

ROZDZIAŁ XVIII

Ireneusz Fura

Centrum Szkolenia Łączności i Informatyki w Zegrzu

WSPÓŁCZESNE NIEBEZPIECZEŃSTWO XXI WIEKU JAKIM JEST CYBERTERRORYZM

Wstęp

Koniec XX i początek XXI wieku to okres gwałtownego rozwoju nowych technologii informatycznych, komputerów i Internetu. Niekontrolowany rozwój tego medium, a także znaczny stopień „usieciowienia” współczesnych społeczeństw sprawił, że pojawiły się nowe, dotychczas niespotykane zagrożenia, które w znaczący sposób mogą zagrozić krytycznej infrastrukturze państwa. Najdobitniejszym tego przykładem były wydarzenia w Estonii, która w maju 2007 roku musiała zmierzyć się ze zmasowanymi cyberatakami, będącymi odwetem za przeniesienie pomnika Żołnierzy Armii Czerwonej z centrum Tallina na podmiejski cmentarz wojskowy. Biorąc pod uwagę znaczenie technologii informatycznych we współczesnym świecie oraz realną groźbę wykorzystania ich przeciwko bezpieczeństwu państwa zachodzi potrzeba znalezienia odpowiedzi na pytanie, w jakim stopniu Polska jest narażona na zagrożenia płynące z globalnej sieci oraz czy zaistniała potrzeba wypracowania kompleksowej i efektywnej strategii obrony przed cyberterroryzmem? **Cyberterroryzm** to określenie pewnego rodzaju przestępstw, dokonywanych w wirtualnym świecie Internetu, mających jednak realne odniesienie w życiu i bezpieczeństwie obywateli różnych krajów świata. Cyberprzestępstwa mogą polegać np. na wykorzystywaniu globalnej sieci do kontaktów między sobą różnych komórek terrorystycznych w celu planowania ataków zbrojnych, itp. Komputery i sieć Internet stały się nieodłączną częścią naszego życia codziennego. Używane przez jednostki, jak i całe społeczeństwa służą automatyzowaniu, przyspieszaniu wykonywanych przez nas czynności. Sprawne działanie prawie wszystkich dziedzin gospodarki, a w szczególności energetyki, transportu, komunikacji, sfery bankowości, sieci komputerowych, jest ściśle zależne od przepustowości, sprawności i niezawodności tych technologii⁵⁵. Uszkodzenie któregośkolwiek elementu mogłoby spowodować paraliż całego kraju.

⁵⁵Z. Ciekanowski, S. Wojciechowska-Filipek, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni Jednostki – Organizacji – Państwa*, CeDeWu, Warszawa 2016, s. 152.

W przeszłości bezpośredni atak na infrastrukturę był możliwy tylko w sposób bezpośredni. Wraz z rozwojem sieci telekomunikacyjnych pojawiło się nowe niebezpieczeństwo, „cyberzagrożenie”. Już nie trzeba przekraczać granic politycznych by dokonać ataku terrorystycznego. Co więcej, wykrycie ataku z zastosowaniem technologii informatycznych na etapie planowania i przygotowywania jest całkowicie niemożliwe. Sam atak cyberterrorystyczny można przeprowadzić w ciągu minut lub sekund, a jego skutki mogą być o wiele poważniejsze niż przy zastosowaniu konwencjonalnej broni. Dostrzegając te niebezpieczeństwa należy zdefiniować i ocenić zagrożenia płynące z wykorzystania sieci telekomunikacyjnych i komputerów przeciwko jakiemuś narodowi lub rządowi z przyczyn politycznych lub ideologicznych.

1. Ataki cyberterrorystyczne

Cyberterroryzm nie jest zjawiskiem nowym. Sam termin pojawił się już w 1979 roku, kiedy to szwedzkie Ministerstwo Obrony umieściło go w swoim raporcie o zagrożeniach komputerowych, rekomendując by rząd zaangażował się w monitorowanie zarówno publicznych, jak i prywatnych sieci komputerowych. Na początku lat dziewięćdziesiątych przestrzeń cybernetyczną (Cyberspace), jako piąty model wojny, wyróżniono w popularnym „modelu Wardena”. Do arsenału środków walki włączono m.in. wirusy komputerowe, robaki, konie trojańskie, impulsy elektromagnetyczne służące zniszczeniu sieci i komputerów przeciwnika, czy strumienie danych o dużym natężeniu powodujące ich krótkotrwałe lub długotrwałe blokowanie. Nie ma jednej, powszechnie przyjętej definicji cyberterroryzmu. Specjaliści z Akademii Obrony Narodowej w „Analizie systemowej zjawiska cyberterroryzmu” definiują go, jako: „politycznie motywowany atak lub groźbę ataku na komputery, sieci, lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów”⁵⁶. Podobne definicje znajdziemy w dokumentach amerykańskiego Departamentu Stanu, czy FBI. Dorothy E. Denning, profesor amerykańskiego Uniwersytetu Georgetown zajmująca się naukowo problemami bezpieczeństwa przestrzeni informatycznej, zwraca szczególną uwagę na wymiar i skalę ataków. By zakwalifikować konkretny atak w cyberprzestrzeni za cyberterroryzm, musi on „skutkować przemocą w stosunku do ludzi lub własności, lub przynajmniej powodować strach.” Najlepszymi przykładami, według Denning, mogą być takie ataki z wykorzystaniem sieci teleinformatycznych, które w swoich skutkach prowadzą „do śmierci, okaleczenia ciała, eksplozji, rozbicia się sa-

⁵⁶J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013, s. 131.

molotów, zanieczyszczenia wody lub drastycznych strat ekonomicznych.” Poważne ataki na infrastrukturę mogą być zakwalifikowane, jako akty cyberterroryzmu w zależności od ich skali. Wszystkie definicje mają jeden element wspólny – o cyberterroryzmie możemy mówić jedynie wtedy, kiedy mamy do czynienia z politycznie motywowanym atakiem z użyciem sieci teleinformatycznych. W pozostałych przypadkach takie ataki klasyfikuje się zazwyczaj, jako cyberprzestępstwa nie mające podtekstu politycznego. Nie można również łączyć cyberterroryzmu z tzw. hacktivismem (połączenie słów hacker i activism). Pojęcie to używane jest do określania działań o charakterze hackerskim celem osłabienia normalnego funkcjonowania systemów informatycznych, połączonych z propagandą i wyrażaniem opinii o charakterze politycznym. Działania te, w odróżnieniu od cyberterroryzmu, nie powodują większych zniszczeń w infrastrukturze istniejącej poza cyberprzestrzeni.

Nie mamy wątpliwości, że współczesność staje się coraz bardziej skomplikowana, mniej przejrzysta i trudniejsza do przyswojenia. Neurastenia współczesnych zachowań społecznych jest pochodną niemożności zrozumienia przez człowieka wszystkich procesów i zjawisk zachodzących w jego otoczeniu. Naturalne poznanie świata, wcześniej ograniczane brakiem informacji, aktualnie zostało utrudnione przez nadmiar danych o skrajnie zróżnicowanym poziomie istotności. Mówi się już o szumie, a nawet smogu informacyjnym, przyznając coraz wyraźniej, że selekcja wiedzy będzie jedną z najtrudniejszych umiejętności ery informacyjnej. Jeśli prawdą są doniesienia o wykorzystaniu przez przeciętnego człowieka zaledwie 1/3 możliwości percepcyjnych mózgu, to tym bardziej frustrująca staje się ta wiadomość w kontekście uświadamiania sobie, że mózg ten ma ograniczoną wydolność, której – w przeciwieństwie do komputera – nie można zwiększyć rozszerzeniem parametrów twardego dysku czy szybszego procesora. Bezsprzecznie frustrujemy się tym jako członkowie społeczeństwa i jako badacze. Warto zadać sobie pytanie, czy ten szybko zmieniający się świat, niosący ze sobą nowe zagrożenia dla funkcjonowania społeczeństwa, jest materiałem analitycznym dla politologów, czy może raczej dla socjologów, informatyków lub prawników? Globalizacja przytłoczyła badaczy z wielu dziedzin swym wszechobecnym charakterem, zmusiła humanistów do przyznania, że nauki ścisłe są dla nich co najmniej pomocne, a może nawet nieodzowne w procesie badawczym. Wydobyła i wyostrzyła zjawisko poznawczego synkretyzmu, skutkiem którego nie sposób już odpowiedzialnie rozdzielać tradycyjnie rozumianych dyscyplin naukowych.

Terrorysty poszukują popularności i dążą do uzyskania korzystnych dla nich zmian politycznych poprzez wprowadzanie zamieszania, rozległych zniszczeń lub stanu realnego zagrożenia motywowanego ideologią

lub poglądami⁵⁷. Terrorysty najczęściej uciekają się do brutalnych ataków destrukcyjnych, bardzo dokuczliwych i dobrze widocznych dla społeczeństwa. Aczkolwiek eksperci uważają, że ataki na systemy teleinformatyczne nie zastąpią bardziej efektywnych fizycznych akcji terrorystycznych, ataki te mogą być prowadzone jako „wspomagające” dla uzyskania wyższej skuteczności typowej akcji terrorystycznej, poprzez utrudnienie działań ratowniczych i koordynowania reakcji na atak fizyczny. Dodatkowo ataki na sieci i systemy teleinformatyczne mogą obezwładnić niektóre środki ochrony fizycznej, co również może pogłębić skutki ataku. Bezpośrednio po ataku fizycznym terroryści mogą też atakować systemy teleinformatyczne w celu zdobycia informacji o planowanych i wdrażanych działaniach antyterrorystycznych, co pozwoliłoby im pokrzyżować plany takiej akcji.

Grupy terrorystyczne mogą stanowić niewielkie, kilkusobowe zespoły amatorów (lub nawet pojedyncze osoby), aż do dużych struktur quasi-militarnych doskonale wyszkolonych i wyposażonych. Znane są przypadki sponsorowania takich grup oraz szkolenia i wyposażania ich zarówno przez sekty i grupy wyznaniowe, jak i niektóre państwa nazywane obecnie „bandyckimi”.

Systemy teleinformatyczne nie stanowią jednak szczególnie atrakcyjnego celu dla terrorystów w porównaniu z obiektami tradycyjnych ataków. Mogą natomiast stanowić cel pośredni lub wspomagający. Dotyczy to szczególnie systemów słabo zabezpieczonych, możliwych do „złamania” bez większych nakładów sił i środków.

Typowe umiejętności techniczne terrorystów sprowadzają się zasadniczo do możliwości produkowania różnorodnych bomb, itp. oraz organizowania i prowadzenia fizycznych operacji – ataków.

Jednakże niektóre grupy terrorystyczne dysponują sporymi środkami finansowymi pochodzącymi m.in. z produkcji pirackiego oprogramowania, hackerstwa i nielegalnej produkcji np. skanerów i dekoderek TV. A więc dysponują znaczącymi umiejętnościami technicznymi. Wielu studentów wybitnych technicznych uczelni europejskich i amerykańskich wraca do swoich macierzystych krajów stanowiąc potencjalne źródło specjalistycznej wiedzy i umiejętności dla prowadzenia cyberterroryzmu. Podobnie jak większość innych organizacji przestępczych, stosują bez skrupułów i z powodzeniem podsłuchy linii telekomunikacyjnych, transmisji internetowych itp. Grupy terrorystyczne wykorzystują również w swojej działalności najnowsze zdobycze w dziedzinie systemów łączności i informatyki – np. telefonię komórkową (wraz z WAP) i technologie szyfrowania. Stosują również broadcasting poprzez Internet, TV i inne powszechnie dostępne techniczne środki rozpowszechniania typowo propagandowych informacji⁵⁸.

⁵⁷Z. Ciekanowski, *Cyberterroryzm*, [w:] *Zabić tysiące przestraszyć miliony*, WSiP, Warszawa 2009, s. 154.

⁵⁸Z. Ciekanowski, S. Wojciechowska-Filipek, op. cit., s. 192.

Do najważniejszych metod ataków cyberterrorystycznych należą:

- social engineering (wykorzystywanie niekompetencji osób, które mają dostęp do systemu);
- bugs and backdoors (korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł: komputerowe wirusy, robaki i bakterie);
- authentication failuers (zniszczenie mechanizmu autoryzacji);
- protocol failures (wykorzystywanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi procesorami);
- information leakage (zdobywanie informacji dostępnych tylko dla administratora, niezbędnych do funkcjonowania sieci);
- bomby logiczne (uruchamiające dodatkowe funkcje elementu logicznego komputera i zakłócające tym samym jego działanie);
- stealing passwords (metody polegające na uzyskaniu dostępu do sieci);
- konie trojańskie (programy wykonujące działania niezależnie od woli użytkownika);
- chip ping (uzyskiwanie dostępu przez doinstalowanie dodatkowych chipów);
- „tylne drzwi” (wejście do systemu z ominięciem jego warstwy ochronnej);
- spoofing (podszywanie się);
- hijacking (przechwytywanie transmisji między dwoma systemami);
- sniffing (śledzenie ruchów w sieci);
- receptor van Eycka (podglądanie efektu wysyłania przez monitor silnego sygnału elektronicznego);
- DOS (Denial of Service, odmowa usługi – blokowanie pojedynczej usługi sieciowej bądź blokowanie pracy całego serwera, czasem przez przeciążenie go za pomocą niezliczonej ilości pytań);
- E-mail bombing (wysyłanie tysięcy wiadomości e-mail w celu blokowania działania poczty elektronicznej);
- Broń częstotliwości radiowej (radio frequency, RF – urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego, używane do niszczenia technicznych urządzeń elektronicznych oraz zbiorów informatycznych);
- Flooding (wysyłanie do atakowanego komputera takiej ilości żądań, której nie jest on w stanie obsłużyć);
- Spamming (natarczywe i nieukierunkowane przesyłanie pocztą elektroniczną niezamówionych ofert handlowych)⁵⁹.

⁵⁹K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Wydawnictwo Trio Collegium Civitas, Warszawa 2008, s. 46.

Omawiając wszystkie zagadnienia związane z cyberterroryzmem i zagrożeniem, jakim jest on dla bezpieczeństwa informacyjnego, trzeba podkreślić z całą mocą: sieć komputerowa jest w dzisiejszej epoce siecią nerwową kraju. W krajach szeroko pojmowanego Zachodu, niezakłócone działanie cyberprzestrzeni jest podstawą niezakłóconego funkcjonowania gospodarki, ale także bezpieczeństwa kraju⁶⁰.

Należy zwrócić w tym miejscu szczególną uwagę na zagrożenie, jakim jest najgroźniejsza postać cyberterroryzmu tzw. swarming attack oraz trzeba sobie uświadomić skalę niebezpieczeństwa spowodowanego jej zastosowaniem. To metoda polegająca na generowaniu i nałożeniu na siebie ataków przeciwko infrastrukturze krytycznej państwa prowadzonych w cyberprzestrzeni. W związku z atakiem w cyberprzestrzeni zakłóceniu ulega przede wszystkim działanie materialnych elementów infrastruktury krytycznej państwa obrazowym przykładem takich działań i ich skutków jest atak na budynek mieszczący istotny węzeł internetowy i zespół routerów, co może spowodować skuteczne załamanie komunikacji internetowej odczuwalne w skali regionu bądź nawet kraju.

Palącą kwestią cyberprzemocy zajęła się również Międzynarodowa Organizacja Policji Kryminalnej Interpol, która podzieliła przestępczość komputerową na:

- naruszenia praw dostępu do zasobów,
- oszustwa przy użyciu komputera,
- powielanie programów,
- sabotaż sprzętu i oprogramowania,
- przechowywanie zabronionych prawem zbiorów,
- przestępstwa popełnione w sieci⁶¹.

Skuteczna walka z cyberterroryzmem ma również inne, bardziej mroczne oblicze. Jest nim dobrowolne zrzeczenie się niektórych praw i wolności osiągniętych lub wywalczonych w procesie ewolucji społeczeństw i systemów politycznych. Mam tu na myśli wyrażenie zgody na większą formę inwigilacji obywateli przez państwo.

Wszyscy zdajemy sobie sprawę z faktu, że świat po 11 września zmienił się niewyobrażalnie i to niestety w ciągu jednej chwili. W związku z tym, międzynarodowy terroryzm musi napotkać globalną konsolidację współpracy, mającą na celu minimalizację skutków jego oddziaływania. Ogólnosiwiatowe działania antyterrorystyczne osiągnęły niespotykane wcześniej rozmiary, niestety w myśl maksymy, że cel uświęca środki. Nie jest to może najidealniejsze rozwiązanie, ale czy jest lepsze?

Sceptycy uznają, że zagrożenie cyberterrorystyczne jest bardziej wymysłem literatury fantastyczno-naukowej niż realną groźbą dla współczesne-

⁶⁰Tamże, s. 76.

⁶¹Tamże, s. 46.

go świata. Będą mówić – nie bez pewnej racji – o tym, że podobne przewidywania były już często formułowane, a jednak nie doszło do żadnego ataku cyberterrorystycznego na dużą skalę. Warto się jednak zastanowić, czy brak „osiągnięć” terrorystów w wykorzystaniu globalnej sieci do własnych celów jest dowodem na to, że znajduje się ona poza ich obszarem zainteresowania? Czy osoby wskazujące na cyberterroryzm, jako realne zagrożenie dla bezpieczeństwa narodowego i międzynarodowego wkładają tylko swoją cegiełkę do „histerii terrorystycznej”, jaka ma miejsce po 11 września 2001 roku. A może jednak cyberterroryzm w niedługim czasie ma szansę stać się jednym z największych wyzwań współczesnego świata?

Paul Levinson zwraca uwagę – oddając jednocześnie hołd Marshallowi McLuhanowi - że dopiero teraz, w dobie Internetu, możemy mówić o powstaniu pierwszej globalnej wioski, „społeczeństwa on-line”. Szybki rozwój technologii informatycznych sprawia, że państwa wysokorozwinięte stają się jeszcze bogatsze, a dystans między Północą i Południem jeszcze się pogłębia. Paradoksalnie jednak wzrasta zagrożenie atakiem cyberterrorystycznym. W dobie, gdy informacja jest towarem najcenniejszym, wyższy poziom bezpieczeństwa osiągają gospodarki państw mało osieciowanych, nie związane z systemem globalnej sieci. Natomiast uderzenie na kraje Europy Zachodniej, Stany Zjednoczone czy Japonię może doprowadzić do paraliżu całego sektora infrastruktury krytycznej.

2. Cyberterroryzm a Polska

Polska dopiero staje przed trudnym zadaniem budowy społeczeństwa informacyjnego. Liczba naszych rodaków poruszających się po sieci nie jest powodem do dumy i mamy wiele do nadrobienia także na tym polu, w porównaniu do państw Unii Europejskiej. Internet przestał być już jednak traktowany jako ciekawostka, sprzed byłego Centrum Informacyjnego Uniwersytetu Warszawskiego zniknęły długie kolejki, natomiast coraz częściej słysząc o nowych pomysłach związanych z wykorzystaniem globalnej sieci: podpis elektroniczny, głosowanie przez Internet, polska biblioteka internetowa, e-government, e-commerce, wiele, wiele innych. Wszystko to sprawia, że z wolna skracamy dystans dzielący nas od państw najbardziej osieciowanych. Zagrożenie cyberterrorystyczne jest jednak nadal postrzegane w kategoriach fantastyczno-naukowych, co implikuje potrzebę stworzenia kampanii medialnej o bezpieczeństwie informacyjnym.

Mimo, że Polska nie jest z informatyzowana w tak dużym stopniu jak inne państwa zachodnie, należy zakładać, że może ona w najbliższej dekadzie stać się celem cyberataków. Dlaczego?

Po pierwsze, procent użytkowników Internetu w polskim społeczeństwie stale wzrasta. W latach 2000-2008 wzrost użytkowników wyniósł

4,2%. Według danych Internet World Status w Polsce zarejestrowanych jest około 16 milionów użytkowników, co stanowi 41,6% całej populacji. Polska sytuuje się w pierwszej dziesiątce krajów o największej liczbie użytkowników Internetu zaraz po Niemczech, Wielkiej Brytanii, Francji, Włoszech i Hiszpanii. Należy zakładać, że „usieciowienie” Polski będzie wzrastać również w następnych latach.

Po drugie, znaczny odsetek Polaków korzysta już np. z możliwości obsługi kont bankowych, telefonów komórkowych przez internet. Praktycznie każdy bank w Polsce oferuje dostęp do swoich usług za pomocą komputera. Według raportu Rady Bankowości Elektronicznej przy Związku Banków Polskich liczba klientów korzystających z tego typu usług przekroczyła już 11 milionów, z czego 6,4 miliona to klienci aktywni (dokonali co najmniej 4 transakcje płatnicze). Rada prognozuje wzrost liczebności tej grupy do 10 milionów w 2010 roku.

Po trzecie, krytyczna infrastruktura techniczna Polski (administracja rządowa, służby, wojsko, transport, energetyka) jest już w znacznym, chociaż nadal odbiegającym od standardów światowych, stopniu zinformatywowana. „Usieciowieniu” Polski ma sprzyjać opracowana przez MSWiA *Strategia rozwoju społeczeństwa informacyjnego w Polsce do 2013 roku*.

Po czwarte, Polska jako uczestnik operacji stabilizacyjnych w Iraku, czy Afganistanie jest „na celowniku” grup terrorystycznych, które mogą zastosować wobec niej atak cybernetyczny. Prawdopodobieństwo to jest na tyle wysokie, że grupy takie jak Al-Kaida zrozumiały użyteczność stosowania cyberbroni w działaniach zmierzających do osiągnięcia swoich celów⁶².

Po piąte, relacje Polski z Rosją nie układały się w ostatnim czasie najlepiej. Rosja jest jednym z głównych krajów podejrzewanych o wzmożone zainteresowanie i używanie cyberszpiegostwa i cyberterroryzmu. Dotyczy to zarówno służb specjalnych, jak i prywatnych hackerów. Można zakładać, że w razie pogorszenia stosunków między oboma państwami może dojść do prób ataku przez sieci informatyczne na polską infrastrukturę tak, jak miało to miejsce w przypadku Estonii.

Po szóste, Polska – jak każdy inny kraj – jest narażona na liczne próby cyberszpiegostwa dokonywanego przez służby specjalne obcych państw. Dotyczy to zarówno szpiegostwa administracji państwowej, przedsiębiorstw państwowych oraz firm prywatnych. Tym bardziej, że od 1996 roku incydenty związane z użyciem sieci teleinformatycznych w Polsce sukcesywnie się nasilały.

⁶²D. Verton, *Black Ice – niewidzialna groźba cyberterroryzmu*, Helion 2004, s. 81.

3. Cyberterroryzm a ryzyko jakie za sobą niesie

Cyberterroryzm nie jest odrębnym rodzajem terroryzmu, ale zaliczany jest do globalnych zagrożeń. Zjawisko to może prowadzić do ogólnie globalnego paraliżu, bez powodowania fizycznych zniszczeń. Działalność cyberterrorystyczna ma na celu paraliż przede wszystkim systemów łączności, systemów obronnych czy sieci bankowych. Może również przyczynić się do katastrof lotniczych lub kolejowych. Zgodnie ze słowami B. Bolechów – „[...] sabotaż ze strony jakiegokolwiek włamywacza komputerowego, a skoordynowany sabotaż może uniemożliwić funkcjonowanie całego kraju. Stąd wzięty się liczne spekulacje na temat infoterroryzmu i cyberwojny”⁶³. Walka z cyberterroryzmem wymaga o wiele większej koordynacji niż w przypadku innych działań. W literaturze przedmiotu formułują się liczne definicje cyberterroryzmu. A. Bógdał-Brzezińska przedstawia jedną z nich – „politycznie umotywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury, oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych działań. W szerszym rozumieniu tego słowa jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne”⁶⁴. Można przedstawić jeszcze kilka definicji tego zjawiska:

Dorothy Denning: „[...] groźba lub bezprawny atak wymierzony na system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu”⁶⁵.

James Lewis: „[...] wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań”⁶⁶.

National Infrastructure US Protection Centre: „[...] akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie lub przerwanie świadczenia usług dla wywołania strachu, przez wprowadzenie zamieszania lub niepewności w danej

⁶³B. Bolechów, *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2003, s. 498.

⁶⁴A. Bógdał-Brzezińska A., M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 326.

⁶⁵D. Denning, *Cyberterrorism*, 2000 <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>, (dostęp: 27.03.2016 r.).

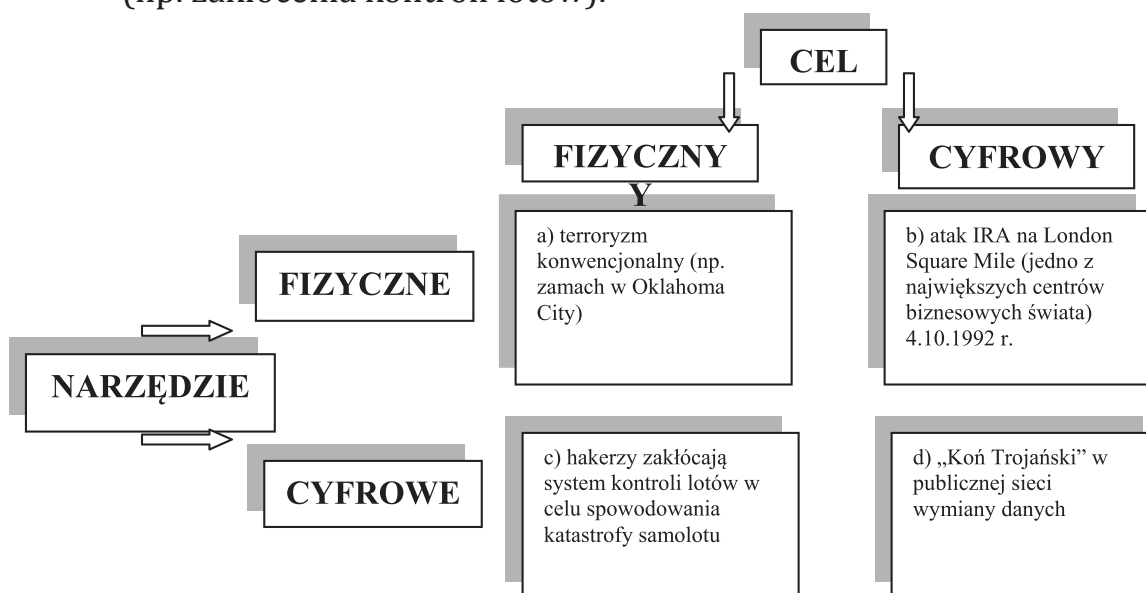
⁶⁶J. A. Lewis, *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002, Center for Strategic and International Studies, <http://www.csis.org/tech/0211lewis.pdf>, (dostęp: 27.03.2016 r.).

populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonych przez terrorystów programu”⁶⁷.

Cyberterroryzm posiada bardzo wiele zalet pod kątem terrorystów. Nie wymaga on wykorzystania środków zagrażających życiu takich jak: broń czy materiały wybuchowe. Cyberterrorysty nie mają konieczności zmieniania swojej lokalizacji, a narzędzia do prowadzenia działalności cyberterrorystycznej są ogólnie dostępne na światowym rynku. Dzięki niewielkiej możliwości wykrycia ataku zalety te czynią cyberprzestępcę niemal doskonałym. Zamach cyberterrorystyczny nie musi mieć fizycznego miejsca – może być on wymierzony w system funkcjonujący w skali nawet globalnej. Utrudnia to znacznie pociąganie sprawców do odpowiedzialności prawnej.

Zjawisko cyberterroryzm ulega ciągłym przemianom przybierając różne formy (schemat nr 1), wraz z rozwojem dostępnych technologii. Możemy podzielić go na dwa rodzaje⁶⁸:

- kiedy technika informacyjna jest celem ataku – cyberterrorysty atakują system informatyczny (elektronicznie i fizycznie) czego efektem są zakłócenia i zniszczenia w tym systemie i związanej z nim infrastrukturze informatycznej (np. energetycznej);
- kiedy stanowi ona tylko narzędzie do osiągnięcia celu – cyberterrorysty manipulują systemem informatycznym (zmiana, kradzież danych) i wykorzystują go do celów do jakich nie był on przeznaczony (np. zakłócenia kontroli lotów).



Rys. 1. Formy zjawiska cyberterroryzmu

Źródło: B. Bolechów, op. cit.

⁶⁷L. Garrison, M. Grand, *Cyberterrorism*, 2001, An evolving concept, NIPC highlights, <http://www.Nopc.gov/publication/highlight/2001/highlight-01-06> (dostęp: 27.03.2016 r.).

⁶⁸B. Bolechów, op. cit.

Powszechność ataków terrorystycznych i cyberterrorystycznych w ostatnich kilkunastu latach sprawia, że przyjmujemy, iż to właśnie działania o tym charakterze stanowią największe zagrożenie, a zarazem wyzwanie w najbliższej przyszłości. Cyberterroryzm w porównaniu z klasycznym terroryzmem jest tańszą formą działalności. Do jego przeprowadzenia potrzebny jest jedynie komputer i podłączenie do sieci. W cyberprzestrzeni nie ma fizycznych barier kontrolnych, granic, celników czy straży granicznej. Zjawisko to wymaga małego przygotowania fizycznego oraz mniejszego zabezpieczenia logistycznego. Do wykonania ataku nie ma konieczności podróżowania. Ryzyko poniesienia śmierci lub jakichkolwiek innych obrażeń fizycznych przy przeprowadzaniu ataku jest niemal znikome, jeśli nie wręcz niemożliwe.

Wiele państw lekceważy fakt, że cyberterrorystyczne ataki mogą породzić się w śmiertelne zagrożenie poprzez:

- przeładowania i zakłócenia funkcjonowania komunikacji telefonicznej blokującej powiadamianie o nagłych wypadkach;
- zakłócenia powietrznej kontroli ruchu;
- uszkodzania rekonfiguracji oprogramowania używanego w szpitalach i ratownictwie medycznym;
- manipulacje treściami receptur w skomputeryzowanych liniach produkcyjnych firm farmaceutycznych;
- zmiany ciśnienia w ropociągach i gazociągach prowadzące do wybuchów;
- kradzież tożsamości;
- sabotaż danych na rynkach finansowych⁶⁹.

Cyberterroryzm stanowi realne zagrożenie przyszłości. Można wymienić systemy, które w dość szczególny sposób mogą być narażone na atak, mimo iż są chronione i zabezpieczone w różnym stopniu:

- system produkcji i dystrybucji żywności, system ochrony zdrowia. Szczególnie niebezpieczne byłyby zakłócenia pracy oczyszczalni i przepompowni wody lub produkcji zakładów farmaceutycznych;
- systemy energetyczne i komunikacyjne. Są one wysoko skomputeryzowane, a ich zakłócenie miałoby bardzo destabilizujący efekt na działanie państwa i życie ludzi. Za szczególnie wrażliwe uważa się systemy telekomunikacyjne, energetyczne, systemy rurociągów dostarczających gaz lub ropę, systemy logistyczne. Niebezpieczeństwo zamachu potęguje fakt, że systemy komunikacji są niezbędne dla sprawnego funkcjonowania administracji oraz służb państwa, które w olbrzymim stopniu korzystają ze zwykłej, cywilnej sieci telekomunikacyjnej;

⁶⁹B. Bógdał-Brzezińska, M. F. Gawrycki, op. cit., s. 41.

- szeroko pojęty system finansowy. Jest, z oczywistych względów, szczególnie chroniony, szczególnie w sektorze bankowym i giełdowym. Jego zakłócenie mogłoby wywołać wielkie niepokoje społeczne, spowodować gwałtowny odpływ gotówki z banków ze wszystkimi tego konsekwencjami dla gospodarki. Podobny w skutkach byłby zamach na system ubezpieczeń społecznych. Wstrzymanie lub nieprawidłowości w wypłatach świadczeń szczególnie godziłoby w prestiż i zaufanie obywateli do państwa;
- infrastruktura i funkcjonowanie transportu. Zależnie od zamierzeń i umiejętności terrorystów atak na koleje lub transport lotniczy mógłby skończyć się przejściowym paraliżem lub nawet katastrofami – zderzeniami pociągów lub samolotów;
- system administracyjny i prawny. Jest on szczególnie narażony na atak, gdyż zarówno w odczuciu terrorystów jak i społeczeństwa może być utożsamiony z państwem i władzą. Szczególnie destabilizujący efekt przyniosłoby zakłócenie systemu podatkowego, oraz systemów łączności służb bezpieczeństwa. Oczywistym dowodem słabości państwa byłoby naruszenie rejestrów skazanych (zniszczenie danych mogłoby przynieść też bezpośrednie korzyści grupom terrorystycznym) lub systemu ewidencji ludności⁷⁰.

Wszystkie ataki z użyciem technologii informatycznych mają kilka wspólnych cech:

- ataki są niezwykle trudne do wykrycia. Osoba zlecająca atak może wynająć wykonawców z całkiem innego kraju;
- istnieje bardzo wysoki stopień anonimowości osób, które przeprowadzają atak;
- występuje niezwykła łatwość przeprowadzania ataków. Do realizacji nie potrzeba niczego więcej jak dostęp do sieci i oczywiście komputer;
- niskie koszty przedsięwzięcia.

Naukowcy z Monterey zdefiniowali trzy poziomy zagrożenia związane z cyberterroryzmem⁷¹:

- SIMPLE – UNSTRUCTURED – cyberterrorysty dokonują prostych włamań do indywidualnych systemów informacyjnych, stosując „narzędzia internetowe” skonstruowane przez kogoś innego. Organizacja terrorystyczna ma niewielką zdolność analizy, dowodzenia, kontroli, oraz uczenia się nowych metod atakowania w cyberprzestrzeni;
- ADVANCED – STRUCTURED – cyberterrorysty dokonują bardziej skomplikowanych ataków przeciwko złożonym systemom i sieciom komputerowym. Posiadają możliwość modyfikacji lub tworzenia

⁷⁰K. Jaroszyński, *Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz Stanach Zjednoczonych*, Warszawa, AON 2001, s. 11.

⁷¹A. Bógdał-Brzezińska, M. F. Gawrycki, op. cit., s. 87.

własnych „narzędzi”, służących do atakowania w cyberprzestrzeni. Mają zdolność analizy celów będących przedmiotem ataku, dowodzenia, kontroli, oraz uczenia się nowych metod atakowania;

- COMPLEX – COORDINATED – cyberterroryści dokonują skoordynowanych ataków, obliczonych na totalną destrukcję zintegrowanego systemu obronnego. Mają możliwość tworzenia skomplikowanych „narzędzi”, służących do niszczenia celów w cyberprzestrzeni oraz analizy celów będących przedmiotem ataku, dowodzenia, kontroli, oraz samodoskonalenia.

Zagadnienia związane z cyberterroryzmem oraz zagrożeniem jakim jest on dla bezpieczeństwa informacyjnego, powodują, iż sieć komputerowa jest w dzisiejszym świecie – siecią nerwową kraju. Widmo ataku w globalnym cyberświecie staje się coraz to bardziej realne. Występujące we współczesnym świecie podziały i towarzyszące temu właśnie przybierają w ostatnich latach coraz bardziej radykalne formy i coraz częściej przenoszone są na wirtualną płaszczyznę⁷².

Główne powody, które mogą skłonić terrorystów do ataków w cyberprzestrzeni:

- niskie koszty takiej działalności, zwłaszcza w porównaniu z kosztami regularnych działań zbrojnych. Jeszcze kilka lat temu na komputer mogli pozwolić sobie tylko dobrze sytuowani, obecnie nie jest to aż tak duży wydatek w rodzinnym budżecie, w dodatku ceny zestawów komputerowych cały czas spadają;
- zanikanie wszelkich granic. Państwa tracą część swojej suwerenności. Nie ma sensu dzielić cyberterroryzmu na „międzynarodowy” czy „narodowy”. Ataku można dokonać z każdego miejsca na ziemi, w którym jest dostęp do sieci. Zacierają się granice między tym co prywatne a państwowe, wojskowe a komercyjne, itd. Konsekwencją zanikania wszelkiego rodzaju barier jest prawdopodobieństwo, że zaatakowane państwo nie będzie sobie zdawało z tego sprawy (zacieranie się granic między wojną a pokojem). W Stanach Zjednoczonych, w publikacjach z przed 11 września 2001 roku, podkreśla się, że terytorium USA przestaje być „sanktuarium” bezpiecznym od wszelkiego rodzaju uderzenia;
- możliwość dokonywania nagłych i nieprzewidywalnych akcji. Ofiary są całkowicie nieświadome i nieprzygotowane do ich odparcia;
- całkowita anonimowość. Powoduje to możliwość manipulowania informacją, utrudnia państwom odparcie ataku i budowanie koalicji;
- minimalne ryzyko wykrycia przygotowanego ataku;
- zamiast uderzać w niewinnych ludzi można sparaliżować system wrogiego państwa, większy efekt propagandowy i uznanie opinii publicznej⁷³.

⁷²J. Horgan, *Psychologia terroryzmu*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 66.

⁷³A. Bógdał-Brzezińska, M. F. Gawrycki, op. cit., s. 88.

Powody skłaniające terrorystów do ataku w cyberprzestrzeni można przedstawić za pomocą tabeli nr1:

Tabela nr 1. Powody skłaniające terrorystów do ataku w cyberprzestrzeni

<i>Dlaczego cyberterroryzm?</i>	<i>Jaki to ma wpływ na bezpieczeństwo?</i>
Niskie koszty	Każdy może zostać cyberterrorystą. Wystarczy mieć komputer, modem i trochę umiejętności.
Działania ponad granicami państw	Nie wiadomo skąd pochodzi atak, kto atakuje i kto za tym stoi.
Postrzeganie zagrożenia	Nie wiadomo, które zagrożenie jest realne, a które wirtualne.
Wykrycie cyberataku	Nie wiadomo, jakie są zdolności i intencję atakującego.
Cel ataku	Nie wiadomo, co będzie celem ataku, ani w jaki sposób zostanie on wykonany.
Budowa koalicji	Nie wiadomo, kto jest swój, a kto obcy.

Źródło: A. Bógdał-Brzezińska, M. F. Gawrycki, op. cit., s.88.

Ważnym aspektem rozważań nad cyberterroryzmem jest analiza celów, przeciwko którym mogą zostać skierowane ataki:⁷⁴

- telekomunikacja (*Telecommunication*) – linie telefoniczne, satelity, sieci komputerowe – komercyjne, wojskowe, akademickie itd.;
- system energetyczny (*Electrical Power System*) – produkcja, dystrybucja energii, a także transport i magazynowanie surowców niezbędnych do jej produkcji;
- produkcja, magazynowanie i transport gazu ziemnego oraz ropy naftowej (*Oil and Gas Delivery and Storage*) – cały proces wydobywania ropy naftowej i gazu ziemnego, magazynowania, przetwarzania i transportu za pomocą rurociągów, statków, transportem kołowym i kolejowym (także dostarczenie paliwa do zamorskich baz wojskowych USA);
- system bankowy i finansowy (*Banking and Finance*) – system przepływu bilionów dolarów poczynając od indywidualnych depozytów po transfer ogromnych sum pieniędzy z jednego krańca świata na drugi. Obejmuje wszystkie dostępne instrumenty operacji finansowych;
- transport (*Transportation*) – transport lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów, oraz cały system wsparcia logistycznego;
- system zaopatrzenia w wodę (*Water Supply System*) – składają się na niego: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania dla rolnictwa, przemysłu, straży pożarnej oraz indywidualnych odbiorców;

⁷⁴Tamże, s. 134.

- służby ratownicze (*Emergency Service*) – w Stanach Zjednoczonych system alarmowy 911 komunikacja z policją, służbą zdrowia, strażą pożarną, itd.;
- ciągłość funkcjonowania władzy i służb publicznych (*Continuity of Government Services*) – wszystkie te elementy, które zapewniają funkcjonowanie lokalnych, regionalnych i centralnych władz oraz systemu publicznego: służba zdrowia, bezpieczeństwo, obrona itd.

Przykładowe akcje, jakie mogą podjąć cyberterroryści:

- propaganda;
- instruktaż i komunikacja: atak na oprogramowanie;
- atak na systemy informacyjne i sprzęt komputerowy;
- wojny internetowe;
- atak fizyczny⁷⁵.

Działania o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania cyberterroryzmu, oraz innych zagrożeń dla bezpieczeństwa państwa: zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa skutkujące zwiększeniem poziomu jej odporności na ataki cyberterrorystyczne; stworzenie i realizacja spójnej dla wszystkich zaangażowanych podmiotów administracji publicznej oraz innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa polityki dotyczącej bezpieczeństwa cyberprzestrzeni; zmniejszenie skutków ataków cyberterrorystycznych, a przez to kosztów usuwania ich następstw; stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnienie bezpieczeństwa cyberprzestrzeni państwa, oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa; zwiększenie kompetencji odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa oraz innych systemów i sieci administracji publicznej; zwiększenie świadomości użytkowników systemów dostępnych elektronicznie i sieci teleinformatycznych w zakresie metod i środków bezpieczeństwa.

Przestępczość informatyczna podlega tym samym normom prawnym, co jakiegokolwiek inny rodzaj przestępczości. Zagrożenie cyberterroryzmem, wraz z jakościowym i ilościowym rozwojem systemów komputerowych stale rośnie. Warto więc zdać sobie sprawę z tego, że cyberterroryzm stanowi realne zagrożenie dla bezpieczeństwa międzynarodowego ze strony cyberterrorystów w XXI wieku. Wraz ze wzrostem internautów na świecie zagrożenie to będzie się zwiększać.

⁷⁵E. Heliżak, W. Lizak, L. Łukaszuk, E. Śliwka (red.), *Terroryzm w świecie współczesnym*, Warszawa – Pieniężno 2004.

Podsumowanie

W ciągu najbliższych 20-30 lat cyberataki staną się coraz bardziej istotnym elementem współczesnej wojny – mówi William Crowell były zastępca dyrektora Agencji Bezpieczeństwa narodowego (NSA). Ofiarą cyberwojen może również paść sektor prywatny przed inwazją na Irak, służby specjalne USA planowały atak na iracki system finansowy. Niedoszło do tego tylko, dlatego że rząd G. Busha obawiał się zachwiania całej bankowości Bliskiego Wschodu a także Europy i USA. Aby ochronić całą infrastrukturę kraju działania wojska muszą być skoordynowane z sektorem prywatnym i finansowym, aby ochronić najważniejsze dla Państwa sektory teleinformatyczne. Kiedyś mówiło się, że rano możemy się obudzić, i znów nie będzie „Teleranka”, tym razem możemy się obudzić i nie będzie Internetu, telefonu, telewizji, a tym samym nie będą funkcjonowały banki, komunikacja, itp. Można mieć wpływ na to, czy atak hakerów, cyberterrorystów się uda. Przede wszystkim warto pomyśleć o dobrym programie antywirusowym w komputerze, telefonie komórkowym, tablecie, etc., bowiem ataki typu DDOS, mogą dotyczyć również naszego komputera.

Bibliografia

1. Ciekanowski Z., Wojciechowska-Filipek S., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni Jednostki – Organizacji – Państwa*, CeDeWu, Warszawa 2016.
2. Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013.
3. Ciekanowski Z., *Cyberterroryzm*, [w:] *Zabić tysiące przestraszyć miliony*, WSZiP, Warszawa 2009.
4. Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Wydawnictwo Trio Collegium Civitas, Warszawa 2008.
5. Verton D., *Black Ice – niewidzialna groźba cyberterroryzmu*, Helion 2004.
6. Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2003.
7. Bógdał-Brzezińska A., M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
8. Denning D., *Cyberterrorism, 2000* <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>, (dostęp: 27.03.2016 r.).
9. Lewis J. A., *Assessing the risk of cyber terrorism, cyber war and other cyber threats, 2002*, Center for Strategic and International Studies, <http://www.csis.org/tech/0211lewis.pdf>, (dostęp: 27.03.2016 r.).

10. Garrison L., Grand M., *Cyberterrorism, 2001, An evolving concept, NIPC highlights*, <http://www.Nopc.gov/publication/highlight/2001/highlight-01-06> (dostęp: 27.03.2016 r.).
11. Jaroszyński K., *Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz Stanach Zjednoczonych*, Warszawa, AON 2001.
12. Horgan J., *Psychologia terroryzmu*, Wydawnictwo Naukowe PWN, Warszawa 2008.
13. E. Heliżak, W. Lizak, L. Łukaszuk, E. Śliwka (red.), *Terroryzm w świecie współczesnym*, Warszawa – Pieniężno 2004.

Liczba znaków ze spacjami: 39 853