynoszą znaczne szkody dla bezpieczeństwa i porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich, zdrowia i życia ludzi. Incydent poważny z kolei, powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości usługi kluczowej. Incydent istotny to taki, który ma istotny[16] wpływ na świadczenie usługi cyfrowej. Incydent w podmiocie publicznym[17] rozumiany jest jako incydent powodujący lub mogący spowodować obniżenie jakości lub przerwanie przez podmiot publiczny realizowanego zadania publicznego[18].

Analizując znaczenia poszczególnych typów incydentów, do zdarzeń o charakterze terrorystycznym można zaliczyć incydenty krytyczne. Choć nie każdy incydent krytyczny będzie miał charakter terrorystyczny. Uznanie incydentu krytycznego za działanie terrorystyczne będzie zależało od dodatkowych czynników. Zgodnie polskim prawem, a dokładnie z § 20 art.

[15] https://sjp.pl/incydent (dostęp: 17.06.2021).

[16] Uznaje się, że incydent ma istotny wpływ, jeśli wystąpił jeden z czterech poniższych przypadków. Pierwszy, gdy usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 mln użytkownikogodzin (ilość odciętych od usługi użytkowników UE przez godzinę). Drugi, gdy została utracona integralność, autentyczność lub poufność przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług cyfrowych a w takiej sytuacji znalazło się ponad 100 tys. użytkowników UE. Trzeci, gdy na skutek incydentu wystąpiło ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych. Czwarty, gdy konsekwencją incydentu dla jednego lub więcej użytkowników UE są straty materialne przekraczające co najmniej 1 mln EUR. Rozporządzenie wykonawcze komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26/48 z 31.01.2018), art. 4 ust. 1.

[17] Incydent w podmiocie publicznym dotyczy instytutów badawczych. Do Wojskowych Instytutów Badawczych zaliczają się: Wojskowy Instytut Techniczny Uzbrojenia; Wojskowy Instytut Łączności, Wojskowy Instytut Chemii i Radiometrii, Wojskowy Instytut Techniki Pancernej i Samochodowej, Wojskowy Instytut Techniki Inżynieryjnej, Wojskowy Instytut Medycyny Lotniczej, Wojskowy Instytut Medyczny, Wojskowy Instytut Higieny i Epidemiologii oraz Instytut Techniczny Wojsk Lotniczych. Dz.U. z 2020 r. poz. 1369, art. 4 pkt. 8; https://www.gov.pl/web/obrona-narodowa/wojskowe-instytuty-badawcze (dostęp: 22.06.2021 r.).

[18] Dz.U. z 2020 r. poz. 1369, art. 2 pkt. 5-9.

115 Kodeksu karnego, za przestępstwo o charakterze terrorystycznym uznaje się czyn zabroniony, który jest zagrożony karą pozbawienia wolności o górnej granicy co najmniej 5 lat oraz popełniony (lub groźba popełnienia) w celu: poważnego zastraszenia wielu osób; zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej[19]. Przy czym nie można wykluczyć, że incydenty inne niż krytyczne nie będą miały związku z zagrożeniami terrorystycznymi.

Zapewnienie bezpieczeństwa w cyberprzestrzeni jest problematyczne ze względu na powszechność wykorzystywania różnego rodzaju urządzeń podłączonych do sieci (m.in. telefony, komputery) oraz usług, które dostępne są m.in. dla żołnierzy. Powyższe wymaga od sił zbrojnych wykrywania i obsługi różnego rodzaju zdarzeń, do których zaliczają się również zdarzenia związane z terroryzmem. Trudność polega na ocenie, czy zdarzenie, z którym mamy do czynienia ma charakter terrorystyczny[20], czy też nie. Jeżeli z incydentu bezpośrednio nie wynika jego charakter, niezbędnym może być pozyskanie dodatkowych informacji z innych źródeł pozwalających określić, czy jest on związany z terroryzmem. Nie można wykluczyć przypadku, gdy posiadane informacje nie pozwolą na zaklasyfikowanie zdarzenia jako incydentu terrorystycznego. Dopiero po jakimś czasie może okazać się, że zdarzenie, które wystąpiło w przeszłości miało charakter terrorystyczny ze względu na swoje implikacje. W związku z powyższym, zadania realizowane w celu przeciwdziałania incydentom o charakterze terrorystycznym, będą tożsame z zadaniami realizowanymi w celu przeciwdziałania innym incydentom i służące zapewnieniu ogólnopojętego cyberbezpieczeństwa.

ZADANIA WYNIKAJĄCE Z AKTÓW PRAWNYCH

Ustawa o krajowym systemie cyberbezpieczeństwa

Siły Zbrojne RP realizują zadania w zakresie przeciwdziałania zagrożeniom terrorystycznym w przestrzeni powietrznej, morskiej i lądowej jak również w cyberprzestrzeni[21]. Dokumentem

[19] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. Nr 88 poz. 553), art. 115 § 20.

[20] Nie zawsze będzie można jednoznacznie stwierdzić, że zostało popełnione przestępstwo o charakterze terrorystycznym.

[21] Zgodnie ze strategią Cyberbezpieczeństwa RP na lata 2019-2024 dąży się do pozyskania przez SZ RP zdolności do realizacji pełnego spektrum działań militarnych w cyberprzestrzeni na takim samym poziomie jak w domenie lądowej, powietrznej czy morskiej. Do zdolności tych zalicza się m.in. rozpoznanie zagrożeń, ochronę i obronę sieci i systemów teleinformatycznych oraz zwalczanie źródeł cyberzagrożeń. Uchwała nr 125 Rady Ministrów z dnia 22

rangi ustawy, w którym określono zadania w cyberprzestrzeni dla resortu obrony narodowej jest ustawa o krajowym systemie cyberbezpieczeństwa. Z uwagi na fakt, że z racji pełnionej funkcji Minister Obrony Narodowej (MON) odpowiedzialny jest za całokształt przedsięwzięć realizowanych przez resort obrony, to jego zadania zostaną przedstawione w pierwszej kolejności, a następnie zadania innych elementów.

Ataki terrorystyczne w cyberprzestrzeni mogą być przeprowadzane z wykorzystaniem np. sieci Internet[22], która ma zasięg globalny. Niemniej jednak to nie jedyna sieć, w której możemy mieć do czynienia z incydentami terrorystycznymi. Tego typu sytuacje mogą mieć miejsce m.in. w sieciach sojuszniczych[23]. W związku z powyższym nie może dziwić fakt, że jednym z zadań MON jest odpowiedzialność za współpracę w obszarze obrony narodowej w zakresie cyberbezpieczeństwa z właściwymi elementami w NATO, Unii Europejskiej oraz w innych organizacjach międzynarodowych. Kolejnym zadaniem jest zapewnienie SZ RP zdolności do prowadzenia działań militarnych w układzie krajowym, w ramach sojuszu oraz z koalicjantami, w sytuacji zagrożenia cyberbezpieczeństwa, które powoduje konieczność działań obronnych. Ustawodawca narzucił powyższe zadanie MON m.in. z powodu możliwości wystąpienia ataków terrorystycznych w cyberprzestrzeni, którym można przeciwstawić się militarnie. Następnym zadaniem dla MON jest rozwijanie umiejętności zapewniających siłom zbrojnym cyberbezpieczeństwo poprzez organizację specjalistycznych przedsięwzięć szkoleniowych. Przy tym zadaniu należy podkreślić, że brak wiedzy z zakresu bezpieczeństwa teleinformatycznego może w znacznym stopniu przyczynić się do większej podatności sił zbrojnych na ataki terrorystyczne. W związku z tym, za konieczne należy uznać rozwijanie umiejętności zarówno użytkowników urządzeń końcowych jak i osób odpowiedzialnych za utrzymanie infrastruktury sieci teleinformatycznych oraz zapewniających im bezpieczeństwo. MON odpowiada również za pozyskiwanie i rozwój narzędzi używanych do budowy zdolności zapewniających

października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* (M.P. z 2019 r. poz. 1037), załącznik s. 19.

[22] Do Internetu połączona jest m.in. sieć teleinformatyczna SZ RP o nazwie MILNET-I i prawdopodobnie z tego względu jest najbardziej narażona na ataki cybernetyczne. Służy ona do przetwarzania dokumentów o klauzuli jawne. Oprócz wyżej wymienionej, w SZ RP wykorzystywane są sieci służące do przetwarzania dokumentów niejawnych o różnych klauzulach o zasięgu zarówno krajowym jak i międzynarodowym. Do sieci tych zaliczają się m.in. MILNET-Z, BERYL, RUBIN, SPINEL, NOAN, BICES, PF-WAN. A. Pestkowski, *Cyberbezpieczeństwo infrastruktury krytycznej nadzorowanej przez administrację samorządową (rozprawa doktorska),* Akademia Sztuki Wojennej, Warszawa 2020, s. 143, 149.

[23] NS WAN (ang. NATO Secret Wide Area Network) to rozległa sieć teleinformatyczna służąca do przetwarzania informacji do klauzuli NATO SECRET. Decyzja Nr 74/Mon Ministra Obrony Narodowej z dnia 27 marca 2013 r. *w sprawie eksploatacji niejawnego systemu teleinformatycznego PL_NS NOAN* (Dz.Urz. MON z 2013 r. poz. 82), ust. 1 pkt 8, ust. 2.

cyberbezpieczeństwo w wojsku. Powyższe jest konieczne m.in. ze względu na ciągły rozwój technologii umożliwiający terrorystom przeprowadzanie coraz bardziej wyrafinowanych ataków. Ale to nie wszystko, warto wymienić jeszcze jedno zadanie polegające na ocenie wpływu incydentów (w tym o charakterze terrorystycznym) na system obronny państwa[24].

W ramach współpracy z NATO w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni, w tym m.in. przeciwdziałanie zagrożeniom terrorystycznym, MON odpowiedzialny jest za prowadzenie Narodowego Punktu Kontaktowego (NPK). Zadaniem NPK jest m.in.: zapewnienie współpracy z właściwymi organami Sojuszu Północnoatlantyckiego, jak również pomiędzy narodowymi i sojuszniczymi siłami zbrojnymi. Koordynuje on działania w zakresie wzmacniania zdolności obronnych do przeciwstawienia się zagrożeniom dla cyberbezpieczeństwa. Ponadto odpowiada za rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa dotyczących obrony narodowej oraz realizacji celów NATO w obszarze cyberbezpieczeństwa i kryptologii[25].

MON jest również organem właściwym do spraw cyberbezpieczeństwa dla podmiotów z sektora ochrony zdrowia, infrastruktury cyfrowej oraz dostawców usług cyfrowych, które są mu podległe lub przez niego nadzorowane oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, dla których jest on organem organizującym lub nadzorującym realizację zadań na rzecz obronności państwa. Jako organ nadzorujący, do jego zadań należy m.in.: przygotowanie, we współpracy z CSIRT MON, CSIRT GOV, CSIRT NASK oraz sektorowymi zespołami cyberbezpieczeństwa, wytycznych, które mają wzmocnić cyberbezpieczeństwo oraz sposoby zgłaszania incydentów. Wzywa, na wniosek CSIRT MON operatorów usług kluczowych oraz dostawców usług kluczowych, do usunięcia podatności, które mogą skutkować wystąpieniem poważnego, istotnego lub krytycznego incydentu, w tym o charakterze terrorystycznym. Uczestniczy w ćwiczeniach dotyczących cyberbezpieczeństwa organizowanych zarówno w Polsce jak i w UE. Może ustanowić dla danego sektora - sektorowy zespół cyberbezpieczeństwa[26]. W ramach realizacji zadań i w uzasadnionych przypadkach może

[24] Dz.U. z 2020 r. poz. 1369, art. 51 pkt. 1-4, 6.

[25] Tamże, art. 52.

[26] Jeżeli MON utworzy taki zespół, informuje o tym jak również o jego zadaniach operatorów usług kluczowych. Sektorowy zespół cyberbezpieczeństwa może być odpowiedzialny za odbieranie zgłoszeń dotyczących incydentów jak również wspieranie w ich obsłudze oraz wspieranie operatorów usług kluczowych w realizacji niektórych zadań. Dodatkowo, sektorowy zespół cyberbezpieczeństwa może mieć w obowiązkach analizę incydentów poważnych a co za tym idzie również szukanie powiązań pomiędzy incydentami jak również wyciągnie wniosków z obsługi incydentów. Ponadto może współpracować z CSIRT MON czy sektorowymi zespołami cyberbezpieczeństwa innych państw. Tamże, art. 44.

współpracować z organami ścigania. Należy podkreślić, że MON może powierzyć jednostkom podległym lub nadzorowanym, wykonywanie niektórych zadań organu właściwego do spraw cyberbezpieczeństwa[27].

Wymienione w poprzednich dwóch akapitach zadania MON, to oczywiście nie wszystko. Zgodnie z art. 27 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa, Minister prowadzi Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego[28] (CSIRT[29] MON), który działa na poziomie krajowym i jest właściwy m.in. w zakresie incydentów związanych ze zdarzeniami oraz przestępstwami (w tym o charakterze terrorystycznym), które godzą w bezpieczeństwo potencjału obronnego państwa polskiego, SZ RP oraz jednostek organizacyjnych podległych lub nadzorowanych przez MON. CSIRT MON jest właściwy w zakresie koordynacji obsługi incydentów zgłoszonych przez podległe oraz nadzorowane przez MON podmioty. W ramach wyżej wymienionych, mieszczą się także podmioty, których systemy lub sieci teleinformatyczne objęte są jednolitym wykazem instalacji, obiektów, urządzeń i usług wchodzących w skład infrastruktury krytycznej. Grupę uzupełniają przedsiębiorcy prowadzący działalność mającą szczególne znaczenie gospodarczo-obronne i w stosunku do których MON jest organem organizującym i nadzorującym realizację przedsięwzięć na rzecz obronności państwa. Mając na uwadze elementy leżące we właściwości CSIRT-u MON, do jego podstawowych zadań należą m.in.: reagowanie na zgłoszone incydenty w tym incydenty o charakterze terrorystycznym jak również klasyfikowanie incydentów oraz ewentualna zmiana ich klasyfikacji. Może prowadzić niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego, istotnego i krytycznego, wystąpić do właściwego organu do spraw cyberbezpieczeństwa o usunięcie przez operatorów kluczowych usług lub dostawców usługi cyfrowych podatności mogących m.in. umożliwić atak terrorystyczny w cyberprzestrzeni. CSIRT może wystąpić do operatorów usług kluczowych o informacje techniczne dotyczące incydentu krytycznego lub poważnego, niezbędne do analizy i koordynacji obsługi incydentu. W przypadku zidentyfikowania zagrożeń dla cyberbezpieczeństwa, w tym terrorystycznych, wydaje komunikaty o powyższym fakcie. Do istotnych zadań należą również: monitorowanie zagrożeń i incydentów na poziomie krajowym; szacowanie ryzyka (w tym prowadzenie dynamicznej analizy ryzyka), które związane jest z

[27] Tamże, art. 26 ust. 5, art. 41 pkt. 6, 9 i 11, art. 42 ust. 1 pkt. 5, 7, 11, ust. 3, ust. 7, art. 44 ust 1.

[28] Zespół realizuje również wytyczne Prezesa Rady Ministrów dotyczące obsługi incydentów krytycznych. Tamże, art. 67 ust. 2.

[29] Ang. Computer Security Incident Response Team.

zagrożeniami cyberbezpieczeństwa i zaistniałymi incydentami (w tym o charakterze terrorystycznym). CSIRT MON może prowadzić badania urządzeń informatycznych oraz oprogramowania, aby zidentyfikować podatności, które mogą zostać wykorzystane np. w trakcie cyberataku terrorystycznego. Tym samym mogą zagrozić integralności, poufności, rozliczalności, autentyczności lub dostępności danych, które są istotne z punkty widzenia bezpieczeństwa publicznego, lub interesu bezpieczeństwa państwa. Mając powyższe na uwadze, może zalecać stosowanie określonych urządzeń elektronicznych lub oprogramowania. Oprócz prowadzonych badań, CSIRT MON stanowi zaplecze analityczne oraz badawczo-rozwojowe w celu prowadzenia zaawansowanych analiz złośliwego programowania oraz podatności, monitorowania wskaźników świadczących o zagrożeniach w cyberprzestrzeni, rozwijania metod i narzędzi do wykrywania i zwalczania zagrożeń dla cyberbezpieczeństwa oraz opracowania standardów i dobrych praktyk, wspierania podmiotów systemu cyberbezpieczeństwa w Polsce i budowaniu ich potencjału i zdolności, budowania świadomości w obszarze cyberbezpieczeństwa. W jego obowiązkach leży informowanie podmiotów polskiego systemu cyberbezpieczeństwa o incydentach i ryzykach oraz wymiana informacji z państwami UE o incydentach poważnych lub istotnych dotyczących co najmniej dwóch państw członkowskich. Ponadto, przekazywanie informacji do Pojedynczego Punktu Kontaktowego[30] o poważnym lub istotnym incydencie dotyczącym dwóch lub większej ilości państw należących do UE. Dodatkowo, przekazywanie do Pojedynczego Punku Kontaktowego (PPK) zgłaszanych przez operatorów kluczowych usług rocznych zestawień poważnych incydentów, które wpływały na ciągłość świadczonych usług w kraju oraz w państwach UE, jak również zgłaszanych przez dostawców usług cyfrowych rocznych zestawień incydentów istotnych dotyczących co najmniej dwóch państw UE. CSIRT MON ma możliwość publikowania informacji o zagrożeniach w cyberprzestrzeni, podatnościach oraz incydentach krytycznych, jeżeli przyczynią się one do zwiększenia poziomu bezpieczeństwa systemów informacyjnych (w tym ochrony przez zagrożeniami o charakterze terrorystycznym) lub zapewnienia bezpiecznego użytkowania tych systemów. Dodatkowo, CSIRT MON, w ramach wykonywanych zadań, może korzystać z utrzymywanego i rozwijanego przez ministra właściwego do spraw informatyzacji systemu teleinformatycznego, który wspiera współpracę elementów krajowego systemu

[30] Organem prowadzącym Pojedynczy Punkt Kontaktowy jest minister właściwy do spraw informatyzacji. Wyznaczony jest m.in. do wymiany informacji dotyczącej cyberbezpieczeństwa pomiędzy Polską innymi krajami ramach UE. Dz.U. z 2020 r. poz. 1369, art. 48.

cyberbezpieczeństwa, zgłaszania i obsługi incydentów, ostrzeganie o zagrożeniach w cyberprzestrzeni w tym o zagrożeniach o charakterze terrorystycznym, szacowanie ryzyka na szczeblu krajowym oraz rekomendacji działań, które podnoszą bezpieczeństwo w cyberprzestrzeni. Należy podkreślić, że odbieranie zgłoszeń o incydentach czy przekazywanie informacji wymaga od CSIRT-u MON posiadania odpowiednich środków komunikacji wraz z obsługą, określenia sposobu realizacji i umieszczenie informacji o sposobie realizacji w Biuletynie Informacji Publicznej MON[31].

Jak już zostało wcześniej wspomniane CSIRT MON przekazuje informacji m.in. do PPK[32]. Oprócz przekazywania, również odbiera od PPK podobnego rodzaju informacje pochodzące z tożsamych punktów w innych krajach jak również inne informacje pochodzące m.in. z Grupy Współpracy[33]. PPK nie jest jedynym elementem, z którym realizowana jest współpraca. CSIRT MON jest częścią sieci CSIRT UE, w skład której wchodzą CSIRT-y państw członkowskich, ENISA oraz innych instytucji i agencji UE. Ponadto jest częścią krajowego systemu cyberbezpieczeństwa i w celu realizacji swoich zadań może współpracować m.in. z CSIRT GOV[34] i CSIRT NASK[35]. Współpraca obejmuje m.in. opracowanie procedur na wypadek zdarzenia, którego obsługa wymaga współdziałania CSIRT-ów, w tym przekazywanie informacji technicznych dotyczących incydentu, wzajemne powierzanie zadań - głównie w zakresie koordynacji zgłaszanych incydentów (na podstawie porozumień)[36], odbiór zgłoszeń o incydentach i niezwłoczne przekazanie ich do właściwego CSIRT-u, przejęcie i koordynacja lub

[31] Ustawa z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2006 r. nr 104 poz. 709), art. 5 ust. 1 pkt. 2a;* Dz.U. z 2020 r. poz. 1369, art. 2 ust. 2, art. 26 ust. 3 pkt 9 i 14 lit. a-f, pkt 15, ust. 5, art. 27 ust. 2, art. 31, art. 32 ust 1-3, art. 33 ust. 1,art. 35 ust. 5, art. 46 ust. 1.

[32] Za pomocą PPK informowane są inne państwa UE o incydentach poważnych dotyczących tych państw zgłoszonych przez operatorów kluczowych usług lub incydentach istotnych dotyczących co najmniej dwóch państw. Dz.U. z 2020 r. poz. 1369, art. 28 ust. 1 i 3, art. 29.

[33] Grupa Współpracy została ustanowiona w UE w celu wspierania i ułatwiania współpracy na poziomie strategicznym, wymiany informacji pomiędzy państwami Unii, rozwijania zaufania i pewności jak również osiągania wspólnego, wysokiego bezpieczeństwa sieci i systemów informatycznych wspólnoty. W skład grupy wchodzą przedstawiciele państw członkowskich, Komisji Europejskiej oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz.Urz. UE L 194/1 z 19.07.2016 r.), art. 11 ust. 1.

[34] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, który prowadzony jest przez Szefa ABW, realizuje zadania na poziomie krajowym. Dz.U. z 2020 r. poz. 1369, art. 2 pkt. 2.

[35] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, który prowadzony jest przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, realizuje zadania na poziomie krajowym. Dz.U. z 2020 r. poz. 1369, art. 2 pkt. 3.

[36] Powierzanie zadań jest formą wzajemnego wsparcia i optymalizacją wykorzystania potencjałów CSIRT-ów.

przekazanie obsługi incydentów związanych ze zdarzeniami o charakterze terrorystycznym[37], wzajemne informowanie (w tym RCB[38]) o incydentach krytycznych oraz o zagrożeniach cyberbezpieczeństwa[39], jak również opracowanie i przekazanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego[40]. Ponadto bierze udział z pozostałymi CSIRT-ami oraz sektorowymi zespołami cyberbezpieczeństwa[41] w określaniu współpracy obejmującej m.in. koordynację obsługi incydentów poważnych i krytycznych dotyczących Polski oraz więcej niż jednego państwa UE. Wymienia informacje z sektorowymi zespołami cyberbezpieczeństwa w celu przeciwdziałania zagrożeniom w cyberprzestrzeni, w tym o charakterze terrorystycznym. CSIRT MON współpracuje również operatorami usług kluczowych[42] podczas obsługi incydentu poważnego lub krytycznego, odbiera informacje od operatorów m.in. o incydentach (w tym informacje prawnie chronione), zagrożeniach cyberbezpieczeństwa, podatnościach, wykorzystywanych technologiach, dotyczące szacowania ryzyka jak również przekazuje operatorom zgłaszającym incydent poważny informacje o podjętych działaniach mające pomóc w jego obsłudze. Dane z wykazu operatorów usług kluczowych udostępniane są CSIRT-owi MON przez ministra właściwego do spraw informatyzacji. Kolejnym elementem, z którym współpracuje CSIRT MON, są organy ścigania (w tym Żandarmeria Wojskowa) i wymiar sprawiedliwości jak również służby specjalne w trakcie realizowanych przez nie zadań określonych przepisami stosownych ustaw. Wyżej wymienione organy będą zaangażowane w zatrzymanie, oskarżenie i skazanie sprawców ataków terrorystycznych. Jeśli, w wyniku zdarzenia o charakterze terrorystycznym w cyberprzestrzeni doszłoby do naruszenia danych osobowych, CSIRT MON może współpracować z organami do spraw ochrony danych osobowych, we właściwości których leżą zaatakowane

[37] CSIRT MON przejmuje koordynacje obsługi incydentów związanych z zagrożeniami terrorystycznymi dotyczącymi podmiotów leżących w jego właściwościach. Może też przekazać do CSIRT GOV obsługę tego typu incydentów, jeżeli dotyczą podmiotów, które nie leżą w jego odpowiedzialności.

[38] Do RCB, czyli Rządowego Centrum Bezpieczeństwa może być przesłana rekomendacja zwołania Rządowego Zespołu Zarządzania Kryzysowego. Dz.U. z 2020 r. poz. 1369, art. 35 ust. 2 pkt. 2, ust 3.

[39] Przekazywana informacja powinna zawierać wstępną analizę możliwych skutków zdarzenia. Ibidem, art. 35 ust. 2 pkt. 1.

[40] Dokument, w którym wskazuje się zagrożenia (oraz ich scenariusze) m.in. o charakterze terrorystycznym. https://www.gov.pl/web/rcb/raport-o-zagrozeniach-bezpieczenstwa-narodowego (dostęp: 22.06.2021 r.).

[41] Zespół cyberbezpieczeństwa ustanowiony przez właściwy organ do spraw cyberbezpieczeństwa dla sektora: energia, transport, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa. Dz.U. z 2020 r. poz. 1369, art. 44 ust. 1, załącznik nr 1.

[42] Wykaz kluczowych usług ujęty jest w Rozporządzeni 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).

przez terrorystów elementy. Dodatkowo CSIRT MON może współpracować z dostawcami usług cyfrowych, którzy zgłaszają do niego m.in. informacje o incydentach, współpracują przy ich obsłudze oraz zapewniają w niezbędnym zakresie dostęp do informacji o incydentach zakwalifikowanych jako krytyczne. Współpracuje również z podmiotami publicznymi m.in. w zakresie odbioru informacji o incydentach i obsługi incydentu w podmiocie publicznym oraz incydentu krytycznego. Nie należy zapominać o współpracy z Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa. Powyższa współpraca, obejmująca pozostałe CSIRT-y oraz ministra właściwego do spraw informatyzacji, ma na celu zapewnienie spójnego i kompletnego krajowego systemu zarządzania ryzykiem oraz przeciwdziałania zagrożeniom w cyberprzestrzeni o charakterze ponadsektorowym i transgranicznym oraz koordynację obsługi incydentów. Ogólnym przedsięwzięciem CSIRT-u MON jest nawiązywanie współpracy w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa[43].

Ustawa o działaniach antyterrorystycznych

Przedmiotowa ustawa jest zasadniczym aktem prawnym w Polsce dotyczącym działań antyterrorystycznych, niemiej jednak, nie obejmuje kompleksowo wszystkich zasad dotyczących tego typu działań. Powyższe dotyczy nie tylko domeny cyber, ale również morskiej, powietrznej i lądowej. W przypadku domeny cyber, w ustawie ujęto zasady wprowadzania stopni alarmowych CRP. Mianowicie, określone stopnie alarmowe wprowadza się w sytuacji zagrożenia polegającego na możliwości wystąpienia lub wystąpieniu zdarzenia mającego charakter terrorystyczny w systemach teleinformatycznych organów administracji publicznej lub wchodzących w skład infrastruktury krytycznej. Samo wprowadzenie stopnia bezpośrednio nie zależy od SZ RP (chyba, że posiadają informacje świadczące o konieczności wprowadzenia), ponieważ właściwy stopień alarmowy CRP[44] wprowadza Prezes Rady Ministrów (PRM), a w przypadkach niecierpiących zwłoki minister właściwy do spraw wewnętrznych. Po wprowadzeniu, zadaniem dla SZ RP, określonym przez przepisy ustawy, jest wydzielenie uczestników do sztabu koordynacyjnego powołanego przez Szefa ABW. Zadaniem sztabu koordynacyjnego jest przedstawianie propozycji w zakresie zmiany lub odwołania stopnia

[43] Dz.U. z 2020 r. poz. 1369, art. 7 ust. 8 pkt. 3, art. 11 ust. 1 pkt 4 i 5, art. 13 ust. 1, art. 18 ust. 1 pkt 2, 4, 5, art. 22 ust. 1, pkt. 2 i 3, art. 26 ust. 1, ust. 3 pkt 8, 10, 13 i 14 lit. g, pkt. 16, ust. 4, 8, 10; art. 27 ust. 3, art. 28 ust. 2, art. 34 ust. 1, 2 art. 35 ust. 1-4, art. 48 pkt. 1, art. 49 ust. 3.

[44] Przepisy prawa określają cztery stopnie alarmowe CRP nazwane: pierwszy stopień alarmowy CRP (stopień ALFA-CRP), drugi stopień alarmowy CRP (stopień BRAVO-CRP), trzeci stopień alarmowy CRP (stopień CHARLIE-CRP), czwarty stopień alarmowy CRP (stopień DELTA-CRP). Ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* (Dz.U. z 2021 r. poz. 2234), art. 15 ust. 2.

alarmowego oraz zakresu i form współdziałania służb i organów, których przedstawiciele wchodzą w jego skład[45].

Na podstawie przepisów ustawy o działaniach antyterrorystycznych, PRM wydał rozporządzenie w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP. Zgodnie z przepisami przedmiotowego aktu prawnego, po odebraniu zarządzenia PRM o wprowadzeniu stopnia alarmowego CRP, SZ RP powinny poinformować RCB o otrzymaniu zarządzenia. Następnie, powinny przekazać raport o stanie realizacji przedsięwzięć wynikających z wprowadzonego stopnia alarmowego CRP. Czas na przekazanie raportu to maksymalnie 12 godzin od otrzymania informacji o wprowadzeniu stopnia. Ponadto, poszczególne jednostki i komórki organizacyjne SZ RP[46] powinny posiadać plany i procedury realizacji przedsięwzięć w ramach określonych stopni alarmowych CRP, w tym moduły zadaniowe. Powinny one ujmować w szczególności wykaz zadań do wykonania w poszczególnych stopniach[47]. Załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, zawiera również zbiór zadań dla SZ RP, które mają być realizowane po wprowadzeniu określonego stopnia. Należy zauważyć, że wprowadzenie wyższego stopnia obliguje do wykonania zadań określonych również w niższym stopniu lub stopniach. Przykładowo, jeśli wprowadzony jest czwarty stopień CRP, to wykonywane są również przedsięwzięcia z pierwszego, drugiego i trzeciego stopnia. W przypadku wprowadzenia pierwszego stopnia alarmowego, SZ RP mają obowiązek wzmóc monitorowanie stanu bezpieczeństwa systemów teleinformatycznych. Jeśli wydane są zalecenia przez Szefa ABW lub Dowódcę Komponentu Wojsk Obrony Cyberprzestrzeni, to powinny być one realizowane przez SZ RP. Ponadto, wojsko powinno monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej oraz czy dostępne są usługi elektroniczne. Jeśli zaistnieje potrzeba, to należy dokonać zmian w dostępie do systemów teleinformatycznych. Dodatkowo, należy poinformować personel (w szczególności odpowiedzialny za bezpieczeństwo systemów) o potrzebie zwiększenia czujności w stosunku do stanów odbiegających od normy. Powinny również zostać sprawdzone kanały łączności z

[45] Dz.U. z 2021 r. poz. 2234, art. 15 ust. 2, art. 16 ust. 2, art. 17 ust. 1 i 3.

[46] W tym osoby odpowiedzialne za obiekty infrastruktury krytycznej.

[47] Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. *w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych* CRP (Dz.U. z 2016 r. poz. 1101), §3 - §5.

innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami uczestniczącymi w reagowaniu na incydenty bezpieczeństwa. Kolejnym zadaniem jest przegląd procedur oraz zadań związanych z wprowadzeniem stopi alarmowych CRP, a szczególnie zweryfikowanie posiadanych kopi zapasowych systemów związanych z infrastrukturą krytyczną oraz systemów kluczowych dla funkcjonowania organizacji, jak również weryfikacji czasu niezbędnego do przywrócenia prawidłowego funkcjonowania systemu. Dokonać sprawdzenia stanu bezpieczeństwa systemów. Ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne mając na uwadze bieżące informacje oraz prognozy wydarzeń. Ostatnie zadanie wskazane w załączniku, polega na bieżącym informowaniu o efektach przeprowadzanych działań zespołu reagowania na incydenty bezpieczeństwa informatycznego oraz centra zarządzania kryzysowego jak również ministra właściwego do spraw informatyzacji[48].

W przypadku wprowadzenia drugiego stopnia alarmowego CRP (BRAVO-CRP), oprócz zadań zrealizowanych w ALFA-CRP, należy również zapewnić dostęp w trybie alarmowym osób, które są odpowiedzialne za bezpieczeństwo systemów teleinformatycznych. Dodatkowo, całodobowe dyżury powinni pełnić administratorzy systemów kluczowych dla funkcjonowania jednostek i komórek organizacyjnych SZ RP oraz osób posiadających uprawnienia do podejmowania decyzji dotyczących bezpieczeństwa systemów. Trzeci stopień alarmowy CRP (stopień CHARLIE-CRP), wymaga kontynuowania i sprawdzenia realizacji zadań wymienionych w poprzednich stopniach. Ponadto należy wykonać przegląd dostępnych zapasowych zasobów pod kątem możliwości ich użycia w sytuacji wystąpienia ataku terrorystycznego. Dodatkowo, należy przygotować się do uruchomienia planów, zapewniających ciągłość funkcjonowania po zamachu. Czynności powyższe powinny obejmować przegląd i ewentualne sprawdzenie planów awaryjnych oraz systemów jak również przygotować się do zredukowania operacji na serwerach, w celu umożliwienia ich szybkiego i bezawaryjnego zamknięcia. Wprowadzenie czwartego stopnia alarmowego CRP (DELTA-CRP), wymaga dodatkowo uruchomienia planów awaryjnych lub planów zapewniających ciągłość działania SZ RP w przypadku awarii lub utraty ciągłości działania oraz odpowiednio do sytuacji przystąpienia do wykonania procedur przywracania ciągłości działania systemów teleinformatycznych[49].

[48] Dz.U. z 2016 r. poz. 1101, załącznik, rozdz. II pkt 1.
[49] Dz.U. z 2016 r. poz. 1101, załącznik, rozdz. II pkt 2-4.

PODSUMOWANIE

Wnioski z prowadzonych badań wskazują, że SZ RP realizują zadania antyterrorystyczne w cyberprzestrzeni w ramach krajowego systemu cyberbezpieczeństwa. Przedsięwzięcia antyterrorystyczne polegające m.in. na: wykryciu incydentu, sklasyfikowaniu go jako terrorystyczny, rozwijaniu narzędzi zapewniających cyberbezpieczeństwo, pozyskiwaniu wiedzy i doskonaleniu umiejętności umożliwiających przeciwstawienie się przyszłym atakom cyber, koordynowaniu działań w przypadku zamachu, postępu w rozwoju systemów wymiany informacji o zagrożeniach, wykrywaniu i eliminowaniu podatności na ataki, czy współdziałaniu z innymi elementami odpowiedzialnymi za cyberbezpieczeństwo - są tożsame z przedsięwzięciami realizowanymi w ramach ogólnie pojętego bezpieczeństwa cyberprzestrzeni. W związku z powyższym realizując zadania dotyczące cyberbezpieczeństwa realizowane są również zadania antyterrorystyczne w cyberprzestrzeni.

Dodatkowo, badania umożliwiły wykrycie problemów utrudniających przeciwdziałanie zagrożeniom terrorystycznym. Do dwóch zasadniczych należy zaliczyć: kategoryzowanie incydentu jako terrorystyczny oraz brak przepisów umożliwiających działania ofensywne. Odnośnie pierwszego, to pomimo klasyfikowania incydentów zgodnie z przyjętą nomenklaturą (np. krytyczny, poważny itd.), niezwykle trudno jest ocenić czy ma on charakter terrorystyczny czy nie. Powodem może być niewystarczająca ilość informacji na moment ataku, jak również brak szczegółowej wykładni odnośnie oceny incydentu (oprócz ogólnych przepisów KK). W kwestii drugiego, w aktach prawa polskiego, znajdują się przepisy dotyczące ochrony przed zagrożeniami terrorystycznymi, niestety brak jest zasad regulujących działania ofensywne. Tym samym, wpływa to negatywnie na możliwości przeprowadzenia przez siły zbrojne ataku w cyberprzestrzeni, w celu przeciwdziałania zagrożeniom terrorystycznym. Ewentualne działania ofensywne można uzasadniać prawem międzynarodowym tj. art. 51 Karty Narodów Zjednoczonych. Zgodnie z tym przepisem, każdy z członków Narodów Zjednoczonych ma prawo do samoobrony[50] w przypadku napaści zbrojnej. Z kolei za napaść zbrojną można uznać atak terrorystyczny, choć nie zostało to wprost wyartykułowane w prawie międzynarodowym[51].

[50] Karta Narodów Zjednoczonych (Dz.U. z 1947 r. nr 23 poz. 90), art. 51.

[51] W rezolucji Rady Bezpieczeństwa ONZ nr 1386 z 12 września 2001 r., postawienie obok siebie kwestii dotyczącej potępienia ataków terrorystycznych oraz przypomnienia o prawie do samoobrony świadczy o tym, że organ ten przyjął, że zamachy terrorystyczne należy również traktować jako napaść zbrojną. Na tej podstawie Stany Zjednoczone Ameryki ich sojusznicy zaatakowali talibów w Afganistanie w odpowiedzi na atak z 11 września 2001 r. Należy jednak dodać, że w rezolucjach RB ONZ nie uznano wprost zamachu terrorystycznego za napaść zbrojną. Zgodnie z oceną Międzynarodowego Trybunału Sprawiedliwości w kwestii Nikaragui, czy mamy do czynienia z

Zgodnie z polskim prawem, w związku z zagrożeniami w cyberprzestrzeni, można wprowadzić stan wojenny, co może być niezbędne w przypadku terroryzmu państwowego.

Usunięcie wykazanych słabości umożliwi lepsze przeciwdziałanie zagrożeniom terrorystycznym w cyberprzestrzeni.

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENNICTWO
LITERATURE

Godwin III J.B., Kulpin A., Rauscher K.F., Yaschenko V., *Critical Terminology Foundations 2*, The EastWest Institute New York - Information Security Institute Moscow State University 2014.

Kleczkowska A., *Reakcja państwa na napaść zbrojną ze strony aktora niepaństwowego – uwagi na przykładzie doktryny Unwilling or Unable*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2015, vol. XIII, s. 77-98.

Pestkowski A., C*yberbezpieczeństwo infrastruktury krytycznej nadzorowanej przez administrację samorządową* (rozprawa doktorska), Akademia Sztuki Wojennej, Warszawa 2020.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego,* „Zeszyty naukowe Akademii Marynarki Wojennej rok XLVI Nr 1 (160)", Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2005, s. 173-187.

ŹRÓDŁA
SOURCES

Karta Narodów Zjednoczonych (Dz.U. z 1947 r. nr 23 poz. 90).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. *w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)* (Dz.U. UE L 151/15 z 17.04.2019)

Rozporządzenie wykonawcze komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. *ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ* (Dz.Urz. UE L 26/48 z 31.01.2018), art. 4 ust. 1.

napaścią zbrojną świadczy skala i efekt danej operacji. A. Kleczkowska, *Reakcja państwa na napaść zbrojną ze strony aktora niepaństwowego – uwagi na przykładzie doktryny Unwilling or Unable,* „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2015, vol. XIII, s. 90-91.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz.Urz. UE L 194/1 z 19.07.2016 r.).

Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz.U. z 1997 r. Nr 88 poz. 553).

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. z 2017 r. poz. 1932).

Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*, Dz.U. z 2021 r. poz. 2070, art. 3 pkt 3.

Ustawa z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. z 2006 r. nr 104 poz. 709).

Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 2020 r. poz. 1369).

Ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* (Dz.U. z 2021 r. poz. 2234).

Rozporządzeni 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 Prezesa Rady Ministrów z dnia 25 lipca 2016 r. *w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* (Dz.U. z 2016 r. poz. 1101).

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* (M.P. z 2019 r. poz. 1037).

Decyzja Nr 74/Mon Ministra Obrony Narodowej z dnia 27 marca 2013 r. *w sprawie eksploatacji niejawnego systemu teleinformatycznego PL_NS NOAN* (Dz.Urz. MON z 2013 r. poz. 82).

Allied Joint Doctrine for Cyberspace Operations AJP-3.20, NATO Standardization Office, Bruksela 2020 r.