ARCHIWUM KRYMINOLOGII, T. XXVIII, 2005-2006
PL ISSN 0066-6890

SEBASTIAN SERWIAK

CYBERTERRORYZM — NOWE ZAGROŻENIE DLA BEZPIECZEŃSTWA

Ataki terrorystyczne na cele w Stanach Zjednoczonych i w Europie stały się impulsem do rozpoczęcia zakrojonych na ogromną skalę działań zmierzających do zagwarantowania bezpieczeństwa obywatelom tych państw. Przedsięwzięcia te ukierunkowane zostały w głównej mierze na bezpieczeństwo fizyczne przepływu osób i towarów oraz wykrywanie aktywności siatek terrorystycznych. Nowoczesne wolnorynkowe demokracje nie mogą pozwolić sobie na wyizolowanie się ze światowej sieci powiązań ekonomicznych, naukowych ani kulturowych. Krok taki byłby niewątpliwym sukcesem organizacji terrorystycznych. Z tego też powodu wydano znaczne sumy na inwestycje w zakresie bezpieczeństwa ruchu lotniczego, portów morskich, szlaków kolejowych, uszczelnienia granic państwowych i tym podobnych obiektów. Drugie ze wspomnianych wyzwań stojących przed organami ścigania jest jednak znacznie trudniejsze do realizacji. W Unii Europejskiej, Stanach Zjednoczonych, Izraelu oraz w innych państwach wprowadza się w życie kolejne projekty badawcze, które mają w efekcie dać organom ścigania zaawansowane technologicznie narzędzia do walki ze światowym terroryzmem. Narzędzia te to przede wszystkim instalacje sprzętowo-informatyczne służące do analizy otaczających nas zgiełków informacyjnych i wychwycenie z niego podejrzanych rodzajów aktywności. Postulowane systemy mają obejmować kamery przemysłowe, mikrofony, analizę ruchu i danych w sieciach teleinformatycznych oraz wiele innych dostępnych źródeł informacji. Proponowane systemy automatycznego przetwarzania danych charakteryzuje jednak pewna fundamentalna słabość, jaką jest brak uniwersalnego wzorca, na podstawie którego mogłyby one określać, co jest zachowaniem podejrzanym, a co normalnym. W związku z trudnościami, jakich przysparza sama definicja pojęcia terroryzmu, zbudowanie takiego algorytmu nie wydaje się rzeczą łatwą. O ile jednak braki definicyjne, jak wykażę to w niniejszym opracowaniu, można starać się doraźnie skompensować, wykorzystując definicję operacyjną, to chcąc zbudować wiarygodny model „zachowań terrorystycznych", staniemy w pewnym momencie w obliczu znacznie poważniejszej przeszkody, mianowicie braku danych empirycznych. Na tego typu dane składają się na przykład zachowania wykrytych rezydentów grup terrorystycznych, techniki ich finansowania czy choćby szczegóły przygotowań i przeprowadzenia samych zamachów. Jako że wymienione dane mogą pochodzić jedynie od organów ścigania i służb wywiadowczych poszczególnych państw, prawdopodobnie nigdy w całości nie trafią one do niezależnych międzynarodowych grup badawczych[1].

[1] Istnieją ważkie przesłanki pozwalające przypuszczać, iż trudności te można będzie w znacznej mierze wyeliminować, a to za sprawą efektów projektów badawczych z pogranicza sztucznej inteligencji,

Bezpieczeństwo obywateli, poza wymiarem fizycznym, to również zapewnienie niezakłóconego funkcjonowania podstawowych elementów infrastruktury, takich jak elektrownie, ujęcia wody, produkcja żywności czy funkcjonowanie służby zdrowia i innych służb ratunkowych. W tym właśnie aspekcie kluczową rolę do odegrania mają systemy telekomunikacyjne, gwarantujące prawidłowy przepływ komunikatów nadawcy do odbiorcy. Funkcje każdego z tych systemów mogą zostać zaburzone przez konwencjonalne działania terrorystyczne, takie jak podłożenie ładunku wybuchowego, skażenie chemiczne czy biologiczne. Rozwój technologiczny cywilizacji doprowadził jednak do tego, że nasze wirtualne działania w cyberprzestrzeni mają jak najbardziej namacalny efekt w otaczającym nas fizycznym świecie. Taki stan rzeczy powoduje, iż dla przestępców wyłonił się cały wachlarz nowych możliwości, na które powyższe obiekty są automatycznie narażone, dlatego projektując je i chroniąc, musimy uwzględniać nowy typ zagrożenia: cyberterroryzm.

Wraz ze wzrostem uzależnienia funkcjonowania państwa od komputerowych systemów przetwarzania informacji ryzyko ataku cyberterrorystycznego nieuchronnie wzrasta. Ciągła rozbudowa systemów bezpieczeństwa to ogromne nakłady finansowe na wyposażenie techniczne, infrastrukturę i personel. Obiekty takie jak porty morskie i lotnicze, dworce, elektrownie atomowe, miejsca kultu religijnego i obiekty rządowe, w których podnosi się standardy bezpieczeństwa, nie wyczerpują długiej listy potencjalnych celów terrorystycznych[2]. Związane z tym inwestycje finansowe są kosztowne i o czym należy pamiętać - nie jednorazowe. Przyczyniają się one do stałego wzrostu kosztów funkcjonowania państwa, który zapowiada też utrzymująca się tendencja na świecie. Niestety w chwili obecnej większy nacisk kładzie się na zabezpieczenie się przed skutkami klasycznych ataków terrorystycznych niż ich elektronicznych odpowiedników.

Rodzi się jednak pytanie, czy prowadzone z takim rozmachem działania i ponoszone nakłady finansowe na bezpieczeństwo są faktycznie niezbędne, czy istnieje realne zagrożenie atakiem cyberterrorystycznym. Niestety wiele wskazuje na to, że zagrożenie takim atakiem jest realne, choć jego prawdopodobieństwo różne w zależności od stopnia zinformatyzowania społeczeństwa. Popularny w USA termin „cyfrowe Pearl Harbor" bardzo sugestywnie przemawia do wyobraźni wielu decydentów, sugerując, jak poważne mogą być konsekwencje skoordynowanego ataku cyberterrorystycznego (Alexander 1999, 2000).

Na potwierdzenie tej tezy można przywołać wnioski wynikające z odtajnionej części ćwiczeń przeprowadzonych w 1997 r. przez amerykańską National Security Agency pod kodową nazwą ELIGIBLE RECEIVER. Choć głównym celem tych ma-

prowadzonych w kilku ośrodkach na świecie. Na podstawie bardzo obiecujących wstępnych wyników badań nad tzw. „systemami agentowymi" potwierdzono przydatność tego podejścia również do rozwiązywania problemów z zakresu zarządzania bezpieczeństwem. Zasadniczą ideą funkcjonowania tych systemów jest niezależność pojedynczego „agenta" - programu komputerowego, i jego zdolność do uczenia się i tworzenia na bazie tej wiedzy własnych sądów w kwestii tego, co jest zachowaniem normalnym, a co anormalnym, zob. Dobrowolski 2002.

[2] Można wskazać cały szereg szczególnie atrakcyjnych celów zamachów terrorystycznych, z których większość mieści się jednak w kilku podstawowych obszarach, takich jak: telekomunikacja, produkcja i przesyłanie energii, transport osób i towarów, systemy bankowe i finansowe, systemy przetwarzania i zaopatrzenia w wodę, służby ratunkowe oraz administracja państwowa. Szerzej na ten temat: Ścibek 2005, s. 641 i nast.

newrów było Dowództwo Sił Pacyfiku Stanów Zjednoczonych, to ćwiczenia wykazały, iż hakerzy NSA rozmieszczeni w różnych punktach świata są w stanie przy użyciu ogólnodostępnych narzędzi hakerskich osiągnąć znacznie więcej niż tylko zamierzony cel. W trakcie prowadzonych symulacji włamano się m.in. do kilku wojskowych sieci komputerowych, ale najbardziej brzemienny w skutkach był fakt wykazania przez NSA, iż jest w stanie wyłączyć sieć dystrybucji energii elektrycznej na terenie prawie całych Stanów Zjednoczonych. Te skomasowane i skoordynowane elektroniczne ataki zostały dostrzeżone przez nieświadome ćwiczeń FBI i Pentagon, które nie były jednak w stanie im przeciwdziałać ani wykryć źródła ataku (Lawson 2002, s. 6 i nast.).

Ćwiczenia ELIGIBLE RECEIVER udowodniły, że amerykańska sieć energetyczna jest piętą achillesową gospodarki USA. Fakt, iż może ona być zdalnie wyłączona przez terrorystę, szpiega czy popisującego się hakera spędza sen z powiek instytucjom takim jak US-CERT[3]. Najsłabszym ogniwem, jak pokazuje życie, są niedostatecznie lub wcale niezabezpieczone systemy SCADA w podstacjach i serwery w centrach kontroli. Fakt ten potwierdzają też wydarzenia z 2001 r. w Kalifornii, gdzie doszło do poważnego w konsekwencjach włamania do serwera Cal-ISO firmy odpowiedzialnej za zarządzanie większością sieci energetycznej w tym regionie. Włamanie to tajemniczo zbiegło się w czasie z najpoważniejszym lokalnie kryzysem energetycznym 7 i 8 maja 2001 r., w trakcie którego przerwy w dostawie energii elektrycznej dotknęły blisko 400 tys. odbiorców[4].

Nie zawsze efektem ataku terrorystycznego musi być natychmiastowe wywołanie zniszczeń i śmierci ludzi w znacznej skali. Wydaje się, że w dzisiejszym złożonym świecie zależności gospodarczych oraz zależności typu człowiek-maszyna i obywatel-państwo równie skutecznym sposobem walki terrorystycznej może okazać się subtelne oddziaływanie na te relacje i stopniowa ich degeneracja.

Al-Ka'ida postawiła sobie za zadanie nie uwolnienie grupy bojowników czy wyzwolenie danego terytorium, ale zniszczenie zachodniego modelu życia (Bodansky 1999, s. 185 i nast.). Przy tak sformułowanej misji zarówno fizyczna destrukcja

[3] W 1998 r. Prezydencką Dyrektywą Wykonawczą 63 dotyczącą Ochrony Krytycznej Infrastruktury utworzono Centrum Ochrony Krytycznej Infrastruktury (National Infrastructure Protection Center - NIPC), w skład którego weszli przedstawiciele FBI, Departamentu Handlu, Energii, Transportu oraz innych agencji rządowych, jak i reprezentanci sektora prywatnego. Celem działania NIPC, poza samą reakcją na mające już miejsce ataki, była wymiana informacji, analiza i ostrzeganie o istniejących i potencjalnych zagrożeniach, oraz prowadzenie dochodzeń w sprawach dokonanych włamań komputerowych. Obecnie, po powstaniu Homeland Security NIPC, została wchłonięta w jego struktury i funkcjonuje z małymi zmianami jako US-CERT (United States - Computer Emergency Respond Team). Zob. „Terrorism...".

[4] Ataki na Cal-ISO trwały niewykryte przynajmniej przez 17 dni. Jak wykazało śledztwo, hakerzy wykorzystali lukę w systemie Solaris, aby dostać się do serwera. Następnie zainstalowali pakiet narzędzi umożliwiający uzyskanie dostępu na prawach administratora, po czym przystąpili do instalacji w systemie swojego oprogramowania. System Cal-ISO nie był w żaden sposób zabezpieczony przed atakami z sieci, nie posiadał *firewalla,* wykorzystywana konfiguracja była konfiguracją podstawową, a wszelkie logi w jednej kopii przechowywano tylko na tym jednym serwerze. Przedstawiciele Cal-ISO w oficjalnym komunikacie potwierdzili włamanie do ich serwera, zaprzeczyli jednak, iż miało ono wpływ na dostawy energii czy wiarygodność systemu informatycznego Zob.: *Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack,* SANS Institute 2001, A GSEC Practical Assignment.

ośrodków finansowych, przemysłowych czy naukowych, jak i doprowadzenie ich do ruiny finansowej czy chaosu logistycznego wydaje się efektywną metodą walki. Unicestwienie lub choćby osłabienie jednego ogniwa łączącego obywatela zachodniej cywilizacji z jego modelem życia, obniżenie zaufania do instytucji państwowych, poczucia bezpieczeństwa czy wiarygodności informacji przekazywanych mu przez media przybliża terrorystów do destabilizacji systemu demokratycznego. Uzasadnione wydaje się zatem twierdzenie, że niszczenie społecznego zaufania do bezpieczeństwa oferowanego obywatelom przez państwo jest jedną z dróg, jaką z dużą dozą prawdopodobieństwa wybiorą organizacje terrorystyczne. Dotyczy to zwłaszcza grup takich jak Al-Ka'ida, mających wystarczające zaplecze finansowe i kadrowe do prowadzenia działań cyberterrorystycznych na szeroką skalę. Mimo że cyberprzestrzeń nie odegrała jeszcze znaczącej roli w działaniach terrorystycznych, wiele przemawia za tym, iż jest to wręcz wymarzone narzędzie do prowadzenia tego typu walki[5]. Świadczą o tym niewysokie koszta organizacji i przeprowadzenia zamachu, doskonałe możliwości komunikacji i koordynacji działań, ciągle niska świadomość społeczna istniejącego zagrożenia oraz łatwy dostęp do specjalistycznej wiedzy i niezbędnych narzędzi programowych[6]. Koronnym argumentem na rzecz tej formy realizacji aktu terrorystycznego jest jednak fakt, iż cyberterrorysta, w przypadku jeżeli atak się nie powiedzie, nie ginie ani nie zostaje natychmiast aresztowany, a tym samym wyeliminowany jako zagrożenie. Przeciwnie, nabiera on doświadczenia i przygotowuje się do kolejnego zamachu. Jest to o tyle istotne, że wbrew obiegowej opinii większość terrorystów nie podejmuje misji samobójczych. Zgodnie z danymi Centralnej Agencji Wywiadowczej (CIA), statystycznie 62% przeprowadzających zamachy terrorystów ma plan awaryjny bądź plan ucieczki, jeżeli sytuacja nie ułoży się po ich myśli (Ganeles 2002, s. 620).

Część uczestników dyskusji o realności zagrożenia podnosi kwestie, iż niektóre kraje uznawane za wspierające terroryzm, takie jak na przykład Afganistan, mają słabo rozwiniętą infrastrukturę teleinformatyczną i przez to są niezdolne do podjęcia ofensywnych działań cyberterrorystycznych. Ma to być konsekwencją faktu, iż brak tam fachowej wiedzy oraz ekspertów branży IT, gotowych do przeprowadzenia takiego typu ataku, czy wręcz samej świadomości istnienia takich możliwości. Pogląd ten wydaje się jednak nieco naiwny w świetle otaczających nas faktów. Już w 1996 r. Osama bin Laden wyposażył swoją kryjówkę w górach Afganistanu w laboratorium komputerowe i realizowany drogą satelitarną dostęp do internetu (Arquilla, Ronfeldt,

[5] Cyberprzestrzeń odegrała istotną, a według niektórych decydującą rolę, w przypadku zorganizowania i koordynacji ataków na wieże WTC 11 września 2001 r. Zaszyfrowana komunikacja, którą posługiwali się autorzy i wykonawcy tego projektu, umożliwiła im sprawne i skryte funkcjonowanie i komunikowanie się praktycznie bez groźby wykrycia przez służby wywiadowcze. Sprawcy wykorzystywali do komunikacji strony internetowe, co jest bezpieczniejsze niż poczta elektroniczna, oraz stosowali kryptografię. Nie jest to zresztą jedyny przypadek stosowania kryptografii przez terrorystów. W trakcie zamachu bombowego na WTC w 1993 r., jak wykazało śledztwo, uczestniczący aktywnie w jego organizacji i aresztowany w 1995 r. na Filipinach Ramzi Yousef miał na swoim laptopie zaszyfrowane dane dotyczące przygotowania i koordynacji tego zamachu oraz kilku innych nowych akcji terrorystycznych. Zob. Kelly 2001; także: Statement 2001.

[6] W trakcie wspomnianego już starcia informacyjnego pomiędzy Izraelem a Autonomią Palestyńską po obu stronach konfliktu powstały strony WWW oferujące wszystkim chętnym pełny zakres wiedzy, szkolenie i narzędzia konieczne do prowadzenia tej sieciowej wojny. Przykładem jest izraelska strona internetowa: www.wizel.com.

Zanini 1999). Historia uczy nas też, iż terroryści mogą przeprowadzić dowolny atak, wykorzystując naszą własną infrastrukturę przeciw nam, i mogą to zrobić 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. Teleinformatyczne podziemie dysponuje ludźmi o ogromnej wiedzy i zdolnościach, którzy są w stanie przeprowadzić najbardziej finezyjny atak informatyczny, kwestią jest jedynie cena takiej usługi. Istnieją też symptomy wskazujące na okoliczność, iż doszło do nawiązania na tym polu, przynajmniej sporadycznej, współpracy pomiędzy organizacjami terrorystycznymi a zorganizowanymi grupami przestępczymi. Grupy przestępcze funkcjonują jako nieformalne przedsiębiorstwa nastawione na generowanie maksymalnych zysków, nie są przy tym związane ramami prawnymi i moralnymi. W tym świetle wydaje się mało prawdopodobne, aby przy odpowiedniej stymulacji finansowej nie zdecydowały się dokonać zamachu, a przynajmniej wyposażyć składających zamówienie w odpowiedni sprzęt, wiedzę i ludzi (Brenner, Goodmann 2002; Barkham 2001, s. 107).

Szczęśliwie do przeprowadzenia naprawdę złożonego ataku cyberterrorystycznego potrzeba czasu na jego przygotowanie. Czas planowania i przygotowania zamachu jest jednym z nielicznych czynników, który daje szansę organom ścigania i bezpieczeństwa państwa na przeciwdziałanie. W przypadku komputerów ma on też szczególne znaczenie z innego powodu. Tutaj bowiem paradoksalnie sami hakerzy komputerowi w znacznym stopniu przeciwdziałają możliwości organizacji złożonych, wielopoziomowych i długofalowych aktów cyberterrorystycznych. Ci pasjonaci sprzętu komputerowego i techniki spędzają życie, wyszukując i demaskując publicznie słabości poszczególnych systemów. Część z nich używa co prawda tej wiedzy nielegalnie dla zabawy, sławy, emocji albo zdobycia pieniędzy. Wszyscy jednak czyniąc tak, demaskują błędy oprogramowania i przyczyniają się walnie do ich stopniowej, systematycznej eliminacji. Szczęśliwie ten ciągły wyścig z czasem utrudnia zaplanowanie - przy wykorzystaniu istniejących luk bezpieczeństwa - złożonego ataku terrorystycznego. Ocenia się, że w dobrze administrowanych systemach wykryte i krytyczne dla działania systemu luki istnieją średnio nie dłużej niż pięć dni.

Inną okolicznością, dzięki której nie doświadczyliśmy jeszcze tego typu ataku, może być również fakt, że obecni liderzy organizacji terrorystycznych są wytworami starego „fizycznego" świata i jego sposobu myślenia i działania. Jednak jest to tylko stan przejściowy. Tak jak w każdej innej instytucji również w szeregach organizacji terrorystycznych zachodzi ciągły proces wymiany pokoleń. Wstępujący w ich szeregi młodzi adepci mają już inne podejście do otaczających ich technologii i wirtualnych światów. Są w pełni świadomi potencjału, jaki niosą one ze sobą. Z tej perspektywy fakt, iż dotychczas nie doświadczyliśmy jakiegoś poważnego zamachu cyberterrorystycznego wydaje się raczej rodzić pytanie o jego termin niż możliwość zaistnienia.

Skuteczne przeciwdziałanie podobnym wydarzeniom oraz ich konsekwencjom wymaga naukowego podejścia do problemu i zbadania go. W tym celu należy zgromadzić niezbędne dane, zbudować hipotetyczne scenariusze ataków i na podstawie tych ustaleń naukowo zbadać problem. Odszukanie i zgromadzenie danych niezbędnych do analizy nie jest jednak rzeczą łatwą. Wracamy tutaj do problemu, który sygnalizowałem już na wstępie niniejszego opracowania; jest nim brak jednej, uznanej definicji tego pojęcia. Nie możemy zatem na tej podstawie stwierdzić, które działania

można określić mianem cyberterroryzmu, a które nim nie są. Teoretycznie znamiona działań o charakterze terrorystycznym może mieć już samo wysłanie poczty elektronicznej, podczas gdy w innych okolicznościach nawet wyłączenie sieci energetycznej i doprowadzenie do wielomilionowych strat w gospodarce wcale takim działaniem być nie musi. Z tego powodu nie możemy niestety definiować pojęcia „cyberterroryzm", odwołując się do definicji „terroryzmu" przede wszystkim ze względów politycznych. Jak głosi często powtarzana, wciąż żywa maksyma: „Człowiek będący dla jednych terrorystą dla innych jest bojownikiem o wolność". W podobnym duchu wypowiadał się również Jaser Arafat - nieżyjący lider Autonomii Palestyńskiej[7].

Wobec zaistniałej sytuacji możemy szukać pomocy u znawców tematu oraz korzystać z definicji operacyjnych terroryzmu oraz cyberterroryzmu funkcjonujących na potrzeby konkretnych instytucji mających do czynienia z tą problematyką.

Przyjmuje się, iż samo pojęcie „cyberterroryzm" powstało w 1997 r. za sprawą niejakiego Barry'ego C. Collina, naukowca z Instytutu Bezpieczeństwa i Wywiadu (Institute for Security and Intelligence) w Kalifornii, który zdefiniował je jako połączenie cybernetyki i terroryzmu (Krasavin 2000). W tym samym roku Mark Pollitt, agent specjalny FBI, przedstawił definicję operacyjną cyberterroryzmu, uznając go za „zaplanowany, politycznie umotywowany atak przeprowadzony przez subnarodowe grupy lub tajnych agentów przeciwko informacjom, systemom komputerowym, i danym, co skutkuje przemocą wobec niemilitarnych celów" (Collin 1996; cyt. za: Krasavin 2000). Opis ten jest logicznym rozwinięciem definicji terroryzmu przyjętej przez Departament Stanu w Tytule 22 Kodeksu Stanów Zjednoczonych, Sekcji 2656F(d), gdzie czytamy: „Terroryzm oznacza zaplanowaną, politycznie motywowaną przemoc, podjętą przez subnarodowe grupy lub tajnych agentów przeciw niemilitarnym celom, zwykle mającą wpłynąć na opinię publiczną"[8]. W tym samym miejscu możemy również odnaleźć definicję terminu „terroryzm międzynarodowy", który został scharakteryzowany jako „terroryzm z udziałem mieszkańców terytorium więcej niż jednego kraju".

Wcześniej, bo od lat 80. XX w. Federalne Biuro Śledcze posługiwało się terminem „terroryzm" definiowanym jako „bezprawne użycie siły lub przemocy przeciwko osobom lub przedmiotom w celu zastraszenia lub dokonania wymuszenia na rządzie, grupie ludzi lub jakiejkolwiek ich części dla osiągnięcia politycznych lub społecznych celów"[9]. Powyższa definicja posłużyła jako punkt wyjścia dla uznanej w świecie ekspert Dorothy E. Denning do stworzenia własnej definicji cyberterroryzmu, który określiła ona jako bezprawny atak i groźby ataku przeciwko komputerom, sieciom i informacjom w nich przechowywanym, jeżeli mają na celu zastraszenie lub dokona-

[7] „(...) różnica między rewolucjonistą a terrorystą sprowadza się do tego, o co każdy z nich walczy. Ktokolwiek broni słusznej sprawy, walczy o wolność i wyzwolenie swego kraju od najeźdźców, osadników i kolonistów, nie może być nazwany terrorystą (...)" - J. Arafat, *Przemówienie na forum Zgromadzenia Ogólnego ONZ 13 listopada 1974 r,* cyt za: Hoffman 1999, s. 24.

[8] „The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.", Title 22 of the United States Code, Section 2656f(d) (1994).

[9] „The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives." U.S. Department of Justice, FBI, Terrorism in the United States 34 (1988).

nie wymuszenia na rządzie lub społeczeństwie w celu osiągnięcia politycznych bądź społecznych celów (Denning 2000).

Jak wynika z powyższego krótkiego zestawienia, definicje cyberterroryzmu mają charakter zawężający w stosunku do swoich pierwowzorów, definicji terroryzmu. Cyberterroryzm jest jedynie nowym wcieleniem starego zjawiska. W sposób naturalny zatem różne funkcjonujące definicje terroryzmu obejmują swoim znaczeniem jego szczególne odmiany, takie jak cyberterroryzm czy bioterroryzm.

Warto jeszcze przytoczyć definicję, jaką posługuje się NIPC, instytucja kluczowa w amerykańskim systemie zwalczania i przeciwdziałania cyberprzestępczości oraz cyberterroryzmowi. Instytucja ta określa cyberterroryzm jako czyn kryminalny popełniony z wykorzystaniem komputerów, powodujący przemoc, śmierć i/lub zniszczenia i tworzący poczucie zagrożenia w celu zmuszenia rządu do zmiany jego polityki. Aby więc w tym ujęciu mówić o cyberterroryzmie, musimy wypełnić kryteria politycznej motywacji, niszczycielskiego efektu oraz wykorzystania technologii komputerowej.

Żadna z powyższych charakterystyk cyberterroryzmu, podobnie jak w przypadku definicji terroryzmu, nie jest jednak w pełni satysfakcjonująca. Najpoważniejszy zarzut, jaki można sformułować, to niebezpieczeństwo stosowania zbyt szerokiej wykładni do przedstawionych definicji. Przy takiej interpretacji do grupy aktów terrorystycznych można zaliczyć również działalność aktywistów społecznych. Agitacja obywatelska skutkująca zalewem serwerów ministerstwa e-mailami o treści stanowiącej protest przeciwko określonej polityce rządu może doprowadzić do zablokowania systemu pocztowego i być zinterpretowana jako zamach o podłożu politycznym.

Niebezpieczeństwo zaistnienia podobnego scenariusza skłania część autorów do wyraźnego wyodrębnienia tego typu sytuacji. Wspomniana już Dorothy E. Denning proponuje termin „haktywista" na określenie grupy ludzi, którzy posługując się swoimi umiejętnościami i wiedzą informatyczną, wykorzystują je do walki w ramach przyznanych im demokratycznych swobód obywatelskich (Denning 2000). W tym kontekście blokadę serwera pocztowego należy porównać do zorganizowanej akcji protestacyjnej polegającej na fizycznej blokadzie danego urzędu, co jest spotykaną i akceptowaną w demokracjach formą manifestacji niezadowolenia społecznego.

Przedstawione poglądy nie wyczerpują oczywiście rozległego zagadnienia, jakim jest próba zdefiniowania cyberterroryzmu, mają jedynie wprowadzić czytelnika w tę tematykę. Problem ten został szerzej omówiony choćby przez A. Bogdół-Brzezińską i M.F. Gawryckiego, którzy zbudowali własną roboczą definicję cyberterroryzmu, określając go jako politycznie motywowany atak lub groźbę ataku na komputery, sieci lub systemy informacyjne dla zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów. W szerszym rozumieniu ma to także być wykorzystanie internetu przez organizacje terrorystyczne do komunikowania się, propagandy i dezinformacji (Bógdał-Brzezińska, Gawrycki 2003, s. 73). Właśnie ze względu na wyróżnienie i zwrócenie uwagi czytelnika na aspekt działań logistycznych i informacyjnych grup ekstremistycznych definicja ta jest szczególnie warta przytoczenia. Zasygnalizowany tu aspekt zostanie szerzej omówiony w dalszej części niniejszego opracowania.

Definicyjne rozważania prowadzone na temat aktywności terrorystycznej w cyberprzestrzeni dodatkowo komplikuje problem oddzielenia jej od zjawiska wojny informacyjnej (*information warfare*). Jest to stosunkowo nowe zagadnienie, bar-

dzo poważnie traktowane zwłaszcza przez rządy krajów zaawansowanych technologicznie. Wojna informacyjna winna być rozumiana w dwójnasób: jako nowe rodzaje uzbrojenia oraz jako kompletnie nowy wymiar konfliktów międzynarodowych. W pierwszym ujęciu przez wojnę informacyjną będziemy rozumieć wykorzystanie nowych rodzajów broni oddziaływujących na systemy elektroniczne przeciwnika. Chodzi tu o bezpośredni wpływ na sytuację na polu bitwy w drodze niszczenia i zakłócania systemów informatycznych wroga, zdobywania danych strategicznych dotyczących na przykład ilości i rodzajów środków walki, ich położenia, stanu, a jednocześnie ochrony własnych zasobów. W przypadku obu operacji militarnych w Zatoce Perskiej mieliśmy przykład takiej właśnie wojny informacyjnej przy całkowitej dominacji wojsk amerykańskich nad irackim przeciwnikiem. Systemy zwiadu elektronicznego, satelity i odbiorniki GPS, płynny przepływ danych między jednostkami operującymi na polu bitwy a dowództwem, w połączeniu z systematycznym niszczeniem i zakłócaniem irackich systemów łączności, wytworzyły absolutną hegemonię informacyjną wojsk koalicji.

Wojna informacyjna w drugim ujęciu może mieć charakter czysto wirtualny i w całości rozegrać się w cyberprzestrzeni, tak jak to miało miejsce w przypadku opisanego dalej konfliktu chińsko-amerykańskiego. W praktyce jednak większość podejmowanych obecnie działań militarnych wykorzystuje w różnym stopniu obie wspomniane formy wojny informacyjnej. Działania wojenne prowadzone są przy użyciu najnowocześniejszego uzbrojenia, jakie posiada dana strona, a równolegle przez dostępne media realizowana jest kampania propagandowa. O tym jednak, iż cały czas mamy do czynienia z dwiema twarzami tego samego zjawiska, świadczy wspólny cel obu tych działań. Jest nim oczywiście, tak jak w przypadku tradycyjnego fizycznego konfliktu, uzyskanie absolutnej dominacji, w tym przypadku informacyjnej.

Oddziaływanie na opinię publiczną stanowi oręż walki przede wszystkim podmiotów niepaństwowych: mniejszości etnicznych, narodowych, czyli grup o nieproporcjonalnie mniejszej sile militarnej niż przeciwnik. Doskonałym przykładem przewagi, jaką może dać skutecznie przeprowadzona wojna informacyjna jest konflikt w Chiapas. 1 stycznia 1994 r., kiedy w życie wchodził układ o wolnym handlu w Ameryce Północnej NAFTA, partyzanci z EZLN[10], nazwani później zapatystami, wypowiedzieli posłuszeństwo rządowi Meksyku. Walczyli przeciwko globalizacji, okrutnemu traktowaniu Indian i krzywdzącym stosunkom panującym na meksykańskiej wsi. Domagali się dymisji rządu Meksyku i reformy rolnej. Przeciwko rebeliantom skierowano wojsko, któremu powierzono misję stłumienia powstania. Media znajdujące się pod kontrolą władz miały ukazać widzom na całym świecie „jedyny słuszny" obraz tego konfliktu. Rząd Meksyku nie docenił jednak potęgi drzemiącej w internecie. Rebelianci i ich sympatycy założyli na całym świecie kilkanaście stron WWW traktujących o powstaniu w Chiapas i jednocześnie propagujących cele ich walki zawarte w *Declaración de la Selva Lacandona*. Rząd Meksyku traktował te działania jako zwykłe utarczki słowne, podczas gdy tak naprawdę była to prawdziwa wojna informacyjna, którą z druzgoczącą przewagą wygrywali zapatyści. Za pomocą internetu rozpowszechniano bieżące informacje i zdjęcia, ale również koordynowano działania militarne i organizację masowych manifestacji na całym świecie popierających dąże-

[10] Ejército Zapatista de Liberación Nacional, Chiapas Watch, http://www.zmag.org.

nia zapatystów w Meksyku. Ostatecznie wirtualna wojna doprowadziła do ugięcia się rządu Meksyku pod wpływem ciągłej presji opinii międzynarodowej. Rząd wstrzymał operacje militarne i zgodził się na rozmowy z ludźmi, których niedawno określał mianem „terrorystów", oraz przyznał im status „obywateli w stanie rebelii". Rewolucja w Chiapas była jakościowo inna niż większość działań partyzanckich prowadzonych w Ameryce Południowej i Łacińskiej. Okazała się ogromnym i niespodziewanym sukcesem nowej taktyki wojskowej - totalnej wojny informacyjnej[11].

Również w trakcie konfliktu bałkańskiego w Kosowie mieliśmy do czynienia z wojną informacyjną (Becker 1999). W tym przypadku obie strony prowadziły działania wymierzone w systemy przeciwnika. Odpowiedzią na akcje militarne NATO były ataki odwetowe na serwery NATO i rządu Stanów Zjednoczonych polegające na ich blokowaniu oraz zmianie wyglądu stron (Alexander 1999/2000, s. 83). Oprócz działań obliczonych na destrukcję Serbowie podjęli również akcję informacyjno-propagandową, rozsyłając do stacji telewizyjnych, dzienników, a nawet pojedynczych senatorów listy elektroniczne z apelami „o przerwanie bombardowań szkół, szpitali i innych obiektów, w których giną cywile" (Ashle 1999, s. 10). Na czas trwania konfliktu zawiązały się grupy wspierające obie strony i walczące ze sobą nawzajem. Działania przeciwko Stanom Zjednoczonym i NATO poparli hakerzy z Rosji. Kiedy zbombardowana została ambasada Chin w Belgradzie, bardzo aktywnie włączyli się do tego konfliktu hakerzy chińscy, którym przypisuje się m.in. włamanie na strony Białego Domu w Waszyngtonie.

Te wirtualne wojny oficjalnie przybierają charakter pojedynków między hakerami wywodzącymi się z państw będących stronami konfliktu lub sympatykami jego uczestników[12]. Choć utarczki te wyglądać mogą na spontaniczne poparcie polityki swojego rządu, to prawdziwych inicjatorów i sponsorów tych przedsięwzięć można jedynie się domyślać. Istnieją uzasadnione podejrzenia, że tego typu wirtualne wymiany ciosów są wykorzystywane do testowania systemów bezpieczeństwa informatycznego zaangażowanych państw oraz własnych możliwości ofensywnych. Klasycznym przykładem takiego konfliktu jest trwająca z krótkimi przerwami od 1999 r. wojna hakerów pomiędzy Chinami a Tajwanem[13]. W tym przypadku nie sposób odróżnić, czy ataki elektroniczne podejmowane są z pobudek czysto patriotycznych, czy też są sterowane przez poszczególne rządy. Do grupy podobnych batalii można również zaliczyć sytuację panującą między Indiami a Pakistanem czy konflikt izraelsko-palestyński. W przypadku tego ostatniego warto zwrócić uwagę na mało znany fakt, iż armia izraelska w prowadzonych działaniach militarnych na terenie Autonomii

[11] !Zapatistas! Documents of the New Mexican Revolution, http://lanic.utexas.edu/project/Zapatistas, także: http://www.eco.utexas.edu/facstaff/Cleaver/chiapas95.html.

[12] Do „wybuchu" wojny informacyjnej doprowadzić może nawet pojedynczy incydent. Do najpoważniejszego konfliktu tego typu w ostatnim czasie doszło w kwietniu 2001 r. po zderzeniu nad terytorium Chin chińskiego myśliwca z amerykańskim samolotem szpiegowskim EP-3. Grupy hakerów z Chin i Stanów Zjednoczonych przez dwa miesiące dokonywały ataków na strony WWW „wrogiego" państwa, zmieniając ich wygląd i treść bądź blokując do nich dostęp. Na przykład na stronach chińskich instytucji rządowych i firm pojawiały się hasła: „Gdzie nasz samolot, złodzieje?!"; zob. Gawrycka 2001.

[13] Wojna informacyjna wybuchła po tym, jak prezydent Tajwanu Li Teng-hui wypowiedział się, że stosunki z ChRL mają charakter specjalnych stosunków międzypaństwowych i wezwał do traktowania Tajwanu i Chin jako równoprawnych państw; zob. Laris 1999.

Palestyńskiej systematycznie i planowo niszczy infrastrukturę sieci komputerowych i likwiduje centrale operatorów internetowych (Shahtman 2002).

Niejasne relacje i brak wyraźnej granicy między cyberterroryzmem a walką informacyjną dodatkowo komplikują próby zdefiniowania obu tych zjawisk. Niektórzy autorzy dla rozróżnienia walki informacyjnej od cyberterroryzmu proponują posłużyć się kryterium podmiotowym rozgraniczającym państwa od aktorów niepaństwowych. W takiej sytuacji z cyberterroryzmem mielibyśmy do czynienia, gdy stroną atakującą jest aktor niepaństwowy. W przeciwnym przypadku, kiedy działania ofensywne prowadzi państwo, mamy do czynienia z wojną informacyjną. Pogląd ten jest jednak mocno kontrowersyjny i trudno się z nim zgodzić, gdyż stawia on wszelkie ruchy narodowowyzwoleńcze, w tym walczące o swe prawa mniejszości narodowe, w bardzo niekorzystnym położeniu.

Powyższe krótkie rozważania pokazują, z jakimi trudnościami trzeba się zmierzyć, aby stworzyć funkcjonalną i precyzyjną definicję cyberterroryzmu. Istniejące rozbieżności interpretacyjne powodują, iż wciąż trwa dyskusja co do istoty samego terroryzmu. W przypadku cyberterroryzmu na powyższe problemy nakłada się dodatkowo szereg złożonych zagadnień związanych z funkcjonowaniem społeczeństwa informacyjnego (Sieber 1998). W związku z tymi trudnościami i brakiem definicji, którą można by się posłużyć, należy raczej skupić się na opisowej prezentacji zagrożeń zaliczanych do cyberterroryzmu. Podobne stanowisko można także znaleźć w dokumentach Rady Europy (Council of EUROPE6... 2003, s. 125), która nie dała pełnej akceptacji jednej określonej definicji cyberterroryzmu, a jedynie posiłkowo posługuje się definicją zaproponowaną w art. 1 projektu International Convention to Enhance Protection from Cybercrime and Terrorism[14].

Katalog sposobów, na jakie terroryści mogą wykorzystać komputery, wydaje się ograniczony jedynie ich inwencją i rozwojem sieci. Poczynając od sabotażu, możemy tu znaleźć komunikację, szkolenie, propagandę, szerzenie nienawiści, rekrutację, gromadzenie funduszy i wiele, wiele innych. Oczywiście nie jest to pełna lista, ale wynikające z tych działań zagrożenia można usystematyzować w trzech kategoriach:

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

Pierwszą z form aktu cyberterrorystycznego - atak na system - można scharakteryzować jako działanie stawiające sobie za obiekt system operacyjny komputera i/lub jego oprogramowanie w celu przejęcia kontroli nad jego funkcjami lub uczynienia go nieużytecznym. Zdecydowana większość działań hakerskich w internecie ma taki właśnie charakter. Są to na przykład robaki internetowe, wirusy czy popularne ostatnio ataki (D)DoS ((Distributed) Denial of Service)[15]. W parze z prostotą dzia-

[14] Projekt dostępny jest pod adresem http://conventions.coe.int/Treaty/en/treaties/html/185.htm.

[15] O ile pierwsze trzy zjawiska wymagają wysokich kwalifikacji i specjalistycznej wiedzy do swojego powstania, to ostatni rodzaj ataków (D)DoS jest na tyle prosty, że przeprowadzić go może praktycznie każdy średnio zaawansowany użytkownik komputera przy użyciu dostępnego w internecie gotowego oprogramowania z dołączonymi podręcznikami obsługi. Mówiąc o prostocie działań, mamy oczywiście na myśli algorytm działania, nie warstwę informatyczną wytworzonych kodów. W warstwie logicznej atak (D)DoS to nic innego jak „bombardowanie" połączeniami upatrzonego celu tak, iż niemożliwe jest zrealizowanie jakiegokolwiek połączenia z nim przez uprawnionych użytkowników. Odpowiednikiem podobnego zachowania ze „świata fizycznego" jest ciągłe dzwonienie przez grupę osób pod wybrany

łania idzie ich ogromna skuteczność i niszczycielska siła. Ataki (D)DoS generujące gigantyczny ruch internetowy ukierunkowany na konkretny serwer powodują, iż jest on praktycznie niedostępny dla innych uprawnionych użytkowników[16].

Grupa ta obejmuje też bardziej niebezpieczne zamachy, w których dąży się do przejęcia całkowitej kontroli nad zaatakowanym komputerem. Zastosowanie znajdują tu Konie Trojańskie i Back Door (z ang. Tylne Drzwi). Pierwsze z nich to specjalne programy rozpowszechniane po internecie najczęściej w postaci atrakcyjnych darmowych załączników do poczty elektronicznej, drugie przeważnie umieszczane są skrycie w kodzie programów już na etapie pisania oprogramowania, bądź tworzone i pozostawiane przez administratorów systemów w użytkowanych przez nich maszynach. W tak zainfekowanych komputerach istnieje możliwość umieszczenia snifferów lub podobnie działających programów służących do przechwytywania loginów i haseł użytkowników. Przeprowadzanie ataku tego typu, zwłaszcza na systemy, które odgrywają istotną rolę w funkcjonowaniu jakiegoś podmiotu, wymaga na ogół wysokich kwalifikacji i czasu[17]. Zdarza się, że aby przeprowadzić tego typu atak, sprawca musi dysponować specjalistyczną wiedzą z zakresu funkcjonowania konkretnego systemu. Tak było w przypadku włamania do systemu informatycznego zarządzającego funkcjami oczyszczalni ścieków w Maroochy Shire w Australii, gdzie były pracownik wypuścił do sieci miejskiej i oceanu miliony litrów nieprzerobionych ścieków. Włamywacz miał głęboką wiedzę o funkcjonowaniu systemu oraz posiadał na swoim laptopie wykradzione oprogramowanie sterujące tą oczyszczalnią. Jak ujawniono w trakcie śledztwa, nie był on w stanie dokonać swojego włamania od razu. Udało mu się to dopiero za 46 razem, ale - co szczególnie niepokojące - administrator nie zauważył pierwszych 45 prób (Berinato 2002b).

Obiektem zamachu w drugiej z wyodrębnionych kategorii są dane przechowywane i przetwarzane w systemie komputerowym. Ze względu na to, co jest prawdziwym celem stojącym za uzyskaniem nielegalnego dostępu do informacji, możemy mówić o dwóch podkategoriach. W pierwszym przypadku dobrem, przeciw któremu kieruje

---

numer, co całkowicie paraliżuje jego funkcjonowanie. W przypadku internetu liczba „dzwoniących" komputerów idzie w tysiące i znaczna część z nich jest na ogół wykorzystana wbrew woli użytkowników - mamy wtedy do czynienia z tak zwanymi „zombie".

[16] Dotychczas najpoważniejszy przypadek takiego ataku nie był aktem terrorystycznym i miał miejsce w lutym 2000 r., kiedy również nasze media informowały o ataku na serwery Yahoo!, Amazon.com i CNN, które zostały przeciążone i wyłączone na kilkanaście godzin. Przywrócenie ich pełnej funkcjonalności trwało kilka dni. Spowodowane tym atakiem szkody szacowane były na 1,2 mid dolarów amerykańskich.

Za pierwszy atak cyberterrorystyczny metodą (D)DoS uznawana jest blokada serwerów kilku ambasad Sri Lanki, dokonana przez separatystów tamilskich, którzy zarzucili serwery pocztowe tysiącami elektronicznych listów. Atak składał się z około 800 listów dziennie i trwał przez około 2 tygodnie. Treść tych listów była następująca: „Jesteśmy Czarnymi Tygrysami Internetu i robimy to, aby zakłócić waszą komunikację"; zob. Milone 2002.

[17] Szeroko komentowanym włamaniem o podobnym *modus operandi* była sprawa Solar Sunrise, gdzie trzech młodych hakerów (dwóch szesnastolatków ze Stanów Zjednoczonych i jeden osiemnastolatek z Izraela *alias* Analyzer) włamało się do systemów wojskowych w Kalifornii, wykorzystując powszechnie znaną lukę w systemie bezpieczeństwa systemów Sun Solaris, i przejęło kontrolę na poziomie administratora *(root)* nad całym systemem operacyjnym. Statement for the Record of Ronald L. Dick, Director National Infrastructure Protection Center Federal Bureau of Investigation on the Issue of Intrusions into Government Computer Networks Before the House Energy and Commerce Committee, Oversight and Investigation Subcommittee, Washington DC, 5 kwietnia 2001.

swe działania przestępca, jest wiarygodność systemu oraz zaufanie doń użytkowników, w drugim chodzi o kradzież informacji.

Wprowadzenie do systemu komputerowego nowej informacji lub modyfikacja istniejącej, co objawi się w dysfunkcjach kontrolowanego przez ten system urządzenia lub procesu, zaliczymy naturalnie do pierwszej podkategorii. Warunkiem powodzenia takiego przedsięwzięcia jest dokonanie zmian w sposób niezauważalny dla operatora systemu. Prawdziwe straty mają dopiero przynieść decyzje i działania podjęte przy wykorzystaniu nowych, spreparowanych danych. Atakowany system musi być postrzegany jako działający poprawnie.

Ataki tego typu bazują na założeniu, że użytkownicy systemów komputerowych ufają informacjom, które czerpią z określonych, pewnych źródeł istniejących w internecie. Strony WWW oferujące wybór aktów prawnych Sejmu RP, notowania spółek giełdowych czy analizy i raporty umieszczane na serwerach Ministerstwa Finansów to źródło wiedzy dla przedsiębiorców i zwykłych obywateli[18]. Komputery te są potencjalnym celem zamachowców planujących wywołanie choćby częściowej dezorganizacji funkcjonowania danego społeczeństwa. Ataki wymierzone w tego typu serwisy informacyjne, choć nie o charakterze aktów terrorystycznych, lecz działań typowo przestępczych, miały już wielokrotnie miejsce w przeszłości i dotyczyły przede wszystkim manipulacji kursami akcji spółek giełdowych.

Idąc dalej, w omawianej podkategorii umieścimy też działania wymierzone bezpośrednio w infrastrukturę, która wykorzystuje w swym funkcjonowaniu informacje i polecenia otrzymywane z zewnątrz. Chodzi tu przede wszystkim o systemy informatyczne odpowiedzialne za kierowanie ruchem pociągów, dystrybucję energii elektrycznej czy rozmieszczanie bagaży na pokładach samolotów i statków. Udane włamanie i wpływ na przetwarzanie danych w tych systemach są w stanie spowodować zniszczenia materialne i ofiary śmiertelne w ludziach. Jest mało prawdopodobne, że błąd oprogramowania czy wirus komputerowy sprawi, iż samoloty zaczną spadać z nieba, jak miało to miejsce w bardziej śmiałych wizjach konsekwencji Y2K (z ang. problemu roku 2000). Jednakże sparaliżowanie systemów informatycznych zarządzających ruchem pasażerów na lotniskach w połączeniu z deklaracją dowolnej organizacji terrorystycznej, iż jest to ich zamierzone i kontrolowane działanie, może doprowadzić do groźnego w konsekwencjach wybuchu paniki. Wszczęcie procedur bezpieczeństwa i żądanie natychmiastowego ściągnięcia na ziemię wszystkich pozostających w powietrzu samolotów może w niektórych przypadkach wiązać się z podejmowaniem niepotrzebnego ryzyka. Podobnie wroga ingerencja w oprogramowanie systemu rozplanowania ładunku na pokładzie samolotu i w konsekwencji niewłaściwe rozmieszczenie ciężaru może mieć potencjalnie katastrofalne skutki.

Naturalnie systemy podatne na takie zdalne ataki występują przeważnie w państwach wysoko uprzemysłowionych i mocno zinformatyzowanych. W praktyce najbardziej narażone na tego typu akty terrorystyczne wydają się kraje Europy Zachodniej, dynamicznie rozwijające się pod względem technologicznym społeczeństwa Azji, ale przede wszystkim, głównie z uwagi na uwarunkowania polityczne, zagrożone są Stany Zjednoczone. W latach 70. XX w., kiedy w USA dokonywała się rewolucja informatyczna, zagrożenie cyberterroryzmem nie było na ogół brane pod uwagę.

[18] http://www.sejm.gov.pl, http://www.gpw.com.pl, http://www.mf.gov.pl.

Menadżerowie skuszeni wizją redukcji kosztów powszechnie wdrażali w przedsiębiorstwach systemy SCADA (Supervisory Control and Data Acquisition) umożliwiające zdalne zarządzanie funkcjami oddalonego elementu infrastruktury. W przypadku sieci energetycznych SCADA służy m.in. do zdalnej kontroli transformatorów, tak aby żadna elektrownia nie została przeładowana. Poza sieciami energetycznymi systemy te wdrożone zostały w wielu innych gałęziach gospodarki, takich jak sieci wodociągowe, tamy, telekomunikacja. Jedną z niewielu gałęzi gospodarki, która oparła się pokusie wprowadzenia systemów SCADA w swoich placówkach, była energetyka jądrowa. The Nuclear Regulatory Commission (NRC) odpowiedzialna za politykę nuklearną państwa, mając na uwadze bezpieczeństwo zabroniła tego typu rozwiązań[19].

Druga z podkategorii to klasyczna kradzież danych komputerowych z systemu. W przypadku działań o charakterze terrorystycznym chodzi głównie o gromadzenie danych pomocnych przy wyborze celu i przygotowaniach do zamachu. Obiektem ataku mogą być praktycznie wszelkie informacje, nie tylko tak oczywiste jak plany architektoniczne obiektów, grafiki pracy służby ochronnej, ale również prywatne zdjęcia zawierające wizerunki osób, przypadkowo skadrowane budynki i ich wnętrza czy prywatna korespondencja pracowników mówiąca o ich zwyczajach, rozkładzie dnia itp. Praktycznie nie można przewidzieć, jakie dane wzbudzą zainteresowanie terrorystów[20]. Nawet w przypadku wykrycia odróżnienie tych działań od akcji o charakterze czysto kryminalnym czy szpiegowskim nie wydaje się możliwe.

Trzecia kategoria, wsparcie klasycznych form działalności terrorystycznej, jest najszersza z dotychczas omawianych. Wsparcie technologiczne ma przede wszystkim charakter logistyczny i organizacyjny. Internet stwarza fantastyczne możliwości komunikacji zwłaszcza tym, którzy chcą czynić to, pozostając niezauważonymi przez organy ścigania i tak anonimowymi jak to tylko możliwe[21]. Komputery oferują ponadto zaawansowane techniki ukrywania przekazywanej treści, takie jak kryptografia i steganografia, nie wymagając przy tym od użytkownika profesjonalnego przygotowania.

Internet to również efektywne narzędzie propagandy. Rozpowszechnianie za pośrednictwem stron WWW, list dyskusyjnych czy poczty elektronicznej poglądów, celów oraz „osiągnięć" poszczególnych ugrupowań uznawanych za organizacje terrory-

[19] Nie znaczy to oczywiście, iż elektrownie atomowe są bezpieczne wobec ataków polegających na manipulacji otrzymywanymi przez ich systemy danymi. W literaturze można znaleźć ciekawy przykład możliwości, jakie daje odpowiednie wykorzystanie tradycyjnych ładunków wybuchowych do symulacji wstrząsów tektonicznych i spowodowania automatycznego wyłączenia elektrowni atomowej. Instalacje przemysłowe tego typu wyposażone są bowiem w czujniki sejsmiczne, które w przypadku wykrycia wstrząsów alarmują system komputerowy zarządzający pracą obiektu, a ten w celu zabezpieczenia reaktora przez wyciekiem rozpoczyna procedurę wyłączenia reaktorów atomowych, http://www.nrc.gov/; zob. też Berinato.

[20] Oddziały amerykańskie zabezpieczyły w trakcie operacji w Afganistanie laptopy należące do członków organizacji Al-Ka'ida, na których znajdowały się strukturalne i funkcjonalne plany zapór wodnych oraz informacje dotyczące komputerowego systemu zarządzania systemami wodnymi, elektrowni atomowych oraz stadionów sportowych znajdujących się na terenie Stanów Zjednoczonych i Europy; zob. Council of Europe 2003, s. 132.

[21] Służby prowadzące dochodzenia w sprawie wydarzeń z 11 września dowiodły, że część z porywaczy w tygodniach poprzedzających atak koordynowała swoje działania przy wykorzystaniu zapewniających znaczną anonimowość kawiarni internetowych oraz czynnych całą dobę sklepów Kinko na Florydzie; zob. Johnson 2001.

styczne jest już normalnym przejawem działalności tych formacji[22]. Namawianie do nienawiści, szerzenie agresji czy wzniecanie niepokojów społecznych to domena nie tylko fanatyków religijnych, lecz także wypaczonych organizacji anarchistycznych i nacjonalistycznych. W skrajnych formach zachowania takie mogą być traktowane jako przejawy wojny informacyjnej, ale z przesłanek politycznych większy komfort i swobodę działania daje atakowanym państwom uznanie tych praktyk po prostu za przejawy terroryzmu. Po stronie krajów, które tak czynią, stoi ważny argument, iż prowadzona elektronicznie działalność informacyjno-propagandowa może mieć za cel rekrutację nowych kadr, także rekrutację *on-line*. Że nie są to obawy bezpodstawne świadczy choćby przypadek z 1995 r. kiedy to tą drogą został zwerbowany Zijjad Chalil, informatyk Columbia College z Missouri. Będąc aktywistą muzułmańskim i działając prężnie w campusie, nawiązał on liczne kontakty internetowe z organizacjami muzułmańskimi na świecie, również z tymi o zdecydowanie radykalnych poglądach. Swoją postawą zwrócił uwagę organizacji Osamy bin Ladena i wkrótce stał się jednym z jego zaufanych współpracowników. Chalil organizował na terenie Stanów Zjednoczonych zakupy telefonów satelitarnych, komputerów i urządzeń elektroniki wywiadowczej (Weimann 2004).

W trakcie wojny w Iraku terroryści sięgnęli po internet w jeszcze innym celu, użyli go mianowicie bezpośrednio do prowadzenia wojny psychologicznej. Swój główny cel, szerzenie strachu, realizowali, nagłaśniając w internecie groźby egzekucji, a następnie rozpowszechniając filmy z ich przebiegu. Działanie takie wydaje się mieć bardzo silny wpływ na odbiorcę, głównie ze względu na to, iż ofiara przestaje być anonimową liczbą w medialnym komunikacie. Terroryści, stawiając odroczone w czasie ultimatum wycofania wojsk, dają zachodnim mediom szansę, aby te „zaprzyjaźniły" odbiorców z przetrzymywanym zakładnikiem. Egzekucja takiej osoby postrzegana jest jako śmierć kogoś znajomego, kogoś z własnego otoczenia. Tego typu zabieg ze strony zamachowców przybliża psychologicznie poczucie zagrożenia z „odległego zamorskiego kraju" tuż na próg domu odbiorców informacji prasowych. Mamy tu więc do czynienia z nowym zjawiskiem, jakim jest częściowa rezygnacja ze skomplikowanych i drogich operacji przeciwko dużym grupom ludności i zindywidualizowanie zagrożenia. Wydaje się, że jest to ewolucja działań terrorystycznych w odpowiedzi na pewną społeczną znieczulicę powstałą przez nadmierne medialne eksponowanie samych liczb zabitych i rannych w kolejnych zamachach terrorystycznych.

Jeśli chodzi o propagandę i wojnę psychologiczną, nasuwają się pewne spostrzeżenia co do podmiotów, na które działalność ta jest ukierunkowana. Wydaje się, iż w ślad za Gabrielem Weimannem można tu wskazać trzy zasadnicze grupy adresatów: obecni i przyszli poplecznicy, międzynarodowa opinia publiczna oraz opinia publiczna wrogiej strony (Weimann 2004).

- Pierwszej grupy dotyczy poruszona już kwestia agitacji i rekrutacji nowych członków, ale również działalność związana ze zbieraniem funduszy na funkcjonowanie organizacji (zagadnienie to zostanie omówione szerzej nieco dalej).
- Grupa druga i wpływanie na światową opinię publiczną wiąże się z zabiegami, jakie podejmują radykalne organizacje w celu pozyskania sobie jej przychylności przez prezentację celów i motywów podjęcia określonych działań. Strony zawierają-

[22] http://www.jihadunspun.net, http://electronicintifada.net, http://www.hizbollah.org.

ce te informacje prezentują skrajnie subiektywny punkt widzenia z obszernym tłem historycznym usprawiedliwiającym podjętą walkę. Witryny internetowe tej grupy, w przeciwieństwie do poprzedniej, są wykonane w wielu wersjach językowych. Część organizacji kładzie szczególny nacisk na kontakty z dziennikarzami, którym poświęca specjalną uwagę, proponując, jak na przykład Hezbollah, stały kontakt przez e-mail.

- Grupa trzecia wymierzona w opinię publiczną atakowanego społeczeństwa obejmuje działania mające na celu z jednej strony jego zastraszenie i demoralizację, z drugiej zaś rozbudzenie społecznego poczucia winny i wywołanie dyskusji publicznej co do racji w konflikcie, a docelowo - osłabienie poparcia publicznego dla rządzącego reżimu.

Uzupełniając podział G. Weimanna, trzeba zaznaczyć, iż podejmowane działania propagandowe czy same zapowiedzi zamachu mogą niekiedy wyjść poza zaproponowaną powyżej klasyfikację. Bywają one bowiem ukierunkowane na dezinformację i służą jedynie odwróceniu uwagi organów bezpieczeństwa od faktycznie obranego celu zamachu. Te ostatnie stanowiłyby więc niejako czwartą grupę w przyjętym tu podziale adresatów.

Wracając do form wsparcia działalności terrorystycznej przez narzędzia internetowe, zatrzymamy się przez chwilę przy scenariuszu, w którym fizyczny akt terrorystyczny będzie sprzężony z następującą po nim kampanią dezinformacyjno-propagandową. Kluczem do sukcesu jest tutaj nadanie spreparowanym informacjom pozorów autentyczności. Platformą wyprowadzenia takiego ataku mogą zostać witryny internetowe wiarygodnych dla odbiorców stacji takich jak CNN, BBC czy Reuters[23]. Ewentualna manipulacja zawartością ich elektronicznych serwisów informacyjnych czy też podszycie się pod nie, z technicznego punktu widzenia nie są technologicznym wyzwaniem. Natomiast potencjalne społeczne i polityczne konsekwencje takiej skoordynowanej maskarady są ogromne. Dodatkowe niebezpieczeństwo stanowi również fakt, że duże agencje informacyjne są pierwotnym źródłem informacji dla wielu mniejszych lokalnych dzienników i stacji radiowych. Można na przykład wyobrazić sobie sytuację, gdzie po atakach na wieże WTC z 11 września 2001 r. przeprowadzono by starannie zaplanowaną i zakrojoną na szeroką skalę ofensywę informacyjną zmierzającą do przeniesienia choćby częściowej odpowiedzialności za ten zamach na izraelski Mosad[24]. Gdyby operacja zakończyła się powodzeniem, nawet późniejsze wielokrotne dementowanie przez media wcześniejszych doniesień nie byłoby już w stanie całkowicie unicestwić żyjącego własnym życiem „faktu prasowego". Przypuszczalną konsekwencją tego procesu byłby wzrost nastrojów antysemickich.

W świetle powyższych rozważań można postawić pytanie, czy niedestrukcyjną, propagandową aktywność grup terrorystycznych można na pewno uznać za działalność terrorystyczną ze wszystkimi tego konsekwencjami. Niektórzy autorzy skłaniają się w tym przypadku ku nazwaniu tego zjawiska miękkim terroryzmem (Bóg-

[23] http://www.cnn.com, http://www.reuters.pl/, http://www.reuters.com, http://www.bbc.co.uk.

[24] W rzeczywistości po wydarzeniach z 11 września w różnych grupach dyskusyjnych w internecie pojawiły się głosy, iż w jakimś stopniu za zamachy te współwinę ponosi izraelski Mosad. Wywiad Izraela miał wiedzieć o planowanych działaniach terrorystów, ale celowo, aby doprowadzić do konfrontacji militarnej Stanów Zjednoczonych ze światem arabskim, danych na ten temat nie ujawnił. Świadczyła o tym jakoby rzekoma nieobecność fatalnego dnia osób pochodzenia żydowskiego w wieżowcach WTC. Z internetu plotka ta przeciekła do świata fizycznego i zaczęła żyć własnym życiem.

dał-Brzezińska, Gawrycki 2002, s. 65). Pogląd ten jest jednak krytykowany przez państwa czynnie zaangażowane w zwalczanie światowego terroryzmu. Niezależnie od nomenklatury pozostaje faktem, iż organizacje terrorystyczne są świadome zalet sieci komputerowych i już teraz szeroko wykorzystują internet w swoich działaniach.

Na zakończenie tej części rozważań wysunięto jeszcze jedną, być może najważniejszą kwestię, a mianowicie finansowania terroryzmu przy wsparciu internetu. Chodzi tu zarówno o propagandę i zbieranie składek od sympatyków, jak i organizację oraz realizację przedsięwzięć o charakterze czysto kryminalnym. Do 2001 r. Hamas posiadał w Teksasie organizację charytatywną HLF (Holy Land Foundations for Relief and Development) i za pośrednictwem jej witryny WWW zbierał fundusze transferowane następnie na własne konta. Oprócz zbiórek mamy tu też do czynienia z działalnością kryminalną. Nie jest już chyba dla nikogo tajemnicą, że cyberprzestępczość skierowana przeciwko bankom i instytucjom finansowym przynosi ogromne zyski. Dane FBI za lata 90. XX w. mówiły, że dzięki komputerom rocznie kradziono około 3-7,5 mid dolarów. Jednorazowo amerykańskie banki w wyniku „tradycyjnych" napadów traciły w tym okresie średnio około 8 tys. dolarów amerykańskich, podczas gdy przeciętna kradzież informacji z systemu komputerowego kosztowała bank około 100 tys. dolarów, a oszustwo komputerowe już około 0,5 min dolarów (Jakubski 1996). Dochody ze skradzionych kart kredytowych, włamania na elektroniczne konta bankowe, sfingowane przelewy elektroniczne czy wymuszenia na centralach banków to tylko niektóre przykłady tego, jak terroryści przy użyciu nienowych przecież 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. Bez tych danych natomiast nie jest możliwe ani zwalczanie takich nadużyć, ani precyzyjne szacowanie utraconych sum czy choćby liczby podobnych przypadków na świecie. Istniejący stan rzeczy powoduje, że zdobywane tą drogą środki finansowe zdają się być poza realną kontrolą, co również nie jest bez znaczenia dla starających się pozostać w ukryciu siatek terrorystycznych.

Innym związanym pośrednio z internetem i systemami komputerowymi źródłem finansowania działalności ekstremistycznej jest produkcja i dystrybucja podróbek towarów. Płaszczyzna ta jest obecnie najlepiej udokumentowaną sferą przenikania się i współpracy zorganizowanych grup przestępczych oraz organizacji o zabarwieniu terrorystycznym. W orbicie zainteresowania leżą tu takie produkty, jak podróbki ubrań, alkoholu, papierosów, płyt CD i DVD oraz oprogramowania komputerowego. O ciągłym wzroście aktywności na tym polu ostrzegał sekretarz generalny Interpolu Ronald K. Noble (2003). W swoim przemówieniu podał on przykłady podobnej działalności m.in. z terenu Północnej Irlandii, Kosowa, północnej Afryki oraz Czeczenii. W przypadku separatystów czeczeńskich rosyjskie FSB przeprowadziło likwidację fabryki płyt CD, której zysk oszacowano w granicach od 500 tys. do 700 tys. dolarów amerykańskich miesięcznie. Aby przybliżyć te liczby, warto nadmienić, iż według ocen ekspertów całkowity koszt planowania i realizacji zamachu na World Trade Center w Nowym Jorku wyniósł mniej niż 500 tys. dolarów amerykańskich. Zestawienie to jednoznacznie wskazuje, iż nie można pozwolić sobie na traktowanie tego typu aktywności przestępczej po macoszemu.

Szczególnie wrażliwym punktem funkcjonowania rozwiniętych społeczeństw jest sprawność infrastruktury telekomunikacyjnej. Nowoczesne systemy telekomunikacyjne to przede wszystkim skomputeryzowane centra przetwarzające dane, które już ze swojej natury są szczególnie narażone i wrażliwe na ataki cyberterrorystyczne. Dotyczy to zarówno systemów telefonii stacjonarnej, komórkowej, jak i satelitarnej[25]. Po części winę za taki stan rzeczy ponoszą firmy produkujące i wdrażające oprogramowanie i sprzęt telekomunikacyjny, które nierzadko prowadzą politykę „przez tajność do bezpieczeństwa". Słabe strony systemu nie są niezwłocznie eliminowane, ale „ukrywane" w utajnionej dokumentacji specjalistycznej i artykułach fachowych, gdzie opisana jest dokładnie specyfika tych słabości. Jak łatwo się domyślić, wiedza ta szybko trafia w ręce osób niepowołanych[26]. Konsekwencje ewentualnego wyłączenia systemów telekomunikacyjnych na określonym obszarze - poza oczywistą uciążliwością dla społeczeństwa - byłyby dotkliwe zwłaszcza w kontekście funkcjonowania służb ratunkowych.

Szczególną groźbę stanowi atak zmierzający do wyłączenia internetu jako całości. Realizacji tego może służyć zablokowanie podstawowych serwerów DNS tłumaczących adresy IP[27]. Niezależnie od tego, czy byłby to atak przeprowadzony w sposób klasyczny z użyciem materiałów wybuchowych, czy też elektronicznie, jego efekty byłyby wszechogarniające. Faktycznych skutków wyłączenia internetu nie sposób co prawda przewidzieć, ale niestety nawet optymistyczne prognozy mówią o chaosie. Niewątpliwie brak komunikacji upośledziłby całe sektory gospodarki, utrudnił bądź uniemożliwił wymianę informacji, zawieranie niektórych kontraktów oraz realizację transakcji handlowych. Przyniosłoby to również stratę dla świata nauki korzystającego powszechnie z możliwości swobodnej wymiany poglądów oraz dostępu do baz danych, jakie oferują złącza teleinformatyczne. Oczywiście nawet w rozwiniętych państwach istnieją grupy ludzi, którzy konsekwencji takiego stanu rzeczy by nie odczuli lub co najwyżej uważali je za drobną niedogodność. Bo choć czarne scenariusze i negatywy można mnożyć, to wydaje się, że dzisiejszy świat, tak mocno uzależniony od techniki, byłby jednak w stanie funkcjonować bez globalnej sieci. Prawdopodobnie po okresie początkowego zamieszania funkcjonalność najważniejszych dla społeczeństwa służb i systemów, takich jak straż pożarna, policja, szpitale itp., udałoby się przywrócić i zarządzać nimi przy wykorzystaniu dostępnych zasobów.

Kolejnym potencjalnym celem ataków terrorystycznych są systemy przetwarzania i zaopatrzenia w wodę. Jednak z uwagi na powszechną świadomość zagrożenia tych obiektów wydają się one być całkiem dobrze zabezpieczone przed atakiem z sieci

[25] W 1999 r. doszło prawdopodobnie do włamania i częściowego przejęcia kontroli nad brytyjskim satelitą wojskowym. Służby brytyjskie nigdy jednak nie zdecydowały się wypowiedzieć na ten temat.

[26] Na co dzień z faktu słabego zabezpieczenia central telefonicznych korzystają tzw. pajęczarze. Są to osoby, które włamują się do systemów kompanii telekomunikacyjnych przy użyciu najwymyślniejszych technik i korzystają z usług tychże za darmo. Znany jest nawet przypadek, gdzie jeden z pajęczarzy, John Draper, otrzymał pseudonim Kapitan Chrupka (z ang. *Captain Crunch)* po tym jak odkrył, iż zwykła torebka po chrupkach może generować dźwięk o częstotliwości 2,4 kHz, otwierający dostęp do linii międzymiastowej. Niestety tak jak możliwe jest darmowe korzystanie z usług, tak możliwie jest uzyskanie wpływu na powyższy system w stopniu umożliwiającym jego wyłączenie; zob. Parker 1994.

[27] W październiku 2002 r. doszło do tego typu zamachu, kiedy zaatakowanych zostało metodą (D)DoS 13 podstawowych serwerów DNS. W kulminacyjnym punkcie ataku przez 6 godzin działały jedynie 4 serwery DNS, http://www.fbi.gov.

komputerowej. Wykorzystywane systemy SCADA są bardzo mocno zindywidualizowane przez eksploatujące je lokalnie podmioty. Z tego względu włamanie do takiego systemu wymagałoby dysponowania niedostępną powszechnie specjalistyczną wiedzą na temat funkcjonowania tego konkretnego urządzenia. Stacje uzdatniania wody, gdzie zdalnie zarządza się dozowaniem chemikaliów, są wyposażone w niezależne systemy kontroli i powiadamiania o stężeniu związków chemicznych kluczowych dla jakości i bezpieczeństwa wody. Serwery komputerowe odpowiedzialne za gromadzenie tych danych posiadają profesjonalnie przygotowane oprogramowanie i umieszczone są w fizycznie odciętych strefach dostępu z pełnym całodobowym monitoringiem. Nawet jeżeli w jakiś sposób napastnikowi udałoby się pokonać wszystkie te przeszkody i spowodować nasycenie wody pitnej ilością chloru stanowiącą zagrożenie dla zdrowia ludzi, to i tak woda przesyłana przez system transportowy poddawana jest wielokrotnej kontroli chemicznej jej składu, a każda nieprawidłowość jest zgłaszana alarmem za pośrednictwem wydzielonych łączy lub mikrofal (Berinato 2002a).

Pewne zagrożenie istnieje też w przypadku niektórych zapór wodnych wyposażonych w zdalne systemy sterowania przepływem wody połączone z centralą za pomocą publicznych łączy. Rozwiązanie takie niesie ze sobą niewielkie, ale realne prawdopodobieństwo nielegalnej ingerencji w system i przejęcia kontroli nad niektórymi jego funkcjami. W najgorszym przypadku włamanie takie może jedynie doprowadzić do kontrolowanego otwarcia śluz i stopniowego spuszczenia zasobów wody ze zbiornika, co jednak nie stanowi bezpośredniego zagrożenia dla zdrowia i życia ludzi. Naturalnie, tak jak w każdym najlepiej nawet zabezpieczonym technicznie obiekcie, krytyczną składową stanowi czynnik ludzki. Odpowiedni system rekrutacji i bieżącej kontroli personelu jest niezbędnym elementem również tego systemu bezpieczeństwa.

Poza spektakularnymi akcjami cyberterrorystom pozostaje jeszcze inny rodzaj skrytego oddziaływania na zinformatyzowane gospodarki i społeczeństwa Zachodu. Niektórzy autorzy przestrzegają przed groźbą zaatakowania przez programy pasożytnicze newralgicznych zbiorów informacji przechowywanych w systemach takich jak bazy danych meldunkowych, ubezpieczenia społecznego, rejestry pojazdów, rejestry medyczne itp.[28] Te działające niemal niezauważalnie i przez lata programy powodują degenerację i przekłamania w gromadzonych danych. Pomijając już ogromne koszta społeczne i finansowe odbudowania czy weryfikacji takich baz, realizacja bieżących zadań na podstawie zafałszowanych przesłanek wprowadziłaby

[28] W styczniu 1999 r. miały miejsce wydarzenia, które jednoznacznie wskazują, iż bazy danych nie są wystarczająco zabezpieczone przed włamaniami. System komputerowy amerykańskiej Narodowej Biblioteki Medycznej (National Library of Medicine -NLM), służący tysiącom lekarzy i specjalistów branży medycznej jako źródło najnowszych informacji o chorobach, sposobach leczenia, lekach i ich dawkach, został spenetrowany przez włamywacza. Haker pobrał z serwerów systemu setki plików wspomnianych danych medycznych. Ponieważ zachodziło ryzyko, iż część z przechowywanych informacji mogła zostać przypadkowo lub celowo zmieniona w trakcie włamania, atak ten został potraktowany przez FBI jako zagrożenie dla bezpieczeństwa publicznego. Dochodzenie FBI zidentyfikowało włamywacza jako byłego programistę komputerowego NLM, który do włamania wykorzystał „tylne drzwi" stworzone przez siebie jeszcze w trakcie pracy nad kodem bazy danych. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington DC, 28 marca 2000 r.

znaczny, narastający w czasie chaos w funkcjonowaniu administracji publicznej (Berinato 2002b).

Na zakończenie tych rozważań trzeba wspomnieć jeszcze o swoistej konwergencji, jaka ma miejsce pomiędzy klasycznymi formami zamachu a atakiem elektronicznym. W chwili obecnej w rękach terrorystów mogą już znajdować się urządzenia, stworzone z myślą o ataku skierowanym *stricte* na systemy komputerowego przetwarzania danych i zawarte w nich informacje. Jest to tak zwana broń elektromagnetyczna: bomby i pistolety generujące promieniowanie radiowe, elektromagnetyczne lub mikrofalowe. Instrumenty te tworzą silne pole bądź wiązkę promieniowania zdolne z odległości uszkodzić układy półprzewodnikowe, magnetyczne nośniki danych i inne czułe elementy tych urządzeń i w konsekwencji trwale zniszczyć same urządzenie oraz zapisane na nich informacje. Prace nad tego typu układami prowadzone były w wielu krajach świata, przypuszcza się jednak, że najprawdopodobniej wiedza niezbędna do ich konstrukcji mogła „wyciec" z któregoś z krajów byłego Związku Radzieckiego.

Podsumowując niniejsze opracowanie, trzeba niestety stwierdzić, że ogólny stan zabezpieczenia systemów informatycznych, zwłaszcza tych odpowiedzialnych za funkcjonowanie istotnej infrastruktury, pozostawia jeszcze wiele do życzenia. Oczywiście przedstawiony tutaj obraz nie jest pełny, bo wykorzystane do ilustracji problemów przykłady dotyczą głównie Stanów Zjednoczonych, ale wydaje się, iż z uwagi na technologiczne zaawansowanie tego państwa i powszechność stosowania pewnych rozwiązań jest to obraz miarodajny. Istniejący stan rzeczy jest w decydującej mierze pochodną faktu, iż znaczna część systemów elektronicznych i informatycznych stanowiących obecnie potencjalny cel była projektowana i budowana w innych czasach, kiedy jeszcze idea światowej pajęczyny spinającej ze sobą wszystkie komputery kiełkowała jedynie w pracowniach kilku wiodących uczelni technicznych na świecie. Te niezależnie projektowane i wdrażane rozwiązania nie byłyby więc siłą rzeczy przygotowane do współdziałania i ochrony swoich zasobów w ramach szerszych struktur, w jakich przyszło im pracować. W tym kontekście nasze zapóźnienie technologiczne stawia nas paradoksalnie w korzystniejszej sytuacji, niż znajdują się inne wyżej rozwinięte społeczeństwa zachodnie. Przede wszystkim Polska dysponuje obecnie ogromnym potencjałem informatycznym i dopiero tworzy nowoczesne zintegrowane systemy teleinformatyczne, w związku z czym nie musimy się borykać z problemami modernizacji działających podmiotów. Dodatkową korzyść możemy wynieść z faktu, iż część kosztów budowy tych systemów możemy pokryć z funduszy europejskich. Co więcej, każdy zakończony sukcesem projekt badawczy z tego zakresu opłaci się nam w dwójnasób. Po pierwsze, przez poprawę ogólnego poziomu bezpieczeństwa, po drugie, otrzymamy gotowy komercyjny produkt generujący wymierne zyski. Zarówno przygotowane, jak i planowane do finansowania tylko przez samą Komisję Europejską projekty badawcze i wdrożeniowe jasno wskazują, iż finansowe wsparcie dla projektów z zakresu bezpieczeństwa publicznego to w najbliższych latach tendencja trwała. Aby jednak nie zmarnować tego szczególnego zbiegu okoliczności, musimy już teraz uświadomić sobie skalę wyzwania i podjąć planowe, konsekwentne działania zmierzające do zabezpieczenia państwa i obywateli przed skoordynowanym i skomasowanym atakiem cyberterrorystycznym.

LITERATURA

Alexander Y. (1998). *Cyber Terrorism and Information Warfare: Threats and Responses,* 16 kwietnia, Proceedings report of seminar held at Potomac Institute for Policy Studies, Arlington, Virginia.

Alexander Y. (1999/2000). „Terrorism in the twenty-first century: Threats and responses", Symposium Terrorism and Business DePaul University 2000, *DePaul Business Law Journal,* jesień/wiosna.

Arquilla J., Ronfeldt D., Zanini M. (1999). *Networks, Netwar and Information-Age Terrorism in Countering the New Terrorism,* http://www.rand.org/ publications/ MR/MR989/MR989.chap3 .pdf.

Ashle D. (1999). „Crisis in Yugoslavia; Battle spilling over onto the Internet", *Los Angeles Times,* 3 kwietnia.

Barkham J. (2001). „Information warfare and international law on the use of force", *New York University Journal of International Law and Politics,* jesień.

Becker E. (1999). „Pentagon sets up new center for waging cyberwarfare", *New York Times,* 8 października.

Berinato S. (2002a). *Debunking the Threat to Water Utilities,* http://www.cio.com/ archive/031502/ truth_sidebar2.html.

Berinato S. (2002b). *The truth about cyberterrorism,* http://www.cio.com/archive/03 1502/truth.html.

Bodansky Y. (1999). *Bin Laden: The Man Who Declared War on America.* Rocklin CA: Prima Publishing Co.

Bógdał-Brzezińska A., Gawrycki M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa: Oficyna Wydawnicza Aspra-Jr.

Brenner S.W., Goodman M.D. (2002). „In defense of cyberterrorism: An argument for anticipating cyber-attacks", *University of Illinois Journal of Law, Technology and Policy,* wiosna.

Collin B. (1996). *The Future of CyberTerrorism,* Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago.

Denning D.E. (2000). „Cyberterrorism" Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University, 23 maja.

Denning D.E. (2000). *Hacktivism: An Emerging Threat to Diplomacy,* http://www.afsa.org/ fsj/ septOO/ Denning.cfm.

Dobrowolski G. (2002). *Technologie agentowe w zdecentralizowanych systemach informacyjno-decyzyjnych.* Kraków: AGH Uczelniane Wydawnictwo Naukowo-Dydaktyczne.

Ganeles Ch. (2002). „Technological advancements and the evolution of terrorism", *ILSA Journal of International and Comparative Law 2001,* wiosna: International Law Weekend Proceedings.

Gawrycka I. (2001). „Cyberporachunki", *Życie Warszawy* z 18-19 października.

Hoffman B. (1999). *Oblicza terroryzmu.* Warszawa: Bertelsmann Media.

Jakubski K.J. (1996). „Przestępczość komputerowa - zarys problematyki", *Prokuratura i Prawo,* nr 12.

Johnson K. (2001). *Hijackers 'Emails Sifted for Clues Computers messages were sent uncoded,* USA Today, http://www.usatoday.com/usatonline/20011001/3496196s.htm.

Kelly J. (2001). *Terror groups hide behind Web encryption, USA Today,* 5 lutego; także: Statement for the Record of Ronald L. Dick, Director National Infrastructure Protection Center Federal Bureau of Investigation on the Issue of Intrusions into Government Computer Networks Before the House Energy and Commerce Committee, Oversight and Investigation Subcommittee Washington DC, 5 kwietnia.

Krasavin S. (2000). *What is Cyber-terrorism,* http://www.giac.org/practical/Serge_Krasavin_GSEC.doc, 27 lipca.

Laris M. (1999). „Chinese Web Warriors; Hackers in Taiwan, China, Trade Shots In Internet Skirmish", *The Washington Post* z 11 września.

Lawson S.M. (2002). *Information Warfare: An analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure,* SANS Institute.

Milone M.G. (2002). „Hacktivism: Securing the national infrastructure", *Business Lawyer,* listopad.

Noble R.K. (2003). „The links between intellectual property crime and terrorist financing", *Before the United States House of Representatives Committee on International Relations,* 16 lipca.

Organised Crime Situation Report 2004, Focus on the threat of cybercrime. Strasburg, Council of Europe, 23 grudnia 2003 r.

Parker D.B. (1994). „Sieciowi piraci", *Świat Nauki,* maj.

Shahtman N. (2001). *Israel Blocks Palestinian ISP,* http://www.wired.com/ news/ politics/ 0,1283,53873,00.html, 16 lipca.

Sieber U. (1998). *Legal Aspects of Computer Related Crime in the Information Society,* COMCRIME-Study, prepared for the European Commission, 1 stycznia.

Ścibek E. (2005). „Prawne i organizacyjne aspekty typowania obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa" w: E. W. Pływaczewski (red.), *Przestępczość zorganizowana, świadek koronny, terroryzm w ujęciu praktycznym,* Kraków: Kantor Wydawniczy Zakamycze.

US Foreign Policy Agenda (2001). „Terrorism. Threat Assessment, Countermeasures and Policy", *An Electronic Journal of the US. Department of State,* t. VI, nr 3, listopad.

Weimann G. (2004). *www.terror.net - How Modern Terrorism Uses the Internet,* http://www.usip.org/ pubs/ specialreports/ srll6.html.