FAE Policy Paper
nr 20/2016

Piotr ZIELNIAK

Zdolności ofensywne USA w cyberprzestrzeni

Stany Zjednoczone posiadają najbardziej zaawansowane zdolności ofensywne w środowisku wirtualnym. Amerykańscy hakerzy wykonali wiele operacji z użyciem ataków cyfrowych na całym świecie wymierzonych w różnego rodzaju cele. Biorąc pod uwagę coraz większe zagrożenie w świecie wirtualnym, można z dużą dozą pewności stwierdzić, że Stany Zjednoczone częściej będą sięgały po cyberataki w swoim arsenale.

Historia

Pierwszym, najbardziej znanym incydentem użycia ofensywnych zdolności Stanów Zjednoczonych są lata 80. XX wieku. Amerykanie przy pomocy złośliwego oprogramowania zainstalowanego w mechanizmie kontrolującym pracę gazociągów, doprowadzali do wybuchu na Syberii. Historia ta została jednak opisana tylko w jednej książce – wspomnieniach jednego z oficerów CIA i podważona m.in. przez profesora *King's College* Thomasa Rida. Wydaje się, że ma on rację, w tamtych czasach trudno było o stworzenie zaawansowanego programu wpływającego na działanie elementów infrastruktury krytycznej. Pierwszy złośliwy program – robak Morris – pojawił się dopiero kilka lat później.

Po zakończeniu Zimnej Wojny pojawiły się informacje o wykorzystaniu ofensywnego potencjału w cyberprzestrzeni za czasów George H. W. Busha. Miało mieć to miejsce podczas pierwszej wojny w Zatoce Perskiej (1990-91). Komputery wspomagały główne działania, ale planowano także wykorzystanie ich w celach ofensywnych. Jednym z pomysłów było wysłanie oddziałów specjalnych wraz z hakerami do Iraku z zadaniem włamania się do lokalnych sieci i zainstalowania złośliwego oprogramowania. Głównodowodzący wojskami koalicji generał Norman Schwarzkopf uznał jednak, że misja jest zbyt ryzykowana i grozi pojmaniem amerykańskich żołnierzy, dlatego nie wyraził na nią zgody.

Pojawiły się również informacje, że Amerykanie mieli sprzedać Irakijczykom drukarki z wmontowanym złośliwym oprogramowaniem stworzonym przez NSA. Tzw. „bomby logiczne" miały się uaktywnić i uszkodzić odpowiednie monitory i drukarki, znacznie utrudniając komunikację i dostęp do informacji. Wydaje się jednak, że była to mistyfikacja. W tamtym czasie technologia informacyjna była dopiero w początkowej fazie rozwoju i przygotowanie tak skomplikowanej operacji wykraczało poza możliwości jakiegokolwiek państwa na świecie. Ponadto należy zauważyć, że w siłach zbrojnych USA nie rozwinięto koncepcji doktrynalnych

ani również nie wyznaczono odpowiedniej instytucji odpowiedzialnej za działania w środowisku wirtualnym. Nie stworzono mechanizmu procesu podejmowania decyzji oraz nie odpowiedziano na pytanie o zgodność takich operacji z obowiązującym prawem konfliktów zbrojnych. Dlatego wydaje się, że atak na irackie drukarki nie miał miejsca.

Podobne informacje pojawiły się przy okazji wojny w Kosowie w 1999 roku. Amerykanie mieli rzekomo przeprowadzić zaawansowane operacje w cyberprzestrzeni wymierzone w obronę przeciwlotniczą przeciwnika, ataki na konta bankowe należące do Miloszevicia oraz włamanie do serbskich baz danych. Po raz kolejny wydaje się, że niewielkie jest prawdopodobieństwo, że omawiane operacje miały jednak miejsce. W tamtym czasie Serbia posiadała bardzo słabo rozwinięta infrastrukturę informacyjną, a wojsko nie używało internetu do komunikacji. Ponadto, w początkowej fazie operacji, NATO wskazało, że celem wojny informacyjnej są przede wszystkim radary i stacje przekaźnikowe, a nie podłączone do sieci komputery. Trzecim argumentem jest fakt, że cyberataki były praktycznie nierozwinięte zarówno w doktrynie wojskowej Stanów Zjednoczonych, jak i NATO. Nie stworzono również żadnej opinii prawnej dotyczącej sposobu działania, co wzbudzało obawę wśród dowódców wojskowych, że mogą oni zostać pociągnięci do odpowiedzialności karnej.

W latach 90. ub. wieku mówiono wiele o potencjalnych atakach cyfrowych, ale nie miały one miejsca. Jedynie NSA za pomocą utworzonego w 1997 roku zespołu Tailored Access Operation prowadziło działania szpiegowskie, włamując się do sieci i systemów wrogich państw. Nie są jednak znane żadne szczegóły na ten temat.

Wojsko traktowało ataki cyfrowe jako część wojny informacyjnej i operacji informacyjnych, która miała wspierać działania jednostek konwencjonalnych. Brakowało dokumentów strategicznych oraz jednostek gotowych do przeprowadzenia autonomicznych cyberataków, dlatego większość informacji o potencjalnych atakach cyfrowych w latach 90. nie jest prawdziwa.

Pierwsze ofensywne kroki Stanów Zjednoczonych w cyberświecie

Sytuacja uległa zmianie za czasów administracji prezydenta George W. Busha. W 2002 roku weszła w życie prezydencka dyrektywa nr 16 nosząca nazwę „Wytyczne dla prowadzenia ofensywnych operacji w cyberprzestrzeni" (*To Develop Guidlines for Offensive Cyber-*

Warfare). Treść dyrektywy do dzisiaj pozostaje tajna. Tworząc ten dokument wzorowano się na doktrynach strategicznych użycia broni jądrowej, a podczas pracy nad nią pojawiło się wiele problemów. Część osób zaangażowanych w ten proces podważała sens przeprowadzania cyberataków, wskazując na wysokie ryzyko zniszczenia obiektów cywilnych. Zneutralizowanie sieci energetycznych mogło prowadzić do paraliżu wrogiej bazy wojskowej, ale również szpitali czy innych obiektów cywilnych, co oznaczałoby złamanie prawa międzynarodowego. Wykorzystanie cyberataków stanowiło generalnie element tzw. Doktryny Rumsfelda, zakładającej, że nowoczesne siły zbrojne wyposażone w najbardziej zaawansowaną technologię, będą w stanie pokonać każdego adwersarza, gdziekolwiek się znajduje.

W 2003 roku wraz z inwazją na Irak rozważano zastosowanie ataków cyfrowych przeciwko kontom bankowym Saddama Husajna i irackiemu systemowi finansowemu. Zrezygnowano z niej obawiając się, że efekty mogą nie być ograniczone tylko do Iraku i doprowadzić do międzynarodowego chaosu gospodarczego oraz naruszyć obowiązujące prawo, w końcu banki są instytucjami cywilnymi. Nie oznacza to jednak, że Stany Zjednoczone zrezygnowały z jakichkolwiek działań wymierzonych w reżim Saddama Husajna. Włamano się do irackich sieci wojskowych i rozesłano wiadomości poczty elektronicznej z komunikatem o zbliżającej się inwazji i wezwaniu do poddania się. Wielu dowódców podążyło za tymi wskazówkami i złożyło broń przed nacierającym amerykańskim wojskiem.

Amerykańskie siły zbrojne przygotowywały się do kontynuowania działań w środowisku wirtualnym. W tym celu powstała koncepcja programu Suter, którego głównym zadaniem było atakowanie systemów komputerowych i sieci należących do przeciwnika, w szczególności odpowiedzialnych za obronę przeciwlotniczą. Niewiele jednak wiadomo na temat tego programu i jego bojowego użycia.

W 2008 roku, doszło do kolejnych cyberataków, przeprowadzonych za kadencji George W. Busha. Miały one odbywać się na obszarze Iraku, który przez prezydenta Busha został określony strefą wojny. Utworzono specjalny zespół zadaniowy, złożony z przedstawicieli Departamentu Obrony i Departamentu Sprawiedliwości oraz agencji wywiadowczych. Operacje polegały na atakach DDoS skierowanych na przeciążenia serwerów, na których znajdowały się strony internetowe Al-Kaidy, ale również tworzenie fałszywych stron internetowych, podszywających się pod witryny dżihadystów. Udało się również wielokrotnie złamać

zabezpieczenia sieci i systemów komputerowych używanych przez terrorystów i rozpowszechnić fałszywe wiadomości.

Specyficzny obrót przybrała operacja przeprowadzona wraz z saudyjskim wywiadem przeciwko stronie i forum używanym do rekrutacji terrorystów. Stany Zjednoczone i Arabia Saudyjska stworzyły internetowy punkt rekrutacyjny dla terrorystów, którzy byli monitorowani przez służby obu państw. Jednak forum stało się zbyt popularne, przez co liczba rekrutów stale się zwiększała, a ujęcie ich wszystkich było niemożliwe. Stanowili oni coraz większe zagrożenie dla amerykańskich żołnierzy, dlatego postanowiono o jej unieszkodliwieniu. W tym celu utworzono grupę złożoną z przedstawicieli Departamentu Obrony, CIA, Departamentu Sprawiedliwości, Biura Dyrektora Wywiadu oraz NSA. Pomimo sprzeciwu CIA strona została wyłączona, a do tego zadania została wyznaczona NSA. Przypadkowo jednak wyłączono również 300 serwerów w Arabii Saudyjskiej, Niemczech i Teksasie. Był to przykład na to, że operacje w środowisku wirtualnym mogą być bardzo nieprecyzyjne. Incydent ten wywołał również konflikt w środowisku wywiadowczym pomiędzy CIA oraz NSA i doprowadził do napięć w stosunkach z wywiadem Arabii Saudyjskiej.

Omawiając amerykańskie zdolności w cyberprzestrzeni, nie można nie wspomnieć o tzw. patriotycznych hakerach, którzy są głównie kojarzeni z Chinami i Rosją, ale występują też w Stanach Zjednoczonych. Brali oni udział w cyberpotyczce z chińskimi odpowiednikami w 2001 roku po kolizji amerykańskiego i chińskiego samolotu. Dwa lata później zabrakło ich wsparcia w kampanii skierowanej przeciwko Irakowi. Powodem ich absencji było oficjalne ostrzeżenie wystosowane przez władze amerykańskie, że jakiekolwiek operacje skierowane przeciwko irackim systemom komputerowym będą traktowane jako nielegalne i atakujących spotka kara przewidziana w amerykańskim prawie. Na tym właśnie polegała różnica w podejściu prezentowanym przez rząd Stanów Zjednoczonych a Chin i Rosji, gdzie władze tych dwóch państw aktywnie zachęcały swoich „patriotycznych hakerów" do przeprowadzania ataków.

Operacja „Igrzyska Olimpijskie" (*Olympic Game)*

Rosnące zagrożenie ze strony Iranu, który podejrzewano o rozwój własnego programu nuklearnego, zaniepokoiło polityków w Stanach Zjednoczonych i Izraelu. W szczególności, że

w 2005 roku prezydentem Iranu został Mahmud Ahmadineżad, słynący z agresywnych wypowiedzi m.in. pod adresem Izraela, wielokrotnie nawołujący do jego zniszczenia. Waszyngton i Tel Awiw podejrzewały, że Irańczycy potajemnie rozwijają swój arsenał nuklearny i zdecydowali się działać.

Wprowadzono w życie nowatorski plan, który polegał na wykorzystaniu nowoczesnego programu komputerowego do zniszczenia wirówek wzbogacania uranu typu IR-1, poprzez spowolnienie lub przyspieszenie ich działania. Celem operacji było nie tylko dokonanie fizycznych zniszczeń, ale również zasianie niepewności wśród irańskich inżynierów, a także podważenie ich kompetencji. Głównym problemem było dostarczenie złośliwego oprogramowania do celu – czyli ośrodka wzbogacania uranu w Natanz, którego sieci i systemy został zbudowane w technologii *air-gap*. W końcu i ten problem udało się przezwyciężyć i dostarczyć złośliwe oprogramowanie przy pomocy przenośnych dysków pamięci. Operacja była kontynuowana przez administrację Baracka Obamy.

Czas cyberataków

Prezydent Barack Obama bardzo szybko dostrzegł znaczenie cyberbezpieczeństwa. Jako pierwszy amerykański przywódca poświęcił przemówienie temu problemowi, co mogło wskazywać, że obszar ten będzie odgrywał istotną rolę. Przed odniesieniem się do konkretnych ataków warto wspomnieć, że Barack Obama podpisał tajną dyrektywę PPD-20 wprowadzającą zasady przeprowadzania operacji ofensywnych w cyberprzestrzeni. Zastąpiła ona dokument podpisany przez prezydenta Busha. Jej treść została ujawniona przez Edwarda Snowdena.

PPD-20 wyodrębniła szereg rodzajów operacji. W ramach obrony infrastruktury informacyjnej Stanów Zjednoczonych wymieniono operacje obronne w cyberprzestrzeni (*Defensive Cyber Effects Operations* – DCEO) oraz nieinwazyjne operacje obronne w cyberprzestrzeni (*Nonintrusive Defensive Countermeasures* – NDCM). Ich głównym zadaniem była ochrona Stanów Zjednoczonych przed spodziewanym zagrożeniem, jak również rozpoczętym już atakiem. Główna różnica między działaniami polegała na wykorzystaniu w trakcie DCEO sieci nienależących do rządu amerykańskiego, bez uzyskania zgody ich właścicieli. Ten typ operacji umożliwiał manipulowanie, zakłócanie, wyłączanie a nawet niszczenie elementów wchodzących w skład infrastruktury informacyjnej. PPD-20 wyodrębniła

również operacje polegające na zbieraniu informacji (*Cyber Collection*) poprzez uzyskanie nieautoryzowanego dostępu do infrastruktury informacyjnej przeciwnika. Zakładano, że wykonujący te operacje zostaną niewykryci. Dyrektywa obszernie opisywała operacje ofensywne w cyberprzestrzeni (*Offensive Cyber Effects Operations* – OCEO). Rozumiane były w bardzo szeroki sposób i obejmowały wszystkie operacje poza DCEO, NDCM, Cyber Collection, przeprowadzone z zamiarem wywołania efektów poza sieciami należącymi do amerykańskiego rządu. Wyraźnie zaakcentowano, że wszystkie operacje ofensywne muszą być wykonywane zgodnie z prawem międzynarodowym, co potwierdza stanowisko Stanów Zjednoczonych.

Odchodzący prezydent George W. Bush poinformował swojego następcę o operacji „Igrzyska Olimpijskie" podczas jednego ze spotkań. Barack Obama entuzjastycznie podszedł do tego programu i zgodził się kontynuować kampanię. Co więcej, zwiększył on częstotliwość ataków i w przeciwieństwie do swojego poprzednika planował doprowadzić do powstania poważnych zniszczeń w krótkim okresie czasu. Zdecydowano się umieścić o wiele bardziej niszczycielską wersję oprogramowania w sieciach ośrodka Natanz. W latach 2009-2010 udało się zniszczyć 1 tys. wirówek, co stanowiło 20% wszystkich wykorzystywanych w tym miejscu. Irańczycy bardzo szybko zastąpili je nowymi, zdecydowanie bardziej wydajnymi.

W 2010 roku operacja musiała zostać zakończona, ponieważ robak Stuxnet przez przypadek został wypuszczony do Internetu, gdzie wykryła i zbadała go białoruska firma zajmująca się złośliwym oprogramowaniem. W ten sposób został on zdemaskowany i w momencie jego odkrycia ogłoszony najbardziej zaawansowanym złośliwym oprogramowaniem w historii. Jako pierwszy wykorzystywał wiele podatności *zero day*, podczas gdy inne programy korzystały z maksymalnie jednej. Wykorzystanie Stuxnetu było przełomowym wydarzeniem w dziejach działań w cyberprzestrzeni, stanowiąc pierwszy przypadek, kiedy program komputerowy był zdolny do zniszczenia przedmiotów fizycznych. Pokazywał, że broń cyfrowa może w przyszłość zastąpić siłę militarną, a państwa myślące o swoim bezpieczeństwu muszą coraz poważniej brać pod uwagę cyberbezpieczeństwo. Trudno jest oszacować efekt użycia programu Stuxnet – część ekspertów uważa, że faktycznie przyczynił się do spowolnienia pracy nad wzbogacaniem uranu, podczas gdy inni uważają, że nie miał większego wpływu, ponieważ

głównie niszczył stare wirówki, które bardzo szybko były zastępowane przez nowsze, usprawnione wersje.

Stuxnet rodził również konsekwencje prawne. W końcu atak na obiekt cywilny, jakim był ośrodek w Natanz, stanowił złamanie prawa konfliktów zbrojnych. Wcześniej Stany Zjednoczone przeciwstawiały się uchwaleniu nowego traktatu międzynarodowego regulującego działania w cyberprzestrzeni argumentując, że obowiązuje normy mają również zastosowanie w środowisku wirtualnym. Stuxnet uwydatnił hipokryzje Stanów Zjednoczonych w tym obszarze.

Nie był to jedyny element kampanii cyberataków wymierzonych w Iran. W 2009 roku Obama zlecił stworzenie szerszego planu ataków, który został nazwany „Nitro Zeus". Obejmował on wyłączenie irańskiej obrony przeciwlotniczej, sparaliżowanie systemów komunikacyjnych oraz kluczowych elementów sieci energetycznych. W jego realizację zaangażowano tysiące osób ze społeczności wywiadowczej oraz wojskowych. Dodatkowo wydano miliony dolarów na wprowadzenie złośliwego oprogramowania do irańskich sieci, które mogłyby zostać uruchomione w dowolnym momencie. Szczególnym zainteresowaniem cieszył się ośrodek wzbogacania uranu w Fordo, który był uważany za jeden z najtrudniejszych celów ewentualnego ataku zbrojnego. Przy planowaniu ataku cyfrowego, postanowiono powtórzyć schemat znany z ataku na ośrodek w Natanz. „Nitro Zeus" miała służyć jako opcja awaryjna na wypadek niepowodzenia negocjacji z Iranem. W końcu jednak przedstawiciele reżimu ajatollahów przystali na zachodnie warunki i zgodzili się na zredukowanie o 2/3 liczby wirówek w ośrodku Fordo, dlatego też prezydent Obama zdecydował o odwołaniu całej operacji.

Nie był to jednak koniec kampanii w cyberprzestrzeni. Stany Zjednoczone kontynuowały działania w środowisku wirtualnym skupiając się jednak bardziej na działaniach szpiegowskich. Szybko stworzono do tego odpowiednie narzędzia. Pierwszym z nich był robak Duqu, odkryty w 2011 roku przez naukowców z uniwersytetu w Budapeszcie. Według ekspertów z branży IT miał on zostać stworzony przez tych samych autorów, co Stuxnet, ale w odróżnieniu od swojego protoplasty nie powodował zniszczeń fizycznych, tylko zajmował się zbieraniem informacji na temat systemów kontroli SCADA używanych w przemyśle. Miał on też wykradać cyfrowe certyfikaty bezpieczeństwa. Zdaniem ekspertów głównym zadaniem nowego programu było przygotowanie kolejnego ataku przeprowadzonego przez oprogramowania podobne do *Stuxnetu*.

W 2012 roku wykryto kolejne złośliwe oprogramowanie stworzone na bazie Stuxnetu. Program noszący nazwę Flame zbierał informacje z sieci i systemów telekomunikacyjnych państw Bliskiego Wschodu, głównie z Iranu. W opinii ekspertów był on jeszcze bardziej zaawansowany niż Stuxnet, a w momencie odkrycia uznano go za najbardziej złożony, złośliwy program komputerowy, jaki powstał w historii. Miał on możliwość nagrywania dźwięku, robienia zrzutów ekranu (*screenshotów*), śledzenie wpisywanych na klawiaturze znaków oraz nagrywania rozmów na Skype. Flame został wyposażony w mechanizm samodestrukcji, który został aktywowany po jego wykryciu i w ten sposób uległ on zniszczeniu. Ujawnione przez Snowdena dokumenty wskazały, że jego autorem było amerykańskie NSA i brytyjskie GCHQ. Innym odkrytym w 2012 roku, podobnym programem był *Gauss*. Jego głównym celem była kradzież haseł, głównie do kont bankowych w Libanie i Iranie. Został również stworzony przez Stany Zjednoczone i ich sojuszników.

Wszystkie programy były głównie wymierzone w Iran i miały na celu zebrać jak najwięcej informacji na temat programu nuklearnego tego państwa. Wyjątkiem był tutaj Stuxnet, który poza aktywnością szpiegowską skupiał się na niszczeniu wirówek do wzbogacania uranu w ośrodku Natanz.

„Igrzyska Olimpijskie" były najbardziej rozbudowaną operacją ofensywną w cyberprzestrzeni. Stany Zjednoczone prowadziły tam też inne działania ofensywne. Pierwszoplanową rolę odgrywała działająca w ramach NSA grupa elitarnych hakerów TAO. Głównym celem były Chiny. Zespół amerykańskich hakerów zdobył dowody na włamania dokonane przez Państwo Środka do sieci amerykańskich przedsiębiorstw zbrojeniowych, dzięki czemu wiedziano, kto jest autorem operacji szpiegowskich wymierzonych w obiekty w Stanach Zjednoczonych. Amerykanie włamali się również do sieci i systemów jednej z największych na świecie firm telekomunikacyjnych Huawei, podejrzewając że przedsiębiorstwo służy jako przykrywka do działalności szpiegowskiej. NSA spenetrowała sieci 60 placówek akademickich, w tym Pekińskiego Uniwersytetu Tsingua, uznawanego za jedną z najlepszych placówek naukowych w kraju. Amerykańskich hakerów interesowała przede wszystkich sieć edukacyjno-naukowa, gdzie zgromadzona została baza danych o milionach chińskich obywateli. Ponadto uniwersytety służą jako miejsce rekrutacji hakerów pracujących dla chińskiego rządu. Amerykanie w ten sposób chcieli poznać tożsamość swojego przeciwnika.

Nie tylko Chiny były celem amerykańskich agencji szpiegowskich. W 2010 roku włamano się do skrzynki pocztowej prezydenta Meksyku Felipe Calderóna, a następnie, wykorzystując serwis poczty elektronicznej prezydenta, uzyskano dostęp do najważniejszych informacji na temat polityki zagranicznej, gospodarki oraz sytuacji wewnętrznej w kraju. Operacja ta może dziwić, ponieważ Calderón uchodził za bliskiego sojusznika Stanów Zjednoczonych, współpracującego w walce z handlarzami narkotyków. Amerykanie chcieli mieć jednak pewność, że faktycznie jego słowa mają przełożenie na działanie oraz obawiano się też możliwego zamachu stanu. W 2012 roku podczas kampanii prezydenckiej w Meksyku śledzono również korespondencje jednego z kandydatów – Enrique Peña Nieto.

NSA nie tylko jednak szpiegowało meksykańskich polityków. Skala prowadzonych działań w cyberprzestrzeni przez tę agencję była ogromna. Jej początków nie można utożsamiać tylko i wyłącznie z kadencją Baracka Obamy, ale to właśnie za jego prezydentury osiągnęła ona największe rozmiary. Wśród operacji szpiegowskich obok opisanego PRISM, prowadzono również program „Informator bez granic" (Boundless Informant) które gromadził dane na temat wysłanych wiadomości poczty elektronicznej oraz nawiązanych połączeń telefonicznych z całego świata, m.in. z Niemiec, Brazylii, czy Francji. W ramach innych programów szpiegowano również dyplomatów ONZ i urzędników UE. NSA nie tylko gromadziła dane, ale również starała się złamać kody szyfrujące używane przy transakcjach internetowych (Project Bullrun), dążyła do zidentyfikowania użytkowników sieci TOR (Egotistical Giraffe) czy razem z Kanadą prowadziła program „Olympia", którego celem było brazylijskie Ministerstwo Górnictwa i Energetyki.

Interesujące są też działania szpiegowskie podjęte przeciwko izraelskim bezzałogowym statkom latającym. NSA i Centrali Łączności Rządowej (*Government Communications Headquarters* – GCHQ) udało się złamać szyfrowaną transmisję między nimi a stacjami naziemnymi, co umożliwiło dostęp do obrazu przesyłanego z drona. NSA zaangażowana była w wywiad gospodarczy, szpiegowanie polityków, dyplomatów, wojska oraz obywateli innych państw. Dane zbierane przez nią były również udostępniane innym agencjom wywiadowczym, przede wszystkim sojusznikom w ramach tzw. sojuszu pięciorga oczu. Działania NSA wywołały falę oburzenia na całym świecie, jednak jest ona niezrozumiała. Zadaniem agencji

wywiadowczej jest pozyskiwanie danych i nikogo nie powinno to dziwić. Szpiegowanie zawsze było przecież elementem działalności państwa na arenie międzynarodowej.

Amerykanie przeprowadzali też operacje w cyberprzestrzeni, wspierające konwencjonalne działania wojskowe. Zarówno w Iraku jak i Afganistanie, jednostki Armii i Piechoty Morskiej oraz wysłanych w teren oficerów NSA, przeprowadzały operacje wymierzone w ośrodki dowodzenia oraz centra telekomunikacyjne. Często dostarczając błędne informacje talibom udało się ich wciągnąć w pułapkę i wyeliminować. Nie były to jedyne działania podjęte w celu wsparcia jednostek walczących z wrogiem. W 2011 roku hakerzy Marynarki Wojennej USA wspomogli operację w Libii, namierzając urządzenia elektroniczne i radiowe przeciwnika, ułatwiając w ten sposób nakierowanie ataków na jego pozycję

Bardzo interesującym przypadkiem był nieudany cyberatak na systemy teleinformatyczne Korei Północnej. W latach 2009-2010 próbowano zainstalować złośliwe oprogramowanie, podobne do Stuxnetu, którego zadaniem byłoby zniszczenie wirówek odpowiedzialnych za wzbogacanie uranu. Działają one na podobnej zasadzie do tych używanych w ośrodku Natanz. Atak się jednak nie powiódł, ponieważ nie udało się dostarczyć programu do północnokoreańskich sieci. Korea Północna jest jednym z państw z najmniejszą ilością internautów i stron internetowych, a internet jest tam zarezerwowany wyłącznie dla elity. Ma to swoje pozytywne strony, czyniąc z tego państwa niezwykle trudny cel dla ataków cybernetycznych.

W 2016 roku działania ofensywne zostały również wymierzone przeciwko Państwu Islamskiemu (IS). Pierwszy raz w historii odpowiadać za nie miał United States Cyber Command (USCYBEROM), utworzone w 2011 roku dowództwo odpowiedzialne za operacje w cyberprzestrzeni. Do 2016 roku większość ataków przeprowadzana była przez NSA. Ofensywa w cyberprzestrzeni przeciwko kalifatowi napotkała jednak wiele problemów, a dowodzący USCYBERCOM admirał Mike Rogers był za nią mocno krytykowany. Było to spowodowane faktem, że Amerykanie przygotowani byli do konfrontacji z innymi państwem, a nie organizacją asymetryczną, taką jak Państwo Islamskie.

Amerykanie nie zawsze musieli osobiście przeprowadzać cyberataki. Mogli pomóc swoim sojusznikom w ich przeprowadzeniu. Mogło to mieć miejsce przy kradzieży maili doradcy prezydenta Putina, Władysława Surkowa, dokonanej przez ukraińskich hakerów.

Amerykańskie służby miały wspomóc Ukraińców swoimi zaawansowanymi zdolnościami i dzięki temu udało im się pozyskać dane.

Podsumowując

Stany Zjednoczone są niekwestionowanym mocarstwem w cyberprzestrzeni, dysponując najbardziej zaawansowanymi zdolnościami ofensywnymi w środowisku wirtualnym. Amerykańskie służby dysponują najbardziej zaawansowanym sprzętem, najstarszymi i najbardziej doświadczonymi jednostkami operującymi w świecie wirtualnym. Przeprowadziły one liczne ataki ukierunkowane na poufność danych, integralność oraz dostępność usług internetowych.

Największym atutem Amerykanów jest fakt, że większość oprogramowania i sprzętu komputerowego używanego na świecie jest właśnie produkcji amerykańskiej i jak wiemy z informacji ujawnionych przed Edwarda Snowdena służby współpracują z sektorem prywatnym, instalując tzw. tylne furtki. Służą one właśnie do przeprowadzania ataków. Biorąc jednak pod uwagę, że coraz więcej jest technologii nie amerykańskiej na rynkach światowych oraz wzrost popularności szyfrowania, coraz trudniej będzie Stanom Zjednoczonym przeprowadzać ofensywne działania, a ich siła na tym polu będzie również spadać.

Kontakt

Fundacja
Aleksandra Kwaśniewskiego
„Amicus Europae”

Aleja Przyjaciół 8/5
00-565 Warszawa

Tel. +48 22 622 66 33
Tel. +48 22 622 66 03
Fax:+48 22 629 48 16

email: fundacja@fae.pl, www.fae.pl

FAE Policy Paper nr 20/2016

Zdolności ofensywne USA w cyberprzestrzeni

Autor: Piotr Zielniak

Absolwent Uniwersytetu Warszawskiego. Niezależny dziennikarz oraz ekspert. W kręgu jego zainteresowań leżą nowe technologie, wojna informacyjna oraz polityka bezpieczeństwa Stanów Zjednoczonych Ameryki.

Nadrzędną misją **Fundacji „*Amicus Europae*”** jest popieranie integracji europejskiej, a także wspieranie procesów dialogu i pojednania, mających na celu rozwiązanie politycznych i regionalnych konfliktów w Europie.

Do najważniejszych celów Fundacji należą:

- Wspieranie wysiłków na rzecz budowy społeczeństwa obywatelskiego, państwa prawa i umocnienia wartości demokratycznych;
- Propagowanie dorobku politycznego i konstytucyjnego Rzeczypospolitej Polskiej;
- Propagowanie idei wspólnej Europy i upowszechnianie wiedzy o Unii Europejskiej;
- Rozwój Nowej Polityki Sąsiedztwa Unii Europejskiej, ze szczególnym uwzględnieniem Ukrainy i Białorusi;
- Wsparcie dla krajów aspirujących do członkostwa w organizacjach europejskich i euroatlantyckich;
- Promowanie współpracy ze Stanami Zjednoczonymi Ameryki, szczególnie w dziedzinie bezpieczeństwa międzynarodowego i rozwoju gospodarki światowej;
- Integracja mniejszości narodowych i religijnych w społeczności lokalne;
- Propagowanie wiedzy na temat wielonarodowej i kulturowej różnorodności oraz historii naszego kraju i regionu;
- Popularyzowanie idei olimpijskiej i sportu.