Marek Górka
Politechnika Koszalińska

Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa

Selected aspects of the definition of cyberterrorism and their importance in the perspective of security policy

Słowa klucze: cyberterroryzm, cyberprzestępstwo, cyberataki, cyberzagrożenie, polityka bezpieczeństwa

Key words: cyber terrorism, cybercrime, cyberattacks, cyber threats, security policy

Streszczenie

Cyberterroryzm stwarza poważne i szybko rozwijające się zagrożenia dla społeczeństwa oraz infrastruktury krytycznej państwa. Fakt ten wywołuje istotne zmiany w zakresie zapobiegania oraz zwalczania terroryzmu. Cyfrowy świat, w którym żyje społeczeństwo zapewnia szerokie możliwości dla cyberprzestępczości, ponieważ inicjuje i zachęca do wykorzystania ukrytych możliwości Internetu. Cyberterroryzm jest rodzajem przestępstwa, który jest skierowany przeciwko państwu i jego obywatelom. Obecnie sieci komputerowe są zagrożone i codziennie atakowane z powodu m.in. niezdolności do utrzymania dynamicznego rozwoju usług internetowych oraz szeroko dostępnych narzędzi i technik hakerskich. Jest to najbardziej trudne wyzwanie w walce cyberterroryzmem. Jednak sam termin jest często niewłaściwie wykorzystywany i nadużywany. Zrozumienie niebezpieczeństwa cyberterroryzmu musi zaczynać się od klarownego określenia jego definicji.

Abstract

Cyberterrorism creates serious and rapidly growing threats to society and the critical infrastructure of the state. This creates significant changes in the prevention and fight against terrorism. The digital world in which society is lived provides a wide range of opportunities for cybercrime as it initiates and encourages the use of hidden Internet capabilities. Cyberterrorism is a crime that is directed against the state and its citizens. Currently, computer networks are at risk and are attacked daily due to inter alia. The inabi-

lity to maintain dynamic development of web services and widely available hacking tools and techniques. This is the most difficult challenge in the fight against cyberterrorism. However, the term itself is often misused and abused. Understanding the dangers of cyberterrorism must begin with a clear definition of its definition.

Technologia zrewolucjonizowała wymianę informacji między ludźmi, stając się w ten sposób podstawowym filarem nowoczesnego społeczeństwa. Z drugiej jednak strony stworzyła nowe problemy i zagrożenia bezpieczeństwa. Obecnie infrastruktura krytyczna wielu państw napotyka coraz większe cyberzagrożenia ze względu na ustawiczny postęp w dostępnie do złośliwych narzędzi programowych, a także z uwagi na wciąż rozwijające się nowe technologie. Kluczowy jest również rosnący proces automatyzacji, który stwarza więcej możliwości do zaistnienia cyberataku. Ponadto nie zawsze zapewniona zostaje wystarczająca ochrona przed nieautoryzowanym użyciem systemów informatycznych. Liczba ataków na systemy informatyczne w przeciągu pierwszej dekady XXI wieku, których motywacją były zarówno cele kryminalne, jak i polityczne wrosła do ogromnych rozmiarów na całym świecie.

Nowoczesna era cyfrowa została nazwana „wiekiem informacji"[1]. Społeczeństwo na całym świecie stało się trwale uzależnione od technologii. Powszechnie znana jest już teza sformułowana przez Departamentu Obrony USA, iż cyberprzestrzeń jest piątą domeną konfliktu po przestrzeni: powietrznej, lądowej, morskiej oraz kosmicznej.

Proponowana praca skupia się na pojęciu cyberterroryzmu i dokonuje ocenić jego potencjalne zagrożenie dla bezpieczeństwa narodowego. Jednym z celów artykułu jest skonfrontowanie podobieństw i różnic między takimi zjawiskami, jak cyberterroryzm, cyberprzestępstwo, wojna cybernetyczna (cyberwojna), hakerstwo oraz hacktivism. Warto zauważyć, że nie ma wypracowanej jednoznacznej definicji cyberterroryzmu na gruncie naukowym, podobnie jak nie ma w przypadku klasycznego zjawiska terroryzmu, którego ramy definicyjne trudno jest sprecyzować. Dodatkowym zadaniem do zrealizowania w pracy jest próba odpowiedzi na pytanie czy cyberterroryzm jest obecnie realnym zagrożeniem? Jeśli tak, to jaka jest jego definicja? Jakie są różnice między nim a cyberwojną i cyberprzestępczością? Jakie wydarzenia mogą inicjować cyberataki i dlaczego terroryści decydują się stosować technologię informacyjną i komunikacyjną? Ważną refleksją podjętą w pracy jest próba zastanowienia się, które elementy bezpieczeństwa państwa mogą stać się celami ataków cybernetycznych?

Pytanie typu w jakim stopniu współczesne państwo może być narażone na cyberterroryzm, nie jest tylko wyzwaniem dla służb odpowiedzialnych za bezpieczeństwo państwa, ale jest również problemem badawczym, z którym zmierzyć musi się nauka.

[1] N. Ayres, L.A. Maglaras, *Cyberterrorism targeting the general public through social media*, „Security and Communication Networks" 2016, vol. 9 (15), s. 2864–2875.

Praca jest także okazją do podjęcia refleksji na temat tego, jaka forma terroryzmu (cyber czy konwencjonalna) w drugiej dekadzie XXI wieku jest najbardziej prawdopodobnym zagrożeniem dla bezpieczeństwa narodowego?

Najnowsze rozwiązania technologiczne zwiększają powagę zagrożeń nad dotychczasowymi, klasycznymi wyzwaniami wobec bezpieczeństwa narodowego, wzbudzają również szereg lęków i niepokojów zarówno na międzynarodowym, jak i lokalnym poziomie. Pojęcie bezpieczeństwa stopniowo ewoluowało, zwłaszcza od czasu rozpadu Związku Radzieckiego i końca zimnej wojny. Jednocześnie globalizacja zmieniła międzynarodowe zasady oraz normy codziennego życia, ułatwiła i przyspieszyła przepływ kapitału oraz technologii, z jednoczesnym osłabieniem barier narodowych. Podmioty pozarządowe odgrywają obecnie kluczową rolę w polityce międzynarodowej, niektóre z nich stanowią zagrożenie, a inne spełniają rolę pomostu między społecznościami i narodami. Główną tezą pracy jest stwierdzenie, że zjawisko cyberterroryzmu prowadzi do takich samych lub większych zagrożeń jak konwencjonalny terroryzm.

1. Cyberprzestrzeń

Przed przystąpieniem do analizy samego pojęcia cybetrroryzmu, warto zastanowić się czym jest cyberprzestrzeń i dlaczego jest ona tak ważna dla polityki bezpieczeństwa państwa? Rozwija się ona bardzo szybko. W ciągu ostatnich dwóch dekad charakteryzuje się dynamicznymi zjawiskami zachodzącymi na poziomie politycznym, społecznym, jak i gospodarczym. Obecnie wiele dziedzin życia, począwszy od handlu poprzez edukację, kulturę, innowację po aktywność polityczną istnieje w cyberprzestrzeni. Eksperci przypuszczają, że do 2020 roku, czyli około 40 lat po stworzeniu Internetu, prawie 5 mld ludzi stanie się uczestnikami tej nowej globalnej społeczności[2].

Oprócz dużych możliwości, jakie stwarza Internet dla firm, rządów i pojedynczych osób, cyberrzeczywistość tworzy także zagrożenia dla bezpieczeństwa. Systemy komputerowe obsługujące infrastrukturę krytyczną są odpowiedzialne za kontrolowanie i działanie elementów sieci przesyłowej, jak energia elektryczna, woda oraz telekomunikacja. A zatem im bardziej świat staje się uzależniony od cybertechnologii, tym liczba potencjalnych celów cyberataków rośnie.

Okazuje się, że specyfika Internetu, którą można odczytać jako zaletę w procesie funkcjonowania społeczeństwa obywatelskiego, może stanowić także silne argumenty, które przekonują grupy terrorystyczne do wykorzystania i przeniesienia swojej

[2] J.D. Negroponte, S.J. Palmisano, A. Segal, *Defending an Open, Global, Secure, and Resilient Internet*, Nowy Jork 2013, s. 3–7.

działalności na poziom cyberprzestrzeni. Zapewnienia ona terrorystom anonimowości, która jest głównym powodem utrudniającym ich śledzenie. Inną zaletą jest łatwy dostęp do technologii, której obsługa nie jest skomplikowana i stwarza możliwość kierowania akcją z ogromnej odległości. Zakres oraz siła oddziaływania cyberataku jest ogromna przy niskich kosztach. Cyberprzestrzeń stwarza także niespotykane dotąd możliwości przepływu informacji, co sprawia że wymiana informacji jest niemal natychmiastowa. Z uwagi na powszechność zastosowania technologii w życiu publicznym, terroryści posiadają ogromny wybór co do celów ataku, mogą to być bowiem sieci komputerowe firm, banki, szpitale, transport publiczny itd. Warto także zwrócić uwagę, że każdy dokonany akt terrorystyczny przyciąga uwagę mediów, z tą różnicą, że cyberterroryści posługując się Internetem mają wpływ na charakter i rodzaj przekazu, który sami tworzą[3].

2. Terroryzm tradycyjny a cyberterroryzm

Zagrożenie terroryzmem nigdy nie było tak widoczne i odczuwalne jak obecnie. W ciągu ostatnich trzydziestu lat groźba terroryzmu oraz strachu przed nim stale wzrasta. Jednak dopiero na początku drugiego tysiąclecia, w wyniku dominacji cybertechnologii, działania terrorystów stały się jeszcze bardziej niebezpieczne i destrukcyjne, a sprawcy takich czynów są znacznie bardziej nieuchwytni.

Dzisiejszy świat stoi w obliczu nowych i nieznanych rodzajów broni. Międzynarodowy system bezpieczeństwa oraz służby wywiadowcze i kontrwywiadowcze, których nadrzędnym celem jest ochrona państwa i jego obywateli, nie są w stanie sprostać temu nowemu przeciwnikowi. Integracja świata wirtualnego i fizycznego stanowi główne wzywanie przed służbami antyterrorystycznymi[4]. Brak skuteczności wybranych metod i strategii, opracowanych w celu zwalczania terroryzmu w ostatnich latach, może świadczyć o ich nieskuteczności.

Na początek warto rozpocząć rozważania od zdefiniowania czym jest terroryzm? Jak różni się to pojęcie od cyberterroryzmu oraz w jaki sposób technologia może mieć wpływ na ewolucję tego zjawiska? Wiele konstrukcji definicyjnych dotyczących terroryzmu podkreśla czynniki, które pozwalają zaklasyfikować określone wydarzenia w zakres tego pojęcia. Przede wszystkim musi to być zorganizowana przemoc, która wywołuje uczucie niepokoju, paniki i strachu w społeczeństwie. Kluczowy jest

[3] M. Voicescu, *Cyber terrorism and bioterrorism – new forms of terrorists action. size, effects and countermeasures*, International Scientific Conference „Strategies XXI" 2012, vol. 3, s. 313–318.

[4] J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, „CRS Report for Congress", 22.01.2007, s. 3–6.

także aspekt naruszenia dotychczasowych norm i zwyczajów życia publicznego. Podstawowym elementem takiej działalności muszą być także motywacje polityczne, które poprzez zrealizowane lub udaremnione ataki mają wpływać na podejmowane decyzje określonych władz[5].

Analiza literatury przedmiotu wskazuje, że polityczny charakter jest elementem, który oddziela terroryzm od innych działań przestępczych zazwyczaj motywowanych względami finansowymi lub przyczynami osobistymi. Z drugiej jednak strony kwestie ekonomiczne mogą współwystępować z politycznymi. Trudno także ocenić zaangażowanie polityczne określonych grup, ponieważ ich silnie zideologizowany program i radykalizm inicjuje także postulaty polityczne[6]. Nie inaczej jest także z osobistymi frustracjami, które bardzo często występują wśród pracowników instytucji o charakterze strategicznym dla bezpieczeństwa państwa. Ich wiedza oraz umiejętności mogą posłużyć jako narzędzia do dokonania zemsty, przybierającej często formę ataku terrorystycznego bądź sabotażu, skierowanego wobec dotychczasowego otoczenia.

Grupy terrorystyczne dążą do zapewnienia wsparcia finansowego, pozwalającego na planowanie i przeprowadzanie ataków, zwłaszcza jeśli nie mają sponsorów. Dlatego należy poddać rozwadze możliwość rozszerzenia definicji terroryzmu o motywacje ekonomiczne. Z drugiej strony wykorzystanie sieci komputerowych do wspierania działań o charakterze przestępczym, np. wprowadzanie do legalnego obrotu pieniędzy uzyskanych z nielegalnych źródeł, będzie przejawem cyberprzestępczości. Dlatego do jasnego sklasyfikowania czynności określanych bądź nie jako terrorystyczne wymagane jest pogłębione rozeznanie operacyjne, jak i badawcze.

Eksperci uważają, że cyberterroryzm może być bardziej tragiczny w skutkach niż konwencjonalny terroryzm[7]. Ryzyko polega na tym, że cyberterroryzm może być skierowany na infrastrukturę odpowiedzialną za m.in.: kontrolę ruchu lotniczego, zapór wodnych, a także infrastruktury finansowej i handlowej[8]. Na podstawie powyższych uwag można zauważyć, że terroryzm, jak i cyberterroryzm polega na wykorzystaniu informacji jako metody wpływu i manipulacji.

Dotychczas terrorysta chcąc spowodować masowe zniszczenie lub chaos mógł planować np. atak na elektrownię. W celu realizacji takiego planu musiał niepostrzeżenie przedostać się na teren zakładu, przedtem jednak pokonać szereg barier fizycz-

[5] S. Topor, *Cyber criminal and cyber terrorist – two concepts that need to be differently treated*, International Scientific Conference „Strategies XXI" 2016, vol. 3, s. 181–186.

[6] Ibidem.

[7] J. Matusitz, *Cyberterrorism: Postmodern State of Chaos*, „Information Security Journal: A Global Perspective" 2008, vol. 17 (4), s. 179–187.

[8] L. Jarvis, S. Macdonald, L. Nouri, *The Cyberterrorism Threat: Findings from a Survey of Researchers*, „Studies in Conflict & Terrorism" 2014, vol. 37 (1), s. 68–90.

nych. W erze cyfrowej tradycyjne środki ochrony, takie jak wysokie ogrodzenie, monitoring oraz wartownicy nie mają znaczenia. W takim przypadku sieć, przy pomocy której nadzorowana jest praca elektrowni, może być kontrolowana przez hakerów znajdujących się w dowolnym miejscu na świecie[9]. Rosnąca dostępność technologii komputerowej stworzyła nowe narzędzia, dzięki którym terrorysta może zaplanować i przeprowadzić ataki. Choć nie zdarzyły się do tej pory akty cyberterroryzmu w tak tragicznym wymiarze, jak klasyczne zamachy terrorystyczne, to jednak część badaczy przypuszcza, że państwa skazane są na powtórzenie zamachu w cyberprzestrzeni, w takiej skali jak to miało 11 września 2001 roku[10].

3. Definicje cyberterroryzmu

Brak jasnej definicji, czym jest cyberterroryzm, a także rozmyte granice w zakresie geograficznym, politycznym, a także znaczeniowym, wynikające z przenikania i krzyżowania się pojęć oraz zjawisk, zmuszają do usystematyzowania dotychczasowych zjawisk w zakresie nauk społecznych oraz określenia granic semantycznych zaistniałych procesów. Pomimo tego, że żadna pojedyncza definicja terminu jeszcze nie została ujednolicona w literaturze przedmiotu, warto przytoczyć najważniejsze interpretacje pojęcia cyberterroryzmu, które funkcjonują w zakresie nauk o polityce i nauk o bezpieczeństwie.

Określenie „cyberterroryzm" po raz pierwszy użył Barry Collin, starszy pracownik naukowy w Instytucie Bezpieczeństwa i Wywiadu w Kalifornii, w 1980 roku[11]. Termin ten odnosił się do sklasyfikowania ataku komputerowego jako „cyberterroryzmu". Jednak z uwagi na brak doprecyzowania w niej intencji jaka przyświecała stronie atakującej oraz braku określenia tożsamości sprawcy ataku, jest to definicja wysoce problematyczna, szczególnie w kontekście dynamicznie zmieniających się relacji międzynarodowych, których odzwierciedleniem jest także cyberprzestrzeń[12].

Popularna definicja obecna w literaturze przedmiotu określa cyberterroryzm jako bezprawny atak lub groźbę ataku na komputery, sieci oraz informacje (przechowywane w niej). Przeprowadzany jest on za pośrednictwem komputerów, w realizacji celów politycznych poprzez zastraszenie i próby zmuszania władzy państwowej lub jej

[9] Ch. Pedersen, *Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security*, „Pepperdine Policy Review" 2014, vol. 7 (1), s. C1–C21.

[10] Y. Lappin, *Virtual Caliphate*, Waszyngton 2011, s. 142.

[11] A. Kontselidze, *Cyberterrorism – when technology became a weapon*, „European Scientific Journal" 2015, s. 24–29.

[12] A. Alqahtani, *The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia*, „International Conference on Information Warfare and Security" 2013, s. 231–236.

obywateli do określonych zachowań. Dla części badaczy, aby określić działania mianem cyberterroryzmu konieczne jest zaistnienie wymogu fizycznego uszkodzenia, w przeciwnym razie przypadek taki można sklasyfikować w kategoriach „haktywizmu"[13].

Z kolei ekspert do spraw bezpieczeństwa Dorota Denning definiuje cyberterroryzm jako politycznie motywowane działania hakerskie, których zamiarem jest spowodowanie poważnych szkód, takich jak utrata życia lub uszkodzenia w obszarze gospodarczym[14]. Podkreśla ona także, że cyberterroryzm jest zjawiskiem łączącym terroryzm i cyberprzestrzeń. Zjawisko to rozumiane jest jako bezprawny atak lub groźba ataku na komputery, sieci oraz wykorzystywanie przechowywanych informacji w celu zastraszania lub zmuszania państwa i jego obywateli do określonych zachowań[15]. Uwypukla również warunek, iż aby móc uznać taki atak za przejaw cyberterroryzmu, powinien on prowadzić do przemocy wobec osób lub mienia bądź przynajmniej doprowadzić do uszkodzenia, które wygeneruje wystarczająco dużo społecznego strachu z powodu takich tragicznych wydarzeń, jak np. wybuchy lub katastrofy w obszarze transportu publicznego, zanieczyszczenie wody lub awarie systemu finansowego[16].

W podobnym tonie opisują cyberterroryzm inni badacze, wskazując że jest to rodzaj terroryzmu motywowany politycznie z wykorzystaniem komputerów, informacji, aplikacji pomocnych w nawiązywanie kontaktów oraz technologii infrastruktury, w celu przeprowadzenia destrukcyjnych i szkodliwych działań terrorystycznych[17]. W kontekście dwóch ostatnich definicji można uznać, że cyberterroryzm jest przejawem ewolucji tradycyjnego terroryzmu, który dostosował się do wymagań życia informacyjnego.

Następną definicję rozpowszechniło Federalne Biuro Śledcze (FBI) proponując uznać cyberterroryzm za atak z premedytacją, motywowany politycznie, wobec informacji, systemów komputerowych, oprogramowania i danych, przeprowadzany przez grupy narodowe lub tajnych agentów[18]. Na tej podstawie można wysnuć hipotezę, że cyberterroryzm powinien być zdefiniowany jako zorganizowane i przemyślane

[13] A. Dean, *Cyber Threats in the 21st Century*, „Security" 2012, vol. 49 (9), s. 70.

[14] D. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militacy*, red., J. Arquilla, D. Ronfeldt, Santa Monica 2001, s. 281–288.

[15] A. Alqahtani, *The Potential Threat of Cyber-Terrorism...*, s. 231–236.

[16] D. Denning, *Cyberterrorism, Prepared for Estimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, http://www.cs.georgetown.edu/~denning/infosec/cvberterror.html [dostęp: 7.10.2016].

[17] W. Webster, F. Cilluffo, *Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo*, Waszyngton 1998, s. 48–62.

[18] M. Voicescu, *Cyber terrorism and bioterrorism*..., s. 313–318.

działanie mające na celu wywołanie zakłóceń, blokady wybranej usługi, zniszczenie bądź uszkodzenie oprogramowania, aby zastraszyć lub zmusić rządy lub organizacje do określonych działań w wymiarze politycznym, religijnym lub ideologicznym[19].

A zatem jedną z konstytutywnych cech definicji cyberterroryzmu jest zdolność do popełniania konkretnych działań terrorystycznych przy użyciu komputera oraz uzyskania nieproporcjonalnych skutków awarii, paraliżu i zakłóceń w funkcjonowaniu instytucji oraz obiektów użyteczności publicznej. Drugim aspektem konsekwencji ataków cybernetycznych jest zwiększenie paniki i eskalacji negatywnych emocji w społeczeństwie poprzez wpływanie, zniekształcanie lub kontrolowanie procesu informacyjnego, co w konsekwencji zwiększa efekt i wydajność całego działania terrorystycznego.

Przy próbie zdefiniowania zjawiska cyberterroryzmu pozostawia się na marginesie rozważań i taki fakt, że początek tego zjawiska, jak i jego finalne konsekwencje nie istnieje tylko w cyberprzestrzeni. Jego skutki mogą mieć wymiar fizyczny, możliwe jest bowiem zniszczenie dowolnego urządzenia, systemów i sieci informacyjnych, oprogramowania komputerowego oraz baz informacyjnych funkcjonujących w wybranej społeczności.

Jednym z podstawowych wyzwań stojących przed próbą zdefiniowania cyberterroryzmu jest trudność w identyfikacji podmiotu odpowiedzialnego za uruchomienie cyberataku. Jak się okazuje na arenie międzynarodowej jest to kluczowa kwestia, bowiem w zależności od tego, który podmiot jest inicjatorem ataku (może to być bowiem państwo, organizacja terrorystyczna bądź haker), zależy rodzaj i siła zastosowanego odwetu. Cyberterroryzm może być również działalnością indywidualnej osoby.

4. Wybrane aspekty cyberterroryzmu

Określenie ram definicyjnych nie wystarczy jednak w zrozumieniu zagrożeń wywołanych cyberterroryzmem. Postęp technologiczny sprawił, że cyberzagrożenia w ostatnich latach stały się jednym z głównym problemów dla wielu urzędów państwowych.

Według Dorothy E. Denning, aby zrozumieć potencjalne zagrożenie cyberterroryzmu należy wziąć pod uwagę dwa czynniki: po pierwsze, czy istnieją cele, które są podatne na atak; a po drugie czy terroryści mają zdolność i motywację, aby je zaatakować[20].

[19] S. Topor, *Cyber criminal and cyber terrorist...*, s. 181–186.
[20] Ibidem.

Cyberatakami zagrożone są nie tylko zasoby informacyjne przechowywane w cyberprzestrzeni, ale wszystkie krytyczne elementy infrastruktury, które opierają się na technologii informacyjnej. Choć prawdopodobnie nie da się zapobiec zagrożeniu cyberterroryzmem, to ważnym aspektem dla bezpieczeństwa narodowego jest zidentyfikowanie luk, które mogą zostać wykorzystane do przeprowadzenia ataków terrorystycznych, zarówno w cyber, jak i konwencjonalnym wymiarze. Dzięki temu będzie możliwe ograniczenie strat i szkód po incydentach terrorystycznych[21].

Ponieważ elementy, takie jak infrastruktura krytyczna czy system finansowy, opierają się w głównej mierze na systemach informatycznych, należy przypuszczać, że jakakolwiek awaria spowodowana aktem cyberterroryzmu będzie bardzo kosztowna i szkodliwa dla państwa, a tym samym będzie stanowić bezpośrednie zagrożenie dla bezpieczeństwa narodowego.

Na podstawie dotychczasowej wiedzy i doświadczenia można wyszczególnić dwa główne kierunki ataków cyberterroryzmu: pierwszy typ obejmuje działania polityczne zmierzające do awarii lub całkowitego zniszczenia określonego celu. Efekty takiego ataku są bardzo podobne do skutków działań przeprowadzonych w formie konwencjonalnego terroryzmu. Drugi typ to działania, które polegają na użyciu technologii informacyjnych i komunikacyjnych, a realizowane są przez hakerów, poprzez m.in. wirusy lub ataki Dos i DDoS oraz nieautoryzowany dostęp do prywatnych, korporacyjnych lub rządowych systemów z zamiarem oglądania, kopiowania bądź zniszczenia danych[22].

W kontekście ewolucji warto podkreślić potencjał grup terrorystycznych, który polega na umiejętności adaptacji do wymogów życia codziennego bezpośrednio zależnego od technologii informacyjnej. Cyberterroryzm zagraża więcej niż tylko jednemu lub dwóm obszarom infrastruktury krytycznej; wpływa na wszystkie systemy komputerowe, które zarządzają krytyczną infrastrukturę począwszy od sieci elektroenergetycznej, wodnej, urządzeń do sektorów transportu i bezpieczeństwa publicznego po globalne giełdy finansowe.

Chociaż terroryści mogą dokonywać cyberataków na wybrany fragment infrastruktury, to jest również prawdopodobne, że mogą kierować swoje działania na gospodarkę państwa jako całość. W tym przypadku celem byłoby zainicjowanie wielu cyberataków z zamiarem stworzenia ogromnej niestabilności, pogrążając w ten sposób w chaosie całe państwo[23].

---

[21] A. Alqahtani, *The Potential Threat of Cyber-Terrorism...,* s. 231–236.

[22] M. Gorge, *Cyberterrorism: Hype or Reality?,* „Computer Fraud & Security" 2007, vol. 2, s. 9–12.

[23] J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack...,* s. 3–6.

Realizacja cyberzagrożeń zwiększa dystans pomiędzy agresorem a ofiarą, ponadto relacja między tymi stronami traci czynnik bezpośredni czy też osobisty, jak to ma miejsce w klasycznym konflikcie. Działania w cyberprzestrzeni uwalniają od potrzeby prowadzenia organizacji, której jedną z cech jest zhierarchizowana struktura. Ponadto dezaktualizują one znaczenie posiadania i kontrolowania określonego terytorium geograficznego dla cyberterrorystów[24].

Cyberterroryzm umożliwia wyrządzenie szkód bez przykrych konsekwencji dla ich autora, bowiem tego typu działania przy wykorzystaniu technologii pozwalają zachować anonimowość i dokonywać ataków na ogromne odległości, dzięki czemu istnieją niewielkie szanse na złapanie ich sprawcy. Jest to więc sposób na to, aby „słabsza" strona zaatakowała „silniejszego" przeciwnika, z jednoczesnym wyrządzeniem jemu jak największych strat[25].

5. Pojęcie cyberterroryzmu wobec innych cyberzagrożeń

Różnice między wspomnianymi powyżej zjawiskami (cyberwojna, cyberprzestępczość, cyberterroryzm) stają się coraz bardziej rozmyte. Różnorodność sprawców takich działań, jak: pojedyncze osoby, organizacje lub zideologizowane grupy bądź instytucje państwowe komplikują nie tylko definicje, ale i wybór oraz stosowanie działań defensywnych przed cyberzagrożeniami. Stąd jak można zrozumieć występujące podobieństwa, które zacierają granice semantyczne między zjawiskiem cyberataku, cyberprzestępstwa, cyberwojny czy też cyberterroryzmu[26]. Każde z powyższych zjawisk w cyberprzestrzeni posiada własne, indywidualne motywacje oraz cele, które jednak w praktycznym działaniu wzajemnie nakładają się na siebie.

5.1. Cyberprzestępstwa

Warto zwrócić uwagę na potrzebę ustalenia granic między takimi pojęciami, jak choćby cyberterroryzm i cyberprzestępczość, które mają również znaczenie dla określenia sposobów ich zwalczania. W literaturze przedmiotu za główną różnicę między atakiem cybernetycznym i cyberterroryzmem uważa się kwestię intencji czy też motywacji sprawcy. Osoba dokonująca cyberataku może mieć m.in. motywy finansowe. Natomiast najważniejszą intencją cyberterrorysty jest zawsze motyw polityczny, społeczny lub religijny. Innymi słowy aktywność w cyberprzestrzeni w obu przypadkach

[24] A. Dean, *Cyber Threats...*, s. 70.

[25] T. Regan, *When terrorists turn to the Internet Seemingly unconnected events may have a more sinister source: Series*, „The Christian Science Monitor", 1.07.1999, s. 17.

[26] A. Dean, *Cyber Threats...*, s. 70–76.

może być analogiczna, jednak jej uzasadnienie, będące podstawą działania w cyberprzestrzeni, będzie już odmienne[27].

Cyberprzestępstwa stanowią obecnie najbardziej rozpowszechnioną formę cyberzagrożeń; są one bardziej powszechne niż zjawisko cyberterroryzmu czy też wojny cybernetycznej toczonej przez państwa. Jednak główną różnicą między atakiem cybernetycznym i cyberterroryzmem jest intencja sprawcy.

Niektórzy cyberprzestępcy tworzą zorganizowane grupy do prowadzenia cyberprzestępczości. Przyjęcie specjalistycznych zestawów umiejętności i profesjonalizacja praktyk biznesowych stale rośnie m.in. na skutek posiadanych umiejętności technicznych oraz niezbędnych narzędzi i zasobów, które służą następnie do prowadzenia cyberprzestępczości[28]. Na ten proceder składa się wiele różnych działań, które występują w różnej formie, jak np. oszustwa, fałszerstwa, kradzież własności intelektualnej, ingerencja w system danych, nielegalny dostęp do urządzeń i przechwytywania sygnału elektronicznego.

Jednym z najbardziej rozpowszechnionych metod są przestępstwa finansowe, które mogą wydawać się zupełnie niezwiązane z aktami cyberterroryzmu, ale w rzeczywistości są one ze sobą zintegrowane. Obecnie wiele organizacji terrorystycznych dokonuje tego typu przestępstw, jak fałszowanie kart kredytowych lub kradzież tożsamości, które pozwalają na dostęp do kont bankowych, a tym samym umożliwiają finansowanie działalności terrorystycznej[29]. Okazuje się więc, że kradzież tożsamości w rzeczywistości może być elementem większego ataku terrorystycznego. Badacze zauważają również, że podziemny świat cyberprzestępczości jest także swoistym „poligonem" dla hakerów, którzy rozwijają i doskonalą swoje umiejętności[30].

5.2. Hakerzy

Grupy terrorystyczne mogą rekrutować wysoko wykwalifikowanych hakerów (na podstawie motywacji ideologicznych lub finansowych), aby za pomocą ich umiejętności dokonywać działań cyberterrorystycznych. Analizując charakter działań hakerów, cyberprzestępców oraz cyberterrorystów można stwierdzić, że nie ma większych różnic w metodach działania wśród tych grup. Obecnie hakerzy mogą umożliwić dostęp do każdej sieci komputerowej. Posiadają oni umiejętności oraz narzędzia umożliwiające zainfekowanie określonych urządzeń szkodliwym oprogramowaniem.

[27] Ibidem, s. 70–76.

[28] Ibidem.

[29] D. Negroponte, S.J. Palmisano, A.Segal, *Defending an Open...*, s. 23; J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack...,* s. 18; Y. Lappin, *Virtual Caliphate...*, s. 98.

[30] J. Carr, *Inside Cyber Warfare, 2nd Edition Mapping the Cyber Underworld*, Publisher: O'Reilly Media 2011, s. 22–25.

Podstawowe różnice pozwalające odróżnić działalność cyberterrorystyczną od cyberprzestępczej polega nie tyle na zastosowaniu metod w uzyskaniu określonych celów, ale na ich sposobie wykorzystania. Przykładem ilustrującym powyższą odmienność jest sytuacja polegająca na uzyskaniu dostępu do pewnego rodzaju informacji, np. hasła dostępu. Jest to oczywiście działalność sprzeczna z prawem, jednak w przypadku hakera nie będzie miała ona takich konsekwencji społecznych, oczywiście pod warunkiem że nie zostanie ona ujawniona i wykorzystana przeciwko wybranej osobie. Natomiast działalność cyberterrorystyczna polega na wykorzystywaniu wykradzionych informacji, które następnie mogą posłużyć do przeprowadzenia ataków lub wspierania na dalszym etapie działalności terrorystycznej. Okazuje się zatem, że nie każde zagrożenie ujawnienia skradzionych informacji z komputerów powinno być traktowane jako cyberterroryzm.

Kluczowa różnica odnosi się do działania zmierzającego do zmiany procesów, instrukcji lub innych procedur niezbędnych do funkcjonowania określonego systemu. Zmiany takie w niektórych przypadkach mogą doprowadzić do tragicznych konsekwencji. Oczywiście czym innym będzie naruszenie integralności systemu w celu krytyki, ośmieszenia wybranej osoby lub zamanifestowania określonych poglądów. Tego typu działania nie mają na celu doprowadzenia do uszkodzenia lub zniszczenia wybranych obiektów. Czym innym jest za to cyberterroryzm, którego działania polegają na naruszeniu integralności systemu w celu uzyskania kontroli nad systemami odpowiedzialnym za utrzymanie kontaktu elektronicznego, obsługi transportu, elektryczności czy też pracę i funkcjonalność szpitali, banków itp.

Innym ważnym rozróżnieniem jest możliwość dostępu do informacji i zasobów informacyjnych. Jeżeli system jest elementem strategicznej infrastruktury krytycznej, jak np. bazy informacyjne policji lub innych służb odpowiedzialnych za bezpieczeństwo narodowe, to ich zablokowanie może być potraktowane jako wspierania działań terrorystycznych. Podobnie jak odmowa usługi komputerowej odpowiedzialnej za transport publiczny, której konsekwencje mogą być tragiczne. Różnica zatem polega na stopniu wrażliwości informacji oraz zasobów obsługiwanych przez określony system, co ma bezpośrednie przełożenie na konsekwencje takiego ataku[31].

Zdaniem badaczy część hakerów może reprezentować podobne cechy charakteru do terrorystów. Analogia pomiędzy tymi stronami opiera się przede wszystkim na narcystycznym zaburzeniu osobowości. Wśród takich osób zauważyć można najczęściej wysokie poczucie własnej wartości, przekonanie o sukcesie, silną potrzebę przyciągnięcia uwagi i podziwu innych, negatywne reakcje w sytuacji zagrożenia własnych uczuć, a także brak empatii[32].

[31] S. Topor, *Cyber criminal and cyber terrorist...,* s. 181–186.
[32] Ibidem.

Zdolność do wywołania cyberataku, a tym samym stworzenie zagrożenia dla bezpieczeństwa publicznego ze strony władz obcego państwa, organizacji terrorystycznej lub hakera w rzeczywistości są analogiczne. W kontekście prowadzonej analizy, ważne jest wskazanie na różnice, jakie występują pomiędzy określeniem przejawu hakerstwa i cyberterroryzmu. Terroryzm jest zbrodnią, ale nie każde przestępstwo lub niezgodne z prawem korzystanie z systemu komputerowego jest aktem terrorystycznym. Przede wszystkim, aby zakwalifikować działania w cyberprzestrzeni jako akt cybernetycznego terroru muszą one zostać popełnione przez terrorystów, a nie przez hakerów. Literatura przedmiotu wskazuje również na odmienne cele, haker bowiem w przeciwieństwie do terrorysty nie kieruje się celami politycznymi ani nie ma zamiaru zabijać ludzi, by wywołać panikę lub szerzyć strach. Zatem cyberterroryzm musi być rozumiany jako atak, mający swój początek w cyberprzestrzeni, motywowany politycznie, którego celem jest – poprzez wykorzystanie sieci komputerowej – zagrożenie dla życia lub inne poważne konsekwencje dla bezpieczeństwa publicznego oraz wywołanie paniki i strachu w społeczeństwie[33].

5.3. Cyberatak

Do głównych skutków cyberataków należy zaliczyć awarię, dysfunkcjonalność bądź paraliż systemów odpowiedzialnych za pracę określonych urządzeń kluczowych dla wykonywania statutowych zadań przez instytucje państwowe lub niepubliczne. Przejawem takiej dysfunkcjonalności systemu może być zakłócenie integralności urządzeń, poprzez zmianę informacji lub danych; zablokowanie dostępu do systemu obsługującego określone urządzenia dla upoważnionych użytkowników; ujawnienie poufnych informacji istotnych z punktu widzenia żywotnych interesu organizacji, wystosowanie wirtualnych komend lub poleceń prowadzących do awarii, w skutek których nastąpi fizyczne zniszczenie określonych urządzeń. Łatwo dostrzec, że konsekwencje przedstawionych działań mogą wchodzić w zakres pojęciowy zarówno cyberprzestępstw, jak i cyberterroryzmu[34].

Cyberataki najczęściej kierowane są na elementy infrastruktury krytycznej, takie jak: usługi finansowe, produkcja, telekomunikacja, przesył i zarządzanie energią elektryczną czy też sieci wodociągowe. Innym ważnym celem cyberataków są instytucje państwowe, szczególnie w obszarze sprawowania władzy, jak: Kancelaria Prezydenta, Urząd Rady Ministrów, parlament, biura poselskie, czy też instytucje zajmujące się bezpieczeństwem publicznym.

Dużym zagrożeniem są wirusy lub konie trojańskie, których przeznaczeniem – jednym z wielu – jest zainfekowanie komputera, aby był on dostępny dla przejęcia

[33] M. Voicescu, *Cyber terrorism and bioterrorism*..., s. 313–318.
[34] A. Dean, *Cyber Threats*..., s. 70–76.

i zdalnego sterowania. Do sytuacji takich dochodzi najczęściej w przypadku, jeśli użytkownik otworzy załącznik e-mail lub kliknie na podany link na stronie internetowej. Złośliwe oprogramowanie może skanować komputer ofiary w celu pozyskania poufnych informacji (np. data urodzenia, numery kont bankowych itp.), które następnie mogą być sprzedawane online lub wykorzystywane do produkcji fałszywych dokumentów tożsamości. Realizacja takiego zamierzenia stanowi duże ułatwienie dla wielu grup terrorystycznych, dla których docieranie do celu w niepostrzeżony sposób stanowi gwarancję np. przeprowadzenia zamachu.

Ponadto wewnętrzni pracownicy mogą uzyskać dostęp do poufnych danych o instytucji, w których pracują[35]. Sposoby rozpowszechniania złośliwego oprogramowania nie są ograniczone tylko i wyłącznie do sieci. Nośniki pamięci będące zarazem upominkiem rozdawanym na targach i konferencjach mogą okazać się również sposobem pozwalającym na dostęp do zabezpieczonych systemów. A zatem ominięcie systemu bezpieczeństwa jest możliwe z powodu nieuwagi, czasami złośliwości wynikających z frustracji zawodowej pracownika.

Duże znaczenie dla cyberbezpieczeństwa ma dynamicznie rozwijająca się działalność tzw. botnetów. Jest to sieć zainfekowanych komputerów kontrolowanych zdalnie przez atakującego. Botnety prowadzone przez przestępców mogą być wykorzystane przez terrorystów lub służby państwowe w celu zdobycia poufnych danych, pozyskania funduszy lub zakłócenia dostępu do krytycznej infrastruktury krajowej[36]. Tysiące takich komputerów może pracować równocześnie paraliżując pracę wybranych ofiar. Botnety, które specjalizują się w pozyskiwaniu danych są w stanie przechwytywać zawartość zaszyfrowanych stron i modyfikować je w czasie rzeczywistym.

Cyberatak nie jest odczuwany jednakowo we wszystkich dziedzinach. Mała firma może nie być w stanie przetrwać nawet jednego znaczącego ataku cybernetycznego. Z drugiej strony firmy często nie zdają sobie sprawy, że zostały ofiarami cyberprzestępców. W wielu przypadkach instytucje nie są w stanie odzyskać poniesionych strat, które również nie są możliwe do oszacowania. W trosce o własną reputację wiele firm woli nie ujawniać, że ich systemy zostały naruszone.

Przy analizie możliwości zaistnienia cyberataku trudno jest stwierdzić z pełnym przekonaniem, że infrastruktura krytyczna pozostanie nietknięta i zawsze będzie funkcjonalna w razie potrzeby. Prawdopodobnie przy wystarczających nakładach czasu, motywacji i środków, terrorysta bądź haker będzie prawdopodobnie w stanie przeniknąć każdy system, który jest dostępny bezpośrednio z Internetu.

---

[35] Ibidem.

[36] K.L. McLaughlin, *Cyber Attack! Is a Counter Attack Warranted?*, „Information Security Journal: A Global Perspective" 2011, vol. 20 (1), s. 58–64; T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2011, vol. 35(1), s. 5–32.

5.4. Cyberwywiad

Cyberszpiegostwo polega na wykorzystywaniu systemów komputerowych lub technologii informacyjnej do nielegalnego uzyskania poufnych informacje od rządu, sektora prywatnego lub innego podmiotu[37]. Cyberwywiad dotyczy przede wszystkim nieupoważnionych działań, takich jak: przeglądanie i kopiowanie danych, a także pozyskiwanie – poprzez bezprawne testowanie konfiguracji komputerów oraz mechanizmów obronnych systemu – informacji na temat technologii i zabezpieczeń instytucji docelowej.

Służby wywiadowcze są szczególnie zainteresowane informacjami odnoszącymi się po pierwsze do technologii, w tym także wojskowych po drugie do informacji na temat treści związanych ze strategią rozwoju i po trzecie do prowadzonych negocjacji oraz zawieranych umów dotyczących działalności gospodarczej. Rząd Stanów Zjednoczonych szacuje, że ponad sto organizacji pracujących na rzecz obcego wywiadu regularnie próbuje się włamać do systemów komputerowych administracji rządowej oraz firm amerykańskich. Większość ataków cybernetycznych kierowanych na infrastrukturę USA prawdopodobnie pochodzi z strony Chin[38].

Zagrożenia cybernetyczne mają szczególne znaczenie dla władz Kremla. Rosyjski rząd, w tym jego wojsko, rozwija systemy wywiadowcze w celu poprawy ich ofensywnych i defensywnych cybermożliwości. Rosja prowadzi szereg działań, w tym gromadzenie informacji gospodarczych i technologicznych na temat państw zachodnich.

Również Chiny próbują pozyskać informacje z zakresu polityki, handlu i bezpieczeństwa. Głównymi sprawcami tych czynności jest Departament Trzeci Armii Ludowo-Wyzwoleńczej. Wysoce prawdopodobna jest teza, że w innych częściach globu, a nawet wobec własnego sektora prywatnego mogą być przeprowadzanie podobne działania. Można także przypuszczać, że informacje dotyczące konkretnej technologii, którą Chiny zamierzają rozwijać lub realizować są i będą centralnym punktem zainteresowania służb wywiadowczych tego państwa. Chińscy hakerzy kierują swoje działania w różne sektory przemysłu zachodnich państw, w tym elektroniki, telekomunikacji, energetyki, lotnictwa i obrony. Prawdopodobne odbiorcami skradzionych danych handlowych są chińskie przedsiębiorstwa państwowe, które dominują w chińskiej gospodarce[39].

Rządy wielu państw znacznie poszerzyły liczbę personelu służb wywiadowczych oraz przeprowadzanych przez nich operacji, które są bezpośrednim następstwem zamachów z 11 września. Pomimo jednak wzrostu liczby agencji wywiadowczych oraz

[37] A. Dean, *Cyber Threats...,* s. 70–76.
[38] Ibidem.
[39] Ibidem.

osiągnięć technologicznych i wzrostu budżetu głównym problemem wywiadu jest niewystarczająca liczba analityków[40]. Okazuje się bowiem, że służby wywiadowcze bardzo dobrze radzą sobie z wypełnianiem jednego z głównych swoich obowiązków, jakim jest pozyskiwanie informacji. Jednak drugim zadaniem – równie trudnym i ważnym – jest ich właściwa analiza, polegająca m.in. na interpretacji, scalaniu i weryfikacji danych. Innymi słowy służby pozyskują więcej informacji niż są w stanie przyswoić i zanalizować.

5.5. Cyberwojna

W obszarze prowadzonego cyberkonfliktu obie walczące ze sobą strony wykorzystują informacje za pomocą środków technologicznych z urządzeń lub systemów w celu uzyskania przewagi nad przeciwnikiem. Walka opiera się na trzech zasadach odnoszących się po pierwsze do poziomu wywiadu, czyli pozyskiwania i gromadzenia informacji; po drugie do elementu cybermilitarnego dotyczącego przeprowadzania ataków i po trzecie kontrwywiadowczego, polegającego na zapewnieniu ochrony dla własnych zasobów informacyjnych oraz innych aktywów.

Pod pewnymi względami konsekwencje cyberwojny mogą być analogiczne, jak w przypadku prowadzenia konwencjonalnej w wojny. Jednak zauważyć należy, że w przypadku – znanych już opinii publicznej – cyberataków, które miały miejsce np. w Kirgistanie w styczniu 2009 roku, czy też w Estonii na przełomie kwietnia i maja 2007 roku, trudno jest do końca zidentyfikować, który podmiot (państwo, organizacja, osoba) jest odpowiedzialna za atak.

Zdolność krajów do określenia źródła cyberataku, może prowadzić do odwetu zarówno w cyberprzestrzeni, jak i w tradycyjnym znaczeniu. Odwet może być zinterpretowany jako samoobrona, jeśli jest ona proporcjonalna i dokonana z konieczności.

Wiosną 2007 roku, praca rządowych systemów komputerowych w Estonii została zakłócona poprzez liczne ataki cybernetyczne. Ataki – jak początkowo sądzono – zostały zaaranżowane przez rosyjskie grupy przestępcze i prawdopodobnie za wiedzą władz Kremla. Botnety zostały wykorzystane do przeciążenia estońskich stron internetowych, w wyniku czego ofiarą padły m.in. systemy rządowe, kanały medialne czy też serwery bankowe.

Podobna sytuacja wystąpiła w czerwcu 2008 roku na Litwie, której rząd stanął w obliczu cyberataków, a które były odpowiedzią na uchwaloną przez parlament – trzy dni wcześniej – ustawę zakazującą używania symboli komunistycznych. W wyniku decyzji władz litewskich ponad trzysta stron internetowych zostało zaatakowanych.

[40] M.M. Aid, *Intel wars: The secret history of the fight against terror*, Nowy Jork 2012, s. 214.

W dniu 20 lipca 2008 roku strona internetowa Prezydenta Gruzji została unieruchomiona w wyniku ataku *Denial of Cyber Service* (DOCS). W dniu 8 sierpnia 2008 roku, doszło ponownie do skoordynowanego cyberataku na gruzińskie strony rządowe, w tym samym czasie, kiedy siły rosyjskie były zaangażowane w walkę z siłami gruzińskimi. Konflikt ten uważany jest za pierwszy tego typu, w którym przeprowadzone były równocześnie działania zbrojne przy użyciu środków konwencjonalnych, jak i cybernetycznych.

W dniu 18 stycznia 2009 roku, dwa główne serwery internetowe w Kirgistanie zostały sparaliżowane przy użyciu ataków typu DDoS. Ataki miały miejsce w tym samym dniu, kiedy to strona rosyjska naciskała rząd w Kirgistaie, aby ten zamknął dostęp do bazy lotniczej w Manas w Biszkeku dla sił wojskowych USA. Podsumowując, można zauważyć, że prawie każdy konflikt polityczny i wojskowy w obecnych czasach ma swój odpowiednik w cyberprzestrzeni.

6. Cyberpropaganda

Zagrożenie stwarzane przez cyberterroryzm polega na wzbudzaniu strachu, poprzez stymulowanie określonych emocji wykorzystując do tego celu nowoczesne technologie informacyjne. Ważny jest także zawarty w komunikatach propagandowych określony przekaz składającego się z kodów kulturowych, odwołujących się do estetyki popkultury, dzięki czemu dokonuje się wzmocnienia tradycyjnego wsparcia dla działalności terrorystycznej.

Cyberterroryści wykorzystują efekt globalizacji i możliwości nowoczesnej technologii do planowania, koordynowania i realizacji swych kampanii. Są oni szczególnie sprawni w użyciu serwisów społecznościowych, takich jak Facebook i Twitter, które pozwalają im z jednej strony zbierać informację, a z drugiej promować i rozpowszechniać swój przekaz niemal bez ograniczeń. Ponieważ celem terrorystów jest generowanie rozgłosu i zwrócenie uwagi na ich przyczyny, Internet stanowi więc wygodne narzędzie pozwalające na ominięcie cenzury i udostępnianie niefiltrowanych wersji transmitowanych wydarzeń na całym świecie. Nie dziwi więc fakt, że terroryści wykorzystują Internet do realizacji swoich celów[41].

Przykładem są artykuły w magazynie „Inspire", instruujące jak zbudować bombę przy wykorzystaniu dostępnych środków w domu lub w którym miejscu najlepiej podłożyć i zdetonować ładunek, aby spowodować jak najwięcej szkód. Dzięki Internetowi nie ma już potrzeby podróży do Afganistanu na szkolenie terrorystyczne.

[41] G. Weimann, *Cyberterrorism. How Real Is the Threat?*, „Special Report" 2014, vol. 119, s. 1–12.

Wszystkie przykłady z zakresu działań terrorystycznych mogą być czytane i oglądane przez każdego z laptopem podłączonym do Internetu. Podsumowując cyberprzestrzeń jest przydatna dla terrorystów, ponieważ za jej pomocą można komunikować się z publicznością, znaleźć potencjalnych rekrutów wśród swoich zwolenników i uruchomić kampanie psychologiczną[42].

Reasumując, okazuje się zatem, że Internet jest potężnym narzędziem do rozprzestrzeniania ideologii oraz prowadzenia rekrutacji. Na przykład w Iraku, powstańcy wykorzystywali cyberprzestrzeń, nie tylko aby koordynować ataki na siły zbrojne, ale filmowali zamachy, po czym udostępniali materiały w celu propagowania własnych sukcesów[43]. Tak tworzony przekaz w cyberprzestrzeni wzmacniał i jeszcze bardziej radykalizował grupy o skrajnych przekonaniach. Internet okazał się więc doskonałym narzędziem komunikacji i indoktrynacji.

Pomimo tego że dokonywane są wysiłki w celu likwidowania bądź marginalizowania tego typu stron, to nadal pojawiają się nowe witryny moderowane przez organizacje terrorystyczne. Dopiero od niedawna służby wywiadowcze rozpoczęły monitorowanie tego typu miejsc w cyberprzestrzeni, obawiając się że mogą one przyczynić się do rozwoju działalności terrorystycznej[44]. Istnieje również opinia, iż w interesie bezpieczeństwa publicznego jest to, aby nie zakłócać tego typu komunikatów i stron internetowych, ponieważ pozwalają one zbierać i gromadzić informacje wywiadowcze[45]. Jednak monitorowanie Internetu jest trudnym zadaniem z uwagi na ogromną liczbę stron internetowych oraz dynamiczny proces rozpowszechniania informacji.

7. Wolność *vs* bezpieczeństwo

Cyberataki są tanie i łatwo je realizować, ale koszt dla ich ofiar jest ogromny, bowiem ich konsekwencje mogą być wycenione na setki milionów dolarów, wliczając dodatkowo reputację instytucji lub organizacji, utratę zaufania obywateli bądź klientów oraz zwiększoną kontrolę i nadzór nad społeczeństwem, który stoi często w sprzeczności z takimi wartościami, jak wolność i prywatność.

[42] Najbardziej bezpośrednim zagrożeniem jest niezliczona liczba stron internetowych propagujących terroryzm. Oprócz propagandowego przekazu zawierają one także materiały szkoleniowe dotyczące np. właściwego działania broń, budowy urządzeń wybuchowych oraz sposobów na zmaksymalizowanie jej skuteczności. Co najważniejsze, strony te mogą edukować terrorystę, w jaki sposób zaplanować i przeprowadzić ataki na cele zarówno wojskowe jak i cywilne, za: Y. Lappin, *Virtual Caliphate*..., s. 47–53.

[43] Ch. Pedersen, *Much Ado about Cyber-space*..., s. C1–C21.

[44] Ibidem.

[45] J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack*..., s. 17.

Ochrona przed terrorystami bądź cyberterrorystami rodzi problemy etyczne, bowiem pojawia się pytanie jak daleko może posunąć się rząd oraz podległe mu służby, aby zapewnić bezpieczeństwo swym obywatelom z jednoczesną troską o nienaruszanie swobód osobistych. Współcześnie prawie wszystkie kraje w dużym stopniu opierają się na technologii informatycznej, która jest częścią komfortu życia współczesnego człowieka. Być może współczesne społeczeństwo stoi przed wyzwaniem polegającym na przystosowaniu się do życia z możliwością zaistnienia zamachu terrorystycznego. Dlatego rządy muszą znaleźć kompromis godzący ze sobą dwie sprzeczne wartości, jakimi są bezpieczeństwo i wolność. Warto również zauważyć, że metody zwalczania grup terrorystycznych oraz eliminacja tworzonych przez nich zagrożeń wzbudza wiele kontrowersji, co może prowadzić do eskalacji przemocy i konfliktu w społeczeństwie, a pośrednio prowadzić do hamowania zdolności do skutecznego zapobiegania atakom terrorystycznym.

Zakończenie

Analiza cyberterroryzmu polega na zrozumieniu jego możliwości uderzenia w każdy cel bez względu na położenia geograficzne. W przypadku przeprowadzenia cyberataków pierwszymi celami są komputery i sieci, jednak ostatecznymi ofiarami takich działań są zawsze ludzie.

Każdy atak cybernetyczny może doprowadzić do zakłóceń w pracy i funkcjonalności technologii komputerowej. W przypadku takiej sytuacji najbardziej narażone na cyberataki są systemy komputerowe obsługujące infrastrukturę krytyczną czy też finansową. W tym kontekście kluczową rolę odgrywa bezpieczeństwo zakładów energetycznych oraz elektrowni jądrowych, które mogą być podatne na ataki cybernetyczne. Ważnym aspektem bezpieczeństwa jest również kontrola ruchu lotniczego czy też kolejowego.

Dla wielu państw rewolucja technologiczna zmieniła sposób działalności rządu, jak również codzienne życie obywateli. Asymetryczne zagrożenia stwarzane przez m.in. ataki terrorystyczne oraz nieodłączna słabości cyberprzestrzeni stanowią obecnie poważne zagrożenie dla bezpieczeństwa państwa. W ostatnich latach ataki na infrastrukturę krytyczną oraz systemy informatyczne stają się coraz częstsze i skomplikowane, gdyż terroryści oraz przestępcy stają się coraz bardziej profesjonalni. Zagrożenia w cyberprzestrzeni są trudne do określenia ze względu na dynamiczny rozwój technologii. Podobnie trudno jest zidentyfikować źródła ataków i ludzkie motywy, które są ich główną przyczyną, a nawet trudno jest przewidzieć dalszy scenariusz cyberataku wraz z jego konsekwencjami.

Bibliografia

Aid M. M., *Intel wars: The secret history of the fight against terror*, Nowy Jork 2012.

Alqahtani A., *The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia*, „International Conference on Information Warfare and Security" 2013.

Ayres N., Maglaras L. A., Cyberterrorism targeting the general public through social media, „Security and Communication Networks" 2016, vol. 9 (15).

Carr J., *Inside Cyber Warfare, 2nd Edition Mapping the Cyber Underworld*, Publisher: O'Reilly Media 2011.

Dean A., *Cyber Threats in the 21st Century*, „Security" 2012, vol. 49 (9).

Denning D., *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militacy*, red. J. Arquilla, D. Ronfeldt 2001.

Denning D., *Cyberterrorism, Prepared for Estimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, http://www.cs.georgetown.edu/~denning/infosec/cvberterror.html.

Gorge M., *Cyberterrorism: Hype or Reality?,* „Computer Fraud & Security" 2007, vol. 2.

Jarvis L., Macdonald S., Nouri L., *The Cyberterrorism Threat: Findings from a Survey of Researchers*, „Studies in Conflict & Terrorism" 2014, vol. 37 (1).

Kontselidze A., Cyberterrorism – when technology became a weapon, „European Scientific Journal" 2015.

Lappin Y., *Virtual Caliphate*, Waszyngton 2011.

Matusitz J., *Cyberterrorism: Postmodern State of Chaos*, „Information Security Journal: A Global Perspective" 2008, vol. 17 (4).

McLaughlin K.L., *Cyber Attack! Is a Counter Attack Warranted?*, „Information Security Journal: A Global Perspective" 2011, vol. 20 (1).

Negroponte J. D., Palmisano S.J., Segal A., *Defending an Open, Global, Secure, and Resilient Internet*, Nowy Jork 2013.

Pedersen Ch., *Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security*, „Pepperdine Policy Review" 2014, vol. 7 (1).

Regan T., *When terrorists turn to the Internet Seemingly unconnected events may have a more sinister source: Series*, „The Christian Science Monitor", 1.07.1999.

Rid T., *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2011, vol. 35 (1).

Rollins J., Wilson C., *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, „CRS Report for Congress", 22.01.2007.

Topor S., *Cyber criminal and cyber terrorist – two concepts that need to be differently treated*, International Scientific Conference „Strategies XXI" 2016, vol. 3.

Webster W., Cilluffo F., *Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo*, Waszyngton 1998.

Weimann G., *Cyberterrorism. How Real Is the Threat?*, „Special Report" 2014, vol. 119.

Voicescu M., *Cyber terrorism and bioterrorism – new forms of terrorists action. size, effects and countermeasures*, International Scientific Conference „Strategies XXI" 2012, vol. 3.