Wiesław Smolski
Niepaństwowa Wyższa Szkoła Pedagogiczna w Białymstoku

Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa

1. Wprowadzenie do problematyki cyberterroryzmu

Na początku należałoby się zastanowić, co to jest cyberterroryzm. Specjaliści zajmujący się cyberterroryzmem wskazują na trudności w zdefiniowaniu tego pojęcia. Trudno stwierdzić, które działania można określić mianem cyberterroryzmu, a które nie.

Za twórcę tego pojęcia uznaje się Barry'ego Collina, pracownika *Institute for Security and Intelligence* z Kalifornii, który w latach 80. użył go dla określenia połączenia cyberprzestrzeni i terroryzmu[1]. Według B. Collina, cyberterroryzm to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji[2].

D. Denning podaje definicję zawężającą, a w szczególności stwierdza, że 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[3]. Uzupełniając swoją definicję, dodaje, iż za atak cyberterrorystyczny można uznać tylko taki akt, który powoduje bezpośrednie szkody człowiekowi i jego mieniu lub przynajmniej jest na tyle znaczący, że budzi strach.

Natomiast Robert Kośla definiuje cyberterroryzm jako działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy[4].

Według R. Kośli, w pojęciu tym mieści się także wykorzystywanie systemów teleinformatycznych do dezinformacji, walki psychologicznej itp. Celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki.

Cyberterroryzm, jako specyficzna kategoria zagrożeń, obejmuje działania w stosunku do systemów teleinformatycznych, podejmowane, by osiągnąć konkretne cele terrorystyczne.

---

1 D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 79

2 K. C. White, *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998, s. 10.

3 D. E. Denning, *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, Washington, 23 maja 2000.

4 *R. Kośla, Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski. Wystąpienie na konferencji w Bemowie*, 29 listopada 2002.

Typy cyberterroryzmu wyróżniamy w oparciu o kryterium podmiotowe i przedmiotowe[5]. Stosując pierwsze z nich, mówimy o cyberterrorystach i ich ofiarach, czyli o podmiotach działań i podmiotach ataku. W kontekście stosunków międzynarodowych podmioty ataku stanowią uczestnicy państwowi i niepaństwowi. Wśród podmiotów działań możemy wyróżnić grupy zorganizowane i cyberterrorystów indywidualnych. Wśród grup zorganizowanych istnieją zarówno klasyczne organizacje terrorystyczne jak Tamilskie Tygrysy, *Hezbollah* czy *Al-kaida*, które oprócz środków konwencjonalnych wykorzystują w swoich działaniach zarówno cyberprzestrzeń, jak i grupy terrorystyczne, składające się z hakerów komputerowych działających w zasadzie wyłącznie w cyberprzestrzeni. Jeśli chodzi o cyberterrorystów indywidualnych, to istnieje około kilku tysięcy osób, które można określić mianem profesjonalnych hakerów. Są to ludzie posiadający ściśle określone kwalifikacje, którzy dokładnie wiedzą, co robią. Są to osoby, które za odpowiednią opłatą mogą zrobić wszystko, mogą więc wykonywać zadania o charakterze politycznym, zlecone przez organizacje terrorystyczne. Kryterium przedmiotowe dotyczy skutków ataków cyberterrorystycznych. Posiadają one aspekt militarny, gospodarczy i polityczny. Przykładem skutków militarnych jest działalność hakerów komputerowych wynajętych przez władze chińskie, którzy wykradli tajne informacje z laboratorium badań nad bronią nuklearną w Los Alamos w Nowym Meksyku. Fakt ten miał miejsce pod koniec lat 90. ubiegłego stulecia a był utrzymywany w tajemnicy do 2000 roku. Dochodzenie przeprowadzone w tej sprawie ujawniło, że Chiny uzyskały informacje o „każdej amerykańskiej głowicy nuklearnej".

2. Obszary zagrożeń cyberterrorystycznych

W przypadku podziału na obszar zagrożeń cyberterrorystycznych mamy do czynienia z atakami na[6]:

- **systemy wojskowe,** które przechowują informacje o położeniu satelitów, rozmieszczeniu wojsk oraz broni, prowadzących badania nad nowymi rodzajami broni, systemami łączności itp. Najwięcej włamań tego rodzaju zanotowano podczas trwania zimnej wojny, a głównymi sprawcami byli z reguły agenci innych wywiadów;
- **systemy przedsiębiorstw,** które przechowują informacje ważne z punktu widzenia działalności firmy, np.: informacje o rezerwacjach, o klientach, o wykorzystywanych technologiach itp. Głównymi sprawcami byli i nadal są najczęściej

[5] P. Maj, *Cyberterroryzm w stosunkach międzynarodowych*, „Consensus. Studenckie Zeszyty Naukowe" 2001, nr 1.

[6] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, AON, Warszawa 2002.

pracownicy (lub byli pracownicy), którzy współpracują z konkurencją lub też pałają chęcią zemsty za słabe wynagrodzenie itp.;

– **systemy wchodzące w skład tzw. „infrastruktury krytycznej państwa",** czyli systemy: bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, służb do działań w sytuacjach wyjątkowych, które przechowują informacje ważne dla bezpieczeństwa państwa. Sprawcami tych ataków mogą być zarówno pracownicy firm związanych z ww. systemami oraz – co nie jest nieuniknione – terroryści.

W kontekście dalszych rozważań warto przeanalizować poglądy Stanów Zjednoczonych, według których prawdopodobieństwo ataku cyberterrorystycznego jest pierwszym krokiem do podjęcia niezbędnych działań, służących zapobieżeniu temu zagrożeniu. Następnym krokiem jest zdefiniowanie potencjalnych celów, które cyberterroryści mogliby zaatakować w pierwszej kolejności.

W pierwszym raporcie z września 1997 roku zdefiniowali oni pojęcie „infrastruktury krytycznej" (*critical infrastructure*), której zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo ekonomiczne państwa. Określili także osiem głównych elementów tej infrastruktury[7]:

– **telekomunikacja** (*Telecommunication*) – linie telefoniczne, satelity, sieci komputerowe – komercyjne, wojskowe, akademickie itd.;
– **system energetyczny** (*Electrical Power System*) – produkcja, przesyłanie i dystrybucja energii, a także transport i magazynowanie surowców niezbędnych do jej produkcji;
– **produkcja, magazynowanie i transport gazu ziemnego i ropy naftowej** (*Oil and Gas Delivery and Storage*) – cały proces wydobycia ropy naftowej i gazu ziemnego, magazynowania, przetworzenia i transportu za pomocą rurociągów, statków, transportem kołowym i kolejowym (także dostarczanie paliwa do zamorskich baz wojskowych USA);
– **system bankowy i finansowy** (*Banking and Finance*) – system przepływu bilionów dolarów, poczynając od indywidualnych depozytów po transfer ogromnych sum pieniędzy z jednego krańca świata na drugi. Obejmuje wszystkie dostępne instrumenty operacji finansowych;
– **transport** (*Transportation*) – transport lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz cały system wsparcia logistycznego;
– **system zaopatrzenia w wodę** (*Water Supply System*) – składają się na niego: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania

[7] A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Warszawa 2003.

wody, dostarczania dla rolnictwa, przemysłu, straży pożarnych oraz indywidualnych odbiorców;
- **służby ratownicze** (*Emergency Service*) – w Stanach Zjednoczonych system alarmowy 911: komunikacja z policją, służbą zdrowia, strażą pożarną itd.;
- **ciągłość funkcjonowania władzy i służb publicznych** (*Continuity of Government Services*) – wszystkie te elementy, które zapewniają funkcjonowanie lokalnych, regionalnych i centralnych władz oraz systemu publicznego: służba zdrowia, bezpieczeństwo, obrona itd.

W Polsce pierwsze prace zmierzające do ochrony krytycznej infrastruktury teleinformatycznej państwa rozpoczęły się pod koniec XX wieku. W 1996 roku powstał *Computer Emergency Response Team* Polska (*CERT* Polska), który w ramach instytutu badawczego Naukowej i Akademickiej

Sieci Komputerowej (NASK) zajął się bezpieczeństwem teleinformatycznym. *CERT*, czyli zespół do spraw reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego, to nazwa, pod którą w większości krajów Unii Europejskiej, Szwajcarii oraz w USA funkcjonują jednostki powołane do zwalczania incydentów komputerowych. Są to zazwyczaj ośrodki działające przy uczelniach technicznych lub firmach informatycznych.

W 2008 roku powołano zespół reagowania na incydenty komputerowe – *CERT. GOV.* Jest on częścią Agencji Bezpieczeństwa Wewnętrznego (ABW) – Departamentu Bezpieczeństwa Teleinformatycznego i ma wszystkie uprawnienia właściwe tym służbom. W Departamencie Informatyki i Telekomunikacji MON powstał natomiast *MIL-CERT* dla sił zbrojnych. Żadna z polskich instytucji rządowych nie jest jednak w stanie samodzielnie bronić się przed atakami hakerów, dlatego *CERT* Polska we współpracy z Departamentem Bezpieczeństwa Teleinformatycznego ABW stworzył system wczesnego ostrzegania o zagrożeniach internetowych o nazwie *ARAKIS*. Zawiadamia on o próbach rozprzestrzeniania się robaków sieciowych, bonetów, skanowaniach danych z zewnątrz oraz infekcjach komputerów wewnątrz chronionej sieci. Jego zadaniem jest wykrywanie zagrożeń, które mogą wskazywać na atak, a nawet na przygotowania do niego.

Z raportów przygotowanych przez Federalne Biuro Śledcze dla Departamentu Obrony wynika, że „internauci" z Arabii Saudyjskiej, Indonezji i Pakistanu wielokrotnie sprawdzali systemy amerykańskich zabezpieczeń sieci telefonicznych, systemu alarmowego 911, sieci energetycznej, wodociągów, gazociągów i elektrowni atomowej. W jednym z komputerów skonfiskowanych w Afganistanie, należących do członka *Al-Kaidy*, znaleziono „Podręcznik Sabotażu", ściągnięty ze stron *Societe Anonyme*. Na stronach islamskich chatów, powiązanych z organizacją byłego przywódcy Osamy Bin Ladena,

znaleziono narzędzia służące skanowaniu komputerów w celu znalezienia dziur w systemach zabezpieczeń. Powyższe potwierdza, że atak cyberterrorystyczny na infrastrukturę krytyczną jest w polu zainteresowania organizacji terrorystycznych, a w szczególności *Al-Kaidy*.

3. Wybrane przykłady działalność organizacji terrorystycznych w cyberprzestrzeni

Aby znaleźć hakerów pracujących lub działających na rzecz organizacji terrorystycznych typu *Al-Kaida,* należy przyjrzeć się krajom finansującym terroryzm, takim jak Iran i Syria oraz innym państwom sponsorom, jak pakistański wywiad wojskowy ISI (*Inter – Services Intelligence*), można ich znaleźć w setkach madras, szkół religijnych, w których młodzi chłopcy otrzymują tyle samo wiedzy technicznej, co nienawiści do Zachodu. Na dodatek istnieje wiele dowodów działalności hakerów wśród wciąż rosnącej rzeszy bezrobotnych rosyjskich naukowców mających przeszkolenie i doświadczenie wywiadowcze, a także wśród zorganizowanych grup przestępczych Rosji, Malezji, Chin, Japonii, Kolumbii i Meksyku. Wiele ludzi nie rozumie istoty cyberterroryzmu, ponieważ wędrując po Internecie nie znaleźli się sami pod gradem ,,zer i jedynek" wycelowanych w ich komputer, ale właśnie na tym polega fundamentalne niezrozumienie istoty zjawiska. W cyberterroryzmie głównym celem jest niszczenie gospodarki wrogiego narodu, zaś śmierć i strach stanowią pożądany dodatek, który cyberterrorystom udaje się uzyskać przy okazji.

Od początku lat 90. *Al-Kaida* do wsparcia swych działań terrorystycznych stosuje wszystkie dostępne nowoczesne technologie. Ostatnio wysiłki organizacji skupiły się na użyciu zaawansowanych technologii informatycznych jako narzędzia do poznawania słabych punktów celów, na przykład inżynierskich niedociągnięć w konstrukcji mostów, tam, elektrowni i różnego rodzaju budynków. Ta ewolucja wskazuje, że w przyszłości należy się obawiać planów bardziej bezpośredniego wykorzystania Internetu jako broni ofensywnej.

Amerykańska wojna z terroryzmem po atakach z 11 września 2001r. na wiele sposobów przyczyniła się do szybkiego przejmowania przez organizacje terrorystyczne taktyk walki cybernetycznej. Zdziesiątkowanie przez Amerykanów scentralizowanego sztabu *Al-Kaidy* w Afganistanie zmusiło ją do przeorganizowania się w sieć komórek powiązanych ze sobą o wiele mniej sztywnymi więzami hierarchicznymi i luźniejszymi sposobami sterowania i wydawania rozkazów. Groźba cyberataków ze strony organizacji terrorystycznych w rodzaju *Al-Kaidy* nie zależy wyłącznie od woli ścisłego kierownictwa i najbardziej zawziętych i radykalnych bojowników ,,świętej wojny".

W cyberprzestrzeni istnieje wielu sprzymierzonych hakerów i internetowych aktywistów, którzy deklarują chęć zaangażowania się w to, co nazywają „cyberdżihadem" lub świętą wojną elektroniczną przeciwko Zachodowi, a zwłaszcza Izraelowi i Stanom Zjednoczonym.

Na przykład Malezja staje się cybernetycznym centrum sympatyzujących z *Al-Kaidą* hakerów i twórców wirusów. Powstała grupa znana jako *MHA* (*Malaysian Hacker Association*), czyli stowarzyszenie hakerów malezyjskich, bardzo aktywna w regionie, która przejawia sympatie proislamskie i proalkaidowe.

Od 2002r. analitycy ds. bezpieczeństwa zaczęli obserwować oznaki rodzącej się współpracy różnych hakerskich grup propalestyńskich, które zaczęły koordynować ataki mające na celu poparcie intifady. Były to wystąpienia przeciwstawiające się amerykańskiej wojnie z terroryzmem oraz agresjom, które określano jako agresja Indii przeciwko muzułmanom w Kaszmirze. Mowa tu o grupach *Unix Security Guards (USG), Word's Fantabulous Deficers (WFD)* i *Anti-India Crew (AIC)*. Przykładowa działalność powyższych „grup" to niszczenie stron WWW oraz umieszczanie na nich informacji antyamerykańskich i antyizraelskich.

Na Środkowym Wschodzie grupy terrorystyczne w rodzaju *Al-Kaidy, Hamasu* i *Hezbollahu* dzięki aktywnemu wykorzystaniu komputerowych technologii szyfrowych i kawiarni internetowych potrafią utrzymywać wysokie tempo operacji. Grupy te wykazują tendencje do przechodzenia od tradycyjnych form terroryzmu sponsorowanego przez rządy do nowego modelu, w którym Internet, obok innych nowoczesnych technologii, jest wykorzystywany do zbierania funduszy oraz do ciągłej rekrutacji nowych sympatyków.

Istnieje coraz więcej dowodów wskazujących, że *Al-Kaida* ewaluuje w stronę korzystania z cyberbroni i że zapoczątkowała ten sposób myślenia terrorystów i naszego ich postrzegania. Komórki *Al-Kaidy* coraz częściej wykorzystują w działaniach systemy informatyczne w których gromadzą szczegółowe informacje na temat potencjalnych celów. Za pomocą Internetu pozyskują dane wywiadowcze o przyszłych obiektach ataku, zwłaszcza „węzłach krytycznych" dla gospodarki, a nowoczesne oprogramowanie umożliwia im analizowanie materiału i poszukiwanie słabych punktów konstrukcji oraz przewidywanie wystąpienia reakcji kaskadowych atakowanych systemów.

Al-Kaida oraz inne organizacje terrorystyczne dysponują trzema wielkimi atutami – przekonaniem o słuszności ataków, potrzebnymi zasobami i możliwością czekania na właściwy moment – czynnikami potrzebnymi do stosowania cybertaktyki w przyszłości[8].

[8] D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Gliwice 2004.

4. Wojny w cyberprzestrzeni

Wojny internetowe to akcje, mające na celu zakłócenie działania, uszkodzenie lub zniszczenie oprogramowania, komputerów lub sieci informacyjnych jakiegoś państwa bądź organizacji, dokonane przez aktorów niepaństwowych w odpowiedzi na podobny atak przeprowadzony przez innych aktorów niepaństwowych. Wojny internetowe są przełożeniem realnego konfliktu lub napięcia do cyberprzestrzeni, gdzie dochodzi do wirtualnego starcia. Udział w nich biorą przede wszystkim mniej lub bardziej zorganizowane grupy hakerów, ale także cyberterroryści.

Powyższa definicja zdaniem autora mieści się w ramach ogólnego pojęcia walki informacyjnej. Mówiąc jednak o „wojnie internetowej" mamy na myśli przede wszystkim działania z udziałem państw (choć oczywiście mogą w niej brać także udział aktorzy niepaństwowi). Termin „wojny internetowe" dotyczy zaś wyłącznie takich akcji, w których państwa są celami ataków, ale nie są w sposób bezpośredni zaangażowane w wirtualne starcia. Na przykład, jeżeli hakerzy rosyjscy zaatakują systemy informacyjne Stanów Zjednoczonych, na co w odpowiedzi amerykańscy hakerzy uderzą na Rosję, to mamy do czynienia z wojną internetową. Natomiast jeżeli w konflikt w cyberprzestrzeni zaangażowałyby się państwa ze wszystkimi swoimi środkami, to jest to już walka informacyjna.

Pojęciu „wojny internetowej" bliższy jest termin J. Arquilli i D. Ronfeldta — *netwar*, czyli konflikt o niskiej intensywności między państwami i aktorami niepaństwowymi, takimi jak międzynarodowe organizacje terrorystyczne, partyzanci, handlarze narkotyków[9].

Niektórzy autorzy (m.in. M. Libicki) posługują się pojęciem „wojny hakerów". Termin ten jest zdecydowanie najbliższy naszemu rozumieniu wojen internetowych, jednak ogranicza on uczestników konfliktu do wąskiej grupy osób (hakerów).

W wirtualnych starciach mogą brać udział także cyberterroryści i takie przypadki miały już miejsce, chociaż ich rola nie była dotychczas pierwszoplanowa. W starciach między poszczególnymi grupami, celami ataków jest oprogramowanie, komputery, sieci komputerowe rządu, organizacji użyteczności publicznej, wojska czy firm komercyjnych. Słowem, działania takie stanowią istotne zagrożenie dla bezpieczeństwa państwa. Jest to dowód na to, że warto w tej pracy wspomnieć również o takim zjawisku.

Pierwszą wojnę internetową wywołał **konflikt w Kosowie**. W czasie wirtualnego konfliktu w Kosowie użyto całego wachlarza środków. Wykorzystano Internet do propagandy, komunikowania się, demonizowania przeciwnika (dezinformacja), atakowania za pomocą wirusów, *Distributed of Service (DoS), Distributed Denial of Service (DDoS),*

[9] J. Arquilla, D. Ronfeldt, Cyberwar is coming! „Comaparative Strategy" 1993.

e-mail bombingu, włamywania się na strony internetowe itd. Internet wspierał oficjalną propagandę zarówno natowską, jak i jugosłowiańską. Serbowie wysyłali pocztą elektroniczną tysiące e-maili do różnego rodzaju organizacji, prasy, radia, telewizji i rządów państw NATO z apelem o zaprzestanie bombardowania. Część e-maili miało charakter zdecydowanie antynatowski i antyamerykański, inne skupiały się na masakrach, które powodowały naloty dokonywane przez natowskie samoloty. Tom Reid, londyński korespondent „*Washington Post*", stwierdził, że otrzymywał w czasie konfliktu około 20–50 listów elektronicznych dziennie od serbskich profesorów z różnych uniwersytetów i aktywistów z prośbą o apel, by wstrzymać bombardowania. „Pamiętaj, że pod twoimi bombami giną ludzie"[10]. Inny e-mail brzmiał: „W ostatnich dziewięciu dniach barbarzyńcy z NATO zbombardowali szkoły, szpitale, mosty, zabijając wielu ludzi. Cały czas jest im mało i teraz zaczynają niszczyć nasze dziedzictwo kultury, które najlepiej świadczy o istnieniu naszego narodu". Poczty elektronicznej wysyłanej przez serbskich aktywistów było tak wiele, że tego typu wiadomości spamowe „Wall Street Journal" nazwał *Yugospamami*[11].

Także NATO, Amerykanie i Brytyjczycy używali Internetu do celów propagandowych. W przypadku Stanów Zjednoczonych działania te miały charakter uzupełniający oficjalną propagandę. Brytyjskie *Foreign Office* opracowało natomiast kompleksowy plan działań w Internecie. Zamieszczono na swoich stronach WWW list ministra spraw zagranicznych Robina Cooka, zapewniający, że akcja sił sprzymierzonych nie jest skierowana przeciwko Serbom, ale przeciwko Slobodanowi Miloszeviciovi. Ówczesny minister obrony Wielkiej Brytanii, George Robertson kazał tłumaczyć na serbsko-chorwacki i umieszczać w Internecie ocenzurowane przez Belgrad wiadomości, dotyczące przebiegu konfliktu.

Główny ciężar wirtualnego starcia ogniskował się jednak wokół działalności różnego rodzaju grup hakerów, popierających Serbów bądź Albańczyków z Kosowa (i tym samym akcję wojsk NATO). Obie strony atakowały także za pomocą *e-mail bombingu*. Rzecznik NATO Jamie Shea potwierdził, że pod koniec marca 1999 roku natowski serwer pocztowy został „przepełniony" i pojawiły się trudności z odbiorem poczty elektronicznej, ponieważ niezidentyfikowana osoba wysyłała na serwer dwa tysiące e-maili dziennie. Działania serbskich hakerów wspierali rosyjscy i chińscy koledzy. Chińczycy aktywnie włączyli się w konflikt po zbombardowaniu przez natowskie samoloty ambasady Chin w Belgradzie.

[10] A. Pratkanis w wywiadzie udzielonym R. Montgomery'emu pt. Enemy in S/te - lt's Time to Join the Cyberwar, „Daily Telegraph", 19 kwietnia 1999.

[11] E. J. Polloc, A. Petersen, *Unsolidted E-Mail Hits Targets in America in First Cyberwar*, „Wall Street Journal", 8 kwietnia 1999.

W sumie, podczas bombardowania Jugosławii zostało zaatakowanych blisko 100 serwerów NATO. Według natowskich specjalistów przynajmniej w części odpowiedzialni są za to hakerzy zatrudnieni przez jugosłowiańskich wojskowych. Atakowano w najróżniejszy sposób. Nie unikano nawet rozsyłania wirusów.

W przypadku **konfliktu izraelsko-arabskiego** napięcie w cyberprzestrzeni wyczuwało sie od 1999 roku, jednak impulsem do rozpoczęcia wojny internetowej stał się wybuch drugiej intifady. Po porwaniu w październiku 2000 roku trzech żydowskich żołnierzy przez *Hezbollah*, proizraelscy hakerzy włamali się na strony tej organizacji. Umieszczono na niej gwiazdę Dawida, izraelski hymn *Hatikvah* i hebrajskie napisy. Później uderzono na palestyńskie strony rządowe oraz strony organizacji terrorystycznych. W odpowiedzi propalestyńscy hakerzy włamali się na strony Knesetu, które w wyniku *e-mail bombingu* zostały przez kilka godzin zablokowane. Podobny atak, trwający przeszło trzydzieści godzin, przeprowadzono na strony Ministerstwa Spraw Zagranicznych, gdzie umieszczono komunikaty nawołujące do przyłączenia się do wojny internetowej z Izraelem. Kolejnymi „ofiarami" propalestyńskich hakerów były strony Kancelarii Prezesa, Rady Ministrów oraz Ministerstwa Obrony.

Obie strony konfliktu prowadziły intensywną akcję propagandową, mającą na celu zdobycie ewentualnych sprzymierzeńców. W Internecie funkcjonowała strona poświęcona „elektronicznej intifadzie" (*Electronic Intifada*). Dla równowagi warto wymienić także podobną, tyle że proizraelską stronę utworzoną w Stanach Zjednoczonych — *Middle East Forum*.

Zarówno palestyńscy, jak i izraelscy hakerzy umieszczali w Internecie oprogramowanie, mające pomóc w wirtualnej wojnie. Już w październiku 2000 roku Izraelczycy stworzyli stronę *Wizel.com*, na której umieszczono program do przeprowadzania ataków typu *DoS*. Za jego pomocą włamano się na sześć różnych stron *Hezbollahu*, jedną *Hamasu* oraz do palestyńskich komputerów rządowych.

Podobnie postępowali propalestyńscy hakerzy. Na swoich stronach także umieszczali niezbędne oprogramowanie do ataków w cyberprzestrzeni z dokładną instrukcją obsługi. Udostępnione narzędzia miały być wykorzystywane tylko „przeciwko Żydom i Izraelczykom". Za ich pomocą atakowano strony *Wizel.com* oraz Banku Izraela i giełdy w Tel-Awiwie.

Jedna z propalestyńskich grup, *Unity*, opracowała nawet czteroczęściowy plan wojny internetowej, polegający na zniszczeniu izraelskiej infrastruktury internetowej. Pierwsza faza, to uderzenia na izraelskie serwery rządowe; druga – atak na cele ekonomiczne, np. Bank Izraela; trzecia – uderzenie w głównych dostawców usług internetowych. Kulminacją (czwarta faza) ma być skomasowany atak na strony *e-commerce*,

w celu „doprowadzenia do straty milionów dolarów w wyniku przerwanych transakcji" oraz atak na cele zagraniczne (np. w Stanach Zjednoczonych).

Specjaliści przyznają, że powyższe działania Palestyńczyków w Internecie były szczegółowo koordynowane i bardzo dobrze przygotowane. Pomagali im w tym hakerzy z różnych części świata, nie tylko z państw arabskich. Natomiast, wśród grup propalestyńskich hakerów działali także cyberterroryści z *Hezbollahu, Hamasu, Al-Kaidy* i innych organizacji. Na przykład dwóm złapanym hakerom, oskarżonym o atakowanie izraelskich stron, udowodniono związki z *Hezbollahem.* Dlatego też izraelska armia, prowadząc operacje antyterrorystyczne na terytoriach Autonomii Palestyńskiej, przywiązywała dużą uwagę do „odcięcia" Palestyńczyków od Internetu.

Konflikt chińsko-amerykański – 1 kwietnia 2001 roku amerykański samolot zwiadowczy EP-3 z 24-osobową załogą na pokładzie musiał awaryjnie lądować na południu Chin, po kolizji z chińskim myśliwcem. Zginął pilot Wang Wei. Pekin oskarżył Waszyngton o szpiegostwo. Napięcie we wzajemnych stosunkach trwało jedenaście dni.

Wydarzenie to stało się pretekstem do wybuchu kolejnej wojny internetowej. Według strony amerykańskiej pierwsi zaatakowali Chińczycy. *CNN* na swoich stronach internetowych podała: „Pierwszego maja chińscy hakerzy zaatakowali amerykańskie serwery. Pretekstem była decyzja prezydenta George'a W. Busha o sprzedaży broni Tajwanowi oraz awaryjne lądowanie na terenie ChRL amerykańskiego samolotu"[12]. Dodatkowo Centrum Ochrony Narodowej Infrastruktury (*National Infrastructure Protection Center*, *NIPC*) – agenda *FBI* zajmująca się przestępczością komputerową – ostrzegała, że między 30 kwietnia a 7 maja może dojść do wzmożonych ataków chińskich hakerów oraz wzywała do monitorowania sieci i wzmocnienia zabezpieczeń na serwerach pocztowych.

W rzeczywistości pierwsi zaatakowali amerykańscy hakerzy. Już tydzień po incydencie z pierwszego kwietnia nasiliły się włamania na chińskie strony internetowe. Akcję rozpoczęła amerykańska grupa *PoisonBOx*. Na stronach chińskich instytucji i firm pojawiły się pornograficzne obrazki i obraźliwe hasła: „Ja dobry Chińczyk, ja lubić malihuana!", „Gdzie nasz samolot złodzieje?!", „Nienawidzimy Chin. Oddajcie nasz samolot!" W ciągu paru dni dokonano kilkuset ataków, m.in. na *China Telecom*, *China Nuclear Information Center* oraz strony rządowe.

Chińscy hakerzy wypowiedzieli amerykańskim wojnę. Grupy: *The Honkres Union of Chine (HOC), Primus Chinaren, Redfreedom, Red-Crack czy Chinese Red Guest Network Security Technology Altiance* zapowiedziały, że zdobędą tysiące amerykańskich stron w odpowiedzi na „niczym nie sprowokowany i skandaliczny atak USA na Chiny". *HOC* w manifeście umieszczonym w Internecie napisała: „Kochamy nasz kraj

[12] L. Gawrycka, *Cyberporachunki*, „Życie Warszawy" 18–19 sierpnia 2001.

i nasz naród. Gdy nas wzywa, poświęcimy mu wszystko". Na stronie *KillUSA.com* wszyscy, którzy chcieli wziąć udział w antyamerykańskiej krucjacie mogli znaleźć potrzebne do tego oprogramowanie. Szybko wojna chińsko-amerykańska uległa umiędzynarodowieniu. Amerykanów wsparli hakerzy z Arabii Saudyjskiej, Pakistanu, Indii, Brazylii, Argentyny i Malezji, natomiast Chińczyków – hakerzy z Korei, Indonezji i Japonii.

Chińscy hakerzy, bardzo dobrze zorganizowani i przygotowani, koordynowali swoje akcje za pomocą *IRC* lub poczty elektronicznej. Uderzono m.in. na Biały Dom, Departament Pracy, Departament Zdrowia, Departament Energetyki, Departament Spraw Wewnętrznych, Izbę Reprezentantów i Dowództwo Marynarki Wojennej. Atakowano także małe amerykańskie firmy *e-commerce.*

W rewanżu Amerykanie również zaatakowali strony lokalnych władz chińskich, strony rządowe oraz komercyjne.

W wyniku obopólnych działań zdobyto półtora tysiąca stron amerykańskich i ponad 300 chińskich. Chińscy hakerzy udoskonalili metodę ataku typu *DDoS,* który okazał się niezwykle skuteczny. Do walki wykorzystywano także wirusy, m.in. stworzony specjalnie na tę okazję przez jednego z członków *HOC, Lion.* Uważa się także, że robak *Co-de Red* jest pokłosiem konfliktu chińsko-amerykańskiego.

Chińsko-amerykańska wojna internetowa dała dużo do myślenia amerykańskim specjalistom, zajmującym się bezpieczeństwem informacji. Stwierdzono, że po pierwsze ataki hakerów stają się coraz groźniejsze i że nie wiadomo, czy następna wojna nie spowoduje znacznie groźniejszych skutków. O powadze sytuacji świadczy choćby fakt opublikowania przez *NIPC* raportu ostrzegającego przed skutkami ataku chińskich hakerów. Po drugie, w czasie wirtualnego konfliktu rola rządu chińskiego nie była jasna. Oficjalnie nie popierał on działalności hakerów, ale też nie podjął żadnych działań, mających na celu ich powstrzymanie. Co pewien czas w amerykańskiej prasie podnoszone są głosy, że chińscy wojskowi chcą wykorzystać „niezależnych" hakerów, aby przetestować formy walki informacyjnej i jednocześnie sprawdzić amerykańskie i tajwańskie zabezpieczenia[13].

Po trzecie, specjaliści wskazują na możliwość wykorzystania tego typu konfliktów do własnych celów, na przykład przez cyberterrorystów. Zastanawiano się, dlaczego w konflikt nie zaangażowali się, po żadnej ze stron, hakerzy z byłego Związku Radzieckiego. Stwierdzono, że ta neutralność mogła przybrać charakter pozorny i hakerzy, umiejętnie podając się za Amerykanów lub Chińczyków, mogli dalej podsycać walkę. Byłoby to praktycznie nie do wykrycia, a koszty takiej wojny mogłyby drastycznie się zwiększyć.

[13] B. Miller, Worries of Cyberattacks on U.S. Are Aired, „Washington Post", 26 kwietnia 2002.

5. Podsumowanie

Cyberprzestrzeń staje się istotnym „elementem nerwowym" gospodarki państwa. Jest to system sterowania gospodarką kraju, złożony z setek tysięcy połączonych ze sobą komputerów, routerów, przełączników i linii światłowodów, które pozwalają działać państwowym infrastrukturom. Infrastruktura teleinformatyczna ma wiele słabych punktów, które mogą umożliwić przeprowadzenia cyberataku obniżając w istotny sposób ich sprawność.

Cyberterroryzm staje się najbardziej nieprzewidywalnym sposobem oddziaływania zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Pojawiła się kategoria infrastruktury krytycznej, której zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo państwa. Główne jej elementy to: telekomunikacja, system energetyczny, system bankowy, produkcja oraz sieć transportu gazu ziemnego i ropy naftowej, transport, system zaopatrzenia w wodę, służby ratownicze oraz ciągłość funkcjonowania administracji publicznej.

Czy możemy się uchronić przed cyberterroryzmem? Odpowiedź nie jest jednoznaczna i prosta, myślę, że raczej nie, istnieje jednak kilka sposobów na określenie wystąpienia groźby cybrataku. Istotne jest również określenie właściwej polityki bezpieczeństwa w tej dziedzinie.

A oto kilka wniosków wynikających z pracy:

- cyberterroryzm jest jedną z nowych broni wykorzystywaną do destrukcji systemów teleinformatycznych państwa w celu osiągnięcia zamierzonych korzyści politycznych, ekonomicznych lub ideologicznych;
- cyberterroryzm jest szczególnie atrakcyjną formą walki wynikającą z faktu, że cechują go niskie koszty takiej działalności, zwłaszcza w porównaniu z kosztami regularnych działań zbrojnych;
- obszarami zainteresowań cyberterrorystów są zarówno systemy wojskowe (militarne), jak i cywilne (niemilitarne);
- niezwykle skutecznymi a zarazem najbardziej niebezpiecznymi atakami są ataki odmowy usługi *DoS* i *DDoS* oraz ataki wykorzystujące programy złośliwe, czyli wirusy, robak i bakterie;
- działalność organizacji terrorystycznych w cyberprzestrzeni jest faktem, dysponują oni zarówno potencjałem finansowym, jak i doskonale przygotowaną kadrą informatyków gotowych wykorzystać swoje umiejętności realizując cele ideologiczne, ekonomiczne lub polityczne;
- wojna oraz konflikty w cyberprzestrzeni są jednym z wymiarów współczesnego pola walki, o czym dobitnie wykazały konflikty zarówno militarne, jak i cywilne; zastosowane w nich metody ataków wpływały w sposób znaczący na

przebieg konfliktów a w przypadku konfliktów tzw. ideologicznych powodowały destabilizację życia politycznego i gospodarczego państwa;
– ze względu na wiele niebezpieczeństw w Internecie, szczególną uwagę powinno się zwrócić na problem bezpieczeństwa systemów informatycznych oraz edukacji użytkowników i osób decydujących o bezpieczeństwie systemów teleinformatycznych.