"The Knight of Freedom - Rycerz Wolności"

Pulaski Policy Papers

No. 7/09
21 IV 2009

www.pulaski.pl

Komentarz Międzynarodowy Pułaskiego

Warsaw, Poland

Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem

Marcin Łapczyński

Koniec XX i początek XXI wieku to okres gwałtownego rozwoju nowych technologii informatycznych, komputerów i Internetu. Niekontrolowany rozwój tego medium, a także znaczny stopień *„usieciowienia"* współczesnych społeczeństw sprawił, że pojawiły się nowe, dotychczas niespotykane zagrożenia, które w znaczący sposób mogą zagrozić krytycznej infrastrukturze państwa. Najdobitniejszym tego przykładem były wydarzenia w Estonii, która w maju 2007 roku musiała zmierzyć się ze zmasowanym cyberatakami, będącymi odwetem za przeniesienie pomnika żołnierzy Armii Czerwonej z centrum Tallina na podmiejski cmentarz wojskowy. Biorąc pod uwagę znaczenie technologii informatycznych we współczesnym świecie oraz realną groźbę wykorzystania ich przeciwko bezpieczeństwu państwa zachodzi potrzeba znalezienia odpowiedzi na pytanie, w jakim stopniu Polska jest narażona na zagrożenia płynące z globalnej sieci oraz czy zaistniała potrzeba wypracowania kompleksowej i efektywnej strategii obrony przed cyberterroryzmem?

Cyberterroryzm jako źródło zagrożenia – próby definicji

Cyberterroryzm nie jest zjawiskiem nowym. Sam termin pojawił się już w 1979 roku, kiedy to szwedzkie Ministerstwo Obrony umieściło go w swoim raporcie o zagrożeniach komputerowych, rekomendując by rząd zaangażował się w monitorowanie zarówno publicznych, jak i prywatnych sieci komputerowych[1]. Na początku lat dziewięćdziesiątych przestrzeń cybernetyczną (Cyberspace), jako piąty model wojny, wyróżniono w popularnym „modelu Wardena"[2]. Do arsenału środków walki włączono m.in. wirusy komputerowe, robaki, konie trojańskie, impulsy elektromagnetyczne służące zniszczeniu sieci i komputerów przeciwnika, czy strumienie danych o dużym natężeniu powodujące ich krótkotrwałe lub długotrwałe blokowanie.

Nie ma jednej, powszechnie przyjętej definicji cyberterroryzmu. Specjaliści z Akademii Obrony Narodowej w *„Analizie systemowej zjawiska cyberterroryzmu"* definiują go 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"*[3]. Podobne definicje znajdziemy w dokumentach amerykańskiego Departamentu Stanu, czy FBI. Dorothy E. Denning, profesor amerykańskiego Uniwersytetu Georgetown zajmująca się naukowo problemami bezpieczeństwa przestrzeni informatycznej, zwraca szczególną uwagę na wymiar i skalę ataków. By zakwalifikować konkretny atak w cyberprzestrzeni za cyberterroryzm, musi on *„skutkować przemocą w stosunku do ludzi lub własności, lub przynajmniej powodować strach."* Najlepszymi przykładami, według Denning, mogą być takie ataki z wykorzystaniem sieci teleinformatycznych, które w swoich skutkach prowadzą *„do śmierci, okaleczenia ciała, eksplozji, rozbicia się samolotów, zanieczyszczenia wody lub drastycznych strat ekonomicznych."*[4] Poważne ataki na infrastrukturę mogą być zakwalifikowane jako akty cyberterroryzmu w zależności od ich skali.

Wszystkie definicje mają jeden element wspólny - o cyberterroryzmie możemy mówić jedynie wtedy, kiedy mamy do czynienia z politycznie motywowanym atakiem z użyciem sieci teleinformatycznych. W pozostałych przypadkach takie ataki klasyfikuje się zazwyczaj jako cyberprzestępstwa niemające podtekstu politycznego. Nie można również łączyć cyberterroryzmu z tzw. hacktivismem (połączenie słów hacker i activism). Pojęcie to używane jest do określania działań o charakterze hackerskim celem osłabienia normalnego funkcjonowania systemów informatycznych, połączonych z propagandą i wyrażaniem opinii o charakterze politycznym. Działania te, w odróżnieniu od cyberterroryzmu, nie powodują większych zniszczeń w infrastrukturze istniejącej poza cyberprzestrzenią[5].

Skala i charakter zagrożenia

Analizując zagrożenia płynące z cyberprzestrzeni, warto przywołać kilka ciekawych faktów. Jedynie we wrześniu 2007 roku liczba komputerów w Stanach Zjednoczonych „zniewolonych" przez hackerów z Chin wyniosła ponad 730 tysięcy. W ubiegłym roku liczba ataków na serwery Departamentu Obrony USA wzrosła aż o 46%. Departament Stanu szacuje, że dziennie jego sieć informatyczna narażona jest na 6 milionów ataków. Biorąc pod uwagę źródła tego zjawiska, trzeba zauważyć, że typowe grupy terrorystyczne są tylko jednym z nich. Atak może pochodzić także ze strony „państw zbójeckich" lub innych mających określone cele polityczne (najczęściej Chiny, Rosja czy Kuba), ze strony sympatyków terrorystów, czy wreszcie ze strony indywidualnych hackerów pragnących zademonstrować swoje zdolności, czy uprzykrzyć życie instytucjom państwowym, politykom lub firmom, z których polityką się nie zgadzają.

Internet i sieci teleinformatyczne są także chętnie wykorzystywane przez rządy, armie i służby specjalne wielu państw do tzw. cyberszpiegostwa. Już w latach 80. Zachodnioniemieccy hackerzy, na zamówienie KGB, kopiowali tajne dane z serwerów Departamentu Obrony USA. W czasie wojny w Kosowie w 1999 roku, amerykańskie służby specjalne prowadziły akcję o kryptonimie „Matrix", która miała sparaliżować

elektroniczną i telefoniczną sieć Serbii. W odwecie serbscy hackerzy zablokowali serwery Sojuszu Północnoatlantyckiego[6].W tym samym roku rosyjscy cyberszpiedzy wykradli, prawdopodobnie z amerykańskich serwerów rządowych, tajne informacje o systemach naprowadzania amerykańskich rakiet. Jednak najbardziej znaną operacją szpiegowską w globalnej sieci, była operacja „Titan Rain" przeprowadzona w latach 2003-2005 przez chińskich hackerów na zlecenie chińskiej armii. Hackerzy przeczesali sieci takich firm i instytucji, jak Lockheed Martin, Sandia National Laboratories czy NASA. Od czerwca do sierpnia 2007 roku ofiarami ataków, prawdopodobnie chińskiej armii, padły sieci rządowe Niemiec, Wielkiej Brytanii, Francji czy Nowej Zelandii[7]. Wszystkie ataki z użyciem technologii informatycznych mają kilka cech wspólnych, dzięki którym ich liczba w najbliższym czasie może wzrosnąć:

- Po pierwsze - są one niezwykle trudne do wykrycia. Zlecający atak może wynająć wykonawców z innego kraju lub przeprowadzić ataki z publicznej kawiarenki internetowej,
- Po drugie – wysoki stopień anonimowości osób przeprowadzających ataki[8].
- Po trzecie - duża siła rażenia. Były szef FBI Jim Settle powiedział kiedyś „Dajcie mi 10 hackerów a w ciągu 90 dni powalę ten kraj [USA] na kolana[9]".
- Po czwarte - niezwykła łatwość przeprowadzenia ataków. Kraje o małej potędze mogą stanowić poważne zagrożenie dla światowych potęg militarnych i ekonomicznych.
- Po piąte - niskie koszty przedsięwzięcia. Często wystarczy mały program ściągnięty z Internetu za kilka dolarów. Obecnie, według szacunków ekspertów, w sieci umieszczonych jest ponad 68 tysięcy (!) programów mogących służyć potencjalnym cyberterrorystom.

Estonia jako ofiara cyberterroryzmu

„Gaśnie światło, Internet nie działa. Banki są zamknięte, nie można skorzystać z bankomatu. Radio i telewizja milczą. Lotniska i dworce kolejowe puste. Za to ulice – zupełnie zakorkowane. Po długiej nocy pojawiają się szabrownicy – policja nie jest w stanie przywrócić porządku. Nikt nie ma dostępu do pieniędzy, jedyne, co się teraz liczy to paliwo, jedzenie i woda. Zaczyna się panika...[10]". To nie scenariusz filmu z gatunku horroru czy science-fiction, a cytat z wystąpienia Samiego Saydjari, szefa organizacji Professionals for Cyber Defense, przed Komisją Bezpieczeństwa Wewnętrznego Izby Reprezentantów Stanów Zjednoczonych, które odbyło się w kwietniu 2007 roku. Wystąpienie Saydjari'ego miało miejsce w przededniu wydarzeń, które na nowo zwróciły uwagę świata na zagrożenie płynące z cyberprzestrzeni. Od 27 kwietnia do 11 maja 2007 roku ofiarą cybernetycznych ataków stała się Estonia. W odpowiedzi na decyzję estońskich władz o przeniesieniu pomnika upamiętniającego żołnierzy Armii Czerwonej (tzw. Brązowego Żołnierza), w kraju wszczęte zostały zamieszki. Sieć teleinformatyczna kraju doprowadzona została do stanu krytycznego.

Warto nadmienić, że Estonia bardzo często nazywana jest „E-stonią" ze względu na bardzo wysoki stopień zinformatyzowania. Ponad 90% transakcji bankowych dokonuje się tam on-line, istnieje możliwość składania deklaracji podatkowych przez Internet. Każdy obywatel posiada Digital ID, który umożliwia nawet głosowanie przez Internet. Estoński rząd wprowadził system „e-valitsus" (e-państwo), dzięki któremu wspiera proces informatyzacji. Sam gabinet kontaktuje się w dużym stopniu za pomocą komputerów, a wszystkie rządowe dokumenty są dostępne w sieci. Znacznie skraca to czas pracy i zwiększa wydajność[11]. Wszystkie te czynniki sprawiły, że estońska infrastruktura teleinformatyczna okazała się doskonałym celem cyberataków. W szczytowym momencie, czyli w obchodzony w Rosji Dzień Zwycięstwa 9 maja, ruch na estońskich stronach www wzrósł ponad dwudziestokrotnie. Największe 10 ataków miało siłę ponad 90 Mb/s i trwały nieprzerwanie ponad 10 godzin. Zablokowane zostały strony rządowe, kancelarii prezydenta, głównych gazet, padły systemy bankowe, czy wreszcie wewnętrzna sieć estońskiej policji. Estończycy byli odcięci od dostępu do informacji w Internecie, a także, co gorsze, od dostępu do banków i pieniędzy[12]. Funkcjonowanie administracji państwowej, w dużym stopniu zinformatyzowanej, stanęło pod znakiem zapytania. Według słów estońskiego ministra obrony Jaaka Aaviksoo, „pierwszy raz zdarzyło się, żeby cyberataki stanowiły poważne zagrożenie dla bezpieczeństwu całego narodu[13]". Władze Estonii zastanawiały się nad odwołaniem się do artykułu 5. Traktatu Waszyngtońskiego, mówiącego o wzajemnej pomocy państw członkowskich NATO w razie ataku na terytorium jednego z nich.

Nie można stwierdzić jednoznacznie, kto stał za kwietniowymi atakami na Estonię. Jak już wspomniano wcześniej, sprawców i rzeczywistych zleceniodawców cyberataków bardzo trudno jest namierzyć. Analiza specjalistów pokazała, że część komputerów dokonujących ataków była zarejestrowana w administracji prezydenta Rosji, ale większość ataków pochodziła z zainfekowanych komputerów w Egipcie, Wietnamie oraz Peru. Faktem jest jedynie to, że z racji na zaszłości historyczne i prestiżowe, Rosja mogła być zainteresowana przeprowadzeniem takiego ataku. Dla Rosjan pomnik Brązowego Żołnierza był hołdem złożonym żołnierzom Armii Czerwonej, którzy wyzwalali kraje bałtyckie spod niemieckiej okupacji w 1944 roku. Dla Estończyków pomnik był symbolem długich lat sowieckiej okupacji.

Reakcje na zagrożenie cyberterroryzmem

Wydarzenia w Estonii dały impuls wielu państwom i rządom do wypracowywania koncepcji obrony przed

zagrożeniami cyberterroryzmu. Stany Zjednoczone stworzyły Narodowy Wydział ds. Bezpieczeństwa Cybernetycznego w Departamencie Bezpieczeństwa Narodowego. W ostatnim czasie Departament wraz z Narodową Agencją Bezpieczeństwa stworzyły jednostkę złożoną z ponad 2000 specjalistów, którzy pracować będą nad mechanizmami obrony, ale także nad rozwinięciem własnych możliwości dokonania takich ataków[14]. Stany Zjednoczone powołały także Air Force Cyber Command, którego zadaniem będzie obrona przed atakami w cyberprzestrzeni oraz szkolenie wojska do tego typu zadań[15].

Comprehensive Political Guidance, przyjęty na szczycie NATO w Rydze w 2006 roku zakłada w najbliższej dekadzie rozwój "zdolności do ochrony systemów informacji o szczególnym znaczeniu dla Sojuszu przed cyberatakami[16]". Rok po wydarzeniach w Estonii, w maju 2008 roku, Sojusz Północnoatlantycki otworzył w Tallinie Centrum Doskonalenia Obrony przed Cyberatakami (Cooperative Cyber Defence Centre of Excellence). Centrum ma prowadzić badania i wspierać przygotowania państw członkowskich w kwestii obrony przed cyberatakami. Spośród ponad 30 pracowników ponad połowa to specjaliści z krajów, które podpisały dokumenty powołujące do życia Centrum – Estonii, Litwy, Łotwy, Niemiec, Hiszpanii, Włoch oraz Słowacji[17]. Wolę przystąpienia do Centrum wyraziła także Turcja oraz Stany Zjednoczone. Centrum oficjalnie rozpoczęło swoje działanie z początkiem stycznia 2009 roku. Na podstawie postanowień Protokołu Paryskiego z 1952 roku, NATO nadało Centrum status międzynarodowej organizacji bezpieczeństwa[18].

Sama Estonia, która padła ofiarą zmasowanych cyberataków, 8 maja 2008 roku przyjęła kompleksową Narodową Strategię Bezpieczeństwa Informatycznego[19]. Dokument ten, wypracowany wspólnie przez kilka ministerstw, jest pierwszym krokiem w kierunku zapewnienia efektywnej polityki obrony przed zjawiskiem cyberterroryzmu. Strategia opiera się na 5 głównych założeniach: wzroście środków obrony przed zagrożeniami cybernetycznymi ze szczególnym uwzględnieniem instytucji rządowych i infrastruktury krytycznej, umocnieniu zdolności w dziedzinie bezpieczeństwa informacyjnego, stworzeniu odpowiednich podstaw prawnych, wspieraniu współpracy międzynarodowej oraz upowszechnianiu wiedzy na temat zagrożeń płynących z sieci wśród społeczeństwa[20].

Nieformalne spotkanie ministrów obrony państw NATO, które odbyło się w lutym 2009 roku w Krakowie, było ostatnim spotkaniem w tym składzie przed kwietniowym jubileuszowym szczytem Sojuszu w Strasburgu/Kiehl. Trochę niezauważenie przemknęły słowa Jaapa de Hoop Scheffera zapowiadające włączenie zagrożenia cyberterroryzmem i bezpieczeństwa informatycznego do przygotowywanej nowej koncepcji strategicznej Sojuszu. Na konferencji zorganizowanej przez krakowski Instytut Studiów Strategicznych Scheffer dał wyraźny znak, że Sojusz nie może pozostać obojętny wobec zagrożeń niekonwencjonalnych, takich jak cyberterroryzm, piractwo, a także implikacji m.in. ze zmian klimatycznych, czy bezpieczeństwa energetycznego. Wiele racji miał sekretarz generalny NATO mówiąc, że „cyberataki nie wymagają użycia ani jednego żołnierza, czy naruszenia granic – mogą jednak sparaliżować działanie państwa"[21].

Wydaje się, że nowa koncepcja strategiczna Sojuszu będzie krokiem w dobrym kierunku, a państwa członkowskie Sojuszu rozpoczną prace nad konstruowaniem narodowych strategii zapobiegania i zwalczania zagrożeń płynących z globalnej sieci. Tym bardziej, że nowa natowska koncepcja powinna zawierać konkretną definicję zjawiska cyberterroryzmu, która może posłużyć za punkt wyjścia w przygotowywaniu dalszych dokumentów i strategii. Świętując 60. urodziny Sojusz musi jednoznacznie określić swoją rolę i zadania w kontekście bezpieczeństwa informatycznego oraz zapewnić, że koncepcja sojuszniczej solidarności będzie miała zastosowanie także w przypadku zagrożenia cyberterroryzmem.

Cyberterroryzm w kontekście Polski

A jak wygląda sprawa z polskiej perspektywy? Mimo, że Polska nie jest zinformatyzowana w tak dużym stopniu jak Estonia i inne państwa zachodnie, należy zakładać, że może ona w najbliższej dekadzie stać się celem cyberataków. Dlaczego?

- Po pierwsze, procent użytkowników Internetu w polskim społeczeństwie stale wzrasta. W latach 2000-2008 wzrost użytkowników wyniósł 4,2%. Według danych Internet Word Status w Polsce zarejestrowanych jest około 16 milionów użytkowników, co stanowi 41,6% całej populacji[22]. Polska sytuuje się w pierwszej dziesiątce krajów o największej liczbie użytkowników Internetu zaraz po Niemczech, Wielkiej Brytanii, Francji, Włoszech i Hiszpanii. Należy zakładać, że „usieciowienie" Polski będzie wzrastać również w następnych latach.
- Po drugie, znaczny odsetek Polaków korzysta już np. z możliwości obsługi kont bankowych, telefonów komórkowych przez Internet. Praktycznie każdy bank w Polsce oferuje dostęp do swoich usług za pomocą komputera. Według raportu Rady Bankowości Elektronicznej przy Związku Banków Polskich liczba klientów korzystających z tego typu usług przekroczyła już 11 milionów, z czego 6,4 miliona to klienci aktywni (dokonali co najmniej 4 transakcje płatnicze). Rada prognozuje wzrost liczebności tej grupy do 10 milionów w 2010 roku[23].
- Po trzecie, krytyczna infrastruktura techniczna Polski (administracja rządowa, służby, wojsko, transport, energetyka) jest już w znacznym,

chociaż nadal odbiegającym od standardów światowych, stopniu zinformatyzowana. „Usieciowieniu" Polski ma sprzyjać opracowana przez MSWiA „Strategia rozwoju społeczeństwa informacyjnego w Polsce do 2013 roku".

- Po czwarte, Polska jako uczestnik operacji stabilizacyjnych w Iraku, czy Afganistanie jest „na celowniku" grup terrorystycznych, które mogą zastosować wobec niej atak cybernetyczny. Prawdopodobieństwo to jest na tyle wysokie, że grupy takie jak Al-Kaida zrozumiały użyteczność stosowania cyberbroni w działaniach zmierzających do osiągnięcia swoich celów[24].
- Po piąte, relacje Polski z Rosją nie układały się w ostatnim czasie najlepiej. Rosja jest jednym z głównych krajów podejrzewanych o wzmożone zainteresowanie i używanie cyberszpiegostwa i cyberterroryzmu [25]. Dotyczy to zarówno służb specjalnych, jak i prywatnych hackerów. Można zakładać, że w razie pogorszenia stosunków między oboma państwami może dojść do prób ataku przez sieci informatyczne na polską infrastrukturę tak, jak miało to miejsce w przypadku Estonii.
- Po szóste, Polska – jak każdy inny kraj – jest narażona na liczne próby cyberszpiegostwa dokonywanego przez służby specjalne obcych państw. Dotyczy to zarówno szpiegostwa administracji państwowej, przedsiębiorstw państwowych oraz firm prywatnych. Tym bardziej, że od 1996 roku incydenty związane z użyciem sieci teleinformatycznych w Polsce sukcesywnie się nasilały[26].

Rekomendacje dla Polski

Biorąc pod uwagę powyższą argumentację oraz rozwój sytuacji międzynarodowej, zadziwia nie wypracowanie przez Polskę żadnej strategii przeciwdziałania i walki z cyberterroryzmem oraz zagrożeniami płynącymi z cyberprzestrzeni. Pozytywnym krokiem jest umieszczenie w Strategii Bezpieczeństwa Narodowego RP z 2007 roku podrozdziału dotyczącego Bezpieczeństwa Informacyjnego i Telekomunikacyjnego (pkt. 3.8.) [27]. Biuro Bezpieczeństwa Narodowego przygotowuje zespół ekspertów ds. cyberterroryzmu. To właśnie BBN miałby stać się miejscem spotkań przedstawicieli resortów spraw wewnętrznych i administracji, obrony narodowej i finansów oraz ekspertów zajmujących się problematyką bezpieczeństwa państwa [28]. Dobrym rozwiązaniem było także utworzenie 1.02.2008 roku, w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW, Zespołu Reagowania na Incydenty Komputerowe – CERT. To pozytywny sygnał, niemniej wydaje się również zasadnym:

- Stworzenie w najbliższym czasie odrębnej, spójnej i efektywnej strategii zapobiegania i obrony przed cyberterroryzmem na wzór estońskiej Strategii Bezpieczeństwa Informatycznego,
- Zharmonizowanie polskiego ustawodawstwa w zakresie bezpieczeństwa informatycznego,
- Utworzenie scentralizowanej jednostki rządowej (swoistego centrum antykryzysowego) na bieżąco monitorującej sytuację w kraju i na świecie oraz koordynującej działania instytucji w razie kryzysu,
- Utworzenie komórek zajmujących się problemami bezpieczeństwa infrastruktury w poszczególnych jednostkach administracji państwowej i samorządowej lub nadanie kompetencji lokalnym jednostkom obrony cywilnej w tym zakresie,
- Włączenie się polskich ekspertów ds. bezpieczeństwa informatycznego w prace utworzonego przez NATO Centrum Doskonalenia Obrony przed Cyberatakami,
- Wspieranie badań naukowych dotyczących bezpieczeństwa informatycznego,
- Upowszechnianie przez instytucje rządowe i pozarządowe wiedzy o zagrożeniach związanych z użytkowaniem Internetu,
- Zintensyfikowanie współpracy międzynarodowej z organizacjami i instytucjami zajmującymi się obroną przed zjawiskami cyberterroryzmu.

Najważniejsza wydaje się jednak zmiana nastawienia polityków i zwykłych użytkowników Internetu do zagrożeń płynących z sieci teleinformatycznych. Bez zrozumienia skali i skutków potencjalnego zagrożenia nie może być mowy o wypracowaniu skutecznej strategii walki z cyberprzestępczością i cyberterroryzmem.

* * * * *

Marcin Łapczyński – ekspert Fundacji im. Kazimierza Pułaskiego. Absolwent Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego (specjalizacja: bezpieczeństwo i studia strategiczne). Studiował również na Uniwersytecie Wileńskim oraz w Moskiewskim Państwowym Instytucie Stosunków Międzynarodowych (MGIMO). Obecnie kontynuuje naukę na Central European University w Budapeszcie. Zajmuje się problematyką państw bałtyckich, Rosji i obszaru poradzieckiego oraz bezpieczeństwa międzynarodowego.

politycznym, które nastąpiły w Polsce po 1989 roku. Ideały generała Kazimierza Pułaskiego (wolność, sprawiedliwość i demokracja) stanowią inspirację dla wszelkich inicjatyw podejmowanych przez Fundację. Działania Fundacji obejmują m.in.: prowadzenie badań naukowych, opracowywanie publikacji i analiz, przygotowywanie seminariów oraz konferencji, edukowanie i wspieranie liderów www.instytutprzywodztwa.pl

Fundacja jest organizatorem Warszawskiego Regionalnego Kongresu Organizacji Pozarządowych www.warsawcongress.pl, Akademii Młodych Dyplomatów www.akademia.diplomacy.pl oraz wydawcą Platformy Komunikacyjnej dla Organizacji Pozarządowych www.non-gov.org

Fundacja przyznaje Nagrodę im. Kazimierza Pułaskiego "Rycerz Wolności" dla wybitnych postaci zasłużonych w promowaniu demokracji. Nagrodę dotychczas otrzymał profesor Władysław Bartoszewski, profesor Norman Davies, Alaksandar Milinkiewicz, lider demokratycznej opozycji na Białorusi oraz prezydent Lech Wałęsa.

Fundacja Pułaskiego jest jedną z dwóch polskich organizacji pozarządowych posiadających status organizacji partnerskiej Rady Europy. Więcej o Fundacji na www.pulaski.pl

Komentarz Międzynarodowy Pułaskiego to pogłębione analizy istotnych dla Polski zagadnień z zakresu polityki międzynarodowej, gospodarki światowej bądź bieżących wydarzeń w polskiej polityce. Dokument publikowany jest w dwóch wersjach językowych, polskiej i angielskiej. Osoby chcące publikować swoje oryginalne prace w Komentarzu proszone są o kontakt z Redaktorem Naczelnym p. Dominikiem Jankowskim djankowski@pulaski.pl Żeby regularnie otrzymywać kolejne numery KMP należy podać swój e-mail na stronie www.pulaski.pl

The cyber terrorism threat and the Polish defence strategy

Marcin Łapczyński

The end of the 20th century and the beginning of the 21st is a period of intensive development for new computer technologies and the Internet. It is the uncontrolled development of this medium along with the increasing amount of networking in today's society that has contributed to the appearance of new, previously unknown threats, which might pose a substantial danger to a country's critical infrastructure. The most evident example of this took place in Estonia. In May 2007 the country found itself under a complex series of cyber attacks in retaliation for moving the monument to the Red Army soldiers from the centre of Tallinn to the suburban military cemetery. Considering the importance of computer technologies in the contemporary world and the existing threat that they might be used against a country's security, a question arises here: to what extent is Poland endangered by threats coming from the global network, and is there already a need to come up with an effective strategy to be used against cyber terrorism?

Cyber terrorism as a source of threat: attempted definitions

Cyber terrorism is not a new phenomenon. The term itself appeared already in 1979 when the Swedish Defence Ministry put it in its report focusing on computer threats, recommending that the government should get involved in monitoring both public and private computer networks[29]. At the beginning of the nineties cyberspace was mentioned in the popular "Warden model" as the fifth war model[30]. Computer viruses, worms, Trojans, electromagnetic impulses, serving to destroy an opponents' network and computers, were all regarded as a war arsenal. There were also data streams of high intensity causing their short or long-term blocking.

There is no single, commonly-used definition of cyber terrorism. Experts from the Polish National Defence University in "The system analysis of cyber terrorism" define it as *"a politically motivated attack or a threat of attack on computers, networks or information systems to destroy the infrastructure, and pose a threat or force a government or people to realize certain goals"*[31]. Similar definitions can be found in the documents in the U.S. Department of State, or FBI. Dorothy E. Denning, professor of the Georgetown University, who conducts researches on the problems of security in cyberspace, points at the dimension and scale of these attacks. In order for a certain attack to qualify as cyber terrorism, it has to *"result in violence*

towards people or property or at least cause a certain degree of fear". The best examples, according to Denning, can be attacks which use teleinformatic networks which result in *"death, injuries, explosions, plane crashes, water pollution or drastic economic losses"*[32]. Serious attacks on infrastructure can be regarded as cyber terrorism depending on their scale.
All the definitions have one denominator – cyber terrorism occurs only when an attack has political grounds. Otherwise such attacks are defined as cyber crimes without political implications. Cyber terrorism should not be linked with the so called hacktivism (a combination of *hacker* and *activism*). The term is used to describe hacker-like activities which aim at weakening computer systems and motivated by a certain propaganda and expression of political opinions. Such activities, unlike cyber terrorism, do not cause major damages in infrastructure outside cyberspace[33].

The scale and character of the threat

Analyzing the threats coming from cyberspace it is worth mentioning a few interesting facts. Only in September 2007 the number of computers in the U.S. "violated" by hackers from China totalled 730 thousand. In 2008 the number of attacks on U.S. Department of Defence's servers rose by 46%. The Department of State estimates that its computer system faces 6 million attacks daily. It is essential to note that typical terrorist groups are just one of these sources. An attack may also come from the "rogue states" or others having certain political aim (such as China, Russia or Cuba), terrorism sympathizers, or individual hackers wanting to demonstrate their skills or making the life of state institutions, politicians and companies unbearable.
The Internet and teleinformatic systems are also applied eagerly by governments, armies, and secret service of numerous countries for so-called cyber spying. In the eighties hackers from West Germany, under orders from the KGB, copied secret data from the servers of the U.S. Department of Defence. During the war in Kosovo in 1999 American secret service led an operation codenamed "Matrix", which aimed at paralyzing electronic and telephone systems in Serbia. In retaliation, Serbian hackers blocked NATO servers[34]. The same year Russian cyber spies stole, probably from American government servers, secret information about U.S. missiles guiding systems. But the most famous spying operation in global network was the "Titan Rain" operation conducted from 2003 to 2005 by Chinese hackers under orders from the Chinese army. The hackers combed through the networks of Lockheed Martin, Sandia National Laboratories and NASA. From June to August 2007 Germany, Great Britain, France, and New Zealand were the probable victims of the Chinese army[35].

All the attacks were conducted by means of computer technologies that share certain common features that may determine their increase in the near future:

- Firstly – they are extremely difficult to track down. The one ordering an attack may hire executors from other countries or conduct them from a nearby internet café.
- Secondly – people conducting the attacks enjoy a high degree of anonymity[36].
- Thirdly – a great firepower. A former FBI chief Jim Settle said once "give me 10 hackers and in 90 minutes I will bring this country (USA) down"[37].
- Fourthly – an immense ease of conducting the attacks. The weaker states may pose a substantial danger to military and economic superpowers.
- Fifthly – low costs of the enterprise. Small software downloaded from the Internet for a few dollars may suffice. At present, according to experts, there are more than sixty-eight thousand (!) programmes on-line which might serve potential cyber terrorists.

Estonia as a victim of cyber terrorism

"(…) The lights (…) suddenly go out… The Internet, too, is down… the banks are closed and the ATMs aren't working. The streets are jammed… Radio and TV stations aren't broadcasting. The telephone and Internet still aren't working… The airports and train stations have closed. After a long, restless night, morning comes… People are beginning to panic, and local law enforcement can't restore order… People's life savings are out of reach and worthless. The only things of value now are gasoline, food and water…"[38].
This is by no means the scenario of a horror film but a quote from a speech by Sami Saydjari, head of the Professionals for Cyber Defense, which he gave in front of the Committee on Internal Security of the U.S. House of Representatives in April 2007. Saydjari's statement took place few days before the events which turned the world's attention to the dangers coming from cyberspace. From April 27 to May 11, 2007, Estonia was the victim of cyber attacks. The riots started after the decision of the Estonian government to relocate the monument commemorating the Red Army soldiers (the so-called Bronze Soldier). The computer and telephone networks of the country were brought to a standstill.
It is worth mentioning that Estonia is often called "E-stonia" for its high level of computerization. More than 90% of bank transactions are done on-line. It is possible to file tax forms on-line. Every citizen possesses a digital ID which even enables voting on the Internet. The Estonian government has implemented "e-valitsus" (e-state) system which facilitates the process of developing a country's information technologies. The cabinet itself uses computers for maintaining contacts, and all the government files are accessible on-line. This shortens

hours of work and increases efficiency[39]. All these factors caused the Estonian computer infrastructure to be a perfect target for cyber attacks. At the peak time, on May 9, the day Russia celebrates Victory Day, online traffic on the Estonian websites increased by twenty times. The most spectacular ten attacks were more than 90 Mb/s strong and they lasted continuously for ten hours. The government's, the president's chancellery, and the main newspapers' sites were blocked. The banking systems and the internal network of the police broke down as well. Estonians were cut off from any information on the Internet, and worse, from their banks and their money[40]. The functioning of the state administration, to a large extent computerized, was put into question. According to the Estonian Defence Minister Jaak Aaviksoo, *"it is the first time cyber attacks have created a serious threat to the nation's security"*[41]. Estonian government was even considering the application of the Washington Treaty, article 5, on mutual assistance of NATO members in case an attack on the territory of one of them should occur.
It is impossible to determine who is responsible for the April attacks in Estonia. As mentioned before, it is extremely difficult to locate who ordered and conducted the cyber attacks. The analyses have shown that part of computers which were used for the attacks came from Egypt, Vietnam and Peru. The fact is that due to various historic reasons, Russia might have been interested in conducting such an attack. For the Russians, the monument of the Bronze Soldier was a homage paid to the soldiers of the Red Army who liberated the Baltic States from German occupation in 1944. For the Estonians the monument was a symbol of the long Soviet occupation of their territory.

Reactions to the threat of cyber terrorism

The events in Estonia urged many countries and governments to work on a concept of protection from threats of cyber terrorism. The U.S. has created the National Cyber Security Centre in the Department of Homeland Security. Recently the Department, together with the National Security Agency, has introduced a unit composed of two thousand specialists who are to work on the defence mechanisms and also on developing their own capabilities of conducting such attacks[42]. The U.S. has also set up the Air Force Cyber Command to defend against attacks in cyber space and train the army on these types of tasks[43].
The Comprehensive Political Guidance adopted during the NATO summit in Riga in 2006 assumed the development of "skills of defending the information systems of crucial importance to the Alliance against cyber attacks"[44]. A year after the events in Estonia, in May 2008, NATO opened the Cooperative Cyber Defence Centre of Excellence in Tallinn. The centre will conduct research and will support the preparation of the member states to defend themselves against cyber attacks. Among thirty employees, more than a half comprises specialists from the countries who signed the document creating the Centre – from Estonia, Lithuania, Latvia, Germany, Spain, Italy and Slovakia[45]. The will of accession was also expressed by Turkey and the U.S. The Centre officially began work at the beginning of January 2009. Fulfilling the resolutions of the Paris Protocol from 1952, NATO granted the Centre the status of an international security organization[46].
Estonia, who has herself been a victim of numerous cyber attacks, accepted a comprehensive Estonian Cyber Security Strategy on May 8, 2008[47]. The document, formulated as a joint effort of a few ministries, is the first step towards ensuring an effective defence policy against cyber terrorism. The strategy is based on five main assumptions: an increase in the means of defence against cybernetic threats, paying particular attention to government institutions and critical infrastructure; strengthening the skills in the area of information security; creating adequate legal binds; supporting the international cooperation; and finally disseminating the knowledge on potential dangers in networks among society[48].
An informal meeting of defence ministers of NATO member states which took place in February 2009 in Krakow was the last one in that format before the April anniversary summit in Strasburg/Kehl. The words by Jaap de Hoop Scheffer signalling the implementation of a cyber terrorism threat and computer security into the already prepared new strategic concept of NATO somehow went unnoticed. At the conference organized by the Krakow Institute of Strategic Studies, Scheffer indicated that the Alliance cannot remain indifferent towards unconventional threats such as cyber terrorism, piracy, and also the implications of climate change or energy security. The secretary general was perfectly right when he said that "cyber attacks do not require a single soldier or territory encroaching – but they can paralyze a country's functioning[49].
It seems that the new strategic concept of the Alliance will be a step forward, and the member states will start working on creating national strategies of prevention and combat of these threats. Even so the new NATO concept should give a concrete definition of cyber terrorism which may serve as a starting point in preparing further documents and strategies. Celebrating its 60th anniversary, NATO must unambiguously describe its role and tasks in the context of IT security and ensure that the concept of Alliance's solidarity will apply also in the case of the cyber terrorism threat.

Cyber terrorism in the context of Poland

What is the Polish perspective here? Despite the fact that Poland is not as computerized as Estonia or other Western states, one can assume that the country may

become a target of cyber attacks in the near future. Why?

- First of all, the percentage of Internet users in the Polish society has been constantly growing. Between 2000 and 2008 the number of users grew by 4.2%. The Internet Word Stats indicates that in Poland there are around 16 million users registered, which accounts for 41.6% of the whole population[50]. Poland is listed within the first ten countries with the largest number of Internet users, just behind Germany, Great Britain, France, Italy, and Spain. This is going to rise in the nearest years.
- Secondly, a considerable percentage of Poles use bank accounts and mobile phones through the Internet. Practically every bank in Poland has access to its online services on their offer. According to a report by the Rada Bankowości Elektronicznej (the E-Banking Council) of the Polish Bank Association, the number of customers using e-banking has exceeded 11 million already, where 6.4 million comprise active customers (have conducted at least four payment transactions). The Council predicts that the rise in this group will reach 10 million by 2010[51].
- Thirdly, the critical technical infrastructure of Poland (state administration, services, military, transport, and energy sector) is already computerized, perhaps still not to such a degree as the world standards would indicate. Poland's computerization will further develop due to "A strategy of information society development in Poland until 2013" drawn up by the Ministry of Interior.
- Fourthly, Poland as a participant of the operation in Iraq and Afghanistan is a possible target of the terrorist groups who may conduct a cyber attack. The probability is high enough as groups such as Al-Qaida understand the possibilities of using cyber weapon in achieving their goals[52].
- Fifthly, relations between Poland and Russia have not been the best recently. Russia is one of the main suspects of using cyber spying and cyber terrorism[53]. This refers both to secret service and private hackers. One can assume that in case the relations should worsen between the two countries, there might be attempts to attack Polish critical infrastructure as it took place in Estonia.
- Sixthly, Poland, like any other country, is exposed to cyber spying from foreign intelligence agencies. Affected by this are state administration, state and private companies. Even so, since 1996 the incidents where the teleinformatic network was applied have been increasing in Poland[54].

Recommendations for Poland

Considering the above arguments and the development of the international situation, it is surprising that Poland has not worked out a strategy to prevent and fight cyber terrorism and the many attendant threats coming from cyber space. Including a chapter referring to Information and Telecommunication Security (par. 3.8) in the National Security Strategy from 2007 is a step forward[55]. The National Security Bureau (Biuro Bezpieczeństwa Narodowego – BBN) is preparing a team of experts on cyber terrorism. It is the BBN that would be a place of meetings for the representatives of the ministries of interior, national defence and finance, and experts on state security [56] . The creation of the Computer Emergency Readiness Team (CERT) within the Department of Tele-information Security in ABW (Agencja Bezpieczeństwa Wewnętrznego – Internal Security Agency) on February 1, 2008, was also a good step forward. This is a positive sign, but still the following seem to be essential:

- Creating a separate, coherent and effective strategy of prevention and defence against cyber terrorism following the example of the Estonian Computer Security Strategy.
- Harmonizing Polish legislation on computer security.
- Creating a centralized government unit (a certain anti-crisis centre) monitoring the situation in the country and abroad and coordinating the activities of an institution in case of crisis.
- Creating units to deal with the problems of infrastructure security in individual units of state and local administration or give such competences to local units of civil defence.
- Participation of Polish computer security experts in the works of the NATO Cyber Defence Centre,
- Supporting scientific research on computer security.
- Disseminating knowledge on potential threats coming from Internet by government institutions and NGOs.
- Intensifying the international cooperation with institutions working on defence against cyber terrorism.

Changing the attitudes of politicians and ordinary users of the Internet towards all the threats coming from cyber space seems to be the most important. Without understanding the scale and results of potential threats it is impossible to work out an effective strategy for fighting cyber crimes and cyber terrorism.

Article translated by Justyna Pado

* * * * *

Marcin Łapczyński – expert of the Casimir Pulaski Foundation, graduated from the Institute of International Relations of the University of Warsaw (specializing in security and strategic studies). He also studied at the University of Vilnius and the Moscow

State Institute of International Relations (MGIMO). He is currently continuing his studies at the Central European University in Budapest. He works on the issues of international security, the Baltic States, Russia and the post-Soviet region.

The Casimir Pulaski Foundation is an independent, non-partisan institution with a mission to promote freedom, equality and democracy as well as to support actions of strengthening civil society. The foundation carries out activities both in Poland and abroad, among others in Central and Eastern Europe and in North America.

The Casimir Pulaski Foundation was founded due to political changes that took place in Poland after 1989. The principal values of Casimir Pulaski (freedom, justice and democracy) are an inspiration for every initiative undertaken by the Foundation. A few of the Foundations activities include: conducting scientific research, preparing publications and analyses, organizing seminaries and conferences, providing education and support for leaders www.instytutprzywodztwa.pl

The Foundation is the main organizer of the Warsaw Regional NGOs Congress www.warsawcongress.pl, the Academy of Young Diplomats www.akademia.diplomacy.pl and publisher of the Communication Platform for Non-Governmental Organizations www.non-gov.org

The Foundation also awards the Casimir Pulaski Prize "The Knight of Freedom" to outstanding people who have made a significant contribution in promoting democracy. So far the prizewinners were: professor Władysław Bartoszewski, former minister of foreign affairs of Poland, historian professor Norman Davies, Alaksandar Milinkiewicz, leader of democratic opposition in Belarus and Lech Wałęsa, former President of Poland.

The Casimir Pulaski Foundation is one of only two Polish institutions that have a partnership status with the Council of Europe. More about Foundation at: www.pulaski.pl

Pulaski Policy Papers are analyses of foreign policy, international economy and domestic politics issues, essential for Poland. The papers are published both in Polish and English. Researchers willing to publish new articles in Pulaski Policy Papers are asked to contact the Chief Editor Mr Dominik Jankowski djankowski@pulaski.pl If you would like to receive new issues of PPP please add your e-mail at www.pulaski.pl

Przypisy końcowe / Endnotes

[1] *The Vulnerability of the Computerized Society* - Considerations and Proposals' Report by a Swedish Government Committee (ADB och samhällets sårbarhet, övervaganden och forslag, Sårbarhetskommiteé), Stockholm 1979; A. Adamski, *Cyberterroryzm,* [w:] V. Kwiatkowska-Darul (red.), „Terroryzm. Materiały z sesji naukowej. Toruń 11.04.2002 r.", Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika w Toruniu.

[2] P. Sienkiewicz, H. Świeboda, E. Lichocki, *Analiza systemowa zjawiska cyberterroryzmu,* Akademia Obrony Narodowej, http://www1.aon.edu.pl/zen2/index.php?option=content&task=view&id=571 (12.09.2008).

[3] Ibidem

[4] D. E. Denning, *Cyberterrorism,* Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives, 23.05.2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[5] V. Mitliaga, *Cyber-terrorism: A Call for Governmental Action?,* British and Irish Law, Education and Technology Association 16th Annual Conference, Edynburg, 9-10.04.2001, http://www.bileta.ac.uk/01papers/mitliaga.html, s. 5.

[6] D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool For Influencing Foreign Policy,* [w:] J. Arquilla, D. Ronfeldt (red.), *Networks and Netwars: The future of terror, crime and militancy,* Santa Monica 2001, s. 268.

[7] *Merkel Calls on China to Respect International Rules*, Serwis Internetowy Deutsche Welle z 27.08.2007 r., http://www.dw-world.de/dw/article/0,2144,2753209,00.html.

[8] T. Shimeall, P. Williams, C. Dunlevy, *Countering New Cyber War*, "NATO Review", Winter 2001/2002, http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf, s. 17-18.

[9] B. Gagnon, *Are We Headed for a "Cyber-9/11?": The American Failure in Cyberstrategy,* Center for United States Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, Occasional Paper nr 5, Quebec 2004, http://www.dandurand.uqam.ca/download/pdf/articles/cyber911.pdf, s. 3.

[10] *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action,* Testimony of Sami Saydjari Before the House Committee on Homeland Security 25.04.2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf, s. 1.

[11] Patrz: E-Eesti/E-Estonia, http://web-static.vm.ee/static/failid/286/E-Estonia_uus.pdf.

[12] *Rosyjscy hackerzy podbijają Estonię*, „Gazeta Wyborcza", 17.05.2007, http://gospodarka.gazeta.pl/technologie/1,81010,4140556.html.

[13] J. Davis, *Hackers Take Down the Most Wired Country in Europe,* „Wired Magazine", 15.09.2007,

http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[14] *World War III. A Cyber War has begun*, Raport The Technolytics Institute, September 2007, www.technolytics.com/Cyber_War_Released.pdf, s. 2.

[15] C. Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Congressional Report Service' Report for Congress, 20.03.2007, www.fas.org/sgp/crs/natsec/RL31787.pdf, s. 8-9.

[16] J. Ryan, *"iWar": A new threat, its convenience – and our increasing vulnerability*, "NATO Review", Winter 2007, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

[17] *Defence Policies '07 in Brief: Estonia, Latvia and Lithuania*, "Baltic Security and Defense Review", vol. 10, 2008, www.bdcol.ee/files/files/documents/Research/12_%20%20Defence%20Policy.pdf, s. 262.

[18] Cooperative Cyber Defence Centre of Excellence International Status, http://www.ccdcoe.org/38.html

[19] Estonian Cyber Security Strategy, MON Estonii, http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.

[20] *Estonian approach to Cyber Security: Estonian National Strategy on Cyber Security and Cooperative Cyber Defence Centre of Excellence,* Przemówienie ministra obrony Jaaka Aaviksoo na forum OBWE, 4.07.2008, http://www.mod.gov.ee/?op=body&id=494&prn=1.

[21] *Nowe NATO rodzi się w Krakowie,* Gazeta Wyborcza, 19.02.2009, http://wyborcza.pl/1,76842,6297288,Nowe_NATO_rodzi_sie_w_Krakowie.html.

[22] Internet World Stats 2008, http://www.internetworldstats.com/europa.htm#pl.

[23] *Z bankowości elektronicznej korzysta już ponad 11 milionów użytkowników*, „Gazeta Prawna", 16.10.2008, s. 8.

[24] D. Verton, *Black Ice - niewidzialna groźba cyberterroryzmu*, Helion 2004, s. 81.

[25] D. E. Denning, *Is Cyber Terrorism Coming?,* Prezentacja w Naval Postgraduate School, Center of Terrorism and Irregular Warfare, Monterey, 2.05.2002, http://handle.dtic.mil/100.2/ADA485000.

[26] Raport CERT Polska za 2007 rok, http://www.cert.pl/PDF/Raport_CP_2007.pdf, s. 13.

[27] Strategia Bezpieczeństwa Narodowego RP 2007, http://www.bbn.gov.pl/dokumenty/SBN_RP.pdf.

[28] *Polska chce walczyć z cyberterroryzmem*, Gazeta.pl Gospodarka 20.12.2007, http://gospodarka.gazeta.pl/gospodarka/1,33181,4779921.html.

[29] *The Vulnerability of the Computerized Society* - Considerations and Proposals' Report by a Swedish Government Committee (ADB och samhällets sårbarhet, övervaganden och forslag, Sårbarhetskommiteé), Stockholm 1979; A. Adamski, *Cyberterroryzm,* [w:] V. Kwiatkowska-Darul (red.), "Terroryzm. Materiały z sesji naukowej. Toruń 11.04.2002 r.", Publishing house *Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika* in Toruń.

[30] P. Sienkiewicz, H. Świeboda, E. Lichocki, *Analiza systemowa zjawiska cyberterroryzmu,* the National Defense Academy, http://www1.aon.edu.pl/zen2/index.php?option=content&task=view&id=571 (12.09.2008).

[31] Ibidem.

[32] D. E. Denning, *Cyberterrorism,* Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives, 23.05.2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[33] V. Mitliaga, *Cyber-terrorism: A Call for Governmental Action?,* British and Irish Law, Education and Technology Association 16th Annual Conference, Edynburg, 9-10.04.2001, http://www.bileta.ac.uk/01papers/mitliaga.html, s. 5.

[34] D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,* [w:] J. Arquilla, D. Ronfeldt (ed.), *Networks and Netwars: The future of terror, crime and militancy,* Santa Monica 2001, p. 268.

[35] *Merkel Calls on China to Respect International Rules*, On-line news service: Deutsche Welle z 27.08.2007 r., http://www.dw-world.de/dw/article/0,2144,2753209,00.html.

[36] T. Shimeall, P. Williams, C. Dunlevy, *Countering New Cyber War*, "NATO Review", Winter 2001/2002, http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf, p. 17-18.

[37] B. Gagnon, *Are We Headed for a "Cyber-9/11?": The American Failure in Cyberstrategy,* Center for United States Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, Occasional Paper no. 5, Quebec 2004, http://www.dandurand.uqam.ca/download/pdf/articles/cyber911.pdf, p. 3.

[38] *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action,* Testimony of Sami Saydjari before the House Committee on Homeland Security 25.04.2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf p. 1.

[39] See: E-Eesti/E-Estonia, http://web-static.vm.ee/static/failid/286/E-Estonia_uus.pdf.

[40] *Rosyjscy hackerzy podbijają Estonię*, „Gazeta Wyborcza", 17.05.2007, http://gospodarka.gazeta.pl/technologie/1,810104,4140556.html.

[41] J. Davis, *Hackers Take Down the Most Wired Country in Europe,* "Wired Magazine", 15.09.2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[42] *World War III. A Cyber War has begun*, Report of the Technolytics Institute, September 2007, www.technolytics.com/Cyber_War_Released.pdf, s. 2.

[43] C. Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Congressional Report Service' Report for Congress, 20.03.2007, www.fas.org/sgp/crs/natsec/RL31787.pdf, p. 8-9.

[44] J. Ryan, *"iWar": A new threat, its convenience – and our increasing vulnerability*, "NATO Review", Winter 2007, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.
[45] *Defence Policies '07 in Brief: Estonia, Latvia and Lithuania*, "Baltic Security and Defense Review", vol. 10, 2008, www.bdcol.ee/files/files/documents/Research/12_%20%20Defence%20Policy.pdf, p. 262.
[46] Cooperative Cyber Defence Centre of Excellence International Status, http://www.ccdcoe.org/38.html
[47] Estonian Cyber Security Strategy, National Defense Ministry of Estonia, http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
[48] *Estonian approach to Cyber Security: Estonian National Strategy on Cyber Security and Cooperative Cyber Defence Centre of Excellence,* a speech by defense minister, Jaak Aaviksoo, during the OSCE conference, 4.07.2008, http://www.mod.gov.ee/?op=body&id=494&prn=1.
[49] *Nowe NATO rodzi się w Krakowie,* Gazeta Wyborcza, 19.02.2009, http://wyborcza.pl/1,76842,6297288,Nowe_NATO_rodzi_sie_w_Krakowie.html.
[50] Internet World Stats 2008, http://www.internetworldstats.com/europa.htm#pl.
[51] *Z bankowości elektronicznej korzysta już ponad 11 milionów użytkowników*, „Gazeta Prawna", 16.10.2008, p. 8.
[52] D. Verton, *Black Ice - niewidzialna groźba cyberterroryzmu*, Helion 2004, p. 81.
[53] D. E. Denning, *Is Cyber Terrorism Coming?,* Presentation in the Naval Postgraduate School, Center of Terrorism and Irregular Warfare, Monterey, 2.05.2002, http://handle.dtic.mil/100.2/ADA485000
[54] A report by CERT Poland for 2007, http://www.cert.pl/PDF/Raport_CP_2007.pdf, p. 13.
[55] National Defense Strategy of Poland, 2007, http://www.bbn.gov.pl/dokumenty/SBN_RP.pdf.
[56] *Polska chce walczyć z cyberterroryzmem*, Gazeta.pl Gospodarka 20.12.2007, http://gospodarka.gazeta.pl/gospodarka/1,33181,4779921.html.

REKLAMA

V POLSKO-NIEMIECKIE FORUM GOSPODARCZE

KOLONIA - WARSZAWA

V Polsko-Niemieckie Forum Gospodarcze to piąta edycja międzynarodowego projektu organizowanego przez studentów Uniwersytetu w Kolonii oraz Szkoły Głównej Handlowej w Warszawie. Odpowiedzialność za organizację Projektu wzięły na siebie Studenckie Koło Naukowe Współpracy Europejskiej oraz Kölner Verein für Europäische Zusammenarbeit e.V.

Projekt składa się z dwóch części: niemieckiej, która odbędzie się w dniach 22-26 kwietnia 2009r. w Kolonii i Frankfurcie nad Menem oraz części polskiej zaplanowanej na 6-10 maja 2009r. w Warszawie. Projekt obejmuje część merytoryczną składającą się z prelekcji w języku angielskim i niemieckim oraz część kulturalną służącą integracji między studentami.

6 MAJA 2009 (ŚRODA) PRZYLOT UCZESTNIKÓW

7 MAJA 2009 (CZWARTEK) SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE,
Wyzwania polityki zagranicznej wobec zmieniającej się sytuacji na arenie międzynarodowej.
AMBASADA NIEMIEC W WARSZAWIE

8 MAJA 2009 (PIĄTEK) GIEŁDA PAPIERÓW WARTOŚCIOWYCH W WARSZAWIE
Funkcjonowanie rynku kapitałowego w dobie światowego kryzysu.

9 MAJA 2009 (SOBOTA) WIZYTA W PARLAMENCIE RP ORAZ ZWIEDZANIE WARSZAWY

10 MAJA 2009 (NIEDZIELA) WYLOT UCZESTNIKÓW

SPONSORZY I PARTNERZY

PATRONI MEDIALNI