ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 889 ACTA POLITICA NR 34 2015

DOI: 10.18276/ap.2015.34-06

Krzysztof Bielski*

CYBERTERRORYZM – NOWE ZAGROŻENIE BEZPIECZEŃSTWA PAŃSTWA W XXI WIEKU

Wstęp

Postęp, jaki dokonał się w ostatnich trzydziestu latach, ułatwił życie człowieka na wielu płaszczyznach, wymiana informacji nigdy nie przebiegała tak szybko i sprawnie przy niskich kosztach eksploatacji mediów. Dzięki narzędziu, jakim jest internet oraz wszelkim urządzeniom, dzięki którym on funkcjonuje, proces globalizacji przybrał na sile, łącząc nawet najodleglejsze zakątki świata, do których można teraz dotrzeć jednym kliknięciem klawisza. Działalność państw coraz częściej przechodzi na pole elektroniczne, na którym pomija się użycie papierowej formy komunikacji. Działanie infrastruktury krytycznej jest regulowane przez komputery, które stanowią niezbędny element w jej codziennej eksploatacji. Można pokusić się o stwierdzenie, że internet jest praktycznie wszędzie, gdyż nie potrzeba używać kabla, aby korzystać z niego w danej chwili.

Jak każde narzędzie, internet może zostać użyty w dobrych celach, między innymi do nauki, komunikacji, wymiany danych czy zawierania nowych znajomości. Z drugiej jednak strony może służyć do prowadzenia działań natury przestępczej, a nawet terrorystycznej. Internet jest zdecentralizowany i nie charakteryzuje się żadną oficjalną strukturą, regulującą działalność użytkowników, stanowi bardzo dobrą bazę do prowadzenia różnego rodzaju agitacji, rekrutacji, komunikacji czy wymiany handlowej między rozmaitymi ugrupowaniami. Wraz

* mgr Krzysztof Bielski, doktorant w Instytucie Politologii i Europeistyki Uniwersytetu Szczecińskiego, e-mail: puchoo@wp.pl

z jego ciągłym rozwojem na sile przybierają nowe zjawiska, które do niedawna omawiane były jedynie w kręgach naukowców, a nawet w literaturze science-fiction, jednak postęp, jaki dokonał się w XX i XXI wieku sprawił, że stały się one faktem. Jednym z takich zjawisk jest cyberterroryzm – zjawisko młode i ciągle przybierające nowe formy. Często jego definicje są znacząco różne, nawet w obrębie jednego państwa, jak w przypadku Stanów Zjednoczonych, gdzie różne agencje inaczej podchodzą do działalności terrorystycznej w ogóle. Każde państwo ma dodatkowo odmienne regulacje dotyczące działalności przestępczej w sieci oraz różne określenia prawne charakteryzujące czyny zabronione. Brakuje wspólnej międzynarodowej regulacji, która harmonizowałaby działania poszczególnych państw w zakresie walki z cyberterroryzmem, jednak na terenie Unii Europejskiej podjęto kroki w celu ujednolicenia prawodawstwa, które ma stanowić podstawę do dalszych krajowych regulacji. Przejście na działalność elektroniczną państwa oraz obsługa najważniejszych jego elementów przez komputery, zwłaszcza infrastruktury krytycznej, nie uszło uwadze terrorystów, którzy – tak jak technologia – unowocześniają swoje techniki działania, w tym wypadku wykorzystując internet do prowadzenia działalności terrorystycznej i destabilizacji działania różnego rodzaju podmiotów.

W niniejszym artykule podjęto próbę definicji zjawiska cyberterroryzmu, oceny jego znaczenia dla bezpieczeństwa państwa oraz zagrożenia, jakie ze sobą niesie. Dodatkowo podjęto próbę oceny przygotowania państwa na wypadek wystąpienia tego zjawiska oraz możliwości skutecznego osądzenia sprawców ataku cyberterrorystycznego. Zasadnicze pytania, na które autor poszukiwał odpowiedzi to przede wszystkim: czy państwa, w tym Polska, są świadome zagrożeń cyberterrorystycznych? Czy są one odpowiednio przygotowane, zarówno na gruncie prawnym, jak i instytucjonalnym? Czy cyberterroryzm zastąpi tradycyjne działania ugrupowań terrorystycznych, czy też będzie ich uzupełnieniem? Jakie działania należy podjąć w celu lepszej walki z cyberterroryzmem?

Niniejszy artykuł został w głównej mierze oparty na krajowych publikacjach naukowych uzupełnionych przez publikacje anglojęzyczne, zwłaszcza naukowców amerykańskich, którzy ze zjawiskiem cyberterroryzmu mieli styczność w swojej pracy. Na uwagę zasługują takie pozycje, jak *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* Aleksandry Suchorzewskiej, w której poddano analizie polski dorobek prawny w zakresie walki z cyberterroryzmem oraz podjęto próbę jego oceny. Pozycja *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie* autorstwa Agnieszki Bógdał-Brzezińskiej i Marcina Floriana Gawryckiego w bardzo

przystępny sposób ukazuje typologię i charakterystykę ataków cyberterrorystycznych. *Cyberterroryzm. Nowe wyzwania XXI wieku* jest cenną pozycją, zawierającą zbiór artykułów opisujących różne aspekty cyberterroryzmu, począwszy od rozważań teoretycznych, a skończywszy na konkretnych praktycznych przykładach ataków. Bardzo cenną pracą jest *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, w której zawarte są artykuły autorstwa zarówno prawników, jak i politologów, co pozwala na zapoznanie się ze zjawiskiem cyberterroryzmu z punktu widzenia dwóch różnych dziedzin naukowych. Wykorzystano również rządowe dokumenty, które w bezpośredni sposób odwoływały się do bezpieczeństwa w sieci oraz działań mających na celu walkę z cyberterroryzmem. Stanowią one podstawę do oceny przygotowania państwa oraz jego świadomości wobec nowych zagrożeń, jakie niesie za sobą rozwój internetu oraz technologii teleinformacyjnej. Przytoczone definicje amerykańskich specjalistów, zwłaszcza Dorothy Denning, posłużyły do dalszego rozważania na temat natury cyberterroryzmu oraz ustalenia, kiedy należy uznać dane zjawisko za takowy czyn.

Definicja terroryzmu

Definicja terroryzmu jest niejednoznaczna i niejednorodna, istnieje wiele opinii oraz czynników charakteryzujących to zjawisko. Społeczności międzynarodowej nie udało się niestety wypracować jego wspólnej definicji. Mianem terroryzmu określa się różne postawy czy zachowania, począwszy od działań o charakterze rewolucyjnym, a skończywszy na czynach kryminalnych. Dużą rolę w kreowaniu tego pojęcia odgrywają mass media, które swoją działalnością, często szkodliwą, nadużywają tego terminu w celu zdyskredytowania danej osoby czy organizacji. Często wieloletnie ugrupowania terrorystyczne przekształcają swoją działalność ze zbrojnej na bardziej pokojową, jednak tę zmianę trudno pokazać, jeżeli ich obraz był przez lata przedstawiany w negatywnym świetle. Trudności ze zdefiniowaniem tego pojęcia występują również ze względu na osobiste aspiracje czy oczekiwania poszczególnych grup naukowców, instytucji czy ośrodków analitycznych. Każda z nich poszukuje innych aspektów czy czynników, które w danym czasie ją interesują w prowadzonych badaniach. Różnorodność ataków terrorystycznych również nie sprzyja wypracowaniu wspólnego stanowiska, o czym świadczą rozbieżności dotyczące opracowaniu uniwersalnej definicji wewnątrz Organizacji Narodów Zjednoczonych, a nawet wewnątrz jednego państwa, jak np. USA, gdzie nie ma wspólnej na poziomie

federalnym definicji, za to wypracowały je poszczególne agencje bezpieczeństwa[1]. Definicja cyberterroryzmu nastręcza dodatkowych trudności ze względu na krótki okres występowania tego zjawiska.

Wspólnym elementem terroryzmu i cyberterroryzmu pozostaje użycie przemocy (lub groźba jej użycia) – najczęściej skierowanej przeciw ludności cywilnej – przez różne grupy ekstremistyczne, zbrojne, religijne czy polityczne, do osiągnięcia własnych celów. Terrorystów możemy uszeregować ze względu na rodzaje ich motywacji. Wymienić tu można terrorystów tak zwanej „jednej sprawy", którą starają się zakończyć przez wykorzystanie przemocy. Do tej grupy można zaliczyć osoby walczące o prawa zwierząt czy nawet związane z ruchami antyaborcyjnymi. Drugą grupę stanowią terroryści ideologiczni, promujący swoje poglądy polityczne także poprzez użycie przemocy. Trzecia grupa złożona jest z terrorystów nacjonalistycznych, którzy walczą o niepodległość i prawo do samostanowienia na obszarze przez siebie zamieszkiwanym. Ostatnia grupa składa się z terrorystów religijnych, którzy według własnego uznania walczą w imię boga.

Przez lata grupy terrorystyczne powstawały z większym lub mniejszym nasileniem, z czego wiele zawiązanych w XX wieku przetrwało do dzisiaj. Działalność grup terrorystycznych i metody prowadzonej przez nie walki cały czas ewoluują – postęp technologiczny, który spowodował skomunikowanie całego świata poprzez internet nie uszedł uwadze terrorystów, którzy zaczęli go wykorzystywać do własnych celów.

Internet wykorzystywany jest głównie do rekrutacji, radykalizacji, propagandy czy zbiórki funduszy na działalność przestępczą tychże grup. Dodatkowo jest to bardzo dobry i efektywny środek do wydawania poleceń członkom organizacji. Terroryści umiejętnie wykorzystują sieć do dotarcia do masowych odbiorców. W przeciwieństwie do tradycyjnych mediów, takich jak telewizja, radio i prasa, internet pozwala na bardzo dużą swobodę wyrażania myśli i opinii, często niepopartych żadnymi dowodami czy źródłami.

Nieodłącznym elementem działalności grupy terrorystycznej są rekrutacja i radykalizacja, które odbywają się wśród użytkowników różnego rodzaju forów czy czatów, które nie są poddane ścisłej regulacji i cenzurze, jak w przypadku tradycyjnych środków komunikacji. Proces rekrutacji przebiega początkowo jak zwykła rozmowa, jednak już na tym etapie grupa sonduje, czy potencjalna osoba może stać się członkiem grupy czy też nie, bazując na jej wypowiedziach i zachowaniach w cyberprzestrzeni.

---

[1] S. Wojciechowski, *Terroryzm. Analiza pojęcia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1, s. 54–56.

Wraz z nadejściem XXI wieku uległa zmianie struktura organizacji terrorystycznych: wcześniej większość z nich charakteryzowała się tradycyjną, wojskową strukturą z naczelnym dowódcą i ścisłą kontrolą działań. Wraz z rozwojem internetu organizacje uległy rozbiciu na małe, połączone ze sobą grupy, które kontaktowały się jedynie w sieci wymyślnymi szyframi i kodami, często znajdując się na różnych kontynentach. Pozyskiwanie funduszy, wraz z rozwojem internetowej bankowości, również stało się o wiele łatwiejsze – pod przykrywką działalności charytatywnej grupy terrorystyczne mogą w łatwy i wygodny sposób zdobyć pieniądze niezbędne do prowadzenia walki[2].

Połączenie działalności terrorystycznej z wykorzystaniem nietradycyjnych środków komunikacji, w tym przede wszystkim internetu, doprowadziło do powstania nowych zjawisk, z którymi należy podjąć skuteczną walkę. Wśród nich znajduje się, coraz większe zagrożenie bezpieczeństwa państwa, cyberterroryzm, z którym należy walczyć zarówno na płaszczyźnie formalno-prawnej, jak i militarnej.

Definicja cyberterroryzmu

Cyberterroryzm jako zjawisko i metoda walki jest stosunkowo młody, jego obszarem zainteresowania jest właściwie każdy obiekt funkcjonujący w cyberprzestrzeni. Po raz pierwszy obydwa pojęcia pojawiły się latach osiemdziesiątych ubiegłego wieku. Autorem pojęcia cyberterroryzmu był Barry Collin, który określił je jako przejście terroryzmu ze świata realnego do wirtualnego[3], natomiast pojęcia cyberprzestrzeni użył po raz pierwszy William Gibson w powieści science-fiction zatytułowanej „*Neuromancer*"[4]. Cyberprzestrzeń została ukształtowana przez trzy procesy[5]:

---

[2] J. Charvat, *Cyber Terrorism: A new dimension in battlespace*, w: *The virtual battlefield: perspectives on Cyber Warfare*, ed. Ch. Czosseck, K. Geers, Amsterdam 2009 s. 79–83, https://ccdcoe.org/sites/default/files/multimedia/pdf/05_CHARVAT_Cyber%20Terrorism.pdf (15.07.2015).

[3] W.L. Tafoya, *Cyber Terror*, „FBI Law Enforcement Bulletin" 2011, vol. 80, no. 11, s. 2, https://leb.fbi.gov/2011/november/leb-november-2011 (15.07.2015).

[4] Cyberprzestrzeń William Gibson opisał w taki oto sposób: „To jest cyberprzestrzeń. Konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych... Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność..." W. Gibson, *Neuromancer*, Warszawa 1999.

[5] P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, t. 13, z. 2, s. 585, http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf (15.07.2015).

– integracji form przekazu i prezentacji informacji, który przyniósł multimedialność infosfery,
– konwergencji systemów informatycznych i telekomunikacyjnych,
– integracji technosfery, co doprowadziło do ukształtowania i ujednolicenia platformy teleinformatycznej.

Cała sfera teleinformatyczna jest obszarem współpracy zarówno pozytywnej, jak i negatywnej. Do pozytywnej można zaliczyć z pewnością edukację, komunikację społeczną czy gospodarczą, negatywną stanowią zaś[6]:

– cyberinwigilacja (kontrola społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach totalitarnych i autorytarnych),
– cyberprzestępczość (wykorzystanie cyberprzestrzeni do celów kryminalnych w szczególności w ramach przestępczości zorganizowanej),
– cyberterroryzm (wykorzystanie cyberprzestrzeni do działań terrorystycznych),
– cyberwojny (użycie cyberprzestrzeni jako wymiaru prowadzenia działań wojennych).

Na atak narażone są w szczególności elementy infrastruktury krytycznej państwa, organizacji czy wspólnoty – czyli takie, które służą prawidłowemu i sprawnemu funkcjonowaniu organów państwowych, służących przede wszystkim obywatelom. Do infrastruktury krytycznej możemy zaliczyć systemy zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, bankowych, finansowych, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, przechowywania i składowania substancji chemicznych i promieniotwórczych[7]. Wszystkie te elementy są szczególnie narażone na atak pochodzący z sieci, a zakłócenie ich działania może skutkować poważnym stratami materialnymi oraz osobowymi. Rodzaje cyberataków możemy podzielić na mające miejsce wyłącznie w cyberprzestrzeni oraz ataki fizyczne na systemy informacyjne. Metod ataków jest wiele, warto jednak przedstawić kilka z nich[8]:

1. Ataki wykorzystujące złośliwe oprogramowania (wirusy, bakterie, robaki), które samoistnie zarażają określone obszary komputera, powodując, że nie działa on w należyty sposób. Zarażone komputery, z powodu

---

[6] Tenże, *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, K. Kisielnicki, K. Rajchel, Warszawa 2009.

[7] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1–2, s. 28.

[8] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 138–154.

nieprawidłowego funkcjonowania, generują straty, które można szacować nawet w miliardach złotych.

2. Bomba logiczna – rodzaj wirusa komputerowego, który uruchamiany jest przez konkretne zdarzenie, wpisanie komendy, uruchomienie programu.
3. Koń trojański – program, który może wykonywać niepożądane działania bez wiedzy użytkownika, usuwać pliki, formatować dysk czy przesyłać dane do osób trzecich.
4. *Chipping* – umieszczanie w komputerach chipów, zawierających oprogramowanie dające dostęp do systemu, w którym zostały zainstalowane.
5. Tylne drzwi (*backdoor*) – tworzone w celu naprawiania późniejszych błędów w oprogramowaniu z możliwością wykorzystania ich do włamania się do komputerów użytkowników korzystających z takiego oprogramowania.
6. *Spoofing* – podszywanie się pod użytkowników danego systemu w celu jego destabilizacji.
7. *Hijacking* – polega na przechwyceniu transmisji odbywającej się między dwoma systemami i wykorzystaniu jej do własnych celów.
8. *Sniffing* – tropienie (podsłuchiwanie) ruchu w sieci. Programy wyłapują wiadomości i zapisują je na dysk w celu dalszego przetworzenia i wyłowienia haseł czy danych osobowych.
9. *Denial of service* (DoS), *distributed denial of service* (DDos) – są to działania polegające na zablokowaniu działania konkretnego serwisu sieciowego, zawieszeniu komputera przez przesyłanie potężnego pakietu danych z różnych źródeł.

Do przykładowego cyberataku doszło w Estonii w 2007 roku. W państwie tym prawo do dostępu do internetu jest gwarantowane konstytucyjnie, decyzje kolejnych rządów estońskich sprawiły, że wszelka działalność urzędów przeszła z papierowej na elektroniczną. Ataki były związane z decyzją o usunięciu pomnika żołnierzy radzieckich z centrum Tallina i wystąpiły one w tym samym czasie, co zamieszki na ulicach miasta. Sprawcy dokonali ataków typu DDoS, strumień danych zablokował dostęp do witryn internetowych. Hakerzy uderzyli przede wszystkim w strony rządu oraz partii politycznych, następnie zaatakowane zostały strony medialne, nieprzypadkowo, bo 9 maja, czyli w rocznicę zakończenia drugiej wojny światowej w Rosji. Hakerzy uderzyli również w system bankowy, uniemożliwiając przeprowadzenie jakichkolwiek transakcji. Ataki były skoordynowane, jednak przeprowadzone z różnych zakątków świata, z państw

o różnej polityce wobec cyberterroryzmu czy hackingu w ogóle. Rodzi to potrzebę koordynacji działań zarówno na poziomie międzynarodowym, jak i wewnątrz poszczególnych państw. Estonia jest członkiem zarówno Unii Europejskiej, jak i Paktu Północnoatlantyckiego (NATO), jednak obydwie organizacje nie były w stanie odeprzeć takiego ataku ani przewidzieć jego skali i skutków dla całego społeczeństwa[9].

Tak jak w przypadku klasycznego terroryzmu, nie istnieje wspólna definicja charakteryzująca działalność przestępczą w sieci. Często w literaturze możemy spotkać się z zamiennym stosowaniem takich pojęć jak cyberprzestępczość, cyberwojna czy haktywizm. Należy przy tym uważać, gdyż nie każda czynność może zostać zakwalifikowana jako czyn stricte terrorystyczny czy nawet przestępczy. Jak wskazuje Tomasz Szubrycht, postrzeganie cyberterroryzmu możemy podzielić na trzy grupy: pojęcia prezentowane w mediach, definicje obowiązujące w gronie specjalistów, definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyki[10].

Warto także przytoczyć kilka definicji, które opisują to zjawisko.

1. Dorothy Denning: Cyberterroryzm jest zbieżnością cyberprzestrzeni i terroryzmu. Odnosi się on zarówno do bezprawnych ataków oraz gróźb ataków na komputery, sieci i przechowywanych w nich informacji w celu zastraszenia lub zmuszenia rządu czy decydentów, w celu wsparcia celów politycznych czy społecznych. Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują poczucie strachu. Ataki, które prowadzą do śmierci czy uszkodzenia ciała, eksplozje, a także poważne straty ekonomiczne mogą być tego najlepszym przykładem. Poważne ataki na infrastrukturę krytyczną mogą zostać uznane za akt cyberterroryzmu w zależności od wyrządzonych szkód. Ataki które zakłócają nieistotne usługi lub są kosztownymi uciążliwościami, nie muszą stanowić aktu cyberterroryzmu[11].
2. James A. Lewis: „cyberterroryzm jest użyciem sieci oraz narzędzi komputerowych w celu sparaliżowania działania narodowej infrastruktury

---

[9] M. Czepielewski, *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii)*, w: *Cyberterroryzm. Nowe wyzwania…*, s. 178–188.

[10] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1, s. 175.

[11] D. Denning, *Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 2000, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (15.07.2015).

krytycznej (sieci energetycznych, transportowych, systemów rządowych), zastraszenia czy wymuszenia na rządzie lub populacji określonych zachowań”[12].

3. M. Pollit: „Cyberterroryzm jest zaplanowanym i politycznie umotywowanym atakiem przeciwko systemom, programom komputerowym oraz bazom danych, który skutkuje przemocą wobec celów niewojskowych, popełnionych przez grupy ponadnarodowe lub tajnych agentów”[13].

Jak możemy zauważyć, powyższe definicje różnią się między sobą w sposobie definiowania zjawiska cyberterroryzmu przede wszystkim określeniem celu ataku cyberterrorystycznego. Część badaczy opowiada się za traktowaniem cyberterroryzmu jako działania wymierzonego głównie w systemy informatyczne oraz sprzęt, jaki jest przez nie obsługiwany, z pominięciem typowych działań terrorystycznych, w których dochodzi do śmierci osób, uszkodzeń ciała czy poważnych strat materialnych. Bardzo ważnym czynnikiem, powodującym cyberterroryzm – tak jak i klasyczny terroryzm – jest czynnik psychologiczny. Wpływa on na spotęgowanie obaw przed atakiem, który może zakłócić prawidłowe funkcjonowanie danego państwa. Definicja cyberterroryzmu nie może ograniczać się jedynie do obszaru zagrożeń niematerialnych, popełnianych wyłącznie w sieci i wpływających na działanie systemów teleinformatycznych. Potencjalny atak może wyrządzić daleko idące straty materialne w rzeczywistym świecie – ludzie mogą zginąć lub decyzje przez nich podejmowane będą sprzeczne z ich wolą, która zostanie podporządkowana działaniom terrorystów. Nie każde działanie można uznać za akt terrorystyczny. W dobie internetu wiele osób preferuje działania w sieci od agitacji prowadzonej w sposób tradycyjny, warto przytoczyć przykład tzw. haktywistów. Podstawową różnicą między tą grupą a grupą terrorystyczną, jest cel działalności – haktywiści nie dążą do wyrządzenia szkód, w wyniku których ludzie giną lub są zastraszani groźbą utraty życia. Głównym ich celem są protesty i zakłócenie porządku publicznego poprzez zakłócenie działania stron rządowych. Najlepszym tego przykładem mogą być protesty społeczne wobec wprowadzenia ACTA w 2012 roku. Linia podziału może się jednak zacierać,

---

[12] J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, 2002, s. 1, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (15.07.2015).

[13] M.M. Pollit, *Cyberterrorism – Fact or a Fancy?*, w: *Focus on Terrorism*, ed. E.V. Linden, New York 2007, s. 67, https://books.google.pl/books?id=wl=-D42sYMDIC&pg=P65A&dq-Cyberterrorism+%E2%80%93+Fact+or+Fancy&hl=pl&sa=X&redir_esc=y#v=onepage&q=Cyberterrorism%20%E2%80%93%20Fact%20or%20Fancy&f=false (15.07.2015).

kiedy terroryści dotrą do haktywistów i zwerbują ich w celu pracy na własny użytek[14].

Akty cyberterrorystyczne nie ograniczają się tylko do działalności terrorystów, gdyż mogą być one popełniane zarówno przez grupy typowo przestępcze, jak i polityczne. Aby uznać czyn za cyberterrorystyczny, powinien on być przede wszystkim przeprowadzony przy użyciu elektronicznych narzędzi (komputer, internet) w celu destabilizacji funkcjonowania wybranego celu. Atak powinien skutkować poważnymi stratami materialnymi lub ludzkimi, wywołać efekt psychologiczny w postaci poczucia strachu i zagrożenia, które wpłyną na zmianę zachowań lub postępowania danej grupy społecznej, politycznej lub gospodarczej. Bez znaczenia pozostaje wtedy charakter ugrupowania lub osoby odpowiedzialnej za jego przeprowadzenie.

Ochrona instytucjonalno-prawna

Skuteczne rozwiązania prawne stanowią podstawę działań przeciwko każdemu popełnianemu przestępstwu. Przestępstwo popełnione w sieci lub za jej pomocą powinno być traktowane na równi z innymi. Polska będąc członkiem Unii Europejskiej (UE) korzysta z jej dorobku prawnego, które uzupełnia krajowe ustawodawstwo. Niestety w polskim prawie pojęcie cyberterroryzmu nie występuje bezpośrednio, podobnie jak w ustawodawstwie unijnym. W celu zbadania tego zjawiska należy przeanalizować dorobek prawny, dotyczący zarówno terroryzmu, jak i przestępczości komputerowej.

Wraz z postępująca globalizacją oraz dynamicznym rozwojem technologii informacyjnej państwa zaczęły przykładać większą wagę do zapewnienia bezpieczeństwa teleinformatycznego. Katalizatorem zmian w sposobie myślenia stały się wydarzenia z 11 września 2001 roku. Obowiązująca w Polsce Strategia Bezpieczeństwa Narodowego z 2000 roku straciła swoją aktualność, konieczne było opracowanie jej nowej wersji, która została opublikowana w 2003 roku i wraz z doktryną bezpieczeństwa UE stanowiła podstawę działań zmierzających do zmniejszenia prawdopodobieństwa wystąpienia ataku terrorystycznego. W kolejnych wersjach Strategii podkreślono niebezpieczeństwo, mogące mieć swe źródło w sieci; wersja z 2007 roku zwróciła uwagę na przestępczość cybernetyczną, omawiając bezpieczeństwo ekonomiczne, oddzielono również

[14] G. Weimann, *Cyberterrorism. How real is the threat?*, United States Institute of Peace Special Report, May 2004, s. 3, www.usip.org/sites/default/files/sr119.pdf (15.07.2015).

część, która omawiała bezpieczeństwo informacyjne oraz teleinformatyczne. W Strategii podkreślono konieczność zapobiegania próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa poprzez redukowanie jej podatności na to oddziaływanie. Zwrócono również uwagę na potrzebę tworzenia długofalowych planów ochrony kluczowych systemów teleinformatycznych oraz na odpowiednie zabezpieczenie dostępu do informacji niejawnych[15]. Zaktualizowana wersja Strategii w 2014 roku wyraźnie wskazała na zagrożenia natury informatycznej w punkcie 31: „Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci internet pojawiły się nowe zagrożenia, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw”[16]. Z powyższego opisu można wysnuć wniosek, że Polska jest coraz bardziej świadoma zagrożeń cybernetycznych.

Jak zauważa Aleksandra Suchorzewska, w polskim prawie brakuje jednej regulacji prawnej, która zawierałaby wszystkie przepisy dotyczące odpowiedzialności za nadużycia związane z technologią informacyjną[17]. Przepisy są rozproszone i zawierają je między innymi: Kodeks karny oraz Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. nr 133 poz. 883), Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 1994 r. nr 24 poz. 83), Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. nr 144 poz. 1204). Dodatkowo polskie ustawodawstwo musi uwzględniać dorobek prawodawstwa europejskiego, na który składają się Konwencja o Cyberprzestępczości oraz ramowa decyzja Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne. Podstawą prawną w kwestii osądzenia sprawców ataków cybernetycznych pozostaje kodeks karny, w szczególności rozdziały XIV, w którym poruszono kwestię terroryzmu

---

[15] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007, http://www.umwd.dolnyslask.pl/fileadmin/user_upload/Bezpieczenstwo/Prawo/Strategia_Bezpieczenstwa_Narodowego.pdf (15.07.2015).

[16] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 19, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (15.07.2015).

[17] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 206.

oraz XXXIII, gdzie przedstawiono kwestię przestępstw przeciwko ochronie informacji.

W ramach krajowych działań rząd polski podjął się stworzenia następujących programów: Rządowego programu obrony cyberprzestrzeni RP na lata 2009–2011[18] oraz na lata 2011–2016[19]. Dodatkowo 28 sierpnia 2012 roku Ministerstwo Administracji i Cyfryzacji przedstawiło dokument pt. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[20], który oparto m.in. o założenia programu obrony cyberprzestrzeni RP na lata 2009–2011. Swoim zasięgiem dokument ten obejmuje administrację rządową:

1. Urzędy obsługujące naczelne organy administracji rządowej: Prezesa Rady Ministrów, Radę Ministrów, ministrów i przewodniczących określonych w ustawach komitetów.
2. Urzędy obsługujące centralne organy administracji rządowej: organy inne niż w/w, tj. organy podporządkowane Prezesowi Rady Ministrów bądź poszczególnym ministrom.
3. Urzędy obsługujące terenowe organy administracji rządowej: wojewodów, organy administracji zespolonej i niezespolonej.
4. Rządowe Centrum Bezpieczeństwa.

Jednocześnie jest on rekomendowany dla administracji samorządowej szczebla gminnego, powiatowego i wojewódzkiego oraz innych urzędów, w tym: Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu Rzeczypospolitej Polskiej, Kancelarii Senatu Rzeczypospolitej Polskiej, Biura Krajowej Rady Radiofonii i Telewizji, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Biura Krajowej Rady Sądownictwa, urzędów organów kontroli państwowej i ochrony prawa, Narodowego Banku Polskiego, urzędu Komisji Nadzoru Finansowego, państwowych osób prawnych i innych niż wymienione wyżej państwowe jednostki organizacyjne[21].

By skutecznie zapobiegać zagrożeniom cyberterroryzmu, nie wystarczą tylko dobre rozwiązania prawne, potrzebne są wyspecjalizowane grupy, agencje, które będą odpowiadały za monitoring bezpieczeństwa. W Polsce w ramach struktur

---

[18] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011*, Warszawa 2009, http://bip.msw.gov.pl/download/4/4297/program20ochrony20cyberprzestrzeni.pdf (15.07.2015).

[19] *Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016*, Warszawa 2010, http://bip.msw.gov.pl/download/4/7445/RPOC-24092010.pdf (15.07.2015).

[20] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf (15.07.2015).

[21] Tamże, s. 7.

Agencji Bezpieczeństwa Wewnętrznego (ABW) powołano 1 lutego 2008 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT GOV PL, do którego zadań należy[22]:

- kreowanie polityki bezpieczeństwa w zakresie ochrony przed cyberzagrożeniami,
- koordynacja przepływu informacji między podmiotami w związku z cyberzagrożeniami,
- współpraca międzynarodowa w zakresie ochrony cyberprzestrzeni,
- pełnienie nadrzędnej roli w stosunku do wszystkich krajowych instytucji, organizacji oraz podmiotów resortowych w zakresie ochrony cyberprzestrzeni,
- gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla infrastruktury krytycznej Polski,
- reagowanie na incydentalne zakłócenia bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem infrastruktury krytycznej,
- analiza powłamaniowa z wykorzystaniem narzędzi informatyki śledczej,
- tworzenie polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej,
- szkolenie i uświadamianie przedstawicieli instytucji państwa,
- konsulting i doradztwo w zakresie cyberbezpieczeństwa.

Jak możemy zauważyć, Polska jest coraz bardziej świadoma zagrożeń, które pochodzą z sieci. Tradycyjne metody terrorystyczne stanowią równie poważne zagrożenie, co ich cyberterrorystyczny odpowiednik, a połączenie tych dwóch sposobów działania może skutkować poważnym zakłóceniem funkcjonowania państwa w wielu sektorach, począwszy od dostaw surowców, a skończywszy na systemie bankowym.

Zakończenie

Podsumowując rozważania dotyczące cyberterroryzmu należy stwierdzić, że jest on poważnym zagrożeniem bezpieczeństwa współczesnego państwa. Postępujący rozwój sieci teleinformatycznych oraz internetu przynosi wiele korzyści dla funkcjonowania różnych podmiotów zarówno politycznych, jak i gospodarczych, jednak niesie za sobą tyle samo zagrożeń. Odpowiadając na wcześniej

---

[22] E. Lichocki, *Bezpieczeństwo teleinformatyczne sił zbrojnych Rzeczypospolitej Polskiej w dobie zagrożeń cybernetycznych*, w: *Cyberterroryzm. Nowe wyzwania…*, s. 589–590.

postawione pytania stwierdzić należy, że państwa są świadome zagrożeń natury cyberterrorystycznej oraz cyberprzestępczości w ogóle. Polskie rozwiązania prawne są wystarczające do osądzenia potencjalnych sprawców przestępstw z użyciem systemów teleinformatycznych, jednak powinny być one uporządkowane i doprecyzowane, gdyż są rozproszone w wielu aktach prawnych, zaś ich interpretacja może nastręczać trudności ze względu na brak powszechnej definicji cyberterrorozmu w polskim prawodawstwie. W tym celu powinna zostać opracowana odrębna ustawa bądź wydane rozporządzenie, które w sposób bezpośredni odwoływałoby się do zjawisk wymienionych między innymi w strategii bezpieczeństwa z 2014 roku. Odpowiadając na kolejne pytanie, czy cyberterroryzm zastąpi tradycyjnie działania terrorystyczne, stwierdzić trzeba, że tak się nie stanie. Działania w sieci będą uzupełniały klasyczne ataki terrorystów, które w połączeniu z nimi mogą poważnie zagrozić bezpieczeństwu państwa, zwłaszcza jego infrastrukturze krytycznej. Ataki estońskie mogą być wzorcowym przykładem cyberterroryzmu, kiedy normalne funkcjonowanie państwa zostało praktycznie wstrzymane, wywołując panikę wśród obywateli. Dodatkowo prowadzona działalność rekrutacyjna i agitacyjna w internecie może dostarczać coraz to nowych osób zasilających szeregi organizacji terrorystycznych, w tym specjalistów zajmujących się informatyką lub bezpieczeństwem systemów teleinformatycznych z różnych zakątków świata. Należy przy tym uważać, aby nie ograniczać swobody wypowiedzi w sieci, skuteczne ściganie terrorystów nie może polegać na cenzurze treści publikowanych w internecie.

Aby skutecznie walczyć z zjawiskiem cyberterroryzmu, niezbędna jest harmonizacja działań państw, przede wszystkim na polu prawnym. Poszczególne kraje mają różne regulacje dotyczące przestępczości w sieci, dodatkowo brak wspólnej definicji cyberterroryzmu może rodzić problemy ewentualnego osądzenia sprawców przestępstwa. Trzeba zauważyć, że atak może być przeprowadzony z dowolnego zakątka świata, w dowolnym państwie i może być wymierzony w inny podmiot, który znajduje się na innym kontynencie, wykrycie sprawcy lub sprawców jest utrudnione, a często nawet niemożliwe.

Konkludując – cyberterroryzm jest zagrożeniem bezpieczeństwa państwa w XXI wieku i nie powinien być w żadne sposób bagatelizowany. Rozwiązania prawne i instytucjonalne należy skonstruować w takich sposób, aby umożliwiały skuteczne wykrycie i osądzenie sprawców ataku. Dodatkowo powinna mieć miejsce ścisła współpraca między państwami w celu wypracowania definicji tego zjawiska oraz skutecznego ścigania przestępców.

Bibliografia

Bógdał-Brzezińska Agnieszka, Gawrycki Marcin Florian, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Charvat Japiag, *Cyber Terrorism: A new dimension in battlespace*, w: *The virtual battlefield: perspectives on Cyber Warfare*, red. Christian Czosseck, Kenneth Geers, Amsterdam 2009, https://ccdcoe.org/sites/default/files/multimedia/pdf/05_CHARVAT_Cyber%20Terrorism.pdf (15.07.2015).

Czepielewski Mateusz, *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii)*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. Tadeusz Jemioła, Jerzy Kisielnicki, Kazimierz Rajchel, Warszawa 2009.

Denning Dorothy, *Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 2000, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (15.07.2015).

Gibson William, *Neuromancer*, Warszawa 1999.

Kowalewski Jakub, Kowalewski Marian, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1–2.

Lewis James, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, „Center for Strategic & International Studies, 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (15.07.2015).

Lichocki Ernest, *Bezpieczeństwo teleinformatyczne sił zbrojnych Rzeczypospolitej Polskiej w dobie zagrożeń cybernetycznych*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. Tadeusz Jemioła, Jerzy Kisielnicki, Kazimierz Rajchel, Warszawa 2009.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf (15.07.2015).

Pollit Mark, *Cyberterrorism – Fact or a Fancy?*, w: *Focus on Terrorism*, ed. Edward V. Linden New York 2007, s. 67, https://books.google.pl/books?id=wl-Ds42YMDIC&pg=PA65&dq=Cyberterrorism+%E2%80%93+Fact+or+Fancy&hl=pl&sa=X&redir_esc=y#v=onepage&q=Cyberterrorism%20%E2%80%93%20Fact%20or%20Fancy&f=false (15.07.2015).

Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011, Warszawa 2009, http://bip.msw.gov.pl/download/4/4297/program20ochrony20cyberprzestrzeni.pdf (15.07.2015).

Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016, Warszawa 2010, http://bip.msw.gov.pl/download/4/7445/RPOC-24092010.pdf (15.07.2015).

Sienkiewicz Piotr, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, t. 13, z. 2, http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf (15.07.2015).

Sienkiewicz Piotr, *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. Tadeusz Jemioła, Jerzy Kisielnicki, Kazimierz Rajchel, Warszawa 2009.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007, http://www.umwd.dolnyslask.pl/fileadmin/user_upload/Bezpieczenstwo/Prawo/Strategia_Bezpieczenstwa_Narodowego.pdf (15.07.2015).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (15.07.2015).

Suchorzewska Aleksandra, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Szubrycht Tomasz, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1.

Tafoya William, *Cyber Terror*, „FBI Law Enforcement Bulletin" 2011, vol. 80, no. 11, https://leb.fbi.gov/2011/november/leb-november-2011 (15.07.2015).

Weimann Gabriel, *Cyberterrorism. How real is the threat?*, United States Institute of Peace Special Report, May 2004, www.usip.org/sites/default/files/sr119.pdf (15.07.2015).

Wojciechowski Sebastian, *Terroryzm. Analiza pojęcia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1.

Streszczenie

Wraz z postępem technologicznym i rozwojem światowego internetu, zagrożenie nowymi formami terroryzmu zaczęło przybierać na sile. Jednym z tych zjawisk jest pojawienie się cyberterroryzmu, który jest połączeniem klasycznych działań terrorystów z wykorzystaniem najnowszych urządzeń teleinformatycznych. Państwa oraz organizacje pozarządowe są coraz bardziej świadome zagrożeń pochodzących z sieci i podejmują się walki z nimi w celu ochrony najważniejszych elementów infrastruktury krytycznej, gwarantujących sprawne funkcjonowanie państwa. Ataki cyberterrorystyczne nie zastąpią tradycyjnych działań terrorystycznych, jednak będą coraz bardziej złożone i będą się wzajemnie uzupełniać. Państwa muszą być gotowe zarówno na poziomie prawnym, jak i praktycznym na wystąpienie ataku cyberterrorystycznego, by móc go skutecznie odeprzeć i osądzić sprawców.

Słowa kluczowe: cyberterroryzm, bezpieczeństwo państwa, terroryzm

CYBER TERRORISM – A NEW THREAT TO NATIONAL SECURITY IN THE TWENTY-FIRST CENTURY

Summary

With advances in technology and the development of the global Internet, the emergence of new forms of terrorism began to gain momentum. One of these phenomena is the emergence of cyber-terrorism, which is a combination of classic terrorist methods with usage of the latest IT devices. Countries and NGOs are increasingly aware of the threats coming from the web and take up the fight to protect the most important elements of critical infrastructure that ensures functioning of the state on an efficient level. Cyberterrorist attacks will not replace traditional terrorist activities, however, they will become more complex and will complement each other. Countries must be ready both on the legal and practical area when a cyberterrorist attack occurs, in order to effectively repel and prosecute their perpetrators.

Keywords: cyber-terrorism, national security, terrorism