Sławomir WIERZBICKI[1]

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach[2]

Instytut Nauk Społecznych i Bezpieczeństwa

s.wierzbicki@wp.mil.pl

WOJNY CYBERNETYCZNE JAKO ELEMENT NIEKONWENCJONALNEJ KONFRONTACJI MIĘDZYPAŃSTWOWEJ. PRAGMATYCZNA RZECZYWISTOŚĆ, NIEUNIKNIONA PRZYSZŁOŚĆ

ABSTRAKT: Celem niniejszego artykułu jest zbadanie zjawiska wojny cybernetycznej, jako elementu niekonwencjonalnej konfrontacji międzypaństwowej we współczesnych stosunkach międzynarodowych. Konstrukcja niniejszej pracy, podyktowana próbą osiągnięcia odpowiedzi na powyższy temat badawczy, sprowadziła autora do przyjęcia następującej struktury. W pierwszej części pracy, przedstawiono rozwój sprzętu komputerowego i sieci informatycznych wespół z uwidocznieniem znaczenia cyberprzestrzeni. Następnie, opisano uwarunkowania teoretyczne przedmiotowej problematyki, w szczególności podstawowe determinanty, kategorie ataków z sieci oraz ich klasyfikacje. W dalszej kolejności, ukazano praktyczne aspekty zastosowania powyższych ataków biorąc za punkt widzenia konkretne casusy tj. Kosowa, Chin, Estonii, Gruzji oraz Iranu. Na koniec zaś poddano pod rozwagę cyberwojny poruszając różnice i podobieństwa oraz płynące z nich wnioski na przyszłość.

SŁOWA KLUCZOWE: cyberwojna, cyberprzestrzeń, bezpieczeństwo, internet, Kosowo, Chiny, Estonia, Gruzja, Iran

CYBERWAR AS AN ELEMENT UNCONVENTIONAL INTERSTATE OF CONFRONTATION. PRAGMATIC REALITY, INEVITABLE FUTURE

ABSTRACT: The aim of this article is to examine the phenomenon of cyber warfare as part of an unconventional confrontation between states in contemporary international relations.

[1] Mgr Sławomir Wierzbicki, doktorant Instytutu Nauk Społecznych i Bezpieczeństwa Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Prace magisterską na temat: *Neokonserwatyzm w kształtowaniu polityki bezpieczeństwa USA w latach 2001-2009* obronił w 2014 r. Pełnił funkcję zastępcy redaktora naczelnego uczelnianego czasopisma: „Kuryer Uniwersytecki". Kierował *Studenckim Kołem Naukowym Bezpieczeństwa Narodowego*. Przebywał na wyjeździe studyjnym (projekt) w *Permanent Mission of the Republic of Poland to the United Nations Office and the International Organizations in Vienna.* Uczestnik projektu realizowanego przez konsorcjum naukowo-przemysłowe w zakresie obronności i bezpieczeństwa państwa: *System Bezpieczeństwa Narodowego RP*. Obecnie pracownik Wojskowego Centrum Edukacji Obywatelskiej. Obszar badawczy: systemy bezpieczeństwa międzynarodowego; transatlantycki system bezpieczeństwa; polityka zagraniczna i bezpieczeństwa USA, ZSRR, Federacji Rosyjskiej; geopolityka Europy Środkowej i Wschodniej; integracja europejska.

[2] Siedlce University of Natural Sciences and Humanities, Social Science and Security.

The construction of this study, dictated by an attempt to achieve a response on the above research subject, brought the author to adopt the following structure. The first part of the work presents the development of computer hardware and networks together with visualizing the cyberspace importance. Next, the conditions of this theoretical issues, in particular, the basic determinants categories of network attacks and their classifications are presented. Further, the practical aspects of the application of those attacks are shown, taking a point of view specific casus i.e. Kosovo, China, Estonia, Georgia and Iran. At the end, the cyberwars were under consideration including the differences, similarities and lessons learned for the future.

KEY WORDS: Cyberwar, cyberspace, security, internet, Kosovo, China, Estonia, Georgia, Iran

WPROWADZENIE

Nie będzie nadużyciem nazwanie obecnych czasów epoką informacji. Technologia rozwija się w coraz szybszym tempie. Rozwój gospodarczy spowodował przyrost środków finansowych przez co stało się możliwe znacznie lepsze finansowanie nauki. Wpłynęło to na rozwój ośrodków naukowych zajmujących się wybranymi dziedzinami. Nauka, która dawniej była finansowana przez państwo lub w niektórych dziedzinach przez kościół, obecnie stała się również dobrem dostępnym dla każdego, który odważy się ją rozwijać.

Dynamiczny rozwój doprowadził do powstania pierwszych komputerów, a w 1969 r. uruchomienia pierwszej zdecentralizowanej sieci, którą wykorzystywało wojsko oraz instytucje naukowe. *Sensu largo* zrodził się ARPANET (*Advanced Research Projects Agency Network*), pierwowzór obecnego internetu. Jednakże pełne wykorzystanie możliwości, jakie niósł za sobą powyższy postęp technologiczny, nastąpił dopiero w ostatniej dekadzie XX w. Współcześnie internet jest synonimem swobodnej wymiany informacji zarówno tej legalnej, jaki i bezprawnej, a wiedza stała się ogólnodostępna[3].

Tak zarysowany informacyjny postęp mający swoje zalety, doprowadził również do powstania nowych zagrożeń. Zaistniałą sytuację potęguje już nie tylko pobieranie nauki informatyki w szkołach. Precyzyjniej ujmując, wystarczy być indywidualnym dysponentem komputera, aby samodzielnie zdobyć wirtualną wiedzę. Ponadto istotnym czynnikiem stała się integracja coraz większej liczby elementów z dnia codziennego. Technologia zaś taka jak komputer wraz z siecią, początkowo dostępna tylko dla państwa, stała się tak popularna, że kwestią czasu pozostawało wykorzystywanie jej w celach destruktywnych. Obecnie coraz bardziej powszechnym zajwiskiem są proste cyberataki, a problem bezpieczeństwa cyfrowego nie jest już publiczną tajemnicą, *a fortiori* przyszłością. Problem ten w sposób ewolucyjny będzie się stale nasilać.

Celem autora nie jest wyczerpanie tematu, a jedynie subiektywne wyeksponowanie zjawiska wojny cybernetycznej, nabierającej rozpędu i znaczenia w obecnych oraz przyszłych konfliktach zbrojnych. Uzmysłowienie powagi sytuacji, jak również możliwego scenariusza „cybernetycznego Pearl Harbor", wymogło na autorze konieczność przybliżenia dotychczaso-

[3] Do powyższych refleksji skłonił autora: A. Bojczuk, *Internet: agresja i ochrona*, Wrocław 1998, s. 29-35.

wego bilansu związanego z areną wirtualnych pól bitewnych i poddania ich pod prognostyczną refleksję.

UWARUNKOWANIA PROBLEMATYKI W SFERZE TEORETYCZNEJ

Wojna cybernetyczna podobnie jak cyberterroryzm jest coraz częściej wybieraną metodą walki we współczesnych konfrontacjach międzypaństwowych. Samo zjawisko przeniesienia ataków do strefy cyberprzestrzeni daje się stosunkowo łatwo wyjaśnić. Po pierwsze najważniejszym powodem jest cena przeprowadzenia takiego ataku. Niejednokrotnie w takiej operacji jedynymi kosztami jakie może ponieść atakujący to cena za zakup sprzętu komputerowego. Po drugie w przypadku powyższych ataków możliwe jest przeprowadzenie jej z każdego miejsca na ziemi. Innymi słowy, zanikają jakiekolwiek granice, państwowe oraz organizacyjne. I wreszcie, jeżeli sprzęt komputerowy ofiary nie jest dostępny bezpośrednio z sieci, to można wtedy przeprowadzić atak za pomocą umiejętności socjotechnicznych. Jak diagnozuje jeden z największych i najbardziej rozpoznawalnych przestępców branży komputerowej, Kevin Mitnick: „popularne jest powiedzenie, że bezpieczny komputer to wyłączony komputer. Zgrabne, ale nieprawdziwe: oszust po prostu namawia kogoś do pójścia do biura i włączenia komputera”[4].

W wojnie cybernetycznej, jak w każdej innej wojnie na podłożu konwencjonalnym, zasadniczym pytaniem, stawianym przez planistów, jest pytanie o cel ataków. Zgodnie z klasyfikacją sporządzoną w raporcie pt. *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* , czytamy: „Bezprawny atak (lub groźba ataku) na komputery, sieci oraz informacje w nich zawarte, ukierunkowane na zastraszenie, lub zmuszenie rządu oraz społeczeństwa w celu osiągnięcia korzyści politycznych oraz społecznych”[5].

Zgodnie z powyższym można wywnioskować, że nie chodzi *stricte* o ataki przeprowadzane na same systemy, ale również na konkretny sprzęt. Wobec tego można zastosować następujący podział przeprowadzanych ataków:

- w sferze materialnej – atak na sprzęt komputerowy (*hardware*);
- w cyberprzestrzeni – atak na oprogramowanie (*software*).

Jednocześnie w literaturze przedmiotu wskazuje inny, dodatkowy podział[6]:

- kategoria I – użycie technologii w tradycyjny sposób: komunikacja, zbieranie informacji, zdobywanie środków finansowych;
- kategoria II – użycie starych technik przeciw infrastrukturze teleinformatycznej. Będzie to użycie np. siły fizycznej przeciw sprzętowi komputerowemu;

[4] K. Mitnick, W. Simon, *Sztuka podstępu: łamałem ludzi, nie hasła,* Gliwice 2003, s. 24.

[5] “Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives”. C. Wilson, *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilitiesand Policy Issues for Congress,* http://wlstorage.net/file/crs/RL32114.pdf, s. 8. (12.06.2015).

[6] *Vide:* A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym* świecie, Warszawa 2003, s. 139.

– kategoria III – użycie technologii w celu niszczenia jej samej, np. ataki za pomocą wirusów.

Kategoria pierwsza nie jest tematem niniejszego opracowania, z tego względu nie będzie analizowana. Tymczasem kategoria druga wyraźnie akcentuje, że ataki na sprzęt są prowadzone metodami starymi. Jest to rozwiązanie niewymagające wiedzy informatycznej. Względem przeszłości zaszła jedynie zmiana celów. Rozpatrując przypadki tego typu ataków, konieczne jest rozważenie ich pod względem metod „tradycyjnych”[7]. Rozwijając tematykę klasyfikacji ataków powstała próba pogrupowania ich wedle kategorii[8]:

– *stealing passwords* (kradzież hasła) – zbiór metod, których celem jest zdobycie hasła do systemu;
– *social engineering* (inżynieria społeczna) – wykorzystywanie słabości czynnika ludzkiego, manipulacje;
– *bugs and backdoors* (błędy oraz tzw. tylnie drzwi) – wykorzystywanie błędów w oprogramowaniu;
– *authentication failures* (błędy w autoryzacji) – wykorzystywanie oraz łamanie systemów autoryzujących;
– *protocol failures* (błędy w protokołach) – wykorzystywanie błędów w protokołach komunikacyjnych – zbiorach reguł, które są wykorzystywane przez programy do komunikacji między sobą;
– *information leakage* (wyciek informacji) – bezprawne zdobycie dostępu do informacji, które są niezbędne do funkcjonowania sieci;
– *denial of service* (odmowa usługi/wyczerpanie usługi) – uniemożliwienie korzystania z serwisu przez przepełnienie zasobów, np. serwera.

Należałoby również wymienić podział ze względu na skutek, jaki atakujący zamierzają osiągnąć[9]:

– *corruption* (uszkodzenie) – bezprawna zmiana informacji;
– *leakage* (wyciek) – wydostanie się informacji do miejsc jej nieprzeznaczonych;
– *denial* (odmowa) – spowodowanie niedostępności sieci, maszyny lub programu.

Znacznie precyzyjniejszą klasyfikację ataków dokonuje Neumann i Parker[10]:

– *external information theft* (kradzież informacji zewnętrznej) – kradzież informacji przez osobę niezwiązaną np. z firmą;

[7] Warto odnotować, że w latach 70. ubiegłego wieku Czerwone Brygady dokonały ataków na firmy komputerowe, z przekonaniem, że niszczą serce państwa. Równocześnie za inny przejaw agresji z wykorzystaniem metod tradycyjnych można uznać casus paraliżu japońskiego przypisywanemu grupie „Frakcji Środka”. Liderzy siatki doprowadzili do poważnych uszkodzeń infrastruktury energetycznej państwa oraz awarii telefonicznego systemu sterowania ruchem kolejowym. Szacuje się, że na skutek ataków około 6,5 miliona obywateli japońskich doświadczyło trudności logistycznych w poruszaniu się po kraju. Głównym celem, który przyświecał Frakcji Środka była chęć okazania solidarności ze strajkującymi kolejarzami oraz demonstracja sprzeciwu wobec prywatyzacji kolei. *Vide:* R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku,* Warszawa 2011, s. 59.

[8] Do powyższych wniosków skłonił autora: A. Bógdał-Brzezińska, M.F. Gawrycki, *op. cit.*, s. 142-144.

[9] *Ibidem.*

[10] *Ibidem.*

- *external abuse of resources* (zniszczenie sprzętu) – uszkodzenie nośników danych;
- *masquerading* (udawanie) – podanie się za inną osobę;
- *pest programs* (wirusy) – infekcja złośliwym oprogramowaniem;
- *bypassing authentication or authority* (omijanie zabezpieczeń autoryzujących) – łamanie haseł;
- *authority abuse* – nadużycia władzy (na przykładzie fałszowania danych);
- *abuse through inaction* (szkoda przez zaniechanie) – świadome niewłaściwe zarządzanie;
- *indirect abuse* (nadużycia pośrednie) – użycie programów trzecich do stworzenia złośliwego oprogramowania.

W ogólnym rezultacie klasyfikacja Neumanna oraz Parkera mogłaby się zdawać poprawną. Choć trzeba pamiętać, że takie orzecznictwo należałoby postawić dopiero w momencie, gdy kategorie zostaną ze sobą połączone w jednolitą całość. W przeciwnym wypadku klasyfikacja ataku mogłaby stać się niemożliwa, ponieważ często łączy się ze sobą kilka metod ataków.

UWARUNKOWANIA PROBLEMATYKI W SFERZE PRAKTYCZNEJ

CASUS KOSOWA Z 1999 ROKU

Najogólniej biorąc, ataki cybernetyczne w Kosowie rozpoczęły się jeszcze przed operacją Allied Forces zorganizowaną przez siły Sojuszu Północnoatlantyckiego (*North Atlantic Treaty Organization* – NATO) w marcu 1999 r. W październiku 1998 r. serbska grupa Black Hand dokonała ataków na albańską witrynę internetową oraz groziła kolejnymi atakami, a także na serwisy internetowe NATO[11].

Pierwotnie strona amerykańska nie zamierzała długo czekać i błyskawicznie dokonała rozeznania w kontekście możliwie całkowitego odcięcia Jugosławii od Internetu. Mimo wszystko, z obawy o ludność, która na skutek takiego posunięcia zostałaby pozbawiona dostępu do sieci internetowej i zdana wyłącznie na propagandowy przekaz władz, plan zamrożono, a społeczność mogła w dalszej mierze korzystać z dostępu do sieci i konfrontować napływające wiadomości. Równocześnie kampania gróźb związana z kolejnymi atakami w sieci została rozpoczęta 27 marca 1999 r. Rosyjska strona internetowa (gazeta.ru) podała wówczas informację o ataku na portal Białego Domu, co zresztą zostało odparte przez USA informacją, że strona została zamknięta z powodu awarii sprzętu[12].

Mimo wszystko ataki nie ustawały, dochodziło nawet do stu dziennie. Warto jednak podkreślić, że były to ataki na serwery udostępnione publiczne, przez co sytuacja nie miała większego wpływu na funkcjonowanie NATO. Ponadto sam Sojusz Północnoatlantycki przyznał, że na tego typu ataki nie zamierza odpowiadać. Dopiero na skutek presji amerykańskiej stosowne

[11] *Vide:* K. Mitnick, W. Simon, *op. cit.*, s. 24.
[12] Do powyższych wniosków skłonił autora: Ł. Szmurmiński, *Wojna w internecie – walka informacyjna,* [w:] A. Kozieł, K. Gajlewicz (red.), *Media masowe wobec przemocy i terroryzmu,* Warszawa 2009, s. 142-143.

działania zostały podjęte. Starano się manipulować kontami bankowymi oraz przeprowadzać ataki na jugosłowiańską obronę przeciwlotniczą. Na ataki typu *e-mail bombing*, które skierowano przeciw NATO, odpowiadano *per analogiam*. Z jednej strony zaatakowano witrynę gov.yu, co poskutkowało jej zablokowaniem. Z drugiej strony posunięcie te spotkało się z negatywnym nastawieniem dostawcy internetowego, który odciął od Internetu jej koordynatora – Richarda Clarka, za łamanie antyspamowej polityki firmy. Notabene swoją obecność zademonstrowała również amerykańska grupa Team Sploit, która na kilku stronach umieściła tekst „Powiedzcie swoim rządom, aby zakończyły tę wojnę"[13].

W końcowych etapach walki podmieniano zawartości witryn internetowych. I tak, chociażby działacze z Black Hand dokonali włamań na portale artbell.com, gdzie umieszczono tekst potępiający atak NATO na Jugosławię. Agresorzy ponadto zamieścili na jednym z albańskich portali internetowych następującą informację: „Kontynuujemy usuwanie albańskich kłamstw z internetu". Jak diagnozuje Szurmiński, stronie serbskiej pomagali aktywiści z Rosji oraz Chin, którzy m.in. na amerykańskim portalu internetowym *Orange Coast College* umieszczali wulgarne sformułowania wobec prezydenta Williama J. Clintona. Działanie to sprowokowało prezydenta do podjęcia zdecydowanych kroków w odwecie, stając się ważnym element toczącej się gry nerwów i debaty w Białym Domu nad przeciwstawianiem się tego typu atakom.

W toczących się w przestrzeni cybernetycznej rozgrywkach dokonano równocześnie ataków na portale Departamentu Energetyki, Departamentu Spraw Wewnętrznych oraz Służby Parków Narodowych. Z kolei na ataki ze strony chińskich aktywistów odpowiedziały grupy Bronc Buster Zyklon które zaatakowały chińskie serwery, co utrudniło tamtejszej ludności poruszanie się po sieci[14].

W konkluzji należałoby podkreślić, że podczas konfliktu w Kosowie nie wykorzystano zaawansowanych technik. Były to głównie ataki *e-mail bombing* oraz podmiany stron internetowych. Warto jednak zauważyć, że strefa ta zaczęła być powoli wykorzystywana do celów politycznych.

CASUS CHIŃSKI Z 2001 ROKU

Pierwszego kwietnia 2001 r. nowo wybrany prezydent Stanów Zjednoczonych republikanin George W. Bush został poddany pierwszej ważnej próbie decyzyjnej. Tego „czarnego dnia" doszło do kolizji chińskiego myśliwca z amerykańskim samolotem zwiadowczym EP-3. W wyniku zderzenia śmierć poniósł chiński pilot, a samolot amerykański musiał awaryjnie lądować na terytorium Chin, które oskarżyły tym samym USA o prowadzenie szpiegostwa. Niespełna tydzień po toczących się ostrych wymianach dyplomatycznych na linii Pekin-Waszyngton, amerykańska grupa sonB0x włamała się na strony kilku istotnych chińskich

[13] *Ibidem*, s. 146.
[14] *Ibidem*, s. 145-146.

przedsiębiorstw. Zawarte treści podmieniono na grafiki pornograficzne oraz obwieszczono je takimi hasłami jak: „Gdzie nasz samolot złodzieje?!"; „Nienawidzimy Chin. Oddajcie nasz samolot!"[15]. Dopełniono to również kilkoma innymi atakami przeprowadzonymi na witryny rządowe Państwa Środka.

W efekcie Chińczycy podjęli działania odwetowe za: „niczym niesprowokowany i skandaliczny atak USA na Chiny"[16]. Warto podkreślić, że w tym celu powstała specjalna witryna KillUSA.com, z której możliwe było pobranie oprogramowania umożliwiającego ataki. W dodatku zarówno Pekin, jaki i Waszyngton zostały wsparte w swoich działaniach przez strony trzecie. Chinom pomogły takie państwa jak: Indonezja, Japonia czy Korea. Amerykanom natomiast pomogli hakerzy z Arabii Saudyjskiej, Argentyny, Brazylii, Indii, Malezji oraz Pakistanu. W trakcie prowadzonej konfrontacji Chińczycy zdołali zaatakować portale: Białego Domu, Departamentu Pracy, Departamentu Zdrowia, Departamentu Energetyki, Departamentu Spraw Wewnętrznych, Izby Reprezentantów oraz Dowództwa Marynarki Wojennej. Na odpowiedź amerykańską nie trzeba było długo czekać. W krótkim czasie chińskie strony rządowe przestały działać, a na stronie jednego z ministerstw zamieszczono zniszczoną flagę chińską[17].

Ostatecznie 7 maja 2001 r. na portalu ChinaByte zamieszczono ogłoszenie wzywające do wstrzymania działań. Szacuje się, że w wyniku ataków ucierpiało około półtora tysiąca stron amerykańskich oraz około trzystu chińskich[18]. Prowadzona wojna uświadomiła stronom konieczność przykładania większej uwagi do wzmacniania własnego cyberbezpieczeństwa. Niemniej jednak warto zauważyć, że rząd chiński, który w rzeczywistości nie poparł, ale też nie powstrzymywał ataków po tych wydarzeniach postanowił wykorzystać potencjał niezależnych działaczy. Jak podaje w swoich pracach Roman Szymaniuk, już w 2002 r. minister bezpieczeństwa publicznego Chin stwierdził, że „wirusy to narzędzia masowego ataku". Autor dodaje również, że „w kraju kształci się hakerów mających działać na zlecenie rządu"[19].

Dopiero w 2011 r. ChRL oficjalnie potwierdziła przeprowadzanie szkoleń dla przyszłych hakerów. Jak stwierdzono, powstała jednostka o nazwie Blue Army, której wydźwięk ma charakter *stricte* defensywny, polegający na zabezpieczeniu oraz odpowiadaniu na potencjalne ataki[20].

CASUS ESTOŃSKI Z 2007 ROKU

Estonia jest państwem europejskim, które posiada jedną z najbardziej rozwiniętych sieci teleinformatycznych. Dzięki rozbudowanej sieci możliwe jest choćby oddawanie swojego

[15] A. Bógdał-Brzezińska, M.F. Gawrycki, *op. cit.,* s. 174.
[16] *Ibidem,* s. 174.
[17] Powyższe refleksje powstały w oparciu: *ibidem,* s. 175-176.
[18] Xu. Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications,* Lexington 2007, s. 54-55.
[19] Powyższe cytaty za: R. Szymaniuk, *Cyberterroryzm – wcale nie wirtualne zagrożenie*, „Kwartalnik Bellona", nr 4, 2009, s. 56.
[20] *Chiny: zatrudniamy 30 hackerów*, http://niebezpiecznik.pl/post/chiny-zatrudniamy-30-hackerow/ (13.06.2015).

głosu wyborczego online, czy też składanie deklaracji finansowych. Ponadto estoński parlament uznał dostęp do sieci internetowej za jeden z podstawowych praw człowieka. Takie „usieciowienie" Estonii ma z jednej strony zalety, a z drugiej strony swoje wady. Szczególnie te drugie bezwzględnie zostały wykorzystane w 2007 r., gdy miał miejsce konflikt między Rosją a Estonią. *Casus belli* tzw. rosyjsko-estońskiej „wojny o historię", sprowadzał się do przeniesienia Brązowego Żołnierza – pomnika Armii Czerwonej. Dla strony rosyjskiej symbol ten stanowił element upamiętniający sowieckich żołnierzy, poległych podczas „wyzwalania Tallina z rąk nazistów". Z kolei przez Estończyków postrzegany był jako symbol okupacji państwa. Decyzja o przeniesieniu pomnika ze śródmieścia Tallina na podmiejski cmentarz wojskowy doprowadziła do konsternacji mniejszość rosyjską. Swój sprzeciw wyrażano poprzez agresywne demonstracje wzniecane przez środowiska nacjonalistyczne. Gdy z jednej strony na ulicach toczyły się walki pomiędzy aktywistami a służbami porządku publicznego, to z drugiej strony do prawdziwej wojny doszło w estońskiej cyberprzestrzeni. Rosyjskie cyberataki skierowano w niemal każdy sektor bezpieczeństwa państwa, a nawet oświaty[21].

W najbardziej szczytowym momencie, czyli w Dzień Zwycięstwa, obchodzony w Rosji 9 maja, ruch na estońskich stronach WWW wzrósł ponad dwudziestokrotnie, osiągając tym samym apogeum, a celem stał się nawet sektor prywatny. Warto odnotować, że w pewnej chwili sytuacja w estońskiej cyberprzestrzeni wymknęła się spod kontroli, a próba przywrócenia *status quo ante* okazała się niemożliwa. Dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi online i wstrzymać transakcje zagraniczne. Zamarła też strona największego dziennika „Postimees". Cyberwojna trwająca trzy tygodnie, ukazała jak bezbronne wobec cyberterroryzmu może stać się społeczeństwo małego państwa. Najdobitniej podsumował to estoński minister obrony Jaaka Aaviksoo, mówiąc: „pierwszy raz zdarzyło się, żeby cyberataki stanowiły poważne zagrożenie dla bezpieczeństwa całego narodu"[22]. Z analitycznego punktu widzenia doskonale wyraził się na ten temat Gadi Evron, izraelski ekspert ds. bezpieczeństwa, stwierdzając iż „za pomocą cyberbomby Estonia została niemal zepchnięta do epoki kamiennej"[23].

W odpowiedzi na powyższe ataki, państwa Organizacji Traktatu Północnoatlantyckiego, zadecydowały o wysłaniu do Estonii ekspertów w dziedzinie cyberbezpieczeństwa. Nominalnie ich zadaniem było wsparcie estońskich informatyków walczących z problemami sieci. Skądinąd problemem prawnym pozostawało definiowanie ataków cybernetycznych. NATO, jako sojusz zbiorowej obrony, nie mógł operować w ramach artykułu 5. Traktatu Waszyng-

[21] Powyższy akapit powstał w opracowaniu: M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations", tom 42, Warszawa 2010, s. 62; J. Jalonen, *Dni, które wstrząsnęły Estonią,* http://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (13.06.2015).

[22] J. Davis, *Hackers Take Down the Most Wired Country in Europe*, „Wired Magazine", http://www.wired.com/ politics/security/magazine/15-09/ff_estonia?currentPage=all (13.06.2015).

[23] G. Evron, *Estonia and Information Warefare,* http://www.podcastchart.com/podcasts/defcon-15-video-speeches-from-the-hacker-conventions/episodes/gadi-evron-estonia-and-information-warefare (13.06.2015).

tońskiego, ponieważ cyberataki nie są uznawane za akcje militarne, choć niewykluczone, że w przyszłości ta definicja zostanie o powyższe poszerzona[24].

Można by wnioskować, że dla zwykłego Estończyka cyberataki były raczej frustrujące niż niebezpieczne. Utrudniły one komunikację i przepływ informacji np. w postaci realizacji płatności. Z drugiej strony skala ataków spowodowała też szkody finansowe np. wśród banków internetowych. Niezależnie od tego zastosowane metody agresji nie należały do unikatowych, a wręcz można pokusić się o stwierdzenie, że były dość prymitywne i z pewnością nie wystarczyłyby w kompleksowym zniszczeniu infrastruktury informatycznej estońskiego społeczeństwa. Pomimo tego, efekt psychologiczny został osiągnięty: zawieszenie usług bankowych nawet na pewien czas starczyło, aby zaniepokoić zwykłego mieszkańca Talina.

CASUS GRUZIŃSKI Z 2008 ROKU

Następnym ważnym wydarzeniem w cyberprzestrzeni był konflikt między Gruzją a Rosją z 2008 r. Do dziś istnieją realne przesłanki świadczące o zaangażowaniu w ataki rosyjskich służb specjalnych takich jak Główny Zarząd Wywiadowczy (GRU), czy Federalna Służba Bezpieczeństwa (FSB), które miały jakoby kontrolę nad botnetem dokonującym ataków[25]. Pierwsze wzmianki o agresji wirtualnej pojawiły się 5 sierpnia. Gruzini wówczas zablokowali swoimi działaniami dostęp do osetyńskich portali informacyjnych oraz radia rządowego. W efekcie tego ataku rodzime media rozpoczęły nadawać informacje podawane przez gruzińską stację Alania TV[26].

Wobec powyższego strona rosyjska nie pozostała bierna i dokonała analogicznego odwetu. Ataki zostały przeprowadzone między innymi na witrynę prezydenta Micheila Saakaszwilego, gruzińskiego rządu, ministra spraw zagranicznych oraz ministra obrony. Atakami DDoS (*distributed denial of service*, rozproszona odmowa usługi) zablokowano dostęp do serwerów naukowych, jak również wiodących portali informacyjnych. W wyniku tego odwetu strona gruzińska straciła możliwość przekazywania informacji opinii międzynarodowej w tym chociażby perswadowania własnego stanowiska na temat toczącego się konfliktu. Miron Lakomy przekonywał, że rządowe organa musiały stosować rozwiązania tymczasowe jak na przykład: ministerstwo spraw zagranicznych zaczęło korzystać z blogów Google. W walce zastosowano również atak *deface*, którym podmieniono zawartość strony prezydenta Gruzji, a treść portalu zstąpiono zdjęciem Adolfa Hitlera. W zaistniałej sytuacji jednym z rozwiązań, na jakie udało się zresztą zdobyć rządowi Tbilisi, było skorzystanie z serwerów ulokowanych w innych krajach. Z pomocą zaangażowały się tutaj: Polska, Ukraina czy też Estonia, które udostępniły swoje zasoby wspomagające[27].

[24] *Vide:* M. Lakomy, *op. cit.*, s. 61.
[25] J. Leyden, *Russian spy agencies linked to Georgian cyber-attacks,* http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/ (31.08.2015).
[26] Powyższy akapit powstał w opracowaniu: J. Farwell, R. Rohozinski, *Stuxnet and the Future of Cyber War*, "Survival Global Politics and Strategy" vol. 53 no.1, s. 26; M. Lakomy, *op. cit.*, s. 141.
[27] Streszczenie poglądu za: *ibidem*, s. 147-148.

Jednocześnie dokonując porównania z uprzednio opisanymi aktami wirtualnej agresji, również i w tym przypadku nie użyto zaawansowanych metod ataków. Były to głównie ataki DDoS oraz tzw. *website defacement*. Niemniej uderzająca była kwestia zablokowania możliwości prezentowania gruzińskiego stanowiska na arenie międzynarodowej. Było to postępowanie niezwykle zbliżony do wydarzeń z Kosowa w 1999 r., kiedy także planowano odciąć tereny Jugosławii od dostępu do sieci. Ukazuje to, że działania w cyberprzestrzeni, a mające skutki w rzeczywistości są niemal tożsame. W przypadku Jugosławii postanowiono pozostawić dostęp do sieci z zamierzeniem umożliwienia ludności dostępu do większej ilości źródeł informacji, a przez to łatwiejszej ich weryfikacji. W przypadku Gruzji zauważono tę zależność, w wyniku czego ofiarami ataku padły strony informacyjne. Uniemożliwiło to obywatelom zdobywania informacji o zaistniałych zdarzeniach i uruchomiło napęd rozwijający działalność propagandową.

CASUS IRAŃSKI Z 2010 ROKU

Za najbardziej znane, a zarazem najlepiej dopracowane ataki uważa się te, które zostały przeprowadzone na Islamską Republikę Iranu. Inicjacja powstrzymywania nuklearnego programu Iranu została nazwana mianem „Olympic Games" i według niektórych źródeł,-powstała na skutek bezpośredniej decyzji 43. Prezydenta USA George'a W. Busha. Pierwotnie działania miały na celu zahamowanie, lub wstrzymanie wzbogacania uranu do poziomu krytycznego i tym samym nie prowokowanie Iranu do walki zbrojnej. Nie jest do końca jasne, kiedy rozpoczęło się wdrażanie ataków na irański program atomowy. Niemniej, za oficjalną datę przyjmuje się rok 2010, który związany jest właśnie z odkryciem wirusa Stuxnet. Dokonała tego jedna z białoruskich firm antywirusowych. Choć trzeba zaznaczyć, że z biegiem czasu wyszło na jaw, że Stuxnet nie jest jedynym wirusem zaaplikowanym w irański program nuklearny. Dopełnienie jego agresywności zostało powiązane z innymi wirusami tj. Duqu, Flame oraz Gauss. Jak przypuszcza Farwell, wszystkie zostały napisane przez ten sam podmiot, pomimo tego, że każdy z wirusów miał inne w swoim założeniu zadanie techniczne do wykonania[28]. Autor skoncentruje swoją uwagę na wirusie Stuxnet. Niemniej, kilku informacji dotyczących jego szczepów nie można pominąć.

I tak wirus Flame został w ostatecznym rozrachunku zlokalizowany w Iranie, Libanie, Zjednoczonych Emiratach Arabskich, Izraelu, Sudanie, Syrii, Arabii Saudyjskiej oraz Egipcie Zwykło się przyjmować, że łącznie zainfekował około 5 tys. komputerów. Jego głównym zadaniem było monitorowanie otoczenia. Najprościej ujmując, wirus ten potrafi wykradać pliki, aktywować mikrofony w komputerach, przez co rejestrować dźwięki w otoczeniu, wykonywać zrzuty ekranu oraz wyszukiwać telefony za pomocą protokołu Bluetooth. Flame ponadto został z czasem wyposażony w dodatkowy moduł, którego komenda nakazywała mu się odin-

[28] Do powyższych refleksji skłonił autora: J. Farwell, R. Rohozinski, *The New Reality of Cyber War*, „Survival Global politics and strategy", vol. 54 no.4 August-September 2012, s. 109; P. Konieczny, *Stuxnet – czyli co już wiemy o przełomowym robaku?*, http://niebezpiecznik.pl/post/stuxnet/ (13.06.2015).

stalować w momencie zrealizowania zadania[29]. Wirus Duqu podobnie jak Flame został stworzony w celu kradzieży danych. Jego zadaniem było przesyłanie na docelowy serwer zrzutów ekranu, zapisu wciśniętych klawiszy oraz zbieranie informacji na temat uruchomionych procesów. Identycznie jak w przypadku wirusa Flame, Duqu odinstalowuje się, jednakże ze względu na wbudowany kod dokonuje tego dopiero po upływie 36 dni. *Ad extremum,* wirus Gauss został napisany w podobny sposób jak jego poprzednicy. Dzieli z nimi fragmenty kodu i jest przez to jedynym dowodem na to, że wirusy są napisane przez ten sam zespół. Gauss w odróżnieniu od dwóch uprzednio opisanych wirusów wykrada dane związane z finansami[30]. Do zadań wirusa Gauss należą[31]:

- przechwytuje ciasteczka i hasła z przeglądarek;
- wykrada pliki konfiguracyjne i wysyła je autorom trojana;
- infekuje dyski USB;
- kradnie dane dostępowe do banków (głównie z Bliskiego Wschodu: Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank, Credit Libanais, Citibank, PayPal);
- kradnie dane dostępowe do portali społecznościowych, skrzynek e-mail i kont IM.

Spośród wyżej wskazanych Stuxnet był pierwszym z odkrytych wirusów, które zostały wymierzone w irański program atomowy. Wirus błyskawicznie został okrzyknięty największym krokiem do przodu w dziedzinie cyberwojny, ale równocześnie wykazano, że nie jest on tak zaawansowanym narzędziem, za jaki się go uważano. Głosy z zarzutami, były wymierzone w jakość kodu programu. Ponadto przyjmuje się, że Stuxnet posiada podstawowe i mało rozwinięte sposoby omijania zabezpieczeń programów antywirusowych. Jak zauważają wybitni eksperci, J. Farwell oraz R. Rohozinski Stuxnet zawiera w sobie kilka ataków zwanych *zero-day exploits*[32]. Innymi słowy, działalność Stuxnetu jest tylko zlepkiem wielu innych linii kodu. Nie jest to innowacja, ponieważ podobne techniki stosowano już wcześniej podczas ataku na Dowództwo Centralne USA (*United States Central Command* – USCENTCOM), skąd kradziono dokumenty niejawne[33].

J. Farwell i R. Rohozinski posuwają się w swoich analizach dalej i nazywają Stuxnet Frankensteinem, właśnie z powodu dodania do niego kilku ataków *zero-day*. Swoją drogą, takie nazewnictwo znajdzie również potwierdzenie w fakcie modułowości nie tylko Stuxneta, ale również pozostałych wirusów. Wszystkie cztery zostały skonstruowane z modułów. Pewne części kodu wirusów powtarzają się w każdym z czwórki, która została użyta przeciw Iranowi[34].

---

[29] *Vide:* J. Farwell, R. Rohozinski, *The new reality..., op. cit.,* s. 109; P. Konieczny, *Flame – mówią, że gorszy od Stuxneta,* http://niebezpiecznik.pl/post/flame-mowia-ze-gorszy-od-stuxneta/ (13.06.2015).

[30] Powyższy akapit opracowany w oparciu: *Duqu – nowy Stuxnet,* http://niebezpiecznik.pl/pos t/duqu-666/ (13.06.2015); J. Farwell, R. Rohozinski, *The new reality..., op. cit.,* s. 110.

[31] *Gauss – kolejny członek rodziny Stuxnet, Duqu, Flame, op. cit.*

[32] Wykorzystanie luki w oprogramowaniu, która nie została wcześniej ogłoszona, przez co nie jest uwzględniona np. w aktualizacjach; najczęściej dostępne na czarnym rynku.

[33] *Vide:* J. Farwell, R. Rohozinski, *Stuxnet…*, s. 25.

[34] *Ibidem,* s. 26.

Ostatecznie należy przyjąć, że zbytnie rozwinięcie kodu mogło spowodować zawężenie osób, które byłyby w stanie napisać taki program. Ponadto, każde dodatkowe dni mogły nie być na tyle cenne dla twórców by poświęcać środki finansowe oraz czas na przedłużenie żywotności wirusa. Stuxnet zainfekował w sumie ponad 60 tys. komputerów, a przeszło połowa z nich należała do Iranu. Wirus ten został również odnaleziony w innych krajach tj. Indie, Indonezja, Chiny, Azerbejdżan, Korea Południowa, Malezja, Stany Zjednoczone, Wielka Brytania, Australia, Finlandia i Niemcy W ogólnym bilansie należałoby podkreślić, że Stuxnet w odróżnieniu od wirusów Duqu, Flame'a oraz Gaussa, miał przed sobą postawiony zupełnie odmienny cel. Przed wymienionymi, trzema wirusami postawiono zadanie kradzieży informacji. Podczas gdy działalność Stuxnetu miała charakter *stricte* sabotażowy – spowolnienie irańskiego programu nuklearnego[35].

Stuxnet był wymierzony w konkretny rodzaj sprzętu. Atakował oprogramowanie firmy Siemens: WinCC oraz PCS 1 – programy zarządzające procesami przemysłowymi. Docelowym przeznaczeniem miała być zmiana ustawień fabrycznych w powyższych programach. Wnikając w komputery zainstalowane przy maszynach odpowiedzialnych za wirówki, przejmował kontrolę nad stosownym programem i zmieniał prędkości obrotowe silnika wirówek[36]. W krótkich odstępach czasu wirówki przełączały się między małymi a wysokimi prędkościami, do czego nie były pierwotnie przystosowane. W ten prosty sposób przejmując kontrolę nad prędkością, z jaką pracowały wirówki, uniemożliwiono oddzielanie uranu, a tym samym dokonano sabotażu, zatrzymując progres niebezpiecznego programu nuklearnego[37].

Stuxnet wpływał na pracę wirówek w ośrodku wzbogacania paliwa jądrowego w Natanz, prawdopodobnie od pierwszej połowy 2009 r. Na podstawie różnych doniesień około 1.000 wirówek w Natanzu zostało uszkodzonych. Celem były nie tylko wirówki jawne, ale przede wszystkim wirówki tajne. Ponadto istnieją rozbieżne opinie na temat długości przerw w pracy tego ośrodka, gdyż władze irańskie celowo dezinformowały w tej sprawie, nie chcąc ujawnić, jak duże poniosły straty z powodu tego cyberataku[38].

Pomimo względnej złożoności Stuxnet został szybko rozbrojony. W przeciągu kilkunastu miesięcy jego cechy techniczne były dobrze znane ekspertom. Iranowi zaś w rozszyfrowaniu właściwości wirusa dopomógł proces *crowdsourcingu.* Umożliwiło to pozyskanie od

[35] *Ibidem*, s. 26-27.

[36] Silniki osiągając duże prędkości, oddzielały uran-235, który następnie może być wykorzystany w reaktorach lub przy budowie broni jądrowej.

[37] *Ibidem*, s. 28.

[38] Do powyższych refleksji sprowadził autora: J. Warrick, *Iran's Nataz: nuclear facility recovered quickly from Stuxnet cyberattack,* „Washington Post", 16 February 2011, http://www.washingtonpost.com/wp-dyn/content/ article/2011/02/15/AR2011021505395.html (13.06.2015). Warto zaznaczyć, że atak, który zostały przeprowadzony na wirówki w Natanz, nie musi być przeznaczone tylko do wskazanego celu. Stuxnet cechując się bardzo dobrymi właściwościami technicznymi, może być zastosowany wszechstronnie. Innymi słowy, równie dobrze może się sprawdzić w elektrowni w USA, czy chociażby w fabryce samochodów. Ponadto, niektóre z jego podstawowych parametrów technicznych, w tym korzystanie z baz serwerów DNS sprawiają, że znacznie trudniej jest go znaleźć niż w przypadku bardziej zaawansowanego oprogramowania złośliwego. Konkludując, atakujący nie musi dostarczyć niepożądanych danych na pamięci USB (Stuxnet), lecz może użyć konwencjonalnych technologii do rozprzestrzeniania robaka i rozpowszechnić go tak szeroko jak to możliwe.

zewnętrznie wynajętego podmiotu technicznej wiedzy na temat wirusa. Jednocześnie nie ma jasnych dowodów, że Stuxnet miał na celu wystawić irańskiego prezydenta – Mahmuda Ahmadineżada na krytykę opinii publicznej, z powodu braku umiejętności obrony własnych kluczowych instalacji przed atakami cybernetycznymi. Niemniej trzeba sobie uzmysłowić, że Stuxnet może zostać użyty jako narzędzie do osłabiania i destabilizacji władzy w państwie[39].

Współcześnie jest już wiadomym, że w ogólnym bilansie zarejestrowano 23 proc. spadek liczby działających wirówek spowodowanych działaniem Stuxnetu. Sami zaś Irańczycy wciąż wyrażają zadziwienie ze stopnia łatwości obejścia ich własnej obrony. Zresztą, gdyby nawet wierzyć pierwszym przekazom strony irańskiej, że szkoda została szybko ograniczona i naprawiona, to z drugiej strony nie ulega wątpliwości, że w środowisku nie pozostała pewnego rodzaju obawa, że w przyszłych atakach mogą być użyte bardziej skomplikowane „robaki", które wyrządzą znacznie poważniejsze i bardziej trwałe szkody[40].

W opinii Ajatollahów ślad za Stuxnetem prowadził do Stanów Zjednoczonych. Oskarżenia padły także pod adresem Izraela. Przypuszczano, że to właśnie te państwa z powodu niepowodzeń w zatrzymaniu irańskiego programu nuklearnego uciekły się do walki w świecie cyfrowym. Równocześnie warto pamiętać, że poparcie powyższych działań – zniszczenie irańskiego projektu – znalazło swoich zwolenników wśród innych państw arabskich tj. Arabia Saudyjska, Zjednoczone Emiraty Arabskie, Egipt, Jordania czy Bahrajnu Współcześnie uważa się, że to izraelski Mossad był odpowiedzialny za infekcje w irańskich ośrodkach atomowych. Niemniej z operacyjnego punktu widzenia Tel Awiw nie musiał być w tej misji głównodowodzącym. Bardziej prawdopodobnym jest, że były nim Stany Zjednoczone Ameryki.

PODSUMOWANIE

Ciągły rozwój technologii spowodował powstanie nowych zagrożeń – cyberzagrożeń. Ataki w cyberprzestrzeni są stosowane coraz częściej nie tylko przez podmioty pozapaństwowe, ale również przez same państwa. Cyberprzestrzeń jest ciągle rozwijana. Utworzenie jej było naturalnym biegiem zdarzeń. Przykłady pokazują, że cyberwojna już teraz umożliwia wyrządzanie szkód, które zniszczą duże projekty państwowe.

Atak na Iran był znaczącym krokiem do przodu w dziedzinie cyberwojny. W porównaniu z wcześniej dokonywanymi atakami, jak przykładowo typ DDoS na estoński system, co uniemożliwiło dokonywanie płatności oraz *deface* albańskich stron internetowych gdzie zamieszczono inwektywy pod adresem ówczesnego prezydenta Billa Clintona, ataki te można uznać za ataki o charakterze propagandowym. Nie tylko blokowano dostęp do informacji przez ataki DDoS, ale również dokonywano aktów wandalizmu, niszcząc portale przez podmienienie treści np. na hasła patriotyczne, czego dokonali Chińczycy w przypadku witryny Białego Domu.

[39] Powyższy akapit rozwinięty w oparciu: J. Farwell, R. Rohozinski, *Stuxnet..., op. cit.*, s. 28.
[40] *Ibidem*, s. 29-30.

Casus irański był operacją o znacznie bardziej zaawansowanym przebiegu. Pierwszym problemem było wprowadzenie wirusa do systemu odciętego od sieci. Dokonano tego dzięki, zainfekowanej pamięci USB, którą jeden z pracowników podpiął do komputera obsługującego systemy w obiekcie przemysłowym w Natanz, wprowadzając tym samym wirusa. Ponadto atak na Iran odczuły inne państwa. Podejrzewa się, że również problemy z pierwszą indyjską satelitą wywołał właśnie Stuxnet[41]. I gdyby temu wierzyć, to stwarza to problem polityczny na znacznie szerszą skalę. W praktyce w wyniku błędu celem ataku może stać się sojusznik.

Przypadek Iranu pokazuje, że cyberwojna weszła w nowy rozdział. Wynikiem działań nie były już tylko uszkodzone witryny internetowe. Skutki były znacznie dalej posunięte. Zatrzymano naukowy projekt innego państwa, doprowadzając do zniszczenia niezbędnej aparatury. Wywołało to również ożywioną dyskusję na temat klasyfikacji działań w cyberprzestrzeni. Zaczęły pojawiać się pytania, czy można działania takie uznać za akt agresji, użycia siły lub wypowiedzenia wojny? W opinii autora trudno o jednoznaczną i kompleksową odpowiedź w tym zakresie. Należy pamiętać, że każde rozwiązanie jest zależne od konkretnej sytuacji. Każda musi być rozpatrywana osobno ze względu na uwarunkowania polityczne, ale również przez wzgląd na skalę skutków.

BIBLIOGRAFIA

Białoskórski Robert. 2011. Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Warszawa: Wydawnictwo WSCiL.

Bógdał-Brzezińska Agnieszka, Gawrycki Marcin. 2003. Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warszawa: ASPRA-JR.

Bojczuk Adrian. 1998. Internet: agresja i ochrona. Wrocław: Wydawnictwo Robomatic.

Chiny – zatrudniamy 30 hackerów. 2011 W http://niebezpiecznik.pl/post/chiny-zatrudniamy-30-hackerow/.

Davis Joshua. 2007. Hackers Take Down the Most Wired Country in Europe, „Wired Magazine". W http://www.wired.com/politics/security/magazine/1509/ff_estonia?currentPage=all.

Duqu – nowy Stuxnet. 2011. http://niebezpiecznik.pl/pos t/duqu-666/.

Evron Gadi. 2006. Estonia and Information Warefare. W http://www.podcastchart.com/ podcasts/defcon-15-video-speeches-from-the-hacker-conventions/episodes/gadi-evron-estonia-and-information-warefare.

Farwell James, Rohozinski Rafal. 2011. „Stuxnet and the Future of Cyber War". Survival Global Politics and Strategy 53(1) : 23-40.

Farwell James, Rohozinski Rafal. 2012. "The New Reality of Cyber War". Survival Global Politics and Strategy 54(4) : 107-120.

Jalonen Jussi. 2009. Dni, które wstrząsnęły Estonią W http://www.eesti.pl/dni-ktore-wstrzasnely -estonia-11963.html.

Konieczny Piotr. 2012. Flame – mówią, że gorszy od Stuxneta W http://niebezpiecznik.pl/ post/ flame-mowia-ze-gorszy-od-stuxneta/.

[41] Wskazuje na to w swojej analizie: J. Farwell, R. Rohozinski, *Stuxnet…*, *op. cit.*, s. 34.

Konieczny Piotr. 2011. Stuxnet – czyli co już wiemy o przełomowym robaku? W http:// niebezpiecznik.pl/post/stuxnet/.

Lakomy Miron. 2010. „Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku". Stosunki Międzynarodowe – International Relations 42 : 55-73.

Mitnick Kevin, Simon William. 2003. Sztuka podstępu: łamałem ludzi, nie hasła. Gliwice: Helion.

Sanger David. 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran W http:// www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against iran.html?pagewanted=all&_r=1&/.

Szmurmiński Łukasz. 2009. Wojna w internecie – walka informacyjna. W Media masowe wobec przemocy i terroryzmu. Warszawa: ASPRA-JR, 137-150.

Szymaniuk Roman. 2009. „Cyberterroryzm – wcale nie wirtualne zagrożenie". Kwartalnik Bellona 4 : 56-64.

Warrick Joby. 2011. Iran's Nataz: nuclear facility recovered quickly from Stuxnet cyberattack. „Washington Post" W http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html.

Wilson Clay. 2008. Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilitiesand Policy Issues for Congress W http://wlstorage.net/file/crs/RL32114.pdf.