Mariusz PALA[1]

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Instytut Nauk Społecznych i Bezpieczeństwa

mariusz_pala@wp.pl

WYBRANE ASPEKTY BEZPIECZEŃSTWA W CYBERPRZESTRZENI

ABSTRAKT: Niniejszy artykuł, przedstawia współczesne zagrożenia w cyberprzestrzeni. W dobie powszechnej informatyzacji posiadamy dostęp do Internetu i możemy swobodnie komunikować się ze wszystkimi na świecie za pomocą komunikatorów czy poczty elektronicznej, co powoduje, że możemy mieć dostęp do najbardziej aktualnych informacji. Internet stał się obszarem, gdzie można dokonywać również różnego rodzaju nadużyć. Korzystają z niego nie tylko przestępcy czy służby specjalne wielu państw, ale również terroryści. Terroryzm, w klasycznym rozumieniu jest formą protestu lub walki, których celem jest zwrócenia na siebie uwagi opinii publicznej bądź władz państwowych. Terroryści stosują narzędzia należące do zbioru nielegalnych metod, zakazanych przez prawo międzynarodowe i napiętnowanych przez międzynarodowe organizacje. Najnowszą formą działań terrorystów jest aktywność w cyberprzestrzeni. Celem cyberterrorystów, jest opanowanie najważniejszych sektorów, a następnie monopolizacja dostępu do informacji.

SŁOWA KLUCZOWE: cyberprzestrzeń, cyberterroryzm, cyberprzestępczość.

SELECTED ASPECTS OF CYBERSPACE SECURITY

ABSTRACT: This article provides information about contemporary threats to information security in cyberspace. In the age of universal computerization, worldwide Internet access we are freely to communicate with all the world via instant messengers or e-mail, what gives the access to the most current information. The Internet has become an area of various kinds of abuse. The Internet is used not only by criminals or secret services of many countries, but also terrorists. Terrorism in the traditional sense is a form of protest or struggle, aimed at the achievement of some objective and to attract attention of public opinion or the government. Terrorists use the tools belonging to the collection of illegal methods that are banned by international law and condemned by international organizations. The latest form of terrorist activity is cyberspace activity. Cyberterrorists aim to control the most important sectors and the monopolization of the information access.

KEYWORDS: cyberspace, cyberterrorism, cybercrime.

[1] Mgr Mariusz Pala – doktorant Instytutu Nauk Społecznych i Bezpieczeństwa Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach; major; pracuje w Centrum Wsparcia Teleinformatycznego Sił Zbrojnych, na stanowisku Szefa Wydziału Dozoru Systemów Łączności w Pionie Zarządzania i Sterowania Systemami Łączności. Prowadzi badania na temat strategii przeciwdziałania zagrożeniom informacyjnym w SZ RP.

WPROWADZENIE

Obecnie, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa i obronności państwa. Koniecznością jest zatem, stworzenie mechanizmów rozpoznania zagrożeń istniejących w cyberprzestrzeni takich jak: cyberterroryzm, cyberprzestępczość, cyberwojna oraz innych form działań, mogących powodować zakłócenia w funkcjonowaniu krytycznej infrastruktury państwa.

Celem artykułu jest krótkie przedstawienie zagrożeń wynikających z rewolucji technologicznej, ukazanie sposobów dokonywania ataków w cyberprzestrzeni oraz ogólne omówienie sposobów finansowania działalności organizacji terrorystycznych w cyberprzestrzeni, jak również współpracy międzynarodowej w celu zwalczania cyberterroryzmu. Autor dąży do wskazania możliwych działań, które pozwolą na ich zapobieganie. Cyberterroryści wykorzystują cyberprzestrzeń do manipulowania informacją, transferu danych, rozpowszechniania propagandy, czy idealizowania własnych poglądów. Poprzez ataki na infrastrukturę krytyczną państwa, komunikacje, transport, telemedia, system ochrony zdrowia i wiele innych, cyberataki mogą zagrażać życiu i zdrowiu ludności. Rozwój technik informacyjnych, powoduje powstanie zagrożeń dla stabilności bezpieczeństwa państwa i jego mieszkańców. Poważnym wyzwaniem staje się zapewnienie przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego w cyberprzestrzeni. Odpowiednie działania techniczno-eksploatacyjne oraz proceduralno-organizacyjne, pozwolą zmniejszyć ryzyko wystąpienia zagrożeń w systemach informacyjnych. Z tego względu, konieczne są kompleksowe działania pozwalające na zwiększenie zdolności do zapobiegania i zwalczania zagrożeń w cyberprzestrzeni w czasie pokoju, kryzysu czy wojny. Odpowiednio wypracowane koncepcje i strategie połączone z planami ciągłości działania, powinny skutecznie realizować ochronę infrastruktury krytycznej państwa.

CHARAKTERYSTYKA CYBERPRZESTRZENI I KIERUNKI JEJ EWOLUCJI

Cyberprzestrzeń, to kolejny po lądzie, morzu, przestrzeni powietrznej i kosmicznej, wymiar konfrontacji zbrojnej wyróżniony w popularnym „modelu Wardena”[2]. Termin ten został po raz pierwszy użyty przez Williama Gibbsona w powieści „Burning Chrome” w 1984 r. Nie dotyczył on jednak technicznych zagadnień, jedynie scharakteryzował przestrzeń społeczną[3]. Autor wyżej wymienionej książki, cyberprzestrzeń nazywał matrycą. W chwili obecnej używa się tego słowa do nazwania wirtualnej przestrzeni, gdzie komputery i media cyfrowe komunikują się ze sobą za pomocą globalnego systemu komunikacji – Internetu, który

[2] Na początku lat dziewięćdziesiątych XX w. przestrzeń cybernetyczną, jako piąty model wojny, wyróżniono w popularnym „modelu Wardena”, (ujęciem współczesnej walki, w którym piątym wymiarem walki jest przestrzeń cybernetyczna); J. Warden, *The Enemy as System*, „Airpower Journal”, Spring 1955.

[3] A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterrozryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 11.

został ukształtowany dzięki zaistnieniu konsolidacji różnych form przekazywania informacji na skutek ucyfrowienia – zgodności działania systemów telekomunikacyjnych i teleinformatycznych oraz połączenia technosfery – która doprowadziła do otrzymania platformy teleinformatycznej. Inaczej cyberprzestrzeń, to system powiązań internetowych, który tworzy przestrzeń komunikacyjna[4].

Z jednej strony cyberprzestrzeń jest przestrzenią współpracy, która niesie za sobą pozytywne skutki prowadzące do rozwoju komunikacji społecznej, bezpieczeństwa powszechnego i gospodarki i edukacji. Z drugiej strony, jest przestrzenią, w której występują negatywne skutki, wyrażające się kontrolowaniem społeczeństwa za pomocą specjalnych narzędzi teleinformatycznych stosowanych przez służby państwowe (cyberinwigilacja). Kolejnym negatywnym skutkiem jest wykorzystanie sieci informatycznych do przestępczości o charakterze ekonomicznym – w ramach przestępczości zorganizowanej (cyberprzestępczość) – oraz wykorzystania sieci do w działań terrorystycznych (cyberterroryzm). Ostatnim negatywnym działaniem w cyberprzestrzeni, jest prowadzenie działań wojennych (cyberwojna)[5].

Początki sieci komputerowej datuje się na lata sześćdziesiąte XX w., a więc okres zimnej wojny. W tym czasie w Stanach Zjednoczonych powstał projekt systemu łączności, którego bezpośrednim następstwem było utworzenie w 1969 r. sieci ARPANET (*Advanced Research Projects Agency Network*), uznawanej za poprzedniczkę Intrenetu[6]. Wstępnie sieć łączyła cztery komputery w USA. Jej zadaniem było sprawdzenie łączności transmisji danych w przypadku uszkodzenia pewnej jej części. Z upływem czasu, dołączały do projektu inne ośrodki naukowe i rządowe. Nadszedł spektakularny rozkwit sieci i powstanie systemu Telnet, pozwalającego na łączenie się z innymi komputerami jak również dopuszczającego zdalną pracę na nich tak, jak na komputerze lokalnym. Po raz pierwszy została wysłana wiadomość za pomocą poczty elektronicznej (e-mail). Doszło do pierwszego połączenia międzykontynentalnego. W ten właśnie sposób, powstał Internet. Pojawiły się pierwsze przypadki oszustw i sabotażu. Rozpoczął się również proces masowego przetwarzania informacji o danych osobowych, będący naruszeniem praw obywatelskich i zagrożeniem dla osób korzystających z sieci internetowych. Wystąpiły pierwsze nadużycia komputerowe w postaci hackingu. W drugiej połowie lat 80. XX w. zaczęła zwiększać się szybkości transmisji w sieci. Zaczęły podłączać się do niej nowe ośrodki państw spoza USA. Rozpoczęło się tworzenie pierwszych nielegalnych, pirackich kopii oprogramowania. W Polsce początki Internetu datuje się na 1991 r. Pierwszy polski węzeł internetowy oraz instytucja NASK (Naukowe i Akademickie Sieci Komputerowe) powstał na Uniwersytecie Warszawskim.

[4] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego* „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1, 2005, s. 173-175.
[5] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioła, J. Kisielniecki, K. Rajchel. (red.), Cyberterroryzm-nowe *wyzwania XXI wieku*, Warszawa 2009, s. 46.
[6] T. Szubrycht, *op. cit.*, s. 180.

Głównym zadaniem instytucji była organizacja sieci w Polsce. Połączenie się ze sobą ośrodków na całym świecie spowodowało powstanie internetowego systemu informacyjnego www, który przyczynił się do wzrostu informacji umieszczanych w Internecie. W latach dziewięćdziesiątych XX w. zakupy dokonywane w sklepach internetowych stały się zjawiskiem normalnym[7]. W chwili obecnej, poprzez komputery oraz urządzenia mobilne, staliśmy się uczestnikami systemu sieciowego o charakterze globalnym. Dzięki Internetowi, przy pomocy poczty elektronicznej, rozpowszechniła się komunikacja miedzy ludźmi w różnych zakątkach naszej planety. Łatwiejsze stało się wyszukiwanie informacji na interesujące nas tematy. Powszechność sieci spowodowała jednak, że zaczęto jej również używać do nielegalnych celów.

Rozważając, czym jest cyberprzestrzeń i popełniane w niej przestępstwa, należy dokonać podziału rodzajów czynów w niej zabronionych. Do pierwszej kategorii przestępstw, zaliczam takie formy działania jak oszustwa i fałszerstwa. Popełniane są one przy wykorzystaniu sieci informatycznych. Następną, równie groźną odmianą cyberprzestępczości, jest wytwarzanie, rozpowszechnianie, pozyskiwanie oraz posiadanie treści nielegalnych w systemie informatycznym. Trzecim rodzajem, są przestępstwa dotyczące sieci – głównie chodzi o ataki na systemy informatyczne oraz hakerstwo. Do czwartej kategorii, zaliczamy kopiowanie i rozpowszechnianie w celach zarobkowych, utworów objętych prawem autorskim.

Natomiast Komisja Europejska do cyberprzestępstaw zalicza:

- przestępstwa przeciwko poufności, integralności i dostępności danych, dotyczące nielegalnego dostępu do systemów – czyli hacking, podsłuchiwanie i podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe;
- manipulacja fakturami lub kontami firmowymi, nieprawdziwe aukcje czy nielegalne używani kart kredytowych, komputerowe podróbki, molestowanie dzieci, ataki na życie ludzkie, manipulowanie systemami szpitalnymi lub kontrolą ruchu powietrznego;
- przestępstwa „contentowe", obejmujące dziecięcą pornografię, dostarczanie instrukcji zachowań przestępczych, oferty popełniania przestępstw, molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji oraz internetowy hazard;
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, takie jak: nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych itp.[8]

Opublikowany w 2007 r. raport Europolu, przedstawia rodzaje cyberprzestępczości w ujęciu wertykalnym i horyzontalnym. Ujęcie wertykalne dotyczy przestępstw, które dokonywane są wyłącznie w cyberprzestrzeni i nie istnieją poza nią. Wśród nich możemy wyróżnić hacking, crimewarem, spamming. W ujęciu horyzontalnym, dla ułatwienia

[7] J. Wójcik, *Przestępstwa komputerowe*, Cześć I, Warszawa 1999, s. 52.
[8] T. Szubrycht, *op. cit.*, s. 174.

przestępstwa, wykorzystuje się techniki komputerowe oraz informatyczne. Wyróżniamy tu (jako najgroźniejsze): pornografię dziecięcą, piractwo intelektualne, nielegalne wykorzystanie kart płatniczych, kradzież danych osobowych (*phishing*), cyberterroryzm[9] oraz pranie brudnych pieniędzy (*cyberlaundering*). W Polsce do głównych zagrożeń w cyberprzestrzeni zaliczamy: oszustwa, wyłudzanie pieniędzy, e-maile z informacją o podłożeniu ładunku wybuchowego, kradzież danych. Zagrożenia te mogą mieć miejsce wyłącznie przy użyciu oprogramowania destrukcyjnego zaprojektowanego przez cyberprzestępców.

Twórcą pojęcia cyberterrozryzmu był Barry Collin, który w 1996 r. w swoim wystąpieniu *The Future of Cyber Terrorism,* określił cyberterroryzm jako efekt konwergencji cybernetyki i terroryzmu. Również Dorothy E. Denning pisała, że: „cyberterroryzm to konwergencja terroryzmu i cyberprzestrzeni”[10]. Tym samym uznała, że cyberprzestępczość, to bezprawne zamachy lub ich groźby na sieci i systemy komputerowe oraz informacyjne, które mają na celu zastraszenie lub zmuszenie władz do spełnienia żądań politycznych czy społecznych, powodujących skutki o cechach przemocy wobec osób i mienia – wzbudzanie strachu, spowodowanie śmierci lub uszczerbku na zdrowiu, eksplozji lub dużych szkód majątkowych[11].

Można spostrzec, że przestępstwa informatyczne zawierają bardzo duży przedział ataków. Próba zrozumienia wielu typów aktywności cyberprzestępców jest tak samo ważna, jak próba zabezpieczenia własnego systemu przed atakiem ze strony hakerów. Według firmy Symantec, przestępstwem komputerowym można nazwać każde przestępstwo, które zostało popełnione przy pomocy komputera, sieci czy specjalnego oprogramowania.

Bardzo poważnym zagrożeniem są wirusy, które uniemożliwiają prawidłowe działanie systemów komputerowych sterujących pracą infrastruktury istotnej dla funkcjonowania państwa. Rezultatem, jest przerwanie dopływu energii, brak możliwości działania systemów komunikacji, czy konieczność zamknięcia systemów bankowych. Ponadto rozprzestrzenia się chaos informacyjny, spowodowany publikowaniem fałszywych informacji na stronach internetowych. W społeczeństwie wybucha panika, a przestępczość diametralnie wzrasta. W obecnym czasie, takie sytuacje stają się coraz bardziej realne. Żyjemy w społeczeństwie o charakterze informacyjnym, w którym jednym z najcenniejszych dóbr jest informacja. Wiele aspektów życia obywatela i wiele sektorów gospodarki staje się zależne od poprawnego działania sieci i systemów informatycznych. P. Sienkiewicz wyróżnił sześć podstawowych powodów, które przemawiają za wykorzystywaniem cyberterroryzmu do osiągnięcia określonych celów:

– niski koszt tej działalności, zwłaszcza porównując z kosztem regularnych działań zbrojnych;

[9] *Ibidem*, s.175.
[10] *Ibidem*, s. 160.
[11] *Ibidem*, s. 161.

- zanikanie wszelkich granic (państwa tracą część swojej suwerenności) – zacierają się granice między tym, co prywatne a państwowe, wojskowe a komercyjne itd. Konsekwencją zanikania wszelkich barier jest prawdopodobieństwo, że zaatakowane państwo nie będzie sobie z tego zdawało sprawy (zacieranie się granic między wojną a pokojem);
- możliwość dokonywania nagłych i nieprzewidywalnych akcji – ofiary są całkowicie nieświadome i nieprzygotowane do ich odparcia;
- całkowita anonimowość – powoduje możliwość manipulowania informacją, utrudnia państwom odparcie ataku i budowanie koalicji;
- minimalne ryzyko wykrycia przygotowywanego ataku;
- zamiast uderzać w niewinnych ludzi można sparaliżować system wrogiego państwa;
- większy efekt propagandowy i uznanie opinii publicznej[12].

Ponadto przestępca, który wykorzystuje cyberprzestrzeń do ataku terrorystycznego nie naraża własnego życia, a jego umiejętności nie musza być wygórowane. Walka z cyberterroryzmem wymaga dużo większej koordynacji niż przy tradycyjnych sposobach działania. Odszyfrowanie kodu danych czy włamanie się do systemu staje się prostsze w miarę, jak rozprzestrzenia się powszechny dostęp do sieci komputerowych. W efekcie, każdy człowiek może zostać cyberprzestępcą. Jedną z klasyfikacji zagrożeń w cyberprzestrzeni przedstawia Włodzimierz Gogołek, prezentując ją w siedmiu kategoriach:

- *stealingpasswords* – metody polegające na uzyskaniu haseł dostępu do sieci;
- *social engineering* – wykorzystanie niekompetencji osób, które mają dostęp do systemu teleinformatycznego;
- *bugs and backdoors* – korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł;
- *authenticationfailures* – zniszczenie mechanizmu używanego do autoryzacji;
- *protocolfailures* – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami lub procesami;
- *information leakage* – atakujący zdobywa informacje dostępne tylko dla administratora;
- *denial of service* – uniemożliwienie korzystania użytkownikom z systemu[13].

Globalny rozwój wykorzystania cyberprzestrzeni w społeczeństwie informacyjnym niesie za sobą wiele zagrożeń. Mogą one odnosić się do wszystkich dziedzin bezpieczeństwa narodowego, od zagrożeń na małą skalę, aż do cyberwojny włącznie. Obiektem cyberwojny, są elementy infrastruktury tak cywilnej jak i wojskowej. Są to systemy, sieci teleinformatyczne i oferowane przez nie usługi wykorzystywane przez administrację rządową, organy władzy ustawodawczej, strategicznych przedsiębiorców, czy służby mundurowe, które powinny być

[12] *Ibidem*, s. 50.
[13] W. Gogołek, *Manipulacja w sieci*, [w:] B. Siemienicki (red.), *Manipulacja, media, edukacja*, 2007, s. 321.

objęte ochroną w cyberprzestrzeni - niezbędne jest skoordynowanie tych działań przez służby mundurowe i cywilne w zakresie zwalczania zagrożeń w cyberprzestrzeni.

TERRORYZM W CYBERPRZESTRZENI

Terroryzm, to jedno z zagrożeń czasów współczesnych. Współczesne ataki terrorystyczne stanowią potwierdzenie istnienia tego faktu. Kiedy 11. września 2001 r. zaatakowano jedno z największych mocarstw świata, Stany Zjednoczone, problem związany z terroryzmem nabrał znaczenia globalnego i stał się jedynym z głównych zagrożeń dla bezpieczeństwa międzynarodowego. Od tego momentu, za jedno z najważniejszych zadań, rząd USA postawił sobie ochronę infrastruktury krytycznej[14].

Zjawisko terroryzmu powszechnie definiowane jest jako:

(…) *planowana, zorganizowana i zazwyczaj uzasadniana ideologicznie, a w każdym bądź razie posiadająca polityczne podłoże motywacyjne, działalność osób lub grup mająca na celu wymuszenie od władz państwowych, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań, czy postaw, a realizowana w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszającego rozgłosu w opinii publicznej oraz z reguły polegające na zastosowaniu środków fizycznych, które naruszają dobra osób postronnych, tj. takich, które nie dały wyrazu swemu negatywnemu nastawieniu do aktu terrorystycznego, jego celu lub uzasadnienia ani nawet do określonej ideologii czy zapatrywań*[15].

Obecnie możemy zidentyfikować zagrożenia terrorystyczne w cyberprzestrzeni. W wielu państwach powstają cybercentra oraz cyberdowództwa powołane do zwalczania terroryzmu zagrażającego obronności i infrastrukturze państwa. W Polsce do tego typu działań, powołany jest Zespół Polityki Bezpieczeństwa Cyberprzestrzeni RP.

Z kolei Brian Jenkins określa terroryzm jako:

(…) *działania, które mogą przyjąć formy klasycznych aktów kryminalnych, takich jak morderstwa, podpalenia, użycie materiałów wybuchowych. Różnią się jednak od zwykłych działań kryminalnych tym, że są dokonywane ze szczególnie przemyślanym zamiarem wywołania paniki, zaburzenia porządku czy zastraszenia populacji, w celu destrukcji porządku publicznego, sparaliżowania możliwości reagowania społeczeństwa, zwiększenia poczucia bezradności i nieszczęścia wspólnoty*[16].

[14] A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013, s. 86.
[15] P. Sienkiewicz, *Ucieczka od wolności w globalnym społeczeństwie informacyjnym*, Szczecin 2005, s. 32.
[16] T. Szubrycht, *op. cit.*, s. 176.

Ponadto terroryzm jest zagrożeniem, które łączy w sobie trzy istotne wymiary: społeczny, ekonomiczny i finansowy. Internet stał się równoległą płaszczyzną funkcjonowania człowieka, a cyberprzestrzeń integralnym składnikiem świata realnego. Cyberprzestrzeń stała się przestrzenią, na której dostrzec można koegzystencje dobra i zła, ścieranie się ze sobą różnych ideologii. Warto zaznaczyć, że zagrożenie, jakie niesie ze sobą Internet jest nieograniczone. Postęp cywilizacyjny, obejmujący zmiany w każdym aspekcie życia człowieka, przyniósł ogromne udogodnienia w procesach wytwarzania, przekazywania i modyfikowania informacji. Mimo nieocenionych dobrodziejstw, jakie niesie ze sobą Internet, cyberprzestrzeń przynosi ze sobą także uzależnienie od technologii informacyjnych oraz zagrożenie związane z nową formą terroryzmu, czyli cyberterroryzmem.

Literatura, podobnie jak w przypadku pojęcia terroryzmu, bogata jest w definicje cyberterroryzmu. D. E. Denning określa cyberterroryzm, jako:

> (...) *groźbę lub bezprawny atak wymierzony w 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*[17].

Często pojęcia cyberterrozryzmu i cyberataku są mylone ze sobą, co prowadzi do wielu nieporozumień. Warto zaznaczyć, że według D. E. Denning politycznie umotywowany cyberatak może być przejawem cyberteroryzmu. Dotyczy to jednak przypadku, który nie tylko zakłóca porządek prawny i ekonomiczny, ale także pociąga za sobą ogromne straty[18].

Współczesne organizacje terrorystyczne wykorzystują do ataków sieci teleinformatyczne. Sieć, pozwala im zdobyć międzynarodowy rozgłos, sprawia że odznaczają się wysokim stopniem zorganizowania oraz mają znaczne zasoby środków ekonomicznych i technicznych. Nie bez znaczenia jest działalność propagandowa, służąca – jak w przypadku Al-Kaidy – do rekrutacji nowych członków, dostarczania instrukcji wykonania bomb czy przeprowadzania zamachów terrorystycznych wykorzystując inne metody i środki działania. Ostatnie lata przynoszą coraz większe obawy przed atakami terrorystycznymi w cyberprzestrzeni. Społeczeństwa obawiają się zamachów, a strach wzmaga brak wiedzy, co do czasu i celu ewentualnego ataku.

Eksperci zajmujący się zwalczaniem cyberterroryzmu sądzą, iż cyberterroryści stają się dużo większym zagrożeniem od terrorystów używający bomb czy broni palnej. Haker, włamując się do systemu komputerowego, może spowodować większą katastrofę, w której śmierć poniesie więcej osób, niż w klasycznym zamachu terrorystycznym z użyciem broni lub

[17] *Ibidem*, s. 176.
[18] *Ibidem*, s. 103.

bomb. Zatem liczba ofiar spowodowanych przez ataki cyberterrorystyczne może być znacznie wyższa. Warto podkreślić, iż namierzanie cyberterrorystów jest zajęciem niezwykle kosztownym. Wymagany jest do tego wyspecjalizowany sprzęt, a ludzie zajmujący się zwalczaniem tego rodzaju przestępców muszą posiadać odpowiednie kwalifikacje. Haker z własnego domowego komputera może skrzywdzić wiele osób, nawet z państw znajdujących się na innej półkuli ziemskiego globu. Przeciętnie uzdolniony haker, posiada umiejętności zatarcia po sobie śladów, natomiast „dobry" haker, nie pozostawi po sobie prawie żadnych śladów. Służby powołane do walki z cyberprzestępczością starają się nie pozostawać w tyle i kształcą wyspecjalizowanych pracowników, bowiem dobrego hakera może złapać tylko lepszy od niego haker. Jednak identyfikacja cyberterrorystów jest niezmiernie trudna i często zdarza się, że pozostają oni bezkarni.

Powstało wiele publikacji na temat wybitnych hakerów. Warto wspomnieć jednego z nich – Ehuda Tenenbauma, posługującego się pseudonimem *Analyzer*. Gdy był nastolatkiem potrafił włamać się do zabezpieczonych bankowych systemów teleinformatycznych, dzięki czemu posiadał dostęp do 120 tys. bankowych kont. Haker wysłał również do FBI hasła dostępowe do wielu serwerów rządowych. Działania *Analyzera* nie spowodowały żadnych strat, a on sam nie wyrządził nikomu krzywdy. Należy podkreślić, iż gdyby tak zdolny haker jak E. Tenenbaum, współpracował z organizacjami terrorystycznymi, takimi jak Hamas, Hezbollah czy Al-Kaida, mógłby w znacznym stopniu zaszkodzić wielu strukturom państwowym lub organizacjom międzynarodowym. *Analyzer* był bezpieczniejszy w rękach policji niż na wolności. Po jego aresztowaniu inni hakerzy dali dowody swojego wzburzenia poprzez różnego rodzaju ataki hakerskie[19].

Cyberterrorystami, najczęściej zostają ludzie dobrze wykształceni, absolwenci dobrych uczelni, ludzie o ponadprzeciętnej inteligencji. Z pozoru wydają się być osobami przeciętnymi, które starają się nie zwracać na siebie uwagi. Ich praca odbywa się najczęściej w domu przy komputerach, jednak skutki ich działania mogą mieć tragiczne konsekwencje. W porównaniu z klasycznym terroryzmem, cyberterroryzm jest tańszą formą działalności. Do przeprowadzenia ataku terrorystycznego potrzebny jest jedynie komputer i podłączenie do sieci a nie broń czy materiały wybuchowe. Celem ataków jest wniknięcie do systemu teleinformatycznego i wymuszenie, pożądanego z punktu widzenia terrorystów działania.

Walka z cyberterroryzmem narzuca konieczność wydania znacznych nakładów finansowych, ale także wykształcenia odpowiednich umiejętności przez służby specjalne. Środki wydawane przez państwa, przy znacznych zasobach organizacji terrorystycznych, są niestety zbyt małe, aby sprostać nowym wyzwaniom. Ważną sprawą, jest wypracowanie pewnego modelu strategii mogącej pomóc w zwalczaniu cyberterrorystów, a także tworzenie porozumień miedzy poszczególnymi państwami, starającymi się zwalczać i ograniczać cyberterroryzm.

[19] *Ibidem*, s. 54.

Skutkiem działań cyberterrorystów, są nie tylko straty finansowe, ale także zagrożenie życia ludzkiego na ogromną skalę. Jednym z ostatnich i jednocześnie niezwykle spektakularnym przejawem terroryzmu w cyberprzestrzeni, był cyberatak na Estonię. Jak poinformowała „Rzeczpospolita"[20], hakerzy z Rosji przypuścili zmasowany atak na estońskie strony internetowe. Zablokowano serwery najważniejszych państwowych instytucji, banków, czołowych gazet i partii politycznych. Był to element rosyjskiej kampanii, wymierzonej we władze Estonii, które w maju 2007 r. usunęły z centrum Tallina pomnik ku czci żołnierzy Armii Czerwonej. Warto nadmienić, że Estonia bardzo często nazywana jest „E-stonią" ze względu na bardzo wysoki stopień zinformatyzowania. Estońska infrastruktura teleinformatyczna okazała się doskonałym celem cyberataków. Sytuacja była na tyle poważna, że cyberinwazją zajęły się służby NATO i UE. Rosyjscy hakerzy uszkodzili bowiem łącza pomiędzy Tallinem a tymi organizacjami. Przedstawiciel Sojuszu podkreślił wówczas, że atak na jednego członka NATO jest atakiem na cały sojusz. Unia Europejska poruszyła tę sprawę podczas szczytu UE-Rosja, w czerwcu 2007 r. Choć Moskwa oficjalnie temu zaprzeczyła, Estończycy nie mają wątpliwości, że za cyberatak odpowiedzialny jest Kreml. Część z nich, została bowiem przeprowadzona z rosyjskich rządowych komputerów[21].

Współczesny świat niesie ze sobą rozwój nowoczesnych technologii, które generują wiele możliwości, również potencjalnych zagrożeń. W Polsce systemy teleinformatyczne nie są jeszcze na tak wysokim poziomie jak choćby w krajach lepiej rozwiniętych, ale zagrożenie cyberterroryzmem istnieje. Najlepiej rozwinięte państwa, gromadzą znaczące fundusze na budowę strategii obrony bezpieczeństwa teleinformatycznego. Główną przyczyną, na jaką wskazują, jest właśnie rosnące zagrożenie cyberterroryzmem.

Cyberterroryści posiadają coraz większe możliwości techniczne. W przyszłości ofiarami cyberataków może stać się każde państwo, w tym również Polska. O tym, że między światowymi mocarstwami toczy się cyberkonflikt, nie trzeba nikogo przekonywać. Dzieje się tak od momentu, gdy media elektroniczne stały się najważniejszym środkiem komunikacji i źródłem informacji.

Powyższe przykłady wskazują na istotne znaczenie informacji we współczesnym świecie, a także na kreowanie rzeczywistości przez media. Potwierdza się teza, iż ten, kto dysponuje informacją ma władzę, może zatem zapewnić bezpieczeństwo poprzez monitorowanie źródeł, rodzajów i skali zagrożeń, a tym samym, zapobiegać powstawaniu zagrożeń oraz usuwać skutki zagrożeń w cyberprzestrzeni.

Istnieje wiele instytucji zajmujących się ciągłym monitorowaniem w sieci. W razie zagrożenia reagują na wszelkie incydenty, podejmując prewencyjne działania. Na najniższym szczeblu są administratorzy sieci teleinformatycznych. Oprócz rozwiązań o charakterze

[20] P. Zychowicz, *Cyberinwazja na Estonię z rosyjskich komputerów,* „Rzeczpospolita", nr 115, 18.05.2007, s. A1, A6.
[21] J. Bednarek, A. Andrzejewska, *Cyber świat Możliwości i zagrożenia,* Warszawa 2009, s. 35.

techniczno-organizacyjnym, wspomnieć należy o próbie stworzenia uregulowań prawnych, umożliwiających skuteczne przeciwdziałanie, zwalczanie i wykrywanie zagrożenia dla bezpieczeństwa teleinformatycznego państwa. W Polsce, odniesienia do sfery bezpieczeństwa teleinformatycznego znajduje się w kodeksie karnym. Nie został jednak stworzony żaden spójny dokument tworzący podstawy do odpowiedniej interpretacji przestępstw komputerowych, w tym również cyberterroryzmu.

W dobie zachodzących procesów globalizacyjnych i rosnących współzależności pomiędzy państwami oraz podmiotami publicznymi, skuteczność aktywności państwa w wielu dziedzinach zależy od sprawności ochrony informacji, która stanowi zasób strategiczny państwa. Państwo ze swojej strony, powinno zapewnić w obszarze ochrony krytycznej infrastruktury teleinformatycznej w cyberprzestrzeni, daleko idące wsparcie w zakresie budowy systemów zapewniających bezpieczeństwo informacji. Działania te powinny zostać uregulowane w jednolitym akcie prawnym.

ŹRÓDŁA FINANSOWANIA CYBERTERRORYZMU

Terroryści wymuszają na rządach i wpływowych osobach określone dobra, czynią to jednak, krzywdząc innych ludzi, organizując zamachy, porwania, uprowadzenia itp. Trzeba zaznaczyć, że terroryści zwykle przekonani są, iż walczą w słusznej sprawie. Terrorystom zależy na rozgłoszeniu ich działalności i wzbudzeniu strachu w ludziach. Poprzez przemoc, terroryści egzekwują należne im – ich zdaniem – przywileje. Zorganizowanie zamachu terrorystycznego na ogromna skalę i uzyskanie przy tym rozgłosu, wymaga wielkich nakładów finansowych. Brak środków finansowych często sprawia, że zamachy nie dochodzą do skutku lub są nieskuteczne, albo nie są realizowane na taka skalę, jakiej oczekiwaliby terroryści. Niestety, współcześnie duże organizacje terrorystyczne, takie jak Al-Kaida, mają do swojej dyspozycji ogromne zasoby materialne – setki milionów dolarów. Terroryzm to nie tylko ludzie, którzy stoją za zamachami, ale także środki finansowe, technologie i szeroko pojęte wsparcie logistyczne. Terroryści werbują ludzi, organizują sprzęt, czuwają nad łącznością oraz komunikacją. Gdyby terrorystom zabrakło funduszy, musieliby zakończyć swoja działalność. Dlatego, tak istotne jest likwidowanie źródeł wspomagania organizacji terrorystycznych[22].

Terroryści pozyskują środki na swoją działalności ze źródeł legalnych, jak też całkowicie nielegalnych. Często zdarza się, że osoby wspierające terroryzm posiadają dochodowe firmy i wspierają organizacje terrorystyczne zupełnie jawnie – finansują ich działalność. Wśród podmiotów finansujących działalność organizacji terrorystycznych wymienić można:

- osoby prywatne;
- fundacje;
- organizacje charytatywne;

[22] A. Bernard, *Strategia terroryzmu*, Warszawa 1978, s. 32.

- akcje humanitarne;
- kościoły i związki wyznaniowe.

Z kolei do nielegalnych źródeł finansowania działalności terrorystycznej należą:

- przemyt i produkcja narkotyków;
- przemyt towarów na znaczną skalę;
- fałszowanie pieniędzy i kart kredytowych;
- kradzieże i wymuszenia okupów, napady na banki czy konwoje wartości pieniężnych.

Wojciech Jasiński zaznaczył, że użycie środków pochodzących z działalności przestępczej jest możliwe dzięki praniu pieniędzy. Aby osiągnąć cel organizacje posługują się instytucjami finansowymi, legalnymi przedsiębiorstwami handlowymi, spółkami, fundacjami i innymi instytucjami. „Czynniki, takie jak ekonomiczna globalizacja, otwarte granice oraz istna eksplozja technologii informacyjnej, również mają swój udział w zdobywaniu funduszy na zbrodniczą działalność.”[23].

Organizacje terrorystyczne dofinansowywane są przez państwa, organizacje charytatywne, przedsiębiorstwa, jak również osoby prywatne. Przejmujący jest fakt, że taką drogę finansowania jest niezwykle trudno zidentyfikować, ponieważ mamy do czynienia w tym wypadku z postępowaniem odwrotnym do prania pieniędzy, a więc z „brudzeniem” funduszy. W ten sposób pieniądze zgromadzone w legalny sposób, trafiają do organizacji terrorystycznych, które posiadają potem fundusze na przeprowadzanie zamachów.

Kolejnym typem opłacania terrorystów jest jawna działalność gospodarcza. Należy podkreślić, że działające na rzecz organizacji terrorystycznych podmioty gospodarcze, parają się szczególnie handlem nieruchomościami, ropą, złotem, elektroniką, używanymi samochodami i ubraniami, eksportem i importem żywności oraz inwestycjami giełdowymi. W celu pozyskania funduszy, organizacje terrorystyczne przejmują również kontrolę nad legalnymi instytucjami społecznymi. Są to wspomniane wcześniej organizacje charytatywne, które gromadzą pieniądze poprzez:

- zbieranie składek członkowskich lub subskrypcje wydawnictw;
- sprzedaż publikacji;
- organizowanie wydarzeń kulturalnych i społecznych;
- kwestowanie w ramach danej społeczności;
- apele do zamożnych członków społeczności;
- przyjmowanie darowizn.

Jeśli chodzi o organizacje islamskie, nierzadkim zjawiskiem jest zbieranie pieniędzy od członków społeczności muzułmańskiej w czasie spotkań towarzyskich, biznesowych lub poprzez bezpośrednią kwestę w imieniu organizacji charytatywnych. Tak zebrane fundusze trafiają wprost w ręce terrorystów, którzy z kolei mogą w legalny sposób dysponować

[23] *Ibidem*.

zebranymi środkami. Najbardziej zaangażowane w udzielanie wsparcia finansowego owym „organizacjom dobroczynnym", są bogate rody i instytucje, a w szczególności z Arabii Saudyjskiej i niektórych krajów islamskich. W państwach, w których rządy nie posiadają wystarczających środków, by zapewnić obywatelom powszechny system opieki zdrowotnej lub też edukacji, terroryści wykorzystują ten fakt i budują paralelne instytucje publiczne, takie jak szkoły, ośrodki zdrowia i inne instytucje społeczne, robiąc to rzecz jasna w celu ukrycia swoich rzeczywistych zamiarów. W związku z tym źle funkcjonujące państwo jest idealną pożywką dla terroryzmu[24]. Takim państwem jest Sudan, w którym słabość i nieefektywność centralnych władz państwowych oraz trwająca od lat wojna domowa spowodowały, że kraj ten stał się atrakcyjnym azylem dla wielu ugrupowań terrorystycznych.

Głównym źródłem finansowania terrorystów jest jednak działalności przestępcza. Do „prani" pieniędzy i swojej działalności, terroryści wykorzystują różne środki, firmy, technologie i ludzi. Działalność terrorystyczna, wymaga sporych nakładów finansowych.

Informatyzacja banków i obiektów infrastruktury krytycznej państwa, spowodowała ataki hakerskie na wykorzystywane przez nie systemy informatyczne, w celu pozyskania zasobów finansowych. Organizacje terrorystyczne ponoszą koszty nie tylko zakupu odpowiedniego sprzętu informatycznego, ale także, przeszkolenia grup do działania o charakterze kryminalnym w cyberprzestrzeni. Jedną z form działania cyberterrorystów, jest przeprowadzenie bezpośredniej penetracji systemów informatycznych, wykorzystywanych w pracy w banku lub innych instytucjach finansowych.

Organizacje terrorystyczne, do zdobywania środków finansowych, wykorzystują również Internet. FBI poinformowało opinie publiczną, że w latach dziewięćdziesiątych XX w., za pośrednictwem komputerów dokonano kradzieży w przedziale od 3 do 7,5 mld dolarów. Ponadto organizacje terrorystyczne czerpią olbrzymie środki ze skradzionych kart kredytowych, fałszywych przelewów elektronicznych, czy wymuszeń na instytucjach finansowych.

Reasumując, pieniądze zdobyte przez cyberkradzieże, mogą z łatwością posłużyć do finansowania ataków terrorystycznych i działalności propagandowej terrorystów.

MIĘDZYNARODOWA WSPÓŁPRACA W ZWALCZANIU CYBERTERRORYZMU

Bardzo istotnym aspektem w walce z cyberterroryzmem jest współpraca w wymiarze międzynarodowym. Polskie organizacje reagujące na incydenty w cyberprzestrzeni, współpracują bądź należą do międzynarodowych organizacji, które przeciwdziałają zagrożeniom w cyberprzestrzeni. Możemy wyróżnić:

– *NATO Cyber Defence Management Authority*;

[24] A. Bernard, *op. cit.*, s. 38.

- *Cooperative Cyber Defence Centre of Excellence* (CCDCoE), działające w ramach Sojuszu Północnoatlantyckiego;
- *European Network and Information Security Agency* (ENISA), działająca w ramach państw członkowski UE;
- *Forum of Incident Response and Security Teams* (FIRST), organizacja zrzeszająca zespoły CERT (*Computer Emergency Response Team*) z całego świata[25].

Funkcjonowanie w aspekcie międzynarodowym umożliwia szybką wymianę potrzebnych informacji między zespołami, co umożliwia bardzo szybkie reagowanie na kolejne zagrożenia generowane poprzez Internet. Branie udziału w przedsięwzięciach tego typu organizacji, umożliwia także porównywanie rozwiązań technologicznych w zaprzyjaźnionych państwach, jak również powstawanie ujednoliconego systemu zabezpieczeń, który może gwarantować wysoki ich poziom we wszystkich krajach zrzeszonych[26].

Natomiast główne instytucje, odpowiadające za bezpieczeństwo informatyczne w Polsce to:

- Ministerstwo Spraw Wewnętrznych i Administracji;
- Agencja Bezpieczeństwa Wewnętrznego;
- Ministerstwo Obrony Narodowej;
- Służba Kontrwywiadu Wojskowego.

Wszystkie instytucje wchodzące w skład infrastruktury krytycznej państwa mają wzmożony obowiązek dbać o sferę informatyczną swojej działalności, od której zależeć może płynność działań całego państwa. Istnieją również specjalne zespoły, które sprawują opiekę nad sferą cyberbezpieczeństwa, których głównym zadaniem jest podejmowanie niezbędnych działań w sytuacjach zagrożenia systemów teleinformatycznych. Są to:

- CERT.GOV.PL – zespół działający w ramach Agencji Bezpieczeństwa Wewnętrznego, którego zadaniem jest ochrona systemu administracji państwowej;
- Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej;
- CERT-y, działające w ramach operatorów telekomunikacyjnych jak:
  - CERT Polska, działający w ramach Naukowej i Akademickiej Sieci Komputerowej;
  - CERT Orange Polska (Computer Emergency Response Team).

Branie udziału w działaniach podejmowanych przez tego typu organizacje, umożliwia także obserwowanie rozwiązań technologicznych zaprzyjaźnionych państw. Przyczynia się również do powstawania ujednoliconego systemu zabezpieczeń, który może gwarantować wysoki poziom ochrony we wszystkich krajach zrzeszonych w danej organizacji[27].

[25] CERT Polska – zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci.
[26] K. Żukrowska, M. Grącik, *Bezpieczeństwo międzynarodowe*, Warszawa 2006, s. 187.
[27] *Ibidem*, s. 187.

Funkcjonowanie danych instytucji państwowych w strukturach międzynarodowych, umożliwia szybką wymianę potrzebnych informacji między zespołami, co umożliwia bardzo szybkie reagowanie na kolejne zagrożenia generowane w Internecie. Kwestia bezpieczeństwa teleinformatycznego w Polsce, dotyczy obszarów technicznych, prawnych, organizacyjnych i międzynarodowych. Wymaga gigantycznego zaangażowania ze strony instytucji dbających o bezpieczeństwo w sieci oraz władz zarówno w polskiej przestrzeni i na świecie. Zabezpieczenia polskich struktur na wypadek ewentualnego ataku cyberterrorystycznego, są stale doskonalone. Niestety cyberterroryści, także rozwijają nowe rodzaje ataków, przy pomocy najnowszych technologii i mogą przeprowadzać ataki na wybrane obiekty za pomocą sieci teleinformatycznych. Ataki cyberterrorystyczne mają zasięg ogólnoświatowy, gdyż globalna sieć połączeń internetowych oraz komunikacyjnych pozwala na ich koordynowanie i przeprowadzanie ataków ze znacznych odległości. Cechą ataków w cyberprzestrzeni jest niski koszt przygotowania operacji terrorystycznych, natomiast koszty budowania systemów zabezpieczających są bardzo duże. Istnieje małe ryzyko zidentyfikowania sprawcy, ponieważ ataki mogą być przeprowadzane z każdego miejsca na świecie. Najbardziej zagrożonymi obszarami są:

- administracja państwowa,
- systemy bankowe,
- nadzór ruchu w sieciach transportowych,
- systemy energetyczne,
- systemy kontroli lotów[28].

Mówiąc o cyberterroryzmie, w odniesieniu do bezwzględnej ochrony i intensywnego promowania podstawowych swobód[29], na szczególną uwagę zasługują, powstałe w 2008 r., organizacje non-profit *The International Multilateral Partnership Against Cyber Threats* (IMPACT). Działalność IMPACT nastawiona jest na analizę poważnych zagrożeń związanych z cyberprzestrzenią i infrastrukturą krytyczną.

Działa w czterech obszarach:

- całodobowo obserwuje stan cyberprzestrzeni na świecie, publikuje wiadomości na stronie www oraz posiada zamkniętą sieć dla specjalistów (jak Facebook), poprzez system *Global Response Center*;
- prowadzi szkolenia, które koordynują i dostarczają miejsca na przeprowadzenie szkoleń i szerzenia najlepszych praktyk na poziomie ministrów;
- przeprowadza badania nad bezpieczeństwem, które dostarczają ekspertyz, jednocześnie współpracując z ponad dwudziestoma centrami doskonałości oraz uczelniami;
- prowadzi centrum współpracy międzynarodowej, w zakresie cyberprzestępczości[30].

[28] *Ibidem*, s. 189.
[29] *Ibidem.*
[30] *Ibidem.*

Jest niezaprzeczalnym faktem, że cyberterroryzm to istotne zagrożenie w XXI w. W Internecie, agresję należy zwalczać wszelkim sposobami. Przede wszystkim, trzeba zwrócić uwagę użytkownikowi korzystającemu z sieci, na zagrożenia związane z brakiem kontroli cyberprzestrzeni i niebezpieczeństwami związanymi z aktywnością terrorystów w sieci. Ponadto, trzeba pozyskiwać środki na nowoczesny sprzęt dla służb specjalnych, odpowiedzialnych za namierzanie i zwalczanie cyberterroryzmu, przy jednoczesnym ograniczaniu źródła finansowania terrorystów. Konieczne jest utworzenie rozbudowanej strategii, dotyczącej wielu aspektów ochrony sieci teleinformatycznych, która pozwoli zminimalizować skutki ataków cyberterrorystów. Ważną rolę w zwalczaniu cyberterroryzmu odgrywają strategie bezpieczeństwa większości państw i organizacji międzynarodowych, w tym NATO i UE. Państwa członkowskie Sojuszu Północnoatlantyckiego, przyjęły na szczycie w Lizbonie w 2010 r. nową koncepcję strategiczną[31], wskazując na ataki cybernetyczne, jako jedno z istotnych zagrożeń bezpieczeństwa dla państw członkowskich Sojuszu Północnoatlantyckiego. Opracowana została również nowa strategia bezpieczeństwa cybernetycznego Unii Europejskiej[32]. Obejmuje ona kwestie związane z cyberprzestrzenią pod kątem spraw wewnętrznych, polityki zagranicznej, wymiaru sprawiedliwości i rynku wewnętrznego.

Obecnie istnieje duże ryzyko wystąpienia ataku cyberterrorystycznego wymierzonego w infrastrukturę krytyczną państwa. Zadaniem instytucji odpowiadających za bezpieczeństwo informatyczne, jest umiejętność wykrywania zamachów w cyberprzestrzeni i zabezpieczenia się przed ich oddziaływaniem na podsektory infrastruktury krytycznej. W Polsce, zasygnalizowane zostało bezpieczeństwo w cyberprzestrzeni, w opracowanej w 2007 r. *Strategii bezpieczeństwa narodowego RP*. Kolejnym dokumentem, jaki zasygnalizował nowe zagrożenia, była *Strategia rozwoju systemu bezpieczeństwa narodowego RP w latach 2012-2022* oraz *Strategia obronności RP*. W sferze militarnej, w 2008 r., Minister Obrony Narodowej wydał decyzję, w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej. Utworzony został System Reagowania na Incydenty Komputerowe, którego koordynatorem jest obecnie Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

W maju 2008 r. w Brukseli, szefowie Sztabów Generalnych Estonii, Hiszpanii, Litwy, Łotwy, Niemiec, Słowacji i Włoch, podpisali Memorandum o utworzeniu w Tallinie Centrum Kompetencyjnego ds. Obrony Teleinformatycznej (T*he Concept for Cooperative Cyber Defense Centre of Excellence* – CCDCOE). W listopadzie 2011 r., do Centrum przystąpiła Polska oraz Stany Zjednoczone.

[31] XXII szczyt NATO w Lizbonie odbył się w dniach 19-20 listopada 2010 r. w Portugalii. Summit meetings of Heads of State and Government Lisbon, Portugal-Topics (ang.)nato.int. (18.11.2010).
[32] *EU International Cyberspace Policy*, http://eeas.europa.eu/policies/eu-cyber-security/index_pl.htm (07.02.2013).

W 2011 r. amerykańska administracja, zaprezentowała międzynarodową strategię dla cyberprzestrzeni. Amerykanie zaproponowali wzmocnienie współpracy z organizacjami międzynarodowymi i państwami. Niestety, problem braku spójnych rozwiązań systemowych i prawnych w zapewnieniu bezpiecznego działania w cyberprzestrzeni, nie został rozwiązany.

PODSUMOWANIE

Cyberprzestrzeń staje się „układem nerwowym" państwa. Jest to system sterowania krajem, złożony z tysięcy połączonych ze sobą systemów komputerowych, które pozwalają działać państwowym podsektorom infrastruktury. Cyberprzestrzeń wraz z Internetem stworzyła istotne zależności, które w nieprzewidywalny i groźny sposób zmieniają swoją naturę. Systemy teleinformatyczne mają wiele słabych punktów, które mogą umożliwić przeprowadzenie cyberataku obniżając w istotny sposób bezpieczeństwo informacyjne państwa. Zatem cyberprzestrzeń stała się nowym obszarem, w którym należy dokonać licznych zmian w pragmatyce i prawno-organizacyjnym wymiarze funkcjonowania systemów zapewniających bezpieczeństwo w sieci, w skali globalnej i lokalnej.

Powyższe rozważania pozwalają na stwierdzenie, że na cyberzagrożenia należy spojrzeć wieloaspektowo, gdyż są liczne i złożone. Ochrona sieci i systemów teleinformatycznych wymaga specjalistycznej wiedzy i doświadczenia. Cyberprzestrzeń stanowi wyzwanie dla bezpieczeństwa narodowego i publicznego. W większości krajów infrastruktura o znaczeniu krytycznym jest podłączona do Internetu, dlatego należy pamiętać o jej właściwej ochronie. Najbardziej zagrożone systemy teleinformatyczne, są w sektorze prywatnym. Zaprezentowane informacje, należy traktować, jako zarys problemów związanych ze szkodliwymi działaniami w cyberprzestrzeni.

BIBLIOGRAFIA

Bednarek Józef, Anna Andrzejewska (red.). 2009. *Cyber świat. Możliwości i zagrożenia,* Warszawa, Wydawnictwo Żak.

Bernard Andrzej. 1978. *Strategia terroryzmu*. Warszawa: Wydawnictwo Ministerstwa Obrony Narodowej.

Bógdał-Brzezińska Agnieszka, Marcin Gawrycki. 2003. Cyberterrozryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warszawa: Fundacja Studiów Międzynarodowych, Oficyna Wydaw. ASPRA-JR.

Gogołek Włodzimierz. 2007. Manipulacja w sieci W Manipulacja, media, edukacja. Wydawnictwo Adam Marszałek.

EU International Cyberspace Policy. http://eeas.europa.eu/policies/eu-cyber-security/index_pl.htm.

Podraza Andrzej, Paweł Potakowski, Krzysztof Wiak. 2013. Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna. Warszawa: Wydawnictwo Difin.

Sienkiewicz Piotr. 2009. Terroryzm w cybernetycznej przestrzeni W Cyberterroryzm – nowe wyzwania XXI wieku. Warszawa: Wyższa Szkoła Informatyki, Zarządzania i Administracji.

Sienkiewicz Piotr. 2005. Ucieczka od wolności w globalnym społeczeństwie informacyjnym, Szczecin.
Szubrycht Tomasz. 2005. „Cyberterroryzm jako nowa forma zagrożenia terrorystycznego". Zeszyty Naukowe Akademii Marynarki Wojennej". 1(160): 173–187.
Wójcik Jerzy Wojciech. 1999. Przestępstwa komputerowe. Cześć I. Fenomen cywilizacji. Warszawa: Centrum Informacji Menedżera.
Zychowicz P. 2007. „Cyberinwazja na Estonię z rosyjskich komputerów", Rzeczpospolita 115 (7712) : A1, A6.
Żukrowska Katarzyna, Małgorzata Grącik. 2006. Bezpieczeństwo międzynarodowe: teoria i praktyka. Warszawa: Szkoła Główna Handlowa.