Płk (s) Zbigniew Cezary MICHALSKI

WOJNY CYBERNETYCZNE

Wstęp

Globalna rewolucja informacyjna, tocząca się na świecie stanowi dla ludzkości olbrzymi skok cywilizacyjny. Bowiem prowadzi społeczeństwa od ery przemysłowej do informacyjnej. Oznacza to w praktyce, oparcie na komputerach i technikach informatycznych niemal wszystkich dziedzin działalności państwa, a także sfery prywatnej.

W przypadku państwa są to w szczególności dziedziny newralgiczne obejmujące systemy, które zapewniają bezpieczeństwo wewnętrzne, obronę militarną, zarządzanie finansami, komunikację, transport, połączenia telemedialne, ochronę życia i zdrowia, osiągnięcia nauki i techniki, przemysłu zbrojeniowego i inne.

Zasadniczą rolę wiążącą te dziedziny w formie komunikacji i technik informatycznych odgrywa dziś Internet i jego Sieć globalna. Warto przy tym zauważyć zadziwiającą karierę Internetu i sieci. Zwłaszcza, że Internet wymyślony najpierw jako sieć połączonych komputerów wojskowych służących do celów militarnych, miał przetrwać wojnę jądrową, a obecnie przekształcił się w światowy system komunikacji informacyjnej. Czynnikiem pobudzającym te przemiany stało się zakończenie zimnej wojny, umożliwiając gwałtowny rozwój Internetu.

Obecny stan tego systemu pozwala na swobodne przemieszczanie w formie cyfrowej potencjału myśli ludzkiej i dorobku cywilizacyjnego między wszystkimi podmiotami podłączonymi do światowej sieci internetowej. Dzięki temu, jednym kliknięciem komputera można przenieść cenne informacje z jednego krańca naszego globu na drugi. Co więcej zasługą opracowania naukowej teorii informacji[1], możliwa jest szybka i bezbłędna łączność, prowadząca do

[1] Teoria informacji – została zapoczątkowana w latach 40. XX wieku przez Claude'a Shannona amerykańskiego inżyniera, który opracował naukę o łączności. Nauka ta, rozwijana przez wielu uczonych stanowi podstawę dla wielu nowoczesnych technologii od płyt DVD, przez łączność satelitarną o kody paskowe, nauki o kosmosie, dekodowanie genomów organizmów żywych (np. DNA) i innych. Źródło: Robert Matthews, 25 wielkich idei, Teoria informacji Centrum Kształcenia Akademickiego, Gliwice 2008.

stosowania takich technik jak kompresja danych i korekcja błędów a także możliwość magazynowania i wydajnego przekazywania informacji oraz wykorzystywania jej do różnych celów praktycznych.

Stąd dzisiejsza Sieć internetowa, wraz z dołączonymi do niej sieciami różnych podmiotów branżowych jest pełna tajemnic z różnych ważnych dziedzin (bankowych, obronnych, technologicznych, naukowych i osobistych).

Wbrew słusznym założeniom, powszechna dostępność Internetu i jego Sieci, uznawana do niedawna jako zaleta, stała się teraz największą jego wadą. Okazało się, że istotne informacje przekazywane tą drogą, czy korzystanie z zalet Internetu i jego Sieci w trakcie zarządzania newralgicznymi dziedzinami, są łakomym kąskiem dla cyberszpiegów i złodziei. Wykradają oni pieniądze z bankowych kont oraz tajemnice militarne i produkcyjne. Nie mniejsze szkody powoduje zakłócanie lub niszczenie sieci służących do działalności podmiotów czynione w przy pomocy złośliwych wirusów komputerowych.

Taką przestępczą działalność w sieci prowadzą obecnie nie tylko grupy wyspecjalizowanych hakerów międzynarodowych, ale też wielkie korporacje, czy nawet duże państwa. Szczególnie czynią tak kraje, które dążą do uzyskania przewagi militarnej, konkurencyjnej czy dla korzystania z cudzego postępu technologicznego.

Dlatego czołowe państwa świata pod pozorem zwalczania cyberterroryzmu powołał u siebie organy, dowództwa, sztaby i jednostki wojskowe do przeciwdziałania cyberszpiegostwu i przygotowywania wojny cybernetycznej. Z tych powodów coraz częściej spotyka się poglądy, że każdy współczesny konflikt powinien rozpocząć się od cyberataku lub cyberwojny z przeciwnikiem. Powinna ona przede wszystkim zniszczyć zaplecze logistyczne (wojskowe i cywilne), odsłonięte systemy dowodzenia i łączności oparte na technikach informatycznych.

Stąd niebezpieczeństwo rozpętania wojny cybernetycznej jest na wyciągnięcie ręki. Zresztą wielu naukowców i strategów głosi, że wojny cybernetyczne już trwają (przykład Estonii).

Początki i rozwój Internetu jego Sieci światowej

Powstanie Internetu wiązało się, podobnie jak wiele innych kluczowych odkryć i wynalazków z potrzebami militarnymi. Zwłaszcza, że Internet zrodził się w świecie wielce skłóconym, którego napięcia o mało nie przerodziły się w wojnę nuklearną, grożącą zagładą naszej cywilizacji. W tak zapalnej

atmosferze zimnej wojny, wyłoniła się w kierownictwie wojskowym Stanów Zjednoczonych, potrzeba zbudowania nowych mocno utajnionych technik komunikacyjnych dla armii. Miały one służyć do przepływu informacji między komputerami wojskowymi.

Inspiracją do takich poszukiwań była rywalizacja między super mocarstwami o dominację militarną w przygotowywanej wojnie nuklearnej. Dlatego w latach 60. XX wieku kierownictwo amerykańskiego Pentagonu zleciło grupie uczonych i inżynierów opracowanie systemu informacyjnej sieci komunikacyjnej, która przetrwa wojnę jądrową.

Zleceniobiorcą tego ważnego zadania była agencja DARPA (Defense Advanced Research Project Agency), będąca instytucją ministerstwa obrony USA. Agencja stanowi do dzisiaj badawcze zaplecze Pentagonu odpowiedzialne za rozwój nowych technologii wojskowych. Mimo wysokiego budżetu (około 3,2 mld dolarów) służącego do finansowania małych lecz wysoko sprawnych firm badawczych i uczelnianych zakładów rozwojowych, DARPA zatrudnia u siebie tylko 240 pracowników, w tym 140 wybitnych ekspertów technicznych. Głównym powodem powstania tej agencji w 1958 r. był szok dla amerykańskiego społeczeństwa i kręgów wojskowych spowodowany nieoczekiwanym wystrzeleniem przez ZSRR pierwszego sztucznego satelity Ziemi, czyli „Sputnika 1".

Jednym z rozwiązań powstałych w 1969 r. pod egidą DARPA była sieć informatyczna „Arpanet", która dała początek dzisiejszemu Internetowi. Dalsze losy Internetu i jego Sieci okazały się sensacyjnymi. Już pod koniec zimnej wojny do powstałej w ten sposób sieci Arpanetu, dołączyły sieci uczelniane i biblioteczne, przyjmując dzisiejszą nazwę „Internet".

Był to praktyczny sprawdzian możliwości stworzenia sieci informacyjnej na szerszą skalę. Próby wypadły pomyślnie i do tak poszerzonej sieci zaczęły dołączać sieci informatyczne gałęzi biznesu, handlu, szkolnictwa i inne oraz komputery prywatne, tworząc wielo milionową sieć internetową. Najszybszy rozwój Internetu zanotowano w latach 90. XX wieku.

W tym czasie Tim Berners, brytyjski uczony z „CERN Laboratory for Particle Physics w Szwajcarii, opracował pomysł utworzenia oficjalnej światowej sieci informatycznej pod nazwą WWW (World Wide Web), która zaczęła się rozwijać w wielkich rozmiarach. Wkrótce sieć WWW stała się najbardziej popularną wizytówką Internetu.

Dzisiaj Internet stanowi sieć różnych urządzeń elektronicznych połączonych ze sobą na zasadzie wspólnego „języka" i porozumiewania się kilkoma kliknięciami „myszy" komputerowej. Innymi słowy, „Internetem", „cyberprze-

strzenią", „infostradą" lub „Siecią" nazywa się teraz zbiór systemów służących do porozumiewania się, przekazywania (odbioru) informacji lub gromadzenia (magazynowania) zbiorów informacji i szerokiej wiedzy.

Obecnie powszechna dostępność Internetu obejmująca miliony komputerów, tworzy wiele możliwości komercyjnych, które oferuje światowa sieć, stając się dominującym systemem komunikacyjnym obecnego wieku. Korzyści płynące z Internetu powodują, że jego Sieć skupia większość kanałów telewizyjnych, telekomunikacyjnych i umożliwia dostęp do szeroko rozumianej wiedzy.

Cyberszpiegostwo

Gwałtowny rozwój nauki i techniki na świecie szczególnie w zakresie informacyjnych technologii komunikacyjnych z zastosowaniem komputerów, Internetu, jego sieci i innych urządzeń elektronicznych spowodował nasilenie **cyberszpiegostwa**.

Ma ono obecnie nie mniejszy ciężar gatunkowy niż szpiegostwo tradycyjne. Różnica polega tylko na tym, że jest prowadzone wobec obiektów i systemów znajdujących się w cyberprzestrzeni. Polega ono na nielegalnym zdobywaniu informacji dla danego państwa, bądź dla ważnych korporacji przemysłowych liczących się w skali międzynarodowej.

Tą drogą zdobywane są wiadomości o charakterze wojskowym, gospodarczym, bankowym, naukowo-technicznym (np. nowych technologii produkcyjnych i wynalazków) stanowiących tajemnicę państwową, służbową, firmową i prywatną.

Początki cyberszpiegostwa miały miejsce już w czasie wstępnego rozwoju Internetu. Rozpoczęli go hakerzy „buszujący" w Sieci internetowej, traktując włamania sieciowe do instytucji, przedsiębiorstw, banków i serwerów prywatnych jako „popis" umiejętności komputerowych. Z całej gromady działających na początku hakerów wymienię tylko dwóch, traktowanych jako komputerowych geniuszy wszech czasów.

Pierwszym z nich jest Kevin, Dawid Mitnick, wówczas 18-to latek o pseudonimie „Kondor", który włamywał się bezkarnie w latach 80–90 XX wieku do sieci systemów obronnych i firmowych USA. Mimo trzyletniego pościgu dokonywanego przez amerykańską FBI, schwytano go i osądzono (5 lat więzienia) dopiero w 2000 roku. Został zdemaskowany tylko dzięki pomocy innego hakera – Tsutomu Shimomury. Wyczyny hakerskie Mitnicka stały się

później kanwą filmów pt. „Gry wojenne" reżyserii Johna Badhama oraz filmu pt. „Operation Takedown"

Drugi wspomniany haker Albert Gonzalez, 23 letni amerykański samouk-informatyk, został okrzyczany rekordzistą od włamań do obiektów w Sieci. Korzystając ze współpracy dwóch rosyjskich programistów w latach 2006–2008, wykradł dane komputerowe 130 mln kart bankowych. Skradzione dane sprzedawał osobom trzecim, unikając w ten sposób schwytania. Obecnie siedzi w więzieniu w Brooklinie, oczekując na wyrok, także za inne przestępstwa.

Sukcesy tych i innych hakerów stały się zachętą dla zorganizowanych grup przestępczych[2] do „zawodowego" włamywania się do komputerowych systemów bankowych i prywatnych w celu zdobywania kodów, haseł dostępu, wyprowadzania dużych pieniędzy z kont bankowych oraz dokonywania zadań cyberszpiegowskich na zlecenie organów rządowych i na rzecz korporacji przemysłowych. Ostatnio Royal Bank of Scotland przyznał się, że w wyniku włamań cyberprzestępców poniósł straty w wysokości 5 mln funtów. Według szefa sekcji cyberprzestępczości FBI Jeffrey'a Troy'a piraci komputerowi wykradli w 2009 r. z kont bankowych na świecie 40 mln dolarów. Jednak dobrze zorientowani twierdzą, że wysokość skradzionych przez cyberprzestępców kwot bankowych różni się od ogłoszonych. Bowiem banki w obawie przed utratą renomy ukrywają prawdziwe szkody. Dotyczy to chociażby samych banków amerykańskich, które według Sean Henrego, szefa wydziału internetowego FBI, straciły w 2009 r. z powodu włamań hakerskich do sieci ponad 100 mln dolarów. Pogląd o faktycznych szkodach bankowych dają włamania wykonane przez jedną cyberprzestępczą grupę, która w ciągu 24 godzin za pośrednictwem dziesiątków bankomatów ukradła 10 mln dolarów z 130 banków w 49 miastach na 5 kontynentach. Dlatego bardziej wiarygodnie brzmi wypowiedź byłego szefa amerykańskiego wywiadu James'a Carafano, który uważa, że szkody spowodowane atakami hakerów na całym świecie są jeszcze wyższe i szacuje się je na 2 miliardy dolarów[3].

---

[2] Przykładem takiej mafijnej grupy, dokonującej włamań komputerowych w celach zarobkowych, jest rosyjska RBN (Russian Busines Network) która jest oskarżona o związki z Kremlem. RBN uważana jest za najgroźniejszą grupę piractwa komputerowego, zdominowując światowy rynek prawie wszystkich podejrzanych branż online jak pornografia, hazard, spam a także phishing (wyłudzanie danych, haseł i opróżnianie kont bankowych). Źródło: Michał Potocki, Skok na bank, czyli reaktywacja korsarstwa, Dziennik Gazeta Prawna, dodatek „Świat", 8–10 stycznia 2010 r.

[3] Marcin Bosacki z Waszyngtonu, Chiny idą na cyberwojnę, Gazeta Wyborcza, 2 lutego 2010 r.

Drugim nurtem szpiegostwa cybernetycznego prowadzonego przez organy państwowe, bądź organizacje mafijne działające na zlecenie rządów jest szpiegostwo wojskowe i gospodarcze. Do państw przodujących w tym przestępczym procederze zaliczają się Chiny i Rosja. Zmusiło to czołowe państwa Zachodu, które w obronie przed obcym cyberszpiegostwem, starają się dorównać w prowadzeniu podobnej działalności. Zwłaszcza, jak powiedział James Lewis, ekspert amerykańskiego CSIS (Centrum Analiz Strategicznych i Międzynarodowych) i długoletni pracownik amerykańskiej dyplomacji z Pentagonu – Gdy skarżymy się Chińczykom i Rosjanom, że nas szpiegują przez Internet, oni odpowiadają – „przecież robicie to samo!". Mają rację, ale z pewnym uściśleniem – to Ameryka, jej firmy i wojsko – wciąż przoduje w zaawansowanych technologiach. Rosjanie i Chińczycy mają u nas więcej do znalezienia niż my u nich… Jesteśmy w superlidze i możliwości ataku internetowego mamy większe…[4].

Mimo takich opinii, Stany Zjednoczone są ze wszystkich państw NATO najbardziej zagrożone cyberszpiegostwem ze względu na wysoko skomputeryzowane systemy zarządzania cywilnego i wojskowego. Nic dziwnego, że cyberszpiedzy z mniej rozwiniętych gospodarczo państw, od dawna próbują dobrać się do amerykańskich tajemnic wojskowych i technologicznych. Już w latach 80. XX wieku rosyjska KGB została przyłapana, kiedy jej agenci kopiowali dane z serwerów Departamentu Obrony USA. Znacznie większy atak na amerykańskie serwery rządowe został przeprowadzony z Moskwy w 1999 roku. Wprawdzie nie ustalono czy brały w nim udział władze Kremla. Niemniej stwierdzono, że rosyjscy cyberszpiedzy wykradli wtedy tajne informacje o amerykańskich systemach naprowadzania rakiet[5].

Takie wieści o rosyjskim cyberszpiegostwie nadchodzą niemal codziennie. Trudno się temu dziwić, szczególnie po ataku rosyjskich hakerów w 2007 roku na administrację, banki i firmy małej Estonii. Zwłaszcza, że rosyjscy hakerzy i programiści zajmujący się cyberszpiegostwem mają wysoką renomę w tym procederze. Ich specjalnością jest wymyślanie bardzo złośliwych wirusów ułatwiających szpiegowskie i złodziejskie włamania do obiektów internetowych.

Wkrótce po skonstruowaniu i rozpowszechnieniu złośliwego oprogramowania „Malware", ukazał się w sieci kolejny groźny wirus komputerowy pod nazwą „Conficker". Wirus ten wykorzystując lukę w zabezpieczeniach systemu

---

[4] Op. cit.

[5] Na podstawie NATO Review z listopada 2007 r.

operacyjnego Windows zainfekował 9 mln pecetów. Rosyjscy hakerzy, przy życzliwej tolerancji władz, rozwinęli czarny rynek z wirusami. Już za kilkaset euro można u nich kupić gotowe, bardzo skuteczne oprogramowania, które pozwalają nie tylko na uprawianie cyberszpiegostwa, ale również wykradanie kart bankowych, longin, haseł, adresów poczty elektronicznej i włamań do systemów bankowych.

O sprawności rosyjskich hakerów pisały niedawno media USA donosząc, że wykradli oni z kont amerykańskich obywateli dziesiątki milionów dolarów. Pomagają im w tym umiejętności do tworzenia „bonetów:, czyli sieci budowanych bez wiedzy właścicieli pecetów, które składają się z setek tysięcy „zniewolonych" maszyn. Dzięki temu mogą zalewać sieć spamem, przeprowadzać ataki odmowy dostępu do usług (tak zwaną D Do S), blokować dostęp do stron komercyjnych choćby potopem ogromnej ilości jednoczesnych wywołań. Skutkiem takich działań było zablokowanie w sierpniu 2009 r. na wiele godzin systemów Twitter, Facebook, You Tube oraz Live Journal po ataku metodą D Do S[6].

Znacznie większym niebezpieczeństwem dla Zachodu okazała się drapieżna działalność szpiegowska i cyberszpiegowska Chin. Służby specjalne Zachodu, zajęte tropieniem terrorystów islamskich, po atakach z dnia 11 września 2001 r. na USA, zlekceważyły chińskie niebezpieczeństwo. Tymczasem raporty panelu do spraw bezpieczeństwa powołanego przez Kongres Stanów Zjednoczonych oceniają, że chińska działalność szpiegowska stanowi najpoważniejsze zagrożenie dla bezpieczeństwa USA.

W najnowszym raporcie panelu ujawnionym w listopadzie 2009 r. ostrzega się przed nasileniem chińskich cyberataków na amerykańskie instytucje rządowe i firmy. Jest to związane z 9% wzrostem gospodarczym Chin, które chcą swoją potęgą dorównać nie tylko Japonii, ale nawet Stanom Zjednoczonym. W tym dążeniu ma pomagać Chinom wzmożona działalność cyberwywiadu w dziedzinie rozpoznania przemysłowego i wojskowego. Chodzi o to, że Chińczycy potrzebują teraz innowacji technologicznych w związku z nowym 5-letnim programem rozwoju kraju do 2010 r., co mogą ułatwić zawłaszczone zachodnie know-how. Dlatego ich wywiad jak odkurzacz – powiedział funkcjonariusz niemieckiego Urzędu Ochrony Konstytucji (czyli kontrwywiadu) – próbują wyciągnąć z Zachodu wszystkie nowości. Zasysają informację ze świata polityki, wojskowości, gospodarki i nauki[7].

---

[6] Michał Potocki, op. cit., Epidemia w sieci, L. Expansion z listopada 2009 r.

[7] Filip Gończak, Szpiedzy z Pekinu, Newsweek Polska, 1 listopada 2009 r.

Dlatego mnożą się cyberszpiegowskie ataki chińskie na urzędy i gospodarkę USA i inne kraje Zachodu, obliczane na kilkaset dziennie. Największa kradzież danych z instytucji rządowych USA miała miejsce w 2007 r., kiedy zaatakowano Pentagon, Departament Stanu, Energii, Handlu, NASA i służby specjalne. Cyberszpiedzy ściągnęli wtedy co najmniej 10 terabajtów informacji, co odpowiada danym z milionów książek z Biblioteki Kongresu USA. Najbardziej niebezpiecznym było włamanie z listopada 2008 r. do systemu informacyjnego dowództwa Sił Zbrojnych USA, które prowadzi wojny w Iraku i Afganistanie.

W następnych latach zaobserwowano nasilenie chińskiego cyberszpiegostwa. Wielkim sukcesem Chińczyków było wykradzenie z amerykańskiego koncernu lotniczego Lockheed Martin w 2009 r. wielkiej ilości danych komputerowych dotyczących tajnego projektu „niewidzialnego" myśliwca F-35JSF. Wartość skradzionych danych obliczono na około 300 mld dolarów.

Od połowy grudnia 2009 r. do stycznia 2010 r. chińscy cyberszpiedzy zaatakowali co najmniej 34 wielkich firm amerykańskich, z których wykradli tajne dane. Mimo bliskiej współpracy rynkowej firmy Google'a z Chinami, hakerzy z tego kraju w grudniu 2009 r. spenetrowali serwery giganta z Kalifornii. Od chińskiego ataku ucierpiało też 20 innych firm, m.in. Yahoo!, Adobe, Symantec, a także Northrop Grumman, będąca czwartą firmą zbrojeniową świata, produkującą niewidzialne bombowce B-2.

Chińska penetracja wojskowych i przemysłowych serwerów USA jest codziennością. We wrześniu 2009 r. wielokrotnie atakowali oni serwery Pentagonu, a nawet biura samego sekretarza obrony USA Roberta Gatesa. W latach 2003–2005 Chińczycy dokonali wielu udanych włamań szpiegowskich na systemy komputerowe m.in. Wojskowej Akademii Morskiej w Norfolk (kradnąc programy symulujące przyszłe konflikty zbrojne), a także do US Army Information Systems Engineering Command w Forcie Huachuca w Arizonie, Defense Information Systems Agency w Arligton, czy Naval Ocean Systems Center w San Diego. Akcja ta otrzymała nazwę „Tytanowy Deszcz"[8].

Wojny cybernetyczne

Cyfryzacja większości dziedzin zarządzania państwem, w tym jego administracją, obronnością, bezpieczeństwem, gospodarką, finansami, rozwojem

[8] Piotr Czarnowski, Groźby Google'a Chinom niestraszne, Dziennik Gazeta Prawna, 15–17 stycznia 2010 r.

nauki, techniki i in., z użyciem Internetu i jego Sieci, tworzy nie tylko postęp cywilizacyjny, ale również powoduje poważne zagrożenia. Jednym z nich jest wroga działalność hakerów, którzy wykradają z sieci informacje stanowiące ważne tajemnice obronne, gospodarcze, nowości techniczne, zbrojeniowe itp.

Z dotychczasowego opracowania wynika, że sposób organizowania i prowadzenia operacji hakerskich w wirtualnym świecie, niewiele odbiega od metod prowadzenia tradycyjnych działań wojennych. W obydwu przypadkach następuje w zbliżony sposób: wybór obiektu ataku, rozpoznanie celu, szczególnie jego słabych miejsc (cyberszpiegostwo), doboru środków walki, wykonanie skutecznego, najczęściej zmasowanego uderzenia, zdobycie oczekiwanych łupów (atrakcyjnych informacji, wartościowego oprogramowania, tajemnic naukowo-technicznych albo zniszczenia przeciwnika).

Różnicą jest tylko wyprowadzanie pieniędzy z kart bankowych, co jest formą zwykłego złodziejstwa, chociaż czynionego w cyberprzestrzeni przy pomocy technik informatycznych. Mimo to trudno nie dostrzec występowania licznych podobieństw w formach ataków cybernetycznego i militarnego. Na ogół obydwa rodzaje walki nakierowane na ważne cele, są wykonywane przez profesjonalne organy militarne i jednostki wojskowe. Zwłaszcza, że wbrew pozorom większość cyberataków służy w sposób zakamuflowany celom militarnym danego państwa lub wielkiej korporacji.

Dzisiaj specjalne jednostki wojskowe przygotowywane do prowadzenia wojny cybernetycznej posiadają przede wszystkim Chiny, Rosja, Izrael, Iran i Stany Zjednoczone. Ich formowanie przez służby specjalne i organy wojskowe zaczęło się wiele lat temu. Na początku było to werbowanie specjalistów do takich grup, których ówczesnym celem były włamania do sieci wojskowych i przedsiębiorstw tworzących lub posiadających nowoczesną technologię zbrojeniową.

Działania hakerskie tych grup służyły wspomaganiu klasycznych działań wywiadu. Do skuteczności tych działań przekonała się Wielka Brytania, która 25 czerwca 2009 roku powołała u siebie National Cyber Security Center. Do „Centrum" werbuje się byłych cywilnych hakerów w charakterze ekspertów.

Podobną agencję, chociaż wyspecjalizowaną raczej w dziedzinie bezpieczeństwa państwowych systemów informatycznych, utworzyła także Francja. Zaś bogaci Amerykanie w tym celu powołali całe super dowództwo pod kierownictwem czterogwiazdkowego generała. Dlatego wielu znawców tej problematyki wyraża przekonanie, że wojna cybernetyczna między wrogimi państwami lub konkurencyjnymi korporacjami produkcyjnymi – już rozpoczęła się.

Teraz przestrzeń cyfrowa stała się nowym polem walki, zarówno dla państw, jak i przedsiębiorstw. Tym bardziej, że konflikty wirtualne w Sieci

przynoszą realne i bardzo wymierne straty a nawet ofiary ludzkie. Francuski ekspert w dziedzinie nowych technologii Nicolas Arpagian uważa, że cyberprzestrzeń może być współczesnym polem walki na takiej samej zasadzie, jak ląd, woda, przestrzeń powietrzna, czy kosmiczna.

Zdaniem Nicolasa. Arpagiana[9] – cyberwojna opiera się na dwóch filarach: 1) na kanałach informatycznych, które wróg może zdalnie szpiegować, neutralizować lub przejmować nad nimi kontrolę, 2) na światowej sieci informatycznej lub w komputerach, gdzie pojawiają się i są przechowywane szczególnie wartościowe informacje należące do państw, przedsiębiorstw czy osób prywatnych. Takie zasoby informacji można „piratować", podmieniać, fałszować bądź niszczyć.

Cyberwojna może też przynosić rzeczywiste ofiary śmiertelne. Dzieje się tak wskutek cyberataku na systemy jądrowe, energetyczne czy urządzenia do sterowania skomplikowanymi procesami przemysłowymi (np. w dziedzinie chemii), albo w systemach zarządzania gospodarką komunalną (wodą, gazem, światłem, kanalizacją, dostawami i produkcją żywności, ratownictwem itp.). W wyniku cyberataku następuje zakłócenie, lub przerwanie działania systemów, co wobec ustania dostaw energii i zaburzeń w sterowaniu procesami może spowodować katastrofę. Zwłaszcza, że wymienione systemy są kierowane metodami cybernetycznymi. Poglądy te podziela amerykańska FBI, która w styczniu 2009 r. ogłosiła oficjalnie, że możliwość „cybernetycznej apokalipsy" stanowi jedno z głównych zagrożeń dla bezpieczeństwa USA. Przy czym stronami takiej sytuacji mogą być rządy, społeczeństwa czy jednostki ludzkie.

Cytowany Nicolas Arpagian uważa, że cyberwojna może się rozpocząć od zwykłego ataku informacyjnego, jak np. kampania oczerniania Francji prowadzona w Internecie przed igrzyskami w Pekinie i rozwinąć się aż po drastyczne ataki informatyczne. Ataki takie jak w przypadku Gruzji uziemiły jej lotnictwo latem 2008 r. podczas konfliktu z Rosją.

Francja też nie jest poza zasięgiem zagrożenia wojną cybernetyczną – powiedział N. Arpagian. Pod koniec zeszłego roku, dziesiątki komputerów francuskiego ministerstwa obrony, padło ofiarą podrzuconego „robaka" kompu-

[9] „Cyberwojna już trwa" źródło: L'Expansion z listopada 2009 r., Rozmowa z Nicolasem Arpagian'em. Rozmówca jest redaktorem naczelnym kwartalnika „Prospective Strategique",koordynatorem ds. nauczania w Instytut d'Etudes et de Rochercho pour la Securite des Entreprises oraz autorem kilku książek m.in. „La Cyberguerre-Laguerre numerique a commence" (Cybernetyczna wojna – wojna cyfrowa rozpoczęła się).

terowego noszącego nazwę „Conficker". Natomiast samoloty francuskiego lotnictwa marynarki wojennej zostały uziemione wskutek tego samego ataku.

Innym sposobem prowadzenia cyberwojny mogą być zakłócenia systemów kierowania rakietami przeciwnika w taki sposób, żeby pociski te spadały na jakiś szpital, a nie na koszary wojskowe, na które były wcześniej namierzone. Jeszcze bardziej dotkliwym prze kierowaniem informatycznym rakiet w połączeniu z zamachem terrorystycznym mogły być uderzenia dezorganizujące system komunikacji i działalność służb ratowniczych. Taka operacja może zwiększyć bilans strat ludzkich i spowodować frustracje wśród ludności[10].

Prawdopodobieństwo takich scenariuszy ma szanse powodzenia, ponieważ obecne komputery i pośrednictwo Internetu służy w większości do sterowania ważną cywilną i wojskową infrastrukturą. Dotyczy takich branż jak komunikacja, energetyka, przemysł i dystrybucja wody, energii i innych.

Mimo braku ostatecznej definicji określającej czym jest „wojna cybernetyczna" wiele wskazuje, że jej działania już się rozpoczęły. Można je prześledzić na przykładach licznych ataków cybernetycznych dokonywanych przez wrogich hakerów. Są one nakierowane na organy rządowe, centra wojskowe, organizmy przemysłu zbrojeniowego i przeważnie towarzyszą kryzysom dyplomatycznym oraz konfliktom zbrojnym.

Jednym z takich zdarzeń była wojna w Zatoce Perskiej w latach 1990–1991. Zanim przemówiły działa, hakerzy holenderscy żądni wysokiej zapłaty od Saddama Husajna prowadzili od kwietnia 1990 r. do maja 1991 r. włamania do 34 komputerów będących w gestii amerykańskiego Departamentu Obrony. Łupem tych włamań były bogate informacje dotyczące dyslokacji wojsk amerykańskich, ich uzbrojenia, wyposażenia, możliwości działania pocisków Patriot oraz ruchów amerykańskich okrętów w rejonie Zatoki Perskiej.

Informacje te były związane z amerykańskimi przygotowaniami do wojny z Irakiem. Po zdobyciu tych informacji hakerzy usunęli z systemu informatycznego wszelkie ślady włamań. Kiedy już rozpoczęła się inwazja na Irak, amerykańskie służby wojny cybernetycznej dokonały wirtualnego ataku na irackie systemy dowodzenia, paraliżując działanie lotnictwa wojskowego Saddama Husajna. Jednocześnie Amerykanom udało się podrzucić Irakijczykom w czipach drukarek komputerowych złośliwego wirusa AF/91. Działalność tego wirusa sparaliżowała monitory armii Saddama Husajna, utrudniając jego wojskom kierowanie operacjami wojskowymi.

[10] Według: „L'Expansion" z listopada 2009 r.

Działania wojowników wojny cybernetycznej, można też było zaobserwować w czasie wojny w Kosowie w 2001 r. Powodem prowadzenia jednego z wirtualnych starć hakerskich wojny cybernetycznej strony chińskiej z amerykańską, było przechwycenie przez Chiny samolotu szpiegowskiego USA, a także wspomniane wcześniej omyłkowe zbombardowanie ambasady chińskiej w Belgradzie przez samoloty USA w maju 1999 roku.

Jednak najbardziej typowym wyrazem wojny cybernetycznej, był zmasowany atak hakerów rosyjskich na wszystkie serwery i sieć internetową Estonii w maju 2007 r. Eksperci obliczyli, że w tym ataku na małą, liczącą zaledwie 1,4 mln mieszkańców Estonię, lecz mającą jedną z najgęściejszych sieci internetowych w Europie, brało udział około miliona wrogich komputerów. Pretekstem do rozpoczęcia „wojny cybernetycznej" była urażona duma władz Rosji z powodu usunięcia przez Estończyków z centrum Tallina pomnika żołnierza radzieckiego. Początki ataku zostały zauważone 26–27 kwietnia 2007 r., kiedy masowe fale e-maili wraz ze spamem i wirusami dosłownie „zatopiły" serwery estońskiego parlamentu, biura prezydenta i premiera Estonii.

Pod naporem tego cyberataku padł cały system zarządzania administracji państwowej Estonii, banki, poczta, redakcje największych gazet i większość firm. Tylko szkody wywołane unieruchomieniem działalności Hansa – banku przez jedną godzinę wyniosły milion dolarów Specjaliści międzynarodowi oszacowali ogólne szkody finansowe Estonii, jakie spowodowała cyberwojna, na kilka milionów euro. Nie trudno było ustalić skąd został wykonany cyberatak. Bowiem na rosyjskich stronach internetowych hakerzy prowadzili jawną rekrutację ochotników do prowadzenia cyberwojny z Estonią, a nawet podawali szczegółowe instrukcje jak można zaszkodzić sąsiadowi.

Według francuskiego kryminologa Laurence Ifrah, cyberatak na Estonię koordynowała znana rosyjska grupa cyberprzestępcza „Rusian Business Network". Tym samym nie można było dowieść władzom Kremla prowadzenia tej wojny. Chociaż rząd Estonii zwołał w dniu 30 kwietnia 2007 r. nadzwyczajną naradę ekspertów komputerowych, którzy opracowali i pomogli wdrożyć plan przeciwdziałania cyberinwazjii – w całym państwie zapanował chaos w systemach informatycznych i nie tylko.

Mimo pomocy międzynarodowych dostawców Internetu, którzy blokowali fale dopływu rosyjskich śmieci i spamu, w dniach 9–10 maja 2007 r. nastąpił drugi zmasowany cyberatak na estońskie serwery i Sieć. Atak nastąpił kiedy Moskwa świętowała dzień zwycięstwa nad faszyzmem. W tej sytuacji rząd Estonii musiał odciąć na dwie doby swój dostęp do Internetu dla zmniejszenia ponoszonych szkód. Wtedy przestraszona Finlandia podjęła się niezwłocznego

wzmocnienia własnych zabezpieczeń komputerowych przed możliwym cyberatakiem co kosztowało 200 mln euro.

Zaskoczeniem może być informacja, że Rosja będąc inicjatorem opisanej wojny cybernetycznej, sama stała się ofiarą podobnego cyberataku dokonanego przez hakerów z Kaukazu (prawdopodobnie Czeczenów). Celem ataku był system finansowy Rosji, co spowodowało straty rosyjskie obliczone na 300 mln dolarów.

Polska, chociaż jest krajem mniej rozwiniętym informatycznie od innych państw Unii Europejskiej i członków NATO, bywa często narażona na skutki cyberataków. Obliczono, że w 2008 roku wrodzy hakerzy dokonali na nasz kraj aż 500 tysięcy cyberataków. Były one skierowane na komputery i witryny polskich urzędów. We wrześniu 2009 r. rosyjscy hakerzy przypuścili kolejny atak na serwery polskich instytucji państwowych.

Wcześniej cyberatak wykonany w maju 2009 r. na komputery pracowników polskich instytucji państwowych, został udaremniony przez nasz Rządowy Zespół Reagowania na Incydenty Komputerowe, umiejscowiony przy Agencji Bezpieczeństwa Wewnętrznego. Metodą tego ataku było rozsyłanie pocztą elektroniczną złośliwego oprogramowania, które służyło do zbierania informacji, w tym transferowania poza dane instytucje dokumentów z twardych dysków i zasobów sieciowych[11].

Obrona przed skutkami cyberwojny

Obserwowane przejawy skutków wojen cybernetycznych i zbliżone do nich cyberataki szpiegowskie spowodowały, że obecnie wiele państw z całego świata rozwija własne cyberstrategie, mające chronić struktury dowodzenia armią, transportem czy systemami wczesnego ostrzegania przed cyberatakiem. Jest to konieczne, ponieważ życie uczy, że „normalna" wojna może rozpocząć się niespodziewanie i sekretnie w formie cyberwojny. Dlatego teoretycy wojskowi wyrażają pogląd, że każda tradycyjna wojna współczesna, powinna rozpoczynać się od cyberwojny, a conajmniej od cyberataku na przeciwnika w przestrzeni wirtualnej. Wtedy ataki prowadzone w cyberprzestrzeni będą rozszerzały arsenał tradycyjnych środków walki.

[11] Porównaj: Krzysztof Głowacki: Straż wirtualna, Polska Zbrojna, 8 listopada 2009 r.

Uzasadnieniem potrzeby wykonania takiej wojny lub cyberataku są niskie koszty ich prowadzenia w porównaniu z tradycyjną wojną. Można to zauważyć chociażby porównując drastycznie wysokie ceny najnowszych modeli samolotów bojowych, czołgów, rakiet naładowanych skomplikowaną elektroniką i innego sprzętu wojskowego. Tym bardziej, że wyprodukowanie i użycie nowoczesnego sprzętu wojskowego – nie przesądza dzisiaj o wielkości strat i zniszczeń zadanych przeciwnikowi z powodu wysokiej skuteczności dzisiejszych środków obrony i nie decyduje o ostatecznym zwycięstwie w wojnie.

Tymczasem skutki cyberataku i wojny cybernetycznej mogą być kolosalne w skali państwa. Bowiem dla sparaliżowania ważnych serwerów w ministerstwie obrony, sztabie armii, zakłóceniu strategicznej komunikacji informatycznej, zdobycie super tajnych informacji, czy rozkojarzenie systemów infrastruktury wojskowej i cywilnej, wystarczy mądry program komputerowy i grupa zdolnych hakerów.

Dlatego na całym świecie trwa cichy wyścig zmierzający do przygotowania lub obrony przed skutkami wojny cybernetycznej Prowadzą je nie tylko potęgi atomowe, ale też mniej rozwinięte państwa świata. W maju 2008 r. Pentagon w raporcie opracowanym dla Kongresu USA podał, że chińska armia utworzyła specjalne jednostki do prowadzenia wojny informatycznej.

W tym celu chińskie laboratoria opracowują, przy użyciu nowoczesnej technologii, nowe niezwykle złośliwe wirusy i robaki komputerowe. Skuteczność ich działania jest wypróbowywana w Internecie na szkodę Japonii, Korei Południowej, Tajwanu, USA i krajów NATO. Władze Pekinu przechwalają się, że za 40 lat Ch R L będzie w stanie wygrać cyberwojnę z każdym wrogiem. Dążenia chińskie potwierdza praktyka.

Stany Zjednoczone chociaż posiadają najbardziej rozbudowany system ochrony własnych struktur informatycznych, wciąż doznają wrogich cyberataków. Według NATO Review z 2007 r. odpowiedzią na cyberataki było powołanie do życia w połowie sierpnia 2007 r. „Ar Force Cyber Command" (Cybernetycznego Sztabu Sił Powietrznych), którego zadaniem jest „trening i wyposażenie jednostek zdolnych do prowadzenia globalnych operacji w cyberprzestrzeni". Równocześnie władze USA utworzyły Narodowy Wydział do spraw Bezpieczeństwa Cybernetycznego w Departamencie Bezpieczeństwa Narodowego. Wydział ten ma przygotowywać obronę przed atakami w cyberprzestrzeni.

Tymczasem w marcu 2009 r. amerykański senat zajął się ustawą, która ma powołać urząd narodowego doradcy do spraw cyberbezpieczeństwa, który ma nadzorować prace nad zabezpieczeniami w Narodowej Agencji Bezpieczeń-

stwa (NSA), siłach powietrznych, Departamencie Bezpieczeństwa Krajowego (DHS) i 10 innych agencjach rządowych. Ustawa wyposaży tego urzędnika w nadzwyczajne uprawnienia, w tym do wyłączania federalnych sieci w razie poważnego zagrożenia.

Uchwalenie ustawy może oznaczać poważną kontrolę a nawet ograniczenie działań w cyberprzestrzeni. Zwłaszcza, że wszystkie koncerny zbrojeniowe mają już własne wydziały do zwalczania cyberbezpieczeństwa i starają się o rządowe fundusze na ten cel. Tym samym wydatki rządu USA na bezpieczne sieci komputerowe mają wzrosnąć z 7,4 mld dolarów w 2008 r. do 10,7 mld dolarów w 2013 roku. Należy dodać, że większość dużych krajów NATO (jak Francja, Wielka Brytania i Niemcy) czynią podobne przedsięwzięcia zabezpieczające[12].

Jednak tylko Stany Zjednoczone stały się liderem w tworzeniu nowego rodzaju sił zbrojnych zdolnych nie tylko do obrony przed wrogimi cyberatakami, ale przede wszystkim do prowadzenia działań ofensywnych w cyberprzestrzeni. Świadczy o tym decyzja sekretarza obrony USA z dnia 23 czerwca 2009 r. Decyzja dotyczy powołania Dowództwa Operacji w Cyberprzestrzeni – US Cyber Command (USCYBERCOM), podległego Dowództwu Strategicznemu Stanów Zjednoczonych (USSTRATCOM). W ślad za tym, dla obrony cyberprzestrzeni USA, powołano podobne dowództwa w każdym rodzaju sił zbrojnych.

Pod koniec lipca 2009 r. generał lotnictwa USA Robert Elder z dowództwa tworzonego cybernetycznego centrum dowodzenia ujawnił, że amerykańskie sieci komputerowe są przedmiotem ciągłych ataków przez wszelkich wrogów USA, przede wszystkim Iranu i Chin. Hakerzy z tych krajów próbują wykradać nasze informatyczne tajemnice wojskowe i handlowe – dodał generał. Dlatego przeciwdziałaniem temu zagrożeniu służy wymienione „Centrum" znajdujące się w bazie lotniczej Barksdale w Luizjanie, gdzie pracuje 25 tysięcy ekspertów od Sieci komputerowych i wojny informatycznej[13].

Amerykanie zamierzają sformować specjalną armię wyszkoloną wyłącznie do prowadzenia nowoczesnej cyberkampanii wojennej. Tworzone przez Waszyngton specjalne struktury wojskowe i jego dowództwa służą do koordynowania ochrony systemów komputerowych i mają ściśle współpracować z Agencją Bezpieczeństwa Narodowego (NSA). Na czele obu struktur ma stanąć dotychczasowy szef NSA generał Keith B. Alexander.

---

[12] Jewgienij Morozow: Wróg w sieci, Newsweek Polska, 25 maja 2009 r.

[13] Marek Rybarczyk: Mundur dla hakera, Newsweek, 2 września 2007 r.

Prezydent USA Barack Obama chciałby, żeby w dziedzinie walki z cyberterroryzmem dokonywać bliskiej, lecz nie sformalizowanej współpracy z Kremlem. Chodzi o to aby organy USA miały możliwość penalizacji 50 tysięcy cyberataków jakie codziennie dotykają Stany Zjednoczone.

Jednak Rosjanie domagają się wcześniejszego zawarcia uniwersalnego, międzynarodowego traktatu,, który miałby uregulować zasady zwalczania cyberprzestępców. Tymczasem takie przepisy już zawiera Konwencja Rady Europy z 2004 r. dotycząca cyberprzestępczości.

Problem w tym, że Rosjanie nie aprobują tej Konwencji. Bowiem zawiera ona przepis pozwalający międzynarodowym organom ścigania na podjęcie działań śledczych nawet bez uprzedniego poinformowania o tym lokalnych władz. Natomiast Rosjanie traktują takie działanie jako naruszenie swojej suwerenności. Jest publiczną tajemnicą, że hakerzy rosyjscy i chińscy są w czołówce włamań do sieci komputerowych USA[14].

Mimo takich i innych trudności Amerykanie czynią wielkie postępy, żeby ochronić się przed skutkami wojny cybernetycznej. Ostatnio w USA przeprowadzono największe na świecie ćwiczenia symulujące odparcie cyberataków w takiej wojnie lub dokonanych przez cyberterrorystów. Bowiem Zachód bardziej obawia się coraz większych ataków dokonywanych na centra rządowe, wojskowe czy giełdowe przez hakerów pracujących dla wrogich reżimów czy informatyków powiązanych z islamistami.

Według przyjętych założeń, miejscem ćwiczeń i cyberpoligonem był Waszyngton. Według założeń „wrodzy" hakerzy zaatakowali ćwiczebnie sieci komputerowe należące do rządu, korporacji chemicznych, transportowych i telekomunikacyjnych. Ćwiczebną inwazję prowadzili wybitni specjaliści od bezpieczeństwa komputerowego z Ameryki, Wielkiej Brytanii, Australii, Kanady, Nowej Zelandii i informatycy z kilkudziesięciu firm. Prowadzone ćwiczenia pod kryptonimem „Cyber Storm II", były koordynowane przez Departament Bezpieczeństwa Wewnętrznego USA. Wyniki ćwiczeń wykazały, że zagrożenie jest bardzo realne i może przynosić wymierne straty informacyjne, zakłócenia działalności kluczowych dziedzin USA i wreszcie wielkie szkody liczone w miliardach dolarów.

Zdaniem Roberta Ayers'a specjalisty od spraw cyberterroryzmu z brytyjskiego „Chatham Hause" – nie należy dziwić się obawom Zachodu. Wojny w cyberprzestrzeni już trwają, powiedział R.Ayers. a my mamy do czynie-

[14] Radosław Korzycki: Cyberwyzwanie dla Ameryki, Dziennik – Gazeta Prawna 29 czerwca 2009 r.

nia z nowym rodzajem wyścigu zbrojeń. Nie ma wątpliwości, że im bardziej będziemy uzależnieni od Internetu i komputerów, tym pokusa uderzenia będzie rosła. Gdyby hakerom udało się np. sparaliżować pracę giełdy na Wall Street, gospodarka USA poniosłaby straty liczone w miliardach dolarów[15].

Czy Polska jest przygotowana do odparcia cyberataków?

Z medialnych doniesień wynika, że polskie serwery i Sieci rządowe, wojskowe, instytucji administracji państwowych i samorządowych, banków i ważnych korporacji branżowych były wielokrotnie przedmiotem obcych hakerskich cyberataków. Według informacji ABW dwie trzecie tych ataków w 2009 roku na polskie instytucje rządowe przeprowadzono z terytorium Chin. Drugą bazą wypadową wirtualnych przestępców atakujących RP było terytorium USA (15%). Sporadyczne cyberatakj pochodziły z Tajwanu, Holandii, Turcji i Danii. Eksperci podają, że w zeszłym roku ABW reagowało 6 tysięcy razy w 177 incydentach, które oceniano jako groźne. Co czwarty atak na serwery naszego rządu miał na celu zebranie ważnych informacji i zeskanowanie danych na dyskach komputerów. Na szczęście większość z nich została udaremniona przez patrole Agencji Bezpieczeństwa Wewnętrznego, które wychwytują podejrzane ruchy w Sieci. Zawdzięczać to należy mechanizmom i procedurom funkcjonującym w ramach Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL) działający przy Departamencie Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

Natomiast wczesnym ostrzeganiem o zagrożeniach w naszych sieciach zajmuje się uzupełniająco ARAKIS-GOV, powstały na potrzeby wsparcia ochrony zasobów teleinformatycznych administracji państwowej. Nie jest on typowym systemem zabezpieczającym i nie zastępuje standardowych systemów ochrony sieci jak: firewall, antywirus czy IDS/IPS. Jednak może być, z powodzeniem stosowany jako uzupełnienie tych systemów i powinien dostarczać wymaganych informacji w zakresie bezpieczeństwa informatycznego[16].

Nasz kraj wciąż jest na początku wdrażania procedur zabezpieczających przed cyberprzestępcami i szpiegostwem cybernetycznym. Zwłaszcza, że Polska jako były uczestnik operacji stabilizacyjnych w Iraku i obecny uczestnik w Afganistanie, jest wciąż na celowniku grup terrorystycznych. Tym samym

[15] Mirosław Wlekły: Pierwsze manewry w cyberprzestrzeni. Dziennik – Gazeta Prawna, 17 marca 2008 r.

[16] Krzysztof Głowacki: Straż Wirtualna, Polska Zbrojna, 8 listopada 2009 r.

trzeba się liczyć z możliwością cyberataków na odparcie których należy być przygotowanym. Dlatego zadowolenie wywołuje decyzja szefa naszego MON z listopada 2009 r. o przystąpieniu do prac nad budową Centrum Bezpieczeństwa Cybernetycznego. O dużym znaczeniu tego „Centrum" i całej problematyki cyberwojen dla bezpieczeństwa kraju świadczy fakt, że Centrum Bezpieczeństwa Cybernetycznego ma być zalążkiem przyszłego dowództwa nowego rodzaju Sił Zbrojnych RP[17].

Zakończenie

Cyfrowa rewolucja informacyjna dokonująca wielkiego postępu cywilizacyjnego we wszystkich dziedzinach naszego życia, tworzy równocześnie poważne zagrożenia dla ludzkości. Powszechny dostęp do Internetu i podłączonych do niego systemów sieciowych stał się nie tylko oknem na świat w dziedzinie komunikacji informacyjnej, skarbnicą wiedzy i sposobem na łatwiejsze zarządzanie państwem, ale także dogodną furtką przez którą przenikają przestępcy komputerowi. Są nimi szpiedzy wykradający tajemnice obronne, nowości przemysłowe, naukowe, bankowe włącznie z wyprowadzaniem wielkich pieniędzy z kont bankowych, a także ze sfery prywatnej.

Obecnie już wiemy, że przestępcze zastosowania złośliwych oprogramowań, ciągle doskonalonych (w postaci wirusów komputerowych), są w stanie nie tylko wykradać cenne tajemnice, lecz także blokować a nawet niszczyć systemy sieciowe konkurentów i przeciwników państwowych.

Rezultatem takich działań jest chaos w zarządzaniu państwem, jego systemami obronnymi, infrastrukturami wojskowymi i cywilnymi, powodując nawet szkody i straty fizyczne. Szczególnie ma to miejsce w procesach sterowania urządzeniami jądrowymi, energetyką, wrażliwą produkcją przemysłową, ratownictwem, systemami dowodzenia wojskami i in. Takie scenariusze już teraz tworzą, a nawet wypróbowują (na przykładzie Estonii) państwowi stratedzy militarni i mafijne organizacje przestępcze w postaci „wojen cybernetycznych".

Zagrożenia te są przedmiotem troski i przeciwdziałania nie tylko państw mocno skomputeryzowanych i powiązanych z Internetem obawiających się o własne bezpieczeństwo, ale też organizacji międzynarodowych (ONZ, Rady

[17] Robert Kośla: Obrona przez atak, Polska Zbrojna, 4 kwietnia 2010 r. Autor jest dyrektorem sektora bezpieczeństwa narodowego i obrony na region Europy Środkowej i Wschodniej w Microsoft CEE.

Europy, Unii Europejskiej, NATO i in.). Bowiem dzisiejsza „broń informatyczna" stała się nie mniej groźna niż nowoczesne rakiety i technika wojenna oparta na skomplikowanej elektronice, chociaż nie wymaga ponoszenia wysokich kosztów.

Dlatego wśród liczących się państw świata trwa prawdziwy „wyścig zbrojeń" informatycznych dla opracowania najlepszego sprzętu informatycznego i wymyślnych, niszczących i szpiegowskich programów do wrogich działań w świecie wirtualnym.

Dobrze się stało, że dla wypracowania wspólnej strategii wojennych działań informatycznych, NATO utworzyło w maju 2008 r. w Tallinie międzynarodowe Centrum Doskonalenia d/s Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (ang. Cooperative Cyber Defence Centre of Excellence – CDD CoE). Głównym zadaniem „centrum" jest prowadzenie badań nad bezpieczeństwem, formułowanie strategii obrony, promowanie zmian prawnych w szeroko przyjętym obszarze ochrony krytycznej infrastruktury informatycznej.