ELEMENTY INFRASTRUKTURY KRYTYCZNEJ PAŃSTWA /ORGANIZACJI/ - JAKO OBIEKTY NARAŻONE NA ATAKI CYBERTERRORYSTYCZNE

Marian KOPCZEWSKI

Streszczenie: W XXI wieku, erze innowacji, galopującej techniki, technologii, elektroniki i informatyki powstające w bardzo szybkim tempie nowe technologie stały się czynnikiem, który powoduje, że od momentu ich powstania w cyberprzestrzeni trwa cicha, a zarazem bardzo intensywna wojna. Żołnierzami stali się specjaliści z dziedziny informatyki, analitycy informacji, eksperci od wywiadu i kontrwywiadu czy też zwykli ludzie o zamiłowaniu i pasji jaką jest informatyka i hacking. Społeczeństwo jeszcze do końca nie zdaje sobie sprawy z konsekwencji skutecznie przeprowadzonych ataków terrorystycznych za pomocą Internetu. Różnego rodzaju ataki cyberterrorystyczne, kradzież danych i informacji, szerzenie propagandy przez organizacje terrorystyczne czy też wojna informacyjna, a szczególnie w aspekcie zagrożeń obiektów infrastruktury krytycznej państwa, w tym przedsiębiorstw, jako szczególnie narażonych na atak ze strony cyberterrorystów.

Słowa kluczowe: cyberterroryzm, zagrożenia informacyjne, infrastruktura krytyczna.

1. Cyberterroryzm jako zjawisko wojny informacyjnej

Formy zagrożenia atakiem terrorystycznym można podzielić na pięć tradycyjnych kategorii. Kategorie te charakteryzują się sposobem przeprowadzenia ataku i zawierają się w angielskim akronimie CBERN (chemical, biological, explosives, radiological, nuclear), pod tym skrótem kryją się zagrożenia chemiczne, biologiczne, materiałami wybuchowymi, radiologiczne i nuklearne. Organizacje terrorystyczne w swych dotychczasowych przedsięwzięciach nie posłużyły się jeszcze atakiem radiologicznym i nuklearnym. W dniu dzisiejszym można mówić o rozszerzeniu tego katalogu sposobów przeprowadzenia ataku. Bardzo szybki rozwój technologiczny cywilizacji wprowadza do niego nowy typ zagrożenia terrorystycznego – cyberterroryzmu.

Operacyjne pojęcia cyberterroryzmu. Przyjmuje się, że sam termin cyberterroryzm powstał w roku 1997 za sprawą naukowca z Instytutu Bezpieczeństwa i Wywiadu (Institute for Security and Intelligence) w Kalifornii, Barry'ego C. Collina, który zdefiniował to jako zespolenie cybernetyki i terroryzmu. Również w roku 1997 agent specjalny FBI (Federalne Biuro Śledcze) Mark Pollit wysunął operacyjną definicję cyberterroryzmu jako: zaplanowany, politycznie umotywowany atak przeprowadzony przez tajnych agentów lub subnarodowe grupy przeciwko systemom komputerowym, informacjom i danym skutkującą przemocą wobec niemilitarnych celów.

Refleksje na temat zaangażowania ugrupowań terrorystycznych w cyberprzestrzeni komplikuje dodatkowo aspekt oddzielenia jej od zjawiska wojny informacyjnej (information warfare). Zagadnienie to jest stosunkowo nowe jednakże jest bardzo poważnie traktowane przede wszystkim przez rządy krajów technologicznie zaawansowanych. W

obecnych czasach wojna informacyjna może być rozumiana jako kompletnie nowy wymiar konfliktów międzynarodowych.

Wojnę informacyjną rozumie się jako nowoczesny sposób wykorzystywania systemów informatycznych, który oddziałuje na elektroniczne systemy przeciwnika oraz zniekształca przekazywaną informację, przy jednoczesnej obronie własnych zasobów i systemów informacyjnych. Jest działaniem mającym na celu osiągnięcie przewagi nad „przeciwnikiem" w sferach wiarygodności i skuteczności informacji poprzez jej destrukcję czy zdobywanie strategicznych danych. Wojna informacyjna obejmuje przedsięwzięcia stosowane zarówno w czasie pokoju, jak i wojny, skierowane przeciwko siłom zbrojnym, a także przeciwko ludności cywilnej i jej świadomości, przeciwko systemowi administracji państwowej, systemowi nadzoru produkcji przemysłowej czy też np. nauki. Działania destrukcyjne prowadzone są osobno, bądź też jednocześnie w trakcie procesów przyjmowania informacji, jak również jej przetwarzania i wykorzystywania. Należy podkreślić, że procesy te mogą wywierać istotnymi wpływ na proces podejmowania decyzji. Wojna informacyjna wykorzystywana może być przez cyberterrorystów w celu zdobywania ważnych strategicznych informacji celem ich późniejszego wykorzystania w szeroko pojętych działaniach terrorystycznych. Stronami tego typu konfliktów mogą być zarówno państwa jak i podmioty niepaństwowe. Sytuacja taka rodzi problemy natury prawnej związane ze stosowaniem praw prowadzenia działań wojennych takich jak zasady użycia siły, stosowania blokad itd. Do prowadzenia wojny informacyjnej stosowane są wiedza i narzędzia identyczne z używanymi do popełniania przestępstw komputerowych czy ataków cyberterrorystycznych. Ofiara takiego ataku w chwili jego popełniania nie ma pewności, z którą z tych form się spotkała, dla ofiary ataku efekt jest identyczny. Zasadnicza różnica pomiędzy tymi czynami to motywacja istniejąca po stronie inicjatora tychże ataków.

Brak przejrzystych relacji wraz z nieokreśleniem wyraźnej granicy między walką informacyjna a cyberterroryzmem dodatkowo komplikują próby dokładnego zdefiniowania obu zjawisk. Część autorów dla rozróżnienia cyberterroryzmu od wojny informacyjnej proponują posłużenie się kryterium podmiotowym, które rozgranicza państwa od niepaństwowych podmiotów. W takiej sytuacji mielibyśmy do czynienia z cyberterroryzmem gdy stroną atakującą jest niepaństwowy podmiot. W przeciwnym przypadku, podczas gdy ofensywne działania prowadzi państwo, mamy do czynienia z wojną informacyjną. Pogląd ten jest mocno kontrowersyjny, trudno się z nim zgodzić, gdyż stawia on wszelkie ruchy narodowowyzwoleńcze, w tym walczące o swoje prawa mniejszości narodowe czy etniczne w bardzo niekorzystnym położeniu.

Aby stworzyć precyzyjną i funkcjonalną definicję cyberterroryzmu należy liczyć się z wieloma trudnościami. Rozbieżności interpretacyjne powodują, że wciąż trwa polemika co do istoty zagadnienia terroryzmu. Odnośnie cyberterroryzmu na problemy z ujednoliceniem definicji nakładają się również złożone zagadnienia związane z funkcjonowaniem społeczeństwa informacyjnego. W związku z trudnościami oraz brakiem pojęcia cyberterroryzmu, którego można by użyć należałoby się raczej skupić na opisowej prezentacji zagrożeń zaliczanych do cyberterroryzmu.

Poddając analizie hipotetyczne i istniejące manifestacje cyberterroryzmu okazuje się, że terroryści mogą wykorzystać komputery nie tylko do sabotażu ale również jako narzędzie do komunikacji, propagandy, szkolenia, prowadzenia wojny psychologicznej, a także nawoływania do przestępstw, szerzenia nienawiści, rekrutacji, zbierania czy wręcz zarabiania środków finansowych oraz gromadzenia informacji. Katalog ten jest o wiele szerszy ale wydaje się, że wynikające z tych działań zagrożenia można pogrupować w

trzech kategoriach:

- atak na informacje,
- atak na system,
- wsparcie klasycznych form działalności terrorystycznej.

2. Rodzaje ataków cyberterrorystycznych

Atak na system, można scharakteryzować jako działanie stawiające sobie za cel system operacyjny atakowanego komputera lub/i jego oprogramowanie w celu przejęcia kontroli nad jego funkcjami lub uczynienia go niefunkcjonalnym. Zdecydowana większość hakerskich przedsięwzięć w sieci internetowej ma właśnie taki charakter. Są to na przykład wirusy, robaki internetowe, czy ataki DoS (Denial of Service) i DDoS (Distributed Denial of Service). W parze z niszczycielską siłą i ogromną skutecznością idzie zarazem prostota działania. Zarówno ataki DoS jak i ataki DDoS generujące ogromny ruch internetowy ukierunkowany na konkretny serwer powodują, że jest on praktycznie niedostępny dla innych uprawnionych użytkowników. Dotychczas jednym z poważniejszych przypadków takiego ataku miał miejsce roku w 2000, kiedy również nasze media informowały o ataku na serwery CNN, Amazon.com, Yahoo!, które w rezultacie zostały przeciążone i wyłączone na kilkanaście godzin. Przywrócenie pełnej funkcjonalności zaatakowanych serwerów trwało kilka dni. Straty spowodowane tym atakiem oszacowano na kwotę około 1,2 miliarda USD.

Pierwszy atakiem typu DDoS uznawana jest blokada serwerów ambasad Sri Lanki w kilku krajach. Atak dokonany został przez tamilskich separatystów, którzy zarzucili serwery pocztowe ambasad tysiącami listów elektronicznych. Atak składał się z około 800 listów dziennie przez około 2 tygodnie. Listy zawierały wiadomość o treści: „Jesteśmy Czarnymi Tygrysami Internetu i robimy to, aby zakłócić waszą komunikację". W tej grupie znajdują się również bardziej niebezpieczne akty terrory cybernetycznego, dążące do przejęcia całkowitej kontroli nad zaatakowanym komputerem, zastosowanie znajdują tu Konie Trojańskie i ataki typu Back Door (z ang. Tylne Drzwi). Konie Trojańskie to specjalne oprogramowanie rozpowszechniane w sieci internetowej bardzo często pod postacią darmowych, atrakcyjnych załączników do otrzymanej poczt elektronicznej. Tak zwane Back Door's to luka w kodzie programów, aplikacji, systemów umyślnie utworzona celem późniejszego wykorzystania, powstała już na etapie danego oprogramowania bądź tworzone i pozostawione przez administratorów systemów w użytkowanych przez nich maszynach. W tak zainfekowanych komputerach istnieje możliwość umieszczenia tzw. snifferów, tzw. podsłuchiwaczy sieciowych lub podobnego oprogramowania służącego do przechwytywania loginów i haseł użytkowników. Przeprowadzanie ataku tego typu, zwłaszcza na systemy, które pełnią ważną rolę w funkcjonowaniu danego podmiotu bądź instytucji, wymaga na ogół kwalifikacji, wiedzy i czasu. Aby przeprowadzić tego typu atak, atakujący musi posiadać specjalistyczną wiedzę z zakresu działania konkretnego systemu. Tego typu atak miał miejsce w Australii. Nastąpiło włamanie do systemu informatycznego, który zarządzał funkcjami oczyszczalni ścieków.

Były pracownik do oceanu i miejskiej sieci wypuścił miliony litrów nieprzerobionych ścieków. Sprawca włamania miał głęboką wiedzę o funkcjonowaniu systemu, a także w swoim laptopie posiadał wykradzione oprogramowanie sterujące tą oczyszczalnią. W trakcie prowadzonego śledztwa ujawniono, że sprawca nie był w stanie dokonać włamania od razu. Atakującemu powiodło się dopiero za 46 razem, szczególnie niepokoić może fakt, że wcześniejsze 45 prób ataku nie zostały zauważone przez administratora systemu.

Celem ataku w drugiej z wyodrębnionych kategorii są przetwarzane i przechowywane w systemie komputerowym dane. Z uwagi na to, co jest prawdziwym celem stojącym za uzyskaniem nielegalnego dostępu do informacji można mówić o dwóch podkategoriach. W pierwszym przypadku dobrem, przeciw któremu przestępca kieruje swoje działania jest wiarygodność systemu oraz zaufanie użytkowników do tego systemu, w drugiej podkategorii uwzględnić należy kradzież informacji.

Wprowadzenie do systemu komputerowego nowej informacji lub modyfikacja istniejącej, co objawi się przez dysfunkcjonalność kontrolowanego przez ten system procesu lub urządzenia, zaliczyć można do pierwszej podkategorii. Aby takie przedsięwzięcie się powiodło należy dokonać zmian w niezauważalny przez operatora systemu sposób. Prawdziwe straty mają dopiero przynieść działania i decyzje podjęte w oparciu o nowe, spreparowane dane, z uwzględnieniem tego, iż atakowany system musi być postrzegany jako sprawnie, normalnie i poprawnie działający. Ataki tego typu bazują na założeniu, że użytkownicy systemów komputerowych mają zaufanie do informacji, które czerpią z danych źródeł istniejących w sieci Internet. Strony WWW. zawierające akty prawne Sejmu, Senatu RP, analizy i raporty umieszczane na serwerach np. Ministerstwa Finansów, notowania spółek giełdowych to źródło wiedzy zarówno dla obywateli, przedsiębiorców oraz instytucji pożytku publicznego. Te serwery i komputery mogą być potencjalnym celem zamachowców planujących wywołać choćby częściową dezorganizację funkcjonowania danego społeczeństwa. Wymierzone w tego typu serwisy informacyjne ataki, choć nie miały charakteru aktów terrorystycznych, lecz działań typowo przestępczych, dokonywane były wielokrotnie w przeszłości, przede wszystkim dotyczyły manipulacji notowaniami akcji spółek giełdowych. We wspomnianej wyżej podkategorii umieścić można również działania bezpośrednio wymierzone w infrastrukturę, która wykorzystuje w swoim funkcjonowaniu polecenia i informacje otrzymywane z zewnątrz. Chodzi tu o przede wszystkim o odpowiedzialne np. za kierowanie ruchem pociągów, dystrybucję energii elektrycznej czy nawet rozmieszczenie bagaży na pokładach statków lub samolotów systemy informatyczne. Udane włamanie i wpływ na przetwarzanie danych w tych systemach jest w stanie spowodować ofiary śmiertelne w ludziach i zniszczenia materialne. W małym stopniu jest prawdopodobne, że błędy w oprogramowaniu czy wirus komputerowy mogą spowodować, że z nieba zaczną spadać samoloty, jak miało to miejsce kilka lat temu w bardzo śmiałych wizjach konsekwencji Y2K (problem roku 2000). Sparaliżowanie systemów informatycznych zarządzających ruchem pasażerów na lotniskach w połączeniu z deklaracją dowolnej organizacji terrorystycznej, że jest to ich kontrolowane i zamierzone działanie, może doprowadzić do groźnego wybuchu paniki. Wszczęcie procedur bezpieczeństwa oraz żądanie natychmiastowego ściągnięcia na ziemię wszystkich samolotów w niektórych przypadkach może wiązać się może z podejmowaniem niepotrzebnego ryzyka. Podobnie wroga ingerencja w oprogramowanie zarządzające systemem rozplanowania ładunku na pokładzie samolotu może mieć potencjalnie katastrofalne skutki.

Naturalnie systemy podatne na takie zdalne ataki przeważnie występują w wysoko uprzemysłowionych i zinformatyzowanych państwach. W praktycznym ujęciu tego zagadnienia na ten typ aktu terrorystycznego najbardziej narażone wydają się kraje Europy Zachodniej, rozwijające się technologicznie w bardzo dynamicznym tempie społeczeństwa Azji, ale przede wszystkim, z uwagi na polityczne uwarunkowania, zagrożone są Stany Zjednoczone. W latach siedemdziesiątych zeszłego stulecia, kiedy to w USA zaczęła się dokonywać rewolucja informatyczna, zagrożenie zjawiskiem cyberterroryzmu nie było w ogóle brane pod uwagę. Osoby decyzyjne, skuszone wizją redukcji kosztów w

przedsiębiorstwach zaczęli powszechnie wdrażać systemy SCADA (Supervisory Control And Data Asquisition), które umożliwiają zdalne zarządzanie funkcjami i parametrami oddalonego elementu infrastruktury. W odniesieniu do sieci energetycznych SCADA między innymi służy do zdalnej kontroli transformatorów, działając w ten sposób aby żadna elektrownia nie została przeładowana. Poza sieciami energetycznymi systemy te zostały wdrożone w wielu innych gałęziach gospodarki: tamach, sieciach wodociągowych oraz telekomunikacji. Jedną z niewielu gałęzi gospodarki, która nie wprowadziła systemów SCADA w swoich placówkach była energetyka jądrowa. Mając na uwadze bezpieczeństwo państwa instytucja NRC (The Nuclear Regulatory Commision), która jest odpowiedzialna za politykę nuklearną kraju zabroniła tego typu rozwiązań.

Nie oznacza to, że wszystkie elektrownie atomowe są bezpieczne od ataków polegających na manipulacji otrzymywanymi przez ich systemy danymi. Na przykład odpowiednie wykorzystanie tradycyjnych materiałów wybuchowych użytych w celu symulacji wstrząsów tektonicznych i spowodowania automatycznego wyłączenia elektrowni atomowej. Tego typu instalacje przemysłowe wyposażone są w czujniki sejsmiczne, które w przypadku wykrycia wstrząsów alarmują system komputerowy zarządzający pracą obiektu, a tenże system w celu zabezpieczenia reaktora przed wyciekiem rozpoczyna automatyczną procedurę wyłączania reaktorów atomowych.

Drugą z podkategorii jest klasyczna kradzież z systemu danych komputerowych. W przypadku działań mających znamiona terroryzmu chodzi głównie o gromadzenie danych pomocnych przy wyborze celu i przygotowaniach do dokonania zamachu. Obiektem ataku praktycznie mogą być wszelkie informacje. Nie tylko plany architektoniczne obiektów, grafiki pracy służby ochrony ale również prywatne zdjęcia przedstawiające wizerunki osób, przypadkowo skadrowane budynki i ich wnętrza czy nawet prywatna korespondencja pracowników, która może zawierać informacje o trybie dnia pracy, o ich zwyczajach itp. Nie jest możliwe przewidzieć jakie dane mogą znaleźć się w kręgu zainteresowań terrorystów. W trakcie operacji w Afganistanie oddziały amerykańskie zabezpieczyły należące do członków organizacji Al-Kaida laptopy, zawierające funkcjonalne i strukturalne plany zapór wodnych oraz informacje, które dotyczyły: znajdujących się na terenie Europy i Stanów Zjednoczonych stadionów oraz komputerowego systemu zarządzania systemami wodnymi elektrowni atomowych. Jednakże nawet w przypadku wykrycia odróżnienie tych działań od działań mających charakter kryminalny czy szpiegowski nie wydaje się możliwe.

O trzeciej kategorii o jakiej można powiedzieć to wsparcie klasycznych form działalności terrorystycznej. Jest to najszersza kategoria z dotychczas poruszanych. Wsparcie technologiczne przede wszystkim opiera się na logistyce i organizacji. Internet oferuje przeogromne możliwości komunikacji, zwłaszcza tym osobom, które chcą czynić to pozostając niezauważonymi przez organy ścigania i tak anonimowymi jak to tylko jest możliwe. W tym miejscu można odnotować fakt, iż w toku prowadzonego śledztwa dotyczącego dokonania zamachów z dnia 11 września 2001 roku okazało się, że w tygodniach poprzedzających atak część porywaczy samolotów koordynowała swoje działania wykorzystując zapewniająca znaczną anonimowość kawiarenki internetowe. Komputery również oferują zaawansowane techniki ukrywania przekazywanej treści takie jak steganografia czy kryptografia, nie wymagając od użytkownika profesjonalnego przygotowania.

Wracając do form wsparcia działań terrorystycznych przez narzędzia internetowe można podać scenariusz, w którym fizyczny akt terroru będzie sprzężony z następującą po nim kompanią propagandowo-dezinformacyjną. Kluczem do sukcesu w tej sytuacji jest

ubranie spreparowanych informacji w pozory autentyczności. Platformą takiego ataku mogą zostać witryny internetowe bardzo wiarygodnych odbiorców dzienników, takich jak BBC, Reuters czy CNN, natomiast w Polsce PAP, TVN24, TVP INFO. Ewentualna manipulacja zawartością ich elektronicznych serwisów informacyjnych, czy też podszycie się pod nie, z technicznego punktu widzenia nie jest technologicznym wyzwaniem. Natomiast potencjalne i polityczne konsekwencje tak skoordynowanej, można to nazwać maskarady są ogromne. Dodatkowe niebezpieczeństwo wiąże się z faktem, iż duże serwisy i agencje informacyjne są pierwotnym źródłem informacji dla wielu mniejszych i lokalnych dzienników i stacji radiowych i telewizyjnych. Można na przykład wyobrazić sobie sytuację, gdzie po atak na budynki Word Trade Center z 11 września 2001 roku, przeprowadzono by starannie zaplanowaną i zakrojoną na szeroką skalę informacyjną ofensywę, zmierzającą do przeniesienia chociażby częściowej odpowiedzialności za ten zamach na izraelski wywiad – Mossad.

W przypadku zakończonej powodzeniem operacji, nawet późniejsze wielokrotne dementowanie przez media tych doniesień nie byłoby już w stanie unicestwić żyjącego już własnym życiem tzw. faktu prasowego. Po atakach z dnia 11 września 2001 toku na różnych forach i grupach dyskusyjnych w Internecie można było zauważyć opinie, że w jakimś stopniu izraelski Mossad ponosi współwinę za dokonane zamachy. Wywiad Izraela miał wiedzieć o planowanych działaniach terrorystów, jednak celowo, aby doprowadzić do konfliktu Stanów Zjednoczonych ze światem arabskim, nie ujawnił danych na ten temat. Miała o tym świadczyć rzekoma nieobecność tego dnia w wieżowcach WTC osób pochodzenia żydowskiego. Plotka ta przeciekła z Internetu do świata rzeczywistego i zaczęła żyć własnym życiem. Konsekwencją tej teorii jest wzrost nastrojów antysemickich w pewnych grupach społecznych.

W świetle powyższych analiz można postawić pytanie, czy propagandową i niedestrukcyjną aktywność organizacji terrorystycznych można na pewno i z pełną odpowiedzialnością uznać za działalność terrorystyczną ze wszystkimi tego konsekwencjami. Niektóre opracowania skłaniają się do tego aby takie zjawisko nazwać tzw. miękkim terroryzmem. Tenże pogląd jest kontrowersyjny i poddawany krytyce zwłaszcza przez kraje czynnie zaangażowane w zwalczanie przejawów światowego terroryzmu. Wniosek jaki można wyciągnąć jest taki, że nie ma jednej odpowiedzi na to zagadnienie, bo będzie zależała przede wszystkim od przyjętej definicji terroryzmu czy cyberterroryzmu. Niepodważalnym faktem jest to, że organizacje terrorystyczne są świadome zalet sieci komputerowych i już teraz szeroko wykorzystują Internet w swoich działaniach i będą to robić częściej i na większą skalę.

3. Internet a finansowe wsparcie terrorystów

W tym miejscu chciałbym przedstawić jedne z najważniejszych zagadnień jakim jest finansowanie terroryzmu przy wsparciu Internetu. Chodzi zarówno o szerzenie propagandy, zbieranie składek od sympatyków jak i o realizację i organizację przedsięwzięć o charakterze stricte kryminalnym. Można posłużyć się przykładem witryny internetowej organizacji IRA (Irish Republican Army – Irlandzka Armia Republikańska), która daje możliwość przekazywania darowizn za pomocą karty kredytowej. Do roku 2001 organizacja Hamas posiadała w Stanach Zjednoczonych, w stanie Teksas charytatywną organizację HLF (Holy Land Foundations for Relief and Development) i za pośrednictwem witryny internetowej tejże organizacji zbierała fundusze, które następnie były przeksięgowywane na konta Hamasu. Mając na uwadze działalność kryminalną, dla nikogo

nie jest tajemnica, że cyberprzestępczość skierowana przeciwko instytucjom finansowym i bankom przynosi ogromne zyski. Według danych FBI w Stanach Zjednoczonych w latach dziewięćdziesiątych ubiegłego wieku za pomocą techniki komputerowej dokonano kradzieży od 3 do 7,5 miliardów USD w skali roku. Dla porównania amerykańskie banki w wyniku „tradycyjnych" napadów traciły w tym okresie jednorazowo średnio około 8 tysięcy USD, podczas gdy przeciętna kradzież informacji z systemu komputerowego kosztuje bank w przybliżeniu 100 tysięcy USD, a oszustwo komputerowe około 500 tysięcy USD. Dochody ze skradzionych kart płatniczych, sfingowane przelewy elektroniczne, włamania na elektroniczne konta bankowe czy też wymuszenia na centralach banków to tylko niektóre przykłady tego jak terroryści przy użyciu technik hakerskich są w stanie finansować swoją działalność. Banki na ogół konsekwentnie nie zgłaszają tego typu incydentów organom ścigania, kierując się zasadą, że zła sława może doprowadzić do utraty zaufania klientów i odejścia klientów z banku. Bez takich danych nie jest możliwe precyzyjne szacowanie utraconych kwot środków finansowych ani zwalczanie tego typu nadużyć. Istniejący stan rzeczy powoduje, że zdobywane tą drogą środki finansowe zdają się być poza realną kontrolą, co również na uwadze mają starające się pozostać w ukryciu struktury organizacji terrorystycznej.

Innym pośrednio związanym z systemami komputerowymi i Internetem elementem finansowania działalności terrorystycznej jest produkcja i dystrybucja podróbek towarów. Ta płaszczyzna działalności jest obecnie najlepiej udokumentowaną sferą przenikania się i współpracy zorganizowanych grup przestępczych oraz organizacji o charakterze terrorystycznym. Produktami znajdującymi się w sferze zainteresowania są podróbki alkoholu, papierosów, odzieży, płyt CD i DVD oraz oprogramowania komputerowego. O dużym wzroście aktywności na tym polu działań w swoim wystąpieniu przed Komitetem Izby Reprezentantów Stanów Zjednoczonych ostrzegał Sekretarz Generalny Interpolu Ronald Noble w dniu 16 lipca 2003 roku. W swym przemówieniu Noble podał przykłady podobnej działalności między innymi w Kosowie, Północnej Irlandii, północnej Afryce oraz Czeczenii. W przypadku czeczeńskich separatystów rosyjskie FSB (ФСБ - Федеральная служба безопасности Российской Федерации – Federalna Służba Bezpieczeństwa Federacji Rosyjskiej) przeprowadziło likwidację fabryki płyt CD, której wpływy oceniono w granicach od 500 tysięcy do 700 tysięcy USD w skali miesiąca. Aby zdać sobie sprawę jakie to są kwoty warto nadmienić, że według specjalistów całkowity koszt planowania i realizacji zamachu na Word Trade Center w Nowym Jorku wyniósł mniej niż 500 tysięcy USD. Można z tego wyciągnąć wniosek, że nie można tego typu spraw w przypadku fałszerstw towarów i produktów traktować pobłażliwie i z dystansem gdyż potencjalnie mogą mieć ogromny wpływ na bezpieczeństwo publiczne.

4. Próba oceny realności zagrożenia

Efektem ataku terrorystycznego nie zawsze musi być natychmiastowe wywołanie zniszczeń i śmierci ludzi w dużej skali. W dzisiejszym złożonym świecie gospodarczych zależności, a także zależności człowiek – maszyna, obywatel – państwo równie skutecznym sposobem walki terrorystycznej może okazać się oddziaływanie na te relacje i stopniowa ich degeneracja. Wbrew pozorom, głównym celem Al-Kaidy nie jest uwolnienie grupy bojowników, czy też wyzwolenie danego terytorium, ale zniszczenie zachodniego modelu życia. Przy tak sformułowanej misji zarówno fizyczne zniszczenie ośrodków finansowych, naukowych czy przemysłowych, jak i doprowadzenie ich do finansowej ruiny czy chaosu logistycznego wydaje się efektywną metodą walki. Destrukcja lub choćby osłabienie

jednego ogniwa łączącego obywatela cywilizacji zachodniej z jego modelem życia, poczucia bezpieczeństwa, wiarygodności informacji przekazywanej przez media, czy też obniżenie zaufania do instytucji państwowych przybliża terrorystów do destabilizacji systemu demokratycznego. Uzasadnione wydaje się twierdzenie, że niszczenie społecznego zaufania do oferowanego obywatelom przez państwo bezpieczeństwa jest jedną z dróg, jaką z dużym prawdopodobieństwem wybiorą formacje terrorystyczne. Dotyczy to zwłaszcza takich ugrupowań jak Al-Kaida, które posiadają wystarczająco duże zaplecze kadrowe i finansowe do prowadzenia działań cyberterrorystycznych na dość szeroką skalę. Cyberprzestrzeń nie odegrała jeszcze znaczącej roli w działaniach terrorystycznych to wiele wskazuje na to, że jest to wręcz wymarzone narzędzie do prowadzenia tego typu walki. Przemawiają za tym niskie koszta organizacji i przeprowadzenia zamachu, doskonałe możliwości koordynacji działań i komunikacji, ciągle niska świadomość społeczna istniejącego zagrożenia, a także łatwy dostęp do niezbędnych narzędzi programowych i specjalistycznej wiedzy. Koronnym argumentem za tą formą realizacji działania terrorystycznego jest fakt, że cyberterrorysta, w przypadku jeśli atak się nie powiedzie, nie ginie ani nie zostaje natychmiast aresztowany, w związku z czym wyeliminowany jako zagrożenie. Przeciwnie, terrorysta nabiera doświadczenia i przygotowuje się do kolejnego zamachu. Jest to o tyle istotne, że wbrew obiegowej opinii, większość terrorystów

nie podejmuje zamachów samobójczych. Większość terrorystów przeprowadzających zamachy ma plan awaryjny bądź plan ucieczki, jeśli sytuacja nie ułoży się po ich myśli.

Kiedy trwa dyskusja o realności zagrożenia podnoszone są kwestie, że niektóre kraje uznawane za wspierające terroryzm, są krajami o słabo rozwiniętej infrastrukturze teleinformatycznej i przez to niezdolnymi do podjęcia ofensywnych działań cyberterrorystycznych. Ma to być konsekwencją faktu, że brak tam fachowej wiedzy oraz ekspertów branży IT gotowych do przeprowadzania takiego typu ataku czy wręcz samej świadomości istnienia takich możliwości. Współcześnie taki pogląd wydaje się naiwny w świetle otaczających nas faktów. Już w 1996 roku Osama bin Laden swą kryjówkę w górach Afganistanu wyposażył w laboratorium komputerowe i realizowany drogą satelitarną dostęp do Internetu. Historia również uczy, że terroryści mogą przeprowadzić dowolny atak wykorzystując naszą własną infrastrukturę przeciw nam i mogą zrobić to z dowolnego kraju, takiego jak Filipiny czy Polska. Argument o braku wiedzy eksperckiej, nawet jeżeli byłby prawdziwy, nie wydaje się decydujący, jako, że zawsze na podorędziu pozostaje wykorzystanie najemników. Podziemie teleinformatyczne posiada ludzi o ogromnych zdolnościach i wiedzy, którzy są w stanie przeprowadzić najbardziej wymyślny atak informatyczny, kwestią jest jedynie cena takiej usługi.

Istnieją również symptomy, które wskazują na fakt, że doszło na tej płaszczyźnie do współpracy pomiędzy organizacjami terrorystycznymi, a zorganizowanymi grupami przestępczymi. Zorganizowane grupy przestępcze działają jako nieformalne przedsiębiorstwa nastawione na generowanie maksymalnych zysków, nie są przy tym związane żadnymi ramami prawnymi. Mało prawdopodobne wydaje się, aby przy odpowiedniej finansowej stymulacji nie zdecydowałyby się dokonać zamachu, a przynajmniej wyposażyć składających zamówienie w odpowiednich ludzi i sprzęt.

Do przeprowadzenia naprawdę złożonego ataku cyberterrorystycznego potrzeba czasu aby go przygotować. Czas planowania i przygotowania zamachu jest jednym z nielicznych czynników, który daje szanse organom ścigania i bezpieczeństwa państwa na przeciwdziałanie. W przypadku komputerów czas ma też szczególne znaczenie z innego powodu. Paradoksalnie bowiem sami hakerzy komputerowi w znacznym stopniu przeciwdziałają możliwości organizacji wielopoziomowych, złożonych i długofalowych

aktów cyberterrorystycznych. Owi pasjonaci sprzętu, oprogramowania komputerowego i techniki spędzają życie wyszukując i publicznie demaskując słabości poszczególnych systemów. Część z nich co prawda używa tej wiedzy nielegalnie dla emocji, zabawy, sławy czy chęci zdobycia pieniędzy. Jednakże takie poczynania demaskują błędy w oprogramowaniu i walnie przyczyniają się do ich systematycznej i stopniowej eliminacji. Ten ciągły wyścig z czasem utrudnia zaplanowanie w oparciu o istniejące luki bezpieczeństwa złożonego ataku terrorystycznego, którego konsekwencje mogłyby być poważne i rozległe. W dobrze administrowanych systemach wykryte i krytyczne dla działania systemu luki średnio istnieją nie dłużej niż 5 dni.

Inną okolicznością, dzięki której nie doświadczyliśmy jeszcze tego typu ataku może być fakt, że stojący na czele organizacji terrorystycznych są wytworami starego „fizycznego" świata, jego sposobu myślenia i działania. Jednak należy sobie jak najbardziej zdawać sprawę z tego, że jest to jedynie stan przejściowy.

Tak jak w każdej innej organizacji społecznej czy też instytucji również w szeregach ugrupowań terrorystycznych zachodzi ciągły proces wymiany kadr i automatycznie z tym cyklem następuje wymiana pokoleń. Wstępujący w ich szeregi młodzi ludzie mają już inne podejście do otaczających ich wirtualnych światów i technologii. Są w pełni świadomi potencjału jaki one za sobą niosą. Należy mieć na uwadze, że krytyczna, przemysłowa infrastruktura państwa nie jest dostatecznie chroniona. W Stanach Zjednoczonych przeprowadzono ćwiczenia zorganizowane przez NSA (National Security Agency – Agencja Bezpieczeństwa Narodowego). W czasie ćwiczeń okazało się, że jest możliwe skuteczne przeprowadzenie ataku cybernetycznego na cele w Stanach Zjednoczonych. Chociaż celem manewrów było Dowództwo Sił Pacyfiku Stanów Zjednoczonych, odpowiedzialne za żołnierzy gotowych do interwencji w rejonie Korei i Chin, to ćwiczenia wykazały, że rozmieszczeni w różnych punktach świata hakerzy NSA są w stanie przy użyciu ogólnodostępnych narzędzi hakerskich osiągnąć znacznie więcej niż zamierzony cel. W trakcie prowadzonych symulacji włamano się do między innymi do oficjalnych wojskowych sieci komputerowych zlokalizowanych na Hawajach, w Waszyngtonie czy Chicago. Ponadto hakerzy NSA wykazali, że są w stanie wyłączyć sieć dystrybucji energii elektrycznej na terenie całych Stanów Zjednoczonych. Co prawda symulowane ataki zostały dostrzeżone przez Pentagon i FBI, lecz te instytucje nie były w stanie im przeciwdziałać ani wykryć źródła ataku. Ćwiczenia te udowodniły, że piętą achillesową amerykańskiej gospodarki jest właśnie sieć energetyczna. Fakt, że może być ona zdalnie wyłączona przez szpiega lub terrorystę czy popisującego się hakera niepokoić może takie instytucje jak US-CERT (United States Computer Emergency Readiness Team). Jak pokazuje praktyka najsłabszym ogniwem nie są wcale nie zabezpieczone systemy SCADA w podstacjach i serwery znajdujące się w Centrach Kontroli. Tezę tę potwierdzają wydarzenia z 2001 roku w Kalifornii gdzie doszło do poważnego w konsekwencjach włamania do serwera Cal-ISO (California Independent System Operator – Kalifornijski Operator Systemu), przedsiębiorstwa odpowiedzialnego za zarządzanie większością sieci energetycznej w tym regionie. Włamanie zbiegło się w czasie z najpoważniejszym lokalnie kryzysem energetycznym, w trakcie którego przerwy w dostawie energii elektrycznej dotknęły blisko 400 tysięcy odbiorców. Przedstawiciele Cal-ISO potwierdzili włamanie do ich serwera jednak stwierdzili, że nie miało ono wpływu na dostawy energii czy wiarygodność systemu informatycznego. Ataki na Cal-ISO trwały nie zdemaskowane przynajmniej przez 17 dni. Jak wykazało śledztwo hakerzy wykorzystali lukę w systemie Solaris, aby dostać się do serwera. Następnie zainstalowano pakiet narzędziowy, który umożliwiał uzyskanie dostępu do systemu na prawach administratora, po czym

przystąpiono do instalacji w systemie swojego oprogramowania. System Cal-ISO nie był zabezpieczony przed atakami z sieci, nie posiadał firewall'a (zapory sieciowej), wykorzystywana konfiguracja systemu była konfiguracją podstawową, a wszystkie logi, czyli zapisy zawierające informacje o działaniach i zdarzeniach systemu komputerowego przechowywano na jednym serwerze.

5. Obiekty infrastruktury krytycznej państwa szczególnie narażone na atak cyberterrorystyczny

W aspekcie powyższych wydarzeń zastanowić się warto, jakie jeszcze obiekty zasługują na szczególną uwagę z punktu widzenia ochrony antyterrorystycznej. Poza sieciami energetycznymi należałoby wskazać przynajmniej kilka szczególnie zagrożonych obszarów, takich jak telekomunikacja, zarządzanie gospodarką wodną – tamy, systemy dostawy wody, pozbywania się ścieków, czy transport takich surowców energetycznych jak gaz ziemny i ropa naftowa. Wrażliwym punktem funkcjonowania rozwiniętych społeczeństw jest sprawność infrastruktury telekomunikacyjnej. Nowoczesne systemy telekomunikacyjne to przede wszystkim technologie komputerowego przetwarzania danych, z tego względu są one szczególnie narażone na ataki cyberterrorystyczne. Dotyczy to zarówno systemów telefonii stacjonarnej, komórkowej jak i satelitarnej.

Za taki stan rzeczy po części winę ponoszą firmy zajmujące się produkcją i wdrażaniem sprzętu telekomunikacyjnego i właściwego oprogramowania, które nierzadko prowadzą tzw. politykę przez tajność do bezpieczeństwa. Słabe strony systemów nie są niezwłocznie eliminowane, ale „ukrywane" w utajnionej specjalistycznej dokumentacji i artykułach fachowych, gdzie opisana zostaje specyfika tych słabości. Taka wiedza szybko trafia w ręce osób niepowołanych. Konsekwencje ewentualnego wyłączenia systemów telekomunikacyjnych na danym obszarze, poza uciążliwością dla społeczeństwa, byłyby dotkliwe w kontekście funkcjonowania służb ratunkowych i bankowości.

Szczególnym zagrożeniem w tej sferze jest atak zmierzający do wyłączenia Internetu jako całości. Zrealizowane może to być poprzez zablokowanie serwerów DNS tłumaczących adresy IP. Niezależnie od tego czy byłby to atak przeprowadzony w klasyczny sposób przy użyciu materiałów wybuchowych, czy też elektronicznie, jego efekty mogą być wszechogarniające. Nie da się przewidzieć faktycznych skutków wyłączenia Internetu, niestety nawet najbardziej optymistyczne prognozy mówiące o tych skutkach i ich wpływu na ekonomię są fatalne. Brak komunikacji upośledziłby całe sektory gospodarki, utrudnił bądź uniemożliwił wymianę informacji, zawieranie niektórych kontraktów oraz realizację transakcji handlowych. Byłaby to również strata dla świata nauki, korzystającego powszechnie z możliwości swobodnej wymiany poglądów oraz dostępu do baz danych oferowanych przez łącza teleinformatyczne. W rozwiniętych państwach są grupy ludzi, którzy konsekwencji takiego stanu rzeczy by nie odczuli lub uważali za niedogodność. Mimo iż czarne scenariusze można mnożyć to wydaje się, że dzisiejszy świat, tak mocno uzależniony od techniki, byłby w stanie funkcjonować bez globalnej sieci. Prawdopodobnie po okresie początkowego zamieszania funkcjonalność najważniejszych dla społeczeństwa służb i systemów takich jak policja, straż pożarna, szpitale itp. udałoby się przywrócić i zarządzać nimi w sposób tradycyjny.

Kolejnym przykładem celu ataków terrorystycznych są systemy przetwarzania i zaopatrzenia w wodę. Z uwagi na powszechną świadomość zagrożenia, systemy te wydają się być dobrze zabezpieczone przed ewentualnym atakiem wyprowadzonym z sieci komputerowej. Wykorzystywane systemy SCADA są mocno zindywidualizowane przez eksploatujące je lokalne podmioty. Z uwagi na to, włamanie do takiego systemu

wymagałoby posiadania niedostępnej powszechnie specjalistycznej wiedzy na temat funkcjonowania konkretnego urządzenia. Stacje uzdatniania wody, gdzie zdalnie zarządza się dozowaniem chemikaliów, są wyposażone w niezależne systemy powiadamiania i kontroli stężenia kluczowych dla bezpieczeństwa i jakości wody związków chemicznych. Serwery komputerowe odpowiedzialne za gromadzenie tych danych posiadają przygotowane w profesjonalny sposób oprogramowanie i umieszczone są w fizycznie odciętych strefach dostępu z pełnym całodobowym monitoringiem. Jeżeli w jakiś sposób napastnikowi udałoby się pokonać wszystkie przeszkody i spowodować nasycenie wody pitnej ilością chloru, która stanowiłaby zagrożenie dla zdrowia ludzi to i tak woda przesyłana przez system transportowy poddawana jest wielokrotnej kontroli chemicznej jej składu, a każda nieprawidłowość jest alarmowo zgłaszana za pośrednictwem wydzielonych łączy.

W USA na ten system nakłada się jeszcze fizyczne zabezpieczenie obiektów wodnych przez Gwardię Narodową, co daje w sumie wysoki poziom bezpieczeństwa. Większe zagrożenie występuje w przypadku zapór wodnych i tam. Przeprowadzone analizy wykazały, że część z nich wyposażona jest w zdalne systemy sterowania przepływem wody, które połączone są z centralą za pomocą publicznych łączy. W najgorszym przypadku takie włamanie może doprowadzić do kontrolowanego otwarcia śluz i stopniowego spuszczenia zasobów wody ze zbiornika, ale nawet takie zajście nie stanowi jednak bezpośredniego zagrożenia dla zdrowia i życia ludzi. Tak jak w każdym najlepiej nawet zabezpieczonym technicznie obiekcie, krytyczną składową stanowi czynnik ludzki. Odpowiedni system rekrutacji i bieżącej kontroli personelu jest niezbędnym elementem każdego systemu bezpieczeństwa.

Poza spektakularnymi akcjami terrorystom pozostaje jeszcze inny rodzaj skrytego oddziaływania na zinformatyzowane społeczeństwa i gospodarki państw zachodnich. Są to zagrożenia groźbą zaatakowania przez programy pasożytnicze newralgicznych zbiorów informacji przechowywanych w systemach takich jak, bazy danych meldunkowych, ubezpieczenia społecznego, rejestry medyczne, rejestry pojazdów i inne. Te działające niemal niezauważalnie i przez lata programy powodują degenerację i przekłamania w gromadzonych danych. Pomijając ogromne koszta społeczne i finansowe weryfikacji czy odbudowania takich baz, realizacja i funkcjonowanie bieżących zadań na podstawie takich danych wprowadziłaby narastający, znaczny chaos w funkcjonowaniu administracji publicznej. W dzisiejszych czasach mamy do czynienia ze swoistą konwergencją jaka ma miejsce pomiędzy klasycznymi formami zamachu a atakiem cyberterrorystycznym.

W rękach terrorystów mogą znajdować się urządzenia stworzone z myślą o ataku skierowanym bezpośrednio na systemy komputerowego przetwarzania danych i informacje w nich zawarte. Są to bomby, pistolety generujące promieniowanie radiowe, elektromagnetyczne lub mikrofalowe. Urządzenia te tworzą silne pole bądź wiązkę promieniowania zdolne z pewnej odległości uszkodzić układy półprzewodnikowe, magnetyczne nośniki danych i trwale zniszczyć zapisane na nich informacje. Prace nad tego typu urządzeniami prowadzone były w wielu krajach świata, przypuszcza się, że najprawdopodobniej niezbędna do konstrukcji tych układów wiedza mogła „wypłynąć", z któregoś z krajów byłego Związku Socjalistycznych Republik Radzieckich.

6. Cyberterroryzm w kontekście Polski

W przypadku Polski ciągle jeszcze klasyczne ataki terrorystyczne oparte na którymś ze składników CBERN są w znacznym stopniu większym zagrożeniem niż atak elektroniczny. Oczywiście wraz ze wzrostem uzależnienia gospodarki od komputerowych systemów

przetwarzania informacji ryzyko to będzie rosło. Stopień zależności gospodarki od komputerowych systemów przetwarzania informacji jest znaczny, jednak w większości przypadków wyodrębnione, niezależne systemy informatyczne, w które z zewnątrz za pośrednictwem publicznych złączy nie można ingerować. Większe zagrożenie w tym przypadku stanowić mogą wirusy infekujące systemy przy udziale nieodpowiedzialnych pracowników. Z uwagi na fakt, że w Polsce występuje bardzo mało zdalnych systemów kontroli i zarządzania obiektami o znaczeniu strategicznym przede wszystkim należy uwzględniać ryzyko terroryzmu przy odpowiedzialnym i racjonalnym planowaniu przyszłych inwestycji i polityki teleinformatycznej. Nie oznacza to, że Polska jest całkiem bezpieczna przed różnymi formami tego typu zamachów. Można zaobserwować uzależnienie sprawnego funkcjonowania państwa od różnego rodzaju informacji publikowanych czy przekazywanych za pośrednictwem Internetu. W tym miejscu kryje się potencjalne niebezpieczeństwo manipulacji tymi informacjami. Obok tego istnieje dla Polski wiele zagrożeń o charakterze cyberterrorystycznym na przykład dla Intranetów. Zarówno na świecie jak i w Polsce najpoważniejsze konsekwencje mają zamachy dokonywane przez obecnych lub byłych pracowników. Ludzie ci posiadają niedostępną dla napastników z zewnątrz specjalistyczną wiedzę, którą nabyli w trakcie tworzenia lub zarządzania określonym systemem. Szansą na zabezpieczenie się przed tego typu wypadkami jest prowadzenie przemyślanej i konsekwentnej polityki bezpieczeństwa, na którą składa się zarówno bezpieczeństwo teleinformatyczne, jak i fizyczne komputerów lub serwerów. Szczególną rolę odgrywa prowadzenie tej polityki ma poziom świadomości istniejącego zagrożenia wśród personelu.

Z kolei jako państwo możemy być terytorium, ż którego może być przeprowadzony atak cyberterrorystyczny. Wydaje się, że niewiele można zrobić w tej sytuacji aby zapobiec takiemu rozwojowi wypadków. Można jednak przygotować się do wykrywania i ścigania tego typu przypadków. Obecnie w Polsce nie ma silnej, skonsolidowanej instytucji, która mogłaby się podjąć takiego wyzwania. Ustawowo obowiązek ten zależnie od charakteru sprawy ciążyć będzie na Policji i/lub Agencji Bezpieczeństwa Wewnętrznego to żadna z tych instytucji nie wydaje się być profesjonalnie przygotowana, aby takiemu wyzwaniu skutecznie i w pełni podołać. Przede wszystkim brak jest stosownego zaplecza prawnego, technicznego, ale również odpowiednio licznej i wyszkolonej specjalistycznie kadry zdolnej samodzielnie prowadzić dochodzenia, jak to ma miejsce w przypadku odpowiednich struktur FBI.

Z powodu braku odpowiednich uregulowań normatywnych polski system ochrony teleinformatycznej państwa nie jest zadowalający. Na płaszczyźnie legislacyjnej Polska ma spore zaległości, które utrudniają skuteczne wykrywanie i ściąganie działalności przestępczej w sieciach komputerowych, a istniejące uregulowania nie zawsze odpowiadają wymogom naszych czasów. W marcu 2009 roku przy współpracy Ministerstwa Spraw Wewnętrznych i Administracji oraz Agencji Bezpieczeństwa Wewnętrznego powstał Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011, rozpoczęcie prac nad programem zainicjowane zostało w związku z występującymi, skutecznymi atakami cyberterrorystycznymi w Estonii i Gruzji oraz nasilającym się zagrożeniem cyberterroryzmem na świecie.

Biorąc pod uwagę fakt, że w bardzo szybkim czasie w Polsce wdrażanych jest wiele typowych dla nowoczesnego społeczeństwa informacyjnego rozwiązań teleinformatycznych narasta potrzeba zorganizowanego oraz kompleksowego przeciwdziałania atakom komputerowym. Dzięki dotacjom z Unii Europejskiej administracja publiczna rozwinęła wewnętrzne systemy informatyczne, które wspierają

procesy związane z bezpieczeństwem państwa oraz zarządzaniem państwem. Zostały udostępnione dla podmiotów prawnych i obywateli świadczone drogą elektroniczną usługi. Podmioty komercyjne zwiększyły zakres tego typu usług.

W XXI wieku w obszar teleinformatyki przeniosły się istotne dla prawidłowego funkcjonowania społeczeństwa i państwa procesy. W takiej sytuacji rodzi się potrzeba opracowania programu, który by na poziomie państwa koordynował ochronę jego informatycznych zasobów oraz by działanie państwa i życie polskich obywateli nie zostało sparaliżowane tak jak w Estonii. W wyżej wymienionym programie zawarte są założenia działań o charakterze organizacyjno-prawnym, edukacyjnym oraz technicznym, które mają na celu powiększenie zdolności do zwalczania i zapobiegania zjawisku cyberterroryzmu oraz innych zagrożeń dla bezpieczeństwa państwa pochodzących z publicznych sieci teleinformatycznych.

Do korzyści programu należy zaliczyć:

- zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa skutkujące zwiększeniem poziomu odporności państwa na ataki cyberterrorystyczne;
- stworzenie i realizacja spójnej, dla wszystkich zaangażowanych podmiotów administracji publicznej oraz innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa, polityki dotyczącej bezpieczeństwa cyberprzestrzeni;
- zmniejszenie skutków ataków cyberterrorystycznych, a przez to kosztów usuwania ich następstw;
- stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni państwa oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa;
- zwiększenie kompetencji odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa oraz innych systemów i sieci administracji publicznej;
- zwiększenie świadomości użytkowników systemów dostępnych elektronicznie oraz sieci teleinformatycznych w zakresie metod i środków bezpieczeństwa.

Program ochrony cyberprzestrzeni jest pierwszym tego typu dokumentem w Polsce i ma na celu zainicjowanie działań, które pozwolą stworzyć jedną i spójną strategię ochrony cyberprzestrzeni RP na najbliższe lata, będącą elementem składowym budowy szerokiej strategii bezpieczeństwa państwa. Wraz ze wzrostem ilości informacji i usług przenoszonych do Internetu i innych sieci informatycznych wzrasta również zagrożenie ataku mającego ich zniszczenie lub uniemożliwienie dostępu do nich. Atak ten może być zainicjowany z dowolnego miejsca na świecie. Budowana w ostatnich latach polska strategia przeciwdziałania takim atakom może pozwolić ich uniknąć lub choć zminimalizować ich skutki.

Wnioski

W dzisiejszych czasach, erze komputerów, technologii, informatyki nikt już chyba nie wątpi w ryzyko wystąpienia ataku cyberterrorystycznego wymierzonego w infrastrukturę krytyczną państwa. Prawdziwym zadaniem i zarówno wyzwaniem jest umiejętność wykrywania ataków w przestrzeni wirtualnej w odpowiednim czasie oraz umiejętność skutecznego zabezpieczenia się przed ich działaniem na elementy infrastruktury krytycznej państwa. Nie ma do tej pory jasnej i przejrzystej wizji cyberprzestrzeni, w związku z tym

nie istnieje żaden punkt, z którego można dostrzec nadchodzące ataki i monitorować ich rozprzestrzenianie się. Przełom XX i XXI wieku pokazał, że cyberprzestrzeń powoli staje się swoistym „układem nerwowym" państwa. Tysiące połączonych ze sobą komputerów składa się na system sterowania strukturami administracyjnymi, politycznymi, społecznymi danego kraju oraz pozwalają funkcjonować podstawowym instrumentom infrastruktury. Internet oraz cyberprzestrzeń razem stworzyły pewien rodzaj istotnych zależności, które w groźny i zarazem nieprzewidywalny sposób potrafią zmieniać swoją naturę. Teleinformatyczne systemy wciąż posiadają wiele słabych punktów, które mogą umożliwić przeprowadzenie ataku informatycznego, który obniży w istotny sposób bezpieczeństwo informacyjne. Przed zjawiskiem cyberterroryzmu nie można się uchronić. Postęp technologiczny, rozwój nauk informatycznych, nowe generacje komputerów, procesorów, miniaturyzacja urządzeń, globalny rozwój sieci informatycznej - wszystko to sprawia, że będziemy coraz częściej w środkach masowego przekazu słyszeli o atakach bądź próbach ataków na strony internetowe instytucji państwowych, banków, przedsiębiorstw czy mediów.

Literatura

1. Bógdoł-Brzezińska A., Gawrycki M.F.: Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warszawa, 2003.
2. Hoffman B.: Oblicza terroryzmu. Warszawa, 1999.
3. Jakubki K.J.: Przestępczość komputerowa – zarys problematyki. Prokuratura i Prawo 1996.
4. Kisieliński S.: Rząd chce chronić cyberprzestrzeń RP. Computerworld.pl, 5 lutego 2009.
5. Przestępczość zorganizowana, świadek koronny, terroryzm w ujęciu praktycznym. Pod red. Pływaczewski E. Kraków, 2005.
6. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, Warszawa, 2009.
7. Verton D., Black Ice: Niewidzialna Groźba Cyberterroryzmu. Gliwice, 2004.
8. Wójcik J.: Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne. Warszawa, 2006.
9. Weimann G.: www.terror.net: How Modern Terrorism Uses the Internet. United States Institute of Peace. Washington, 2004.

Prof. dr hab. inż. Marian KOPCZEWSKI
Instytut Polityki Społecznej i Stosunków Międzynarodowych
Politechnika Koszalińska
75-343 Koszalin, ul. Kwiatkowskiego 2e/423
e-mail: marian.kopczewski@tu.koszalin.pl