

lic. Dawid Sawczuk
Państwowa Szkoła Wyższa
im. Papieża Jana Pawła II
w Białej Podlaskiej

CYBERTERRORYZM JAKO ZAGROŻENIE XXI WIEKU

CYBERTERRORISM AS A THREAT OF THE 21ST CENTURY

Streszczenie

W opracowaniu autor przedstawia rozwój elektroniki, informatyki oraz ich wpływ na powstanie tak groźnego dla całego świata zagrożenia, jakim jest cyberterroryzm. Jest to zagrożenie globalne, które może spowodować ogromne straty zarówno w ludziach, jak też straty gospodarcze.

Na przestrzeni XX i początku XXI wieku nastąpił postęp cywilizacyjny w zakresie przesyłu informacji dźwiękowych i wizualnych. Był to czas intensywnego rozwoju elektroniki, komputerów i innych urządzeń mobilnych. Okres, w którym powstało społeczeństwo informacyjne, a informatyka weszła do przemysłu, energetyki, a także innych dziedzin życia gospodarczego i społecznego. Zagadnienie to związane jest także z zagrożeniami w cyberprzestrzeni, które nie dotyczą tylko Polski. W opracowaniu przedstawiono ataki cyberterrorystyczne w Estonii, Gruzji czy Kirgizji. Ataki cyberterrorystyczne na infrastrukturę teleinformatyczną, banki i rząd estoński uświadomiły rządowi europejskim wielkość tego zagrożenia. Spowodowały również rozrost zainteresowania obroną cyberprzestrzeni. Należy pamiętać, że nie da się całkowicie wyeliminować zjawiska cyberprzestępczości, ale współpraca rządów, wspólne monitorowanie zjawisk i ruchów hakerów może wpłynąć na powstrzymanie zagrożenia, jakim jest cyberterroryzm.

Słowa kluczowe: atak, bezpieczeństwo, cyberterroryzm, haker, wojna

Abstract

In the study, the author presents the development of electronics and IT and their impact on the emergence of such a threat to the whole world as cyberterrorism. It is a global threat that can cause enormous human and economic losses.

Over the course of the 20th and early 21st centuries, civilization progressed in the field of audio and visual information transmission. It was a time of intensive development of electronics, computers and other mobile devices. The period in which the information society was created and IT entered industry, energy, and other areas of economic and social life. This issue is also related to threats in cyberspace that do not only concern Poland. The study presents cyber-terrorist attacks in Estonia, Georgia and Kyrgyzstan.

Cyber-terrorist attacks on ICT infrastructure, banks and the Estonian government made European governments aware of the magnitude of this threat. They also caused a growing interest in defending cyberspace. It should be remembered that it is not possible to completely eliminate the phenomenon of cybercrime, but cooperation of governments, joint monitoring of phenomena and movements of hackers may contribute to stopping the threat of cyberterrorism.

Keywords: attack, security, cyberterrorism, hacker, war

Wstęp

Cały wiek XX i początek XXI wieku to intensywny rozwój technologii elektronicznych. Kluczową datą w rozwoju elektroniki i komputerów jest rok 1900. Jest to rok, w którym Herman Hollerith, za pomocą tzw. maszyny liczącej obliczył spis ludności USA.

Rozwój elektroniki i informatyki przyczynił się do powstania społeczeństwa opartego na informacji – czyli tzw. społeczeństwa informacyjnego. Takie społeczeństwo, które jest oparte na informacji ma wiele zalet, np. łatwy dostęp do informacji czy ułatwienia w życiu prywatnym i zawodowym. Zastosowanie technologii informatycznych w gospodarce, przemyśle, energetyce, transporcie przynosi wymierne korzyści finansowe i materialne. Natomiast komputeryzacja wszelkich gałęzi przemysłu spowodowała wzrost bezrobocia nie tylko w Polsce.

Spółeczeństwo oparte na technologiach informatycznych i Internecie narażone jest na wiele zagrożeń. Jednym z nich jest wspomniane wyżej bezrobocie. Użytkownicy Internetu narażeni są na „złe treści” znajdujące się na stronach internetowych. Są to strony z pornografią, w tym pornografią dziecięcą. W Internecie spotkać się można również ze stalkingiem, sextingiem, nawoływaniem do przemocy.

Celem niniejszego opracowania jest pokazanie wpływu rozwoju elektroniki i informatyki na rozwój społeczeństwa informacyjnego oraz przedstawienie cyberterroryzmu jako najgroźniejszego zagrożenia XXI wieku.

Elektronika a społeczeństwo w XX i XXI wieku

Rozwój elektroniki i informatyki trwa już ponad 100 lat. Historia rozwoju komputerów rozpoczyna się w 1900 r. W tym roku Herman Hollerith za pomocą 311 tabulatorów, 20 sorterów i 1021 perforatorów obliczył wyniki spisu ludności Stanów Zjednoczonych. Do obliczeń wyników użył 120 milionów kart perforowanych.

Koniec XX i początek XXI wieku to czas kiedy nastąpił szybki rozwój komputerów. Powstawał coraz nowszy i doskonalszy sprzęt komputerowy. Technologia komputerowa stawała się coraz bardziej rozwinięta. Moc sprzętu stawała się coraz większa, a gabaryty coraz mniejsze.

Koniec lat 90 XX wieku i początek XXI wieku jest czasem intensywnego rozwoju elektroniki i informatyki. Nastąpił szybki rozwój technologii informatycznych,

czego dowodem było powstanie Internetu i jego lawinowy rozwój. Wraz z rozwojem elektroniki i informatyki nastąpił ogromny wzrost przepływu informacji. Rozwój technologii informatycznych przyczynił się do rozwoju technik przetwarzania, gromadzenia, przechowywania, przesyłania i odbioru informacji. Rewolucja technologiczna wprowadziła wiele usprawnień i rozwiązań, które ułatwiły codzienne życie ludzi. Zmieniły się gabaryty i objętość urządzeń. Komponenty, które były wielkości szaf lub pomieszczeń wraz z rozwojem elektroniki i informatyki objętością były coraz mniejsze, ale miały coraz większą „pamięć”. W czasach obecnych ta „pamięć” jest nieporównywalnie większa.

Technologie i urządzenia, tj. Internet, komputery klasy PC, laptopy, tablety, smartfony mają pozytywny wpływ na codzienne życie obywateli każdego państwa. Służą do komunikacji interpersonalnej, rozwijają zainteresowania, służą do prowadzenia działalności gospodarczej i pozwalają na sprawne zarządzanie zespołem pracowników.

Rozwój elektroniki i informatyki w życiu codziennym daje ludziom stały i łatwy dostęp do informacji potrzebnych każdego dnia. Coraz nowsze aplikacje pozwalają dotrzeć do wielu przetworzonych danych. Jest wiele ułatwień, które pozwalają na wymianę danych. Przeszkodą nie są nawet największe odległości¹.

Wiek XXI to czas intensywnego rozwoju technologii mobilnych. Naukowcy Michael Martin Hammer, James Champy, Philip Kotler w swoich pracach udowodnili, że technologie mobilne mają duży wpływ na zmiany, które zachodzą w biznesie, życiu społecznym. Rozwój technologii mobilnych zmienił oblicze współczesnego świata. Dzięki szybkiemu rozwojowi technologii bezprzewodowych każda osoba, posiadająca takie urządzenie „będzie miała dostęp do potrzebnych danych niezależnie od miejsca i czasu”². Nowoczesne technologie mobilne doprowadziły do powstania „społeczeństwa mobilnego”. Społeczeństwo mobilne dużo zyskuje posiadając dostęp do wymienionych urządzeń. Przede wszystkim jest to wygodą dzięki możliwości przesyłania informacji z poziomu urządzenia przenośnego, które zawsze można mieć przy sobie. Do tego nie ma potrzeby noszenia ze sobą złożonego okablowania, gdyż przesyłanie informacji następuje kanałem bezprzewodowym. W wyniku tego jednostka staje się dostępna praktycznie w każdym miejscu na ziemi oraz nie występuje już ograniczenie czasowe. W przesyłanych informacjach mogą być zawierane komunikaty multimedialne dające efekt kontaktu na żywo. Równie istotną korzyścią jest posiadanie dostępu do wielowymiarowej bazy, w której są zawierane wszystkie najważniejsze informacje o stronach, które komunikują się między sobą. Dochodzi do tego możliwość przeniesienia pewnego wycinka życia do przestrzeni wirtualnej³.

Przenośne urządzenia mobilne są używane do kontaktów ze znajomymi (rozmowy, sms, mms), do tworzenia portali internetowych, ściągania plików, przeglądania

¹ Ł. Łysik, P. Machura, *Rola i znaczenie technologii mobilnych w codziennym życiu człowieka XXI wieku*, „Media i Społeczeństwo”, Nr 4/2014, s. 15.

² K. Krzysztofek, *Społeczeństwo w dobie Internetu: refleksyjne czy algorytmiczne?*, w: *Re: Internet – społeczne medium*, Warszawa 2006, s. 24.

³ Ł. Łysik, P. Machura, *Rola i znaczenie...*, dz. cyt., s. 19.

dania informacji, robienia zdjęć, kręcenia filmików i korzystania z gier. Urządzenia mobilne, które były w użyciu kilka lat wcześniej nie miały w sobie tylu opcji, co w chwili obecnej.

Komunikacja mobilna wpłynęła pozytywnie na wiele dziedzin codziennego życia, np. mikroorganizację czasu na logistykę dnia codziennego, zdrowie, bezpieczeństwo, więzy rodzinne. Łatwo więc zauważyć, że rozwój elektroniki, informatyki, technologii mobilnych wpływa na rozwój społeczeństwa, gospodarki, a każda pojedyncza osoba zyskuje wiele udogodnień w życiu⁴.

Zadaniem Internetu jest wyszukiwanie i pozyskiwanie informacji przez każdego użytkownika, które udostępniane są zarówno przez instytucje, jak też osoby prywatne. Wszystkie informacje gromadzone są w systemie WWW (World Wide Web), czyli „ogólnoswiatowa pajęczyna”. Jest to system usług internetowych. W chwili obecnej jest to najpopularniejsza aplikacja, która pozwala korzystać ze wszystkich multimedialnych zasobów internetowych. Aplikacja ta opiera się na rozbudowanym systemie hipertekstowych i hipermedialnych połączeń. Oznacza to, że WWW opiera się na hiperlinkach, które ułatwiają dostęp do wszystkich plików, które są ze sobą wzajemnie powiązane⁵.

W chwili obecnej Internet nie jest już tylko „siecią w sieci”. Jest przede wszystkim globalnym systemem komunikacyjnym, który utworzony jest przez prywatne i publiczne sieci komunikacyjne. Jego działanie jest możliwe dzięki zastosowaniu niekomercyjnych i otwartych standardów telekomunikacyjnych. Zasadą, która reguluje przepływ danych w Internecie jest zasada end-to-end. Zasada ta pozwala na przesyłanie różnych typów informacji, bez preferencji dla jakiegokolwiek szczególnej formy. Sieci, które są ze sobą połączone są całkowicie autonomiczne. Zarządzane są przez prywatnych i publicznych właścicieli. Nie podlegają żadnej odgórnej kontroli. Wszystkie usługi internetowe są koordynowane na zasadach rynkowych. Są uważane za „towar”, a według Justyny Hofmokl za „nowe dobro wspólne”⁶.

„Internet jest siecią globalną, gdzie przesyłanie danych nie wiąże się z żadnymi ograniczeniami terytorialnymi i niepodlegający lokalnym jurysdykcjom”⁷. Przy definicji Internetu należy wspomnieć o technologiach informacyjnych i telekomunikacyjnych (z ang. Information and Telecommunication Technologies–ICT). To właśnie dzięki rozwojowi ICT połączenie komputerów indywidualnych jest możliwe.

Rozwój elektroniki, informacji i spektakularny rozwój sieci internetowych przyczyniły się do intensywnego przepływu informacji od jednego użytkownika do drugiego. W XXI wieku wiedza i informacja jest potrzebna w każdej dziedzinie życia gospodarczego, społecznego i kulturalnego każdego obywatela. Każdy człowiek w swoim życiu podejmuje wiele decyzji dotyczących nie tylko życia osobistego, ale też decyzji, które dotyczą nauki i pracy. Do podjęcia właściwej decyzji

⁴ Tamże, s. 20-21.

⁵ J. Hofmokl, *Internet jako nowe dobro wspólne*, Wyd. Akademickie i Profesjonalne, Warszawa 2012, s. 64.

⁶ Tamże.

⁷ Tamże, s. 65.

potrzebny jest dostęp do aktualnych, sprawdzonych informacji. Potrzeba dostępu do informacji przyczynia się do dalszego, szybkiego rozwoju technologii informatycznych.

Informacja jest niezbędna w życiu każdego człowieka. Jest bardzo ważnym składnikiem jego otoczenia. Jest kluczem do rozwiązania wszystkich problemów oraz wielu zagadnień dotyczących współczesnej cywilizacji. Jest fundamentem dla rozwoju państw i społeczeństw.

Informacja jest bardzo ważnym elementem działalności każdego człowieka. Jesteśmy o czymś informowani, otrzymujemy takie informacje lub sami je poszukujemy. Można powiedzieć, że „podstawą funkcjonowania każdego człowieka w dzisiejszym świecie jest posiadanie określonych informacji”⁸.

Stały dostęp do komputerów, Internetu, telefonów komórkowych i innych urządzeń mobilnych zapoczątkował rewolucję informacyjną. Informacja jest podstawą działania każdego urządzenia. Bez dostępu do informacji nie będzie funkcjonować żadne przedsiębiorstwo, bank, uczelnia, szpital, wojsko czy biblioteki. Nowe technologie ułatwiają życie. Decydują o efektach pracy zakładów przemysłowych, do wzrostu gospodarczego. Właściwa wiedza pozwala na oszczędność energii i surowców, redukcję zatrudnienia. Informacja stanowi o potęgze intelektualnej każdego człowieka.

Dzisiejsze społeczeństwo nazywane „społeczeństwem informacyjnym” nie może obejść się bez korzystania z informacji. Najwięcej informacji, które są potrzebne do życia oferuje Internet. On zmienił wszystko – relacje między ludźmi, działania firm, ich prowadzenie. Ten ma rację i podejmuje trafne decyzje, kto posiada potrzebne informacje. W XXI wieku jest dobrem wspólnym, towarem, który można kupić i sprzedać.

Rozwój elektroniki, informatyki i Internetu ma ogromny wpływ na życie i działalność każdego człowieka żyjącego w społeczeństwie informacyjnym. Każde nowe działanie ma swoje określone skutki zarówno te pozytywne, jak i te o charakterze negatywnym. Dotyczy to zarówno społeczeństwa, jak też każdej pojedynczej osoby.

Zagrożenia z społeczeństwie informacyjnym są różne. Takim nowym zagrożeniem jest uwarstwienie społeczne obywateli. Pod tym terminem kryje się podział społeczeństwa pod różnym kątem np. dostępu do wiedzy, informacji czy kwalifikacji. Dawniej o pozycji w społeczeństwie decydowało pochodzenie, miejsce urodzenia, sytuacja społeczna, majątkowa danej osoby, natomiast w dobie społeczeństwa informacyjnego np. umiejętność posługiwania się technikami informatycznymi, wykorzystywania ich w procesie pracy i nauki. W czasach globalizacji proces uwarstwienia społecznego może mieć zasięg dużo większy. Może dotyczyć nie tylko grup społecznych, ale całych społeczeństw lub państw (np. rozwój społeczeństwa brytyjskiego w porównaniu z np. Sudanem)⁹.

⁸ M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010, s. 104.

⁹ W. Krztoń, *XXI wiek – wiekiem społeczeństwa informacyjnego*, [w:] *Modern Management Review*, Nr 22 (3)/2015, s. 109.

Dużym problemem społeczeństwa informacyjnego jest zapewnienie każdemu człowiekowi równych szans rozwoju. Występująca specjalizacja, potrzeba posiadania pracowników z rzadkimi umiejętnościami i wiedza dyskwalifikuje stare, tradycyjne umiejętności. Dlatego zaobserwować można rozwój edukacji, ale czy wszyscy będą mieli pracę- nie wiadomo.

Bardzo niebezpiecznym zjawiskiem w sieci jest obecnie hackerstwo. Pisarz Stanisław Lem do Internetu odnosił się bardzo sceptycznie. Zwracał uwagę na niebezpieczne zjawisko w Internecie, jakim jest „przyrodzona skłonność człowiekowi do oszustw i nieuczciwości, która za pomocą sieci może silniej się rozwijać. Nie ma żadnych zakazów, więc można kłamać”¹⁰.

Największym zagrożeniem społeczeństwa informacyjnego jest cyberterroryzm. Jest on zagrożeniem dla bezpieczeństwa każdego współczesnego państwa. Ataki cyberterrorystyczne mogą zakłócać normalnie funkcjonujące państwo. Może być przerwane jego funkcjonowanie, w wśród obywateli wywołać panikę. Prowadzona w Internecie agitacja może dostarczać nowych członków do organizacji terrorystycznych, w tym także specjalistów zajmujących się informatyką lub systemami teleinformatycznymi¹¹.

Współczesne zagrożenia w cyberprzestrzeni

Cyberterroryzm jest realnym zagrożeniem dla infrastruktury teleinformatycznej każdego państwa. Ataki cyberterrorystyczne mogą spowodować ogromne straty zarówno w „sieci”, jak też w świecie rzeczywistym. Mogą doprowadzić do załamania gospodarczego i politycznego na całym świecie. Mogą również przyczynić się też do śmierci wielu ludzi.

Najbardziej dokładna definicja cyberataku brzmi następująco: „jest to wrogie wykorzystanie komputerów, ich sieci i innych pokrewnych technologii i urządzeń teleinformatycznych, którego celem jest zablokowanie, zakłócenie, zniszczenie albo uzyskanie informacji, które znajdują się w sieciach i systemach teleinformatycznych lub w innych urządzeniach wykorzystujących ICT. Inaczej mówiąc jest to „zablokowanie, zakłócenie, przejęcie kontroli lub zniszczenie samych sieci i systemów teleinformatycznych albo innych urządzeń, które te technologie wykorzystują”¹².

Naukowcy proponują różne klasyfikacje cyberataków. Najprostszy podział to atak pasywny i aktywny. Inna klasyfikacja ataku to: atak dnia zero i atak dnia następnego. Najbardziej skuteczny jest atak dnia zero, ponieważ wykorzystuje nieodkryty błąd w systemie lub w określonej aplikacji. Taki atak składa się z dwóch etapów. Pierwszy to odnalezienie danej słabości (luki). W drugim etapie dokonuje się nowego, niespotykanego włamania.

¹⁰ S. Lem, *Świat na krawędzi*, Wydawnictwo Literackie, Kraków 2000, s. 166.

¹¹ K. Bielski, *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, [w:] Zeszyty Naukowe Uniwersytetu Szczecińskiego, Nr 889/2015, s. 105.

¹² Tamże.

Pierwszym programem, który był uważany za wirusa był Creeper napisany w 1971 roku przez Boba Thomasa z BBN Technologies. W 1982 roku powstał wirus Elk Cloner, który przy pomocy dyskietek rozprzestrzeniał się na komputery typu Apple II. Był nieszkodliwy. Na monitorach komputerów wyświetlał tekst „It will get on all your disks. It will infiltrate your chips. Yes, it's Cloner.” Początek lat 90-tych XX wieku był dalszym rozwojem wirusów. Były to programy wyspecjalizowane, pozwalające na stworzenie własnych spersonalizowanych wirusów. Były to wirusy o nazwie Michalangelo, Internet Liberation Front. Zainfekowały one komputery należące do NASA i IMG. Staog atakował komputery z oprogramowaniem Linux. W tym samym czasie powstał polimorficzny Marburg.

Na przełomie XX i XXI wieku pojawiły się wirusy, które atakowały pliki HTML i PHP. Późniejsze wirusy były coraz bardziej wyspecjalizowane. Były tak pisane, żeby mogły zainfekować wybrane programy, usługę lub maszynę. Według Karsena Johannsona, wirusy mogą podlegać mutacji. Do rozprzestrzeniania się potrzebują zarażonych plików. Atakują one wybrane typy plików. Modyfikują dane „ofiary” wirusa. Nie infekują dwukrotnie tego samego pliku. Symptomy infekcji wirusem mogą być niewidoczne. Mogą być również odsunięte w czasie¹³.

Wirusy komputerowe są najgroźniejszą i najstarszą metodą ataków w cyberprzestrzeni. Mimo stosowania coraz bardziej zaawansowanych programów antywirusowych wirusy wciąż doprowadzają do strat finansowych i awarii systemów teleinformatycznych.

Ciekawą metodą stosowaną w atakach cyberterrorystycznych są ataki sieciowe (network attack). Polegają one na manipulowaniu danymi, które sterują transmisją pakietów. Przy tych atakach rozpowszechnioną techniką jest IP spoofing. Technika ta polega na uzyskaniu nielegalnego dostępu do sieci dzięki podszyciu się pod adres IP autoryzowanego komputera. Inna technika to sessionhijacking, która wykorzystuje pliki cookie lub cross-sitescripting¹⁴.

Inną metodą stosowaną przez cyberprzestępców jest atak na hasła (password attacks user compromise). Celem takiego ataku jest zdobycie kontroli nad danym komputerem, usługami albo danymi, które są dostępne z kont użytkownika. Atak na hasła można przeprowadzić na różne sposoby. Pierwszym sposobem będzie znajomość danych osobowych użytkownika komputera. Mogą to być również hasła i nazwy użytkownika, które mają bezpośredni związek z jego życiem prywatnym. Posiadane informacje o użytkowniku mogą być przydatne do rozszyfrowania hasła do konta lub komputera. Drugi sposób to „ataki słownikowe” (dictionary attacks). Do ataku wykorzystywane są możliwe hasła ze słowników. Trzeci sposób to ataki typu bruteforce. Jest to program, który z ogromną szybkością wprowadza przy włamaniu do komputera rozmaite, losowo wybrane sekwencje znaków¹⁵.

Do wyżej wymienionych metod ataków cyberterrorystycznych można dodać jeszcze dwa, które są bardzo specyficzne. Pierwszy objawia się działaniami cha-

¹³ K. Johansson, *Computer Viruses. The Technology and Evolution of an Artificial Life Form*, 1994, s. 24-32.

¹⁴ M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s.130.

¹⁵ Tamże, s. 131.

rakterze materialnym. Na ten atak składa się użycie broni elektromagnetycznej (EMP). Drugi to tzw. atak Van Eck Phreaking. Polega on na przechwytywaniu zarówno sygnałów teleinformatycznych i danych, które w formie cyfrowej zawarte są w komputerze. Przechwytywanie odbywa się poprzez monitorowanie pola elektromagnetycznego. Dzięki tej metodzie podsłuchujący może zdobyć wszystkie dane, które w danej chwili znajdują się na monitorze komputera. Nie ma konieczności włamywania się do systemu¹⁶.

Wiek XX i początek XXI wieku to czas intensywnego rozwoju elektroniki i informatyki. Coraz więcej państw i społeczeństw jest uzależniona od informatyki. Współczesne komputery kontrolują i gromadzą informacje, które są istotne w każdej dziedzinie życia społeczeństwa. Są to informacje związane z dostarczaniem energii, która jest „układem krwionośnym każdego państwa”. Jest to komunikacja, transport lotniczy i morski, służby finansowe, dane medyczne, dane dotyczące państwa i wojska. Właśnie te i inne zgromadzone informacje interesują cyberterrorystów. W XXI wieku cyberterroryzm jest najgroźniejszym zjawiskiem w cyberprzestrzeni. Są to bardzo specyficzne działania, których celem jest próba ataku lub atak na sieci komputerowe lub systemy informacyjne, które mogą spowodować zniszczenie infrastruktury państwa. Celem takiego ataku może być próba zastraszenia poszczególnych rządów lub społeczeństw, wyrządzając przy tym ogromne szkody.

Obszarem zainteresowania cyberterrorystów jest więc każdy obiekt, który funkcjonuje w cyberprzestrzeni i umożliwia realizowanie ich celów. Zakłócenia teleinformatyczne i telekomunikacyjne mają wywołać w społeczeństwie niepewność, strach, panikę i ich następstwa¹⁷.

Na celownikach cyberterrorystów jest infrastruktura krytyczna państw, różnego rodzaju organizacji i wspólnot. Infrastruktura krytyczna są to systemy i wchodzące w ich skład powiązane ze sobą funkcjonalnie różne obiekty budowlane, instalacje, urządzenia, kluczowe usługi dla bezpieczeństwa państwa oraz jego obywateli, które służą zapewnieniu sprawnego funkcjonowania wszystkich organów administracji publicznej. Infrastruktura krytyczna to również systemy zaopatrzenia w wodę i żywność, energię i paliwa, łączność i sieci teleinformatyczne, systemy bankowe i finansowe, ochrona zdrowia i ratownictwo. Są to systemy, które zapewniają bezpieczne i sprawne funkcjonowanie administracji publicznej. Są to systemy, które są odpowiedzialne za produkcję, składowanie i przechowywanie oraz stosowanie niebezpiecznych substancji chemicznych i promieniotwórczych. Elementami, które są szczególnie ważne w infrastrukturze telekomunikacyjnej są systemy i sieci telekomunikacyjnych i teleinformatyczne. Są one niezbędne przy wykonywaniu statutowych zadań wszystkich organów administracji rządowej każdego szczebla, wymiany informacji w siłach zbrojnych, rejestrach państwowych w warstwie aplikacyjnej oraz sieci telekomunikacyjnych, które są

¹⁶ M. Lakomy, *Cyberprzestrzeń jako nowy...*, dz. cyt., s.132.

¹⁷

wykorzystywane przez administrację publiczną (rządową i samorządową) i siły zbrojne w warstwie medium transmisyjnego¹⁸.

Teren ataków terrorystycznych jest bardzo duży, trudny do zidentyfikowania. Ciągłe powiększa swój zasięg na nowe strefy. Ze względu na rodzaj cech, który atakowany jest przez cyberterrorystów można wprowadzić następujący podział:

- informatyczne systemy wojskowe, które przechowują np. informacje o rozmieszczeniu i planowanych ruchach wojsk i broni, o systemach łączności w armii albo informacje o prowadzonych badaniach nad nowym uzbrojeniem;
- informatyczne systemy infrastruktury krytycznej państwa — wszelkie systemy opisane wyżej;
- informatyczne systemy przedsiębiorstw, które przechowują strategiczne informacje dla firm (np. wykorzystywane w przedsiębiorstwie technologie, plany rozwoju)¹⁹.

Celem cyberterrorystów są nie tylko systemy informatyczne stosowane w sferze militarnej. Bardzo często atakowane są systemy cywilne. dzieje się tak ponieważ nie istnieje oddzielenie fizyczne sieci wojskowych od sieci komercyjnych i publicznych. Zakłócenia w obiektach, którymi interesują się cyberterroryści może spowodować różne negatywne zjawiska społeczne oraz bardzo często duże straty społeczne²⁰.

Ataki cyberterrorystyczne na wybrane cele i obiekty są atakami, które niosą masowe ofiary i przerażenie wśród społeczeństwa. Zarówno celem, jak i narzędziem jest strach. taki atak wśród społeczeństwa budzi atmosferę strachu, niepewności i utraty zaufania. Bardzo często uzyskanie danych o celach, które mogą być zaatakowane przez cyberterrorystów są ogólnodostępnymi informacjami. Celem ataku nie zawsze musi być infrastruktura teleinformatyczna lub krytyczna danego kraju. Celem mogą być np. firmy publikujące informacje, które popierają globalizację.

Obecnie Internet jest źródłem informacji, z których mogą korzystać cyberprzestępcy. Stanowi on główne narzędzie, służące do uzyskiwania potrzebnych informacji przydatnych do planowania ataku. Atak cyberterrorystyczny może być skierowany przeciwko każdemu elementowi infrastruktury krytycznej i stanowić zagrożenie do funkcjonowania. Każdy jej element działa dzięki komputerom.

Nie jest to przedstawienie sytuacji, która może zdarzyć się w przyszłości. Takie ataki mogą zdarzyć się w każdej chwili, jeśli nie podejmiemy odpowiednich kroków, aby ją jak najskuteczniej chronić. Cyberterroryzm jest najważniejszą i największą groźbą dla świata, jaką daje ludziom wiek XXI.

Poważnym zagrożeniem był atak robaków Code Red w 2001 roku. Code Red przeprowadził bardzo nieudany atak na strony internetowe Białego Domu. Znisz-

¹⁸ J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, [w:] Telekomunikacja i techniki informacyjne, Nr 1-2/2014, s. 28.

¹⁹ Tamże, s. 150.

²⁰ J. Jemioł, *Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku*, Wydawnictwo Naukowe, Kraków, 2005, s. 9.

czył anglojęzyczne strony w Internecie, zainfekował kilka milionów hostów, spowodował opóźnienie produkcyjne w wielu zakładach i spowodował straty gospodarcze w wysokości 2 mln dolarów.

Kolejnym atakiem cyberterrorystycznym, był Moonlight Maze. Trwał on dwa lata (1998-2000), a jego celem były instytucje Stanów Zjednoczonych. Stanowił skoordynowany atak hakerów rosyjskich na serwery amerykańskich instytucji rządowych i prywatnych. Atak Moonlight Maze był skierowany przeciwko Pentagonowi, NASA, Departamentowi Energii, różnym uniwersytetom i instytucjom badawczym. W 1999 roku podczas operacji NATO w Kosowie informatycy Sojuszu Północnoatlantyckiego dokonali wielu ataków cyberterrorystycznych na infrastrukturę teleinformatyczną Serbii. Celem tych ataków było zablokowanie działań serwerów, sieci i komputerów serbskich. W odwecie serbscy hakerzy próbowali zablokować pracę serwerów Paktu Północnoatlantyckiego.

Ataki w Estonii analitycy podzielili na kilka faz. Pierwsza faza była fazą spontaniczną. W czasie jej trwania internauci, którzy popierali mniejszość rosyjską w Estonii zaczęli samoistnie organizować się w sieci. Dzięki forom internetowym, blogom i innym witrynom, które były poświęcone hakingowi, hatywiści patriotyczni oraz zwykli scriptkiddies zainicjowali cyberataki typu DDoS (atak rozproszony odmowy usługi) przeciwko władzom Estonii. Atak DDoS polega na zwieszeniu komputera lub zablokowaniu serwisu sieciowego przez zalewanie sieci bardzo dużą ilością danych. Przy pierwszej fazie ataków cyberterrorystycznych celem były strony rządowe. Do tego ataku posłużyły proste programy i komendy, które były rozpowszechniane w Internecie.

Ataki cyberterrorystyczne na Estonię charakteryzowały się masowością. Od początku brały w nich udział tysiące komputerów, dlatego ich zablokowanie było dość trudne. Według danych Hun-CERT (węgierskiego zespołu CERT) pomiędzy 27 kwietnia a 11 maja 2007 roku w Estonii doszło do 128 ataków metodą DDoS. Z tego 115 ataków przeprowadzono z wykorzystaniem techniki ICMP flood (inaczej ping flood lub smurtattack), a 4 ataki za pomocą TCP Syn flood. Większość ataków trwała około godziny, jednak 15 ataków trwało powyżej 5 godzin (nawet 10 godzin).

Skala tych ataków była bardzo duża, o czym może świadczyć fakt, że przepustowość części z tych ataków zbliżała się do granicy 90 Mb/s. Za większością tych ataków stała sieć botnet, chociaż część z nich dokonywano za pomocą innych narzędzi, mniej skomplikowanych. Udostępniane one były na stronach haktywistów rosyjskich (np. www.zyklonteam). Ochotników do przeprowadzenia ataków szukano również na forach, które nie były związane z rosyjskim hakingiem. Każdy internauta w bardzo łatwy sposób mógł zdobyć środki, które były przydatne do zaatakowania estońskiej sieci²¹. Podczas cyberwojny Estonia była bombardowana ogromną ilością e-maili spamu. Ataki przeciwko Estonii były skierowane na strony władzy ustawodawczej i wykonawczej oraz na strony domowe i konta e-mail polityków estońskich. Przez całą kampanię strony te były atakowane przez cały

²¹ M. Lakomy, *Cyberprzestrzeń jako nowy...*, dz. cyt., s. 192.

czas. Sektor prywatny był także atakowany przez cyberterrorystów. Włamywano się na portale internetowe największych estońskich mediów, przedsiębiorstw budowlanych i telekomunikacyjnych, wybrane elementy infrastruktury teleinformatycznej. W atakach, które były organizowane po 1 maja celem byli dostawcy usług internetowych. Głównym zadaniem ataku było zakłócenie funkcjonowania krajowej estońskiej sieci. Zablokowano również działanie numeru alarmowego 112, dlatego obywatele nie mieli dostępu do służb ratunkowych.

W 2007 roku miał miejsce atak cyberterrorystyczny na sieć informatyczna syryjskiego systemu obrony przeciwlotniczej. Do tego ataku Izrael wykorzystał wirusa komputerowego o nazwie Suter. Wirus ten pozwalał nie tylko na atak na sieci komputerowe i telekomunikacyjne Syryjczyków. Dał też możliwość na monitorowanie i przejęcie kontroli nad systemami radarowymi obrony powietrznej Syrii. Dzięki temu atakowi dokonano bombardowania syryjskiego ośrodka wojskowego, w którym prowadzone były prace nad bronią atomową. Syryjska obrona przeciwlotnicza nie została o tym ataku powiadomiona. Był to atak cyberterrorystyczny na cele militarne²².

Rok 2008 to czas tzw. drugiej wojny cybernetycznej. Celem ataku była wówczas Osetia w Gruzji. Ataki cyberterrorystyczne wystąpiły równolegle z konfliktem w Osetii Południowej. Jeszcze przed wybuchem konfliktu hakerzy gruzińscy dokonali dwóch ataków cyberterrorystycznych na strony internetowe osetyńskiej agencji informacyjnej i radia rządowego w Cchinwali. W wyniku ataków media te nadawały informacje, które podawała Alania TV. Była to gruzińska stacja telewizyjna skierowana do mieszkańców Osetii. Po zaangażowaniu się Rosji w konflikt z Gruzją hakerzy rosyjscy dokonali wielu ataków na strony internetowe najważniejszych instytucji państwowych w Gruzji, między innymi na witrynę Micheila Saakaszwiliego, stronę rządu, ministra obrony i ministra spraw zagranicznych Gruzji. Ataki cybernetyczne zablokowały dostęp do portali komercyjnych i naukowych²³.

W 2008 roku dokonano również ataku cyberterrorystycznego na komputery Pentagonu. Dzięki pamięci USB do amerykańskich sieci wojskowych zostało przeniesione złośliwe oprogramowanie, które bardzo szybko rozprzestrzeniło się na wojskowe sieci. Hakerzy dokonali transferu tajnych, wojskowych danych poprzez zabezpieczone serwery. Przez długi okres czasu atak ten nie był wykryty i był największym w historii włamaniem do sieci militarnych Stanów Zjednoczonych. Prawdopodobnie tego ataku cyberterrorystycznego dokonali rosyjscy hakerzy²⁴.

W 2009 roku chińscy hakerzy przeprowadzili atak pod nazwą Aurora, który był skierowany przeciwko 20 amerykańskim korporacjom: np. Google, Adobe, Systems, Yahoo, Northrop Grumman i Symantek. Celem tego ataku było uzyskanie

²² A. Urbanek, *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, [w:] *Studia nad bezpieczeństwem*, Nr 1/2016, s. 194.

²³ Tamże, s. 18.

²⁴ Tamże.

nowoczesnych technologii i specjalistycznego oprogramowania, którego używały zaatakowane firmy²⁵.

Zagrożenia atakami cyberterrorystycznymi dotyczą również państwa polskiego, zaś pod względem ilości ataków rokiem rekordowym był rok 2013. Zarejestrowanych wówczas zostało 8817 zgłoszeń, natomiast jako incydenty zakwalifikowano 5670 zdarzeń w polskiej cyberprzestrzeni.

Podsumowanie

Wiek XX i początek XXI to okres intensywnego rozwoju elektroniki, a co za tym idzie również rozwój informatyki, między innymi Internetu, w Polsce i na świecie. Rozwój technologii teleinformatycznej przyczynił się do powstania społeczeństwa informacyjnego. W obecnej dobie nikt nie wyobraża sobie życia bez telefonu komórkowego, laptopa czy komputera stacjonarnego. Z każdym dniem urządzenia są coraz bardziej rozwinięte i doskonalsze. Każda gałąź gospodarki poszczególnych państw nie może funkcjonować bez wprowadzenia informatyki i komputerów do swoich zakładów pracy. Jest to bardzo ważne dla rozwoju gospodarczego. Jednak na uwagę należy mieć fakt, że informatyzacja zakładów pracy powoduje wzrost bezrobocia na świecie. Jeden komputer może zastąpić kilku pracowników.

Rozwój technologii informatycznych i zastosowanie ich w różnych gałęziach gospodarki, zarówno w sektorach państwowych i prywatnych, ich nowoczesny rozwój powoduje wzrost zainteresowania tymi przedsiębiorstwami różnych grup przestępczych działających w cyberprzestrzeni.

Cyberprzestępcy, a ściślej rzecz ujmując cyberterrorysty, w swoich rękach mają wiele narzędzi do popełniania cyberataków, stosując przy tym wiele metod działania. Cyberterroryzm i inne przestępstwa, które są dokonywane za pomocą komputerów i Internetu są najgroźniejszym zagrożeniem społeczeństwa informacyjnego XXI wieku.

Cyberterrorysty dokonują różnych ataków. Ich celem są osoby prywatne i publiczne, rządy, banki a nawet państwa, zaś występujący w ich wyniku paraliż jednego sektora gospodarki powoduje dezorganizację dużej części państwa. Atak na Estonię, nazywany często I cyberwojną, spowodował wzrost zainteresowania rządów państw należących do UE ochroną cyberprzestrzeni.

Cyberterroryzmem zainteresowało się również NATO, Europol, Interpol i inne służby. Różne, coraz częściej pojawiające się ataki cyberterrorystyczne sprowokowały Parlament Europejski i Radę Europy do opracowania, a także wydania dyrektyw oraz rezolucji w tej sprawie. Celem tych aktów prawnych była ochrona cyberprzestrzeni państw członkowskich UE. Polska – jako członek UE – do swojego prawodawstwa przyjęła zalecenia unijne i wprowadziła je w życie. Ostatni polski dokument „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022” jest zgodna z wymogami unijnymi. Nie można dopuścić do sytuacji,

²⁵ Tamże, s. 19.

w której cyberterroryści ograniczyliby tradycyjną rolę państwa atakując najbardziej newralgiczne sektory, pozbawiając obywateli informacji lub nią manipulując. Dlatego państwa Unii Europejskiej, jako całość, powinny chronić swoją cyberprzestrzeń. Współpraca państw unijnych przy zwalczaniu cyberterroryzmu i ochronie cyberprzestrzeni przynosi pożądane rezultaty. Wspólne monitorowanie zmian w wykorzystaniu IT, wspólne śledzenie przepływu informacji w Internecie, współpraca rządów i służb przynosi efekty.

W ostatnim okresie poważnych konfliktów w cyberprzestrzeni jeszcze nie było. Były tylko ataki dokonywane przez państwa lub takie ataki, za które państwa były odpowiedzialne. Jednak dzięki odpowiedniemu prawodawstwu i wyspecjalizowanym służbom, mamy na obecną chwilę zagwarantowane bezpieczeństwo.

Literatura:

1. Bielski K., *Nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego”, Nr 889/2015.
2. Hofmokr J., *Internet jako nowe dobro wspólne*, Wyd. Akademickie i Profesjonalne, Warszawa 2012.
3. Jemioł J., *Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku*, Wydawnictwo Naukowe, Kraków, 2005.
4. Johansson K., *Komputer Virusses. The technology and Evolution of an Artificial Life form*, 1994.
5. Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i techniki informacyjne”, Nr 1-2/2014.
6. Krzysztofek K., *Społeczeństwo w dobie Internetu: refleksyjne czy algorytmiczne?*, w: *Re: Internet – społeczne medium*, Warszawa 2006.
7. Krztoń W., *XXI wiek – wiekiem społeczeństwa informacyjnego*, „Modern Management Review”, Nr 22 (3)/2015.
8. Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
9. Lem S., *Świat na krawędzi*, Wydawnictwo Literackie, Kraków 2000.
10. Łysik Ł., Machura P., *Rola i znaczenie technologii mobilnych w codziennym życiu człowieka XXI*, „Media i Społeczeństwo”, nr 4/2014.
11. Urbanek A., *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, „Studia nad bezpieczeństwem”, Nr 1/2016.
12. Wrzosek M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010.