Patryk Jankowski

Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej

Celem publikacji jest wskazanie zagrożeń, jakie niesie zjawisko cyberterroryzmu wobec administracji publicznej, a także zwrócenie uwagi na wieloaspektowość tego zagadnienia. W pracy zostało wyjaśnione pojęcie cyberterroryzmu i problemy w jego zdefiniowaniu. Publikacja ma na celu wskazanie potrzeb, a także możliwych kierunków zmian, mających na celu rozwój i poprawę skuteczności działania organów administracji rządowej. Artykuł przedstawia problem regulacji prawnych w zakresie zwalczania cyberterroryzmu, a także zwraca uwagę na ewolucje prawa. Pomimo stosowania wszelkich środków prewencyjnych, nie istnieje możliwość całkowitego wykluczenia skutecznych ataków. Spowodowane jest to ewolucją technologiczną, która nieustannie prowadzi do rozwoju nowych metod przeprowadzania cyberataków.

1. Uwagi wstępne

W XXI wieku nastąpił gwałtowny postęp technologiczny w obszarze technologii informacyjnych. Dzień bez Facebook'a, wyszukiwarki Google, czy dostępu do poczty elektronicznej wydaje się dziś bardzo trudny dla 'normalnego' człowieka[1]. Dynamizacja Internetu, a także całej sfery informatycznej, jest najszybciej rozwijającym się segmentem życia społecznego[2]. Na podstawie danych firmy We Are Social „od stycznia ubiegłego roku liczba internautów na świecie wzrosła o 10 %"[3]. Natomiast w sierpniu 2017 roku odnotowano, że już blisko 4 miliardy osób ma dostęp do Internetu. Nowoczesne technologie w coraz większy sposób inspirują ludzi. Niektórzy działają dzięki nim dla dobra jednostki, wielokrotnie ułatwiając i ratując życie ludzkie, natomiast inni wykorzystują najnowsze technologie do zabijania i destrukcji, w tym destrukcji instytucji państwowych[4].

„Jutro terrorysta może wyrządzić większe szkody posługując się klawiaturą komputera niż bombą[5]". Obserwując otaczający nas świat, nie sposób nie zgodzić się z tą tezą.

[1]B. Hołyst, K. Jałoszyński, A. Letkiewicz, *Wojna z terroryzmem w XXI wieku,* Szczytno 2009, s. 120.
[2]Ibidem, s. 109.
[3]www.publicrelations.pl. (dostęp: 31.12.2017).
[4]B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 7.
[5]Toffler A., Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s. 220.

Zjawisko cyberterroryzmu zapoczątkowało rozwój technologii teleinformatycznych i globalizacji systemów informacyjnych. 'Winy' za terroryzm z użyciem narzędzi informatycznych nie ponosi jednak rozwój techniki i technologii, tylko ci, w czyich rękach technika jest narzędziem osiągania bezprawnych celów[6]. Zapobieganie terroryzmowi to nie tylko wyzwanie dla wyspecjalizowanych służb. Internet zmienia gruntownie stosunki gospodarcze i społeczne. Występujące w związku z tym problemy administracyjnoprawne, stanowią wyzwanie dla administracji publicznej[7] w zakresie stanowienia, jak i stosowania prawa[8].

Celem artykułu jest określenie zjawiska cyberterroryzmu oraz wyjaśnienie szkodliwości tego zjawiska dla administracji publicznej. Postaram się ponadto wskazać na konieczne działania, które powinien podjąć w tym obszarze ustawodawca. Do opisania problematyki zjawiska cyberterroryzmu zastosowano metodę dogmatyczno – prawną, w ramach której przeprowadzono badanie obowiązujących aktów prawnych i wykorzystano dorobek przedstawicieli doktryny.

2. Problematyka zjawiska

Terroryzm i jego nowe formy od wielu lat są przedmiotem naukowych debat. Problematyczne są pojęcie, ale także rozpoznawanie, przeciwdziałanie, zwalczanie i likwidacja skutków tego zjawiska. Wraz z ewolucją informatyzacji jako szczególnej formy polityki publicznej, zmieniają się poglądy kształtujące w tym zakresie obowiązki władz publicznych. Dotyczą one przedmiotu regulacji, która pod wpływem ewolucji informatyzacji zmienia sposób regulacji prawnej[9]. „Przyjmując cyberterroryzm jako politycznie motywowany atak lub groźbę ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów, możemy wyróżnić dwa rodzaje akcji cyberterrorystycznych: po pierwsze są to destrukcyjne działania informacyjne w cyberprzestrzeni, po drugie ataki fizyczne na systemy teleinformatyczne"[10].

---

[6] R. Kośla, *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*, prezentacja multimedialna, http;/www.cert.pl/PDF /Kosla_p.pdf. s. 189.
[7] Zob. J. Sługocki, *Prawo administracyjne*, *Zagadnienia ustrojowe*, s.13.
[8] G. Szpor, *Problemy administracyjnoprawne związane z ekspansją Internetu*, [w:] *Internet prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W.R. Wiewiórkowski, Warszawa 2012, s. 71.
[9] Ibidem.
[10] P. Sienkiewicz, M. Marszałek, H Świeboda, *Metodologia badań bezpieczeństwa narodowego,* T. 1, wyd.

Utrzymanie bezpieczeństwa państwa na poziomie wielowymiarowym jest skomplikowanym procesem. W jaki sposób zabezpieczyć państwo i jego obywateli przed skutkami cyberterroryzmu, i jaką rolę powinno spełniać w tym zakresie prawo? Każdego dnia, miliardy informacji poddawane są szczegółowej analizie. Na ich podstawie służby odpowiedzialne za bezpieczeństwo państwa, dociekają źródeł i celów ataków terrorystycznych. Jak przewidzieć przestępstwo, które nie zostało jeszcze popełnione? Kiedy i gdzie zostanie przeprowadzony atak w cyberprzestrzeni i jakie przyniesie skutki dla rzeczywistości? O ile prawo karne zajmuje się skutkami i czynami już popełnionym, to prawo administracyjne jest skierowane w teraźniejszość i przyszłość, dlatego wydaje się skuteczniejszym narzędziem zapobiegania opisywanym zjawiskom.

Cyberterroryzm zagraża podstawowym filarom demokratycznego państwa prawnego i podstawowym prawom człowieka i obywatela chronionym przez Konstytucję[11]. Uderzając w infrastrukturę krytyczną państwa, zagraża procesom gospodarczym. Cyberatak - poprzez wzburzenie opinii publicznej - może wpłynąć na wyniki wyborów parlamentarnych, prezydenckich czy samorządowych.

Cyberterroryzm polega generalnie na zaatakowaniu systemów komputerowych za pomocą technologii informacyjnej. Zastosowanie tego rodzaju metod może spowodować blokadę systemów komputerowych i doprowadzić do utraty danych[12]. Narzędziem ataku są różnego rodzaju formy szkodliwego oprogramowania np. tzw. wirusy[13], bakterie, robaki i blokady serwerów[14], czy ataki konwencjonalne[15]. Powyższe działania negatywnie wpływają na bezpieczeństwo w sieci, w tym zwłaszcza bezpieczeństwo instytucji państwowych i finansowych, choć oczywiście terroryści mogą szkody w różnych dziedzinach życia obywateli poprzez zamachy na systemy kontroli lotów, systemy wodociągowe, systemy telekomunikacyjne, systemy energetyczne, system zaopatrzenia w wodę, transport, aż po elektrownie. To tylko niektóre płaszczyzny, które są obiektem zainteresowań terrorystów.

Akademii Obrony Narodowej, Warszawa 2010, s. 216.

[11] Por. I. Lipowicz, *Nowe wyzwania w zakresie ochrony danych osobowych* [w:] *Internet, Ochrona wolności, własności i bezpieczeństwa,* red. G. Szpor, Warszawa 2011, s. 4.

[12] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 23.

[13] Wirusy to programy działające na szkodę użytkowników systemów wbrew ich woli. Głównie służą do uszkadzania baz danych i systemów operacyjnych. Mogą wywołać różne efekty m.in. mogą paraliżować systemy zabezpieczające. Często są przenoszone wraz z pocztą elektroniczną. Zob. M. Adamczyk, *Terroryzm*, Warszawa, 2005, s. 33-35.

[14] Polegają na zmianie lub uszkodzeniu systemów operacyjnych. Prowadzi to do spowolnienia pracy serwera, a później do jego zawieszenia. Zob. M. Adamczyk, *op.cit., s*. 33-35.

[15] Polega on na fizycznym uszkodzeniu elementów systemu komputerowego, infrastruktury telekomunikacyjnej, komunikacyjnej, energetycznej, serwerów. Tego typu atak może prowadzić do nieodwracalnej utraty danych.

Jednak cyberterroryzm to nie tylko działania, które mają na celu doprowadzenie do utraty danych. Cyberterroryzm przejawia się również w prowadzeniu akcji propagandowych i informacyjnych, rekrutacji, radykalizacji wymiany i pozyskiwania informacji. Terroryści przy wykorzystaniu Internetu docierają do dużej rzeszy odbiorców[16]. Głównym ich celem jest zakłócenie porządku publicznego w postaci protestów i zaburzenie działania stron rządowych[17].

Wobec postępującej informatyzacji konieczne jest stworzenie skutecznych rozwiązań systemowych na płaszczyźnie organizacyjno-prawnej[18]. Zgadzam się z I. Lipowicz, że prawne formy działania administracji ewoluują wraz z zadaniami, dla których realizacji powstały[19]. Regulacje prawne dotyczące ochrony administracji publicznej przed zjawiskiem cyberterroryzmu są tworzone za wolno; regulacja dotycząca cyberterroryzmu dopiero się wyodrębnia. Prawo jest - jak to bywa - spóźnione w stosunku do rozwoju nowych form cyberterroryzmu.

3. Definicja cyberterroryzmu

W literaturze przedmiotu występują liczne definicje cyberterroryzmu. Eksperci zwracają jednocześnie uwagę na trudności w zdefiniowaniu tego pojęcia. Problem polega na tym, że jest to zjawisko różnorodne o dynamicznym charakterze. Ponadto występuje pod wieloma postaciami, które zmieniają się pod wpływem rozwoju cywilizacyjnego powodowanego postępem technologicznym[20]. Dylemat definicyjny wywołuje trudności w określeniu, które działania można scharakteryzować mianem cyberterroryzmu[21]. Często publicyści, a nawet eksperci różnych dziedzin, posługują się terminem cyberterroryzmu z powodu jego tzw. medialności, chociaż nie zawsze używają go na określenie zjawiska będącego wynikiem działalności grup terrorystycznych. Nieścisłe posługiwanie się pojęciem cyberterroryzmu może doprowadzić do osłabienia jego znaczenia, zobojętnienia opinii

[16] K. Bielski, *op.cit.,* s. 96.
[17] Ibidem, s. 101. Przykładem tego działania były protesty społeczne przeciwko ACTA w 2012 r.
[18] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski-zarys problemu*, „Bezpieczeństwo narodowe" 2012, nr 22, s. 136.
[19] I. Lipowicz, *Prawne formy działania administracji publicznej –między stabilizacją a potrzebą przełomu*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2016, nr 4, s. 41-55.
[20] A. Olak, A. Krauz, *Zjawisko terroryzmu we współczesnym świecie*, „Kultura bezpieczeństwa" nr 15, s. 189.
[21] A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 63. Autorzy podkreślają, że samo wysłanie poczty elektronicznej może zostać uznane za zagrożenie dla narodowego bądź międzynarodowego bezpieczeństwa.

publicznej na zagrożenie z nim związane. Przykładem niech będzie stwierdzenie, że za określonymi atakami kryją się państwa, które chciały osiągnąć dany cel polityczny lub gospodarczy. Tymczasem atak cyberterrorystyczny może być dziełem jednostki, która nie musi być umotywowana politycznie, a jedynie jej celem jest zademonstrowanie własnych umiejętności[22]. O nadużywaniu pojęcia cyberterroryzmu świadczą informacje podawane w środkach masowego przekazu, które nie znajdują potwierdzenia w otaczającym świecie[23]. T. Szubrycht podkreśla, że cyberterroryzm możemy podzielić na trzy grupy tj. „pojęcie przedstawiane w mediach, obowiązujące definicje w gronie specjalistów, a także definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyki"[24]. W niniejszym opracowaniu zamierzam stosować pojęcie cyberterroryzmu *sensu stricto*, przyjmowane za adekwatne do opisywanego zjawiska w naukach prawnych i w naukach o bezpieczeństwie.

Za twórcę pojęcia cyberterroryzmu uważa się Barry'ego Collina, który w latach 80-tych ubiegłego wieku wykorzystał je dla sformułowania połączenia cyberprzestrzeni i terroryzmu[25]. Autor definiuje cyberterroryzm jako świadome wykorzystanie systemu informacyjnego, sieci komputerowych bądź jej części składowych w zamiarze wsparcia lub usprawnienia akcji terrorystycznej[26].

Zajmująca się problemami bezpieczeństwa w cyberprzestrzeni D. Denning określa z kolei cyberterroryzm jako bezprawny atak lub groźbę ataku na komputery, sieci lub systemy informacyjne w celu zastraszenia lub wymuszenia na rządzie lub ludziach daleko idących politycznych i społecznych celów[27]. Ponadto, według D. Denning, za atak cyberterrorystyczny, może być uznany tylko taki atak, który powoduje bezpośrednie szkody wyrządzone człowiekowi jak również jego mieniu lub jest na tyle znaczący, że budzi strach[28]. W związku z powyższym akt nie wywołujący takich skutków nie jest aktem o charakterze cyberterrorystycznym.

[22]R. Cegiełka, *Zagrożenie terroryzmem. Poczucie bezpieczeństwa na początku XXI wieku,* Warszawa 2015 s. 28.
[23] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego, „*Zeszyty naukowe Akademii Marynarki Wojennej" 2005, nr 1, (160), s. 173.
[24]Ibidem, s. 175.
[25]D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 79.
[26]K.C. White, *Cyber – terrorism: Modem Mayem*, Carlisle 1998, s. 10.
[27]D. E. Denning, *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*,Washington, 23.5.2000 r., http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf, (dostęp: 27.11.2017).
[28] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie państwa*, Białystok 2015, s. 481.

Jedną z polskich definicji cyberterroryzmu przedstawia R. Kośla, który definiuje cyberterroryzm jako działania blokujące, zniekształcające lub niszczące w kontekście informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych, jak również obezwładniające przedmiotowe systemy. Zdaniem Autora termin ten zawiera także wykorzystywanie systemów teleinformatycznych do dezinformacji. R. Kośla zwraca uwagę, że celem ataku nie jest system, lecz przetwarzana informacja[29].

Według M. Gawryckiego cyberterroryzm to „wyrządzenie możliwie dużych strat przeciwnikowi, włącznie z ofiarami ludzkimi, np. włamanie do systemu kontroli lotów lotniska i doprowadzenia do zderzenia samolotów"[30]. H. Świeboda, P. Sienkiewicz, E. Lichocki definiują cyberterroryzm jako „politycznie motywowany atak lub groźbę ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów"[31].

W literaturze przedmiotu nie obowiązuje zatem jedna powszechnie akceptowana definicja cyberterroryzmu. Każda z definicji zwraca uwagę na inny aspekt omawianego zjawiska.

B. Colin podkreśla, że cyberterroryzm jest świadomym wykorzystaniem systemów informacyjnych. Z kolei R. Kośla zwraca uwagę na elementy niszczące w stosunku do przetwarzanej informacji i systemów teleinformatycznych. Natomiast D. Denning wskazuje na bezprawny charakter ataku lub groźbę takiego ataku w celu osiągnięcia korzyści społecznych i politycznych. Łącząc elementy doktrynalnych definicji można uznać, że cyberterroryzm jest szczególną kategorią zagrożeń o charakterze bezprawnym. Obszar jego działania obejmuje systemy teleinformatyczne, wykorzystując je by osiągnąć określony cel terrorystyczny[32].

Podzielam definicję D. Denning. Zawiera ona bowiem, w moim przekonaniu, najważniejsze elementy zjawiska cyberterroryzmu. Po pierwsze zaznacza, że jest to czyn bezprawny (bezprawny zamach). Po drugie, czyn ten powinien być dokonany w określonym

[29] R. Kośla, Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski. Wystąpienie na konferencji w Bemowie, 29.11.2002, cyt. za. W. Smolskim. *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, http://www.repozytorium.uni.wroc.pl/Content/66149/32_Wieslaw_Smolski.pdf, (dostęp: 27.11.2017).
[30] A. Bógdał-Brzezińska, M. Gawrycki, op.cit., s. 61. Por. M. Marszałek, M.J. Limanowski, *Zwalczanie terroryzmu*, Warszawa 2014, s. 283.
[31] P. Sienkiewicz, H. Świeboda, E. Lichocki, *Analiza systemowa zjawiska cyberterroryzmu*, Akademia Obrony Narodowej, http://www1.aon.edu.pl, (dostęp: 12.10.2017).
[32] W. Smolski, *op.cit.,* s. 481.

celu. W tym przypadku w celu zastraszenia, wzbudzenia strachu lub wywarcia presji na przedstawicielach administracji państwowej i społeczeństwie.

Brak jest definicji legalnej pojęcia cyberterroryzmu także w polskim porządku prawnym[33]. Ustawa o działaniach antyterrorystycznych[34] to pierwszy tego typu akt prawny w polskim ustawodawstwie. Nie odnosi się ona jednak bezpośrednio do zwalczania zjawiska cyberterroryzmu i ochrony cyberprzestrzeni. Warto zastanowić się, czy wprowadzenie normatywnej definicji cyberterroryzmu umożliwi wzmocnienie ochrony przed i zwalczanie przestępstw. Trafny wydaje się pogląd, że największe znaczenie dla wolności i bezpieczeństwa jednostek mają jedynie te definicje, które pochodzą od ustawodawcy, co wiąże się z tym, że są zabezpieczone przymusem państwowym[35]. Tymczasem definicje cyberterroryzmu ujęte są w niemających charakteru normatywnego Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011 – 2016 i Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[36]. Obecnie są to dwa podstawowe dokumenty, które są fundamentem realizacji procesu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[37]

Pierwsza z wymienionych uchwał określa cyberterroryzm jako „cyberprzestępstwo o charakterze terrorystycznym"[38]. Według Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[39] cyberterroryzm to „przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni". Również pojęcie cyberprzestrzeni nie posiada jednej, powszechnie uznanej definicji. Termin ten został zdefiniowany w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011 - 2016, według którego cyberprzestrzeń to „cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[40].

[33]A. Sucharzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 168.
[34]Ustawa z 10.6.2016 r. o działaniach antyterrorystycznych (Dz.U. z 2018 r., poz. 452).
[35] S. Wronkowska, *Podstawowe pojęcia prawa i prawodawstwa*, część I. Poznań 2002, s. 80-81. Warto wskazać, że podobne problemy dotyczą także innych krajów, m.in. w Stanach Zjednoczonych agencje rządowe w odmienny sposób postrzegają działalność terrorystyczną.
[36]Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, MAiC, ABW, Warszawa, 25.6.2013 r.,https://cyberpolicy.nask.pl/download/13/32/PolitykaOchronyCyberprzestrzeniRP.pdf, (dostęp: 25.11.2017).
[37]Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, RCB, Warszawa, 6.2010, http:// www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf, (dostęp: 20.11.2017).
[38]Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011 -2016, MSWiA, 6. 2010 r, s. 6.
[39]Polityka Ochrony cyberprzestrzeni RP z 25.6.2013r., op.cit.
[40]Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2010 -2016, op.cit., s. 6.

4. Ochrona prawna przez cyberterroryzmem

Jak słusznie zauważa A. Sucharzewska, w polskim porządku prawnym nie ma jednej powszechnej regulacji prawnej, która zawierałaby zbiór wszystkich przepisów odnoszących się do odpowiedzialności za nadużycia występujące w cyberprzestrzeni[41]. Obecnie podstawowym obszarem zwalczania terroryzmu w zakresie regulacji prawnych jest prawo karne[42]. Drugim jest prawo administracyjne. Jego zasięg obejmuje różnego rodzaju akty normatywne, w których zostały zawarte mechanizmy prawne mające na celu zapobieganie cyberterroryzmowi, a także zwalczanie jego skutków[43]. Zauważalne jest ponadto przenoszenie norm z zakresu zwalczania tego nowego rodzaju przestępczości z obszaru prawa karnego do prawa administracyjnego, a przepisy dotyczące cyberterroryzmu zawarte są w wielu aktach prawnych[44].

Aby przeciwstawić się zjawisku, jakim jest cyberterroryzm, państwo musi stosować i wdrażać kompletne regulacje prawne tzn. muszą one zawierać elementy ustrojowe, materialno-prawne i proceduralne. W jakim akcie prawnym powinny pojawić się regulacje dotyczące przeciwdziałania cyberterroryzmowi, skoro nie ma ich w nowo uchwalonej ustawie o działaniach antyterrorystycznych, jak również w ustawie o zarządzaniu kryzysowym?

Międzyrestorowa grupa przedstawicieli ministerstw Cyfryzacji, Obrony Narodowej, Spraw Wewnętrznych i Administracji, Agencji Bezpieczeństwa Wewnętrznego i Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego opracowała Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022[45]. Głównym celem strategii jest „zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych”[46]. Strategia jest kontynuacją przyjętej przez rząd w 2013 r. Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej i jest wynikiem implementacji Dyrektywy Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[47] tzw. Dyrektywy NIS.

[41] A. Sucharzewska, *op.cit.,* s. 206.
[42]Ustawa z 6.6. 1997 r. – Kodeks karny (Dz.U. z 2018 r., poz.1600).
[43]A. Sucharzewska, *op.cit.,* s. 206.
[44] Polska jako pełnoprawny członek Unii Europejskiej, korzysta z jej dorobku prawnego, uzupełniając krajowe ustawodawstwo - K. Bielski, *op.cit.,* s. 102.
[45]Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, s. 4-5.
[46]Ibidem*,* s. 8.
[47] Dz. U. UE 2016 L194.

W jej świetle, w celu skutecznej walki z cyberterroryzmem należy skoordynować działania przede wszystkim na polu prawnym, ale także organizacyjnym[48]. Rozwiązania prawne w zakresie walki z cyberterroryzmem powinny zostać uporządkowane i doprecyzowane w jednym akcie prawnym. Obecnie są rozproszone w kilku aktach prawnych. Powoduje to trudności w zakresie braku koordynacji działań w tym obszarze. Powyższy element z pewnością wymaga uporządkowania w polskim systemie antyterrorystycznym.

Ochrona cyberprzestrzeni jest jednym z fundamentalnych zadań administracji państwowej. Do skutecznej walki z cyberterroryzmem potrzebne są także wyspecjalizowane agencje, grupy, służby, programy, instytuty, które przy pomocy odpowiednich narzędzi będą monitorowały stan bezpieczeństwa państwa. W Polsce powołanych jest kilka instytucji[49] odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni, których kompetencje normują stosowne ustawy i akty wykonawcze[50]. Doskonałym przykładem takiego programu jest Naukowa Akademicka Sieć Komputerowa, która została utworzona 14.12.1993 r. w ramach instytutu badawczego[51]. W strukturze NASK funkcjonuje zespół CERT Polska. Fundamentalnym zadaniem zespołu jest reagowanie na zdarzenia mające na celu zakłócenie bezpieczeństwa w sieci Internet[52]. Kolejnym przykładem jest Rządowy Zespół Reagowania na Incydenty Komputerowe CERT GOV PL, który został powołany 1.2.2008 r. w ramach struktur Agencji Bezpieczeństwa Wewnętrznego. Do obszaru jego kompetencji należy: kreowanie polityki bezpieczeństwa w zakresie ochrony przed cyberzagrożeniami, koordynacja przepływu informacji między podmiotami w związku z tego typu zagrożeniami, pełnienie nadrzędnej roli w stosunku do wszystkich krajowych instytucji, organizacji oraz podmiotów resortowych w zakresie ochrony cyberprzestrzeni, reagowanie na incydentalne zakłócenia bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem infrastruktury krytycznej oraz współpraca międzynarodowa w zakresie ochrony cyberprzestrzeni[53]. W resorcie obrony narodowej funkcjonuje zespół reagowania na incydenty komputerowe MIL-CERT.PL.

[48]K. Bielski, *op. cit.,* s. 106.
[49]Między innymi Ministerstwo Cyfryzacji, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej, Agencja Bezpieczeństwa Wewnętrznego, Policja.
[50]Ustawa z 4.9.1997 r. o działach administracji rządowej (tekst jedn. Dz.U. z 2018 r., poz. 762).
[51]Instytut badawczy NASK został utworzony na podstawie zarządzenia Nr 5/93 Przewodniczącego Komitetu Badań Naukowych.
[52]P. Trąbiński, *Podział kompetencji w zapewnianiu cyberbezpieczeństwa* [w:] *Internet Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 79.
[53]E. Lichocki, *op.cit.,* s. 589–590.

Odpowiedzialny jest on za kompleksową obsługę zdarzeń pojawiających się w resortowych sieciach informatycznych[54].

5. Infrastruktura krytyczna – definicja legalna, zagrożenia

Cyberterroryzm jest szczególnym zagrożeniem dla elementów infrastruktury krytycznej państwa, a walką z terroryzmem jest ściśle związana z ustawowym obowiązkiem ochrony infrastruktury krytycznej[55]. Infrastruktura krytyczna jest pojęciem prawnym[56]. Przez ten termin należy rozumieć systemy, których zniszczenie lub uszkodzenie może spowodować osłabienie zdolności obronnej, w tym także bezpieczeństwa ekonomicznego państwa, jak również przerwanie ciągłości funkcjonowania władzy oraz służb publicznych[57]. Na mocy ustawy o zarządzaniu kryzysowym[58] pojęcie infrastruktury krytycznej zostało zdefiniowane jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa, a także jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, jak również instytucji i przedsiębiorców. Analiza definicji legalnej infrastruktury krytycznej prowadzi do wniosku, że pod pojęciem tym znajduje się ochrona ważnych zasobów z perspektywy interesu publicznego[59], które są skłonne na różnego rodzaju zagrożenia, w tym terrorystyczne[60].

W ustawie scharakteryzowano reguły zarządzania kryzysowego, interpretowanego jako działalność organów administracji publicznej, której podstawowym zadaniem jest zapobieganie sytuacjom kryzysowym, reagowanie w przypadku wystąpienia okoliczności kryzysowych, a także eliminowanie zaistniałych skutków[61]. Ustawa reguluje wszelkie działania

[54]Decyzja Nr 243/MON z 18.6.2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. MON poz. 203).
[55]M. Kopeć, *Administracyjnoprawne problemy zarządzania kryzysowego, ze szczególnym uwzględnieniem efektywności regulacji prawnej*, Warszawa 2012, s. 329.
[56] T. Długosz, *Ochrona infrastruktury krytycznej w sektorach energetyki sieciowej*, Warszawa 2015, s. 1.
[57]Por. J. Kisielnicki, *Cyberterroryzm jako element zagrożenia współczesnej cywilizacji*, [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009, s. 21.
[58]Ustawa z 26.4.2007 r. o zarządzaniu kryzysowym (Dz.U. z 2018 r., poz. 1401 ze zm.), dalej jako ,,ustawa o zarządzaniu kryzysowym".
[59] Wyróżniamy różne koncepcje interesu publicznego – por. A. Żurawik, *Interes Publiczny* s. 138 i n.. Pojęcie to możemy postrzegać jako san rzeczy, który ma przynieść korzyść np. państwu, społeczeństwu – zob. J. Zimmermann, *Prawo administracyjne*, s. 26.
[60] T. Długosz, *op.cit.,* s. 14.
[61]A. Podraza, P. Potakowski, K. Wiak, *op. cit.,* s. 147 -148.

mające na celu zapewnienie ochrony infrastruktury krytycznej, poprzez podjęcie czynności, które zagwarantują funkcjonalność, ciągłość i integralność infrastruktury krytycznej. Celem tych zadań jest zapobieganie zagrożeniom, słabym punktom, neutralizacja skutków, a także szybkie odbudowanie infrastruktury z powodu awarii lub innych zjawisk zaburzających jej właściwe funkcjonowanie[62]. Ustawodawca wskazuje, że funkcja normatywna infrastruktury krytycznej ma za zadanie zapewnić zbiorowe potrzeby państwa i jego obywateli. Przejawiają się one w sprawnym funkcjonowaniu administracji publicznej, instytucji i przedsiębiorstw. Zgadzając się z T. Długoszem „wartości te można łączyć z porządkiem publicznym, ale również z odpowiedzialnością prawną struktur państwa za zbiorowe bezpieczeństwo, za bezpieczeństwo powszechne[63].

6. Administracja publiczna wobec ataków cybernetycznych

Walka z cyberterroryzmem występuje w obszarze instytucji państwowych administracji publicznej. Jednym z ich zadań jest opracowywanie struktur odpowiedzialnych za zwalczanie zagrożeń cybernetycznych w Internecie. Jak wynika z ustawy o zarządzaniu kryzysowym ochrona infrastruktury krytycznej jest przedmiotem działań na wszystkich szczeblach administracji publicznej[64]. To na ministrach, kierownikach urzędów centralnych administracji rządowej, spoczywa obowiązek opracowywania planów zarządzania kryzysowego[65]. Natomiast wojewoda w ramach swojego urzędu jest zobowiązany do wykonania zadań z zakresu ochrony infrastruktury krytycznej jako zadanie w kwestii zarządzania kryzysowego[66]. Tymczasem realizacja zadań z zakresu ochrony infrastruktury krytycznej jako zadanie w sprawie zarządzania kryzysowego należy do starostów[67], wójtów, burmistrzów i prezydentów miast[68].

Istotnym problemem dotyczącym zapobiegania cyberterroryzmu jest zabezpieczenie systemów teleinformatycznych. Przepisy prawa obciążają obowiązkami podmioty odpowiedzialne za prawidłowe zabezpieczenie i ochronę systemów teleinformatycznych,

[62] *Ibidem*, s. 148.
[63] T. Długosz, *op.cit.,* s. 48.
[64] Artykuły 12-19 ustawy o zarządzaniu kryzysowym.
[65] Artykuł 12 ust. 2 pkt. 4. ustawy o zarządzaniu kryzysowym.
[66] Artykuł 14 ust. 2 pkt. 7. ustawy o zarządzaniu kryzysowym.
[67] Artykuł 17 ust. 2 pkt. 6. Ustawy o zarządzaniu kryzysowym.
[68] Artykuł19 ust. 2. Pkt. 6. Ustawy o zarządzaniu kryzysowym.

w których przetwarzane są tego rodzaju informacje[69]. Systemy teleinformatyczne instytucji państwowych zostały zaatakowane w Polsce w 2012 r.[70]. Ataki polegały na zablokowaniu stron internetowych instytucji administracji publicznej[71]. Powyższa sytuacja pokazała, że strony internetowe w domenie gov.pl nie były i nadal nie są w wystarczający sposób zabezpieczone i konieczne jest wprowadzenie odpowiednich rozwiązań prawnych i organizacyjnych. Z pewnością rozwiązania systemowe wymusiłyby na jednostkach administracji publicznej podjęcie stosownych kroków w zakresie cyberbezpieczeństwa[72].

W 2017 r. grupa posłów[73] wystąpiła z interpelacją w sprawie ataków cybernetycznych do ministrów[74], wnosząc o udzielenie odpowiedzi na poniższe pytania:

1. „Czy w okresie bieżącej kadencji Sejmu RP zostały przypuszczone ataki cybernetyczne na ministerstwo?"
2. „Jakie wnioski zostały wyciągnięte po tym ostatnim ataku cybernetycznym?"
3. „Czy ministerstwo ma odpowiednie zabezpieczenia przed takimi atakami?"
4. „Czy jakiekolwiek firmy zewnętrzne są odpowiedzialne za zabezpieczenie cybernetyczne ministerstwa?"[75]

Na pytanie dotyczące ataków cybernetycznych w bieżącej kadencji Sejmu RP, Ministerstwo Rozwoju i Finansów, Ministerstwo Środowiska, Ministerstwo Sprawiedliwości, Ministerstwo Obrony Narodowej, Ministerstwo Kultury i Dziedzictwa Narodowego, Ministerstwo Sportu i Turystyki, Ministerstwo Spraw Zagranicznych, zarejestrowały zdarzenia, które zostały zaklasyfikowane jako incydenty pochodzące z sieci Internet. Pozostałe, tj. Ministerstwo Energii, Ministerstwo Zdrowia, Ministerstwo Edukacji Narodowej, Ministerstwo Nauki i Szkolnictwa Wyższego, Ministerstwo Infrastruktury i Budownictwa, udzieliły odpowiedzi negatywnej[76]. Na pytanie o odpowiednie zabezpieczenie przed atakami cybernetycznymi, wyżej wymienione Ministerstwa odpowiedziały, że są właściwie

[69]A. Podraza, P. Potakowski, K. Wiak, *op. cit.,* s. 147.
[70] Ataki miały formę haktywizmu w ramach protestu przeciwko podpisaniu przez Polskę dokumentu ACTA. Protesty trwały od 21 do 25.1.2012 r.
[71] Zablokowano strony internetowe tj. sejm.gov.pl, prezydent.gov.pl, premier.gov.pl, abw.gov.pl, cert.gov.pl, ms.gov.pl, msz.gov.pl, mkidn.gov.pl, bor.gov.pl, cbs.policja.pl, policja.pl, partii politycznych.
[72] M. Grzelak, K. Liedel, op.cit.
[73] P. Skutecki, W. Bakun, S. Chruszcz, M. Masłowski, P. Szramka
[74]Interpelacja była skutkiem przeprowadzonych ataków cybernetycznych jednocześnie w ponad 150 krajach w maju 2017 r. Posłowie podkreślili, że według danych Europolu w wyżej wymienionych atakach ucierpiało ponad 200 tys. podmiotów, m.in. brytyjska służba zdrowia, rosyjskie banki, niemiecka kolej, koncern Renault. W Rosji zaatakowano także Ministerstwo Spraw Wewnętrznych, http://sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=39839182, (dostęp: 4.1.2018)
[75]Interpelacja nr 12977, http://sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=39839182, (dostęp: 4.1.2018).
[76]Ibidem.

przygotowane na ewentualne ataki. Instytucje cyklicznie wprowadzają programowe zabezpieczenia, a także wykorzystują narzędzia służące do obrony przed atakami. Systemy operacyjne, oprogramowania i urządzenia poddawane są okresowym analizom ich sprawności i wydajności działania. Ponadto, w niektórych ministerstwach prowadzone są akcje o charakterze edukacyjnym i informacyjnym dla pracowników[77]. 30.6.2017 r. Ministerstwo Cyfryzacji w odpowiedzi na interpelację poselską - zwróciło uwagę na rozróżnienie pojęcia incydent a próba ataku wyjaśniając, że „dopiero skuteczne wykorzystanie podatności" jest zakwalifikowane jako incydent[78]. W sytuacji, gdy wiadomość e-mail zostanie zakwalifikowana jako niebezpieczną to podlega ona zatrzymaniu i nie jest otwierana. Tego typu wiadomości nie są otwierane. Natomiast skuteczne ataki podlegają przeanalizowaniu. Ministerstwo zarejestrowało kilka prób zakłócenia bezpieczeństwa teleinformatycznego. Niemalże wszystkie ataki (w formie wiadomości e-mail) miały na celu wyłudzenie poświadczeń od użytkowników. Nie naruszyły one bezpieczeństwa systemów, jednocześnie o każdym z przypadków została poinformowana Agencja Bezpieczeństwa Wewnętrznego. W zakresie odpowiedniego zabezpieczenia przed atakami cybernetycznymi Ministerstwo Cyfryzacji stosuje zabezpieczenia systemów, sieci a także urządzeń klienckich. Ponadto, podejmowane są działania prewencyjne i edukacyjne w zakresie bezpieczeństwa. Ministrowie podkreślili, że nie ma skutecznej ochrony przed atakami. Dlatego ważna jest dywersyfikacja narzędzi służących ochronie. Mają one na celu zapewnienie ciągłości pracy systemów[79].

7. Wnioski

Cyberterroryzm stanowi istotne zagrożenie dla współczesnej administracji publicznej. Ingeruje w struktury bezpieczeństwa wewnętrznego państwa. Ponadto jest ogromnym niebezpieczeństwem dla społeczeństwa, co więcej może pojawić się w każdym momencie i w każdej dziedzinie naszego życia. Obecnie w czasach globalizacji, rozprzestrzeniania się społeczeństw, przepływu wszelkich dóbr, w tym także informacji, nie należy w żaden sposób lekceważyć tego zjawiska. Państwo powinno podejmować wszelkie działania profilaktyczne, które w pewnym stopniu chociażby zapobiegały negatywnym zjawiskom, jakimi są ataki

[77]Ibidem.
[78]Ibidem.
[79]Ibidem.

cyberterrorystyczne. W celu skutecznej walki z cyberterroryzmem należy wprowadzić odpowiednie normy prawne, które zapewnią skuteczne działanie organów administracji publicznej bez naruszenia podstawowych praw obywatelskich.

Zadaniem państwa jest wdrożenie odpowiednich rozwiązań systemowych w zakresie prewencji i rozbudowy systemu wczesnego ostrzegania przed atakami[80]. Pomiędzy instytucjami zarówno z sektora publicznego i prywatnego powinna nastąpić współpraca i koordynacja działań na rzecz bezpieczeństwa w cyberprzestrzeni[81].

Aktualnie regulacje prawne dotyczące walki z cyberterroryzmem rozproszone są w wielu aktach prawnych i tym samym są nieefektywne w zapobieganiu temu zjawisku. Ustosunkowując się do zadanego wyżej pytania o to w jakim akcie prawnym powinna zostać ujęta opisywana problematyka, uważam, że zasadnym byłoby uchwalenie nowego rozdziału w ustawie o zarządzaniu kryzysowym i obowiązkach administracji publicznej. W celu skuteczniejszej walki z tym zjawiskiem, należy przyśpieszyć uchwalanie regulacji prawnych, jednocześnie jednak trzeba mieć na uwadze, że skuteczna walka z cyberterroryzmem może spowodować ograniczenia w sferze wolności i praw człowieka[82].

[80] M. Grzelak, K. Liedel, *op.cit.,* s. 137.
[81] P.M. Balcerzak, P. Durbajło, *Organizacyjno-prawne aspekty implementacji dyrektywy Parlamentu Europejskiego i Rady z 6.7.2016 r.,* [w:] *Internet Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 47-48.
[82] B. Hołyst, K. Jałoszyński, A. Letkiewicz*, op.cit.,* s. 120.

Cyberterrorism as a contemporary threat to public administration

The aim of the publication is to indicate the threats that cyber-terrorism poses to public administration, as well as to draw attention to the multifaceted nature of this issue. The concept of cyberterrorism and problems in defining it have been explained in the work. The publication is aimed at identifying the needs as well as possible directions of changes aimed at developing and improving the effectiveness of government administration bodies. The work presents the problem of legal regulations in the field of combating cyber terrorism, and also draws attention to the evolution of law. It should be noted that despite all preventive measures, it is not possible to completely exclude effective attacks. This is due to the technological evolution that constantly leads to the development of new methods of cyberattacks.

Patryk Jankowski

Absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, doktorant w Katedrze Prawa Administracyjnego i Samorządu Terytorialnego na Wydziale Prawa i Administracji UKSW.