Waldemar Krztoń

Cyberterroryzm jako zagrożenie bezpieczeństwa w społeczeństwie informacyjnym

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 4, 89-100

2012

AUTOR
mgr Waldemar Krztoń

RECENZENT
płk dr hab. Andrzej Polak

CYBERTERRORYZM JAKO ZAGROŻENIE BEZPIECZEŃSTWA W SPOŁECZEŃSTWIE INFORMACYJNYM

W drugiej połowie lat pięćdziesiątych poprzedniego wieku w społeczeństwie Stanów Zjednoczonych zauważono przemiany, powodujące występowanie cech różniących je od klasycznego społeczeństwa przemysłowego. Zmiany te zaszły po zakończeniu II wojny światowej. Przemiany społeczne były wynikiem dokonującego się postępu w obszarze sposobu przetwarzania i przesyłania informacji. W ostatnim dziesięcioleciu dokonała się pełna integracja systemów informatycznych i systemów telekomunikacyjnych oraz ich globalizacja. Za uwieńczenie pół wieku trwających prac uczonych w sferze technologii informacyjnej można uznać narodziny Internetu.

Internet umożliwił niemalże swobodne dojście do potężnych baz informacyjnych na całym świecie. Gwałtownie wzrosła liczba używanych komputerów, sprzętu telekomunikacyjnego i innych urządzeń elektronicznych. Wydaje się, że takie dziedziny jak: edukacja, nauka, przemysł, opieka zdrowotna, administracja państwowa i wojsko nie mogą już efektywnie funkcjonować bez sprzętu teleinformatycznego.

Myślenie o przyszłości na przełomie wieków zdominowały dwa zjawiska. Pierwsze – to globalizacja, obejmująca przede wszystkim trzy podstawowe obszary: gospodarkę, politykę i kulturę. Ważne znaczenie ma także wymiar technologiczny globalizacji, który (związany ze wzrostem dynamiki zmian w komunikacji i informacji) przyniósł zjawisko swoistego kurczenia się czasu i przestrzeni w skali globalnej. Drugim zjawiskiem jest szybki rozwój technologii teleinformatycznych, którego najbardziej spektakularnym wyrazem jest powstanie Internetu i jego lawinowy rozwój. A zatem Internet jest najbardziej dobitnym przykładem globalizacji systemów informacyjnych.

Stanisław Lem powiedział o Internecie, że: *stanowi odpowiedź na pytanie, które jeszcze nie zostało postawione*[1]. Sytuacja, w której informacja stanowi podłoże funkcjonowania, znalazła swoje odzwierciedlenie w strukturze gospodarki, działaniach militarnych oraz realiach życia społecznego.

[1] J. Michniak, *Bezpieczeństwo teleinformatyczne w organizacji*, wykład, studia podyplomowe, WZiD AON, Warszawa 2011.

Wraz z rozwojem intelektualnym i technicznym coraz większego znaczenia zaczęło nabierać społeczeństwo informacyjne. Żyjąc w społeczeństwie informacyjnym, funkcjonujemy w społeczeństwie sieciowym.

Społeczeństwo informacyjne nie ma jednej wykładni interpretacyjnej. W literaturze przedmiotu spotyka się takie terminy, jak: społeczeństwo informacyjne, społeczeństwo wiedzy, społeczeństwo ery internetowej, społeczeństwo sieciowe, społeczeństwo medialne itp. Większa część uczonych używa pojęcia „społeczeństwo informacyjne", podkreślając ważną rolę systemów informacji i komunikacji występujących w kręgu danego społeczeństwa i stanowiących o jego specyfice, w odniesieniu do innych rodzajów społeczeństw. Społeczeństwo informacyjne można określić jako społeczeństwo wiedzy, które zrodziła wiedza naukowa. Sam termin „społeczeństwo informacyjne" pochodzi z Japonii. Jako pierwszy użył go w 1963 roku Tadao Umesamo w artykule na temat ewolucyjnej teorii społeczeństwa opartego na „przemysłach informacyjnych"[2]. Do Europy pojęcie „społeczeństwa informacyjnego" dotarło w 1978 roku. W latach osiemdziesiątych zaczęło funkcjonować powszechnie także w Stanach Zjednoczonych. Profesor Lesław Haber wymienia charakterystyczne desygnaty tego pojęcia[3]:

– *społeczność posiada rozwinięte środki do wytwarzania, przekazywania informacji i komunikacji;*

– *zdecydowana większość społeczeństwa posiada umiejętności w zakresie posługiwania się i wykorzystania technologii informacyjnych, które stanowią podstawę zatrudnienia i utrzymania;*

– *praktyczne wykorzystanie technologii informacyjnej ma znaczący wpływ na kształtowanie się poziomu dochodu narodowego danego państwa;*

– *zakres stosowanych technologii informacyjnych stanowi wskaźnik rozwoju cywilizacyjnego i kulturowego związanego ze zmianami w dotychczasowych systemach aksjologicznych i społecznych wzorcach zachowań.*

Wobec powyższego, wydaje się zasadne przyjęcie propozycji terminologicznej prof. Piotra Sienkiewicza: *Społeczeństwem informacyjnym określamy taki system społeczny, ukształtowany w procesie modernizacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa /dochodu narodowego/ oraz stanowią podstawę orientacji cywilizacyjnej*[4]*.*

W dzisiejszym świecie opanowanym przez elektronikę, niemal we wszystkich sferach naszego życia, musimy polegać na komputerach i informacji, którą one wytwarzają, gromadzą i przesyłają. Wszystkie dziedziny: nauka,

---

[2] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 42.

[3] L.H. Haber, *Poznawcze aspekty badań nad społecznością informacyjną*, [w:] L.H. Haber (red.), *Mikrospołeczność informacyjna na przykładzie miasteczka internetowego Akademii Górniczo-Hutniczej w Krakowie*, Kraków 2001, s. 44.

[4] T. Goban-Klas, P. Sienkiewicz, wyd. cyt., s. 53.

szkolnictwo, obronność, bezpieczeństwo, handel, transport, ochrona zdrowia, finanse itd., coraz bardziej uzależniają się od środków techniki cyfrowej połączonych ze sobą bezpośrednio i pośrednio. Tworzą one współcześnie jedną infrastrukturę, w obrębie której funkcjonuje tzw. cyberprzestrzeń, zawierająca dane i systemy kluczowe dla wielu dziedzin życia.

Działania prowadzące do pozyskania informacji przemysłowych, finansowych, technologicznych oraz wojskowych, stały się jednym z istotnych elementów życia społeczeństwa informacyjnego. W wielu politycznych, biznesowych i militarnych sytuacjach decyzyjnych mamy do czynienia z asymetrią informacji, (uczestniczą w nich zarówno „dobrze poinformowani", jak i „niepoinformowani"). Globalizacja nie likwiduje, lecz raczej pogłębia zjawisko asymetrii w dostępie do różnych dóbr, także zasobów informacji i wiedzy. Internet nie służy przecież tylko wspomaganiu naszych działań, zaspakajaniu potrzeb informacji i wiedzy. Równolegle z tymi korzyściami pojawiła się groźna strona tej techniki informacyjnej, między innymi cyberterroryzm. Znaczna część internautów podejmuje działania, które trudno uznać za racjonalne, przeciwnie raczej za wręcz niegodziwe.

Wyraźne są też konsekwencje przeobrażania się Internetu dla bezpieczeństwa narodowego i międzynarodowego. Należy pamiętać o tym, że pierwsza sieć komputerowa Arpanet (1969) powstała w ramach programu realizowanego na zlecenie Departamentu Obrony USA. O pierwszej wojnie w Zatoce (1991) pisano, że była to „wojna informacyjna". Niedługo potem pojawiły się pojęcia, takie jak: „wojna cybernetyczna", „wojna sieciowa".

Bezpieczeństwo telekomunikacyjne i teleinformatyczne powinno być najczęściej rozwijane w takich obszarach gospodarki, w których istnieje konieczność wykorzystywania przewagi informacyjnej oraz ochrony jej treści. Znawcy przedmiotu twierdzą, że zasadniczym warunkiem osiągnięcia sukcesu gospodarczego czy militarnego jest dominacja informacyjna. Prowadzone w ostatnich latach działania o charakterze militarnym czy biznesowym potwierdzają prawdziwości powyższej tezy. Przewidywania i wnioski z analizy doświadczeń zmobilizowały specjalistów z dziedziny techniki do poszukiwania nowych efektywnych środków oddziaływania i ochrony infrastruktury informacyjnej (w szczególności systemów informatycznych) państwa, sił zbrojnych, organizacji i firm.

Minęły czasy, kiedy włamania do systemów komputerowych z wykorzystaniem sieci Internet były w dużej mierze rywalizacją pomiędzy hackerami, a administratorami serwerów. Problem zagrożeń związanych z siecią Internet oraz rozwojem e-gospodarki ma duże znaczenie dla bezpieczeństwa finansowego i konkurencyjności firm. Przypadki ataków na powszechnie wykorzystywane serwery państw wysoko rozwiniętych wskazują, że zagrożenia te mogą mieć również znaczenie dla ogólnie rozumianego bezpieczeństwa narodowego. Powszechność sieci powoduje z jednej strony, iż wzrost potencjalnych przeciwników (włamywaczy) jest bardzo duży, a z drugiej strony

większość ludzi wykorzystujących sieć w swojej pracy z konieczności może posiadać tylko fragmentaryczną wiedzę na temat jej bezpieczeństwa i potencjalnych zagrożeń. Zagrożenia związane z siecią Internet można podzielić w następujący sposób[5]:

– *blokowanie dostępu do systemów firmy,*

– *włamania do systemu,*

– *niszczenie lub destabilizacja systemu.*

Różne techniki i sposoby pozwalające obejść zabezpieczenia i ewentualne luki w polityce bezpieczeństwa wykorzystywane są do ataków na systemy komputerowe przy użyciu Internetu. Najczęściej wykorzystywane techniki ataków według profesora Józefa Michniaka to[6]:

– ***skanowanie*** *– działania mające na celu poznanie konfiguracji i rodzaju zabezpieczeń atakowanego systemu;*

– ***sniffing*** *– czyli podsłuchiwanie sieci, jest to najprostszy sposób zdobycia informacji umożliwiających wykonywanie dalszych operacji, większość niezbędnych danych jest przekazywana w sposób niezaszyfrowany;*

– ***spoofing*** *– podszywanie się pod innego nadawcę, wykorzystuje się techniki polegające na zmianie nagłówków przesyłanych pakietów. Ten sposób jest wykorzystywany między innymi do oszukania systemu firewall, przejęcia uwierzytelnionego, połączenia do atakowanego systemu (ispoofing;);*

– ***exploity*** *– wykorzystywanie istniejących błędów w systemie operacyjnym atakowanego komputera – najczęściej przepełnienie bufora;*

– ***DoS*** *– czyli Denial of Service – blokowanie atakowanego systemu lub poszczególnych usług, nie powoduje bezpośrednich strat w systemie komputerowym, ale uniemożliwia jego poprawną pracę;*

– ***konie trojańskie*** *– programy instalowane/uruchamiane świadomie lub nieświadomie przez użytkowników systemu, po uruchomieniu wykonują działania skierowane przeciwko systemowi, najczęściej przekazują na zewnątrz poufne informacje z zaatakowanego komputera lub umożliwiają bezpośrednie przejęcie nad nim kontroli;*

– ***wirusy*** *– programy wyposażone w umiejętność samodzielnego replikowania oraz rozprzestrzeniania się, niszczące lub uszkadzające oprogramowanie zaatakowanego systemu, zagrożenie wirusami wzrosło szczególnie wraz z upowszechnieniem się poczty elektronicznej.*

Wraz z postępem technologicznym zwiększała się rozmaitość dostępnych środków konfliktu. Zaawansowane technologicznie środki walki zaczęły odgrywać coraz większą rolę. Inteligentna broń, umożliwiająca dokonywanie precyzyjnych uderzeń niemal bez strat własnych, a ze znacznymi stratami dla przeciwnika. W dobie konfliktów, w których stroną może stać się organizacja pozbawiona podmiotowości prawno-międzynarodowej, niepo-

[5] J. Michniak, wyd. cyt.

[6] Tamże.

siadająca stałego terytorium ani nawet jasno określonej bazy działania, siły ochrony i bezpieczeństwa muszą przybierać postać pozwalającą na elastyczne reagowanie, z dużą precyzją, na pojawiające się nagle zagrożenia ze strony różnych grup. Poza podmiotami państwowymi mamy do czynienia z podmiotami niepaństwowymi, takimi jak: międzynarodowe koncerny, transnarodowe korporacje wpływające na działania rządów czy grupy nielegalne, w tym zorganizowane grupy przestępcze i organizacje terrorystyczne. Brak określonego terytorium, mobilność celów oraz anonimowość użytkownika na cybernetycznym polu walki, znacznie ogranicza możliwość skutecznego powstrzymania i ochrony.

Rozważania dotyczące cyberterroryzmu warto rozpocząć od podjęcia próby zdefiniowania tego pojęcia. Nie jest to zadanie proste, bowiem mimo wielu prób definiowania nie został powszechnie akceptowany aparat pojęciowy w obszarze walki informacyjnej. Według niektórych koncepcji pojęcie cyberwojny zostało stworzone przez siły zbrojne dla określenia kolejnego, wirtualnego tym razem pola walki. Cyberprzestrzeń, jako zjawisko tworzone przez człowieka, jest jednak płynna i trudna do jednoznacznego zdefiniowania. Określenie cyberprzestrzeń, użyte w 1984 roku przez Williama Gibsona (w powieści science fiction Neuromancer), weszło do powszechnego obiegu na początku lat dziewięćdziesiątych. Według G. Rattray cyberprzestrzeń składa się ze: *sprzętu elektronicznego, sieci, systemów operacyjnych i standardów przesyłania*[7]*.*

Po raz pierwszy pojęcie cyberterroryzm pojawiło się w raporcie o zagrożeniach komputerowych w Szwecji (w 1979 r.): *Obejmował on wszelką działalność z użyciem komputerów, mającą na celu niszczenie systemów teleinformatycznych, systemów nadzoru i kontroli, programów, danych itp., a w konsekwencji zastraszanie rządów i społeczeństw, wywieranie presji psychologicznej, doprowadzenie do zagrożenia życia lub powstania znacznych strat materialnych*[8]*.* Jednakże powszechnie za twórcę pojęcia cyberterroryzmu uznaje się pracownika służb wywiadowczych Stanów Zjednoczonych B. Collina, który w latach osiemdziesiątych ubiegłego wieku użył go dla określenia połączenia cyberprzestrzeni i terroryzmu, ciągle jeszcze jako zjawiska czysto teoretycznego. Połączenie aspektu konwencjonalnego i cybernetycznego daje następującą definicję cyberterroryzmu: *to zdeterminowane i świadome użycie środków walki informacyjnej przez aktorów niepaństwowych lub grupy sponsorowane przez państwa, motywowane politycznie, społecznie, ekonomicznie lub religijnie, w celu zastraszania, wzbudzania*

[7] G.J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004, s. 80.

[8] P. Sienkiewicz, *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym*, [w:] A. Siwik (red.), *Od społeczeństwa industrialnego do społeczeństwa informacyjnego: Księga jubileuszowa dedykowana Profesorowi Lesławowi H. Haberowi w 40-lecie pracy naukowej i dydaktycznej*, Uczelniane Wyd. Naukowo-Dydaktyczne AGH, Kraków 2007, s. 303.

niepokoju i paniki wśród atakowanej ludności oraz doprowadzenia do zniszczenia wojskowych i cywilnych celów[9].

Najprostsze podejście do pojęcia cyberterroryzmu można podać w postaci pozbawionej kontekstu historyczno-środowiskowego definicji: ***cyberterroryzm to połączenie cyberprzestrzeni z terroryzmem***[10]. Podstawą do definiowania terminu cyberterroryzmu jest angielskie pojęcie – *information warfare* – (walka informacyjna), rozumiana: *jako defensywne i ofensywne użycie informacji i systemów informacyjnych do przerwania lub zniszczenia systemów informacyjnych przeciwnika, jego baz danych oraz sieci komputerowych*[11]. Według amerykańskich ekspertów, *cyberterroryzm jest to bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zastraszenia lub wymuszenia na rządzie lub ludziach daleko idących politycznych i społecznych celów*[12].

Profesor Piotr Sienkiewicz twierdzi, że: *cyberterroryzm w wąskim znaczeniu – to działalność terrorystyczna w systemach teleinformatycznych, ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, skutkująca ofiarami śmiertelnymi lub zniszczeniem mienia w znacznych rozmiarach (zazwyczaj celem jest jedno i drugie). W szerszym znaczeniu – jest to wszelka działalność terrorystyczna związana z cyberprzestrzenią (systemami teleinformatycznymi), włączając w to fizyczne ataki na systemy oraz aktywność propagandową. Działalność taka może na przykład przyczynić się do pozyskiwania informacji przydatnych do realizacji bardziej klasycznych akcji terrorystycznych, na przykład zamachów bombowych*[13].

Rozumiejąc cyberterroryzm jako: *politycznie motywowany atak lub groźbę ataku na komputery, sieci, lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów*[14], możemy wyróżnić dwa rodzaje akcji cyberterrorystycznych:

- szkodliwe poczynania informacyjne w cyberprzestrzeni;
- ataki fizyczne na systemy informacyjne.

Powyższe działania mogą się naturalnie razem uzupełniać. Możliwe, że w bliskiej perspektywie możemy być obserwatorami zsynchronizowanego ataku polegającego na cybernetycznym unieruchomieniu sieci teleinformatycznej i równoczesnym wykorzystaniu np. materiałów wybuchowych. Ugrupowania terrorystyczne bardzo dobrze zdają sobie sprawę z wartości

[9] Tamże, s. 303.

[10] L. Wolaniuk, *Cyberterroryzm jako element cywilizacji informacyjnej*, [w:] M. Żuber (red.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i reagowanie kryzysowe*, Wrocław 2006, s. 157.

[11] M. Gałązka, *Zasady prowadzenia walki informacyjnej*, Bellona nr 1, 2007, s. 73–76.

[12] D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

[13] P. Sienkiewicz, wyd. cyt., s. 305.

[14] A. Bogdół-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 73.

zasobów informacyjnych w dzisiejszym świecie, przewidując, że działania obezwładniające infrastrukturę informacyjną spowodują większy efekt niż zwykły akt terrorystyczny.

Cyberterroryzm jest pojęciem, które w Polsce pojawiło się stosunkowo niedawno. Trzeba zaznaczyć, że w krajach o wysokim stopniu rozwoju informatycznego i technologicznego niebezpieczeństwo to jest traktowane priorytetowo. Na przykład w Stanach Zjednoczonych CIA w 1996 r. uznała cyberterroryzm za drugie największe zagrożenie dla amerykańskiego bezpieczeństwa narodowego.

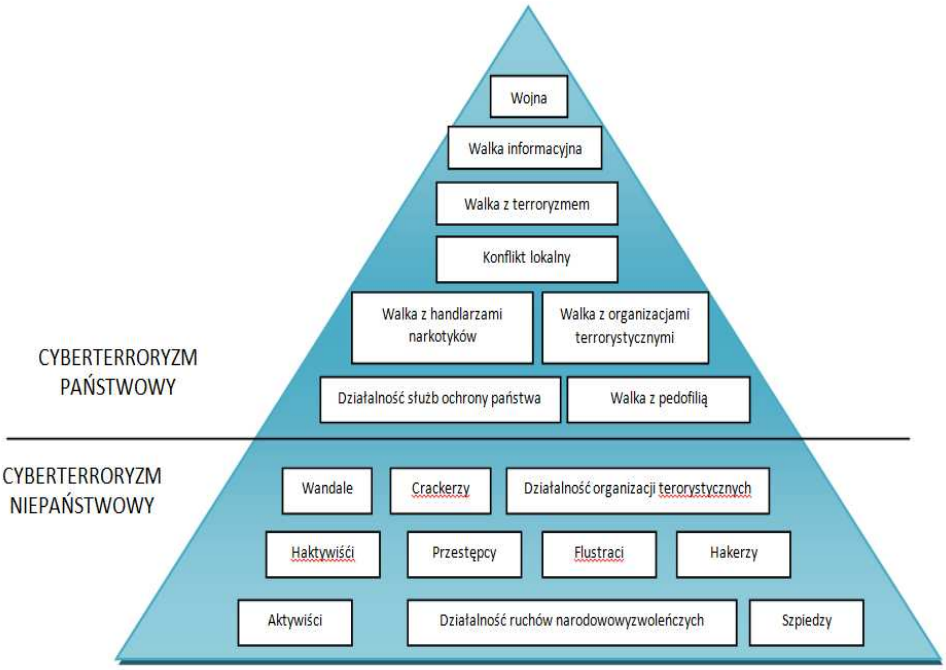
Rozwój zagrożeń niemilitarnych jest zapewne efektem wielorakich przeobrażeń, które dokonały się w świecie w rezultacie procesów globalizacyjnych. Procesy te spowodowały powstanie środowiska bardzo korzystnego dla podmiotów stanowiących zagrożenia asymetryczne. W rezultacie tego grupy niepaństwowe osiągnęły spore zdolności wpływania na sytuację na świecie, a przede wszystkim na stan bezpieczeństwa państw i społeczeństw.

Zagrożenia bezpieczeństwa w społeczeństwie informacyjnym rozpatrywane są w aspekcie zdolności użycia technologii informacyjnych przez środowiska niezadowolenia obywatelskiego, organizacje terrorystyczne, a także oddziaływania środków masowego przekazu na postrzeganie wydarzeń na świecie, w tym przebiegu konfliktów zbrojnych. Niejako równolegle do nowych koncepcji walki zbrojnej postępował proces coraz silniejszego uzależniania się od technologii teleinformatycznych we wszystkich niemal sferach życia społecznego, co niewątpliwie wpływało stymulująco na ich efektywność. Jednakże wraz z pojawieniem się nowych zagrożeń w postaci przestępstw komputerowych istotnym problemem stał się wzrost podatności na zagrożenia informacyjne poszczególnych podsystemów „krytycznej infrastruktury państwa".

W wysoko rozwiniętych społeczeństwach ataki cyberprzestępców stają się szczególnie efektywne, ponieważ cechuje je duża koncentracja urządzeń elektronicznych. W przypadku ataku uszkodzone zostaną nie tylko elementy infrastruktury militarnej, ale również te, które zgodnie z obowiązującymi konwencjami międzynarodowymi podlegają szczególnej ochronie (np. system opieki medycznej). Dobre rozpoznanie potencjalnych zagrożeń jest warunkiem właściwego przygotowania się do zwalczania lub minimalizacji ich negatywnych skutków. Mogą być one dziełem wielu wielce zróżnicowanych podmiotów (np. państwowych lub niepaństwowych).

Każde państwo może być zagrożone atakiem cyberterrorystów ze szkodami tym większymi, im bardzkiej skomputeryzowana jest gospodarka. Z drugiej strony każde państwo może dokonać ataku cybernetycznego, jeżeli tylko znajdą się w nim profesjonalni hakerzy, zdolni i gotowi do jego przeprowadzenia. Po wydarzeniach z 11 września 2001 r. zwrócono uwagę na możliwość podobnych ataków terrorystycznych na całym świecie, w tym

na możliwe i prawdopodobne zmasowane cyberataki na systemy teleinformatyczne USA i sprzymierzeńców, wykorzystywane w walce ze światowym terroryzmem. Wówczas w amerykańskiej ustawie antyterrorystycznej rozszerzono definicję terroru o cyberterroryzm.



Źródło: P. Sienkiewicz, *Bezpieczeństwo…*, wyd. cyt., s. 303.

Rys. 1. Cyberterroryzm państwowy i niepaństwowy

Ze względu na specyfikę cyberprzestrzeni zjawisko cyberterroryzmu trzeba rozpatrywać, jako:

– klasyczny zamach terrorystyczny;
– sposób propagandy i dezinformacji.

Działalność w sieciach teleinformatycznych ułatwia grupom terrorystycznym:

– działalność terrorystyczną *sensu stricte*;
– przesyłanie informacji oraz w miarę niezagrożone komunikowanie się;
– działalność informacyjno-propagandową i zdobywanie rozgłosu;
– penetrację stron www, pozyskiwanie informacji z różnych obszarów;
– zdobywanie środków finansowych – kradzież pieniędzy z kont i kart kredytowych, fingowanie przelewów elektronicznych czy wymuszeń na bankach, do których te banki się nie przyznają.

Internet stał się pozbawionym granic podmiotem trudnym do zlokalizowania dzięki sprawności i szybkości zacierania śladów działań w sieci. Można wymienić wiele powodów przemawiających za wykorzystaniem cyberterroryzmu dla osiągnięcia określonych celów[15]:

– *niskie koszty takiej działalności, zwłaszcza w porównaniu z kosztami regularnych działań zbrojnych (do ataku cyberterrorystycznego wystarczy przeciętny sprzęt komputerowy, dostęp do Internetu i trochę umiejętności);*

– *zanikanie wszelkich granic – państwa tracą część swojej suwerenności – zacierają się granice między tym co prywatne a państwowe, wojskowe a komercyjne itd.; konsekwencją zanikania wszelkich barier jest prawdopodobieństwo, że zaatakowane państwo nie będzie sobie z tego zdawało sprawy (zacieranie się granic między wojną a pokojem);*

– *możliwość dokonania nagłych i nieprzewidzianych akcji – ofiary są, całkowicie nieświadome i nieprzygotowane do ich odparcia;*

– *całkowita anonimowość – powoduje to możliwość manipulowania informacją, utrudnia państwom odparcie ataku i budowanie koalicji;*

– *minimalne ryzyko wykrycia przygotowywanego ataku;*

– *zamiast uderzać w niewinnych ludzi można sparaliżować system wrogiego państwa (większy efekt propagandowy i uznanie opinii publicznej).*

Postępujący proces ogólnoświatowej informatyzacji i rosnące uzależnienie wszystkich dziedzin życia od systemów informatycznych i informacyjnych spowoduje rozszerzenie spektrum zagrożeń informatycznych. Szereg krajów oraz organizacji, a także ugrupowań terrorystycznych, prowadzi działania zawierające elementy walki informacyjnej. Ocenia się, że liczne organizacje i ugrupowania, nie rezygnując z konwencjonalnych form oddziaływania, coraz częściej będą prowadziły ataki techno- i cyberterrorystyczne oraz operacje psychologiczne na szeroką skalę. Nie zastąpią one konwencjonalnego zagrożenia, będą jednakże stanowiły jego istotne uzupełnienie.

W państwach zindustrializowanych będzie rosnąć liczba funkcji realizowanych zarówno przez państwo, jak i instytucje niepaństwowe, z wykorzystaniem technologii informatycznych. *Spotęguje to zagrożenie związane z nielegalnym dostępem do eksploatowanych systemów i zasobów informatycznych. Głównym obiektem ataków przeprowadzanych przez grupy techno-terrorystyczne będzie prawdopodobnie infrastruktura cywilna obejmująca kluczowe instalacje sieci energetycznych, wodociągowych i telekomunikacyjnych. Jej zniszczenie lub czasowe uszkodzenie może dezorganizować pracę sektora publicznego i mediów oficjalnych*[16].

Atakiem cyberterrorystycznym szczególnie zagrożone będą kluczowe systemy informatyczne i bazy danych instytucji państwowych, wojskowych,

[15] P. Sienkiewicz, wyd. cyt., s. 304.
[16] J. Michniak, wyd. cyt.

finansowych, służby publicznej oraz mediów państwowych. *Pożądany efekt takich ataków może obejmować całkowity paraliż zaatakowanych systemów informatycznych i sieci, okresowe ich wyłączanie, powodowanie błędów w danych, wykradanie informacji, wykradanie usług, dostęp do danych oraz wprowadzanie fałszywych informacji. Ponadto atakujący mogliby próbować wstawiać spreparowane elementy do infrastruktury informacyjnej przeciwnika, co umożliwiłoby im monitorowanie, zakłócanie lub niszczenie jego systemów i sieci*[17]. Powyższe działania będą prowadzone zarówno przez istniejące organizacje terrorystyczne, wspomagane przez państwa sponsorujące terroryzm, jak i szereg nowych ugrupowań, niewielkich liczebnie, lecz o charakterze globalnym (mających członków na całym świecie), prowadzących działalność z pobudek politycznych, rasowych, religijnych, ekologicznych i innych. Wśród nich można wyróżnić[18]:

– *fanatyków religijnych (np. islamskich);*

– *ortodoksyjnych działaczy New Age (np. organizacji na rzecz prawa zwierząt, antyglobalistów); posiadają bardzo dobrze, merytorycznie przygotowanych do roli cyberterrorystów członków organizacji; wydaje się, że rozpowszechniane przez nich poglądy raczej nie pozwalają na stosowanie cyberterroryzmu z ofiarami w ludziach;*

– *etniczno-narodowościowych separatystów i rewolucjonistów; bardzo groźna grupa o różnym przygotowaniu specjalistycznym i raczej nieposiadająca obiekcji w stosunku do obiektów ataku;*

– *innego typu ekstremistów, którzy w miarę rozwoju sytuacji na świecie i postępu cywilizacyjnego, mogą się pojawić; właściwie ta grupa może być najgroźniejsza, ponieważ stanowi jeszcze nieokreślone zagrożenie (aż do dnia kiedy zaatakuje) i element przyszłości cywilizacji informacyjnej ze swoimi członkami, ludźmi obytymi z techniką komputerową.*

Cyberterroryzm jest jednym ze środków stosowanych przez organizacje terrorystyczne do ograniczania tradycyjnej roli państwa. Ataki cyberterrorystów mogą być ukierunkowane na informacje stanowiące najbardziej newralgiczne znaczenie dla funkcjonowania państwa. Celem cyberterrorystów staje się opanowanie głównych sektorów, zaś w dalszej kolejności monopolizacja dostępu do informacji. Cyberterroryści analogicznie jak media, manipulują informacjami, a także wykorzystują Internet do przedstawiania swoich poglądów oraz idei terrorystycznych. Profesor Brunon Hołyst uważa, że w walce z cyberterroryzmem powinno przestrzegać się poniższych zaleceń[19]:

– *należy monitorować zmiany w wykorzystaniu IT przez grupy terrorystyczne* (…)*. Najbardziej znaczące trendy, wymagające ścisłej kontroli, to*

[17] G.J. Rattray, wyd. cyt., s. 31.
[18] L. Wolaniuk, wyd. cyt., s. 160.
[19] www.zabezpieczenia.com.pl/ochrona-informacji/cyberterroryzm [dostępne: 03.09.2012].

powstanie nowych, potencjalnie niebezpiecznych grup terrorystycznych, wysoce zinformatyzowanych pod względem organizacyjnym i ofensywnym. Należy zidentyfikować te grupy i śledzić je;

– należy śledzić przepływ informacji w internetowych grupach terrorystycznych. Priorytetem powinno być przechwytywanie wymiany informacji dokonywanej przez terrorystów. Nie można też lekceważyć zbierania informacji wywiadowczych drogą nieelektroniczną;

– należy utrudniać oparte na IT ofensywne operacje informacyjne (przez oddziaływanie na informacje przeciwnika oraz obronę własnych) terrorystów poprzez lepszą ochronę infrastruktury. (…) *Agencje kontr terrorystyczne powinny też rozważyć opcje zatrudnienia większej liczby hakerów i wykorzystywać ich wiedzę w celach defensywnych, a także odwetowych;*

– należy pokonać terrorystów sieciowych ich własnym sposobem: chodzi o użycie sieci do walki z sieciami.

Atak cyberterrorystyczny to każde działanie wymierzone w systemy informacyjne, bez względu na to, czy jest on dokonany za pomocą komputera, czy też nie. Cyberterroryzm rozumiany jest najczęściej, jako działania mające na celu niszczenie bądź zniekształcanie informacji przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych. Najkrócej można to ująć jako działania terrorystyczne w przestrzeni cybernetycznej. Należy zaszczepić w powszechnej świadomości ludzi znaczenie informacji komputerowej, jako czynnika decydującego o istnieniu wszystkiego co ich otacza. Powinno się zmienić sytuacje, w której na etapie edukacji komputerowej uczy się posługiwania narzędziami informatycznymi, pomijając przy tym zupełnie kwestie bezpieczeństwa.

Współczesne myślenie o pokoju i bezpieczeństwie narodowym musi obejmować analizy systemowe zjawiska wojny cybernetycznej oraz związane z nimi zagrożenia i szanse bezpieczeństwa rozwoju. Bezpieczeństwo informacyjne jest trwałym elementem bezpieczeństwa narodowego (międzynarodowego).

CYBERTERRORISM AS A THREAT TO SECURITY IN INFORMATION SOCIETY

Abstract: At the turn of the century two phenomena dominated the thinking of the future. The first one – globalization includes mainly three essential areas as economy, politics and culture. The second phenomenon is a tremendous teleinformation technology progress, spectacularly expressed by the Internet and its rapid development. Information society is gaining more and more importance along with the intellectual and cultural development. Living in information society, we are functioning in a network

society. Globalization does not eradicate but deepens the phenomenon of asymmetry in accessing various goods and information resources. The Internet does not serve only to support our activities, fulfilling our needs, knowledge and wisdom. Parallel to its advantages, a dangerous side of information technology has appeared such as cyberterrorism.