Cyberterroryzm – rzeczywistość czy fikcja?

Aneta Janowska

1. Fikcja?

Wyobraźmy sobie przez chwilę następujący scenariusz:

„7 stycznia – deklaracja wypowiedzenia wojny pojawia się na „zhakowanych" witrynach CNN.com, WhiteHouse.gov, Microsoft.com, Amazon.com i kilkunastu innych. Pod oświadczeniem podpisuje się nie znane dotąd nikomu ugrupowanie terrorystyczne. Trop włamywaczy urywa się w indonezyjskim anonimizerze.

8 stycznia – wybucha plaga wirusów komputerowych i robaków. Większość z nich ma działanie destrukcyjne. Amerykanie uszczelniają ochronę wojskowych i rządowych systemów łączności (*Defense Data Network*, *Intelink*, *GovNet*) oraz uruchamiają awaryjne kanały przepływu tajnych informacji. Militarnych sieci nikt jednak nie atakuje.

9 stycznia – w Chicago i Bostonie nikt nie gasi pożarów, chorzy daremnie czekają na przyjazd karetek, a przestępczość gwałtownie rośnie, gdyż serwery służb ratowniczych i policji są stale bombardowane fałszywymi zgłoszeniami. W Nowym Orleanie dochodzi do wielu wypadków drogowych, po tym, jak na skrzyżowaniach ulic w całym mieście wszystkie światła zmieniły się na zielone. Kontrolę nad sygnalizacją świetlną udaje się przywrócić po kilkunastu godzinach.

11 stycznia – główna fala ataku ukierunkowana jest przeciwko systemom zarządzającym elektrowniami, stacjami wodociągów, bankami oraz przeciw centralom telefonii stacjonarnej i komórkowej. Szacunki mówią, że 40% Amerykanów pozbawionych jest energii lub wody. Nie ukazuje się większość gazet, milknie część stacji radiowych i telewizyjnych. Rzecznik AT&T przyznaje, że jego koncern stracił kontrolę nad większością satelitów telekomunikacyjnych.

12 stycznia – działa wojskowa i rządowa łączność, ale ludność cywilna jest właściwie pozbawiona możliwości wymiany informacji. Internet funkcjonuje z dużym trudem, ale i tak jest głównie źródłem szerzących panikę plotek. Sytuacji nie ułatwia fakt, że popularne serwisy sieciowe są stale atakowane, a ich treść preparowana tak, by pogłębić zamieszanie.

16 stycznia – udaje się przywrócić funkcjonowanie części elektrowni, ale dokonywane są nowe włamania na pracujące dotąd bez przeszkód obiekty. FBI ujawnia, że z terrorystami współpracowały niektóre osoby odpowiedzialne za bezpieczeństwo instytucji publicznych.

18 stycznia – druga fala inwazji. Zakłócane jest funkcjonowanie wież kontroli lotu, automatycznych linii kolei i metra, systemów sterujących rurociągami. Ataki przeprowadzane są zdalnie z serwerów rozsianych zarówno po świecie, jak i zlokalizowanych w Stanach Zjednoczonych. Na komputerach wielu uczelni, firm i instytucji publicznych pozostawiono „zegarowe bomby logiczne" – programy dokonujące ataków na zdefiniowane wcześniej serwery. Doradcy namawiają prezydenta do wydania nakazu wyłączenia najważniejszych serwerów internetowych. Prezydent odmawia.

20 stycznia – źródła zbliżone do CIA podają, że terroryści przejęli głęboko zakamuflowane rosyjskie i chińskie siatki szpiegowskie. Rosja i Chiny zdecydowanie zaprzeczają pogłoskom o swym udziale w cyberataku na USA i składają rządowi amerykańskiemu ofertę pomocy w walce z zagrożeniem.

21 stycznia – straty USA szacuje się na setki miliardów dolarów. Chcący zachować anonimowość wysoki urzędnik Departamentu Stanu przyznaje w wywiadzie dla „Washington Post" – „Zostaliśmy pokonani, a nawet nie wiemy, komu mielibyśmy się poddać" (Dębek, 2001).

Powyższa opowieść brzmi jak początek katastroficznej powieści sensacyjnej. Czy rzeczywiście? Czy cyberterroryzm to wciąż jedynie temat dla scenarzystów i powieściopisarzy o bogatej wyobraźni czy też realne zagrożenie, którego powinniśmy być świadomi i na które powinniśmy się solidnie przygotować?

2. Jak to z cyberterroryzmem było...

Cyberprzestrzeń, a wraz z nią nowy typ zagrożenia, czyli cyberprzestępczość, narodziła się w momencie powstania politycznej koncepcji „autostrad informacyjnych", w czasie kampanii prezydenckiej Billa Clintona w 1992 roku. Koncepcja ta zakładała, że wszelkiego typu informacje zawierające tekst, dźwięk i obraz będą mogły być przekazywane na duże odległości szybko i bez przeszkód.

Świat globalnej sieci coraz bardziej się rozrastał i stawał się coraz bardziej podobny do świata rzeczywistego, dlatego też różne zjawiska istniejące „w realu", w tym przestępczość, a także terroryzm, znalazły swoje miejsce w przestrzeni wirtualnej. Informacja stała się towarem, można ją więc było wykraść, sprzedać, zniszczyć, posłużyć się nią w celu uzyskania korzyści materialnych czy też ideologicznych. Dlatego właśnie jej ochrona stała się kwestią strategiczną.

Jednak pierwsze wzmianki na temat niebezpieczeństwa zamachów terrorystycznych przy użyciu systemów komputerowych pojawiły się już w 1979 roku w raporcie rządu szwedzkiego na temat zagrożeń społecznych związanych z komputeryzacją (Adamski, 2002: 113). Zaś samo słowo „cyberterroryzm" zaczęło być używane już w latach 80. w wypowiedziach amerykańskich specjalistów w dziedzinie wywiadu wojskowego (Adamski, 2002: 114).

Od tego czasu o cyberterroryzmie mówiło się coraz częściej. W latach 90. zawisło nad Stanami Zjednoczonymi widmo „elektronicznego Pearl Harbour". W prasie zaczęły pojawiać się nagłówki informujące o atakach cyberterrorystów. W 1995 roku cybernetyczny

świat obiegła makabryczna wieść, że rząd meksykański zbombardował pewne miasto: „korytarze szpitala w Comitan były pełne trupów, a żołnierze gwałcili kobiety i mordowali dzieci (http://tecfa.unige.ch/etu/E7lb/99/deian/terrorisme.htm). Później dopiero okazało się, że te doniesienia były fałszywe.

W lutym 2000 roku serwery Yahoo, Amazon, CNN, eBay, itp. zostały zaatakowane za pomocą DoS (*denial of service*), co spowodowało wyłączenie na jakiś czas tych serwisów. Dopiero wtedy opinia publiczna zdała sobie tak naprawdę sprawę z tego, że cyberprzestępczość jest faktem. John Deutch, dawny szef CIA, stwierdził, że ataki te były testem skuteczności, przeprowadzonym przez członków organizacji Hezbollah (Bouvier, http://www.frstrategy.org/barreFRS/publications/archives/perspec_strat/51/51-3.asp).

Pod koniec października 2002 roku świat obiegła kolejna elektryzująca wiadomość podana przez FBI. Zaatakowanych zostało 13 podstawowych serwerów DNS („tłumaczą" one adresy internetowe na numeryczne adresy IP, wykorzystywane przez komputery; ich całkowite zablokowanie mogłoby spowodować zupełny paraliż Internetu). W rzeczywistości było to 13 jednoczesnych zmasowanych ataków DDoS (*distributed denial of service*). W krytycznym momencie działały tylko 4 serwery, a cały atak trwał 6 godzin.

Wielką globalną sieć ogarniała również raz po raz panika odmiennej natury: oto pojawiał się wirus, który niszczył wszystko, co napotykał na swojej drodze. Takim wirusem okazał się rzeczywiście słynny *I love you*, który spowodował miliardowe straty na całym świecie. Nawet Pentagon przyznał, że ofiarą tego wirusa padły cztery komputery klasyfikowane jako całkowicie bezpieczne, stanowiące część *Defense Data Network* – wydzielonej infrastruktury wojskowej (Dębek, 2001).

Również początek wojny w Iraku spowodował falę ataków cyfrowych: objawiało się to niszczeniem witryn firm amerykańskich oraz atakami na rządowe i wojskowe systemy informatyczne. Nie był to jednak pierwszy polityczny konflikt w cyberprzestrzeni. W kwietniu 1998 roku hakerzy zagrozili aktem sabotażu wobec indonezyjskiego systemu bankowego, jeżeli kraj ten odmówi uznania wyborów we Wschodnim Timorze.

W 2000 roku grupa pakistańskich hakerów zniszczyła około 600 indyjskich stron internetowych oraz przejściowo przejęła kontrolę nad niektórymi indyjskimi sieciami komputerowymi. W lutym 2001 roku chińscy hakerzy dokonali kilkuset cyberataków na największe japońskie firmy w odwecie za zaostrzenie przez Japonię polityki wobec Chin.

Zaś od marca 1999 do kwietnia 2000 roku dokonano 89 cyberataków na 60 agencji rządowych w Malezji. Celem ataków były głównie „wrażliwe" resorty, takie jak opieka społeczna, imigracja, skarb (Pietrzak, 2002).

Innymi nagłośnionymi publicznie działaniami, nazywanymi powszechnie właśnie cyberterroryzmem, były ataki typu DoS na komputery NATO w czasie wojny w Kosowie w 1999 roku. W stanie wojny, ale wojny elektronicznej, znalazły się Stany Zjednoczone i ChRL w maju 2001 roku, kiedy to amerykańscy hakerzy zaatakowali masowo chińskie strony internetowe. W odpowiedzi Chińczycy włamali się na strony amerykańskiej administracji i wielkiego biznesu. Obyło się bez wielkich strat materialnych, ale efekt pozwolił zdać sobie sprawę z tego, jak mogą wyglądać wojny w przyszłości.

Przykłady podobnych działań można oczywiście mnożyć. Jednak większość ekspertów nazywa je nie cyberterroryzmem, a po prostu cyberprzestępczością, a dokładnie hakingiem, hakingiem politycznym, wojną informacyjną, haktywizmem czy po prostu zwykłym wandalizmem. Jaka jest różnica pomiędzy tymi zjawiskami? W jaki sposób można je zdefiniować?

3. Cyberprzestępczość czy cyberterroryzm?

Komputer może odgrywać trzy zasadnicze role w aktywności kryminalnej.

Po pierwsze, może być celem popełnienia przestępstwa (włamanie do sieci – haking, wprowadzenie wirusa komputerowego). Po drugie, może być narzędziem umożliwiającym popełnienie przestępstwa (rozpowszechnianie pornografii, kradzież, hazard). Może także pełnić tylko funkcje incydentalną w trakcie popełniania przestępstwa – np. jako bank danych.

Międzynarodowa Organizacja Policji Kryminalnych „Interpol" dzieli przestępczość komputerową na:

– Naruszanie praw dostępu do zasobów, a w szczególności:
  • haking, czyli nieupoważnione wejście do systemu informatycznego,
  • przechwytywanie danych,
  • kradzież czasu, czyli korzystanie z systemu poza uprawnionymi godzinami,
  • modyfikację zasobów za pomocą bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego.
– Oszustwa przy użyciu komputera, a w szczególności:
  • oszustwa bankomatowe,
  • fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesorowych),
  • oszustwa na maszynach do gier,
  • oszustwa poprzez podanie fałszywych danych identyfikacyjnych,
  • oszustwa w systemach telekomunikacyjnych.
– Powielanie programów, w tym:
  • gier we wszelkich postaciach,
  • wszelkich innych programów komputerowych,
  • topografii układów scalonych.
– Sabotaż zarówno sprzętu, jak i oprogramowania (DoS).
– Przechowywanie zabronionych prawem zbiorów (pornografia dziecięca).
– Przestępstwa popełnione w sieci (rozpowszechnianie treści).

Cyberterroryści mogą właściwie uciec się do wszystkich opisanych powyżej działań, może je również wprowadzić w życie zwykły, złośliwy, ale zdolny internauta. Co więc je od siebie różni?

Mark Pollit, specjalista FBI, podaje bardzo szeroką definicję cyberterroryzmu. Podkreśla, że słowo to jest kombinacją dwóch innych: cyberprzestrzeni i terroryzmu. Cyberprzestrzeń, czyli świat wirtualny, to „symboliczne, nieprawdziwe, binarne, metaforyczne przedstawienie informacji, miejsce, gdzie działają programy komputerowe i gdzie poruszają się dane". Jeśli chodzi o terroryzm, posługuje się sformułowaniem amerykańskiego Departa-

mentu Stanu, mówiącym, że jest to „celowy, motywowany politycznie akt przemocy skierowany przeciw celom niewalczącym przez grupy subnarodowe lub przez podziemnych agentów". Łącząc obie te definicje otrzymujemy następujący opis cyberterroryzmu: „jest to celowy, motywowany politycznie atak przeciw informacji, systemom komputerowym, programom komputerowym i danym, który skierowany jest przeciw niewalczącym celom przez grupy subnarodowe lub przez podziemnych agentów". Pollit zwraca jednocześnie uwagę, iż należy go odróżniać od innych nielegalnych aktów, takich jak przestępczość komputerowa, szpiegostwo gospodarcze czy też wojna informacyjna (Pollit, http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_factorfantasy.html). Do tej ostatniej zaliczyć można zjawisko określane jako haktywizm, czyli „manifestacje o charakterze propagandowo-politycznym". Polegają one na modyfikowaniu zawartości stron www, na ich podmianie (Adamski, 2002: 118) lub też, w szerszym rozumieniu, na użyciu środków zakłóceń elektronicznych przeciwko wrogim witrynom, czyli na wspomnianym już kasowaniu albo podmianie danych, ale też na atakowaniu wirusami i zablokowaniu poprzez atak DoS (http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_armeabsolue.html). Na skutek działań haktywistów internetowa strona arabskiej telewizji Al-Dżazira, nastawionej wyraźnie antyamerykańsko, przestała nagle działać w marcu tego roku. Zamiast strony głównej portalu pojawiała się amerykańska flaga i napis: „niech zabrzmi wolność".

Dorothy Denning, profesor Uniwersytetu w Georgetown oraz dyrektor Georgetown Institute of Information Assurance, przedstawia cyberterroryzm jako „celowe ataki albo groźby ataków skierowane przeciw komputerom, sieciom i przechowywanym w nim informacjom w celu zastraszenia rządów i społeczeństw czy też wymuszenia na nich jakichś politycznych lub społecznych działań". W dodatku, by można je było nazwać cyberterroryzmem, ataki takie powinny być skierowane przeciw osobom lub własności, albo co najmniej powinny powodować szkody wywołujące strach. Przykładami mogą być ataki, które prowadzą do śmierci lub uszkodzenia ciała, eksplozje, katastrofy lotnicze, zakażenia wody lub też poważne straty ekonomiczne. Mogą nimi być również ataki na krytyczne infrastruktury, w zależności od ich zasięgu (Denning, 2000: http://www.cs.georgetown.edu/%7Edenning/infosec/cybertorror.html).

Według innej specjalistki w dziedzinie cyberprzestępczości – Solange Ghernaouti-Helie, profesora Ecole des Hautes Etudes Commerciales w Lozannie, cyberprzestępczość przyjmuje coraz częściej wymiar cyberterroryzmu, gdyż zasoby informatyczne, związane z krytyczną infrastrukturą niezbędną do życia dla jakiegoś kraju, są dostępne przez Internet, a właśnie przejęcie kontroli nad owymi krytycznymi infrastrukturami, czyli energią, wodą, transportem, telekomunikacją, bankowością i finansami, służbami medycznymi, instytucjami rządowymi, jest celem cyberterrorystów (Mayer, 2002: http://www.terrorisme.net). Jednak cyberprzestępczość jest faktem, a cyberterroryzm wciąż jeszcze pozostaje fikcją. Wydaje się bowiem, że „człowiek-bomba" to skuteczniejsza metoda na przeprowadzenie ataku niż opanowanie bardzo dobrze strzeżonych systemów informatycznych instytucji, mających strategiczne znaczenie dla infrastruktury krytycznej. Stwierdzenie powyższe może potwierdzić fakt, że przed 11 września Bin Laden straszył świat pla-

nowanymi atakami cyberterrorystycznymi, mówiąc, że Al-Kaida jest gotowa użyć komputerów jako broni w walce o swoje ideały – kiedy jednak przyszło mu działać, posłużył się klasycznymi metodami terrorystycznymi.

Dorothy Deening jest zdania, że ryzyko zamachów cyberterrorystycznych jest niewielkie, co nie znaczy jednak, że nie istnieje. Zdawać sobie bowiem należy sprawę, że ryzyko cyberterroryzmu będzie wzrastać w społeczeństwie wraz ze wzrostem znaczenia Internetu w naszym życiu. Już dziś w podstawowych dziedzinach gospodarki, takich jak bankowość, finanse, telekomunikacja, handel – systemy informacji stały się nadrzędne. Dostęp do baz danych, blokada systemów komputerowych mogą skutecznie sparaliżować działanie instytucji, a nawet państwa. Nic więc dziwnego, że sieć może być doskonałym polem działań wojennych. Co więcej, cyberwojnę można prowadzić niezależnie od konfliktu na lądzie i morzu, w dodatku mniejszym nakładem kosztów. Możliwe więc, że mają rację ci, którzy twierdzą, że kolejna wojna światowa może być wojną informatyczną.

Chociaż niektórzy wciąż uważają cyberterroryzm za hasło mające na celu napełnianie kieszeni firmom zajmującym się bezpieczeństwem systemów informatycznych, to jednak władze wielu państw podeszły do tego problemu bardzo poważnie. Już w 1991 roku Amerykańska Rada Badań Naukowych w raporcie „Komputery w niebezpieczeństwie" stwierdziła: „Jesteśmy zagrożeni. Ameryka coraz bardziej zależy od komputerów. To one kontrolują dostawy energii, zarządzają komunikacją, rolnictwem, usługami, finansami. Jutrzejszy terrorysta będzie w stanie więcej zdziałać przy pomocy klawiatury komputera niż bomby" (Adamski, 2002: 114).

Bibliografia

[1] Adamski A. 2002: *Cyberterroryzm*, [w:] „Materiały z konferencji nt. Terroryzmu, 11.04.2002, Wydz. Prawa UMK w Toruniu", Toruń.

[2] Bouvier M.: *Cyberterrorisme – entre mythe et realité*, [w:] http://www.frstrategy.org/barreFRS/publications/archives/perspec_strat/51/51-3.asp.

[3] *Cyberterrorisme*, [w:] http://tecfa.unige.ch/etu/E7lb/99/deian/terrorisme.htm.

[4] *Cyberterrorisme: l'arme absolue sur Internet*, [w:] http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_armeabsolue.html.

[5] Denning D.E. 2000: *Cyberterrorism*, May 23, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U. S. House of Representatives, [w:] http://www.cs.georgetown.edu/%7Edenning/infosec/cybertorror.html.

[6] Dębek P. 2001: *Niewidzialne uderzenie*, [w:] „CHIP online", 30.12.2001.

[7] Mayer JF. 2002: *Le cyberterrorisme: une nouvelle menace?*, [w:] http://www.terrorisme.net „Dossier Cyberterrorisme", 26 septembre 2002.

[8] Pietrzak A. 2002: *Światowy terroryzm*, [w:] „Magazyn globalizacji i integracji europejskiej" nr 6, listopad, Glob@lizator.

[9] Pollit M. *Cyberterrorism – fact or fancy?*, [w:] http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_factorfantasy.html.