Zbigniew CIEKANOWSKI[1]

Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej[2]

zbigniew@ciekanowski.pl

Henryk WYRĘBEK[3]

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach[4]

Wydział Humanistyczny, INSiB

Henryk.Wyrebek@uph.edu.pl

WSPÓŁCZESNE TECHNOLOGIE INFORMATYCZNE – SZANSE I ZAGROŻENIA

ABSTRAKT: Dynamiczny rozwój informatyki spowodował że człowiek jest coraz bardziej uzależniony od komputerów i pochodnych urządzeń. Jeszcze na początku lat 80. XX wieku komputer był jedynie narzędziem, którego głównym przeznaczeniem było wykonywanie skomplikowanych obliczeń naukowych lub użycie w celach militarnych. Obecnie urządzania teleinformatyczne towarzyszą człowiekowi praktycznie w każdym aspekcie jego życia, począwszy od wykonywania zadań służbowych, na relaksie i utrzymywaniu kontaktów ze znajomymi kończąc. Technologie informatyczne zdominowały sposób zarządzania państwem wraz z jego kluczowymi elementami, do których należy m.in. infrastruktura krytyczna. Wraz z rosnącym uzależnieniem funkcjonowania społeczeństwa od technologii informatycznych rosną również zagrożenia płynące z ataków w cyberprzestrzeni. Fakt ten wykorzystują organizacje terrorystyczne, co owocuje pojawieniem się nowego, groźnego dla świata zagrożenia – cyberterroryzmu.

SŁOWA KLUCZOWE: cyberterroryzm, cyberatak, cyberprzestrzeń

MODERN INFORMATION TECHNOLOGIES – OPPORTUNITIES AND THREATS

ABSTRACT: The dynamic development of information technology has caused that man is becoming more and more dependent on computers and related devices. At the beginning of the 1980s computer was only a tool which main purpose was to perform complex scientific calculations or

[1] Zbigniew Ciekanowski – dr hab. profesor Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej. Zainteresowania naukowe skupiają się zarówno wokół zagadnień związanych z zarządzaniem zasobami ludzkimi, zarządzaniem kryzysowym jak i z szeroko rozumianym bezpieczeństwem. Autor kilkudziesięciu książek i ponad stu opracowań krajowych i zagranicznych z powyższej problematyki..

[2] Pope John Paul II State School Of Higher Education in Biała Podlaska.

[3] Henryk Wyrębek – dr hab. profesor Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Zainteresowania naukowo-badawcze koncentrują się wokół problemów interdyscyplinarnych: nauki o zarządzaniu oraz nauki o bezpieczeństwie i obronności. Autor ponad 100 publikacji naukowych.

[4] Siedlce University of Natural Sciences and Humanities.

use in military purposes. Currently, the telecommunication devices accompany man in almost every aspect of life, starting with performing the work tasks, relaxation and maintaining contacts with friends. Information technology dominated the state management with its key elements, one of which is, among others, critical infrastructure. With the growing addiction of society from information technology, also threats from the attacks in cyberspace grow. This fact is used by terrorist organizations, which results in the emergence of a new, dangerous for the world, threat – cyber-terrorism.

KEYWORDS: cyberterrorism, cyberattack, cyberspace

WPROWADZENIE

Z uwagi na rosnące znaczenie systemów teleinformatycznych wykorzystywanych obecnie przez społeczeństwa na całym świecie, a także wchodzących w skład państwowej infrastruktury krytycznej, współczesna doktryna prawna zaczęła interesować się legalnym definiowaniem cyberprzestrzeni. Było to spowodowane ilością specyficznych działań podejmowanych przez ludzi za pośrednictwem komputerów oraz sieci. Konieczne było rozpoznanie nowego cyfrowego środowiska, które nadało zupełnie nowy kształt zawieraniu umów cywilnoprawnych, dokonywaniu czynności administracyjnych, ale i popełnianiu nowoczesnych form przestępczości. Wiele spośród znanych dotychczas czynności prawnych wyraźnie zmieniło się w cyberprzestrzeni, podczas gdy inne dopiero dzięki niej powstały. Poniżej zaprezentowano krótki przegląd definicji cyberprzestrzeni przyjętych na gruncie rządowych dokumentów różnych krajów, w tym definicję cyberprzestrzeni zapisaną w polskiej ustawie, a dalej omówiono, w jaki sposób przyjęcie określonego sposobu charakteryzowania cyberprzestrzeni wpływa na rozumienie tego, czym jest bezpieczeństwo cyberprzestrzeni. Jedną z najbardziej znanych i powszechnie cytowanych jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika terminologii wojskowej oraz powiązanej, według której cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery”[5].

CYBERTERRORYZM

Socjologicznym rozwinięciem koncepcji cyberprzestrzeni jako obszaru komunikacji o światowym zasięgu jest nazwanie jej Nową Wieżą Babel. Cyberprzestrzeń nie tylko zbliża, ale wręcz powoduje mieszanie się kultur, gromadząc idee oraz informacje pochodzące z całego świata. Stwierdzenie, że wyłączenie się z niej spowoduje izolację jednostek, spadek konkurencyjności przedsiębiorstw oraz podrzędność krajów, wskazuje na ogromne znaczenie tego obszaru, służącego uczestniczeniu w nowoczesnej, globalnej społeczności. Innym, ale tak samo interesującym określeniem użytym w strategii francuskiej jest nazwanie cyberprzestrzeni Nowymi

[5] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni* [w:] „Przegląd Bezpieczeństwa Wewnętrznego” nr 9.

Termopilami, gdzie na co dzień dochodzi do niewidocznych w materialnym świecie starć, nie tylko zaburzających poprawne funkcjonowanie systemów czy naruszających dobra prawne ich użytkowników, lecz także mogących zagrozić ludzkiemu życiu. Może się tak zdarzyć, jeśli na przykład zostaną zaatakowane systemy odpowiedzialne za szeroko rozumiane bezpieczeństwo publiczne.

Pomimo wielokrotnie podejmowanych w literaturze przedmiotu prób zdefiniowania cyberterroryzmu, do tej pory specjaliści nie byli wstanie wypracować jednolitej, powszechnie wykorzystywanej definicji tego zjawiska. Dodatkowo niektórzy badacze uważają, iż zamiast tworzyć na siłę nowe pojęcie określające cyberterroryzm, należałoby wykorzystywać znacznie szersze pojęcie jakim jest walka informacyjna[6].

Do pierwszych prób określenia cyberterroryzmu, jako połączenia terroryzmu i cyberprzestrzeni można zaliczyć definicję podaną w latach 80. XX wieku przez B. Collina. Stwierdził on, iż „cyberterroryzm to świadome wykorzystanie systemu teleinformatycznego, sieci komputerowej lub jej części składowych w celu wsparcia bądź też ułatwienia przeprowadzanie akcji terrorystycznej”[7].

Z kolei M. Łapczyński zaznacza, iż termin ten pojawił się już w 1979 r.[8], kiedy szwedzkie Ministerstwo Obrony umieściło go w raporcie o zagrożeniach komputerowych, rekomendując by rząd zaangażował się w monitorowanie, zarówno publicznych, jak i prywatnych sieci komputerowych[9]. Natomiast A. Bógdał-Brzezińska i M. Gawrycki uważają, iż cyberterroryzm jest jednym z najbardziej nieprzewidywalnych sposobów oddziaływania grup zorganizowanych na stabilność działania struktur państwa. Jak zauważają najbardziej zagrożonymi systemami są systemy określane mianem infrastruktury krytycznej, do których należy zaliczyć m.in. telekomunikację, systemy energetyczne, finansowe czy systemy służb ratowniczych[10].

Z kolei amerykańska ekspertka do sprawy cyberbezpieczeństwa D.E. Denning uważa, iż cyberterroryzm jest połączeniem cyberprzestrzeni oraz terroryzmu[11]. Polega on na nielegalnych atakach oraz groźbach ich wykonania wobec komputerów, sieci komputerowych oraz informacjom przez nie przechowywanym w celu zastraszenia lub wymuszenia na rządach państw oraz ich społeczeństwach celów politycznych lub społecznych. Ponadto Denning uważa, iż aby zaliczyć konkretny atak do kategorii ataków cyberterrorystycznych powinien on skutkować przemocą przeciwko ludziom lub mieniu, bądź też wyrządzone szkody powinny skutecznie wywołać poczucie strachu.

[6] A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 70.
[7] W.L. Tafoya, *Cyber Terror*, [w:] „Biuletyn służb porządku publicznego FBI”, październik 2011.
[8] http://konflikty.wp.pl/kat,1020225,title,Czy-grozi-nam-cyberterroryzm,wid,11640989,wiadomosc.html (10.10.2016).
[9] A. Adamski, *Cyberterroryzm*, [w:] V. Kwiatkowska-Darul (red.), *Terroryzm*, Toruń 2002, s. 113-121.
[10] A. Bógdał-Brzezińska, M. Gawrycki, *op. cit.*, s. 70.
[11] *Ibidem*, s. 198.

Natomiast zgodnie z przyjętą definicją przez Narodowe Centrum Ochrony Infrastruktury USA (*National Infrastructure Protection Plan* – NIPC[12])

> *cyberterroryzm jest atakiem kryminalnym popełnionym przy użycia komputera oraz sieci telekomunikacyjnych, powodującym użycie siły, zniszczenie bądź też przerwanie usług w celu wywołania poczucia strachu, poprzez wytworzenie zamieszania i wywołania niepewności w określonej części populacji, w celu wpływania na rządy oraz ludność w sposób, mogący wykorzystać ich reakcje dla osiągnięcia z góry określonych celów politycznych, społecznych, ideologicznych bądź też głoszonego przez terrorystów programu*[13].

Interesujące określenie cyberterroryzmu przestawił w swoim artykule E. Lisocki:

> *Cyberterroryzm jest to przemyślany politycznie lub militarnie motywowany atak albo groźba ataku na systemy i sieci teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno – militarnych działań. Cyberterroryzm jest to również świadome wykorzystanie sieci teleinformatycznych oraz globalnej sieci Internet przez organizacje terrorystyczne, ruchy narodowo – wyzwoleńcze oraz ruchy powstańcze do propagandy, rekrutacji on-line, komunikowania się, mobilizacji, zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej. Cyberatak może być przeprowadzony jako część składowa większej polityczno – militarnej akcji lub samodzielnego ataku*[14].

Na tej podstawie autor wyróżnił dwie formy cyberterroryzmu – państwowy i niepaństwowy.

W powszechnym rozumieniu cyberterroryzm państwowy polega na stosowaniu przez dane państwo zakamuflowanej przemocy fizycznej (w odróżnieniu od polityki terroru), poprzez działalność funkcjonariuszy służb specjalnych lub też grupy tworzonej *ad hoc* ewentualnie najemników, które nie są bezpośrednio powiązane ze strukturami bezpieczeństwa państwa. Terroryzm państwowy może być stosowany jako instrument polityki wewnętrznej wobec opozycji, mniejszości etnicznych itp., jak również polityki zagranicznej – występując przeciwko obywatelom, instytucjom i infrastrukturze obcego państwa. Do form terroryzmu państwowego w cyberprzestrzeni można zaliczyć następujące elementy:

- wojnę informatyczną;
- walkę informacyjną;
- walkę z terroryzmem;
- konflikty lokalne;
- walkę z organizacjami terrorystycznymi;
- walkę z przestępczością;

[12] US National Infrastructure Protection Centre.
[13] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (22.10.2016).
[14] E. Lisocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Gdańsk 2009, s. 58.

– działalność szeroko rozumianych służb ochrony państwa[15].

Z kolei cyberterroryzm niepaństwowy można określić jako działalność organizacji terrorystycznych prowadzony w sposób niezależny od struktur państwowych. Organizacje te mogą stanowić część większej struktury o zasięgu międzynarodowym lub też współpracować z innymi organizacjami terrorystycznymi przy zachowaniu swojej autonomii. Do form takiego cyberterroryzmu możemy zaliczyć: działalność organizacji terrorystycznych, ruchów narodowo – wyzwoleńczych oraz ruchów powstańczych z wykorzystaniem osób takich jak:

– przestępcy;
– hakerzy;
– frustraci;
– crackerzy;
– haktywiści;
– szpiedzy[16].

Obecnie cyberterroryzm staje się coraz częściej stosowanym narzędziem przemocy. Terroryści korzystają z Internetu prawdopodobnie już od chwili, gdy sieć ta pojawiła się na świecie. Oczywiście, jak często i w jakim zakresie, nie wiadomo, gdyż śledzeniem ich poczynań w Internecie zajmują się organizacje, których działalność jest utajniona. W ostatnim czasie pojawiły się jednak informacje, że wzrosło zagrożenie tzw. wojną cybernetyczną. Nie mniej jednak zdaniem analityków FBI tego typu wojna, czy ataki terrorystyczne na sieć internetową nie stanowią obecnie realnego zagrożenia. Wynika to z pewnej sprzeczności: infrastruktura informatyczna, mogąca być przedmiotem ataku terrorystycznego, jest przez terrorystów intensywnie wykorzystywana. Wiadomo np., że Al-Kaida wykorzystuje Internet do działalności handlowej, jak i do planowania działań terrorystycznych.

Prowadząc kwerendę literatury przedmiotu, można również natknąć się na próby podziału ataków cyberterrorystycznych ze względu na metody przeprowadzenia akcji. Wyróżnia się tutaj dwa typy akcji, które mogą się wzajemnie uzupełniać: samodzielne akcje lub akcje będące bardziej złożonego planu. Pierwszym typem są ataki fizyczne na systemy teleinformatyczne prowadzone tradycyjnymi metodami. Pierwsze ataki tą metodą były przeprowadzone już w latach 70. ubiegłego wieku. Włoskie Czerwone Brygady 27-razy obierały za cel firmy elektroniczne i komputerowe. Członkowie brygad uważali, że niszcząc systemy teleinformatyczne uderzają w samo serce państwa. Na bazie tych doświadczeń specjaliści wykazują, iż terroryści nie muszą znać się na informatyce. Potrzebują oni jedynie informacji, gdzie i jak uderzyć na infrastrukturę sieciową, aby sparaliżować życie w krajach wysoko zinformatyzowanych. Z drugiej strony w klasycznym" ujęciu akcja cyberterrorystyczna jest atakiem mającym miejsce w cyberprzestrzeni i polegającym na zaatakowaniu oprogramowania przeciwnika.

CYBERPRZESTRZEŃ

[15] Z. Ciekanowski, *Zwalczanie terroryzmu w Polsce*, Jarosław 2015, s. 86.
[16] Z. Ciekanowski, S. Wojciechowska-Filipek, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni Jednostki – Organizacji – Państwa.* Warszawa 2016, s. 98.

Z uwagi na rosnące znaczenie systemów teleinformatycznych wykorzystywanych obecnie przez społeczeństwa na całym świecie, a także wchodzących w skład państwowej infrastruktury krytycznej, współczesna doktryna prawna zaczęła interesować się legalnym definiowaniem cyberprzestrzeni. Było to spowodowane ilością specyficznych działań podejmowanych przez ludzi za pośrednictwem komputerów oraz sieci. Konieczne było rozpoznanie nowego cyfrowego środowiska, które nadało zupełnie nowy kształt zawieraniu umów cywilnoprawnych, dokonywaniu czynności administracyjnych, ale i popełnianiu nowoczesnych form przestępczości. Wiele spośród znanych dotychczas czynności prawnych wyraźnie zmieniło się w cyberprzestrzeni, podczas gdy inne dopiero dzięki niej powstały. Poniżej zaprezentowano krótki przegląd definicji cyberprzestrzeni przyjętych na gruncie rządowych dokumentów różnych krajów, w tym definicję cyberprzestrzeni zapisaną w polskiej ustawie, a dalej omówiono, w jaki sposób przyjęcie określonego sposobu charakteryzowania cyberprzestrzeni wpływa na rozumienie tego, czym jest bezpieczeństwo cyberprzestrzeni. Jedną z najbardziej znanych i powszechnie cytowanych jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika terminologii wojskowej oraz powiązanej, według której cyberprzestrzeń jest globalną domeną środowiska informacyjnego składającą się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych.

Należy wyjaśnić czym jest cyberprzestrzeń. Początkowo termin ten był wykorzystywany jedynie w powieściach W. Gibsona, twórcy cyberpunku[17], w celu określenia wirtualnej rzeczywistości. W swojej książce, zatytułowanej „Neuromancer" Gibson określił cyberprzestrzeń, jako

> *konsensualną halucynację doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, w tym przez dzieci nauczane pojęć matematycznych (…). Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność… Świetlne linie przebiegały bez przestrzeń umysłu, skupiska i konstelacje danych*[18].

Przedstawiona definicja oczywiście nie odnosi się do dzisiejszych realiów, jednak oprócz zapoczątkowania debaty na temat cyberprzestrzeni, określiła podstawowe pojęcia jakimi są: światowy zasięg, łączenie wszystkich elementów w jedną spójną bazę danych, złożoność oraz niemożność odniesienia cyberprzestrzeni do fizyczności rzeczywistego świata.

Obecnie coraz więcej państw oraz organizacji międzynarodowych rozważa zamieszczenie definicji cyberprzestrzeni w aktach normatywnych. Spowodowane jest to nie tylko rosnącym znaczeniem systemów teleinformatycznych dla społeczeństwa, ale głównie ze względu na oparcie na nich infrastruktury krytycznej państwa.

W literaturze przedmiotu, jedną z najczęściej wykorzystywanych definicji cyberprzestrzeni jest stworzona przez Amerykański Departament Obrony. Opisana w Słowniku Terminologii Woj-

[17] Nurt w literaturze science-fiction oraz kinematografii, który skupia się na ludziach i otaczającej ich zaawansowanej technologii komputerowej i informacyjnej, niekiedy połączony z różnego rodzaju zamieszaniem w społeczeństwie (np. stan wojenny) (https://pl.wikipedia.org/wiki/cyberpunk) (22.10.2016).

[18] W. Gibson, *Neuromancer,* Katowice 2009.

skowej i Powiązanej definicja głosi, iż cyberprzestrzeń jest „globalną domeną środowiska teleinformatycznego, składająca się z zależnych od siebie sieci tworzącą infrastrukturę IT oraz przechowywanych w nich danych, wliczając w to Internet, sieci telekomunikacyjne, systemy komputerowe wraz z tworzącymi je procesorami i kontrolerami”[19].

Z kolei w przyjętej w 2015 r. Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej określono, że cyberprzestrzeń to

> *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń teleinformatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami*[20].

Warto zaznaczyć, iż pojęcie to zostało rozwinięte do miana cyberprzestrzeni RP, będącej w obrębie państwa oraz miejscach, w których funkcjonują przedstawicielstwa RP, wliczając w to placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią Polski, będące pod jej jurysdykcją.

TECHNIKI STOSOWANE PRZEZ CYBERTERRORYSTÓW

Pomysłowość terrorystów planujących ataki terrorystyczne wykracza daleko poza racjonalne myślenie. Do 11 września 2001 r. większość osób utożsamiała narzędzia, którymi mogą posługiwać się terroryści z bronią konwencjonalną i materiałami wybuchowymi. Ataki na WTC oraz Pentagon pokazały, iż terroryści są w stanie wykorzystać niemal każdą dostępną rzecz czy przedmiot, również duże samoloty pasażerskie, aby osiągnąć założone cele. Podobnie jest w cyberprzestrzeni. Od momentu pojawienia się ogólnie dostępnych sieci teleinformatycznych, atakujący wytworzyli niemal niewyobrażalną ilość narzędzi i technik, które są wykorzystywane w atakach na komputery i sieci teleinformatyczne, jak również w koordynowaniu konwencjonalnych ataków.

Ciągła zmienność panująca w świecie teleinformatycznym nie pozwala obecnie na wymienienie wszystkich potencjalnych zagrożeń dla urządzeń teleinformatycznych. Od początku lat 80. XX wieku specjaliści ds. bezpieczeństwa komputerowego byli świadkami masowego wysypu nowych sposobów do przełamania zabezpieczeń lub też oddziaływania na sposób działania danej sieci. Dodatkowym utrudnieniem w próbie określenia wszystkich ataków w cyberprzestrzeni był fakt, iż dana metoda może być rozwijana i modyfikowana powodując wytwarzanie się podgrup. Poniżej przedstawiono podstawowe pojęcia związane z cyberterroryzmem i nowymi technologiami:

[19] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (22.10.2016).
[20] https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html (22.10.2016).

- backdoor – umyślne tworzeniu przez programistów „furtek" w aplikacjach, które w późniejszym okresie umożliwiają dostęp do komputera ofiary poprzez ich wykorzystanie w zainstalowanym oprogramowaniu;
- backdoor-santas – technika polegająca na pozyskiwaniu poufnych danych użytkownika pod pozorem wykonywania pożytecznych czynności;
- bakteria – złośliwe oprogramowania wpływające pośrednio na uszkodzenie danych. Jego działanie polega na ciągłej reprodukcji;
- bomba logiczna – fragment kodu programu komputerowego, bardzo często wirusa zawartego w zwykłym programie lub robaka, umieszczonego w nim bez wiedzy użytkownika;
- bomba pocztowa – metoda wykorzystująca protokoły pocztowe, polegająca na zaśmieceniu skrzynki pocztowej ofiary bardzo dużą ilością wiadomości;
- botnet – sieć zawirusowanych i przejętych komputerów zarządzanych przez serwer twórcy wirusa/bota;
- cookies – jedna z podstawowych technik zbierania informacji o użytkownikach komputerów;
- cracking – metoda wykorzystująca istniejące luki w systemie w celu złamania jego zabezpieczeń;
- dialery – metoda polegające na podmianie telefonicznego numeru dostępowego użytkownika najczęściej na numery wysokopłatne;
- DoS/DDos (*Denial of Service*) – atak na system komputerowy bądź usługę sieciową którego celem jest zakłócenie jej działania;
- expolit – złośliwe oprogramowanie pozwalające na bezpośredni dostęp do komputera ofiary. W tym celu wykorzystywana jest luka w oprogramowaniu znajdującym się na komputerze będący celem ataku;
- hijacking – atak, który polega na przechwyceniu transmisji odbywającej się pomiędzy dwoma komputerami, umożliwiając uzyskanie dostępu do szczególnie chronionych programów oraz danych;
- inżynieria społeczna – metoda ataku polegająca na wykorzystaniu niekompetencji osób oraz ich niewiedzy w zakresie działania systemów komputerowych. Stanowi najczęściej uzupełnienie ataków softwareowych;
- keylogger – oprogramowanie służące do przechwytywania wprowadzanych danych za pomocą klawiatury;
- koń trojański – potocznie nazywany trojanem – programy pozwalające na wykonanie niepożądanego i nieprzewidzianego przez użytkownika działania, np. usunięcie plików, partycji dysku twardego, czy też przekazywać dane do twórcy programu bez wiedzy użytkownika;

- mobler – robak międzyplatformowy, technika oparta na przekazywaniu wiadomości SMS, zapisywaniu informacji o wiadomościach oraz rejestrze połączeń, zdalnym podsłuchiwaniu i łączeniu rozmów konferencyjnych oraz uaktywnianiu usług lokalizacyjnych;
- phishing – metoda oparta głównie na inżynierii społecznej, polegającej na podszywaniu się pod instytucje celem kradzieży danych wrażliwych.
- Robak – złośliwe oprogramowanie, którego celem jest jak najszybsze rozprzestrzenienie się po sieci. Po zagnieżdżeniu się w danym systemie, zaczyna się zachowywać jak wirus, bakteria lub trojan. W odróżnieniu do wirusów, robak nie wymaga uaktywnienia po stronie użytkownika komputera. Wykorzystuje słabe punkty serwerów pocztowych, stron WWW, programów obsługujących czaty internetowe oraz innych popularnych aplikacji;
- rootkit – oprogramowanie maskujące obecność w systemie innych aplikacji zaliczanych do grona złośliwego oprogramowania;
- skanowanie – atak polegający na sondowaniu atakowanego systemu poprzez sprawdzanie jego adresów sieciowych oraz portów sieciowych;
- skimming – technika wykorzystywana w celu nielegalnego skopiowania danych zawartych w pasku magnetycznym karty oraz danych zawartych w chipie znajdującym się na karcie;
- sniffing – technika śledzenia ruchu w sieci. Specjalistyczne oprogramowanie przechwytuje wiadomości przekazywane za pomocą sieci i kopiuje ich treść na dysk twardy atakującego;
- SPAM – w najprostszy sposób metodę tę można wyjaśnić jako niepożądana przez odbiorców wiadomość tekstowa. Główną cechą tej metody jest wysyłanie masowej ilości wiadomości do możliwie największej grupy odbiorców;
- spoofing – technika polegająca na podszyciu się pod dane urządzenie w sieci, w celu dokonania włamania do systemu lub też oszustw komputerowych;
- spyware – programy stosowane w celu prowadzenia szpiegostwa cybernetycznego. Podczas instalacji zainfekowanego programu, bez wiedzy użytkownika, aktywowana jest kolejna instalacja spyware;
- wabbit – złośliwe oprogramowanie, którego zadaniem jest powielanie dowolnego pliku znajdującego się na dysku komputera w celu wyczerpania pamięci użytkowej systemu;
- wirus – typ złośliwego oprogramowania w postaci samoreplikującego się kodu. Jego działanie polega na uszkodzeniu danych, programów czy też modyfikacji działania systemu[21].

W dzisiejszych czasach zdobycze nowoczesnych technologii stały się istotnym elementem egzystencji człowieka. Codziennie miliony ludzi korzystają z komputerów oraz smartfonów. Wraz z upowszechnieniem się wykorzystania komputerów i sieci teleinformatycznych w gospodarstwach domowych, komputer przestał być przestał być postrzegany jedynie jako narzędzie pracy. Obecnie jest potężnym narzędziem multimedialnym, za pomocą którego możemy korzystać z Internetu, oglądać filmy, grać w gry komputerowe. Ponadto dzięki Internetowi ludzie mają możliwość ciągłego pozostawania w kontakcie z innymi. Należy jed-

[21] A. Bógdał-Brzezińska, M. Gawrycki. *op.cit.*, s. 98.

nak zaznaczyć, iż pomimo wykorzystania urządzeń teleinformatycznych w celu zaspokojenia prywatnych potrzeb człowieka są one także narzędziami niezbędnymi do poprawnego funkcjonowania infrastruktury krytycznej państwa. Komputery działające w ramach specjalnie zaprojektowanych sieci są również kluczowym elementem dzisiejszych systemów odpowiedzialnych za automatyzację i obsługę procesów produkcyjnych, kontroli lotów czy też systemów zaopatrywania w wodę i żywność. Komputery stanowią również podstawę systemów odpowiedzialnych za zapewnienie ciągłości działania administracji publicznej, ochrony zdrowia i ratownictwa.

ZAGROŻENIA DLA SYSTEMÓW ZAOPATRZENIA W ENERGIĘ, SUROWCE NERGETYCZNE I PALIWA

Obecnie trudno sobie wyobrazić życie bez energii elektrycznej, czy też paliw, bowiem rozwój cywilizacji jest niemal całkowicie uzależniony od energii elektrycznej, surowców energetycznych i innych nośników. Zapewnienie bezpieczeństwa energetycznego jest jednym z podstawowych zadań każdego z państw. W Polsce, zgodnie z zapisami Ustawy z dnia 10 kwietnia 1997 r. „Prawo energetyczne" (Dz, U, 2015 r. poz. 2365), bezpieczeństwo energetyczne jest stanem gospodarki pozwalającym na pokrycie perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska. Polska jest w stanie osiągnąć ten stan poprzez dywersyfikację źródeł paliw, rozwój infrastruktury związanej z pozyskiwaniem energii ze źródeł odnawialnych, wykorzystanie zdolności krajowych złóż surowców – głównie węgla, umożliwiając nieprzerwalną pracę krajowych systemów energetycznych, nawet w przypadku przerwania dostaw z jednego źródła.

Jednym z pierwszych ataków przeprowadzonych w sektorze energetycznym było włamanie do Departamentu Energetyki USA. W latach 80. XX wieku grupa „hakerów z Hanoweru" włamała się do sieci teleinformatycznej tego departamentu i przez kilka miesięcy analizowała zawarte w niej informacje. Zleceniodawcą tego ataku było najprawdopodobniej KGB.

Obecnie liczba ataków na sektor energetyczny rośnie lawinowo, co znajduje swoje potwierdzenie w odpowiednich raportach tworzonych przez zainteresowane instytucje. Przykładowo działający przy Amerykańskim Departamencie Bezpieczeństwa Wewnętrznego, Zespół ds. Reagowania na Incydenty Komputerowe w Przemysłowych Systemach Kontroli ICS-CERT[22] wykazał, iż w 2011 r. przeprowadzono 198 cyberataków na infrastrukturę przemysłową w tym w szczególności na sektor energetyczny[23]. Jednym z najpoważniejszych ataków cybernetycznych był blackout z 2003 r., który dotknął USA. Brak zasilania objął wówczas swym zasięgiem północnowschodnie i środkowe stany, w których mieszka ponad 50 milionów osób. Za powód awarii pierwotnie uznano błąd programistyczny w systemie sterującym pracą urzą-

[22]Ang.: *The Industrial Control Systems Cyber Emergency Response Team*.
[23]A. Kozłowski, *Cyberbezpieczeństwo infrastruktury energetycznej*, [w:] „FAE Policy Paper" 7/2014.

dzeń korporacji FirstEnergy w Ohio[24]. Jednakże nowe światło na tę sprawę rzucili w 2007 r. Tom Donahue oraz Tim Bennett[25], którzy wykazali, iż blackout z 2003 r. został spowodowany przez chińskich hackerów, powiązanych z Chińską Armią Ludowo-Wyzwoleńczą, którzy przejęli kontrolę nad systemem SCADA zastosowanym w FirstEnergy.

Kolejnym spektakularnym i najszerzej opisywanym przez mass-media był atak przeprowadzony za pomocą wirusa Stuxnet. W 2009 r. przeprowadzono akcję, najprawdopodobniej przez Amerykanów i Izraelczyków, której celem było zniszczenie wirówek wykorzystywanych przez Iran do wzbogacania uranu. Należy podkreślić, iż placówka naukowa w Natanaz, która byłą celem ataku nie była podłączona do sieci Internet. Problem ten został rozwiązany poprzez wprowadzenie złośliwego oprogramowania za pomocą pamięci zewnętrznej USB[26].

Jeszcze innym przykładem może być awaria w dostawie energii elektrycznej w zachodniej części Ukrainy (grudzień 2015/styczeń 2016). Według różnych szacunków prąd nie docierał nawet do 1,4 miliona mieszkań. Najprawdopodobniej doszło do cyberataku, polegającego na infekcji złośliwym oprogramowaniem sieci teleinformatycznej dwóch podstawowych dostawców energii elektrycznej. W jej wyniku doszło do przejęcia kontroli nad komputerami, które miały możliwość zdalnego sterowania funkcjonowaniem stacji transformatorowych. W ten sposób cyberterrorysta był stanie wyłączyć zasilanie we wszystkich kontrolowanych przez komputer podstacjach, a następnie uszkodził system operacyjny głównego komputera w sposób utrudniający przywrócenie poprawnego jego działania.

Na podatność systemów energetycznych na atak cyberterrorystyczny składa się wiele zjawisk. Po pierwsze popularność systemów SCADA[27], czyli systemów mających za zadanie nadzór oraz kontrolę przebiegu procesu technologicznego oraz produkcyjnego, w tym przede wszystkim w zakresie kontroli pracy gazociągów, ropociągów oraz sieci energetycznych. Większość z tych systemów wykorzystuje oprogramowanie zapewniające graficzny interfejs człowiek-maszyna, pozwalający operatorowi na uzyskanie pełnej kontroli nad urządzeniami pracującymi w danym systemie. Należy podkreślić, że systemy te są powszechnie uważane za podatne na cyberatak z jednego powodu – podczas projektowania ich głównych założeń i mechanizmów zabezpieczeń, cyberataki nie były tak powszechne jak dzisiaj.

Jedna z akcji z wykorzystaniem słabego ogniwa zabezpieczeń systemu SCADA miała miejsce w 2012 r.. Zaatakowano wówczas system należący do kanadyjskiej firmy Telvent, będącej operatorem przesyłu ponad połowy gazu i ropy naftowej na obu kontynentach amerykańskich. Zdaniem przedstawicieli firmy, hakerzy uzyskali możliwość przeprowadzenia ataku z wykorzystaniem kontrolowanego przez nich systemu.

[24] https://en.wikipedia.org/wiki/Northeast_blackout_of_2003 (13.11.2016).
[25] http://www.theregister.co.uk/2008/06/02/chinese_blamed_us_power_outage/ (13.11.2016).
[26] Uniwersalna Magistrala Szeregowa – rodzaj magistrali wykorzystywanej w trakcie komunikacji komputera z urządzeniami peryferyjnymi.
[27] SCADA – z ang.: *Supervisory Control And Data Acquisition.*

Kolejnym czynnikiem wpływającym na podatność sektora energetycznego na ataki jest powszechność korzystania z usług podwykonawców. Większość z nich stanowią podmioty, które nie posiadają wystarczających środków finansowych do wprowadzenia stosownych zabezpieczeń. Konieczność połączenia systemów wielu firm znacząco ułatwia atakującym przeprowadzenie skutecznej akcji dzięki wykorzystaniu słabości w systemach zabezpieczeń mniejszych podmiotów.

Trzecim zjawiskiem mającym wpływ na podatność na ataki są wysokie koszty bezpieczeństwa. W niektórych przypadkach rachunek strat i zysków przedsiębiorstwa wskazuje, iż zatrudnienie specjalistów z dziedziny bezpieczeństwa IT oraz inwestycje w wyspecjalizowane zabezpieczenia jest nieopłacalna. Z ekonomicznego punktu widzenia naprawa wyrządzonych szkód dla takich przedsiębiorstw jest mniej kosztowna niż inwestowanie w kolejne zabezpieczenia. Częściowo taki stan rzeczy wynika z ewolucji, a czasem rewolucji w zakresie stosowanych przez atakujących metod. Niestety doprowadza to do swoistej negatywnej symbiozy – przedsiębiorstwa nie wiedzą o atakach, pozwalając hakerom na nieskrępowany dostęp do ich sieci i przetwarzanych informacji.

Ostatnim zagrożeniem, wartym zaznaczenia jest czynnik ludzki, bowiem często najsłabszym ogniwem zabezpieczeń jest człowiek. Ogólna wiedza osób, które nie zajmują się na co dzień problematyką bezpieczeństwa teleinformatycznego jest zazwyczaj na relatywnie niskim poziomie. Jednym z najpowszechniej występujących zjawisk, które mogą doprowadzić do ataku na infrastrukturę sieciową danego przedsiębiorstwa jest słabe zabezpieczenie haseł dostępu do systemu. Użytkownicy wykorzystują najczęściej bardzo łatwe do zapamiętania hasła, których moc zabezpieczeniowa jest znikoma. Zgodnie z danymi zebranymi przez firmę SplashData[28], zajmującej się tworzeniem oprogramowania do generowania silnych haseł, najpopularniejszym hasłem w 2014 r. była kombinacja cyfr „123456", zaś na drugim miejscu uplasowało się słowo „password"[29]. Złamanie takiego hasła jest banalnie proste. Wykorzystywane w tym celu oprogramowanie w pierwszej kolejności próbuje uzyskać dostęp do danego konta za pomocą słów pochodzących ze słownika. Kolejnym błędem jest zapisywanie haseł na kartkach i umieszczanie ich w łatwo dostępnych miejscach. Oczywiście w przypadku zdalnego ataku nie jest możliwe uzyskanie bezpośredniego dostępu do pomieszczeń, jednakże wykorzystując systemu telewizji przemysłowej, czy też prowadząc klasyczną obserwację obiektu można uzyskać potrzebne dane. Przejęte w ten sposób hasła nie tylko ułatwiają przeprowadzenia ataku, lecz również maskują działalność hakerów.

Ataki cyberterrorystyczne mogą przynieść wiele niespodziewanych efektów. Pomimo tworzenia specjalnych planów, mających za zadanie przygotowanie sektora energetycznego na efekty potencjalnych ataków, nie jesteśmy w stanie do końca ich przewidzieć. Skuteczny atak na infrastrukturę energetyczną jest w stanie wywołać poczucie strachu i wywoływać panikę

[28] SplashData – amerykańska firma zajmująca się bezpieczeństwem oprogramowania i usług.
[29] Badanie przeprowadzone na podstawie analizy danych, które wyciekły z popularnych portali społecznościowych oraz usług sieciowych.

wśród ludności. O ile w przypadku okresu letniego brak prądu lub też gazu nie jest aż tak dotkliwy dla społeczeństwa, o tyle w okresie zimowym stwarza realne zagrożenie. W Polsce podstawowym paliwem, wykorzystywanym do ogrzewania domów oraz wody w miejskich instalacjach wodociągowych, obok węgla kamiennego jest gaz ziemny. Uszkodzenie systemów odpowiedzialnych za sterowanie przesyłem i dystrybucją tego paliwa może zaszkodzić całemu społeczeństwu. Brak ogrzewania w mieszkaniach może przyczynić się do pogorszenia zdrowia ludności, a w skrajnych przypadkach również śmierci przez wyziębienie organizmu. Z kolei brak prądu może przyczynić się do wywołania paniki wśród obywateli.

PODSUMOWANIE

Cyberterroryzm stanowi realne zagrożenie dla systemów teleinformatycznych infrastruktury krytycznej państwa, zaś z drugiej potencjalne skutki udanego ataku na systemy infrastruktury mogą nie tylko zdestabilizować funkcjonowanie państwa, lecz również doprowadzić do zagrożenia zdrowia i życia obywateli. Porównując znikome koszty przeprowadzenia ataku cyberterrorystycznego z potencjalnymi skutkami, należy stwierdzić, iż obecnie jest to jedna z najtańszych metod wzniecania paniki i terroru wśród społeczeństwa.

Cyberterroryzm jest zjawiskiem, którego pod żadnym pozorem nie można bagatelizować. Pomimo trudności w określeniu jego źródeł, czy też poprawnym rozpoznawaniu tego zjawiska każde państwo powinno odpowiednio zabezpieczyć systemy teleinformatyczne infrastruktury krytycznej.

Naczelną zasadą powinno być podejmowanie działań nakierowanych na ochronę całej cyberprzestrzeni przed jakimikolwiek przejawami nielegalnego jej wykorzystania.

Na podstawie badań własnych jak i wielu innych badających tę problematykę należy stwierdzić, że niestety w Polsce jak innych krajach niewiele osób ma świadomość z powagi zagrożenia i wielu indywidualnych użytkowników nie wie, w jaki sposób zgłaszać zaobserwowane incydenty. Zagrożenie cyberterroryzmem, wraz z jakościowym i ilościowym rozwojem systemów komputerowych, będzie zatem proporcjonalnie rosło. Szczególnie zagrożone tym rodzajem terroryzmu wydają się państwa o wysokim stopniu uzależnienia infrastruktury od systemów informatycznych, co idzie w parze z powszechnym dostępem do sprzętu komputerowego.

BIBLIOGRAFIA

Adamski Andrzej. 2002. Cyberterroryzm. W Terroryzm, 113-121. Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika w Toruniu.

Bógdał-Brzezińska Agnieszka, Marcin Gawrycki. 2003. Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warszawa: ASPRA-JR.

Ciekanowski Zbigniew. 2015. Zwalczanie terroryzmu w Polsce, Jarosław: PWST-E.

Lisocki E. 2009. Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy. Uniwersytet Gdański.

Tafoya William L. 2011. „Cyber Terror". Biuletyn służb porządku publicznego FBI (10) https://leb.fbi.gov/2011/november/leb-november-2011.

Wasilewski Janusz. 2013. „Zarys definicyjny cyberprzestrzeni". Przegląd Bezpieczeństwa Wewnętrznego 9 (5) : 225-234.

Zbigniew Ciekanowski, Sylwia Wojciechowska-Filipek. 2016. Bezpieczeństwo funkcjonowania w cyberprzestrzeni Jednostki – Organizacji – Państwa. Warszawa: CeDeWu. http://konflikty.wp.pl/kat,1020225,title,Czy-grozi-nam-cyberterroryzm,wid,11640989,wiadomosc.html

http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

http://www.theregister.co.uk/2008/06/02/chinese_blamed_us_power_outage/

https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html