ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
ROK XLVI NR 1 (160) 2005

Tomasz Szubrycht

CYBERTERRORYZM JAKO NOWA FORMA ZAGROŻENIA TERRORYSTYCZNEGO

STRESZCZENIE

Przedstawianie alarmujących wieści dotyczących cyberterroryzmu w środkach masowego przekazu nie znajduje potwierdzenia w rzeczywistości. Stanowisko mediów jest bowiem efektem nieznajomości definicji tej formy terroryzmu. Swoista psychologia strachu przed atakami na struktury informatyczne wynika ze stopnia uzależnienia współczesnych społeczeństw od technologii informatycznej oraz od narastającego zagrożenia aktami terrorystycznymi. Ze względu na potencjalne skutki jest to kusząca forma aktywności terrorystycznej. W artykule przedstawiono kilka, zdaniem autora najbardziej reprezentatywnych, definicji cyberterroryzmu oraz próby klasyfikacji potencjalnych ataków w cyberprzestrzeni[1].

Terroryzm jest problemem towarzyszącym społeczeństwu od dawna. W ostatnich kilku latach jesteśmy świadkami swoistej zmiany jakościowej tego zjawiska. W działania o charakterze terrorystycznym wprzęgnięte zostały nowe środki, które sprawiają, że straty i negatywne skutki społeczne takich działań są coraz groźniejsze dla społeczności międzynarodowej. Psychoza zagrożenia potęgowana jest przez środki masowego przekazu.

Terroryzm jest zjawiskiem trudnym do jednoznacznego określenia, istnieje bowiem bardzo wiele różnorodnych metodologii jego definiowania. Dodatkowo pojęcie to na przestrzeni lat ulegało systematycznym zmianom i modyfikacjom. Słowo terroryzm pochodzi z łaciny i oznacza strach, grozę. Dalej przedstawiono dwie z bardzo wielu pojawiających się definicji tego zjawiska.

[1] Cyberprzestrzeń – to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Ułatwia ona użytkownikowi sieci kontakty w czasie rzeczywistym. Obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych.

SŁOWNIK ENCYKLOPEDYCZNY EDUKACJI OBYWATELSKIEJ: „(...) metoda działania polegająca na: przemocy wobec pojedynczych osób, aparatu władzy, czyli terror indywidualny lub wobec przypadkowych członków społeczeństwa, zamachy na urzędy, lokale publiczne, koszary itp. – terroryzm zbiorowy" [10].

BRIAN JENKINS: „(...) działania, które mogą przyjąć formy klasycznych aktów kryminalnych, takich jak morderstwa, podpalenia, użycie materiałów wybuchowych. Różnią się jednak od zwykłych działań kryminalnych tym, że są dokonywane ze szczególnie przemyślanym zamiarem wywołania paniki, zaburzenia porządku czy zastraszenia populacji, w celu destrukcji porządku publicznego, sparaliżowania możliwości reagowania społeczeństwa, zwiększenia poczucia bezradności i nieszczęścia wspólnoty" [5].

Obie przedstawione definicje nie w pełni charakteryzują akty terroru. W efekcie przeprowadzonej analizy porównawczej różnorodnych (aż 109) definicji terroryzmu oraz opinii zawartej w [7] można stwierdzić, że w większości z nich występują pewne wspólne elementy. Są to: stosowanie przemocy i siły, polityczny aspekt czynu, wywoływanie strachu, groźba jako element zastraszania, skutki i reakcje psychologiczne przeprowadzonych działań.

Na podstawie dostępnych opinii można założyć, że obecnie i w dającej się przewidzieć przyszłości terroryzm będzie jednym z najpoważniejszych zagrożeń współczesnego świata. Ponadto będzie on przyjmował nowe formy działania, które nie były dotychczas spotykane.

POJĘCIE CYBERTERRORYZMU

Ostatnia dekada XX wieku przyniosła poważny postęp cywilizacyjny. Obejmuje on zmiany: technologiczne, polityczne, społeczne i kulturowe. Postęp w globalnych procesach wytwarzania, przetwarzania i przekazywania informacji jest jednym z najważniejszych elementów przedstawionych zmian. Z dobrodziejstw tego postępu korzysta coraz więcej państw, także tych, które dotąd nie dysponowały dostępem do najnowocześniejszych osiągnięć z dziedziny zaawansowanych technologii. Powoduje to jednak postępujące uzależnienie od technologii informatycznych. Sprawia również, że coraz więcej państw staje w obliczu wzrastającego zagrożenia nową formą terroryzmu, a mianowicie cyberterroryzmem[2].

[2] Dla określenia tej formy działalności terrorystycznej używane jest określenie cyberterroryzm, terroryzm informacyjny lub hi-tech terroryzm.

O niebezpieczeństwie aktów terrorystycznych popełnionych za pomocą systemów komputerowych (terroryzm informacyjny), a wymierzonych w życie i zdrowie ludzi, bezpieczeństwo publiczne oraz środowisko naturalne mówi się coraz więcej i coraz powszechniej [11].

Niestety, pojawia się wiele wątpliwości, nieporozumień i niejasności związanych z definiowaniem cyberterroryzmu, podobnie jak ma to miejsce przy definiowaniu terroryzmu. Postrzeganie tego zjawiska można podzielić na trzy grupy:

- pojęcia prezentowane w mediach;
- definicje obowiązujące w gronie specjalistów;
- definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyki.

Poniżej przedstawiono najbardziej reprezentatywne definicje cyberterroryzmu:

(1) Dorothy Denning: „(...) groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu" [4].

(2) James Lewis: „(...) wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań" [8].

(3) US National Infrastructure Protection Centre: „(...) akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i / lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu" [6].

(4) US Federal Bureau of Investigation: „(...) jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny[3], przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne" [6].

[3] Gdy obiekty ataku przybierają charakter militarny, mamy do czynienia z walką elektroniczną w cyberprzestrzeni [przyp. aut.].

(5) M. Pollitt z George Washington University: „(...) jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe" [9].

Analiza przedstawionych definicji pozwala zaobserwować pojawiające się w nich dwa zasadnicze wyróżniki. Definicje (2) i (3) uwzględniają to, że istnieje możliwość wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku cybernetycznego. Definicje (1), (4) i (5) zawierają natomiast określenie, że komputery i systemy informacyjne są celem takiego ataku. Sporny charakter filozofii podejścia do omawianego zagadnienia jest chyba najważniejszym elementem przytoczonych definicji.

Przyjmuje się, że dla sklasyfikowania ataku jako cyberterroryzmu konieczne jest użycie systemu informatycznego lub dowolnego urządzenia elektronicznego. Wielokrotnie cyberterroryzm i cyberatak[4] są traktowane jako elementy równoważne, co w konsekwencji prowadzi do nieporozumień.

D. Denning uważa, że politycznie umotywowany cyberatak, który prowadzi do śmierci, ofiar lub uszkodzeń ciała, eksplozji bądź poważnych strat materialnych, może być przykładem cyberterroryzmu. Takim działaniem nie jest przypadek ataku, który jedynie zakłóca przyjęty porządek prawny lub ekonomiczny lub taki, który nie pociąga za sobą zasadniczych zakłóceń lub strat. Opierając się na przedstawionych definicjach (1), (2) i (4), należy stwierdzić, że do tej pory nie było przypadku cyberterroryzmu. Jeśli zaś zastosuje się kryteria kwalifikacyjne w oparciu o definicję (3), to zdarzyło się kilka przypadków takich działań. Nie były one jednak poparte motywacją polityczną lub inną, która kwalifikowałaby je jako przypadki terroryzmu.

PSYCHOLOGICZNE ASPEKTY CYBERTERRORYZMU

Powszechność aktów terrorystycznych w ostatnich kilku latach sprawiła, że większość specjalistów jednogłośnie przyjmuje, iż to właśnie działania o tym charakterze stanowić będą największe zagrożenie i wyzwanie w najbliższej przyszłości. Akty terroru przyjmują różnorodne formy. Do momentu ich wystąpienia traktowane są jako swoiste *political-fiction*. Można stwierdzić, że terroryzm ostatnich lat osiągnął taki poziom irracjonalności, iż trudno jest przewidzieć, w którą stronę będzie

[4] Ma miejsce, gdy informacje, programy, systemy komputerowe lub bazy danych stają się obiektem ataku [przyp. aut.].

on ewaluował lub jakie nowe formy przyjmie. Tym samym, mimo dotychczasowego braku przykładów cyberataków, należy być świadomym, że groźba ich wystąpienia jest realna. Poniżej przedstawiono systematykę działań przestępczych, które mogą być realizowane w cyberprzestrzeni [1].

CHARAKTER DZIAŁAŃ

Działania bezprawne	Hakerstwo	Szpiegostwo[5]	Cyberterroryzm	Cyberagresja

← Zamierzone i świadome lub niezamierzone i nieświadome działania[6] →

LOKALIZACJA

Terytorium państwa będącego obiektem działań w cyberprzestrzeni	Wody międzynarodowe Międzynarodowa przestrzeń powietrzna	Terytorium państwa wykorzystywane przez obcokrajowców	Inne państwo

EFEKT DZIAŁAŃ

Małe skutki ekonomiczne zakłócenia systemu informatycznego	Małe skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami	Poważne skutki ekonomiczne zakłócenia systemu informatycznego	Poważne skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami	Działania stanowiące zagrożenie dla bezpieczeństwa narodowego

← Zamierzone i świadome lub niezamierzone i nieświadome działania →

Od kilkunastu lat następuje coraz większe uzależnianie się społeczeństw od techniki komputerowej. Jednocześnie cyberprzestrzeń pozostaje dla większości ludzi

[5] Pierwszy przypadek szpiegostwa cybernetycznego miał miejsce w 1986 roku. KGB zwerbowało pięciu niemieckich hakerów, którzy włamali się do amerykańskiego Departamentu Obrony i uzyskane informacje przekazywali Rosjanom.

[6] Działania niezamierzone podejmowane są przez nieświadomego aktora cyberkonfliktu. Osoba (osoby) taka może być świadoma lub nieświadoma nielegalności prowadzonego działania; może nie wiedzieć, iż jest manipulowana przez świadomych aktorów konfliktu w cyberprzestrzeni [1].

swoistą tajemnicą. Trudno zatem się dziwić, że samo wspomnienie o cyberterroryzmie powoduje powszechny niepokój. Z psychologicznego punktu widzenia terroryzm informatyczny zawiera w sobie dwa elementy wywołujące racjonalne i irracjonalne obawy lub strach.

Aspekt irracjonalności sprowadza się do obawy utracenia kontroli nad systemami komputerowymi. Komputery realizują obecnie wiele czynności stanowiących do tej pory domenę człowieka. Wykonują je znacznie szybciej i dokładniej. Dlatego wiele osób obawia się, iż może nadejść moment, w którym to komputery staną się decydentami, a ludzie jedynie wykonawcami. Oczywiście trudno jest racjonalną argumentacją eliminować takie obawy. Dodatkowo są one potęgowane przez mit, że coś, co trudno kontrolować – łatwo zakłócić lub wykorzystać niezgodnie z obowiązującym prawem.

Racjonalne obawy związane są z aktywnością terrorystyczną i przybierają na sile w ostatnich latach. Społeczeństwa zagrożone takimi atakami są w ciągłej obawie co do czasu lub celu ataku. To terroryści wybierają czas i miejsce. W przypadku tej formy terroryzmu obawy podsycane są przez środki masowego przekazu, które w pogoni za sensacją nawet absurdalne zdarzenia obwieszczają jako przypadki cyberterroryzmu. Oczywiście i bez udziału środków masowego przekazu społeczeństwo świadome jest stopnia potencjalnego zagrożenie dzięki istnej pladze komputerowych wirusów[7], trojanów[8], robaków[9], „bomb logicznych”[10] itp.

Jednak to doniesienia prasowe, radiowe i telewizyjne dostarczają fałszywych dowodów na działania cyberterrorystów. Wynika to z braku zrozumienia istoty problemu.

Do podstawowych mitów „cyberterroryzmu” należy utożsamianie każdego niepożądanego wywierania wpływu na działalność w cyberprzestrzeni z terrory-

[7] Wirus to samoreprodukujący się kod, który uszkadza dane lub programy, zmieniając sposób działania sprzętu. Inaczej mówiąc, wirus jest „obcym” fragmentem kodu dołączonym do programu. Wykonanie tego kodu po uruchomieniu programu powoduje odnajdywanie na dysku innych, „niezarażonych” programów i dołączanie do nich kodu wirusa. W ten sposób wirus zaraża coraz więcej obszarów w komputerze.

[8] Trojany – kod udający program użytkowy, który podczas działania może bez wiedzy użytkownika wykonywać potajemne zadania (np. wykradanie danych) lub wyrządzać w komputerze poważne zniszczenia.

[9] Robaki – rodzaj wirusa komputerowego, który potrafi samodzielnie rozsyłać swoje kopie do innych komputerów poprzez połączenia sieciowe.

[10] „Bomba logiczna” – to program ze specjalnym kodem, który po zainfekowaniu komputera lub sieci pozostaje uśpiony do wcześniej określonego wydarzenia, po wystąpieniu którego uaktywnia się i rozpoczyna niszczenie zawartości komputera lub komputerów sieci.

zmem. Tym samym działanie hakerskie[11] nastolatków, tworzenie wirusów komputerowych, działania wymierzone w bazy danych czy sieci komputerowe (pomimo tego, że mogą powodować nawet duże straty materialne) nie powinny być kojarzone z terroryzmem informatycznym (cyberterroryzmem). Poniżej przedstawione zostaną wiadomości, które w znaczący sposób przyczyniły się do podgrzania atmosfery w tym zakresie.

Australia

W listopadzie 2001 roku Vitek Boden (lat 49) został skazany na dwa lata więzienia za wykorzystanie Internetu, radia i ukradzionego oprogramowania do wypuszczenia miliona litrów ścieków do rzeki i wód przybrzeżnych Maroochudore w Queesland w Australii. Skazany był konsultantem przy opracowywaniu projektu wodnego. Opisany atak przeprowadził w marcu 2000 roku, po tym jak odrzucono jego kandydaturę na pracownika władz hrabstwa Maroochy. W efekcie jego działań na akwenie objętym wyciekiem zamarło życie biologiczne, a mieszkańcy tego rejonu ze względu na panujące warunki musieli na okres wielu tygodni opuścić miejsce zamieszkania.

USA

W 1997 roku amerykański nastolatek unieruchomił główną kampanię telefoniczną obsługującą mały port lotniczy w Worcester (Massachusetts) na sześć godzin. W tym czasie wieża kontrolna nie miała możliwości świadczenia usług normalnymi kanałami. Bezpieczeństwo lotów zapewniono dzięki informacjom przekazywanym samolotom przez inne porty lotnicze drogą radiową.

Jak wielkie zagrożenie stanowią takie ataki, można sobie uświadomić, analizując dane dotyczące ataków informatycznych, które wykonywane są na pozawojskowe systemy informatyczne. W 2003 roku szacunkowe straty wywołane takimi atakami wyniosły 82 mld dolarów. Na świecie ich liczba systematycznie wzrasta. W tabeli 1. przedstawiono dane dotyczące ataków na sieci informatyczne w ostatnich latach.

[11] Haker – to zazwyczaj utalentowany programista, włamywacz sieciowy, ekspert z dziedziny bezpieczeństwa systemów komputerowych poszukujący dostępu do zamkniętych systemów w celu poszerzenia wiedzy i zdobywania nowych doświadczeń.

Tabela 1. Globalna statystyka ataków na sieci informatyczne

Lp.	Rok	Liczba ataków
1	1995	4
2	1996	18
3	1997	34
4	1998	269
5	1999	4197
6	2000	7821
7	2001	31323
8	2002	87525

Źródło: M. Pollitt, Cyberterrorism – Fact or Fancy?

Współcześnie każde pojawienie się nowych wirusów, zaatakowanie Internetu czy włamanie do systemów komputerowych utożsamiane jest z terroryzmem. Motywacje do rozpowszechniania takich mitów mają różne podłoże, na przykład poszukiwanie sensacji lub napędzanie koniunktury firmom produkującym specjalistyczne oprogramowanie zabezpieczające.

Tym niemniej, najlepszą i chyba najskuteczniejszą metodą walki z tą formą terroryzmu jest profilaktyka. Jak dotychczas nie odnotowano faktycznych ataków terrorystycznych w cyberprzestrzeni lub z wykorzystaniem techniki komputerowej (pomimo mody i nośności tematu terroru informatycznego). Nie powinno to jednak uśpić czujności czynników odpowiedzialnych za bezpieczeństwo w tym zakresie.

MOŻLIWE FORMY ATAKÓW CYBERNETYCZNYCH

Potencjalny atak terrorystyczny w cyberprzestrzeni może obejmować oprogramowanie przeciwnika (*software*) lub systemy informacyjne i sprzęt komputerowy (*hardware*). Ze względu na różnorodność metod działania oraz różnorodność kryteriów opisu tego zjawiska, nie ma jednoznacznej klasyfikacji. W artykule opierano się na książce A. Bógdał-Brzezińskiej i M. Gawryckiego pt. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie* [2]. Obejmują one wybrane rodzaje stosowanych terminów i metody ich klasyfikacji, które odnoszą się do poziomów ataków w cyberprzestrzeni. Oczywiście nie wyczerpują w pełni przedstawianego problemu.

Pierwszą zaprezentowaną metodą klasyfikacji jest lista siedmiu kategorii działań w cyberprzestrzeni opracowana przez W. Cheswicka i S. Bellovina [2]:

1. *Stealing passwords* – uzyskanie haseł dostępu do sieci.
2. *Sodal engineering* – wykorzystanie niekompetencji osób, które mają dostęp do systemu.
3. *Bugs and backdoors* – korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł.
4. *Authentication failures* – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji.
5. *Protocol failures* – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami lub procesami.
6. *Information leakage* – uzyskanie informacje dostępnych tylko administratorowi, niezbędnych do poprawnego funkcjonowania sieci.
7. *Denial of Service* – uniemożliwienie korzystania z systemu.

F. Cohen, mając na uwadze powyższą listę kategorii, stworzył własną kategoryzację, która uwzględniała przede wszystkim rezultat ataku w cyberprzestrzeni. Rozpatrywane kategorie to:

1. *Corruption* – nieuprawniona zmiana informacji.
2. *Leakage* – informacja znalazła się w niewłaściwym miejscu.
3. *Denial* – kiedy komputer lub sieć nie nadają się do użytkowania.

Warto zauważyć, że wielu specjalistów (w tym J. Howard i T. Longstaff) podkreśla, iż działania w sferze cyberprzestrzeni nie da się zakwalifikować tylko do jednej kategorii. Często są to akcje mieszczące się w wielu kategoriach.

W efekcie takiego ujęcia P. Neumann i D. Parker zaproponowali następujący podział, który opiera się na dostępnych danych empirycznych [2]:

1. *External Information Theft* – przeglądanie oraz kradzież informacji przez osobę spoza systemu.
2. *External Abuse of Resources* – zniszczenie twardego dysku.
3. *Masquerading* – podawanie się za kogoś innego.
4. *Pest Programs* – zainstalowanie złośliwego programu.
5. *Bypassins Authentication or Authority* – złamanie haseł.
6. *Authority Abuse* – fałszowanie danych.
7. Abuse *Through Inaction* – celowe prowadzenie złego zarządzania.
8. *Indirect Abuse* – używanie innych systemów do stworzenia „złośliwych" programów.

Kategoryzacja wprowadzona przez P. Neumanna i D. Parkera wydaje się najpełniejsza, bo daje możliwość klasyfikacji różnego rodzaju ataków. Nie jest to jednak rozwiązanie idealne. Pojawiają się opinie (np. E. Amorosa), że listy empiryczne są mało spójne i logiczne. Ponadto tworzenie długich list, opartych na empirycznych obserwacjach, będzie niepraktyczne.

C. Landwehr i A. R. Buli stworzyli tzw. matryce pojęciowe, które opierają na następujących aspektach [2]:

1. *Genesis* – wykorzystaniu „dziur" w zabezpieczeniach (*security flaw*).
2. *Time of Introduction* – czasie „życia" oprogramowania i sprzętu komputerowego.
3. *Location* – lokalizacji „dziur" w oprogramowaniu i sprzęcie komputerowym.

Stworzenie prezentowanych matryc dokładnie opisuje różnorodne ataki możliwe do przeprowadzenia w cyberprzestrzeni oraz jest przydatne do klasyfikacji tzw. indywidualnych uderzeń (takich, które można przypisać do jednej kategorii). Nie jest to jednak łatwe w przypadku ataków złożonych.

Jak już wspomniano, istnieje wiele różnorodnych klasyfikacji. Ze względów praktycznych ostatnią zaprezentowaną w artykule jest klasyfikacja opracowana przez W. Stallingsa, która uwzględnia [2]:

1. *Interruption* – zabezpieczenie systemu zostało zniszczone lub nie można go zastosować.
2. *Interception* – osoba nieuprawniona zdobyła dostęp do istniejących zabezpieczeń.
3. *Modification* – nieuprawniona grupa nie tylko zdobyła dostęp, ale również manipulowała zabezpieczeniem.
4. *Fabrication* – nieuprawniona grupa wprowadziła sfałszowany obiekt do systemu.

Klasyfikacja ta ma ograniczoną możliwość zastosowania, ponieważ dotyczy jedynie ataków traktowanych jako seria działań.

Wydaje się, że przedstawiona różnorodność klasyfikacji jest dowodem zarówno na wieloaspektowość prezentowanego zagadnienia, jak i na dynamikę zjawisk zachodzących w cyberprzestrzeni.

POTENCJALNE CELE I OBIEKTY ATAKÓW

Panuje powszechna opinia, że coraz więcej społeczeństw w coraz większym stopniu uzależnionych jest od informatyki. Komputery kontrolują lub gromadzą informacje w takich dziedzinach życia, jak: dostarczanie energii, komunikacja, transport lotniczy, służby finansowe, gromadzenie danych medycznych, danych o przestępstwach kryminalnych itp. Istnieje przeświadczenie poparte licznymi dowodami, że współczesny przestępca może ukraść znacznie większe sumy pieniędzy za pomocą klawiatury komputerowej niż za pomocą broni. Tym samym stosując podobna analogię, współczesny terrorysta może dokonać znacznie więcej zniszczeń za pomocą komputera niż bomb. Pamiętać należy jednak, że znacznie łatwiej jest użyć bomb, niż włamać się do systemów komputerowych.

Przy rozpatrywaniu zagadnień cyberterroryzmu należy rozróżnić, jakie działanie jest terroryzmem, a jakie nim nie jest. Rozpatrując zagadnienia związane z nielegalną aktywnością na polu informatycznym, konieczne jest rozróżnienie tak zwanych h a c k t y w i s t ó w . Są oni również zmotywowani politycznie, ale nie mogą być utożsamiani z terrorystami. Ich zasadniczym celem jest protestowanie, manifestowanie lub podejmowanie prób obalenia panującego porządku. Nie zamierzają zadawać śmierci, okaleczać, powodować zniszczeń czy wreszcie szerzyć strachu. Ich działania udowadniają jednak, że cyberterroryzm jest możliwy. Linia rozgraniczenia między cyberterroryzmem a hacktywizmem jest cienka. Musi nam towarzyszyć świadomość, że jeśli terroryści zwerbują lub wynajmą hacktywistę dla swoich celów bądź hacktywiści zdecydują się rozszerzyć zakres działań poprzez zaatakowanie newralgicznych stref działalności państwa – wówczas staną się cyberterrorystami.

Jak już wspomniano, wyróżnić możemy dwa zasadnicze aspekty cyberterroryzmu:

– kiedy celem jest technologia informatyczna;
– kiedy technologia informatyczna jest jedynie narzędziem.

W pierwszym przypadku celem ataków terrorystycznych są systemy informatyczne, atakowane z zamiarem przeprowadzenia sabotażu zarówno elektronicznego, jak i fizycznego. Działania te mogą spowodować zniszczenie, uszkodzenie systemu informatycznego lub dowolnej struktury informatycznej. Efekt ataku uzależniony jest od wykorzystywanej technologii informatycznej oraz charakteru wybranego celu.

Drugi przypadek odnosi się do sytuacji, w której terroryści mogą wykorzystywać narzędzia informatyczne w celu manipulowania, penetracji lub kradzieży danych bądź wymuszenia takiego działania systemu, który jest zgodny z intencją terrorystów.

Jednym z największych zagrożeń – gdy teoretycznie rozpatrywany cyberterroryzm może stać się faktem – byłoby zwerbowanie specjalistów z dziedziny informatyki (programistów) zaangażowanych przy tworzeniu oprogramowania w agencjach rządowych lub dużych korporacjach prywatnych.

Przykładem może być Japonia. W marcu 2000 roku policja japońska ogłosiła, że w pracach nad oprogramowaniem umożliwiającym śledzenie ponad 150 pojazdów policyjnych, w tym pojazdów nieoznakowanych, uczestniczyli aktywni członkowie grupy **Aum Shinryko** (która dokonała ataku gazowego na metro w Tokio). Co więcej, przynajmniej 8 japońskich firm prywatnych i aż 10 agencji rządowych przy pracach nad oprogramowaniem zatrudniało, bezpośrednio lub poprzez kooperantów, członków tej sekty. Tym samym istnieje prawdopodobieństwo zainstalowania przez nich „koni trojańskich" w opracowanym oprogramowaniu, które mogą być w przyszłości wykorzystane do przeprowadzenia ataku cyberterrorystycznego.

Powszechnie przyjmuje się, że terroryści nie posiedli dotychczas wystarczającej wiedzy, by dokonać takich ataków. Sytuacja ulega jednak zmianie. W Afganistanie znaleziono laptopa należącego do **Al-Kaidy**, w którym zainstalowane było specjalistyczne oprogramowanie z zakresu mechaniki i modele elektroniczne tam wodnych, systemów wodociągowych, plany elektrowni atomowych oraz dużych stadionów sportowych w Europie i USA.

Jedyne dotychczas udokumentowane przykłady wykorzystywania przez grupy terrorystyczne techniki informatycznej dotyczą używania Internetu dla celów łączności, werbowania nowych członków, koordynowania klasycznych ataków terrorystycznych, rozpowszechniania ideologii bądź rozpowszechniania informacji o dokonanych atakach. Ostatnie miesiące pokazały, że takie nowoczesne narzędzie jak Internet wykorzystywane jest również jako element szerzenia strachu. Przykładem może być zamieszczenie na stronach internetowych filmów z ideologicznym i politycznym przesłaniem, które dokumentowały egzekucje porwanych w Iraku obywateli różnych państw.

WNIOSKI

Strach informatyczny jest zjawiskiem coraz powszechniejszym, jednak jest on wyolbrzymiony. Pomimo faktu, że pozaprawne ataki informatyczne na newralgiczne składniki narodowej infrastruktury informatycznej stają się coraz powszechniejsze, to nie są one, jak dotychczas, przeprowadzane przez terrorystów. Poziom ich niszczycielskiej siły nie jest ponadto na tyle znaczny, by można go zakwalifikować jako terroryzm informatyczny. Jakkolwiek strach przed tym zagrożeniem jest przesadzony, to nie może być lekceważony czy ignorowany.

Zwalczanie terroryzmu informatycznego stało się nie tylko ważnym zagadnieniem natury politycznej, ale również, a może przede wszystkim, problemem natury ekonomicznej. Po spektakularnych akcjach terrorystycznych we wrześniu 2001 roku federalne władze amerykańskie wydały prawie 4,5 mld $ na zabezpieczenie istniejących systemów informatycznych.

Paradoksalnie, sukcesy w walce z klasycznym terroryzmem mogą sprawić, że terroryści skierują swoje zainteresowanie w stronę nowych metod działania, np. cyberterroryzmu. Może on stać się atrakcyjną formą działania z następujących powodów:

1. W porównaniu z klasycznym terroryzmem jest tańszą formą działalności. Do jego przeprowadzenia potrzebny jest jedynie komputer i podłączenie do sieci. Nie ma potrzeby kupowania lub zdobywania broni czy materiałów wybuchowych. Zasadniczym orężem jest tworzenie wirusów, robaków komputerowych, fałszywek czy „koni trojańskich" i przesłanie ich do wybranego celu ataku. Jeszcze skuteczniejsze, chociaż trudniejsze, jest wniknięcie do systemu i wymuszenie działań, których efekty mogą być z punktu widzenia terrorystów o wiele bardziej pożądane niż tradycyjne akcje terrorystyczne.
2. Przedsięwzięcia informatyczne stwarzają możliwość bardziej anonimowej działalności terrorystycznej niż formy tradycyjne. Jak wielu internautów, terroryści mogą użyć pseudonimów lub wykorzystać opcję użytkownika anonimowego, co sprawi, że zidentyfikowanie prawdziwych nazwisk terrorystów będzie bardzo trudne lub wręcz niemożliwe. W cyberprzestrzeni nie ma fizycznych barier kontrolnych, granic, staży granicznej, celników, których trzeba przechytrzyć.
3. Potencjalna liczba celów ataków informatycznych jest przeogromna. Terroryści mogą zaatakować komputery lub rządowe sieci komputerowe, sieci firm prywatnych czy indywidualnych osób itp. Prawdopodobieństwo znalezienia słabego punktu w zabezpieczeniach jest więc stosunkowo duże. Oczywiście

otwartą pozostaje kwestia znalezienia takiego celu, który ma wystarczająco słabe zabezpieczenie. Dotychczasowe doświadczenia pokazują, że prawdopodobieństwo takiego ataku wcale nie jest małe.

4. Cyberterroryzm wymaga mniejszego treningu fizycznego oraz mniejszego zabezpieczenia logistycznego. Cechuje się ponadto stacjonarnością, tj. dla wykonania ataku nie ma konieczności podróżowania. Przy przeprowadzaniu ataków w cyberprzestrzeni ryzyko poniesienia śmierci lub obrażeń fizycznych przez terrorystów jest znikome. Tym samym wysiłek dla przekonania potencjalnego terrorysty do działań (jego zwerbowania) – znacznie mniejszy.
5. Dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji. Tym samym jeden z zasadniczych celów terrorystów – medialność ataku – jest przeogromna.

BIBLIOGRAFIA

[1] Adkins B., *The spectrum of cyber conflikt from hacking to information warfare: What is law enforcament's role?*, Maxwell AFB, Alabama 2001.

[2] Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003.

[3] Cohen F. B., *Protection and Security on the Information Superhighway*, New York 1995, s. 40 – 54.

[4] Denning D., *Cyberterrorism*, 2000 http://www.cs.georgetown.edu~denning/infosec/cyberterror-GD.doc, stan z dnia 27.03.2004.

[5] Duda D., *Terroryzm islamski*, UJ, Kraków 2002, s. 10.

[6] Garrison L., Grand M., *Cyberterrorism*, 2001, An evolving concept, NIPC highlights, http://www.Nopc.gov./publication/highlight/2001/highlight-01-06.htm, stan z dnia 04.04. 2004.

[7] Kerr K., *Putting cyberterrorism into contex*, AusCERT, 2003.

[8] Lewis J. A., *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002, Center for Strategic amd International Studies, http://www.csis.org/tech/0211lewis.pdf, stan z dnia 27.03.2004.

[9] Pollitt M. M., *Cyberterrorism – Fact or Fancy?*, 2004, http://www.cs.georgetown.edu/~denning/infosechtml/pollitt, stan z dnia 04.04. 2004.

[10] Raczkowski E., *Słownik encyklopedyczny – edukacja obywatelska*, Europa, Warszawa 1999, s. 216.

[11] Rokiciński K., *Wymagania w zakresie współpracy cywilno-wojskowej (CI-MIC) w czasie planowania i przygotowania działań w pasie nadmorskim RP*, II Konferencja „Zarządzanie Kryzysowe", Szczecin 18 czerwca 2004.

ABSTRACT

Alarming news related to cyberterrorism presented in the media are not confirmed in reality. The views of the media result from lack of knowledge of definition of this form of terrorism. Psychology of fear of attacks against information structures stems from the degree contemporary societies depend on information technology and growing threat of terrorist acts. Due to the potential effects it is a tempting form of terrorist activity. The paper presents a few, in the author's view the most representative, classifications of potential attacks in the cyberspace.

Recenzent kmdr por. dr hab. Krzysztof Kubiak