WITAJCIE W CYBERWOJNIE

WARSAW INSTITUTE

— RAPORT SPECJALNY —

WIKTOR SĘDKOWSKI

17/12/2020

- **Pierwsza w historii cyberoperacja „Kukułcze Jajo" finansowana przez sowieckie KGB miała miejsce już w 1986 roku. Odbyła się ona na zlecenie sowieckich służb. Dwie dekady później działania hakerów na stałe wpisały się w arsenał środków używanych przez skonfliktowane państwa. We wrześniu 2010 roku Ralph Langer używając sformułowania „Welcome to cyberwar" dał początek nowej erze konfliktów zbrojnych.**

- **Podstawowymi operacjami w cyberprzestrzeni, prowadzonymi przez wiele państw, są działania szpiegowskie. Fizyczny dostęp do urządzeń nie zawsze jest konieczny, aby przechwycić informacje przesyłane przez sieć.**

- **Cyberwojna między USA i Iranem jest uważana za pierwszy konflikt cybernetyczny. Rozpoczęła się od ataku wirusa Stuxnet na infrastrukturę irańskiego programu nuklearnego. Iran odpowiedział atakiem na sektor prywatny w USA oraz amerykańskich sojuszników. 15 sierpnia 2012 roku w pod nieobecność załogi Saudi Aramco, wirus Shamoon przystąpił do operacji kasowania danych z dysków twardych.**

- **Konflikt miedzy Rosją i Ukrainą rozpoczął się w lutym 2014 roku. W tym samym czasie analitycy firmy F-Secure natknęli się na zmodyfikowaną wersję złośliwego oprogramowania o nazwie BlackEnergy. Konflikt rosyjsko-ukraiński to modelowy przykład wojny hybrydowej, wykorzystującej tradycyjne środki militarne oraz cyberoperacje.**

- **W 2017 roku USA przeznaczyło 6.7 miliardów dolarów na operacje w cyberprzestrzeni, w 2019 budżet wzrósł do 8.5 miliarda dolarów. Szacuje się, że obecnie na świecie brakuje około 3.5 miliona osób z wiedzą oraz doświadczeniem w dziedzinie cyberbezpieczeństwa.**

Wprowadzenie

W ubiegłym wieku Albert Einstein nie chciał przewidywać jakim rodzajem broni będą posługiwać się armie, które staną naprzeciw siebie podczas III Wojny Światowej. Mając jednak na uwadze potencjał i niszczycielską siłę broni atomowej sugerował, że czwarty globalny konflikt odbędzie się przy użyci drewnianych włóczni i kamieni. Ponad pół wieku później w dalszym ciągu ciężko jest przewidzieć, jaki dokładnie arsenał będzie użyty w niewykluczonym światowym konflikcie. Wiemy jednak, że niebrane pod uwagę kilkadziesiąt lat temu obszary pola walki odegrają podczas ewentualnego starcia ważną, a może nawet kluczową rolę.

Pod koniec grudnia 2019 roku USA oficjalnie powołało do życia USSF (United States Space Force), nową gałąź sił zbrojnych, która kilka dekad wcześniej pojawiała się wyłącznie w literaturze i filmach należących do gatunku fantastyki naukowej. To najmłodsza z formacji, która z oczywistych względów do tej pory nie miała szans na sprawdzenie się w boju. Tym samym jej znaczenie w nadchodzących latach nie do końca jest możliwe do przewidzenia. Utrzymujący się przez lata podział na tradycyjne obszary działań wojennych, jakimi były woda, ląd i powietrze, został także poszerzony wcześniej o cyberprzestrzeń. Tutaj, w przeciwieństwie do kosmosu, skuteczność działania została wielokrotnie sprawdzona, a operacje w cyberprzestrzeni od lat prowadzone są na dużą skalę przez wiele stron.

Operacje w cyberprzestrzeni od lat prowadzone są na dużą skalę przez wiele stron.

Cyberprzestrzeń jako obszar działań oficjalnie została uznana w lipcu 2016 podczas szczytu państw członkowskich NATO w Warszawie. To właśnie wtedy członkowie sojuszu zobowiązali się do wdrożenia *Cyber Defence Pledge* uznając za konieczne wzmocnienie cyberbezpieczeństwa krajowych sieci oraz krytycznej infrastruktury. Decyzja państw NATO była podyktowania koniecznością wynikającą z potrzeby unormowania działań operacyjnych w cyberprzestrzeni. Te trwały od kilku lat na pełną skalę, a ich skutki dotykały obywateli wielu państw, oficjalnie nieuwikłanych w konflikt zbrojny.

ŹRÓDŁO: NATO.INT

Nowe pole walki

Sześć lat przed podpisaniem wspomnianej deklaracji, we wrześniu 2010 roku Ralph Langner, specjalista w dziedzinie bezpieczeństwa systemów sterowania, zakończył swoją analizę[1] znanego obecnie wszystkim zainteresowanym tematyką cyberbezpieczeństwa wirusa słynnymi słowami „*Welcome to cyberwar*" - „Witajcie w cyberwojnie". *Stuxnet*, bo to o nim mowa, co prawda nie był pierwszym przypadkiem cyberoperacji, ale z pewnością najsłynniejszym, głównie za sprawą słów kluczowych pojawiających się w artykułach na jego temat: wirus, komputer, elektrownia atomowa.

Do dziś trwają spory między ekspertami o konkretną definicję cyberwojny, a podział między wojną informacyjną a wojną cybernetyczną wydaje się bardzo mglisty i nieprecyzyjny. W przypadku tradycyjnych operacji dezinformacyjnych, jakie miały miejsce podczas dawnych konfliktów, sprawa była prosta. Kolportaż ulotek zawierających fałszywe informacje to bez wątpienia wojna informacyjna. Kradzież planów badawczych z ośrodka naukowego innego państwa to także zgodnie z encyklopedyczną definicją wojna informacyjna. Co jednak w przypadku gdy atakujący, przy pomocy zaawansowanych technik penetruje liczne zabezpieczenia systemów informatycznych firmy produkującej myśliwce F-22 i wykrada szczegóły technologiczne w celu zyskania przewagi na polu

Do dziś trwają spory między ekspertami o konkretną definicję cyberwojny, a podział między wojną informacyjną a wojną cybernetyczną wydaje się bardzo mglisty i nieprecyzyjny.

1. www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz

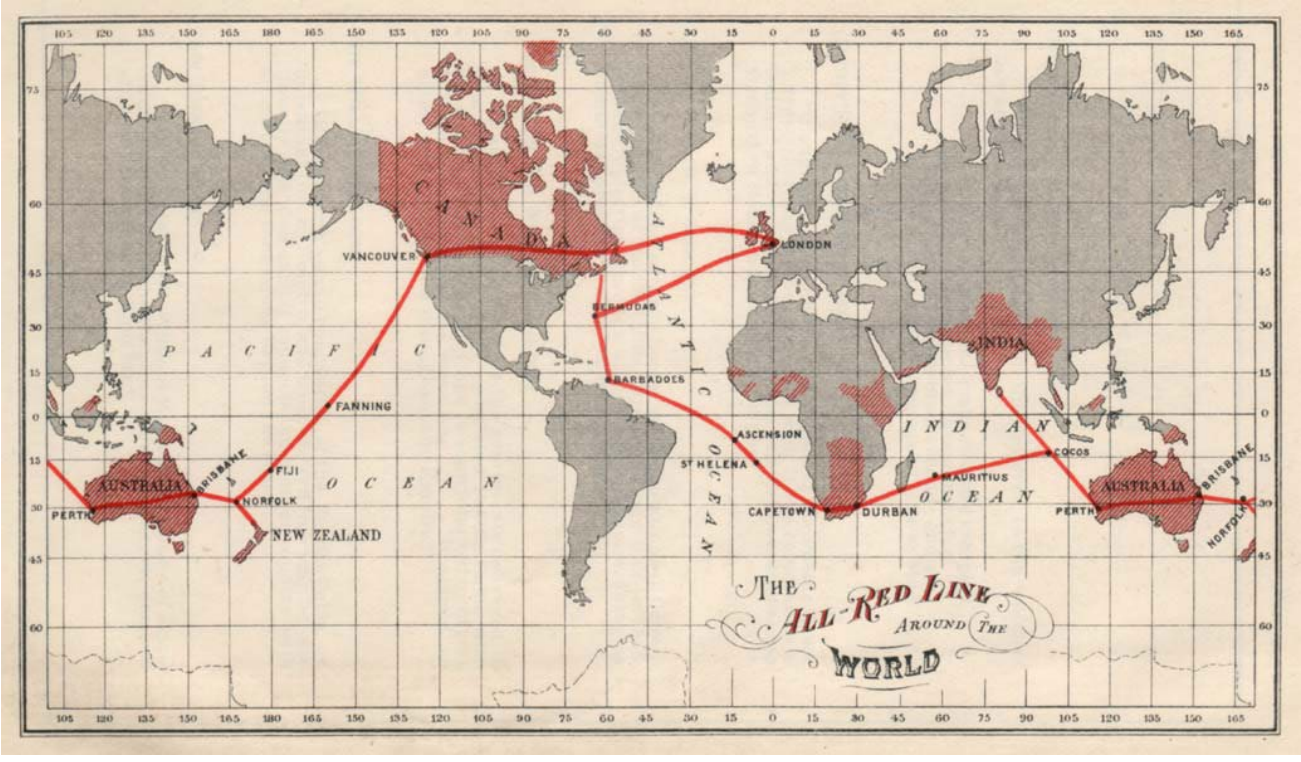
walki? Nadal mamy do czynienia z wojną informacyjną? A jeśli atakujący, w trakcie dostępu do systemów firmy, niepostrzeżenie modyfikuje oprogramowanie myśliwców tak, aby mieć możliwość ich uziemienia? Czy to już cyberwojna? Granica jest jak widać sztuczna i zupełnie niepotrzebna w obecnym świecie - niemal całkowicie uzależnionym od systemów informatycznych.

Wykorzystanie systemów telekomunikacyjnych w celach szpiegowskich ma bardzo długą historię. W 1858 kablem transatlantyckim umożliwiono przesyłanie telegramów między Irlandią a Nową Funlandią, a do roku 1902 roku system telegraficzny rozbudowano w sposób umożliwiający przesyłanie informacji dookoła całej kuli ziemskiej. Centrum systemu, główna stacja kablowa, mieściła się w Portcurno w Kornwalii. Obecnie nieczynna, przekształcona w muzeum stacja, przez dziesiątki lat była głównym miejscem pozyskiwania informacji przez wywiad brytyjski. To właśnie tutaj telekomunikacyjni szpiedzy w styczniu 1917 przechwycili telegram Zimmermana[2], którego ujawnienie bez wątpienia przyczyniło się do decyzji Kongresu Stanów Zjednoczonych o przystąpieniu do I Wojny Światowej.

Operacja „Kukułcze Jajo" była finansowana przez KGB i rozpoczęła się w 1986 roku.

System telegraficzny nie był systemem komputerowym, więc nie sposób przypisać temu zdarzeniu charakteru cyberoperacji. Warto jednak o nim pamiętać, gdyż tego typu manewry nadal stanowią podstawę pozyskiwania danych z nowoczesnych systemów telekomunikacyjnych, które w ostatnim wieku uległy znacznym technologicznym zmianom. Amerykanie zbudowali ARPANET (*Advanced*

ŹRÓDŁO: DOMENA PUBLICZNA



2. www.en.wikipedia.org/wiki/Zimmermann_Telegram

Research Project Agency Network), który przy międzynarodowym wsparciu połączył lokalne sieci w globalny Internet. Ten od 1991 roku używany jest komercyjnie i stanowi integralną cześć życia niemal każdego człowieka. Zanim do wspomnianej pełnej komercjalizacji doszło, mieliśmy do czynienia z uznawanym przez wielu ekspertów pierwszym atakiem na systemy komputerowe. Operacja „Kukułcze Jajo", o której mowa, była finansowana przez KGB i rozpoczęła się w 1986 roku. Niemiecki haker, działając na zlecenie sowieckich służb, wykradał z sieci komputerowych amerykańskich instytucji wrażliwe dane, takie jak kod źródłowy oprogramowania (objętego ograniczeniami eksportowymi), plany wojskowe i hasła systemów. Włamując się do systemów uczelni, laboratoriów oraz komputerów w wojskowej sieci MILNET, haker uzyskał dostęp między innymi do plików z planami użycia broni atomowej na wypadek konfliktu w Europie (jak jednak później udowodniono, były one dostępne publicznie i nie stanowiły tajemnicy). Jego działania odkrył Clifford Stoll – astronom pracujący jako administrator systemu w laboratorium Berkeley. Udało mu się nawet wyśledzić hakera, który operował z terytorium RFN. Dzięki pomocy niemieckiego operatora telekomunikacyjnego hakera złapano w jego domu w Hanowerze i postawiono przed sądem[3]. Włamania, jakich dokonywał niemiecki haker, polegały głównie na odgadnięciu haseł do systemów. W większości przypadków atak był możliwy, gdyż administratorzy nie przywiązywali wystarczającej uwagi do bezpieczeństwa systemu, często nie zmieniając domyślnych haseł.

Dekadę później agencje rządowe w Stanach Zjednoczonych zostały ponownie zinfiltrowane. W lipcu 1998 roku FBI rozpoczęło śledztwo w sprawie przypadkowo odkrytej, podejrzanej aktywność w sieci komputerowej bazy Sił Powietrznych Wright-Patterson. W toku śledztwa zorientowano się, że zaatakowanych instytucji jest więcej: laboratoria badawcze Marynarki Wojennej USA, sieci AFIT (Air Force Institute of Technology), sieci Departamentu Energii, baza Los Alamos[4]. Z tych i wielu innych instytucji hakerzy wykradali niedostępne publicznie dane. Po pewnym czasie śledczy odkryli też, że ta sama grupa odpowiedzialna była za ataki na instytucje w Wielkiej Brytanii, Kanadzie, Niemczech i Brazylii. Włamania dokonywane były przy użyciu znanych, a czasami ogólnodostępnych eksploitów (programów wykorzystujących znane podatności), ponownie więc wykorzystano głównie niefrasobliwość administratorów systemów, którzy na czas nie zabezpieczyli ich przed znanym zagrożeniem.

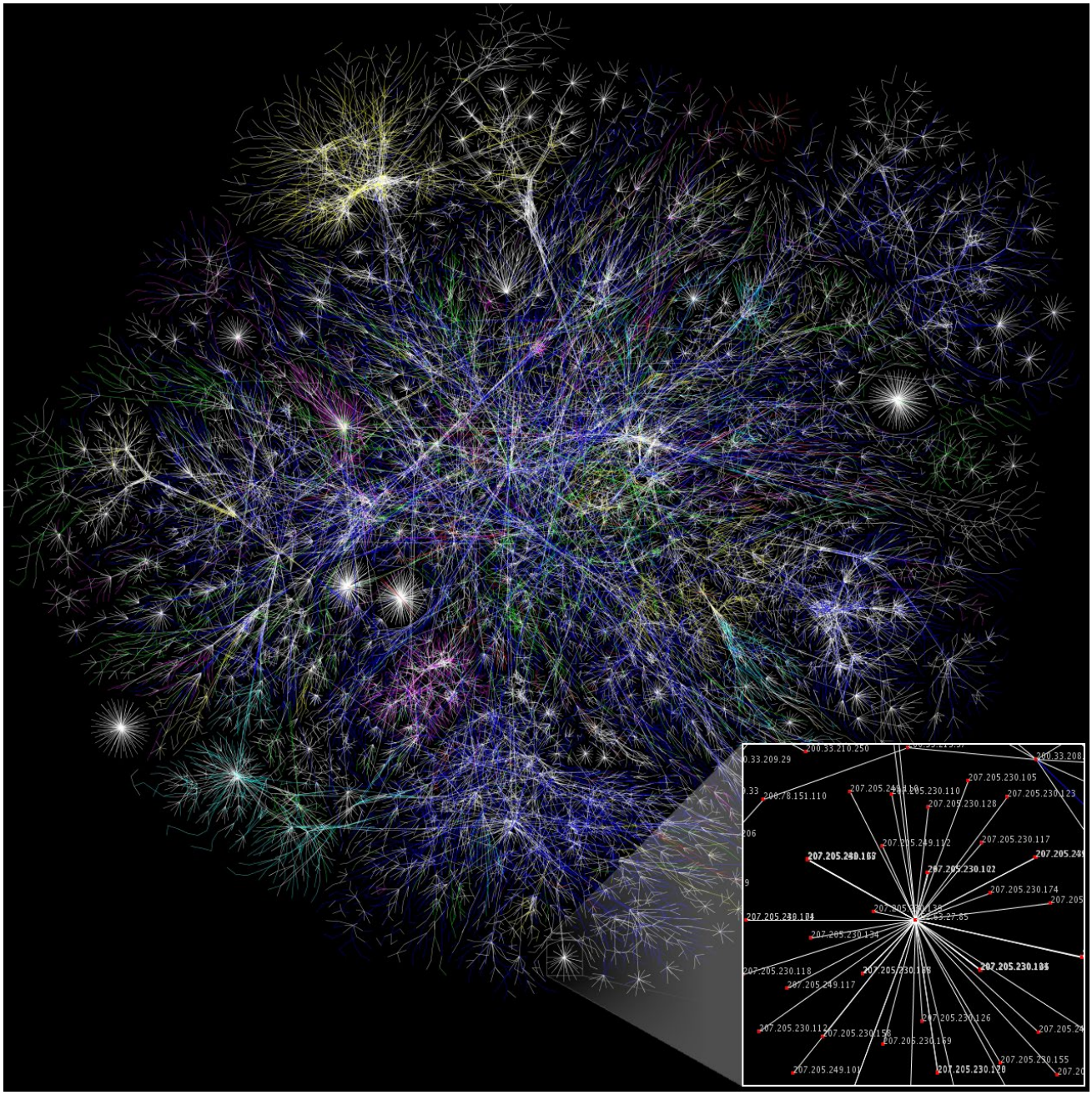
Przewaga własnego boiska

Wspomniana wcześniej XIX wieczna operacja podsłuchiwania informacji w systemie telegraficznym ma swoją kontynuacje po dziś dzień. Systemy telekomunikacyjne są znakomitym źródłem informacji dla agencji wywiadowczych i innych instytucji odpowiedzialnych za bezpieczeństwo państwa. Nic więc dziwnego, że dążą one do przechwytywania jak największej ilości informacji przesyłanych przez sieć. Amerykanie z racji swojej wiodącej pozycji na rynku globalnych firm technologicznych mają niewątpliwie przewagę nad innymi krajami w tej kwestii. Ujawnione przez Edwarda Snowdena w 2013 roku dokumenty ujawniły, że NSA wspólnie z brytyjskim GCHQ miała rzekomo podsłuchiwać dwie największe ówcześnie firmy technolo-

3. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, 2005, Cliff Stoll
4. PENQUIN'S MOONLIT MAZE:The Dawn of Nation-State Digital Espionage, 2017, J.G.-S.,C.R.,D.M.,T.R.

giczne (Google oraz Yahoo). Bez wiedzy obu firm wspomniane agencje wywiadowcze w ramach projektu MUSCULAR podsłuchiwały ruch w kablach telekomunikacyjnych sieci, do której podłączone były centra firm technologicznych[5]. Biorąc pod uwagę fakt, że z usług Google oraz Yahoo korzysta cały świat, dość łatwo dojść do wniosku, że operacja ta miała na celu po prostu wykorzystywanie „przewagi własnego boiska". Mając możliwości technologiczne, NSA oraz GCHQ dążyły do przechwycenia jak największej ilości interesujących ich danych na temat działalności obywateli innych krajów. Innym przykładem takiej aktywności może być infiltracja systemu wideokonferencyjnego Organizacji Narodów Zjednoczonych[6], upubliczniona również w 2013 roku. Tu warto nadmienić, że ONZ, jak wynika z informacji medialnych, mogła być w tym samym czasie podsłuchiwana co najmniej przez 2 kraje. Informacje mieli

ŹRÓDŁO: WIKIMEDIA COMMONS



5. www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links
6. www.latimes.com/world/worldnow/la-fg-wn-nsa-leaks-spying-un-20130826-story.html

zbierać zarówno Amerykanie, jak i hakerzy z Chin[7]. Czasami tego typu przewagę agencje wywiadowcze starają się uzyskać poza granicami własnego kraju. W 2015 roku, po trwającym 10 lat śledztwie, rząd Grecji wskazał agenta NSA jako odpowiedzialnego za założenie nielegalnych podsłuchów w tamtejszym systemie operatora komórkowego *Vodafone*. Połączenia wykonywane przez ponad 100 użytkowników (głównie pracowników rządowych, w tym ówczesnego premiera Grecji) były podsłuchiwane przez nielegalnie zainstalowane na przełącznikach sieciowych oprogramowanie, które w normalnych okolicznościach jest wykorzystywane przez operatorów telekomunikacyjnych w celu legalnego monitorowania transmisji danych (po uzyskaniu stosownych pozwoleń i decyzji)[8]. Fizyczny dostęp do urządzeń nie zawsze jest konieczny do przechwycenia informacji przesyłanych przez sieć. Protokół BGP (*Border Gateway Protocol*) jest podstawą działania współczesnego Internetu. To on decyduje o trasie, jaką mają pokonać dane wysyłane między nadawcą a odbiorcą.

Z założenia trasa ta powinna być jak najkrótsza. Możliwe jest jednak celowe doprowadzenie do sytuacji, w której dochodzi do tak zwanego „wycieku tras" (*BGP Route Leak*). Sytuacja taka miała miejsce chociażby w 2015 roku, kiedy ruch między Koreą Południową a Kanadą został przekierowany przez centra należące do *China Telecom*. Ten sam proceder powtórzył się w 2017 roku i dotyczył przechwycenia ruchu między Szwecją a amerykańskim oddziałem agencji informacyjnej w Japonii. Ostatnia tego typu sytuacja miała miejsce w czerwcu 2019 roku, kiedy to przetrasowaniu uległ ruch operatorów sieci komórkowej działający we Francji, Holandii i Szwajcarii. Przez ponad 2 godziny połączenia wykonywane przez ich klientów przesyłane były przez infrastrukturę *China Telecom*[9].

Ujawnione przez Edwarda Snowdena w 2013 roku dokumenty ujawniły, że NSA wspólnie z brytyjskim GCHQ miała rzekomo podsłuchiwać dwie największe ówcześnie firmy technologiczne .

USA vs Iran

Cyberoperacje wywiadowcze stanowią tylko jeden z rodzajów aktywności w cybernetycznym arsenale. Szeroki wachlarz ataków został użyty przez obie strony konfliktu pomiędzy USA i Iranem. Najbardziej znanym był wspomniany wcześniej *Stuxnet*, wirus, którego zadaniem było uniemożliwienie Iranowi rozwoju programu nuklearnego. *Stuxnet* wykorzystywał nie tylko nieznane publicznie podatności systemu opera-

W wyniku użycia wirusa Stuxnet udało się zniszczyć niespełna tysiąc wirówek w zakładzie wzbogacania uranu, co opóźniło program nuklearny Iranu o ponad 5 lat.

7. www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html
8. www.en.wikipedia.org/wiki/Greek_wiretapping_case_2004-05
9. www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/

cyjnego, ale także luki w bezpieczeństwie sterowników PLC (*Programmable Logic Controller*), które stanowiły integralną cześć systemów w irańskim ośrodku nuklearnym Natanz. W wyniku jego użycia udało się zniszczyć niespełna tysiąc wirówek w zakładzie wzbogacania uranu, co opóźniło program nuklearny Iranu o ponad 5 lat[10]. Twórcy wirusa nie osiągnęli swojego celu małym kosztem; rozwój tak skomplikowanego rozwiązania pochłonął środki przekraczające co najmniej kilkadziesiąt milionów dolarów. Precyzyjne uderzenie wymagało nie tylko pracy programistów, ale też ekspertów posiadających wiedzę na temat systemów ICS, SCADA i samych sterowników Simatic PLC. Z całą pewnością wirus został dokładnie przetestowany zanim uderzył, tak więc zakup samych wirówek P1 używanych w Natanz musiał zostać sfinansowany z budżetu przeznaczonego na rozwój cyberbroni[11]. Iran odpowiedział atakiem na sektor prywatny w USA. W 2012 zaatakowane zostały amerykańskie banki. Niezbyt skomplikowany z technicznego punktu widzenia atak DDoS (*Distributed Denial of Service*) uniemożliwił klientom amerykańskich instytucji finansowych m.in. dostęp do systemów bankowości elektronicznej. Atak trwający przez niemal poł roku dotknął 46 instytucji finansowych (m.in. Bank of America, JPMorgan czy NASDAQ). Pomimo swojej prostoty, wyrządził on szkody wyceniane na dziesiątki milionów dolarów. Odpowiedzialna za atak grupa *Izz ad-Din al-Qassam Cyber Fighters* utrzymywała, że powodem był antymuzułmański film zamieszczony w serwisie *YouTube*. Eksperci w dziedzinie cyberbezpieczeństwa oraz służby wywiadowcze są jednak zgodni, że był to odwet za *Stuxnet*. Odwet dość udany, biorąc pod uwagę stosunek kosztu do wyrządzonych zniszczeń.

Irański atak DDoS dotknął 46 instytucji finansowych (m.in. Bank of America, JPMorgan czy NASDAQ). Pomimo swojej prostoty, wyrządził on szkody wyceniane na dziesiątki milionów dolarów..

Iran otrzymał kolejny cios w 2012 roku. Złośliwe oprogramowanie *Wiper*, uderzyło głównie w sektor produkcji ropy w Iranie, nieodwracalnie kasując dane z tysięcy maszyn w pierwszym kwartale 2012, co przyczyniło się do podjęcia decyzji o odłączeniu wielu systemów od sieci internetowej[12]. Dane usunięte przez malware przepadły na zawsze, tak samo jak informacja o jego autorach.. Firma Kaspersky, próbowała powiązać kod *Wipera* ze *Stuxnetem*[13] jednak oficjalnie nikt nie przyznał się do finansowania tej operacji.

W wyniku ataku wirusa Shamoon Saudi Aramco straciło ponad 30.000 komputerów, wszystkie kluczowe systemy i dane.

Podobnie nieznani są autorzy wirusa *Shamoon*, ktory kilka miesięcy po ataku *Wipera* sparaliżował działalność globalnego lidera w produkcji

10. Countdown To Zero Day, 2015, Kim Zetter
11. www.ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf
12. www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html
13. www.wired.com/2012/08/wiper-possible-origins/

ŹRÓDŁO: PEXELS/MATI MANGO

ropy - Saudi Aramco. Ślady wskazują na Iran[14], który miał oczywisty powód do zaatakowania sojusznika Stanów Zjednoczonych. Saudi Aramco straciło ponad 30.000 komputerów, wszystkie kluczowe systemy i dane. Sytuacja była na tyle poważna, że aby zapewnić ciągłość dostaw zdecydowano się na wysyłanie ropy bez procesowania dokumentów finansowych, licząc na uczciwość kontrahentów. Polityczny powód ataku było dosłownie widać gołym okiem. 15 sierpnia 2012 roku 50.000 pracowników firmy świętowało jedno z najważniejszych wydarzeń w kulturze muzułmańskiej - Noc Przeznaczenia. Pod nieobecność załogi *Shamoon* przystąpił do operacji kasowania danych z dysków twardych, na każdym z nich pierwsze 1024 bajty zostały nadpisane plikiem graficznym przedstawiającym płonącą amerykańską flagę. Oprócz Saudi Aramco w ataku ucierpiały także systemy katarskiego RasGas, producenta i eksportera ciekłego gazu ziemnego. Efekt ataku odczuwalny był na zupełnie innym rynku. Saudi Aramco chcąc przywrócić operacyjność systemów natychmiastowo zamówiło u producentów sprzętu komputerowego dziesiątki tysięcy dysków twardych, co w połączniu z ówczesnymi powodziami w Azji odbiło się na globalnej dostępności i cenach tych podzespołów.

W 2017 roku pojawiła się nowa wersja wirusa *Shamoon*, tym razem niemal doprowadzając do eksplozji w saudyjskiej rafinerii. Wzmożona aktywność Iranu w cyberprzestrzeni obrała za cel nie tylko sojuszników, ale też bezpośrednio Stany Zjednoczone. Dzień po tym jak Prezydent Donald Trump podjął decyzję o wycofaniu się z porozumienia nuklearnego z Iranem (JCPOA) sieć wypełniła się od phishingowych maili, którymi Irańscy hakerzy próbowali zwabić ofiary powiązane z administracją rządową i wszelkimi innymi instytucjami w USA[15]. W zdecydowanej części Amerykanom udało się obronić przed atakami, jednak nie przed wszystkimi[16]. Urzędy w Atlancie zainfekowane przez ransomware

14. www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/
15. www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html
16. www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1

irańskiego pochodzenia przez wiele dni nie były w stanie świadczyć usług. Dwóch irańskich hakerów zostało oskarżonych o atak, a jego skutki wyceniono na 17 milionów dolarów. Podobna historia miała miejsce w Baltimore w maju 2019, w tym przypadku koszt wyniósł 6 milionów. Według Microsoftu w latach 2017-2019 Irańskie cyberoperacje obrały za cel ponad 200 firm i instytucji w Stanach Zjednoczonych.

Siły amerykańskie nie pozostawały dłużne i realizowały własne cyberoperacje w Iranie. O większości z nich zapewne jeszcze przez dłuższy czas opinia publiczna się nie dowie, jednak wielokrotnie pojawiały się informacje na temat zakłóceń pracy systemów infrastruktury krytycznej w Iranie, jak chociażby wspomniany wypadek w Natanz z lipca 2020 roku[17]. Warto wspomnieć, że do walki po stronie USA włączyli się też cywilni aktywiści. W 2018 roku kilka tysięcy urządzeń w Iranie wyświetliło flagę Stanów Zjednoczonych z napisem „Nie mieszajcie się w nasze wybory!". Było to działanie nieznanej grupy, która wykorzystując luki w oprogramowaniu routerów[18] zostawiła tę informację nie tylko w Iranie, ale także m.in. na tysiącach maszyn w Chinach.

Wojna Hybrydowa

Potyczki w cybernetyczne, w których biorą udział USA, Chiny, Korea Północna czy Iran, ograniczają się w większości wyłącznie do cyberprzestrzeni. Oczywiście każdy ze wspomnianych ataków ma swoje konsekwencje polityczne i wpływa w różnym stopniu na gospodarkę i nastroje społeczne ofiary ataku. Największe zagrożenie niosą jednak ataki hybrydowe. Przekonali się o tym sąsiedzi Rosji.

Atak DDoS na Estonię w 2007 roku, o który podejrzewa się stronę rosyjską, był pierwszym atakiem cybernetycznym wymierzonym w cały kraj[19]. Owszem, sparaliżował wszystkie kluczowe systemy telekomunikacyjne w kraju, które przez 22 dni były praktycznie niedostępne, jednak po tym czasie konflikt został zakończony i ład w kraju przywrócony.

Mniej szczęścia mieli Gruzini. W 2008 roku „pierwszy raz, w międzynarodowym konflikcie zbrojnym wystąpił skoordynowany komponent cybernetyczny. Pomimo oczywistych powiązań, istnieją tylko poszlaki, że Federacja Rosyjska była w zaangażowana w atak"[20]. 8 sierpnia wojska rosyjskie przekroczyły granicę z Gruzją. W tym samym czasie rozpoczął się atak DDoS, który podobnie jak rok wcześniej w Estonii sparaliżował systemy telekomunikacyjne. Atak spowodował niemal całkowitą utratę zdolności rządu gruzińskiego do komunikowania się z ludnością i wojskiem. Brak dostępu do informacji wywołał panikę wśród mieszkańców Tbilisi, zwłaszcza po tym, jak pojawiły się operacje dezinforma-

Atak DDoS na Estonię w 2007 roku, o który podejrzewa się stronę rosyjską, był pierwszym atakiem cybernetycznym wymierzonym w cały kraj.

17. www.forbes.com/sites/kateoflahertyuk/2020/07/03/iran-nuclear-facility-explosion-accident-sabotage-or-cyber-attack/
18. www.reuters.com/article/US-iran-cyber-hackers/iran-hit-by-global-cyber-attack-that-left-u-s-flag-on-screens-idUSKBN1HE0MH
19. www.warsawinstitute.org/russia-strengthened-natos-cyber-defence/
20. Participants in Conflict: Cyber Warriors, Patriotic Hackers and the Laws of War", 2013, Heather Dinniss

ŹRÓDŁO: PEXELS/TIMA MIROSHNICHENKO

cyjne dotyczące wojsk rosyjskich wkraczających do stolicy Gruzji. Analitycy są zgodni co do tego, że serwery C&C (*command and control*) koordynujące atak DDoS znajdowały się w Rosji. Przynajmniej część infrastruktury należała do najemnych cyberprzestępców porozumiewających się przy użyciu rosyjskich forów hakerskich.

Cztery dni po przekroczeniu granicy przez rosyjskie wojska ówczesny prezydent Rosji Miedwiediew oświadczył, że cele rosyjskiej operacji wojskowej zostały osiągnięte. 15 sierpnia oba kraje podpisały porozumienie pokojowe, a wojna hybrydowa trwała 5 dni.

Prawdziwa siła cyberoperacji w wojnie hybrydowej została sprawdzona podczas konfliktu Rosji z Ukrainą. To właśnie na Ukrainie swoje zdolności operacyjne ujawniły grupy takie jak *Fancy Bear*[21], *Cozy Bear* i *Sandworm* (autorzy *NotPetya* - najbardziej niszczycielskiego jak dotąd cyberataku) oraz hakerzy innych rządowych i pozarządowych organizacji testujących swoje możliwości w krajowych systemach i sieciach Ukrainy.

Prawdziwa siła cyberoperacji w wojnie hybrydowej została sprawdzona podczas konfliktu Rosji z Ukrainą.

Konflikt miedzy Rosją i Ukrainą rozpoczął się w lutym 2014 roku. W tym samym czasie analitycy firmy F-Secure natknęli się na zmodyfikowane wersję złośliwego oprogramowania o nazwie *BlackEnergy*. Do tej pory malware ten pomagał cyberprzestępcom w dystrybucji spamu, przestępstwach bankowych czy atakach DDoS. Nowa wersja pozwalała na użycie pluginów, które wzbogacały możliwość oprogramowania. Zostało ono natychmiastowo użyte przeciw wielu celom w Polsce oraz Ukrainie[22].

21. www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

22. www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

WHO'S WHO IN RUSSIAN CYBER ESPIONAGE?

CYBER CRIMINALS AND HACKTIVISTS

FSO

Federal Protective Service of the Russian Federation

FSB

Federal Security Service of the Russian Federation

SVR

Foreign Intelligence Service of the Russian Federation

GRU

Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation

SPETSSVJAZ

The FSO's Spetssvyaz sub-unit organizes national government and military communications and ensures the security of the data transmitted along these channels.

16th CENTRE

18th CENTRE

The 16th Centre is the FSBs's main signals and cyber intelligence unit. The cyber operations of the FSB's 18th Centre may have targets outside state borders.

In the cyber sphere, the SVR's activity level and capabilities are not comparable to the other Russian special services, but the SVR is engaged in developing its cyber capability.

6th DIRECTORATE

From the Russian territory, the GRU actively carries out signals and cyber intelligence around the world, possessing the best technological capability among all Russian special services.

TURLA
Snake/Uroburos

APT29
The Dukes/Cozy Bear

APT28
Sofacy/Fancy Bear

APT – or ***Advanced Persistent Threat*** – carefully targeted, long term cyber operations in the course of which attackers combine multiple techniques to obtain the needed information about the target.

ŹRÓDŁO: INTERNATIONAL SECURITY AND ESTONIA 2018, ESTONIAN FOREIGN INTELLIGENCE SERVICE

BlackEnergy został użyty jako backdoor do dostarczania destrukcyjnego komponentu *KillDisk* w atakach na ukraińskie media informacyjne i przemysł elektroenergetyczny. 23 grudnia 2015 doszło do skoordynowanego ataku na regionalne sieci dystrybucji energii elektrycznej. Pojawiły się liczne przerwy w dostawie prądu na całym niemal terytorium Ukrainy. Ponad 50 stacji elektroenergetycznych zostało wyłączonych w wyniku cyberataku. Rok później, na dwa dni przed świętami, rosyjscy hakerzy uderzyli ponownie. Zaatakowana została infrastruktura narodowego operatora sieci energetycznej, w Kijowie zgasło światło. Operatorom udało się przywrócić operacyjność systemu po niespełna godzinie. Mieli dużo szczęścia. Kilka lat po incydencie okazało się że użyty w ataku malware posiadał funkcje podobne do *Stuxneta*. Mógł on zaatakować komponenty systemu ICS (Industrial Controll System) nieodwracalnie niszcząc fizyczne urządzenia, co doprowadziłoby do awarii na znacznie większą skale. Eksperci oceniają, że przywrócenie systemów po awarii, do której całe szczęście nie doszło, mogłoby trwać wiele tygodni, albo nawet miesięcy. Nie jest jasne, czy operacja ofensywna nie powiodła się, czy też po prostu strona atakująca oszczędziła systemy ukraińskie dając jasno do zrozumienia, że jest w stanie je zniszczyć, kiedy tylko zapragnie[23]. Innym przykładem użycia cyberbroni podczas tego konfliktu było wykorzystanie malware biorącego za cel telefony z systemem operacyjnym *Android*. Rosyjska grupa *Fancy Bear*[24] zaprojektowała oprogramowanie, które śledziło lokalizację użytkowników zainfekowanych urządzeń. Попр-Д30.apk przechwytywał listę kontaktów, SMSy, logi połączeń oraz lokalizację urządzenia. Wiele źródeł przypisywało temu złośliwemu oprogramowaniu odpowiedzialność za precyzyjne uderzenia strony rosyjskiej w stanowiska ukraińskiej artylerii. Malware miał rzekomo zdradzać pozycję żołnierzy ukraińskiej 24 i 72 brygady zmechanizowanej. Analitycy firmy *Crowdstrike* wykazali, że malware nie mógł być jedynym źródłem informacji o lokalizacji stanowiska artyleryjskiego. Najprawdopodobniej było ono potwierdzane przez wykorzystywane w konflikcie urządzenia UAV (*unmanned aerial vehicle*).

Obrona

Zapobieganie atakom, nawet tym najbardziej wyrafinowanym, jest możliwe. Wiele firm i rządów w ostatnich latach dokonało ogromnych inwestycji w systemy bezpieczeństwa. Nic dziwnego - analitycy z „Cyber Defense Magazine" przewidzieli w 2019 roku, że skumulowany roczny koszt związany z cyberatakami w 2020 roku wyniesie 6 bilionów dolarów[25]. Dziś wiemy, że się pomylili – koszty będą większe.

W budżetach armii wielu krajów z roku na rok coraz większe kwoty przeznaczane są na jednostki operujące w cyberprzestrzeni. W 2017 roku USA przeznaczyły 6.7 miliardów dolarów na ten cel, w 2019 było to już 8.5 miliarda dolarów. Dla

W 2017 roku USA przeznaczyły 6.7 miliardów dolarów na cyberobronność, w 2019 było to już 8.5 miliarda dolarów.

23. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, 2019, Andy Greenberg
24. www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf
25. www.cybersecurityventures.com/cybersecurity-market-report/

porównania całkowity budżet, którym dysponowało polskie ministerstwo obrony narodowej w 2019 wynosił niespełna 45 miliardów złotych (12 mld USD). Kierownictwa wszystkich armii na świecie widzą potrzebę edukacji kadr w tym obszarze. Szkolenia trwają na każdym szczeblu, czego potwierdzeniem jest fakt, że w 2020 r. w budżecie polskiego resortu obrony narodowej na realizację programu „CYBER.MIL z Klasą" zaplanowano blisko 3,5 mln złotych (1 mln USD). Program ten ma na celu uzbrojenie kandydatów do pracy w instytucjach państwowych oraz Wojskach Obrony Cyberprzestrzeni w wiedzę z zakresu kryptografii, zarządzania bezpieczeństwem informacji i innych dziedzin związanych z cyberbezpieczeństwem[26].

Pieniądze to nie jedyny problem branży. Wiele organizacji, zaczęło tworzyć profesjonalne zespoły bezpieczeństwa IT oraz zespoły reagowania kryzysowego. Niestety, zasoby kadrowe są mocno ograniczone i to nie tylko w Polsce. Szacuje się, że obecnie na świecie brakuje około 3.5 miliona osób z wiedzą oraz doświadczeniem w dziedzinie cyberbezpieczeństwa.

Nie ulega wątpliwości, że wraz ze wzrostem digitalizacji i postępu technologicznego w nadchodzących latach, znaczenie cyberprzestrzeni w życiu jednostek, społeczeństw, państw czy biznesu będzie coraz większe. Jest to jednak sfera, która dla tradycyjnego pojęcia obronności, z uwagi chociażby na mgliście określone granice, wciąż pozostaję nie w pełni unormowana. Niemniej, skuteczne zabezpieczenie krajowej infrastruktury krytycznej oraz obywateli przed zagrożeniami płynącymi z cyberprzestrzeni

Skuteczne zabezpieczenie krajowej infrastruktury krytycznej oraz obywateli przed zagrożeniami płynącymi z cyberprzestrzeni powinno stanowić taki sam priorytet, jak zabezpieczenie fizycznych granic lądowych, morskich czy przestrzeni powietrznej.

powinno stanowić taki sam priorytet, jak zabezpieczenie fizycznych granic lądowych, morskich czy przestrzeni powietrznej. Jak pokazano na przytoczonym przykładzie Iranu, umiejętności projekcji siły na tym stosunkowo nowym polu walki rządzi się odmiennymi prawami, a podmioty, które w konwencjonalnym starciu ze znacznie silniejszym i bogatszym przeciwnikiem byłyby bez szans, za sprawą cyberataków mogą dokonać znacznych szkód. Co nie zmienia faktu, że największe potęgi już dawno osiągnęły dużą przewagę w tym aspekcie. Z czasem ten typ prowadzenia działań wojennych może stać się dominującym i mającym największe przełożenie na globalny układ sił. Decydenci oraz osoby odpowiedzialne za bezpieczeństwo coraz bardziej zdają sobie z tego sprawę, jednak zarówno braki wystarczającej liczby specjalistycznych kadr, jak i sama natura cyberprzestrzeni sprawiają, że jeszcze długo państwa jedynie połowicznie będą w stanie ją kontrolować.

Autor: Wiktor Sędkowski

Wiktor Sędkowski ukończył teleinformatykę na Politechnice Wrocławskiej, specjalizując się w dziedzinie bezpieczeństwa cybernetycznego. Jest ekspertem od zagrożeń cyfrowych. Posiadacz certyfikatu CISSP, OSCP i MCTS, pracował jako inżynier i solution architect dla wiodących firm informatycznych.

26. www.rp.pl/Sluzby-mundurowe/301069964-MON-tworzy-zaplecze-dla-Wojsk-Obrony-Cyberprzestrzeni.html

Warsaw Institute
ul. Wilcza 9, 00-538 Warszawa, Polska
+48 22 417 63 15
office@warsawinstitute.org