Antoni Krauz

Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej w globalnym świecie wiedzy

Edukacja - Technika - Informatyka 4/1, 388-399

2013

Antoni KRAUZ
Uniwersytet Rzeszowski, Polska

Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej w globalnym świecie wiedzy

1. Cyfrowa broń narzędziem destabilizacji infrastruktury krytycznej – implikacja pojęć

Narodowe i globalne systemy komunikacji, cała gospodarka, polityka, obronność, bezpieczeństwo, wojskowość są nasycone technologiami informacyjnymi o zasięgu światowym. Analizując stan bezpieczeństwa państwa, gotowości obronnej czasu pokoju, kryzysu i wojny należy mieć na uwadze infrastrukturę krytyczną o zasięgu lokalnym, krajowym i europejskim, która w głównej mierze oparta jest na systemach infrastruktury informatycznej, w tym globalnym Internecie. Aby posiadać pełny obraz stanu bezpieczeństwa i jego pochodnych oraz zagrożeń obecnie występujących, należy wyjaśnić niektóre pojęcia dotyczące *infrastruktury krytycznej i zasad jej ochrony.*

Zjawisko *infrastruktury krytycznej* o zasięgu krajowym, lokalnym oznacza systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych [Art. 3 pkt 2…].

Pojęcie *europejskiej infrastruktury krytycznej* o zasięgu obejmującym państwa UE oznacza systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach zaopatrzenia w zakresie: energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich

Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie [Art. 3 pkt 2a…].

System *ochrony infrastruktury krytycznej* obejmujący swym zasięgiem obszar krajowy, lokalny oraz UE oznacza wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub *słabym punktom* oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, *ataków* oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie [Art. 3 pkt 3…].

2. Internet jako współczesna groźna broń cyfrowa o zasięgu globalnym

Rewolucja informacyjna na świecie oprócz niewątpliwych zalet we wszystkich dziedzinach życia, w tym: ekonomii, gospodarki, handlu, nauki przyczyniła się również do powstania śmiercionośnej strony techniki informacyjnej zwanej cyberprzestępczością, cyberterroryzmem, cyberwojną, a nawet wojną internetową państwa przeciw państwu. Metody wykorzystania Internetu przez przestępców, terrorystów, hakerów, służb wrogiego państwa potajemnie wdzierających się do systemów komputerowych celem wprowadzenia wirusów, kradzieży informacji, wyłączenia ważnych służb państwowych, publicznych − niepokoją różne instytucje oraz komórki personelu ds. bezpieczeństwa państwa o zasięgu globalnym. Różnorodny, nieprzewidywalny system działania terrorystów, hakerów, grup przestępczych, mafii, grup wyznaniowych, w skali globalnej może być skierowany do wywołania destabilizacji, sabotażu, szantażu, kryzysu, zniszczeń nawet katastrofy w systemach: obrony, ochrony, ekonomii, bankowości, energetyce, zarządzania itp. w dowolnym miejscu na kuli ziemskiej. Postępująca informatyzacja codziennego życia człowieka generuje również powstawanie coraz to większego niebezpieczeństwa ataków hakerskich wszystkich dziedzin życia i gospodarki.

Internet jest obecnie używany nie tylko przez osoby prywatne, ale stanowi również podstawę obsługi i zarządzania infrastrukturą krytyczną praktycznie każdego państwa na świecie. Globalny zasięg ataku – ogólnoświatowa sieć połączeń sprawia, że można zarówno przeprowadzać ataki z każdego miejsca na świecie, jak i uderzyć na niemal każdy obiekt na naszym globie. Rozwój technologii i powszechna informatyzacja sprawiają, że bezpieczeństwo infrastruktury teleinformatycznej w systemie zarządzania infrastrukturą krytyczną jest obecnie kluczowym elementem bezpiecznego funkcjonowania każdego państwa i społeczeństwa [Art. 3 ustawy…].

Udowodniono, że dobry haker w zamian za odpowiednie wynagrodzenie jest w stanie kontrolować cały duży ważny z punktu widzenia bezpieczeństwa zakład techniczny. Sabotaż, szpiegostwo i inne groźne działania w Internecie mogące spowodować cyfrową katastrofę od dawna stanowią poważne zagadnienie globalnego bezpieczeństwa. Niewidzialna walka, która obecnie toczy się na

froncie internetowym jest niezauważalna dla opinii publicznej, natomiast staje się głównym zadaniem przeciwdziałania dla służb wywiadowczych.

Codziennie przez Internet przepływają setki miliardów gigabajtów danych, rocznie stanowi to 10 tryliardów bajtów informacji [„Świat Wiedzy" 2013: 108]. To idealne warunki do tego, aby każdego dnia w światowej sieci pojawiło się tysiące złośliwych programów. Częstotliwość ataków na komputery rządowe rośnie wraz z rozwojem Internetu. W 2015 r. połączonych ze sobą będzie 15 mld komputerów na całym świecie, stworzy to mega gigantyczny poligon do elektronicznych ataków. Umożliwi to zrzeszającym się rządom i wielkim korporacjom wykorzystując hakerów do zaszkodzenia wrogim państwom i konkurencyjnym przedsiębiorstwom [„Świat Wiedzy" 2011: 59].

3. Współczesne występowanie zagrożeń na rubieży internetowej

U podstaw rewolucji informacyjnej i społecznej leży właśnie otwarty, niczym nieskrępowany przepływ informacji. To dzięki wydajnym sieciom informatycznym dokonuje się wielu działań gospodarczo-finansowych, politycznych, administracyjnych na całym świecie. Ataki w cyberprzestrzeni stały się faktem, nie są działaniami wymagającymi wysokich nakładów finansowych, natomiast wywołują ogromne straty ekonomiczne i są działaniami trudnymi do udowodnienia. Ogólnoświatowy zasięg Internetu umożliwia praktycznie niczym nieograniczoną komunikację, a tym samym także planowanie i koordynowanie akcji cyberterrorystycznych, cyberprzestępczych, cyberwojennych. Wraz z rozwojem globalnej sieci internetowej negatywne zjawiska świata realnego, takie jak przestępczość i terroryzm, zaczęły przenikać do świata wirtualnego.

Przestępcy, hakerzy, cyberżołnierze przebywający w różnych miejscach, państwach na świecie mogą przygotowywać wspólny, czy ukierunkowany atak informatyczny bez ograniczeń miejscowych ani czasowych. Jest to czynnik nie do przecenienia, gdyż nie tylko ułatwia podejmowanie działań, ale także ogranicza w dużym stopniu możliwość udaremnienia akcji. Także dostępność narzędzi potrzebnych do przeprowadzenia ataku nie stanowi aktualnie problemu – komputer z dostępem do sieci jest w zasadzie przedmiotem powszechnego i codziennego użytku. Świadczy o tym nasilająca się w ciągu ostatnich lat, na niespotykaną wcześniej skalę, aktywność cyberszpiegów, a także rosnąca liczba ataków dokonanych przez hakerów na komputery państw, np. USA, Niemiec, Indii, Chin, Rosji, Estonii, Japonii, Gruzji, Polski, Egiptu, Tajwanu, Syrii, Ukrainy, to tylko niektóra państwa, które ujawniły tego typu działania. Cały świat obecnie stał się zależny od komputerów. To one są umiejscowione w systemie infrastruktury krytycznej, kontrolują dostawy energii, zarządzają komunikacją, lotnictwem i usługami finansowymi itd. Jutrzejszy, a nawet dzisiejszy terrorysta, przestępca, haker będzie w stanie więcej zdziałać przy pomocy klawiatury komputera niż konwencjonalnej broni, np. fizycznej bomby [*Computers at Risk…* 1991: 7].

4. Czynne znamiona groźnych cyberataków czasu pokoju, kryzysu i wojny

Przy wykorzystaniu nowoczesnych systemów informacyjnych, obecnej technologii i narzędzi elektronicznych, które umożliwiają stosowanie podstępu, infiltracji, siania zagrożeń, podsycania strachu itp. w czasie pokoju, kryzysu i wojny, tworzy się nowy wróg globalny zwany: cyberarmią, cyberhakerami, hakerską partyzantką, cyberprzestępczością, cyberterroryzm wykorzystywany do prowadzenia wojny internetowej, oto przykłady:

- kwiecień 1998 r., Indonezja, hakerzy zagrozili aktem sabotażu wobec indonezyjskiego systemu bankowego, jeżeli kraj ten odmówi uznania wyborów we Wschodnim Timorze;
- 1999 r. Kosowo, cyberterroryści dokonali ataku typu DoS (*Denial of Service*) na komputery NATO w czasie wojny w Kosowie;
- maj 1999 r. Serbia, zbombardowanie ambasady chińskiej w Belgradzie w odwecie spowodowało atak hakerów na amerykańskie komputery rządowe;
- sierpień 1999 r. Taiwan, wybucha wieloletnia wojna internetowa pomiędzy tajwańskimi a chińskimi hakerami;
- luty 2000 r., główne serwery amerykańskich wielkich firm informatycznych Yahoo, Amazon, CNN, eBay, itp. zostały zaatakowane za pomocą DoS *(Denial of Service),* co spowodowało wyłączenie na jakiś czas tych serwisów. Dopiero wtedy opinia publiczna zdała sobie tak naprawdę sprawę z tego, że cyberprzestępczość jest faktem. John Deutch, były szef CIA, stwierdził, że ataki te były testem skuteczności, przeprowadzonym przez członków organizacji Hezbollah;
- 2000 r. Indie, grupa pakistańskich hakerów zniszczyła około 600 indyjskich stron internetowych oraz przejściowo przejęła kontrolę nad niektórymi indyjskimi sieciami komputerowymi;
- luty 2001 r. Japonia, chińscy hakerzy dokonali kilkuset cyberataków na największe japońskie firmy w odwecie za zaostrzenie przez Japonię polityki wobec Chin;
- maj 2001 r., w stanie wojny elektronicznej znalazły się Stany Zjednoczone i ChRL, kiedy to amerykańscy hackerzy zaatakowali masowo chińskie strony internetowe. W odpowiedzi Chińczycy włamali się na strony amerykańskiej administracji i wielkiego biznesu. Obyło się bez wielkich strat materialnych, ale efekt pozwolił zdać sobie sprawę z tego, jak mogą wyglądać wojny w przyszłości;
- sierpień 2005 r. USA, 93 tys. ataków chińskich hakerów na strony internetowe amerykańskich urzędów oraz zakładów zbrojeniowych;
- maj 2007 r. Estonia, Rosyjscy hakerzy atakują w systemie DDoS (*Distributed Denial of Service*). Strategia polegała na wysyłaniu ogromnej liczby żądań połączenia, serwery nie były w stanie ich obsłużyć i padały. Padły największe i najważniejsze strony internetowe w Estonii;

- maj 2007 r. Estonia, w dniu 9 maja – rosyjskich obchodów Dnia Zwycięstwa, nastąpił kolejny duży atak. Wykorzystane wówczas sieci *botnet* liczyły około 10 tys. komputerów. Przez kilka dni e-infrastruktura Estonii legła w gruzach. Zablokowano strony estońskiego rządu, utrudniono pracę banków oraz elektrowni i sparaliżowano Internet;
- sierpień 2007 r. Niemcy, instytucje rządowe rejestrują masowe ataki przypuszczalnie chińskich hakerów;
- wrzesień 2007 r. Syria, hakerzy umożliwiają izraelskim samolotom zbombardowanie laboratorium badań jądrowych;
- styczeń 2008 r. Bliski Wschód, w okolicach Egiptu, w Zatoce Perskiej oraz wzdłuż Półwyspu Arabskiego zniszczonych zostaje wiele światłowodów łączących Europę z Azją;
- marzec 2008 r. Waszyngton, Pentagon informuje, że rok wcześniej, tj. w 2007 r. masowo zaatakowane zostały sieci pełniące ważną funkcję w systemie obronności państwa;
- sierpień 2008 r. Gruzja, równolegle do inwazji rosyjskich oddziałów na Gruzję rosyjscy hakerzy celowo paraliżują tamtejszą sieć internetową;
- listopad 2008 r. Francja, Niemcy, Wielka Brytania, bardzo groźny wirus komputerowy o nazwie *Conficker* infekuje 15 mln komputerów między innymi armii brytyjskiej, francuskiej niemieckiej, został wywołany przez hakerów z Ukrainy [http://tnij.org/grozny-robak 30.06.2013 r.];
- listopad 2008 r. Waszyngton, hakerom udaje się przy pomocy pendrivea zainfekować komputery sił obronnych USA;
- marzec 2009 r. Indie, przy pomocy portali społecznościowych tysiące indyjskich komputerów zastają scalone w ramach nielegalnego *botnetu*;
- kwiecień 2009 r. Niemcy, dochodzi do ponownych ataków systemów internetowych przez chińskich hakerów;
- styczeń 2010 r. Kalifornia, Google oraz dziesiątki innych firm technologicznych zostają zaatakowane przez chińskich hakerów;
- maj 2010 r. Waszyngton, w Stanach Zjednoczonych *Cyber Command* z uwagi na zagrożenie bezpieczeństwa rozpoczyna koordynację obrony amerykańskiej sieci internetowej, systemów informacyjnych;
- czerwiec 2010r. Iran, robak komputerowy *Stuxnet* atakuje irańskie instalacje atomowe;
- rok 2010, Polska, według raportu M. Iwanickiego firmy Symantec Poland pt.: *Norton Cybercrime Raport*, aż 71% użytkowników w Polsce padło ofiarą cyberprzestępczości. Przekładając to na liczby, atakowano 22 tys. Polaków dziennie z tego co minutę 15 osób, straty jakie poniesiono z tego tytułu to 3 mld zł. [„Świat Wiedzy" 2011: 62];
- styczeń 2011 r. Egipt, reżim Mubaraka odłącza Internet w całym Egipcie, żeby utrudnić organizację antyrządowych demonstracji;

- lipiec, sierpień 2011 r. USA, hakerzy skradli setki haseł amerykańskich pracowników rządowych, w tym należące między innymi do osób zatrudnionych w Biały Domu, za atakiem tym stoją prawdopodobnie Chiny;
- październik 2011 r. Newada, wirus atakuje komputery w bazie sił powietrznych Creech w Newadzie, przy pomocy których sterowane są drony, bezzałogowe statki powietrzne armii USA [„Świat Wiedzy" 2011: 61];

Przytoczone przykłady pozwalają zadać stosowne pytanie, czy wojna internetowa się zaczęła? Czy już się od dawna toczy? USA – Pentagon przygotowywał się do tego typu wojny wykorzystując swoich cyberżołnierzy już w 1999 r. (15 lat temu) podczas konfliktu w Kosowie. Stany Zjednoczony były już wówczas w stanie sparaliżować jugosłowiańską sieć telefoniczną i wyczyścić konta prezydenta Serbii Slobodana Milosevicia. Dlaczego tak się nie stało? Eksperci wojskowi twierdzą, że jeśli do ataku nie doszło, to tylko dlatego, że USA nie zamierzały ujawniać się i odkrywać kart przed konkurencją z Chin i Rosji [http://tnij.org/kosowo-cyberwojna 30.06.2013 r.]. Powyższe przykłady dobitnie pokazują, że pytanie „czy" nastąpi kiedyś globalny atak cyberterrorystyczny, powinno być zastąpione przez „kiedy". Waga zagrożenia powoduje, że bezpieczeństwo cyberprzestrzni stało się już jednym z ważniejszych zadań stojących przed forum międzynarodowym.

W obecnym świecie wiedzy obok dotychczasowej wojny klasycznej sukcesywnie pojawia się nowy jej wymiar, tj. wojna cybernetyczna, gdzie środowiskiem pola walki staje się globalna wirtualna przestrzeń cybernetyczna. Ocenia się, że w takiej wojnie strona atakująca przy minimalnych nakładach materialnych zdolna byłaby w znacznym stopniu sparaliżować kluczową infrastrukturę państwa przeciwnika, o ile oparta ona jest w wystarczająco dużym stopniu na systemach informatycznych. Wojna cybernetyczna byłaby więc atakiem asymetrycznym, co pozwoliłoby na prowadzenie tego rodzaju wojen również państwom słabszym przeciwko silniejszym, tego typu asymetria już ma miejsce.

5. Metody i formy cyberataków stosowanych dotychczas w Internecie

W ramach wojny cybernetycznej napastnik może dążyć do realizacji rozmaitych celów strategicznych, od rozpowszechniania propagandy lub wywoływania paniki pośród ludności cywilnej, po trwałe uszkodzenie kluczowych elementów infrastruktury technologicznej (elektrownie, systemy komunikacyjne itp.). Ataki mogą też być narzędziem wywiadu technologicznego i pozyskiwania informacji. W zależności od celu, ataki mogą wykorzystywać pełną gamę narzędzi: komputery zombie używane do ataków DDoS (*Distributed Denial of Service*), *exploity* pozwalające na przejęcie kontroli nad urządzeniami, metody socjotechniczne zmierzające do manipulacji ludźmi itp. Ataki tego typu mogą osłabić lub uszkodzić systemy wykorzystywane przez siły zbrojne przeciwnika, co może doprowadzić do ich całkowitego odsłonięcia na polu walki w czasie wojny elektronicznej. Infrastruktura informatyczna krajów rozwiniętych, tj. USA, Europy

i Azji są najbardziej narażone na cyberatak, cały świat zachodni jest praktycznie otwarty i bezbronny wobec ataków hakerów [Korsuń, Kościelniak 2001].

Ataki cyberterrorystyczne będą szczególnie eksponować słabości systemów komputerowych. Ich konsekwencje najpoważniej odczują ci, którzy są od nich uzależnieni. Zmienia się aktualnie forma ataku z konwencjonalnego na wirtualny. Obecnie zamiast zaporę wodną zburzyć ładunkami wybuchowymi, można ją otworzyć poprzez włamanie się do systemów ją kontrolujących, pociągu nie należy wysadzić za pomocą bomby, ale równie dobrze spowodować katastrofę zmianą jego trasy i kolizją.

W październiku 2002 r. FBI podało, że zaatakowanych zostało 13 podstawowych serwerów DNS („tłumaczą" one adresy internetowe na numeryczne adresy IP, wykorzystywane przez komputery, ich całkowite zablokowanie mogłoby spowodować zupełny paraliż Internetu). W rzeczywistości było to 13 jednoczesnych zmasowanych ataków DDoS. W krytycznym momencie działały tylko 4 serwery, cały atak trwał 6 godzin. Wielką globalną sieć zaatakował wirus, który niszczył wszystko, co napotykał na swojej drodze. Takim wirusem okazał się rzeczywiście słynny *I love you*, który spowodował miliardowe straty na całym świecie. Nawet Pentagon przyznał, że ofiarą tego wirusa padły cztery komputery klasyfikowane jako całkowicie bezpieczne, stanowiące część *Defense Data Network* – wydzielonej infrastruktury wojskowej.

Polska od lat plasuje się w czołówce odnotowujących największą liczbę ataków hakerskich. W opublikowanym niedawno raporcie Symantec poświęconym regionom Europy, Bliskiego Wschodu i Afryki, Polska zajmuje pierwsze miejsce pod względem otrzymywanego *spamu*. Jesteśmy drudzy pod względem posiadanych komputerów tzw. „zombie" zainfekowanych przez szkodliwe oprogramowanie i rozsyłających wirusa na kolejne komputery. Co więcej, aż 11% destrukcyjnej aktywności użytkowników Internetu w przebadanym regionie przypada właśnie na Polskę.

Brytyjskie ministerstwo obrony przekazało informację, że jest atakowane przez hakerów średnio co osiem godzin. Już w kwietniu 2009 r. ujawniono skutki takich ataków na USA, ze strony Chin najprawdopodobniej skradziono dane dotyczące supernowoczesnego niewykrywalnego samolotu myśliwskiego XXI wieku F-35, typu *stealth*. Według Jamesa A. Lewisa z Centrum Studiów Strategicznych i Międzynarodowych w Waszyngtonie cyberszpiegostwo jest najgorszą rzeczą jaka spotkała USA od czasu zdobycia przez ZSSR planów bomby atomowej w latach 40. XX w.

Kolejny przykład cyberwojny to muzułmańscy bojownicy hakują amerykańskie supernowoczesne drony bezzałogowe maszyny latające nad Irakiem, Afganistanem przy pomocy oprogramowania za 26 dolarów. Już w 2009 r. iraccy rebelianci byli w stanie przechwycić transmisję obrazu nadawanego na żywo przez znajdującego się w akcji bojowej drona. Pytanie: ile jeszcze terroryści potrzebują czasu, aby takiego drona zawrócić i uderzyć w zupełnie inny cel.

W 2010 r. przeprowadzono wśród 600 dyrektorów dużych zakładów z 14 krajów ankietę z pytaniem, czy firma była atakowana przez hakerów o dużym potencjale zniszczeń. Ponad połowa ankietowanych odpowiedziała tak, większość zaznaczyła, że stały za tym obce mocarstwa.

Dotychczas i obecnie wrogiem numer jeden w systemie wojny informatycznej są Chiny, które również znalazły się na celowniku ataków hakerskich. W 2010 r. rząd chiński podał, że zarejestrowano w ciągu jednego roku 500 tys. programów złośliwych, „trojanów – koni trojańskich", z czego 14,7% pochodziło z USA, 8% z Indii. Niejako w odpowiedzi odstraszenia podano, że Chiny są w stanie przez około 300 mln użytkowników Internetu zaatakować amerykańskie firmy [„Świat Wiedzy" 2011: 59].

Kolejne groźne zjawisko to luki w systemach informatycznych. Konferencja hakerów *DefCon* w 2011 r. pokazała, że można wgrać program w programowalne sterowniki logiczne (PLC) [„Świat Wiedzy" 2012: 57–58]. Obecnie sterują one wieloma maszynami oraz rejestrują sygnały alarmowe i inne informacje płynące z całego przedsiębiorstwa, np. są sercem i mózgiem elektrowni atomowych, innych dużych ważnych instytucji na całym świecie. Ta luka już została wykorzystana przez hakerów, którzy stworzyli i wprowadzili do systemu irańskiego robaka komputerowego *Stuxnet*[1], prawdopodobnie na zlecenie rządu USA i Izraela celem poważnego zaszkodzenia irańskiemu programowi nuklearnemu. Stąd wniosek cyberhakerzy, cyberprzestępcy, cyberterroryści są w stanie przejąć kontrolę nad programowalnymi sterownikami logicznymi urządzeniami PLC.

Idealnym celem w strukturze infrastruktury krytycznej może być atak informatyczny np. na elektrownie atomowe, wywołać krach na giełdzie itp., czy katastrofę ogólnoświatową. To pytanie zadają sobie dziś służby wywiadowcze na całym świecie. Na razie w prowadzonej zimnej cyberwojnie nie wykorzystuje się tej broni w sposób konwencjonalny, dotychczas ograniczano się jedynie do wirtualnych starć. Już w połowie października 2011 r. na wielu komputerach pojawia się nowy wirus robak *Duqu*, skonstruowany podobnie jak *Stuxnet*, jego zadaniem jest wyśledzenie słabych punktów w systemach przemysłowych i przesłanie informacji do komputera dowodzącego. Według firmy *Symantec* zajmującej się bezpieczeństwem w sieci *Duqu* jest aktywny pod różnymi postaciami już od końca 2010 r.

Zagrożone jest obecnie bezpieczeństwo osób z wszczepionymi urządzeniami medycznymi, np. rozrusznikami serca czy pompami insulinowymi. Przy ochronie bezpieczeństwa firmy IOActive stwierdzono, że wystarczy laptop z odpowiednim nadajnikiem, by przy braku zabezpieczeń z odległości 20 m

[1] *Stuxnet* – wirus jako groźna cyfrowa broń „Aleksandra" (dyrektor NSA Keith Aleksander, czterogwiazdkowy generał USA, nazwa pochodzi od imienia dyrektora NSA), wirus został opracowany przez armię jego agentów z NSA. „Świat Wiedzy", Wyd. Bauer, nr 8, Wrocław 2013, s. 108.

włamać się do implantów i przedstawić pracę pompy lub porazić serce napięciem ponad 800 V – pozbawiając życia człowieka [„Świat Wiedzy" 2012: 80].

Inny sposób cyberataku to wykorzystanie systemu DDoS (*Distributed Denial of Service*). Polega on na zalaniu serwera zapytaniami aż do momentu, w którym się zawiesi. Do tego nie jest konieczne żmudne pozyskiwanie haseł i przełamywanie barier bezpieczeństwa. W planach działania hakerów jest również praca na zamówienie prywatnych organizacji w zakresie wysłania tzw. bomb logicznych, specjalnych trojanów do struktur elektronicznych wrogiego państwa. Prześledzenie tego typu ataków jest niezwykle trudne. Ponadto hakerzy posiadają możliwość posługiwania się cyfrowymi ładunkami wybuchowymi z opóźnionym zapłonem, które mogą być odpalone – aktywowane w określonym czasie, doprowadzając do paraliżu systemu bezpieczeństwa.

6. Podejmowane przeciwdziałania w zakresie cyberataków

Już w początku lat 90., w okresie szybkiego rozwoju sieci komputerowych i wzrostu popularności Internetu, widmo elektronicznego Pearl Harbour zawisło nad Stanami Zjednoczonymi. W efekcie czego w 1997 r. przeprowadzono badania bezpieczeństwa systemów informatycznych w dziewięciu miastach Stanów Zjednoczonych, w tym przeprowadzono podobny test w odniesieniu do sieci komputerowej Pentagonu. Sporządzony raport wskazywał na zagrożenie trzema formami cyberataków: propagandowo-dezinformacyjnymi (modyfikowanie stron WWW), ideologiczny (*spamming*), sabotażem komputerowym (zamachy typu odmowa usługi, rozpowszechnianie wirusów i innych destrukcyjnych programów komputerowych) oraz zamachami na krytyczną infrastrukturę połączonymi z ingerencją w jej funkcjonowanie. Stąd w celu ochrony baz informatycznych w 1998 r. w centrali FBI utworzono Centrum Ochrony Infrastruktury Narodowej (NIPC). Następnie w Centralnej Agencji Wywiadowczej wyodrębniono Centrum ds. Wojny Informacyjnej (Information Warfare Center), zatrudniające tysiąc osób personelu, w tym pozostający w stanie gotowości przez 24 godziny na dobę zespół szybkiego reagowania.

Biały Dom podaje, że obecnie sam Departament Obrony Narodowej USA musi chronić 15 tys. swoich sieci i 7 mln komputerów przed milionami ataków hakerskich rocznie. Z uwagi na dotychczasowe nasilające się z Dalekiego Wschodu ataki informatyczne w maju 2011 r. Pentagon USA z ramienia rządu podał do wiadomości, że poważne ataki hakerskie będą traktowane jak działania wojenne, a Stany Zjednoczone odpowiedzą na nie zbrojnie [„Świat Wiedzy", 2011: 57].

Obecnie suma światowych nakładów na ochronę danych informatycznych wynosi 1600 mld dolarów. Niektóre państwa takie np. jak Korea Północna już posiada w armii jednostki wyszkolonych hakerów nastawione do zakłócania elektronicznej infrastruktury wrogich krajów. Wiele armii ma specjalne jednostki do walki elektronicznej. Stany Zjednoczone w ramach przeciwdziałania ata-

kom cyfrowym utworzyły program *cybernetyczny Pearl Harbor*, w ramach którego utrzymują jedyną w swoim rodzaju armię składającą się z 30 tys. cyberżołnierzy oraz potężny ośrodek wywiadowczy NSA (National Security Agency) zwany Crypto City w stanie Utach [„Świat Wiedzy" 2013: 105], w którym pracuje 20 tys. osób, powierzchnia zajmuje 260 ha. Ich zadaniem jest ochrona urzędów, przedsiębiorstw rządu oraz placówek naukowych i rządowych przed cyfrowymi atakami obcych mocarstw, przede wszystkim Chin [http://tnij.org/cyber-harbor 30.06.2013 r.].

W Polsce również do podmiotów wyspecjalizowanych zajmujących się walką z cyberatakami, cyberterroryzmem należy powołany do życia 1 lutego 2008 r. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, który jest integralną częścią Agencji Bezpieczeństwa Wewnętrznego (Departamentu Bezpieczeństwa Teleinformatycznego) i tym samym posiada wszystkie uprawnienia tej służby. Do jego głównych zadań należy „zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa [Borkowski 2013]. Oprócz posiadania krajowego systemu ochrony cyberprzestrzeni, Polska, jako członek Sojuszu Północnoatlantyckiego, uczestniczy w polityce ochrony przed cyberatakami w ramach NATO i dołączy (zgodnie z zapewnieniami polskiego MSZ) do Centrum Cyberobrony NATO.

Mało kto wie, że włączony komputer podłączony do sieci jest bezpieczny przez 10 min. Każde urządzenie w Internecie jest nieustannym celem skutecznych ataków. Aby ustrzec się przed takim scenariuszem, trzeba zadbać o to, by nasz komputer był na nie odporny. Trzeba także stosować się do kilku elementarnych zasad:

1. Staraj się korzystać ze stron oferujących szyfrowanie (ich adresy zaczynają się od https://) oraz zwracaj szczególną uwagę na komunikaty wyświetlane przez przeglądarkę.
2. Nigdy nie zgadzaj się na zapamiętanie loginu i hasła. Propozycja ta często pojawia się w momencie logowanie.
3. Pamiętaj także, aby po skończonej pracy wylogować się, korzystając z odpowiedniej opcji w serwisie WWW. Jeżeli o tym zapomnisz, serwis nie będzie wiedział, że zakończyłeś już swoją sesję i będzie traktował kolejnego użytkownika, który odwiedzi go niedługo po Tobie tak, jakbyś to Ty kontynuował swoje czynności.
4. Dbaj o swoje hasło. Nigdy nie pozostawiaj go zanotowanego na kartce umieszczonej na komputerze. Pamiętaj, że w miejscu publicznym może ono zostać łatwo podejrzane.

Literatura

Art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (opracowano na podstawie: DzU z 2007 r., nr 89, poz. 590; z 2009 r., nr 11, poz. 59, nr 65, poz. 553, nr 85, poz. 716, nr 131, poz. 1076; z 2010 r., nr 240, poz. 1600; z 2011 r., nr 22, poz. 114).

Art. 3 pkt 2a ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (opracowano na podstawie: DzU z 2007 r., nr 89, poz. 590; z 2009 r. nr 11, poz. 59, nr 65, poz. 553, nr 85, poz. 716, nr 13, poz. 1076; z 2010 r., nr 240, poz. 1600; z 2011 r., nr 22, poz. 114).

Art. 3 pkt 3 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (opracowano na podstawie: DzU z 2007 r., nr 89, poz. 590; z 2009 r., nr 11, poz. 59, nr 65, poz. 553, nr 85, poz. 716, nr 131, poz. 1076; z 2010 r., nr 240, poz. 1600; z 2011 r., nr 22, poz. 114).

Art. 3 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (opracowano na podstawie: DzU z 2007 r., nr 89, poz. 590; z 2009 r., nr 11, poz. 59, nr 65, poz. 553, nr 85, poz. 716, nr 131, poz. 1076; z 2010 r., nr 240, poz. 1600; z 2011 r., nr 22, poz. 114).

Borkowski P. (2013), *Polska wobec zjawiska cyberterroryzmu*, http://www.psz.pl/Piotr-Borkowski-Polska-wobeczjawiska-cyberterroryzmu

Computers at Risk. Safe Computing in the Information Age. System Security Study Committee Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications National Research Council, National Academy Press, (1991).

Encyklopedia popularna (1982).

Furmanek W. (2010), *Edukacja a przemiany cywilizacyjne*, Rzeszów.

http://www.interpactinc.com/IW1-1.pdf 3 15.05.2013r.

http://tnij.org/cyber-harbor

http://tnij.org/grozny-robak

http://tnij.org/kosowo-cyberwojna

Korsuń M., Kościelniak P., *Atak w cyberprzestrzeni*, „Rzeczpospolita" 27.09.2001 r.

Necas P., Kozaczuk F., Olak A., Krauz A., (2012), *Edukacja a poczucie bezpieczeństwa*, Rzeszów.

Nikt nie umknie przed cyberterrorystami, „Puls Biznesu", 06.10.2008 r.

„Świat Wiedzy", (2011), nr 5, Wrocław.

„Świat Wiedzy", (2013), nr 8, Wrocław.

„Świat Wiedzy", (2012), nr 12, Wrocław.

Streszczenie

W zamieszczonym artykule dokonano krótkiej charakterystyki problematyki zagrożeń i niebezpieczeństw spowodowanych rozwojem Internetu. Przedstawiono podejmowane próby ataków informatycznych, prowadzonej wojny internetowej skierowanej na różne dziedziny finansowo-ekonomiczne, administracyjne, militarne o zasięgu globalnym. Dokonano przeglądu różnych form i metod ataku

na infrastrukturę informatyczną, w tym infrastrukturę krytyczną. Przedstawiono rozwój zagrożeń ze strony broni cyfrowej, cyberterroryzmu, cyberprzestępczości, cyberwojny, podano przykłady ataków hakerskich występujących w skali globalnej. Omówiono przykładowy model zabezpieczenia systemu informatycznego komputera, korzystania z Internetu.

Internet tool for the weapon digital Critical Infrastructure in the global world of knowledge

Abstract

In the reproduced article presents a brief characterization of hazards and dangers caused by the growth of the Internet. Are shown attempts to attack information, conducted online war aimed at different areas of financial and economic, administrative, global military. There have been reviews of various forms and methods of attack on infrastructure, including critical infrastructure. Provides an overview of the risks posed by digital weapons, cyberterrorism, cybercrime, cyberwar, are examples of hacking attacks occurring on a global scale. Discussed an example of a computer system security model computer, using the Internet.

Keys word: Internet, critical infrastructure, information attack, cyberwar.