# Cyberterroryzm, cyberprzestępczość – wirtualne czy realne zagrożenie?

Autor tekstu: **Monika Sadlok**

"Piraci komputerowi rozsyłają w świat wirusa, który otwiera na twardym dysku „tylne drzwi", umożliwiające terrorystom zdalne kontrolowanie komputerów elektrowni atomowych, banków, linii lotniczych, laboratoriów farmaceutycznych, wodociągów. Cyfrowa epidemia paraliżuje cały świat"
(-)Meyer E., Kerdellant Ch. „Cyfrowa Katastrofa"

Truizmem pozostaje stwierdzenie, iż Internet zmienił sposób postrzegania otaczającego nas świata. Stał się on bliższy, bardziej zrozumiały, a w dosyć ryzykownej opinii można także stwierdzić bardziej demokratyczny. W sieci każdy ma jednakowe prawa, nie ma już podziału na twórcę i odbiorcę informacji. Internet jest obecny prawie we wszystkich aspektach działalności każdego z nas. Zakupy, obsługa bankowa, załatwienie spraw urzędowych, a nawet dyskusje bardzo często odbywają się w wirtualnej rzeczywistości.

Jednak Internet to nie tylko ułatwienia w codziennym życiu, rozrywka, czy też środowisko pracy, ale także miejsce działalności grup przestępczych. Ataki hakerskie, wirusy, trojany, to pojęcia znane każdemu użytkownikowi sieci. Coraz częściej także, Internet staje się narzędziem wykorzystywanym przez terrorystów. Do niedawna słaba znajomość nowoczesnych technologii informatycznych uniemożliwiała skuteczne prowadzenie działań w cyberprzestrzeni, a próby ataku dotyczyły przede wszystkim infrastruktury.

Prekursorem techno terroryzmu był włoski multimilioner G. Feltrinelli, przywódca i założyciel Grupy Akcji Partyzanckiej (Gruppi d'Azione Partigiana — GAP). Niszczenie centrum komputerowego domów towarowych w Mediolanie, lokalnego biura administracji rządowej w Rzymie, Centrum komputerowego firmy Date — Montedison, terminali, baz danych typu Honey Level 66, zawierającej informacje o skradzionych i zarejestrowanych we Włoszech samochodach, to najbardziej spektakularne przykłady działalności GAP [1]. W latach osiemdziesiątych miejscem działalności cyberprzestępczej stała się Francja, a ich inicjatorami były ugrupowanie lewicowo — anarchistyczne — Komitet na Rzecz Likwidacji lub Powstrzymywania Komputerów (Comite Liquidant ou Detournant les Ordinateurs — CLODO). Członkowie tej organizacji niszczyli przede wszystkim stanowiska komputerowe min. w Banku Rothschilda w Paryżu, Centrum Komputerowym w Tuluzie należącym do Philips Date System. [2]

Obecnie niewątpliwe akty techno — terroryzmu mają nieco inny charakter, tym nie mniej jednak w 2003 roku na terytorium Stanów Zjednoczonych i Wielkiej Brytanii podjęto wiele działań mających znamiona tzw. terroryzmu miękkiego, inspirowane przez ruch proekologiczny. W Sutton Coldfield zorganizowano akcję niszczenia odbiorników sieci komórkowej trzeciej generacji, które zdaniem części ekologów były przyczyną zwiększonej zachorowalności mieszkańców na choroby nowotworowe. W 2006 roku eksplozja ładunku wybuchowego uszkodziła przekaźnik telefonii komórkowej w Inguszetii, dezorganizując na dłuższy czas łączność na obszarze obwodu naurańskiego.

Wraz z upływem czasu grupy terrorystyczne coraz bardziej doceniają planowe, dobrze przeprowadzone akcje w cyberprzestrzeni, nie polegające już na niszczeniu infrastruktury, ale przede wszystkim związane z zdezorganizowaniem pracy wybranych obiektów, systemów lub służb, w celu zwiększenia skuteczności i pola rażenia zamachów terrorystycznych, prowadzonych różnymi sposobami. Najbardziej spektakularny przykład takiego działania to przeprowadzenie 11 września 2001 roku uszkodzenia przez zespół Al. Kaidy systemów identyfikacji samolotów porwanych i wykorzystanych podczas zamachów. Cyberataki nie są już więc tylko wytworem wyobraźni autorów książek o tematyce fantastyki naukowej, ale realnym zagrożeniem, którego skutki mogą być odczuwalne dla każdego z nas, przeciętnego użytkownika sieci energetycznej, informatycznej. Najbardziej prawdopodobne są bowiem ataki przeciw systemom informatycznym użytkowanym w sferze cywilnej. Poziom ich zabezpieczenia jest bowiem z reguły niższy niż systemów wojskowych.

Działalność grup cyberterrorystycznych ma z reguły dwie formy:

1. Metody, które mogą być stosowane przez każdego członka grupy, czyli przede wszystkim okupowanie sieci (Web sit — In), flooding, czyli obciążenie systemu informatycznego dużą liczbą danych, najczęściej za pomocą poczty elektronicznej. Obie metody przede wszystkim znacząco opóźniają, a w konsekwencji uniemożliwiają korzystanie z konkretnej strony WWW, konta, czy

usługi oferowanej przez dany system. Jedną z pierwszych organizacji stosujących te metody w praktyce była organizacja separatystów tamilskich z LTTE okupująca w ten sposób serwer ambasad Sri Lanki w 1998 roku. Obecnie metody te są skutecznie wykorzystywane przez wszelkie ruchy antyglobalistyczne jak francuska Obywatelska Inicjatywa Opodatkowania Obrotu Kapitałowego (Association pour la Taxation des Transactions pour l'Aide aux Citoyens — ATTAC), brytyjską Globalize Resistance.

2. Metody zawierające techniki działania wymagające odpowiedniej wiedzy na temat atakowanych systemów informatycznych oraz dużych umiejętności praktycznych. Do metod tych zalicza się ataki DoS (Denial of Service), który w zamierzeniu ma uniemożliwić użytkownikom korzystanie z wybranej usługi, poprzez destrukcję lub zmianę konfiguracji zasobów systemu. W jego skutecznej realizacji potrzebne są wyspecjalizowane programy takie jak generatory poczty elektronicznej, programy usuwające zasoby pamięci, powodujące przepełnienie stosu systemowego. Na przykład na początku 2003 roku grupa hakerów pochodzących z Arabii, przez godzinę usiłowała zakłócić pracę serwera Światowego Kongresu Żydów. Inne działania to także próby przełamania zabezpieczeń chroniących systemy przed niepowołanym dostępem. Najbardziej spektakularnym, pomimo braku potwierdzenia, był niewątpliwie atak na systemy kontroli lotów USA w zakresie identyfikacji obiektów latających i kierowania ruchem powietrznym 11 września 2001 roku. W sierpniu 2007 roku cały świat przyglądał się serii ataków na estońskie serwery najważniejszych instytucji państwowych. Uczestnicy konferencji BlackHat uznali je za przejaw nowego zjawiska e — zamieszek. Początkowe przypuszczenia, iż zleceniodawcą ataków były władze rosyjskie okazały się bezpodstawne, a źródłem ataku byli zwykli obywatele, nie tylko Rosji, którzy postępując zgodnie z instrukcją zawartą na forach, dokonali tak spektakularnego cyberataku. W 2009 roku przy wykorzystaniu metody DoS dokonano ataku na serwery (Poyereboot.com, odpowiadający za automatyczne odświeżanie witryny internetowej) agencji rządowych prezydenta Ahmedineżada.

Każda działalność terrorystyczna wymaga sporych nakładów finansowych. Nie ważne czy podstawowym narzędziem jest zwykły karabin maszynowy, czy też laptop podłączony do sieci, organizacje terrorystyczne ponoszą związane z tym koszty nie tylko zakupu, ale także przeszkolenia, organizacji ataku, rozpoznania celu itp. Komputeryzacja banków i instytucji finansowych, wykorzystywanie w ich działalności systemów informatycznych, spowodowały, iż stały się one stałym i bardzo kuszącym obiektem ataków hakerskich. Działania o charakterze kryminalnym, służą ugrupowaniom terrorystycznym jako dodatkowa możliwość pozyskania zasobów finansowych. Wśród wielu form działania, najczęściej ataki przeprowadzone są przez bezpośrednią penetrację systemów informatycznych wykorzystywanych w pracy baku lub innej instytucji finansowej, defraudację z użyciem skradzionych kart debetowych i kredytowych, a także bardziej wyrafinowane odzyskiwanie informacji z programów rozliczeń podatkowych osób fizycznych i firm.

W 2000 roku hakerzy należący do Pakistan Hackerz Club, skradli numery kart kredytowych ok. 700 członków i fundatorów proizraelskiej organizacji Amerykańsko — Izraelskiego Komitetu Spraw Publicznych, działającego na terenie Stanów Zjednoczonych. Kolejnym sposobem pozyskania w nielegalny sposób środków finansowych to wykorzystanie grup hakerskich do ataków wymierzonych w systemy informatyczne instytucji finansowych. Jesienią 2000 roku, działając na zlecenie Hezbollahu, podczas tzw. drugiej intifady, hakerzy spenetrowali systemy informatyczne zarządzane przez Bank Izraela i giełdę w Tel Awiwie. Dane dotyczące liczby ataków nie są w tym przypadku znane, powodem jest oczywiście dbałość o renomę instytucji oferujących usługi w sektorze finansowo — bankowym. Każdy ujawniony atak to potencjalnie mniej klientów obawiających się o bezpieczeństwo swoich oszczędności.

Sieć informatyczna służy także rozpoznaniu operacyjnemu terenu planowanego uderzenia. Dostępność szczegółowych map, schematów i zdjęć służy nie tylko celom informacyjnym, ale także umożliwia doskonałe przygotowanie konwencjonalnych ataków terrorystycznych i to przy użyciu legalnych, powszechnie dostępnych narzędzi. FBI wykryło w 2002 roku, iż członkowie Al. Kaidy poszukiwali w Internecie informacji na temat przejęcia kontroli nad pracą obiektów sieci wodociągowych dostarczających wody pitnej do największych miast USA. Służby Wielkiej Brytanii w 2007 roku ujawniły fakt wykorzystania przez irackich terrorystów zdjęć satelitarnych miejsc stacjonowania sił brytyjskich, dostępnych dzięki przeglądarce internetowej Google. Przytoczone informacje dowodzą, że globalna sieć jest zbyt rozległa i niejednorodna pod względem technicznym, finansowym i organizacyjnym, by umożliwić całkowitą kontrolę ruchu w sieci.

Ponadto, w fazie planowania potencjalnych ataków, Internet wykorzystywany jest jako środek łączności. Pierwszą organizacją, która w celach operacyjnych korzystała z poczty elektronicznej była Organizacja Abu Nidala, a obecnie także Hezbollah, Hamas i Al. Kaida. Podczas śledztwa, dotyczącego najbardziej spektakularnego jak dotychczas zamachu terrorystycznego, w 2001 roku,

odkryto, iż porywacze samolotów komunikowali się za pośrednictwem e — maili wysyłanych z miejsc publicznych. Utrzymywali także kontakt poprzez stronę www, której administratorem był jeden z organizatorów zamachów. Popularność, powszechność, anonimowość, to cechy dzięki którym tak znaczącą popularnością cieszą się wśród grup terrorystycznych bezpłatne konta poczty elektronicznej. W ostatnim okresie, zauważalna jest także zwiększona aktywność na forach internetowych i utrzymywanie łączności członków grupy, właśnie przy użyciu tego narzędzia. Pomimo, iż Internet nadaje się także do organizowania ogólnoświatowych protestów, dotychczas nie stwierdzono przypadków takich działań ze strony ugrupowań terrorystycznych. Metoda ta jest jednak popularna wśród członków ruchu antyglobalistycznego. W przyszłości nie można jednak wykluczyć innego scenariusza. Szczególnie, iż dotychczasowe przykłady akcji protestacyjnych podczas tzw. wydarzenia J-18 [ 3 ] zorganizowanego przez anarchistów, przyniosły ich działaniom spektakularny rozgłos. Na razie grupy terrorystyczne starają się wykorzystać siłę rażenia Internetu poprzez prowadzenie kampanii psychologicznych, a więc akcji mających na celu rozpowszechnienie fałszywych informacji, promowanie wyznawanej ideologii, a więc typowych kampanii propagandowych mających na celu dotarcie do jak największej liczby odbiorców, przekonanie ich do swoich racji.

Działania tego typu prowadzą przede wszystkim Al Kaida, ugrupowania palestyńskie, Armia Wyzwolenia Narodowego Imienia Zapaty w Meksyku, afgańscy talibowie, algierska GSPC oraz bojownicy czeczeńscy. W przypadku aktywności propagandowej Al Kaidy stale się ona zwiększa. Na początku 2004 roku organizacja rozpoczęła wydawanie magazynu internetowego „Obóz Treningowy Al. Battara" przygotowujący pod względem mentalnym przyszłych wojowników. Również Czeczeni publikują, za pośrednictwem Internetu, wiele oświadczeń i informacji przedstawiających ich komentarze na temat wydarzeń w republice, najczęściej wykorzystują w tym celu serwer KavkazCenter.com

W październiku 2009 roku FBI wspólnie z egipską policją ogłosiły, że rozbiły największą sieć cyberprzestępczą. Aresztowanych zostało ponad 100 osób, problem jednak w tym, że zazwyczaj udaje złapać się tylko cyfrowe mrówki, które ulegają ogłoszeniom zapewniającym o możliwości łatwego zarobku, a w rzeczywistości, często nieświadomie stają się, elementem zorganizowanej grupy cyberprzestępczej.

Według opublikowanego przez Panda Security styczniowego raportu, Polska znajduje się na 12 miejscu pod względem liczby zawirusowanych komputerów. Pierwsze miejsca należą do Tajlandii, Chin i Tajwanu, gdzie ponad 70 proc. komputerów zainfekowanych jest wirusem, robakiem lub trojanami. Niewątpliwie rok 2010 należał do jednego z najbardziej niebezpiecznych, jeśli chodzi o liczbę dokonanych ataków cybernetycznych. Najbardziej w pamięci utkwił styczniowy atak hakerów na giganta Google oraz ponad 20 innych korporacji. Epicentrum ataków zlokalizowano w Chinach, a ich wysoki poziom wyrafinowania wskazuje, iż w grę wchodzą działania służb specjalnych. Kolejnym ważnym sygnałem ostrzegawczym był Stuxnet, który zainfekował elektrownię atomową Bushehr. Z kolei robak o nazwie „Here you have" stworzony przez organizację „Brygady Tarig ibn Ziyad" miał przypomnieć Stanom Zjednoczonym o 11 września. Miniony rok obfitował także w liczne przykłady e — protestów, wszystko dzięki grupie Anonymous, która występowała przeciwko organizacjom chroniącym prawa autorskie, a pod koniec roku wystąpiła w obronie założyciela Wikileaks.

Polskie służby specjalne potwierdziły próby 185 ataków w cyberprzestrzeni. Opracowana przez rząd Strategia Obrony Cyberprzestrzeni na lata 2011 — 2016, przy współpracy z MSWiA, ABW oraz MON wprowadza „ściganie z urzędu naruszenie bezpieczeństwa w cyberprzestrzeni, które miały miejsce w odniesieniu do podmiotów administracji publicznej i infrastruktury krytycznej" Ponadto planowanie jest powołanie pełnomocnika rządu ds. ochrony cyberprzestrzeni, który ma koordynować pracę ministerstw, policji, Straży Granicznej i służb specjalnych.

Wydaje się, że cyberwojna w Internecie trwa w najlepsze, jednak szczególną uwagę prawdopodobnie przyciągnie rozpoczynający się właśnie nowy jej etap — atak poprzez Cloud computing, czyli „chmurę". To nowa forma korzystania z dobrodziejstw sieci, gdzie zarówno oprogramowanie, jak i dane przechowywane są na serwerach operatora. Dostęp do przeglądarki, w dowolnym miejscu, z dowolnego komputera pozwala użytkownikowi na korzystanie z aplikacji biurowych. Oferta jest na tyle kusząca, iż zainteresowanie nią widać nie tylko ze strony indywidualnych klientów, ale także firm i administracji publicznej. Uzupełnieniem będzie koncepcja smart grid, czyli integracje systemów przesyłu elektryczności z sieciami teleinformatycznymi. Oznacza to możliwość łączenia nie tylko ludzi, lecz także urządzeń zaopatrzonych w mikroprocesory, taki jak lodówka, pralka, telewizja. Jak w tym przypadku wygląda sprawa bezpieczeństwa?

Potencjalny cyberatak, będzie w stanie wyrządzić ogromne, wręcz niewyobrażalne szkody, których skutki odczuje każdy. Ponadto Internet, do niedawna jeszcze symbol wolności, staje się coraz bardziej polem działania kompleksu bezpieczniacko - przemysłowego (nazwa użyta w raporcie NeoComOpticon), czyli współpracy służb bezpieczeństwa z firmami komercyjnymi. Tym ostatnim niewątpliwie zależeć będzie na budowaniu atmosfery strachu, tak aby nowe formy zabezpieczeń znajdowały szybko nabywców.

W przypadku tak szybkiego rozwoju technologii, możliwości wykorzystania sieci, trudno stawiać prognozy dotyczące przyszłości. Można jedynie pokusić się o sformułowanie kilku podsumowujących wniosków:

Cyberprzestępczość, cyberterroryzm, cyberwojna, to już nie zagrożenia o których można przeczytać w literaturze science fiction, ale realne działania, których jesteśmy coraz częściej świadkami. Przed każdym cyberaktakiem można próbować się obronić, nie zawsze obrona będzie skuteczna, ale umożliwi zminimalizowanie strat. Potrzebne są niewątpliwie nowe regulacje prawne i to nie tylko na forum krajowym, ale przede wszystkim na poziomie międzynarodowym, które stanowić będą fundament bezpieczeństwa mieszkańców globalnej wioski.

---

Przypisy:

**[ 1 ]** Campbell A., *A Detailed History of Terrorist and Hostile Intelligence Attacks Against Computer Resources* Fairfax 1992r.

**[ 2 ]** Campbell A., *A Detailed History of Terrorist and Hostile Intelligence Attacks Against Computer Resources* Fairfax 1992r.

**[ 3 ]** Akcja protestacyjne zorganizowana 18 czerwca 1999 roku w Londynie, przeciwko negatywnym skutkom kapitalizmu.

**Monika Sadlok**
Politolożka, obecnie kończy doktorat z zakresu nauk o polityce. Poza pracą naukową, działa również społecznie w "Fundacji Rozwoju Demokracji Lokalnej", w "Stowarzyszeniu Meritum", oraz w "Fundacji Młodzi Twórcy im. prof. P. Dobrowolskiego"

Pokaż inne teksty autora

(Publikacja: 19-01-2011)
Oryginał.. (http://www.racjonalista.pl/kk.php/s,846)

Contents Copyright © 2000-2011 Mariusz Agnosiewicz
Programming Copyright © 2001-2011 Michał Przech

Autorem portalu Racjonalista.pl jest Michał Przech, zwany niżej Autorem.
Właścicielami portalu są Mariusz Agnosiewicz oraz Autor.

Żadna część niniejszych opracowań nie może być wykorzystywana w celach komercyjnych, bez uprzedniej pisemnej zgody Właściciela, który zastrzega sobie niniejszym wszelkie prawa, przewidziane
w przepisach szczególnych, oraz zgodnie z prawem cywilnym i handlowym,
w szczególności z tytułu praw autorskich, wynalazczych, znaków towarowych
do tego portalu i jakiejkolwiek jego części.

Wszystkie strony tego portalu, wliczając w to strukturę katalogów, skrypty oraz inne programy komputerowe, zostały wytworzone i są administrowane przez Autora. Stanowią one wyłączną własność Właściciela. Właściciel zastrzega sobie prawo do okresowych modyfikacji zawartości tego portalu oraz opisu niniejszych Praw Autorskich bez uprzedniego powiadomienia. Jeżeli nie akceptujesz tej polityki możesz nie odwiedzać tego portalu i nie korzystać z jego zasobów.

Informacje zawarte na tym portalu przeznaczone są do użytku prywatnego osób odwiedzających te strony. Można je pobierać, drukować i przeglądać jedynie w celach informacyjnych, bez czerpania z tego tytułu korzyści finansowych lub pobierania wynagrodzenia w dowolnej formie. Modyfikacja zawartości stron oraz skryptów jest zabroniona. Niniejszym udziela się zgody na swobodne kopiowanie dokumentów portalu Racjonalista.pl tak w formie elektronicznej, jak i drukowanej, w celach innych niż handlowe, z zachowaniem tej informacji.

Plik PDF, który czytasz, może być rozpowszechniany jedynie w formie oryginalnej, w jakiej występuje na portalu. **Plik ten nie może być traktowany jako oficjalna lub oryginalna wersja tekstu, jaki zawiera**.

Treść tego zapisu stosuje się do wersji zarówno polsko jak i angielskojęzycznych portalu pod domenami Racjonalista.pl, TheRationalist.eu.org oraz Neutrum.eu.org.

Wszelkie pytania prosimy kierować do redakcja@racjonalista.pl