Zeszyty Naukowe AON nr 3(92) 2013
ISSN 0867–2245

BEZPIECZEŃSTWO NARODOWE

CYBERPRZESTRZEŃ JAKO NOWA JAKOŚĆ ZAGROŻEŃ

dr inż. Andrzej NOWAK
Akademia Obrony Narodowej

Abstract

The article aims at presenting the essence of the concept of 'cyberspace'. Particular attention was put here on the very complicated, scientific and legal lineage related to IT technology, IT systems, etc. The article depicts the examples of the biggest cyber attacks observed in the last decade as well as their relation with other areas of critical infrastructure. There is also a reference to issues concerning the structure of units dealing with the phenomenon, as well as countries which are at the possession of special units to perform tasks within cyberspace. All in all, however, the presented information should be taken as an outline of the tackled problems, an outline organizing the knowledge concerning the multifaceted and interdisciplinary concept of cyberspace.

Key words – cyberspace, hazards, security

Wprowadzenie

Zagrożenia z cyberprzestrzeni nie są niczym nowym. Dzisiejszy obraz cyberprzestrzeni wskazuje na konieczność traktowania tej sfery jako jednej ze strategicznych z punktu widzenia obronności kraju. Wskazują na to dwie podstawowe przesłanki: pierwsza, to fakt, że technologia IT[1] jest kluczowym komponentem infrastruktury krytycznej państwa, np. jest wykorzystywana do zarządzania sieciami energetycznymi, telekomunikacyjnymi, transportowymi, bankowymi, służby zdrowia itp. – dlatego cyberatak na infrastrukturę krytyczną może automatycznie postawić pod znakiem zapytania bezpieczeństwo całego kraju; druga, to znaczenie, jakie zyskują technologie IT w jakiejkolwiek sytuacji konfliktowej, stają się bo-

[1] Za Wikipedią – całokształt zagadnień, metod i środków i działań związanych z przetwarzaniem informacji.

wiem głównym elementem w centrum zarządzania czy też dowodzenia, nie tylko zasobami strategicznymi, ale również siłami zbrojnymi.

Rozważania dotyczące „cyberprzestrzeni" warto rozpocząć od podjęcia próby zdefiniowania tego pojęcia. Nie jest to zadanie proste, bowiem mimo wielu prób definiowania nie został ustalony, powszechnie akceptowany, aparat pojęciowy w tym obszarze, a poszczególne koncepcje adekwatne są do koncepcji i podejść określonych „szkół myślenia".

Określenia „cyberprzestrzeń" – prawdopodobnie – jako pierwszy w 1984 roku użył w swojej powieści *Burning Chrome* amerykański pisarz William Gibson[2]. Był to wygenerowany przez komputer świat immersyjnej[3], wirtualnej rzeczywistości, którą amerykański klasyk cyberpunkowych powieści w pierwszy tomie swojej Trylogii – *Neuromancer* – nazywał też matrycą (matrix). Natomiast, na dobre spopularyzował cybeprzestrzeń powszechny dostęp do Internetu, oraz filmy opierające się na motywach gibsonowskich, jak np. *Johny Mnemonic*, czy trylogia *Matrix,* która oznaczała halucynację.

Ponadto można stwierdzić, że na początku lat 90-tych pojęcie cyberprzestrzeń wchodzi do powszechnego użytku. Już wtedy rozwój technologii informacyjnych był na takim poziomie, że Nicholas Negroponte ogłosił, że składnikiem elementarnym przestał być atom, a została nim cyfra binarna. Natomiast Philiph Elmer DeWitt opisał cyberprzestrzeń jako „przypominającą poziom form idealnych Platona, przestrzeń metaforyczną, rzeczywistość wirtualną"[4]. Nie dajmy się jednak ponieść tego typu fantazjom – cyberprzestrzeń jest domeną fizyczną. Dzisiaj, obok środowiska lądowego, morskiego, powietrznego czy też kosmicznego to kolejne środowisko w którym można prowadzić działania (także militarne). Całkowicie jednak różni się od trzech pozostałych. Przede wszystkim jest w całości dziełem człowieka, a powstała w wyniku stworzenia systemów informacyjnych i sieci umożliwiających komunikację drogą elektroniczną. Dodatkowo uczestnicy tego pola walki mają pełną kontrolę nad właściwościami tego środowiska. Natomiast zniszczenie, uszkodzenia lub choćby zniekształcenie jego cyfrowych składników powoduje zmianę topografii terenu operacji. To tak jakby w trakcie bitwy lądowej nagle zniknęła lub pojawiła się góra. W wojnie cyberprzestrzennej znaczenie całkowicie traci geografia i geopolityka. RAND Corporation[5] w 1995 roku zbadała na zlecenie Departamentu Obrony USA możliwości strategicznej wojny informacyjnej. W raporcie końcowym czytamy: „techniki wojny informacyjnej sprawiają, że odległość geograficzna nie ma znaczenia; cele znajdujące w granicach Stanów Zjed-

[2] William Gibson (ur. 17 marca 1948 w Conway w stanie Karolina Południowa) – amerykański pisarz science fiction, twórca cyberpunku.

[3] Immersja – sytuacja gdy tekstowi towarzyszą obraz, dźwięk, animacje oraz bogaty, oferujący możliwość swobodnego wyboru, system połączeń, może sprzyjać doświadczeniu immersji, zanurzenia się w świecie przez dzieło ewokowanym.

[4] Zob. Gregory J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004, s. 29.

[5] RAND Corporation – amerykańska organizacja badawcza non-profit, pierwotnie sformowana dla potrzeb Sił Zbrojnych Stanów Zjednoczonych.

noczonych są równie wrażliwe jak cele na lokalnym teatrze działań”[6]. Oznacza to, że ataku można dokonać z każdego miejsca na Ziemi.

Podobnie definiowana jest cyberprzestrzeń w i-słowniku: (ang. *cyberspace*; gr. *kybernetes* – sternik, zarządca oraz kontrolować, zarządzać) – w ostatnich latach przedrostek *cyber* – wiąże się z nowymi, elektronicznymi technologiami i jest używany w znaczeniu informatyczny, interaktywny. Innymi słowy pojecie to określa wszystko, co wiąże się z komputerami. Cyberprzestrzeń to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Cyberprzestrzeń, podobnie jak telekomunikacja, ułatwia użytkownikom sieci kontakty, także w czasie rzeczywistym. Przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie. Definicja ta uwzględnia wszystkie systemy komunikacji elektronicznej (w tym również klasyczne sieci telefoniczne), które przesyłają informacje pochodzące ze źródeł numerycznych lub są przeznaczone do numeryzacji. Można zatem stwierdzić, że cyberprzestrzeń powoli staje się podstawowym kanałem wymiany informacji[7].

Natomiast, według Departamentu Obrony Stanów Zjednoczonych, cyberprzestrzeń, obok lądu, morza, powietrza, stała się kolejną przestrzenią prowadzenia walki[8]. Jest ona definiowana jako *współzależna, powiązana ze sobą sieć infrastrukturalna technologii informatycznej, obejmująca Internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego*. Jest to ujęcie kompleksowe. Amerykanie w mniejszym stopniu zwracają uwagę na to, kto jest właścicielem sektora strategicznego, a koncentrują się na jego ochronie. Podobne praktyczne podejście prezentują niektóre kraje zachodnie.

Do polskiego porządku prawnego również zostało wprowadzone pojęcie cyberprzestrzeni. Definicja tego niezwykle ważnego pojęcia, została zawarta w nowelizacji *ustawy, z dnia 30 sierpnia 2011 roku,* o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP. Wskazany akt prawny określa cyberprzestrzeń jako *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt. 3 ustawy z dnia 17 lutego 2005*[9] *roku o informatyzacji działalności podmiotów realizujących zadania publiczne*[10].

[6] Gregory J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004, s. 24.

[7] Zob. i-słownik: http://www.i-slownik.pl/323,cyberprzestrzen/, [27.02.2012].

[8] US Department of Defense Strategy for Operating in Cyberspace, Departament Obrony USA, lipiec 2011 r., http://www.defense.gov/news/d20110714cyber.pdf, [22.08.2011].

[9] System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm. ogłoszonymi w Dz. U. z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362 i Nr 267, poz. 2258, z 2006 r. Nr 12, poz. 66, Nr 104, poz. 708 i 711, Nr 170, poz. 1217, Nr 220, poz. 1600, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 23, poz. 137, Nr 50, poz. 331

Jednocześnie należy stwierdzić, że Ministerstwo Administracji i Cyfryzacji, odpowiedzialne za koordynację ogólnej polityki bezpieczeństwa cyberprzestrzeni RP, dalej pracuje nad definiowaniem trudnych pojęć w dokumencie zwanym „Polityką Ochrony Cyberprzestrzeni RP[11]. W dokumencie tym, w rozdziale „Terminy" definiowana jest Cyberprzestrzeń jako „*przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323)*". W dalszej części nazwano cyberprzestrzeń RP (dalej, jako CRP) – cyberprzestrzenią w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).

I tutaj można zauważyć pewne nieścisłości, gdyż definicja „cyberprzestrzeni" na podstawie przytoczonych przepisów prawa nie obejmuje komputerów obywateli RP, ponieważ wskazuje na urządzenie końcowe[12] – modem, telefon, router bądź karta sieciowa, które są zakończeniem sieciowym wskazanych w definicji przepisów prawa. Biorąc pod uwagę powyższe oznacza to, że komputer lub inny sprzęt, obywatela, przedsiębiorcy, podłączony przez router, modem firmy telekomunikacyjnej do Internetu nie jest częścią cyberprzestrzeni, a zatem nie dotyczą tych urządzeń pojęcia „cyberataku", „cyberprzestępstwa". Dlatego, celowym byłoby zmienić terminy „cyberprzestrzeni" i „cyberprzestrzeni RP", w taki sposób aby definicja obejmowała zasoby techniczne – urządzenia (innymi słowy, doprecyzować zapis z którego wynikałoby, że komputery, serwery, telewizory, dekodery SAT, byłyby określane jako zakończenie sieci – cyberprzestrzeni) każdego użytkownika CRP w tym obywatela i przedsiębiorcy.

Należy zwrócić także uwagę na fakt, że pojęcie „cyberatak"[13] swoim zakresem nie obejmuje ataków przeprowadzonych z cyberprzestrzeni RP w odniesieniu do cyberprzestrzeni innych krajów, ponieważ pojęcie „cyberprzestrzeni" zostało sztucznie zawężone do zasobów technicznych opisanych w przepisach prawa polskiego tj. *Ustawie*

i Nr 82, poz. 556, z 2008 r. Nr 17, poz. 101 i Nr 227, poz. 1505 oraz z 2009 r. Nr 11, poz. 59, Nr 18, poz. 97 i Nr 85, poz. 716.).

[10] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP.

[11] 23 listopada 2012 roku Minister Michał Boni zwrócił się z prośbą o dokonanie zmiany w Wykazie Prac Legislacyjnych i Pozalegislacyjnych Rady Ministrów w tytule dokumentu „Programu Ochrony Cyberprzestrzeni" na „Polityka Ochrony Cyberprzestrzeni RP".

[12] W ustawie znajduje się zapis, „telekomunikacyjne urządzenie końcowe – urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci (art. 2 pkt. 43).

[13] Cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni – Polityka CBR, s. 6.

z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne i dalej prawa telekomunikacyjnego, na które wskazuje w swej treści ustawa przytoczona w definicji cyberprzestrzeni. Oznacza to, że atak przeprowadzony z wykorzystaniem cyberprzestrzeni RP w odniesieniu do cyberprzestrzeni innego państwa, nie jest „cyberatakiem", z uwagi na fakt, że pojęcie „cyberprzestrzen" nie obejmuje swym zakresie pojęciowym cyberprzestrzeni innych państw ewentualnie cyberprzestrzeni globalnej.

Konkludując, celowym jest wskazanie, że pojęcia użyte w dokumencie nie są jasne i zrozumiałe dla każdego obywatela RP i tworzą niepotrzebny bałagan prawny. Opisując precyzyjniej pojęcie „cyberprzestrzeni" odwołuje się do ustawy z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne, która to *ustawa* następnie odsyła do prawa telekomunikacyjnego wskazującego na „zakończenie sieciowe" (cyberprzestrzeni), jakim jest router, modem, karta sieciowa, telefon zlokalizowany u każdego obywatela. Niestety podłączony przez router komputer nie zalicza się już do zasobów cyberprzestrzeni zgodnie z rozwinięciem jej obowiązującej definicji.

W związku z powyższym, należy dostrzec konieczność ponownego zdefiniowania pojęć „cyberprzestrzeń" i „cyberprzestrzeń RP", jak również zastanowić się nad pojęciami „cyberataku", „cyberprzestępstwa" oraz dodać pojęcie „cyberprzestrzeni globalnej", „cyberprzestrzeni innego kraju" i „cyberzagrożenia".

Można by było rozważyć poniżej przedstawione definicje[14]:

„cyberprzestrzeń globalna" lub „cyberprzestrzeń" – system wymiany, przetwarzania informacji (danych) funkcjonujący zgodnie z formalnymi zasadami, uregulowaniami prawnymi obowiązującymi na terytorium poszczególnych państw, działający dzięki połączeniu zasobów technicznych zlokalizowanych na terytorium każdego z tych.

„cyberprzestrzeń RP" – system wymiany, przetwarzania informacji (danych) funkcjonujący zgodnie z formalnymi zasadami, uregulowaniami prawnymi obowiązującymi na terytorium Rzeczypospolitej Polskiej, działający dzięki połączeniu zasobów technicznych zlokalizowanych na jej terytorium.

Należy zwrócić także uwagę na fakt, że dokument „Polityka Ochrony Cyberprzestrzeni RP" znacznie odbiega od standardów, jakie zostały określone w normie PN-ISO/TEC 27001 w odniesieniu do zarządzania bezpieczeństwem informacyjnym – celów stosowania zabezpieczeń i zabezpieczenia, jak też kwestii, które „Polityki Bezpieczeństwa" powinna regulować i jakim powinna odpowiadać tj. „powinna zapewniać, że jest przydatna, adekwatna i skuteczna"[15].

[14] Por. BIODO Uwagi do Polityki Ochrony Cyberprzestrzeni RP. pdf w: http://mac.bip.gov.pl/fobjects/details/3564/biodo-uwagi-do-polityki-ochrony-cyberprzestrzeni-rp-pdf.html, [23.02.2013].

[15] Zob. Norma ISO/TEC 27001:2007, Technika informatyczna, Technika bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa 2007, s. 14.

Przykłady zagrożeń

Cyberprzestrzeń z racji swoich unikalnych właściwości jest szczególnie podatna na akty cyberszpiegostwa, na które – co warto podkreślić szczególnie mocno – straciły monopol państwowe służby specjalne. Dzisiaj, liczącymi się aktorami w tym procederze są konkurencyjne przedsiębiorstwa, instytuty badawcze, uniwersytety, a także pojedynczy, wynajęci do konkretnego zlecenia, hakerzy.

Dla zobrazowania zagrożeń związanych z zagrożeniami z cyberprzestrzeni, warto przytoczyć **fakty najgłośniejszych cyberataków, do których doszło w ostatnim dziesięcioleciu.** Żaden z nich nie został zakwalifikowany jako akt wojny, nie rozwinął się też w oficjalny konflikt, w który zaangażowane zostałyby siły całego rozwiniętego technologicznie państwa. Niemniej, poniższe przykłady stanowić mogą wyobrażenie o zmianach na przyszłych polach walki a może konfrontacji?

„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..."[16]. To nie fragment scenariusza 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 zagrożenia płynące z cyberprzestrzeni. Od 27 kwietnia do 11 maja 2007 roku ofiarą cybernetycznych ataków stała się Estonia.

Pretekstem ataku była decyzja estońskich władz o przeniesieniu pomnika upamiętniającego żołnierzy Armii Czerwonej (tzw. Brązowego Żołnierza), która stała się powodem licznych zamieszek. 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 „evalitsus" (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[17].

[16] 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, s. 1 w: http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf, [25.04.2007].

[17] Patrz: E-Eesti/E-Estonia, http://webstatic.vm.ee/static/failid/286/E-Estonia_uus.pdf, [12.01.2011].

Wszystkie te czynniki sprawiły, że estońska infrastruktura teleinformatyczna okazała się doskonałym celem cyberataków. W szczytowym momencie, czyli w obchodzonym w Rosji 9 maja Dzień Zwycięstwa, 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. Ponadto 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[18]. 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[19]".

Władze Estonii zastanawiały się nawet, nad odwołaniem do artykułu 5 *Traktatu Waszyngtońskiego*, mówiącego o wzajemnej pomocy państw członkowskich NATO w razie ataku na terytorium jednego z nich. Premier Estonii Andrus Ansip pytany o przyczyny zdarzenia stwierdził: „*komputery, które wykorzystano w ataku, miały adres administracji prezydenta Putina. Akcja przeciwko Estonii była doskonale zsynchronizowana – w tym samym czasie demonstranci atakowali naszą ambasadę w Moskwie i przedstawicielstwo linii lotniczych. A oficjalna delegacja rosyjska, która odwiedziła Tallin, stwierdziła, że rząd Estonii powinien się podać do dymisji*".

Podczas „cybernapaści" na Estonię, agresorzy posłużyli się brutalną, lecz skuteczną formą ataku o nazwie DDoS (Distributed Denial of Service). Polega ona na zalewaniu upatrzonych serwerów gigantyczną ilością danych, co powoduje ich przeciążenie, a w efekcie doprowadza do blokady.

Wkrótce po atakach estońskie władze obwiniały Federację Rosyjską, aczkolwiek w czasie 5-letniego śledztwa nie udało się dowieść, że hakerzy działali na zlecenie Kremla. Główna prokurator, Heili Sepp, stwierdziła, że chociaż w trakcie śledztwa udało się ustalić dużą liczbę adresów IP związanych z atakiem, to większość z nich znajdowała się poza granicami Estonii. Niestety prośby o pomoc prawną przy dochodzeniu wysłane do rządów Federacji Rosyjskiej oraz Litwy okazały się bezskuteczne. Z powodu braku dalszych możliwości prowadzenia śledztwa Biuro Prokuratora Generalnego zamknęło postępowanie wraz z końcem lipca 2012 roku[20].

[18] Zob. Rosyjscy hackerzy podbijają Estonię, „Gazeta Wyborcza", 17.05.2007, http://gospodarka.gazeta.pl/technologie/1,81010,4140556.html [28.06.2008].

[19] 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, [26.04.2009].

[20] Zob. http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie, [27.09.2012].

Wyniki analizy specjalistów bezpieczeństwa informacyjnego wskazują[21], że część komputerów dokonujących ataków była zarejestrowana w administracji prezydenta Rosji, ale większość ataków pochodziła z zainfekowanych komputerów w Egipcie, Wietnamie oraz Peru. Na niekorzyść Rosji przemawia jedynie to, że z racji na zaszłości historyczne i prestiżowe, mogła być ona zainteresowana przeprowadzeniem takich działań.

Atak ten spowodował mobilizację Sojuszu Północnoatlantyckiego. W roku 2008 stworzono centrum ds. cyber-obrony, z siedzibą w Tallinie. Miało ono przeprowadzać symulacje, tworzyć specjalne systemy zabezpieczeń, a także przedkładać praktyczne projekty, mające na celu tworzenie podstaw cyber-bezpieczeństwa w NATO. Oczywiście chodziło o bezpieczeństwo systemów informatycznych samej instytucji, a nie krajów członkowskich. Jak się jednak okazuje, centrum to nie funkcjonuje, a przynajmniej nie tak, jak powinno. Powodem takiego stanu rzeczy, są obciążenia zarzutami o współpracę z rosyjskim wywiadem, kierowane pod adresem, pomysłodawcy i głównego dyrektora tegoż centrum. To spowodowało pewnego rodzaju klincz, z którego wyjścia nie znaleziono po dziś dzień.

Jednak estoński przykład to nie jedyny taki w Europie. W roku 2008 doszło aż dwa razy do podobnych incydentów. Pierwszy miał miejsce na Litwie. Niedługi czas po ogłoszeniu zakazu używania i posiadania symboli Związku Radzieckiego, setki stron rządowych zostało przejętych i podmienionych na inne. Zazwyczaj przedstawiały one symbole sowieckie wraz z niecenzuralnymi tekstami odnoszącymi się do władz Litwy. Był to atak mniej paraliżujący niż ten z 2007 roku, lecz ukazał jak prostym może być włamanie do systemów informatycznych należących do władz państwa.

Chronologicznie rzecz ujmując, kolejną ofiarą cyber-ataku stała się Gruzja. Miało to miejsce podczas, a tak naprawdę tuż przed, wkroczeniem armii rosyjskiej na teren Abchazji i Osetii Południowej. Atak miał charakter mieszany, co oznacza kombinację ataków DDoS i przejmowania niektórych witryn. Nie można oprzeć się wrażeniu, iż był to element normalnej rozgrywki wojennej. Paraliż informacyjny jaki zaistniał w Gruzji sprzyjał regularnym działaniom wojennym.

Wszystkie powyższe przypadki mają jeden wspólny mianownik – Federacja Rosyjska. Pomimo braku niezbitych dowodów, wszystkie trzy incydenty miały powiązanie z sytuacjami, w których dochodziło do zagrożenia interesów Moskwy.

Innym problemem, który niepokoił wiele krajów, był Irański program nuklearny. Aby z nim walczyć, zamiast tradycyjnego ataku, skorzystały one zatem z ogromnych możliwości, jakie oferują **cyberataki**. Mianowicie, w irański program nuklearny[22] uderzyły wirusy **Stuxnet, Duqu a następnie Klamer.**

[21] Po ataku Tallin stworzył oddział ochotników, którzy będą bronić kraju podczas cyberwojny, ochotników na razie jest 80. W „cywilu" to informatycy, inżynierowie, pracownicy banków, wielkich korporacji czy ministerstw. Najczęściej młodzi, 20-,30-letni ludzie. Spotykają się co tydzień w Tallinie i Tartu za: http://www.rp.pl/artykul/593688.html [12.02.2013]

[22] Były to miejscowości: Natanz oraz Fordo.

Według firmy **Symantec**, Stuxnet został zaprojektowany specjalnie po to, aby zakłócić pracę oprogramowania odpowiedzialnego za monitorowanie pracy wirówek do wzbogacania uranu w irańskim ośrodku atomowym[23]. Dzięki temu wirus był w stanie doprowadzić do poważnej awarii urządzeń kluczowych dla jego funkcjonowania.

Złośliwe oprogramowanie paraliżowało zarówno komputery jak i zautomatyzowane systemy monitorowania w obu ośrodkach badawczych. Oprócz tego, wirus wybiera losowo kilka maszyn, na których nocą odtwarza utwór „Thunderstruck" autorstwa legendarnego zespołu AC/DC, ustawiając poziom głośności na maksimum[24].

Pierwsze wzmianki dotyczące wirusa **Stuxnet**, odkryto w 2010 roku jako wersję 1.001**.** Natomiast, zebrane do tej pory dane wskazały, że jego najstarsze kompilacje pochodzą z 2005 roku.

Firma **Symantec** opublikowała raport, w którym dowodzi, że już od 2005 roku trwały prace nad wcześniejszą wersją robaka Stuxnet o numerze 0.5[25], który miał operować w Sieci od 2007 roku do 2009 roku. Stuxnet 0.5 nie był tak agresywny, jak jego późniejsze wersje, lecz wciąż był w stanie dokonać poważnych uszkodzeń. Co prawda jego celem również były irańskie instalacje nuklearne, lecz kierował się on inną strategią działania mającą za zadanie wyłączyć zawory w zakładach wzbogacania uranu w Natanz. *„To, czy misja robaka Stuxnet 0.5 powiodła się, nie jest jasne, ale jego nowsze wersje zostały opracowane przy użyciu innych ram rozwoju, stały się bardziej agresywne i zmieniły strategię ataku, która pozwoliła na zmianę prędkości wirówek do wzbogacania uranu"* – czytamy w raporcie firmy Symantec[26]. Podaje ona ponadto, że Stuxnet 0.5 w odróżnieniu od jego późniejszych wersji został opracowany w oparciu o platformę Flamer i nie zawierał żadnych **exploitów Microsoftu**. Podobnie do nich poszukiwał jednak określonego modelu **sterownika PLC** produkcji firmy Siemens.

Jego sposób działania daje podstawy aby przypuszczać, że został on najprawdopodobniej stworzony w celu szpiegowania, przeprogramowywania instalacji przemysłowych i w efekcie paraliżu centralnych jednostek w dużych zakładach przemysłowych. Strach przed Stuxnet-em jest tym większy, im lepiej uzmysłowi-

[23] Podczas prezentacji na konferencji Virus Bulletin 2010 r. w Vancouver ekspert ds. bezpieczeństwa w laboratoriach Symantec-a – Liam O'Murchu, za pomocą elektronicznej pompki powietrza podłączonej do kontrolera SIEMENS S7-300 PLC oraz oprogramowania SIMATIC Step 7 – zaprogramował czas pracy pompki aby działała ona przez 3 sekundy od włączenia. Następnie wprowadził do systemu wirusa Stuxnet, który zainfekował kontroler PLC i zmienił wprowadzone wcześniej parametry czasu pracy pompki wydłużając jej czas pracy do 140 sekund powodując pęknięcie balona – w sytuacji gdyby kontroler PLC był podłączony np. do rurociągu, elektrowni atomowej lub znajdował się na międzynarodowych lotniskach – nie trudno wyobrazić sobie konsekwencje.

[24] Zobacz więcej: http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/07/iran-zaatakowany-przez-ac-dc#ixzz2N9gwDslh, [24.08.2012].

[25] Zob. Stuxnet 0.5: How It Evolved w: http://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved, [27.02.2012].

[26] Tamże.

my sobie skalę tego problemu – specjalnie napisany wirtualny kod może być przyczyną fizycznych (realnych) zmian w fabrykach, przedsiębiorstwach, a nawet w elektrowniach nuklearnych. Po raz kolejny mamy dowód na to, jak cienka w dzisiejszych czasach jest granica między światem wirtualnym a rzeczywistością.

Z technicznego punktu widzenia Stuxnet jest nazwą trojana będącego jedynie elementem całego zagrożenia. Infekcja wirusa Stuxnet przebiega dwuetapowo:

W fazie pierwszej, Stuxnet próbuje rozprzestrzenić się poprzez komputery pracujące pod systemami Windows, jednocześnie ukrywając swoją obecność przed oprogramowaniem zabezpieczającym, przy wykorzystaniu dwóch znanych i dwóch nieopublikowanych luk bezpieczeństwa. Stuxnet: rozprzestrzenia się poprzez dyski wymienne (w systemach z włączona funkcją autostartu po włożeniu nośnika) – komputerowe systemy sterujące urządzeniami przemysłowymi – a już szczególnie strategicznymi, takimi jak np. instalacje nuklearne – które nie mają dostępu do Internetu ze względów bezpieczeństwa; rozprzestrzenia się w sieciach LAN przy wykorzystaniu luki w usłudze Windows Print Spooler; rozprzestrzenia się poprzez System Message Block; wykonuje kopie i uruchamia swój kod na komputerach zdalnych via udziały sieciowe; wykonuje kopie i uruchamia swój kod na komputerach zdalnych pracujących pod kontrolą serwera bazy danych WinCC.

W fazie drugiej Stuxnet szuka jednej rzeczy tj. stacji roboczej z systemem Windows, która prawie zawsze jest oddzielnym stanowiskiem używanym do monitorowania i kontrolowania Przemysłowych Systemów Kontroli – ICS (ang. *Industrial Control Systems*), a w szczególności takiej, która działa w oparciu o Programowalny Sterownik Logiczny PLC firmy Siemens.

Najprawdopodobniej, twórcy Stuxnet-a zdawali sobie sprawę z tego, że tego typu stacje robocze najczęściej są osiągalne dla różnego rodzaju wirusów i malwa re, tylko poprzez nośniki wymienne. Dlatego kiedy Stuxnet znajdzie to czego szuka (specyficzne urządzenie PLC marki Siemens), ukrywa swoją obecność oraz wprowadzone zmiany – zaczyna modyfikować komputerowy system kontroli przemysłowej, sabotując przy tym cały system niczym rootkit.

Ponadto Stuxnet wykorzystywał ważne, podpisane cyfrowo certyfikaty – zainfekowane sterowniki, wspomniane wyżej były podpisane przez dwie zaufane firmy – Realtek oraz JMicron. Certyfikaty te najprawdopodobniej zostały skradzione (obie firmy posiadają biura w Hsinchu Science Park w Tajwanie).

W chwili zarejestrowania pierwszych doniesień o atakach Stuxnet-a, firmy antywirusowe nie były przygotowane na ten rodzaj zagrożenia i wirus został oznaczony jako "*0-day threat*". Obecnie sprawa wygląda nieco lepiej, większość producentów oprogramowania zabezpieczającego dodała w swoich bazach sygnatur odpowiednią szczepionkę wykrywającą tego robaka.

Wszystko wskazuje więc na to, że Stuxnet nie był jednostkowym przypadkiem. Do Stuxneta i Duqu dorzućmy niemieckiego *R2D2* i jest już jasne, że na dobre wkroczyliśmy w erę ***szpiegowskich i rządowych trojanów***. Oprogramowanie stało się bronią. Następcą Stuxneta i Duqu był Flame, będący jednym z najbardziej zło-

żonych i wyrafinowanych złośliwych oprogramowań, jakie widzieliśmy – przedstawia Symantec[27]. Flame może atakować i kraść dane, co więcej może nawet nagrywać dźwięki i wysyłać je z powrotem do hakera. Diametralna różnica polega jednak na tym, że Stuxnet daje sobie rade z jednym celem na raz. Flame natomiast może w tym samym czasie uderzyć w przeszło 600 celów

Co prawda żaden rząd nie przyznał się oficjalnie do ich stworzenia i nikogo za rękę nie złapano. Eksperci są jednak zgodni co do tego, że mieliśmy tutaj do czynienia z amerykańsko-izraelską cybernetyczną akcją[28].

Warto na koniec dodać, że eksperci od bezpieczeństwa są bardzo zaskoczeni tym, iż hakerom, którzy stworzyli wirusy, udało się podszyć pod program Microsoftu. Ponadto ostrzegają, że ta sama metoda mogła zostać wykorzystana do rozsiania innych wirusów, które dopiero czekają na swoje wykrycie.

W ostatnich latach, szpiegowanie w internecie przeżywa rozkwit. Taki przynajmniej można wysnuć wniosek, gdy przyjrzymy się bliżej ujawnionej właśnie operacji „Red October", czyli „Czerwony październik". Tą wykrytą zaawansowaną kampanię cyberszpiegowską wymierzoną **przeciwko instytucjom dyplomatycznym i rządowym na całym świecie** pochwalił się Kaspersky Lab[29].

Jak informuje jeden z największych producentów komputerowego oprogramowania antywirusowego – Kaspersky – w sieci pojawiło się nowe zagrożenie. Skrótowo określane jest ono jako *Rocra*, co w rozszerzeniu ma oznaczać „**Czerwony Październik**" (Red October), (tak nazwano go ze względu na fakt, iż badania rozpoczęły się w październiku 2012 r.). Prawdopodobnie działa on od 5 lat i wykrada informacje z komputerów, smartfonów i urządzeń pamięci masowej głownie w regionie EMEA (Eastern and Central Europe) i Azji Środkowej. „Czerwony październik" ma konstrukcję modułową i jest każdorazowo dostosowywany do potrzeb ataku na konkretną ofiarę. Każdy z ponad tysiąca modułów ma własną funkcję: wykrada hasła, listy kontaktów przechowywane w urządzeniach mobilnych, kopiuje e-maile, rejestruje operacje wykonywane na klawiaturze itp.. Według Kasperski Lab źródłem wirusa jest Rosja, a potężna infrastruktura, złożona z kilkudziesięciu serwerów odpowiedzialnych za jego rozsyłanie, wskazuje, że może być to operacja rządowa, podobnie, jak miało to miejsce w przypadku wirusa Flame. „Czerwony październik" wykazuje również wiele cech wspólnych z odkrytym w 2011 r. wirusem Stuxnet, który w ciągu 11 miesięcy zainfekował 100 tys. komputerów w 155 krajach.

[27] K. Majdan, Wykryto nowe zagrożenie w http://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy, [17.02.2012].

[28] New York Times w czerwcu 2012 roku poinformował, że za stworzeniem wirusa Stuxnet stoją najprawdopodobniej rządy dwóch krajów: USA i Izraela za: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=4&pagewanted=all&, [20.08.2012].

[29] Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide w http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide, [17.02.2013].

Co ciekawe, **Czerwony Październik**, według danych podanych przez Kaspersky Lab, u swoich ofiar stosował taktykę włamywania się etapami na kolejne komputery – najpierw pozyskiwano dane z jednego komputera, za których pomocą stawało się możliwe włamanie do kolejnego, a z kolejnego do trzeciego. I tak dalej…

Kaspersky poinformował w obszernym raporcie, że akcja zakrojona była na niezwykle szeroką skalę. Objęła bowiem 69 krajów na całym świecie. Ofiarami były wysoko postawione osoby w administracji publicznej (dyplomaci, politycy), naukowcy, wojskowi, pracownicy firm energetycznych. Raport został opublikowany 14 stycznia, a Kaspersky badał sprawę od października ubiegłego roku.

Kaspersky zauważa, że w sumie na całym świecie zainfekowano setki komputerów, ale głównie osób pochodzących z byłego bloku sowieckiego oraz z Azji. Najwięcej zarażonych komputerów odkryto w Rosji (35), Kazachstanie (21), Azerbejdżanie (15). Na liście znajdują się jednak także kraje takie jak Belgia (15 zainfekowanych komputerów), Stany Zjednoczone (6), Wietnam (6) czy Szwajcaria (5).

Reasumując powyższe fakty, można stwierdzić, że akcja wymierzona była w osoby, które dysponują ważnymi informacjami, często kluczowymi dla bezpieczeństwa państwa. Infekowano więc komputery polityków i dyplomatów, wojskowych, ale także naukowców, handlowców, osób zajmujących się badaniami nad energią nuklearną, lotnictwem i energetyką.

Na uwagę zasługuje fakt, Polska jest jednym z nielicznych europejskich krajów, w których nie potwierdzono zagrożenia. Kaspersky zauważa, że sieć szpiegowska jest niezwykle zaawansowana. Ale sposób, w jaki udało się przejąć kontrolę nad wybranymi komputerami, był banalnie prosty. Wszystko zaczynało się od podrobionego maila z załącznikiem. Wysyłano przykładowo, informację o tym, że w dobrej cenie na sprzedaż jest samochód dyplomatyczny. W załączniku znajdowały się informacje na temat oferty, ale przede wszystkim – złośliwy kod, wykorzystujący lukę w programach takich jak Word czy Excel. Gdy ofiara otworzyła załącznik, na jej komputerze instalował się trojan. To jednak nie wszystko, – Wirus miał potem możliwość pobierania i instalowania kolejnych modułów złośliwego oprogramowania.

A za jego pośrednictwem hakerzy mieli już dostęp do większości informacji. Mogli przechwytywać pliki z komputera, a nawet z podłączanych USB lub telefonów (iPhone, Nokia, Windows Mobile). Mieli także dostęp do maili pobieranych przez program Outlook oraz do uderzeń w klawisze. Jednym słowem – szpiegostwo było zakrojone na bardzo dużą skalę.

Na jedno z kluczowych pytań – kto to robił? – na razie brak odpowiedzi. Co już wiemy? Kaspersky stwierdził, że serwery znajdują się w Rosji oraz w Niemczech. Exploit, czyli program wykorzystujący lukę w oprogramowaniu (w tym przypadku w Wordzie i Excelu) wyglądał na chiński, a program, który później instalowany był na komputerze ofiary na produkcję rosyjską. Kaspersky zastawił pułapkę w kilku domenach wykorzystywanych przez złośliwe oprogramowanie

i okazało się, że od 2 listopada 2012 do 10 stycznia 2013 zarejestrowano do niej aż 55 tysięcy połączeń. Najwięcej ze Szwajcarii, Kazahstanu, Grecji i Białorusi.

Jak na razie nie ma dowodów na to, że ataki sponsorowane były przez konkretne państwo. Nie wiadomo też, co działo się z wykradzionymi danymi. Mogły być one sprzedawane na czarnym rynku, a mogły być też wykorzystywane przez samych hakerów.

A więc kto? Rząd jakiegoś kraju? Zważywszy na skalę operacji to prawdopodobna wersja – wiele państw prowadzi szeroko zakrojone akcje szpiegowskie i nic dziwnego, że przenoszą się one do Internetu. Przeciwko może, pozornie, wskazywać pochodzenie oprogramowania. Pozornie, bo przecież można przyjąć, że zebrano po prostu najlepszy dostępny software.

Z drugiej jednak strony, państwa niechętnie wykorzystują programy obcego pochodzenia – bezpieczniej jest napisać coś własnego. Może więc jest to raczej wielka akcja międzynarodowej organizacji terrorystycznej?

Powstanie jednostek do walki w cyberprzestrzeni

Z tego co dotychczas przedstawiono wynika jednoznacznie, że powszechna komputeryzacja i dynamiczny rozwój Internetu na początku XXI wieku, wykazują sprzyjanie wykorzystania przez „specjalistów" cyberprzestrzeni, do groźnych działań naruszających bezpieczeństwo wielu państw. W ocenie niezależnych ekspertów, w grupie państw, które jako pierwsze zaczęły stosować na szerszą skalę, planowe i zorganizowane formy cyberataków dla realizacji własnych celów politycznych, wywiadowczych i militarnych, są przede wszystkim: USA, Rosja i Chiny. Amerykanie jednak przyznają, że są daleko w tyle, w tym zakresie, za Rosją i Chinami[30].

W ocenie Pentagonu, czyli Departamentu Obrony USA, powyższe przesłanki, zmuszają Departament Obrony i rząd USA do wzmocnienia systemu obrony państwa przed cyberatakami[31]. Dlatego, organizowane są cybernetyczne siły zbrojne.

Z analizy literatury przedmiotu wynika, że *United States Cyber Command* (*USCYBERCOM*) to specjalna komórka amerykańskiej armii przystosowana do prowadzenia walki na polu najnowszych technologii teleinformatycznych. *USCYBERCOM* rozpoczął swą działalność **21 maja 2010 roku** i od samego początku rekrutuje przede wszystkim specjalistów z zakresu obrony systemów teleinformatycznych, nie jest jednak tajemnicą, że do pracy na rzecz amerykańskiego rządu poszukiwane

[30] USA w obronie przeciw cyberwojnie buduje cyberarmię, w: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html, [08.01.2013].

[31] USA w obronie przeciw cyberwojnie buduje cyberarmię, zobacz w: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html, [08.01.2013].

są również osoby obdarzone unikalnymi umiejętnościami w zakresie naruszania bezpieczeństwa[32].

USCYBERCOM, odpowiada za scentralizowanie tajnych operacji prowadzonych w cyberprzestrzeni i za organizację dostępnych zasobów informacyjnych, a także ochronę amerykańskich sieci wojskowych. Obecnie Pentagon chce zwiększyć jej skład osobowy – z 900 do 4900 osób. W związku z tym mają powstać 3 oddzielne rodzaje „cybernetycznych sił zbrojnych" – 1) Cyber National Mission Forces, 2) Cyber Protection Forces i 3) Cyber Combat Mission Forces[33]

Te pierwsze siły będą odpowiedzialne za ochronę „krytycznej infrastruktury państwa", drugie – za ochronę sieci Departamentu Obrony, a trzecie będą prowadzić planowanie i przeprowadzać planowane ataki w cyberprzestrzeni. Zdaniem amerykańskich ekspertów wojskowych, już dzisiaj i w przyszłości nie liczą się, a jeśli to w niewielkim stopniu – działania sił militarnych między wrogimi stronami, lecz przede wszystkim cybernetyczne[34].

Wnioski te wynikają, przede wszystkim z obserwacji zmian i wydarzeń zachodzących w cyberprzestrzeni. Obserwowane wydarzenia skłoniły Amerykanów do powiększenia swoich cybernetycznych sił zbrojnych. W dzisiejszej cyberprzestrzeni dochodzi do poważnych, świetnie zorganizowanych ataków. Od jakiegoś czasu istnieją też uzasadnione podejrzenia, że USA są atakowane przez obce kraje, albo bardzo dobrze finansowane grupy przestępcze.

Zdaniem Alana Pallera, dyrektora ds. badań w SANS Institute, Chiny i Rosja mają znacznie bardziej rozbudowane i lepiej zorganizowane cybernetyczne armie. USA dopiero starają się im dorównać. Paller uważa, że prawdziwym wyzwaniem będzie znalezienie odpowiedniej liczby specjalistów. *Problem ze znalezieniem tych 4000 jest taki, że każda istotna gałąź gospodarki – banki, firmy energetyczne, telekomunikacyjne, przemysł obronny, szpitale, rząd i samorządy – poszukują tych samych ludzi* – mówi Paller. Zapotrzebowanie na najwyższej klasy specjalistów jest olbrzymie, jednak takich osób brakuje na rynku[35].

[32] *Pentagon buduje cyberarmię* w: http://tech.wp.pl/kat,130034,title,Pentagon-buduje-cyberarmie,wid,15291699,wiadomosc.html?ticaid=110374, [08.01.2013].

[33] Zob. w http://kopalniawiedzy.pl/Cyber-Command-cybernetyczne-sily-zbrojne-NSA-Keith-Alexander,17428, [17.01.2013].

[34] Według najnowszych informacji, Pentagon tworzy kilkanaście „ekip cybernetycznych" (ang. cyber teams), których zadaniem będzie prowadzenie ofensywnych operacji, mających zwalczać zagrożenie Stanów Zjednoczonych atakami cybernetycznymi na ważne obiekty infrastrukturalne. Poinformował o tym 12.03.2013 w senackiej komisji ds. sił zbrojnych generał Keith Alexander, który stoi na czele dowództwa ds. cyberprzestrzeni (United States Cyber Command). Podkreślił, że groźba ataków na sieć elektryczną kraju i inne żywotnie ważne systemy jest realna i że potrzebne są bardziej agresywne posunięcia rządu i sektora prywatnego, mające na celu poprawę obrony przed takimi atakami. Powiedział też, że te ekipy będą działały poza Stanami Zjednoczonymi, ale nie ujawnił, gdzie. Określenia wymaga, według generała, co jest aktem wojny cybernetycznej w: http://niewiarygodne.pl/kat,1031991,title,Pentagon-tworzy-ekipy-do-zwalczania-zagrozen-w-cyberprzestrzeni,wid,15408475,wiadomosc.html?smgajticaid=6103b8 [15.02.2013].

[35] M. Błoński, *USA budują cyberarmię* w: http://www.wykop.pl/ramka/1395241/usa-buduja-cyberarmie.

Na podstawie powyższych faktów należy stwierdzić, że Pentagon podchodzi poważnie do cyberzagrożeń. Departament Obrony Stanów Zjednoczonych postanowił przygotować model Internetu, by ćwiczyć w nim różne możliwe scenariusze przebiegu cyberwojny. Cyberpoligon ma być gotowy już za rok, a posłuży zarówno do testowania działań defensywnych jak i ofensywnych[36].

Plany projektu zostały przygotowane przez firmę Lockheed Martin, która uzyskała grant w wysokości 30,8 mln dol. od Agencji Zaawansowanych Obronnych Projektów Badawczych (DARPA). Konkurencyjny projekt powstał w Laboratorium Fizyki Stosowanej Uniwersytetu Johna Hopkinsa, które otrzymało w tym celu 24,7 mln dolarów.

Cyberpoligon **ma imitować rządowe, wojskowe i komercyjne sieci oraz ludzkie zachowania i słabości** w czasie działania różnych poziomach gotowości obronnej oraz podczas wykonywaniu planów bojowych. DARPA chce, by symulator mógł jednocześnie obsługiwać wiele testów i scenariuszy dotyczących działań ofensywnych i defensywnych, jakich zastosowanie może być w przyszłości konieczne.

Już do tej pory Lockhead Martin i Uniwersytet Johna Hopkinsa powinny stworzyć prototypy cyberpoligonu, które zostaną przedstawione do oceny. DARPA wybierze z nich tylko jeden, który faktycznie zostanie zrealizowany i wdrożony.

Najwyraźniej **rząd USA coraz poważniej podchodzi do cyberzagrożeń** i ma zamiar przygotować się na ewentualne ataki płynące z Internetu. Już wcześniej Pentagon twierdził, że cyberataki będą traktowane z taką samą stanowczością jak tradycyjne ataki wymierzone w bezpieczeństwo kraju.

Kolejnym państwem, które posiada cyberarmię są Chiny. W literaturze przedmiotu podkreśla się fakt, że Chiny od dawna podejrzewane są o cyberataki na cele znajdujące się na terenie innych państwach. Wiele trojanów szpiegowskich prawdopodobnie pochodzi z Chin, lecz nie można tego dowieść z całą pewnością. Jednak 16 lipca 2011 państwowy kanał CCTV 7 (Wojskowość i Rolnictwo) wyemitował program dokumentalny „Technologia wojskowa: nadchodzi internetowa burza", w którym pokazano nagranie ataku wyprowadzonego z chińskiego systemu rządowego na cel położony w USA. Dowód na istnienie oprogramowania umożliwiającego takie ataki to wiadomość na pierwsze strony gazet – przekonywał Mikko Hypponen, szef działu badań F-Secure, fińskiego producenta oprogramowania zabezpieczającego[37].

Ponadto, w wywiadzie dla agencji Xinhua, Geng Yansheng przedstawiciel chińskiego ministerstwa obrony przyznał, że Chiny posiadają jednostkę „wojsk internetowych". Geng Yansheng stwierdził, że celem istnienia jednostki jest obrona chińskiej cyberprzestrzeni przed atakami z zewnątrz, istnieje ona od 2009 roku i liczy około 30 osób. Jednak upublicznione raporty wywiadów wskazują na co

[36] *Pentagon tworzy symulator cyberwojny* w: http://www.pcworld.pl/news/372262/Pentagon.tworzy.symulator.cyberwojny.html, [08.01.2013].

[37] Zob. http://military.cntv.cn/program/jskj/20110717/100139.shtml, [08.01.2013].

najmniej pięcioletnie istnienie chińskiego internetowego oddziału ofensywnego, liczącego też dużo więcej niż 30 osób.

Ściśle tajna jednostka chińskiej armii – ujawniona zostaje także w raporcie amerykańskiej firmy Mandiant, pilnującej bezpieczeństwa w Internecie – i nazywana jest najgroźniejszymi cyberterrorystami świata. *To setki, może tysiące supersprawnych speców od komputerów posługujących się nienaganną angielszczyzną. Kradną strategie i plany biznesowe, e-maile, listy kontaktów, tajne dane firm i instytucji. Nie mamy wątpliwości – działają w Chinach, a chiński rząd dobrze o tym wie*[38].

Autorzy raportu przez sześć lat tropili chińskich hakerów, którzy w tajnych amerykańskich dokumentach figurują jako *Comment Group*. Wszystkie tropy prowadzą do Szanghaju, do dowództwa jednostki 61398 armii chińskiej – przekonują. Siedziba, to biały, niepozorny, 12-piętrowy biurowiec, otoczony restauracjami i budynkami mieszkalnymi, stoi w podupadłej dzielnicy Pudong na przedmieściach Szanghaju.

Postronny obserwator nigdy nie zauważyłby, że właśnie tu znajduje się baza dowództwa tajemniczej Jednostki 61398, która właśnie trafiła na czołówki światowych mediów. Formalna nazwa to *Drugie Biuro Trzeciego Departamentu Sztabu Generalnego Ludowej Armii Wyzwoleńczej*. Oficjalnie biuro nie istnieje w opisach wojskowych struktur.

Ogrom dowodów wskazuje, że 90 proc. ataków pochodzi z Jednostki 61398, grupa miała kilka nazw w tajnych amerykańskich depeszach teraz figuruje jako „Comment Crew" albo „Shanghai Group".

Analizując specjalny raport Mandiant, należy przytoczyć jego najważniejsze tezy i spostrzeżenia: *61398 jest obsadzana przez setki, a może tysiące wydajnych anglojęzycznych hakerów z zaawansowanymi umiejętnościami bezpieczeństwa komputerowego i pracy w sieci. Jednostka włamała się do 141 firm w 20 branżach, z czego 87% z siedzibą w krajach anglojęzycznych. 61398 jest w stanie kraść dane z kilkudziesięciu sieci jednocześnie. Specjalna komórka wykradła setki terrabajtów informacji, w tym plany wojskowe, plany biznesowe, e-maile, a także listy kontaktów*[39].

Oczywiście Chińczycy odpierają zarzuty twierdząc, że ataki hakerskie są „ponadnarodowe i niemal niemożliwe jest wyśledzenie ich źródła". Wygląda więc na to, że jesteśmy świadkami kolejnej batalii toczonej między mocarstwem „u schyłku", a nowym „imperatorem". W tej bitwie, Stany Zjednoczone za żadne skarby nie chcą jednak, oddać swojej pozycji informacyjnego lidera i starają się wpływać na opinię publiczną w celu wykreowania niekorzystnego obrazu Chin. Należy jednak pamiętać o tym, że amerykański miecz jest obosieczny, a USA także dysponują systemami (np. Echelon czy Carnivole) będącymi w stanie inwigilować ludzkość.

[38] Zob. Raport Mandiat APT1 Exposing One of China's Cyber Espionage Units w: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, [22.02.2013].

[39] Tamże s.4.

Kolejnym państwem to Niemcy, które oficjalnie poinformowało, że powołało do życia dwie nowe organizacje rządowe. Ich praca będzie bezpośrednio związana z bezpieczeństwem Internetu i prowadzeniem cyberwojny. Pierwsza organizacja otrzymała nazwę Nationales Cyber-Abwehrzentrum (NCAZ), a druga Nationaler Cyber-Sicherheitsrat. Mają one pilnować niemieckiej infrastruktury przemysłowej i wojskowej przed atakami ze strony hakerów i bronić jej w przypadku wybuchu cyberwojny[40].

Nationaler Cyber-Sicherheitsrat rozpoczęła prace pierwszego kwietnia 2011 roku. Na czele organizacji stanęła Cornelia Rogall-Grothe sekretarz stanu w niemieckim Ministerstwie Spraw Wewnętrznych. Członkami organizacji są także wysoko postawione osoby z ministerstw spraw wewnętrznych, obrony, sprawiedliwości czy finansów. Tymczasem szeregi NCAZ, przynajmniej w początkowym okresie działania, zasilają pracownicy Federalnego Biura ds. Bezpieczeństwa Informacji czy Federalnego Biura Ochrony Konstytucji.

W dokumencie opisującym obie organizacje pojawiają się trzy powody, dla których powołano je do życia. Pierwszym z nich jest rosnące zagrożenie ze strony wyspecjalizowanego malware'u i konieczność posiadania środków umożliwiających wytropienie i odpowiedzenie na cyberataki. Drugim jest rosnąca ilość „czułych punktów" przemysłu, od kiedy w coraz większym stopniu korzysta on z zaawansowanych technologii. Trzecim jest zagrożenie związane z robakami takimi jak Stuxnet. Niemcy wzywają przy okazji Unię Europejską, NATO oraz własne siły zbrojne do zacieśnienia współpracy w celu zabezpieczenia krajów członkowskich przed cyberatakami[41].

Bardziej skomplikowana sytuacja związana z cyberjednostkami jest w Rosji. Pomimo, że w mediach i raportach firm zajmujących się bezpieczeństwem w cyberprzestrzeni, pełno jest oskarżeń pod adresem Rosji, to oficjalnie Rosja dopiero zaczyna tworzyć te formacje.

W marcu 2012 roku Wicepremier Obrony Narodowej Rosji, Dmitrij Rogozin zapowiedział utworzyć CyberDowództwo, powiedział wtedy, że wszystkie dokumenty zostały już przygotowane i wyraził nadzieję, że CyberDowództwo pojawi się bardzo szybko.

Natomiast z informacji, które można znaleźć na stronie „Izwiestii" z 12.02.2013 wynika, że jeśli zostanie zatwierdzony plan utworzenia CyberDowództwa przez przywództwo polityczne Rosji to przed 2014 rokiem Dowództwo rozpocznie swoją pracę[42]. Czytamy tam także, że według wysokiego rangą źródła w Ministerstwie Obrony, przyszłość dowodzenia w ramach CyberDowództwa jest w dużej mierze

[40] Minister Obrony Narodowej otwiera Centrum Cyberobrony Narodowej w: http://www.heise.de/newsticker/meldung/Innenminister-eroeffnet-nationales-Cyber-Abwehrzentrum-1261659.html, [09.10.2012].

[41] Strategia Cyberobrony dla Niemiec w: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf, [08.02.2013].

[42] Zob. W Rosji cyberwojska w: http://bashgazet.ru/rus/news/nrf/2477-v-rossii-poyavyatsya-kibervoyska.html, [08.01.2013].

powtórzeniem funkcji i struktury amerykańskiego USCYBERCOM. Rosyjskie Dowództwo Cyber będzie pracowało dla wojska, organów ścigania i wszystkich władz cywilnych i że głównym celem będzie ochrona interesów narodowych[43].

Przypomnijmy, w Rosji istnieje już kilka organów monitorujących zagrożenia z cyberprzestrzeni. Ministerstwo Spraw Wewnętrznych, posiada biuro „K", natomiast FSB – Centrum Bezpieczeństwa Informacji, natomiast za prowadzenie operacji z dziedziny walki informacyjnej w wymiarze strategicznym odpowiada Kolegium Federalnej Łączności i Informacji (FAPSI).

W literaturze przedmiotu można znaleźć także, wzmianki dotyczące innych państw, które posiadają jednostki przygotowane do walki w cyberprzestrzeni, są to między innymi: Wielka Brytania, Izrael, Iran, Korea Północna.

Polska także powołała do życia nową strukturę organizacyjną pod nazwą: Centrum Bezpieczeństwa Cybernetycznego[44]. Centrum działa w Białobrzegach, gdzie rozlokowany jest 9. Batalion Łączności. Pracuje od lata 2010 roku. I to wszystko, co o nim oficjalnie wiadomo. MON nie chce ujawniać szczegółów. Udało się ustalić, że wojskowi eksperci komputerowi ochraniają urzędy Ministerstwa Obrony Narodowej i dowództwa wojskowe, które są regularnym celem ataków hakerskich. W 2011 r. ministerstwo obrony planowało przeznaczyć miliard złotych na informatyzację. Miał powstać m.in. pierwszy batalion cyfrowy w naszej armii. Żołnierze i ich dowódcy korzystali by z najnowszych zdobyczy techniki, takich jak chociażby wyświetlacze dostarczające potrzebnych informacji na polu walki[45].

Wnioski i podsumowanie

Cyberprzestrzeń stała się nowym obszarem starcia, co pociąga za sobą konieczność dokonania licznych zmian zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa globalnie, czy też w każdym państwie oraz organizacji lokalnie.

Budowa systemu prawnego, stanowiącego odpowiedź państwa na szanse i wyzwania związane z jego obecnością w cyberprzestrzeni, jest zadaniem niezwykle złożonym. Wynika to nie tylko z tempa zmian technologicznych, ale także ze szczególnego charakteru środowiska i jego „interaktywnej" natury.

Kształtując normy prawne na poziomie krajowym, przepisy regulujące współpracę międzynarodową oraz strategie i polityki bezpieczeństwa, należy zatem uwzględniać te dwa podstawowe wyzwania. Konieczność, z jednej strony, szyb-

[43] Zob. Rosyjscy wojskowi przygotowują się do cyberwojen w: http://www.radiovesti.ru/articles/2013-02-12/fm/81961, [08.01.2013].

[44] Wizyta Szefa BBN w Centrum Bezpieczeństwa Cybernetycznego w: http://www.bbn.gov.pl/portal/pl/2/3305/Wizyta_Szefa_BBN_w_Centrum_Bezpieczenstwa_Cybernetycznego.html, [08.02.2013].

[45] Polska armia broni się przed atakami hakerów w: http://wiadomosci.wp.pl/kat,8311,title,Polska-armia-broni-sie-przed-atakami-hakerow,wid,12902309,wiadomosc.html, [08.02.2013].

kiego reagowania, a z drugiej – reagowania na zagrożenia ze strony małych, mobilnych grup stanowią nową jakość w obszarze formułowania przepisów regulujących funkcjonowanie państwa w sferze bezpieczeństwa[46].

Nie można zapominać, że choć zagrożenia w cyberprzestrzeni stanowią odmienną kategorię wyzwań legislacyjno-organizacyjnych, to problemy, które stwarzają, w znacznej mierze przypominają te, generowane przez inne zagrożenia asymetryczne, jak np. terroryzm. Ich wspólną cechą jest zmuszanie struktur państwowych do ewolucji w stronę rozwiązań mniej hierarchicznych, a bardziej elastycznych. Sieciowość, zarówno w wymiarze społecznym, jak i technologicznym, wraz z jej wszystkimi konsekwencjami, zdaje się stanowić jedno z najważniejszych pojęć nowego paradygmatu bezpieczeństwa na poziomie krajowym i międzynarodowym.

Cyberwojna jest faktem. W ciągu ostatniego roku liczba umotywowanych politycznie ataków przez Internet przekroczyła poziom alarmowy. W samych tylko Stanach Zjednoczonych celami ataków były: Biały Dom, Ministerstwo Bezpieczeństwa Wewnętrznego, Tajna Służba Stanów Zjednoczonych (Secret Service) oraz Ministerstwo Obrony. Państwa angażują się w wyścig cyber-zbrojeń i rozwijają możliwości prowadzenia cyber-wojny, w której głównymi celami będą sieci rządowe i infrastruktura o znaczeniu krytycznym. Jednak cyber-wojna, to nie tylko wojna pomiędzy komputerami. Może spowodować prawdziwe zniszczenia w świecie realnym i śmierć wielu osób[47].

Celem cyberbroni jest infrastruktura o znaczeniu krytycznym. Posiadacze broni przygotowują nie tylko cyberobronę, ale także cyberataki skierowane m.in. przeciwko sieciom energetycznym, transportowym, telekomunikacyjnym, systemom finansowym oraz systemom zaopatrzenia w wodę, gdyż można je unieruchomić szybko i stosunkowo niewielkim nakładem sił. W większości krajów rozwiniętych infrastruktura o znaczeniu krytycznym jest podłączona do Internetu i nie jest właściwie chroniona – dlatego te instalacje są szczególnie podatne na zagrożenia. Brak odpowiedniej ochrony oraz brak przygotowania sprawiają, że w dzisiejszych czasach atak na te systemy spowodowałby o wiele większe zniszczenia, niż ataki zdarzające się w przeszłości.

W cyberwojnę uwikłanych jest tak wielu różnych graczy działających na tak wiele rożnych sposobów, że reguły zaangażowania nie są jasno określone. Nie jest też jasne, jakie obowiązki należy powierzyć przedsiębiorstwom i instytucjom w związku z ochroną i edukacją społeczeństwa w zakresie zapobiegania cyberatakom. Bez właściwej definicji brak jest jednoznacznych kryteriów do podjęcia decyzji, kiedy właściwą odpowiedzią na cyber-atak jest reakcja polityczna, a nawet groźba akcji militarnej.

[46] Por. Krzysztof Liedel i Paulina Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, Kwartalnik „Bezpieczeństwo narodowe", Nr 17/2011, s. 25 i dalsze.

[47] Czy trzecia wojna rozpocznie się w Internecie w: http://forum.gazeta.pl/forum/w,101385, 130897447,130920749,Czy_trzecia_wojna_swiatowa_rozegra_sie_w_interneci.html, [14.01.2013].

Najbardziej zagrożony jest sektor prywatny. W wielu krajach rozwiniętych infrastruktura o znaczeniu krytycznym jest własnością prywatną, przez co jest ona znakomitym celem cyberataków. Jednak w zakresie zapobiegania cyberatakom sektor prywatny w znacznym stopniu polega na działaniach rządowych. Jeśli rozpocznie się wirtualny ostrzał, w ogniu walki znajdą się zarówno instytucje rządowe, przedsiębiorstwa, jak i zwykli obywatele. Bez względu w rządową strategię cyber-obrony sektor prywatny nie jest w stanie podjąć skutecznych działań prewencyjnych. Dlatego eksperci nawołują do wydobycia problemu cyberwojny na światło dzienne i przeprowadzenia na jej temat publicznej debaty.

Bibliografia

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.

BIODO Uwagi do Polityki Ochrony Cyberprzestrzeni RP.pdf w: http://mac.bip.gov.pl/fobjects/details/3564/biodo-uwagi-do-polityki-ochrony-cyberprzestrzeni-rp-pdf.html.

Czy trzecia wojna rozpocznie się w Internecie w: http://forum.gazeta.pl/forum/w,101385,130897447,130920749,Czy_trzecia_wojna_swiatowa_rozegra_sie_w_interneci.html.

E-Eesti/E-Estonia, http://webstatic.vm.ee/static/failid/286/E-Estonia_uus.pdf.

Gregory J. Rattray „Wojna strategiczna w cyberprzestrzeni", Warszawa 2004.

http://kopalniawiedzy.pl/Cyber-Command-cybernetyczne-sily-zbrojne-NSA-Keith-Alexander,17428.

http://military.cntv.cn/program/jskj/20110717/100139.shtml.

http://niewiarygodne.pl/kat,1031991,title,Pentagon-tworzy-ekipy-do-zwalczania-zagrozen-w-cyberprzestrzeni,wid,15408475,wiadomosc.html?smgajticaid=6103b8.

http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/07/iran-zaatakowany-przez-ac-dc#ixzz2N9gwDslh.

http://www.heise.de/newsticker/meldung/Innenminister-eroeffnet-nationales-Cyber-Abwehrzentrum-1261659.html.

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=4&pagewanted=all&.

http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie.

http://www.rp.pl/artykul/593688.html.

i-słownik: http://www.i-slownik.pl/323,cyberprzestrzen/.

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.

K. Majdan, Wykryto nowe zagrożenie w http://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy.

Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide w

http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

Krzysztof Liedel i Paulina Piasecka, Wojna cybernetyczna – wyzwanie XXI wieku, Kwartalnik „Bezpieczeństwo narodowe", Nr 17/2011.

M. Błoński, USA budują cyberarmię w: http://www.wykop.pl/ramka/1395241/usa-budujacyberarmie.

Norma ISO/TEC 27001:2007, Technika informatyczna, Technika bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa 2007.

Pentagon buduje cyberarmię w: http://tech.wp.pl/kat,130034,title,Pentagon-budujecyberarmie,wid,15291699,wiadomosc.html?ticaid=110374.

Pentagon tworzy symulator cyberwojny w: http://www.pcworld.pl/news/372262/Pentagon.tworzy.symulator.cyberwojny.html.

Polska armia broni się przed atakami hakerów w: http://wiadomosci.wp.pl/kat,8311,title,Polska-armia-broni-sie-przed-atakami-hakerow,wid,12902309,wiadomosc.html.

Raport Mandiat APT1 Exposing One of China's Cyber Espionage Units w: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

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

Rosyjscy wojskowi przygotowują się do cyberwojen w: http://www.radiovesti.ru/articles/2013-02-12/fm/81961.

Strategia Cyberobrony dla Niemiec w: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf.

Stuxnet 0.5: How It Evolved w: http://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved.

US Department of Defense Strategy for Operating in Cyberspace, Departament Obrony USA, lipiec 2011 r., http://www.defense.gov/news/d20110714cyber.pdf.

USA w obronie przeciw cyberwojnie buduje cyberarmię, w: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP.

W Rosji cyberwojska w: http://bashgazet.ru/rus/news/nrf/2477-v-rossii-poyavyatsya-kibervoyska.html.

Wizyta Szefa BBN w Centrum Bezpieczeństwa Cybernetycznego w: http://www.bbn.gov.pl/portal/pl/2/3305/Wizyta_Szefa_BBN_w_Centrum_Bezpieczenstwa_Cybernetycznego.html.

CYBERSPACE AS A NEW QUALITY OF HAZARDS

Abstract

The article aims at presenting the essence of the concept of 'cyberspace'. Particular attention was placed on the very complicated, scientific and legal lineage related to IT technology, IT systems, etc. The article depicts the examples of the biggest cyber attacks observed in the last decade as well as their relation with other areas of critical infrastructure. There is also a reference to issues concerning the structure of units dealing with the phenomenon, as well as countries which are in the possession of special units to perform tasks within cyberspace. All in all, however, the presented information should be taken as an outline of the tackled problems, an outline organizing the knowledge concerning the multifaceted and interdisciplinary concept of cyberspace.

Key words – cyberspace, hazards, security

Introduction

The hazards stemming from cyberspace are not new phenomena. The present image of cyberspace makes it necessary to treat this sphere as a strategic one for the security of a country. There are two basic reasons supporting the idea: firstly, Information Technology[1] is the key component of the critical infrastructure of a country, e.g. it is used in the management of electricity networks, telecommunications, transport, banking, healthcare, etc. – thus a cyber attack on the critical infrastructure can automatically jeopardize the security of the whole country; secondly, IT plays a significant role in any conflict since it is the key element in management centres as well as command posts concerning not only strategic resources but also the Armed Forces.

The deliberation concerning 'cyberspace' should start with the attempt to define the concept. It is not a simple task, since in spite of numerous efforts there is no commonly accepted concept apparatus within this area, and particular notions are adequate for use in certain 'schools of thought'.

It is very probable that the concept of 'cyberspace' was used for the first time in 1984 by an American writer William Gibson[2] in his novel *Burning Chrome*. It

[1] Wikipedia – the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data

[2] William Gibson (born on 17 March 1948 in Conway, South Carolina) – American science fiction writer, the inventor of cyberpunk.

was a computer generated world of immersion[3], virtual reality, which the American classical writer of the cyberpunk novel referred to in the first volume of his trilogy – *Neuromancer* – as a matrix. However, the term cyberspace was popularized for good by common access to the Internet, as well as films based on Gibson's motives, like e.g. *Johny Mnemonic*, or the trilogy *Matrix, which meant hallucination.*

Moreover, it can be stated that at the beginning of the '90s the concept of 'cyberspace' started to be commonly used. At that moment the development of Information Technology was at such a level that Nicholas Negroponte announced that the atom had ceased to be the elementary element and was replaced by a binary number. Whereas, Philip Elmer DeWitt described cyberspace as 'Plato's plane of ideal forms, metaphorical space, a virtual reality'[4]. However, we should not get carried away by this type of fantasy – cyberspace is a physical domain. Nowadays, except land, sea, air or space there is another environment for human activity (including military ones). Nonetheless, it is very different from the three enumerated. First of all, it is an entirely man-made area, being the result of the creation of IT systems and networks enabling electronic communication. Moreover, the participants of this battle field have full control over the environment's qualities. Still, the destruction or even deformation of the digital elements result in a topographical change of the operation area. It can be compared to a land battle when suddenly a mountain appears or disappears. In cyber warfare, geography and geopolitics are totally meaningless. In 1995, the RAND Corporation[5] was asked by the United States Department of Defense to check the possibilities of strategic information warfare. The final report concludes that the techniques of information warfare totally disregard geographical distance; the goals within the US borders are as susceptible as the ones in the local theatre of war operations[6]. It means that an attack can be carried out from any place on the Earth.

A similar definition is provided by a dictionary 'i-słownik': (Eng. *cyberspace*; Greek *kybernetes* – steersman, governor as well as to control, to manage) – recently the prefix *cyber* – is connected with new, electronic technology and is used in an IT, interactive meaning. In other words, the concept refers to everything connected with computers. Cyberspace is a communication space created by a system of Internet links. Cyberspace, similarly to telecommunications, makes it easier for the network users to contact other people, also in real time. It is the space

[3] Immersion – a situation when a text is accompanied by a picture, sound, or animation as well as a rich system of connections, offering the possibility of free choice, it can facilitate the experience of immersion, being surrounded by the world created by the piece of art.

[4] Vide: Gregory J. Rattray „Wojna strategiczna w cyberprzestrzeni" (original title: *Strategic Warfare in Syberspace*), Warszawa 2004, p. 29.

[5] RAND Corporation – American nonprofit research institution originally formed for the needs of the US Armed Forces.

[6] Gregory J. Rattray „Wojna strategiczna w cyberprzestrzeni" (original title: *Strategic Warfare in Syberspace*), Warszawa 2004, p.24

between open communication through connected computers and IT links in the whole globe. The definition entails all electronic communication systems (including classical telephone networks), which transfer information from numerical sources. Thus, it can be assumed that cyberspace is slowly becoming a basic channel of information exchange[7].

However, according to the US Department of Defense, cyberspace, similarly to the domains of land, sea, and air, has become another domain for warfare[8]. It is defined as *'an interdependent and interrelated infrastructural IT network, including the Internet, telecommunication networks, computer systems and the systems managing production processes and control in strategic sectors connected to national security'.* It is a comprehensive attitude. The Americans pay less attention to the ownership of the strategic sector and focus more on its defence. A similar practical approach is presented by other western countries.

The Polish legal system also defines the concept of cyberspace. The definition of this incredibly important notion is included in the amendment of the Act of 30 August 2011 on the martial law and the competences of the Chief of the Polish Armed Forces and rules governing his subordination to the constitutional bodies of the Republic of Poland. The above document defines cyberspace as the domain of information processing and exchange, created by ICT systems, determined in Art. 3 point 3 of the Act of 17 February 2005 on the computerization of activities of entities performing public tasks[9].

At the same time, it should be stated that the Ministry of Administration and Digitization of Poland, being responsible for the coordination of the general security policy of Polish cyberspace, is still working on providing definitions for difficult concepts in a document entitled 'Polityka Ochrony Cyberprzestrzeni RP' (Polish Cyber Defence Policy)[10]. In this document, in a chapter entitled 'Definitions' Cyberspace is defined as the domain for information processing and exchange, created by ICT systems, determined in Art. 3 point 3 of the Act of 17 February 2005 on the computerization of activities of entities performing public tasks (Journal of Laws No. 64, item 565, with further amendments) alongside with connections between them and relations with the users; in accordance with the Act of 30 August 2011 on the amendment of the Act on martial law and the competences of the Chief of the Polish Armed Forces and regulations governing his subordination to the constitutional bodies of the Republic of Poland and other

[7] vide: i-słownik: http://www.i-slownik.pl/323,cyberprzestrzen/, [27.02.2012].

[8] US Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf, [22.08.2011].

[9] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP (Act of 29 August 2002 on military law and the competences of the Chief of the Polish Armed Forces and rules governing his subordination to the constitutional bodies of the Republic of Poland).

[10] 23 November 2012 the Minister Michał Boni asked for a change in the cabinet's list of legislative and non legislative acts concerning the title of the document 'Programme of Cyberspace Defence' into 'Polish Cyber Defence Policy'.

acts (Journal of Laws No. 222, item 1323). In further part, the cyberspace of the Republic of Poland (referred to as CRP) was defined as such: the cyberspace within the borders of Poland and beyond them, in places where the representatives of the Republic of Poland are present (diplomatic posts, military contingent).

At this point a certain inaccuracy can be noticed, since the definition of cyberspace presented by the quoted law regulations does not entail the computer devices of the citizens of Poland, it mentions terminals such as[11] – modem, phone, router or network interface card. Taking into consideration the above, one can assume that a computer or other device of a citizen or an entrepreneur, connected to the Internet via the router or modem of a telecommunication company is not an element of cyberspace, thus the concepts of a cyber attack or cybercrime are not applicable here. Due to that, it warranted that the definitions of 'cyberspace' and 'the cyberspace of the Republic of Poland' should be changed in such a way that they include technical resource – devices of every user of CRP including every individual citizen and entrepreneurs. In other words, it should be expressed more precisely that computers, servers, TV sets, SAT decoders are all called terminals of cyberspace.

It should be also emphasized that the concept of a cyber attack[12] does not include attacks from Polish cyberspace on the cyberspace of other countries, since the concept was artificially limited to technical resources defined by the Polish law regulations i.e. the Act of 17 February 2005 on the computerization of activities of entities performing public tasks and telecommunication law, referred to by the act quoted in the definition of cyberspace. It means that an attack launched with the use of Polish cyberspace aimed at the cyberspace of another country, is not a 'cyber attack' because of the fact that the concept 'cyberspace' does not include the cyberspace of other countries, nor global cyberspace.

To conclude, it is important to emphasize that the concepts used in the mentioned document are not clear and comprehensible for every citizen of the Republic of Poland and result in an unnecessary legal mess. Specifying the term 'cyberspace', it refers to the Act of 17 February 2005 on the computerization of activities of entities performing public tasks, and the latter refers to the telecommunication law pointing at the 'network termination' (of cyberspace) in the form of a router, modem, network interface card, or a telephone in every citizens' household. Unfortunately, the computer connected by router does not belong to the resources of cyberspace in accordance with the biding definition.

Due to the above mentioned fact, there is a need to redefine the concepts of 'cyberspace' and 'the cyberspace of the Republic of Poland', as well as deliberate on the concepts of a 'cyber attack', 'cybercrime' and, finally, implement the

[11] In the act there is an entry 'telecommunication terminal device – a telecommunication device for a direct or indirect connection to the network termination (Art. 2 point. 43).

[12] Cyber attack – intentional interference in proper cyberspace functioning – Polityka CBR, p. 6.

concepts of ‘global cyberspace’, ‘the cyberspace of another country’ and ‘cyber hazard’.

The definitions presented below could be taken into consideration[13]:

‘global cyberspace’ or ‘cyberspace’ – a system of exchange and processing of information (data) functioning in accordance with formal rules, legal regulations in use in the territories of particular countries, operating thanks to the connection of technical resources located on the territory of every single country.

‘cyberspace of the Republic of Poland’ – a system of exchange and processing of information (data) functioning in accordance with formal rules, legal regulations in use within the territory of Poland, operating thanks to the connection of technical resources local to the territory of Poland.

It should be also noticed that the document ‘Polish Cyber Defence Policy’ is very different from the standards determined in the norm PN-ISO/TEC 2700 as far as the management of information security is concerned – the goals of the application of protection measures as well as the issues which should be regulated by the ‘Policy of Security’ and which should be addressed by the policy i.e. ‘it should safeguard the utility, adequacy and effectiveness’[14].

The examples of hazards

Cyberspace, because of its unique qualities, is especially susceptible to cyber espionage acts, which are no longer reserved to secret services. Today, the most important actors are rival companies, research institutes, universities, as well as individual hackers employed to perform a specific task.

In order to depict the hazards connected with cyberspace, it is worth presenting **facts of the most vivid cyber attacks which took place in the last decade**. None of them was qualified as an act of war, nor resulted in an official conflict involving the forces of the whole technologically advanced country. Nonetheless, the examples presented below can present an imagined image of the future battle field or confrontation.

‘Imagine the lights in this room suddenly go out, and we lose all power. We try to use our cell phones, but the lines of communication are dead. We try to access the Internet with our battery-powered laptops, but the Internet, too, is down. After a while, we venture out into the streets to investigate if this power outage is affecting more than just our building, and the power is indeed out as far as the eye can see. A passer-by tells us the banks are closed and the ATMs aren’t working. The streets are jammed because the traffic lights are out, and people are trying to

[13] cf BIODO Uwagi do Polityki Ochrony Cyberprzestrzeni RP. pdf in: http://mac.bip.gov.pl/fobjects/details/3564/biodo-uwagi-do-polityki-ochrony-cyberprzestrzeni-rp-pdf.html, [23.02.2013].

[14] Vide: Norm ISO/TEC 27001:2007, Technika informatyczna, Technika bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa 2007, p. 14.

leave their workplaces en masse. Day turns to night, but the power hasn't returned. Radio and TV stations aren't broadcasting. Telephones and the Internet still aren't working, so there's no way to check in with loved ones. After a long, restless night, morning comes, but we still don't have power or communication. People are beginning to panic, and local law enforcement can't restore order. As another day turns to night, looting starts, and the traffic jams get worse. Word begins to spread that the US has been attacked—not by a conventional weapon, but by a cyber weapon. As a result, our national power grid, telecommunications, and financial systems have been disrupted—worse yet, they won't be back in a few hours or days, but in months. The airports and train stations have closed. Food production has ceased. The water supply is rapidly deteriorating. Banks are closed so people's life savings are out of reach and worthless. The only things of value now are gasoline, food and water, and firewood traded on the black market. We've gone from being a superpower to a third-world nation practically overnight'[15]. This is not a scenario of a horror or science-fiction film, but a quotation from the testimony of Sami Saydjari, the chief of the organization Professionals for Cyber Defense, before the House Committee of Homeland Security, which took place in April 2007. Saydjari made the speech the day before events which turned the world's attention to the risks stemming from cyberspace. From 27 April to 11 May, 2007 Estonia was a victim of cyber attacks.

The excuse for the attack was the Estonian decision to move a monument commemorating the soldiers of The Red Army (the so called Bronze Soldier), this change resulted in riots. The Estonian ICT network faced a critical point. It is worth mentioning here that Estonia is very often called 'E-stonia' due to its state-of-the-art IT level. Over 90% of bank transactions are carried out on-line, it is possible to send tax declarations through the Internet. Every citizen is in the possession of Digital ID, which enables even voting via the Internet. The Estonian government implemented a system called 'evalitsus' (e-country), by which the process of informatization is supported. The cabinet itself communicates through computers to much an extend, and all government documents are available on-line. It significantly reduces the time and increases the efficiency[16].

All the factors contributed to the cyber attacks on the Estonian ICT infrastructure. At a high point, i.e. on 9 May, celebrated in Russia as Victory Day, the activity on Estonian web pages increased twentyfold. The biggest 10 attacks amounted to 90 Mb/s and lasted continuously for over 10 hours. The pages of the government, chancellery of the president as well as of the leading newspapers were all down. Moreover, banking systems collapsed, and last but not least the network of the Estonian police went down. The Estonians were cut off from Internet

[15] 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, p. 1 in: http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf, [25.04.2007].

[16] Vide: E-Eesti/E-Estonia, http://webstatic.vm.ee/static/failid/286/E-Estonia_uus.pdf, [12.01.2011].

information, as well as more seriously, they had no access to banks and money[17]. The functioning of the state administration, which was wired to much an extend, was suddenly questioned. According to the Estonian Minister of Defence: Jaak Aaviksoo, 'This was the first time that a botnet threatened the national security of an entire nation[18]'.

The Estonian governing bodies also thought about using Article 5 of the Washington Treaty which referred to mutual help of NATO member countries when one of them was the goal of an attack. The Estonian Prime Minister Andrus Ansip, when asked for the reasons of the attack, said that: the computers used for the attack had the IP addresses of Putin's administration. The action against Estonia was well synchronized – at the same time there were attacks on the Estonian Embassy in Moscow and the representatives of air lines. Whereas the official Russian delegation visiting Tallinn said that the Estonian government should hand in its resignation.

During the cyber attack aimed at Estonia, the aggressors used a brutal but very effective form of attack called DDoS (Distributed Denial of Service). By this method, particular servers are flooded by a giant amount of data, which leads to overloading and consequently they are blocked.

Soon after the attacks, the Estonian government put the blame on the Russian Federation, however, a 5-year investigation did not prove that the hackers were following the Kremlin's orders. The general attorney, Heili Sepp, said that in spite of the fact that a significant number of IP addresses connected with the attack were identified, most of them were found outside Estonia. Unfortunately, the letters requesting legal assistance addressed to the governments of the Russian Federation and Lithuania were rejected without any effect. Due to the lack of possibilities to continue the investigation, the office of the general attorney closed the proceedings at the end of July 2012[19].

The analysis conducted by specialists on information security proved[20] that some of the attacking computers were registered to the Russian president's administration, however, most attacks were done through infected computers in Egypt, Vietnam or Peru. The only argument which can be used against Russia is the fact that because of historical and prestige reasons Russia might have been interested in such an operation.

[17] Vide: Rosyjscy hackerzy podbijają Estonię, „Gazeta Wyborcza", 17.05.2007, http://gospodarka.gazeta.pl/technologie/1,81010,4140556.html [28.06.2008].

[18] 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, [26.04.2009].

[19] Vide http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie, [27.09.2012].

[20] After the attack, Tallinn created a group of volunteers who would protect the country during a cyber war. Now it is a group of 80 people. In everyday life these are IT experts, engineers, employees in banks, big corporations or ministers. Usually these are 20 or 30-year-old people. They meet every week in Tallinn and Tartu in: http://www.rp.pl/artykul/593688.html [12.02.2013]

The attack resulted in NATO's mobilization. In 2008 a centre for cyber defence was created with its headquarters in Tallinn. The centre was to carry out simulations, create special systems of protection, as well as to prepare projects aimed at the creation of a basis for cyber-security in NATO. Of course the goal was to safeguard the security of the IT systems of the institution itself, and not of the member countries. It turned out, however, that the centre does not function in the way it should. This is caused by accusations that the originator and the main director of the centre cooperated with Russian intelligence. This resulted in a situation which cannot be solved even today.

However, the Estonian example is not the only one in Europe. In 2008 there were two similar incidents. The first one happened in Lithuania. Soon after a ban on using and possessing symbols of the Soviet Union, hundreds of government pages were taken over and replaced by others. They usually showed Soviet symbols together with vulgar texts referring to the Lithuanian government. The attack was not as paralysing as the one in 2007, but it showed how easy it was for hackers to take down the government's IT systems.

The next victim of a cyber attack, in chronological order, was Georgia. It happened during, or in fact just before the entering of the territory of Abkhazia and South Ossetia by the Russian Army. The attack was of a mixed character, i.e. a combination of DDoS attacks and taking over some Internet websites. It is hard to resist the impression that it was an element of a normal war operation. The information paralysis which happened in Georgia facilitated regular warfare.

All the cases presented above have one common element – The Russian Federation. In spite of the lack of sufficient proof, all the three incidents were connected with situations where the interests of Moscow were put in jeopardy.

Another problem which bothered many countries was the Iranian nuclear programme. Instead of a traditional attack, the countries decided to make use of the possibilities given by **cyber attacks**. Namely, the Iranian nuclear programme[21] was struck by the following viruses: Stuxnet, Duqu and then Flamer

According to the Symantec company, Stuxnet was made expressly to disrupt the work of a programme responsible for centrifuges used for uranium enrichment in an Iranian nuclear plant[22]. The virus was able to cause a serious breakdown of the key devices.

[21] It was in two cities: Natanz as well as in Fordo.

[22] During a presentation on the conference Virus Bulletin 2010 in Vancouver an expert on security, from Symantec, – Liam O'Murchu, using an electronic air pomp connected to a SIEMENS S7-300 PLC controller as well as software SIMATIC Step 7 – programmed the time of the pomp's work so that it operated for 3 seconds from the time it was turned on. Then, he placed a Stuxnet virus into the system infecting the PLC controller and changing the earlier parameters of the time of work extended it to 140 seconds, which caused that the balloon to burst – if the PLC controller was plugged in a pipeline, a nuclear power plant, or was on an international airport – it is easy to imagine the consequences.

The hostile software paralysed both computers as well as automated systems of monitoring in both research institutes. Except that, the virus chooses at random several devices on which at night it plays the song „Thunderstruck" of the legendary group AC/DC at the top volume[23].

The first reference to the Stuxnet virus, was noticed in 2010 as the 1.001 version**.** However, the data gathered up to that moment indicated that its oldest compilations come from the year 2005.

Symantec published a report in which it gives evidence that the work on an earlier version of a Stuxnet worm number 0.5[24] started in 2005 and it was said to operate in the network in the years 2007 and 2009. Stuxnet 0.5 was not as aggressive as the later versions, however, it was still able to make serious damage. It is true that this version also aimed at the Iranian nuclear installations, however it followed a different strategy with the goal to turn off valves in uranium enrichment plants in Natanz. *Whether the mission of Stuxnet 0.5 was successful or not is unclear, but its later versions were made with a different framework of development, they were more aggressive and they changed the strategy of attack, which allowed them to modify uranium enrichment's centrifuge speed as evidenced by* information provided in Symantec's report [25]. What is more, Stuxnet 0.5, unlike its later version, was based on the Flamer platform and did not **exploit any Microsoft vulnerabilities**. However, similarly to them, it looked for a particular model of Siemens PLC.

The way it operates suggests that it was probably created to spy on, re-programme industrial installations, and as a result paralyse central units of big industrial plants. The fear of Stuxnet is bigger if we realize what is the scale of the problem – a special virtual code can be the reason of real modification in factories, companies or even nuclear power plants. This is another proof of how small the difference between the virtual and the real world is nowadays.

From a technical point of view, Stuxnet is the name of a Trojan being only one element of the whole hazard. The infection triggered by Stuxnet is done in two phases:

In the first phase, Stuxnet spreads via computers working under Windows systems, but its presence is hidden from the security software due to the use of two known and two unknown vulnerabilities. Stuxnet is spread through removable drives (in systems with auto start function) – computer systems steering industrial devices – and in particular such systems as nuclear installations which because of security reasons do not have access to the Internet; it spreads in LAN networks via a Windows Print Spooler; it spreads through System Message Block; it makes

[23] See more: http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/07/iran-zaata kowany- przez-ac-dc#ixzz2N9gwDslh, [24.08.2012].

[24] Vide: Stuxnet 0.5: How It Evolved w: http://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved, [27.02.2012].

[25] Ibidem.

copies and starts its code on computers via net share; it also makes copies and starts its code on computers working under the control of data base server WinCC.

In the second phase Stuxnet is looking for one thing i.e. a Windows work station, which is usually a separate post used to monitor and control ICS (*Industrial Control Systems*), and in particular the one which uses Siemens PLC (*Programmable Logic Controller*).

It is most probable that the creators of Stuxnet were aware of the fact that this type of work stations are accessible by different types of viruses or malware only through USB flash discs. Thus, when Stuxnet reaches its target (particular Siemens PLC device), it remains undetected and starts to modify the Industrial Control System, sabotaging the whole system like a rootkit.

Moreover, Stuxnet used valid digitally signed certificates – the aforementioned infected drives were signed by two reliable companies – Realtek and JMicron. The certificates were probably stolen (both companies are located in Hsinchu Science Park in Taiwan).

At the moment when the first Stuxnet's attacks were spotted, anti-virus companies were not prepared for this type of threat and the virus was marked as '*0-day threat*'. The present situation is a little bit better, most producers of anti-virus software supplemented their database of signatures with a proper tool detecting the worm.

It turns out that Stuxnet was not a one-time incident. Except Stuxnet and Duqu there is also R2D2. It all proves that we have definitely entered the era of ***spy and government Trojan Horses****. Software has become a weapon. Stuxnet and Duqu were followed by Flame, which is one of the most complex and sophisticated pieces of malicious software ever seen – as Symantec presents*[26]. Flame is able to attack and steal data, what is more, it can even record voice and send it back to a hacker. However, there is one radical difference, namely Stuxnet is able to deal with one target at a time, while Flame can strike simultaneously over 600 goals.

Although no government officially admitted to creating the virus, and none was caught red handed, the experts are unanimous that the cyber action was carried out on US and Israeli initiative[27].

Finally, it is worth mentioning that the experts on security issues are astonished that hackers who created those viruses were able to hide behind the Microsoft programme. Moreover, they warn that this method might have been used to spread other viruses, which are still there to be discovered.

Recently, Internet espionage is at its peak. At least, we can come to such conclusion when we analyse in more detail the recently revealed operation called

[26] K. Majdan, Wykryto nowe zagrożenie in http://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy, [17.02.2012]

[27] In 2012 the New York Times informed that the Stuxnet virus was most probably created by the governments of two countries i.e. the USA and Israel, vide: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against iran.html?_r=4&pagewanted=all&, [20.08.2012].

'Red October'. Kaspersky Lab boasts of this cyber-espionage campaign targeting **diplomatic and government institutions worldwide**[28]**.**

According to the biggest producer of anti-virus computer software – Kaspersky – in the network there is a new hazard. In short it is called *Rocra*, which is short for **Red October**, (the name stems from the fact that research on the issue started in October 2012). It is very probable that it has operated for 5 years now and it steals information from computers, smartphones and external storage devices in the EMEA region (Eastern and Central Europe) and Central Asia. 'Red October' has a module structure and it changes each time to adjust itself to the needs of the attack on a particular victim. Each of over a thousand modules has its own function: steals codes, contact lists stored on mobile devices, copies e-mails, registers operations performed on the keyboard, etc. According to Kaspersky Lab, the virus comes from Russia, and the huge infrastructure, comprising dozens of servers responsible for its spreading, shows that it might be a governmental operation, similarly to the Flame virus. 'Red October' displays many similarities to the Stuxnet virus discovered in 2011, which managed to infect 100 thousand computers in 155 countries within 11 months.

Interestingly, according to the data provided by Kaspersky Lab, **Red October** used the tactics of breaking into subsequent computers in stages – first it acquired data from one computer and used it to break into another and another one. And so on and so forth...

Kaspersky informed in a detailed report that it was a very wide-reaching action. It struck 69 countries all over the world. The victims included public administration (diplomatic and politics), research institutions, military facilities, and employees of power stations. The report was published on 14 January, and Kaspersky has been investigating the case since last October.

Kaspersky notices that in total there have been hundreds of computers infected worldwide, however mainly the victims come from the former Soviet Bloc as well as from Asia. The biggest number of infected computers was found in Russia (35), Kazakhstan (21), and Azerbaijan (15). The list also includes such countries as Belgium (15 infected computers), the USA (6), Vietnam (6) or Switzerland (5).

Taking into consideration the information presented above, it can be concluded that the action was aimed at people in the possession of important information, usually the core information for national security. The computers which were infected belonged to politicians, diplomacy representatives, researchers, sales representatives, people dealing with nuclear energy, aviation and energy sectors.

It is worth noticing that Poland is one of the few European countries where the hazard was not registered nor proved. Kaspersky notices that the espionage

[28] Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide vide: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide, [17.02.2013].

network is very advanced. However, the way in which the chosen computers are taken control of is surprisingly easy. It is all started with a fake e-mail with an attachment. For instance, information on a diplomatic car for sale was sent. The attachment included details of the offer, but most importantly a malicious code using a vulnerability in MS Word or MS Excel. When the victim opened the attachment, a Trojan was installed on the computer. But this is not everything – the virus was later able to download and install further modules of the malware.

The latter one enabled hackers to have access to most information. They could take over files from a computer or even USB drives or telephones (iPhone, Nokia, Windows Mobile). They also had access to e-mails from Outlook and made use of the keyboard strikes. To make a long story short – the espionage was wide-reaching.

There is still no answer for one of the key questions – who did it? What do we know so far? According to Kaspersky, the servers were located in Russia and Germany. Exploit, the programme using the MS Word and MS Excel vulnerabilities, looked like a Chinese programme, the programme installed on the victim's computer seemed to be produced in Russia. Kaspersky set a trap in a few domains used by the malware and it turned out that in the period of time between 2 November 2012 and 10 January 2013 there were 55 thousand connections. Most of them were registered in Switzerland, Kazakhstan, Greece and Belarus.

So far there is no proof that the attacks were sponsored by a particular country. There is also no information about the fate of the stolen data. It could have been sold on the black market, or might have been used by the hackers themselves.

Thus, who was it? The government of any country? Taking into consideration the scale of the operation it is a very probable version – there are many countries which carry out a far-reaching espionage actions, thus, it is not a surprise that the operations are now located in the Internet. The origin of the software might be the argument against. However this may be illusionary, since we can assume that they decided to use the best available software.

On the other hand, countries are not very eager to use foreign software – it is safer to make your own one. Thus, it might be rather a big operation of an international terrorist organization.

The creation of units for cyberspace warfare

The above presented information leads to a conclusion that the common computerization and dynamic development of the Internet observed at the beginning of the 21st century facilitates the process of using cyberspace for operations which put the security of many countries in jeopardy. According to independent experts, the group of countries which were first to use wide-scale, planned and organized forms of cyber attacks to realize their own political,

intelligence and military goals includes: the USA, Russia and China. Nonetheless, the Americans admit that they are far behind Russia and China on this field[29].

As said by the Pentagon, i.e. the US Department of Defense, the above prerequisites oblige the Department of Defense and the US government to strengthen the national defence system against cyber attacks[30]. This is why cyber forces are called into being.

The analysis of subject literature reveals that the *United States Cyber Command* (*USCYBERCOM*) is a special part of the US Army prepared to run operations on the field of state-of-the-art IT technology. *USCYBERCOM* started its operation on **21 May 2010** and from its first beginnings it recruits mainly specialists on the security of ICT systems, however it is not a secret that that the US government also seeks out people with unique hacking abilities[31].

USCYBERCOM is responsible for the centralization of secret operations run in cyberspace as well as for the organization of the available IT resources and the protection of the US military networks. Presently, the Pentagon wants to expand the personnel from 900 to 4900 people. Thus, there is a plan to create 3 separate cyber forces, namely – 1) Cyber National Mission Forces, 2) Cyber Protection Forces and 3) Cyber Combat Mission Forces[32].

The first forces will be responsible for the protection of the 'critical infrastructure of the country', the second one – for the protection of the network of the Department of Defense, and the third one will carry out planned cyber attacks. According to the American military experts, nowadays and in the future, the operations of the conventional military forces are and will be less significant than cyber operations[33].

The conclusion comes from the observation of the changes and events in cyberspace. Recent events have forced the Americans to expand their cyber forces. In the present cyberspace there are serious, well organized attacks. There are also

[29] USA w obronie przeciw cyberwojnie buduje cyberarmię, in: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html, [08.01.2013].

[30] USA w obronie przeciw cyberwojnie buduje cyberarmię, zobacz in: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html, [08.01.2013].

[31] Pentagon buduje cyberarmię in: http://tech.wp.pl/kat,130034,title,Pentagon-buduje-cyberarmie,wid,15291699,wiadomosc.html?ticaid=110374, [08.01.2013].

[32] Vide: http://kopalniawiedzy.pl/Cyber-Command-cybernetyczne-sily-zbrojne-NSA-Keith-Alexander,17428, [17.01.2013].

[33] According to the latest information, the Pentagon is creating several cyber teams, which are tasked with offensive operations against cyber attacks threatening the US critical infrastructure. This information was given on 12 March 2013 by general Keith Alexander, the commander of the US Cyber Command, to the senate committee on Armed Services. He stressed that the threat of attacks on the US electricity network and other vital systems is real and it requires more aggressive steps of the government and the private sector, aimed at better protection against such attacks. He also said that such teams will operate outside the USA but he did not reveal where exactly. According to the general it is necessary to define the act of cyber warfare, in: http://niewiarygodne.pl/kat,1031991,title,Pentagon-tworzy-ekipy-do-zwalczania-zagrozen-w-cyberprzestrzeni,wid,15408475,wiadomosc.html?smgajticaid=6103b8 [15.02.2013].

well grounded fears that the USA is being attacked by foreign countries, or well-financed criminal groups.

According to Alan Paller, the director for research at the SANS Institute, China and Russia in at the possession of much more developed and better organized cyber forces than the USA. The USA is therefore reduced to trying to catch up with them. Paller thinks that the real challenge is to find the proper number of experts. The problem in finding 4000 experts is that every important branch of the economy – banks, energy companies, telecommunication firms, the defence industry, hospitals, the government – are all looking for the same people. The demand for high-class experts is huge, however there are not enough of them on the job market[34].

Taking into consideration the above facts, it is obvious that Pentagon takes cyber hazards very seriously. The US Department of Defense decided to prepare an Internet simulation to practice different scenarios of cyber warfare. Cyber Range is to be ready next year, and it will be used to test defensive and offensive operations[35].

The plan of the project was prepared by Lockheed Martin, a company which received a grant of 30,8 million dollars from Defense Advanced Research Projects Agency (DARPA). A rival project was created by the John Hopkins University Applied Physics Laboratory, which got for this purpose 24,7 million dollars.

The role of Cyber Range is to **imitate governmental, military and commercial networks as well as human reactions and weaknesses** during operations on different defence levels as well as during the preparation of combat plans. DARPA wants the simulator to carry out simultaneously many tests and scenarios of offensive and defensive operations, which might be necessary in the future.

Up to now, Lockhead Martin and John Hopkins University should have prepared prototypes of Cyber Range, which will be presented for assessment. DARPA will choose only one of the projects, which will be realized and implemented.

Obviously **the US government has a more and more serious attitude to cyber hazards** and intends to prepare well for possible attacks from the Internet. It was much earlier that the Pentagon announced that cyber attacks will be treated as seriously as traditional attacks targeted at national security.

Another country in the possession of Cyber forces is China. The subject literature emphasizes the fact that China has been suspected for a long time of carrying out cyber attacks on targets located in other countries. Probably many any espionage Trojans come come from China, however there is no firm evidence for

[34] M. Błoński, USA budują cyberarmię in: http://www.wykop.pl/ramka/1395241/usa-buduja-cyberarmie.

[35] Pentagon tworzy symulator cyberwojny in: http://www.pcworld.pl/news/372262/Pentagon.tworzy.symulator.cyberwojny.html, [08.01.2013].

that. Still, on 16 July 2011, the national TV channel CCTV 7 (Military and Agriculture) broadcasted a documentary entitled 'Military technology: the Internet storm is coming', which presented an attack initiated by a government system on goals located in the USA. A proof for the existence of such software is a front page piece of news – said Mikko Hypponen, the director of the research department at F-Secure, a Finnish producer of anti-virus software[36].

Moreover, in an interview for the Xinhua agency, Geng Yansheng, the representative of The Chinese Ministry of Defence, admitted that China has a unit of 'Internet Forces'. Geng Yansheng said that the unit is responsible for the protection of Chinese cyberspace against external attacks, it has existed since 2009 and it consists of about 30 people. However, the publicized reports indicate that the Chinese Internet offensive unit has existed for at least five years, with much more than 30 people.

A top secret unit of the Chinese Army was also revealed in a report made by Mandiant, a US company safeguarding security on the Internet – and it is addressed as the most dangerous group of cyber terrorists in the world. These are hundreds or thousands of super-efficient computer experts with a perfect command of English. They steal strategies and business plans, e-mails, and contact lists, as well as confidential data of companies and institutions. The author of the report is absolutely sure that they operate in China, and the Chinese government is completely aware of the fact[37].

The authors of the report traced Chinese hackers for six years, in classified US documents they are called 'Comment Group'. The authors are convinced that all traces lead to Shanghai, to the command of the Chinese Army unit 61398. The headquarters are located in a white, modest, 12-storey office building, surrounded by restaurants and residential buildings in a poor Pudong area in the suburbs of Shanghai.

An incidental observer would never notice that in this exact place there are the command headquarters of the mysterious unit 61398, which is presently the favourite media target. Its formal name is *the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department*. Officially, the bureau does not exist in the description of military structures.

A huge pile of evidence indicates that 90 percent of attacks come from Unit 61398, the group was given several names in classified US correspondence and now it is called 'Comment Crew' or 'Shanghai Group'.

Analysing the Mandiant's special report, it is necessary to quote the most important assumptions and observations: *Unit 61398 is staffed by hundreds and perhaps thousands of people trained in computer security and computer network operations and also proficient in the English language. The unit has stolen*

[36] Vide: http://military.cntv.cn/program/jskj/20110717/100139.shtml, [08.01.2013].

[37] Vide: Raport Mandiat APT1 Exposing One of China's Cyber Espionage Units in: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, [22.02.2013].

hundreds of terabytes of data from at least 141 organizations simultaneously, in 20 major industries, out of which 87% are in English speaking countries. The special unit stole information including military plans, business plans, and e-mails, as well as contact lists[38].

Of course China rejects the accusation, claiming that 'hacker's attacks are supranational and it is almost impossible to trace their source'. Thus, it turns out that we are witnesses to another struggle between a superpower in the twilight, and a new emperor. In this battle, however, the USA does not want to give away the position of IT leader and wants to influence the public opinion in order to create a negative image of China. It should be kept in mind that the US sword is double edged, and the USA also has systems such as Echelon or Carnivole which are able to invigilate people.

Another country is Germany, which released official information that it has created two new governmental organizations. Their work will be directly connected with Internet security and cyber warfare. The first organization is called Nationales Cyber-Abwehrzentrum (NCAZ), and the second one is called Nationaler Cyber-Sicherheitsrat. Their task is to protect German industrial and military infrastructure against attacks from hackers and defend it in the case of an outbreak of cyber warfare[39].

The Nationaler Cyber-Sicherheitsrat started its operation on 1 April 2011. It was headed by Cornelia Rogall-Grothe, Secretary of State in the Ministry of Internal Affairs. The members include prominent people from the ministry of internal affairs, the ministry of defence, the ministry of justice and the ministry of finance. Whereas the personnel of NCAZ, at least at the initial state, includes the employees of the Federal Office for Information Security or the Federal Office for the Protection of the Constitution.

The document describing the two organizations gives three reasons why they were called into being. The first one is the increasing threat caused by specialized malware and the necessity to trace and respond to cyber attacks. The second reason is the increasing number of industry's 'weak points', beginning the moment it uses more and more often state-of-the-art technology. The third one is the hazard connected with worms such as Stuxnet. Germany calls for the European Union and NATO, as well as its own Armed Forces, to tighten cooperation in order to protect the member states from cyber attacks[40].

A more complicated situation connected with cyber units is observed in Russia. In spite of the fact that in the media and reports of companies dealing with security

[38] Ibidem p. 4.

[39] Minister Obrony Narodowej otwiera Centrum Cyberobrony Narodowej in: http://www.heise.de/newsticker/meldung/Innenminister-eroeffnet-nationales-Cyber-Abwehrzentrum-1261659.html, [09.10.2012].

[40] Strategia Cyberobrony dla Niemiec in: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf, [08.02.2013].

in cyberspace there are many accusations aimed at Russia, officially it is only beginning to create such units.

In March 2012 the Deputy of Russian Defence, Dmitrij Rogozin announced the formation of Cyber Command, he said that the whole document had been already prepared and he expressed hope that Cyber Command will be created soon.

Information available on the website of 'Izwiestija' as of 12 February 2013 proves that if the plan of creating the Cyber Command is accepted by the Russian political leaders, the Command will start its operation even before 2014[41]. We can also read there that according to a prominent source in the Ministry of Defence, the future Cyber Command will be very similar to the USCYBERCOM. The Russian Cyber Command will work for the Army, police and all civil authorities and its main task will be the protection of national interests[42].

It is worth keeping in mind that in Russia there are already several bodies monitoring cyber hazards. The Ministry of Internal Affairs has 'K' office, while the Federal Security Service – the Centre of Information Security, and Federal Agency of Government Communications and Information (FAPSI) is responsible for IT warfare operations at a strategic level.

The subject literature also gives information concerning other countries which possess units prepared for cyber warfare, including e.g. Great Britain, Israel, Iran, South Korea.

Poland has also created a new organizational structure called Centrum Bezpieczeństwa Cybernetycznego (Cyber Security Centre)[43]. It is located in Białobrzegi, where there is the 9th Signal Battalion. It has operated since the summer of 2010. And this is everything that is officially known. The Ministry of National Defence does not want to reveal any details. It is known that military computer experts protect the offices of the Ministry of National Defence and command headquarters which are the target of regular hacker attacks. In 2011 the Ministry of Defence planned to spend one milliard zloty for information technology. The plan included inter alia, the first digital battalion in the Army. Soldiers and their commanders would be able to use technical advancements such as displays providing information useful on the battle field[44].

[41] Vide: W Rosji cyberwojska in: http://bashgazet.ru/rus/news/nrf/2477-v-rossii-poyavyatsya-kibervoyska.html, [08.01.2013].

[42] Vide: Rosyjscy wojskowi przygotowują się do cyberwojen in: http://www.radiovesti.ru/articles/2013-02-12/fm/81961, [08.01.2013].

[43] Wizyta Szefa BBN w Centrum Bezpieczeństwa Cybernetycznego in: http://www.bbn.gov.pl/portal/pl/2/3305/Wizyta_Szefa_BBN_w_Centrum_Bezpieczenstwa_Cybernetycznego.html, [08.02.2013].

[44] Polska armia broni się przed atakami hakerów in: http://wiadomosci.wp.pl/kat,8311,title,Polska-armia-broni-sie-przed-atakami-hakerow,wid,12902309,wiadomosc.html, [08.02.2013].

Conclusions

Cyberspace has become a new area of struggle, which results in numerous changes both in the pragmatic as well as the legal-organizational dimension of security systems functioning across the whole world, each country and locally.

The construction of the legal system, as the countries' response to the chances and challenges stemming from cyberspace, is an extremely complex task. It is not only the outcome of the pace of technological advancement but also it stems from the specific character of the environment and its 'interactive' nature.

In order to shape the legal norms on the national level, the regulations concerning international cooperation, as well as strategies and security policy, it is necessary to take into account two basic challenges. The necessity of a fast reaction, on the one hand, and reaction to small, mobile groups, on the other hand, constitute a new quality in the area of creating new legal regulations concerning the security of a country[45].

One cannot forget, that in spite of the fact that cyber hazards are a totally different category of legislative-organizational challenges, the problems which they cause are similar to those generated by other asymmetrical threats, like e.g. terrorism. Their common characteristic is that the country's structures are forced to evolve in the direction of less hierarchical but more flexible solutions. Network ability, both in a social as well as technological dimension, along with all the consequences, seems to be one of the most important concepts of the new security paradigm at the national and international level.

Cyber warfare is a fact. During the last year, the number of politically motivated attacks through the Internet has exceeded the levels of acceptability. In just one country, the USA, the following institutions were the target of attacks: The White House, The Department of Homeland Security, Secret Service, The US Department of Defense. Countries get engaged in the Cyber Arms Race and develop their abilities to carry out cyber warfare in which governmental networks and critical infrastructure will be the main targets. However, cyber warfare is not only a war between computers. It can cause real damage in the real world and can result in the death of many people[46].

Cyber weapons take critical infrastructure as their target. The owners of cyber weapons not only prepare cyber defence but also cyber attacks aimed at among other things energy networks, transportation routes, telecommunication networks, financial systems, and water supply systems; this is due to the fact that they can be quickly immobilized with a relatively small effort. In most developed countries the critical infrastructure is connected to the Internet and it is not sufficiently protected

[45] cf Krzysztof Liedel, Paulina Piasecka, Wojna cybernetyczna – wyzwanie XXI wieku, Quarterly „Bezpieczeństwo narodowe", No 17/2011, p. 25 and further.

[46] Czy trzecia wojna rozpocznie się w Internecie in: http://forum.gazeta.pl/forum/w,101385, 130897447,130920749,Czy_trzecia_wojna_swiatowa_rozegra_sie_w_interneci.html, [14.01.2013].

– this is why those installations are especially susceptible to hazards. A lack of proper protection as well as a lack of preparation are the reason for much more damage being caused by the present attacks than in the case of operations carried out in the past.

There are so many actors involved in cyber warfare acting in so many ways, that the rules of engagement are not clearly defined. It is also ambiguous what duties should be assigned to companies and institutions in connection with the defence and the education of the society in order to prevent cyber attacks. Without a proper definition there are no explicit criteria to take decisions in a situation when the proper response to cyber attack is a political reaction, or even the threat of a military operation.

The private sector is most endangered. In many developed countries the critical infrastructure is in private hands, due to that it is a perfect target of cyber attacks. However, in the scope of the prevention cyber attacks, the private sector depends on the steps taken by the government. In the face of virtual fire everyone is endangered: governmental institutions and companies, as well as every individual citizen. Without the insight into the government strategy on cyber defence, the private sector is not able to take effective preventive measures. Due to that the experts call for an explicit public debate on the problem of cyber warfare.

Bibliography

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.

BIODO Uwagi do Polityki Ochrony Cyberprzestrzeni RP.pdf in: http://mac.bip.gov.pl/fobjects/details/3564/biodo-uwagi-do-polityki-ochrony-cyberprzestrzeni-rp-pdf.html.

Czy trzecia wojna rozpocznie się w Internecie in: http://forum.gazeta.pl/forum/w,101385,130897447,130920749,Czy_trzecia_wojna_swiatowa_rozegra_sie_w_interneci.html.

E-Eesti/E-Estonia, http://webstatic.vm.ee/static/failid/286/E-Estonia_uus.pdf.

Gregory J. Rattray „Wojna strategiczna w cyberprzestrzeni" (the original title: Strategic Warfare in Cyberspace), Warszawa 2004.

http://kopalniawiedzy.pl/Cyber-Command-cybernetyczne-sily-zbrojne-NSA-Keith-Alexander,17428.

http://military.cntv.cn/program/jskj/20110717/100139.shtml.

http://niewiarygodne.pl/kat,1031991,title,Pentagon-tworzy-ekipy-do-zwalczania-zagrozen-w-cyberprzestrzeni,wid,15408475,wiadomosc.html?smgajticaid=6103b8.

http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/07/iran-zaatakowany-przez-ac-dc#ixzz2N9gwDslh.

http://www.heise.de/newsticker/meldung/Innenminister-eroeffnet-nationales-Cyber-Abwehrzentrum-1261659.html.

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=4&pagewanted=all&.

http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie.

http://www.rp.pl/artykul/593688.html.

i-słownik: http://www.i-slownik.pl/323,cyberprzestrzen/.

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.

K. Majdan, Wykryto nowe zagrożenie w http://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy.

Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide in: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

Krzysztof Liedel i Paulina Piasecka, Wojna cybernetyczna – wyzwanie XXI wieku, Quarterly „Bezpieczeństwo narodowe", No 17/2011.

M. Błoński, USA budują cyberarmię w: http://www.wykop.pl/ramka/1395241/usa-buduja-cyberarmie.

Norma ISO/TEC 27001:2007, Technika informatyczna, Technika bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa 2007.

Pentagon buduje cyberarmię w: http://tech.wp.pl/kat,130034,title,Pentagon-buduje-cyberarmie,wid,15291699,wiadomosc.html?ticaid=110374.

Pentagon tworzy symulator cyberwojny in: http://www.pcworld.pl/news/372262/Pentagon.tworzy.symulator.cyberwojny.html.

Polska armia broni się przed atakami hakerów in: http://wiadomosci.wp.pl/kat,8311,title,Polska-armia-broni-sie-przed-atakami-hakerow,wid,12902309,wiadomosc.html.

Raport Mandiat APT1 Exposing One of China's Cyber Espionage Units in: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

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

Rosyjscy wojskowi przygotowują się do cyberwojen in: http://www.radiovesti.ru/articles/2013-02-12/fm/81961.

Strategia Cyberobrony dla Niemiec in: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf.

Stuxnet 0.5: How It Evolved w: http://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved.

US Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf.

USA w obronie przeciw cyberwojnie buduje cyberarmię, in: http://www.wiadomosci24.pl/artykul/usa_w_obronie_przeciw_cyberwojnie_buduje_cyberarmie_259117.html.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP.

W Rosji cyberwojska in: http://bashgazet.ru/rus/news/nrf/2477-v-rossii-poyavyatsya-kibervoyska.html.

Wizyta Szefa BBN w Centrum Bezpieczeństwa Cybernetycznego in: http://www.bbn.gov.pl/portal/pl/2/3305/Wizyta_Szefa_BBN_w_Centrum_Bezpieczenstwa_Cybernetycznego.html.