FAE Policy Paper
nr 18/2014

Andrzej KOZŁOWSKI

Hakerzy ajatollahów

Islamska Republika Iranu jest państwem, które stało się ofiarą najbardziej zaawansowanego ataku w cyberprzestrzeni. Spowodowało to, że irańscy decydenci, przywiązują szczególną uwagę do działań w tym nowym wymiarze, wzmacniając obronę, ale jednocześnie nie zapominają o zdolnościach ofensywnych. Iran powoli staje się jednym z głównym graczy w cyberprzestrzeni, a jego potencjał cały czas rośnie.

Bliski Wschód jest jednym z najbardziej konfliktogennych obszarów na kuli ziemskiej. Rywalizacja mocarstw, globalnych jak i regionalnych powoduje, że teren ten spłynął krwią wielokrotnie. Główna oś sporu rysuje się pomiędzy społecznością państw muzułmańskich a Izraelem, aczkolwiek nie można zapomnieć o rywalizacji między Arabią Saudyjską a Iranem oraz innych pomniejszych konfliktach. Wielowymiarowy konflikt – obejmujący regularne działania wojenne, jak i ataki terrorystyczne – bardzo szybko przeniósł się również do cyberprzestrzeni, gdzie Iran i Izrael wiodą palmę pierwszeństwa w działaniach ofensywnych i defensywnych.

Stuxnet i jego następcy

Przed długi czas Iran nie przywiązywał większej wagi do działalności w cyberprzestrzeni. Punktem zwrotnym okazał się atak z wykorzystaniem robaka *Stuxnet*. Opracowany przez amerykańskich ekspertów, we współpracy z Izraelem, ten złośliwy program zainfekował systemy ośrodka w Natanz, pozostając niewykrytym przez prawie dwa lata, aż do 2010 roku. Przez ten okres irańscy inżynierowie nie mieli pojęcia, co powoduje zniszczenia wirówek do wzbogacania uranu. W kuluarach siedziby Międzynarodowej Agencji Energii Atomowej (MAEA) w Wiedniu, coraz częściej powtarzano tezę o braku odpowiednich kwalifikacji wśród irańskich naukowców. Szacunki co do zniszczeń wywołanych przez *Stuxnet* różnią się w zależności od źródła i nie można jednoznacznie określić wpływu oprogramowania na rozwój programu nuklearnego. Zdecydowanie większe znaczenie miał efekt psychologiczny: oto po raz pierwszy w historii efekty użycia programu komputerowego nie ograniczały się do środowiska wirtualnego, ale oddziaływały na świat rzeczywisty. Uruchomiło to lawinowy napływ apokaliptycznych

scenariuszy, w których terroryści mieliby wejść w posiadanie *Stuxnetu*, przekształcić go i zaatakować infrastrukturę krytyczną Stanów Zjednoczonych. Nic takiego nie miało jednak miejsca, a scenariusz terrorystycznego wykorzystania podobnego oprogramowania wciąż się nie wydarzył.

Kolejnymi zaawansowanymi programami wymierzonymi w Iran były *Duqu* i *Flame*. Zawierały one w sobie elementy tego samego kodu, co ich słynniejszy poprzednik. Wskazuje to, że za stworzeniem obu robaków stała ta sama grupa osób. Prawdopodobnie wszystkie programy były częścią amerykańskiej tajnej operacji „Igrzyska Olimpijskie". *Duqu* i *Flame* działały jednak w inny sposób, niż *Stuxnet*. Ich głównym celem było zbieranie informacji na temat programu atomowego, irańskich polityków oraz wyszukiwanie luk w cyberobronie. Ich zaawansowana budowa i stopień skomplikowania pozwalały mu na aktywowanie mikrofonu i kamer bez wiedzy użytkownika, wykorzystanie wbudowanego aparatu fotograficznego czy przechwytywanie wszystkich informacji wprowadzanych do komputera, a *Duqu* miał nawet wbudowany mechanizm samozniszczenia w celu uniknięcia wykrycia. Za pomocą technologii bezprzewodowych i *bluetooth* przesyłano uzyskane informacje.

Flame miał pozostać w sieciach irańskich, niezauważony, przez ponad pięć lat, zbierając kluczowe informacje. Został wykryty przypadkowo przez błąd popełniony przez Izraelczyków, gdy ci wykorzystali go do nieudanego ataku wymierzonego w irański sektor naftowy. Amerykanie nie ukrywali swojej wściekłości na partnerów z Tel Awiwu, ponieważ *Flame* dostarczał niezwykle ważnych informacji. Zdaniem części ekspertów, Stany Zjednoczone już poradziły sobie z tym problemem i posiadają w irańskich sieciach zdecydowanie bardziej zaawansowane programy szpiegowskie.

Ostatnio wykrytym oprogramowanie szpiegowskim jest *Gauss*, odpowiedzialny za kradzież danych z internetowych kont bankowych. Według ekspertów z firmy komputerowej *Kasperky Lab*, swoją budową przypomina robaki *Duqu* i *Flame*. Robaki szpiegowskie mają dwa główne zadania, z jednej strony mają przygotować grunt do ataków z wykorzystaniem podobnego do *Stuxneta* oprogramowania, z drugiej monitorują stopień zaawansowania irańskiego programu nuklearnego i zbierają informacje na temat sytuacji politycznej i gospodarczej w tym kraju.

Ofensywa przeciwko Iranowi trwa nie tylko w cyberprzestrzeni, ale również uderza w jego zdolności obrony w środowisku wirtualnym, poprzez wykorzystanie klasycznych form walki. W 2013 roku zamordowany został jeden z głównych irańskich dowódców odpowiedzialnych za obronę w cyberprzestrzeni. Sytuacja była podobna do przypadków irańskich naukowców, pracujących przy programie nuklearnym, którzy zginęli w niewyjaśnionych okolicznościach. Oczywistym podejrzanym w obu przypadkach stał się dla Teheranu Izrael.

Irańska cyberdefensywa

Rozwijana dynamicznie od 2010 roku irańska cyberdefensywa miała dwa główne zadania: zapobiegnięcie powtórzenia się scenariusza z wykorzystaniem *Stuxnetu* oraz kontrolę treści w Internecie. Pierwszym krokiem dla zwiększenia zdolności obronnych było stworzenie w 2010 roku – w strukturach irańskiego Korpusu Strażników Rewolucji Islamskiej (*Pasdaran*) – specjalnej komórki do walki w cyberprzestrzeni. Liczy ona ponad 2 tysiące osób, a jej roczny budżet oscyluje na poziomie 80 milionów dolarów. Ponadto, w 2012 roku w Iranie utworzono Najwyższą Radę Cyberprzestrzeni, odpowiedzialną za bezpieczeństwo sieci i ochronę przed atakami z zewnątrz oraz za rozwój zdolności ofensywnych. Do zadań tego organu należy również zbieranie informacji na temat aktywności w Internecie wewnątrz kraju jak i na świecie. Przewodniczącym Rady jest irański prezydent Hassan Rouhani, a w jej skład wchodzą również najważniejsi przedstawiciele kręgów rządowych oraz najważniejsi dowódcy z *Pasdaran*.

Innym podmiotem odpowiedzialnym za bezpieczeństwo w cyberprzestrzeni jest Dowództwo Obrony w Cyberprzestrzeni, które wchodzi w skład Organizacji Obrony Pasywnej przy sztabie generalnym irańskich sił zbrojnych. W skład Dowództwa wchodzą przedstawiciele sił zbrojnych, wywiadu, ministerstwa obrony oraz ministerstwa komunikacji. Głównym zadaniem tego organu jest rozwijanie strategii oraz doktryn obronnych w cyberprzestrzeni dla instytucji państwowych. Nie ma żadnych informacji wskazujących na działalność ofensywną podejmowaną przez tę instytucję.

Ważną rolę w irańskiej cyberobronie pełni również Centrum Bezpieczeństwa Informacji, znane jako MAHER, wchodzące w skład Ministerstwa Komunikacji i Technologii

Informacyjnych. W ramach tej instytucji znajduje się irański zespół reagowania na incydenty w sieci (*Computer Emergency Response Team*, CERT), odpowiedzialny za monitorowanie irańskiego Internetu. Dodatkowo Centrum szkoli informatyków, rozwija mechanizmy reagowania na kryzys w świecie wirtualnym oraz przechowuje niezbędne dane zawierające szczegóły o cyberobronie. Zajmuje się również obroną wszystkich rządowych stron oraz wybranych domen prywatnych. To właśnie informatycy z tej grupy odpowiadali za zwalczanie robaków *Stuxnet* i *Flame*.

Poboczną rolę w zapewnieniu cyberbezpieczeństa odgrywają inne organy, jak np. Najwyższa Rada Rewolucji Kulturalnej, w ramach której znajduje się komitet identyfikowania nielegalnych stron internetowych. Zasiadają w niej: Prokurator Generalny, szef policji, kierownik państwowych mediów oraz ministrowie. Głównym celem pracy tego ciała jest identyfikacja stron internetowych, których zawartość jest niezgodna z irańskim prawem oraz ich blokowanie.

Zdaniem amerykańskich ekspertów zdolności cybernetyczne Iranu cały czas rosną i obecnie znajduje się on w światowej czołówce w tej dziedzinie. W ciągu trzech lat Teheran wydał ponad miliard dolarów na rozbudowę swojego potencjału w przestrzeni wirtualnej i zwiększenie swoich możliwości w cyberprzestrzeni. Znaczenie tego nowego pola walki zostało dostrzeżone przez irańskich najwyższych wojskowych, o czym może świadczyć wypowiedź jednego z generałów *Pasdaran*, który powiedział, że bardziej obawia się ataków w cyberprzestrzeni, niż konwencjonalnej wojny.

Irańczycy, nauczeni doświadczeniem, dynamicznie rozwijają różne metody zwiększenia zdolności obronnych w środowisku wirtualnym oraz kontrolowania zawartości Internetu. Władze w Teheranie obawiają się m.in., że nowoczesna technologia może zostać wykorzystana do przeprowadzenia zamachu stanu. W celu zabezpieczenia się na taką ewentualność blokowane są strony internetowe oraz media społecznościowe, które od czasów „Arabskiej Wiosny" postrzega się jako wyjątkowe niebezpieczne i służące destabilizacji rządów. Zakupiono również (od chińskiej firmy ZRT Corp) specjalne oprogramowanie monitorujące telefony oraz Internet. Wartość kontraktu wynosiła ok. 130 milionów dolarów. Obecnie Iran postrzegany jest jako państwo znajdujące się w czołówce – obok Chin, Korei Północnej, Syrii i Birmy – krajów najskuteczniej monitorujących treść Internetu. Ponadto

wprowadzono nowe regulacje prawne, które nakazują właścicielom kafejek internetowych nagrywać działania użytkowników. Intensyfikacji uległy również działania policji, w ramach której powołano specjalną jednostkę FETA do zwalczania wrogiej działalności w cyberprzestrzeni.

W kwietniu 2012 roku Teheran, w celu ochrony swojego przemysłu naftowego, odciął główne terminale od Internetu. Iran podjął się także ambitnego projektu stworzenia rodzimego Internetu, przyjaznego (*halal*) ideom muzułmańskim w ogóle, a szyickim w szczególności. Głównym jego założeniem jest odcięcie irańskich użytkowników od globalnej sieci i przekierowywanie ich na strony zaprojektowane przez rządowych informatyków w Teheranie. Pozwoli to na pełną kontrolę nad treściami przekazywanymi w sieci. Iran pracuje nad własnymi serwisami poczty elektronicznej, niezależnymi systemami operacyjnymi, wyszukiwarkami oraz innymi niezbędnymi narzędziami. Prace rozpoczęły się w 2009 roku, a według przedstawicieli amerykańskiego wywiadu, na chwilę obecną witryny ministerstw, uniwersytetów i sieci biznesowych działają w nowej konfiguracji. Stworzenie tak skomplikowanego projektu możliwe jest dzięki pomocy ze strony chińskiej firmy Huawei. Irańskie działania podyktowane są chęcią kontrolowania opozycji oraz przeciwników reżimu, jednak mają także utrudnić penetrację sieci komputerowych przez obce państwa. Biorąc pod uwagę, że większość oprogramowania jest amerykańska, a przez co zawiera potencjalne dziury utworzone specjalnie przez NSA, rozwijanie alternatywnych rozwiązań jawi się władzom irańskim jako logiczna konsekwencja i najlepszy możliwy sposób zwiększenia bezpieczeństwa w cyberprzestrzeni.

Iran stara się również izolować systemy należące do aparatu bezpieczeństwa państwa i stworzyć własną sieć, odseparowaną od globalnego Internetu. Pierwszym wcieleniem tego pomysłu jest *Basir*, wewnętrzna sieć Strażników Rewolucji, o istnieniu której świat dowiedział się w marcu 2012 roku. Raporty wskazują, że może ona przetrwać nawet zaawansowane i zmasowane cyberataki.

Ponadto Iran zainwestował w dodatkowe szkolenia z zakresu cyberbezpieczeństwa, zwiększono również liczbę ćwiczeń oraz inspekcji kontrolujących stopień przygotowania systemów cyberobrony w instytucjach państwowych. Wprowadzone środki zdały pozytywnie test w czerwcu 2013 roku, kiedy odbyły się wybory. Systemy komputerowe pracowały

skutecznie, kontrolując treści przesyłane w irańskim Internecie oraz monitorując działalność, uznawaną przez władze za potencjalnie wywrotową.

Iran w natarciu

Doświadczenie ze *Stuxnetem* i jego następcami doprowadziło nie tylko do ulepszenia cyberobrony Iranu, ale również wpłynęło na zdolności ofensywne. Irańska ofensywa na tym polu ma iść w parze z innymi środkami asymetrycznymi wymierzonymi bezpośrednio w Stany Zjednoczone. Dobry przykład stanowi tutaj plan zabicia ambasadora Arabii Saudyjskiej w Waszyngtonie. Obecnie, część ekspertów postrzega irańskich hakerów jako największe zagrożenie dla bezpieczeństwa Stanów Zjednoczonych i ceni ich umiejętności wyżej niż ich odpowiedników z Chin.

Główną instytucją odpowiedzialną za prowadzenie ofensywnych działań w cyberprzestrzeni jest cyberjednostka Irańskich Strażników Rewolucji, która rozwija różne rodzaje złośliwego oprogramowania, zdolności do blokowania komunikacji i sieci Wi-Fi, prowadzi prace nad nowymi sposobami penetrowania sieci komputerowych w celu zbierania informacji i przesyłania ich z powrotem, a także zajmuje się opracowywaniem skutecznych bomb logicznych – programów aktywujących się po danym czasie albo na komendę. Ponadto rozwijane są narzędzia wojny elektronicznej zdolne do zablokowania radarów oraz systemów komunikacji przeciwnika. Wraz z użyciem złośliwego oprogramowania ma to umożliwić przełamanie systemów elektronicznych Stanów Zjednoczonych oraz ich sojuszników w wypadku potencjalnej konfrontacji zbrojnej.

Na usługach reżimu ajatollahów znajduje się również Irańska Armia Cybernetyczna (IRA), która przeprowadziła liczne udane ataki na strony irańskiej opozycji, skutecznie destabilizując możliwości organizacyjne przeciwników reżimu. Oficjalnie jej przedstawiciele odcinają się od jakikolwiek powiązań z władzami w Teheranie, jednak wielu zachodnich ekspertów podejrzewa, że jednostka ta działa na zlecenie irańskiej armii. Podobna sytuacja dotyczy Zespołu Bezpieczeństwa *Ashiyane*, który wspiera „ideały rewolucji islamskiej" i realnie przyczynia się do zwiększenia zdolności Islamskiego Iranu w cyberprzestrzeni, m.in poprzez szkolenie hakerów, umieszczanie na zachodnich i izraelskich stronach internetowych proirańskiej propagandy, jak również podejmowania typowej działalności cyberprzestępczej.

Co więcej, grupa ta założyła forum pod tytułem „Gry Wojenne", na którym odbywają się swoiste zawody hakerów w najskuteczniejszym zaatakowaniu infrastruktury krytycznej Stanów Zjednoczonych. Podobnie jak w przypadku IRA, przedstawiciele *Ashiyane* odcinają się od jakichkolwiek powiązań z władzami w Teheranie. Wykorzystanie teoretycznie niezależnych organizacji i grup jest charakterystyczne dla działania reżimu ajatollahów, czego doskonałym przykładem jest Hezbollah. Wydaje się, że również w świecie wirtualnym Teheran ucieka się do tego typu środków

Początkowe ataki były jednak dość proste i polegały w dużej mierze na zablokowaniu dostępu do stron internetowych. Wśród celów IRA znalazł się np. *twitter* czy strony NASA; udało się również wykraść dane osobowe pracowników tej amerykańskiej agencji. Wraz z upływem czasu irańscy hakerzy podejmowali jednak coraz śmielsze i skuteczniejsze akcje. W 2012 roku przeprowadzono za pomocą samoreplikującego się wirusa ataki na przedsiębiorstwo naftowe Aramaco w Arabii Saudyjskiej, prowadzającej wydobycie ok. 10 proc. ropy naftowej na całym świecie. Napastnikom udało się uszkodzić ponad 30 tys. komputerów. Sprawiło to, że podstawowe operacje wykonywane przez tę firmę zostały czasowo przerwane, a przywrócenie wszystkich systemów doi stanu pełnej używalności zajęło ponad dwa tygodnie. Dodatkowo wirus ten rozpowszechnił się również do sieci innych firm, zajmujących się wydobyciem „płynnego złota".

Należy w tym miejscu podkreślić, że ochrona przedsiębiorstw naftowych zaliczonych do elementów infrastruktury krytycznej miała zawsze priorytetowe znaczenie dla Arabii Saudyjskiej i USA. Jakiekolwiek zakłócenie funkcjonowania sektora naftowego mogłoby mieć poważne konsekwencje dla kształtowania się cen ropy naftowej na świecie. Mimo, iż znalezienie sprawcy ataku jest praktycznie niewykonalne w środowisku wirtualnym, stopień skomplikowania oprogramowania wskazuje, że za jego stworzeniem stoi jakieś państwo. Biorąc pod uwagę napięte relacje między Teheranem a Rijadem, Iran jest tu głównym podejrzanym. Pojawiły się również pewne charakterystyczne cechy, które zwiększają prawdopodobieństwo tej tezy, jak np. fakt, że wirus niszczył wszystkie obrazki przedstawiające amerykańskie flagi.

W 2013 roku hakerzy powiązani z Teheranem przeprowadzili wiele ataków na przedsiębiorstwa amerykańskie i zachodnioeuropejskie w odwecie za nałożenie sankcji

ekonomicznych na Iran, w związku z jego kontrowersyjnym programem nuklearnym. Jedną z najbardziej spektakularnych operacji, za którą stoją irańscy hakerzy, jest atak przeprowadzony w 2013 roku przeciwko stronom amerykańskich banków. Wśród zaatakowanych znalazły się: Citigroup, Wells Fargo, Capital One, HSBC i Bank of America. Klienci tych instytucji mieli poważne problemy z zalogowaniem się do swoich kont czy realizowaniem transakcji on-line. Skala oraz stopień ataków zostały określone przez ekspertów jako wysoce zaawansowane.

W tym samym roku ofiarą irańskich hakerów padły amerykańskie przedsiębiorstwa z sektora energetycznego, a celem ataku były systemy nadzorujące przebieg procesu technologicznego i produkcyjnego. Operacje wymierzone w takie systemy mogą mieć druzgocące konsekwencje, doprowadzając do uszkodzenia linii przesyłowych czy systemów elektrycznych. Uznawane są też za najtrudniejsze do przeprowadzenia. Według doniesień prasowych, administracja prezydenta Baracka Obamy poważnie rozważała przeprowadzenie uderzenia odwetowego w cyberprzestrzeni, ale w końcu zrezygnowano z tego rozwiązania.

Iran nie ogranicza się tylko do celów cywilnych. Skutecznie zaatakował również sieci wewnętrzne amerykańskiej marynarki wojennej i Korpusu Piechoty Morskiej, uzyskując dostęp do dużej ilości danych. Nie udało się jednak pozyskać informacji o charakterze poufnym. Według wstępnych ustaleń, oczyszczenie wszystkich systemów US Navy i USMC ze złośliwego oprogramowania trwało cztery miesiące, co stanowi kolejny dowód na wysokie kwalifikacje Irańczyków.

Celem irańskich hakerów są nie tylko Stany Zjednoczone i Arabia Saudyjska. Wiele z ataków zostało przeprowadzonych także przeciwko Izraelowi. W czerwcu 2013 roku premier Benjamin Netanjahu przyznał, że nastąpiła zdecydowana intensyfikacja ataków wymierzonych w izraelską infrastrukturę; zaatakowano m.in. system wodociągowy w mieście Hajfa. Jeden z izraelskich generałów zaapelował wręcz o stworzenie odpowiednika „Żelaznej Kopuły”[1] w cyberprzestrzeni, w celu przeciwdziałania „wirtualnym” zagrożeniom ze strony wzmożonej aktywności Iranu i innych podmiotów wrogich Izraelowi.

[1] „Żelazna Kopuła” to izraelski system antyrakietowy, przeznaczony do zwalczania pocisków krótkiego zasięgu. Jest powszechnie uznawany za najlepszy na świecie, a swój bardzo udany debiut bojowy przeszedł podczas operacji

Również państwa Europy Zachodniej nie mogą czuć się w pełni bezpieczne. Irańscy hakerzy ukradli z Holandii cyfrowe certyfikaty bezpieczeństwa w sieci, wykorzystując je do włamywania się na skrzynki e-mailowe oraz podsłuchiwania komunikacji. Była to jedna z najbardziej zaawansowanych operacji irańskich w ostatnim czasie.

Iran prowadzi także w cyberprzestrzeni coraz bardziej zaawansowane operacje szpiegowskie. W ostatnich miesiącach media amerykańskie poinformowały o odkryciu zakrojonej na szeroką skalę operacji cyberszpiegowskej pod kryptonimem „Newcaster", przeprowadzanej prawdopodobnie przez Iran, której celem były systemy komputerowe i sieci USA, Wielkiej Brytanii, Izraela i Francji. Pierwsze oznaki działalności irańskich cyberszpiegów datować można na początek 2011 roku. W początkowej fazie operacji utworzono sieci fałszywych profili w mediach społecznościowych, podszywając się pod znanych dziennikarzy, pracowników administracji amerykańskiej, dyplomatów, wojskowych czy członków Kongresu. Stworzono konta na takich portalach jak *Facebook, LinkedIn* czy *Twitter*. Fałszerzy cechowała dbałość o szczegóły, stworzono wiarygodne historie potwierdzone przez założony przez nich portal NewsOnAir.org. Ta technika cyberszpiegostwa nie należy do nowych, ale skala jej wykorzystania świadczy o dużych zdolnościach irańskich cyberszpiegów. W fazie drugiej wykorzystano stworzone wcześniej konta do nawiązania bliższych znajomości z członkami administracji rządowych. Starano się stworzyć taki poziom zaufania, który pozwoli na przesłanie wiadomości ze szkodliwym programem. Irańczykom udało się dotrzeć do ponad 2000 osób, większość z nich stanowili dyplomaci i politycy ze Stanów Zjednoczonych, Arabii Saudyjskiej, Wielkiej Brytanii czy Izraela. Nie wiadomo jednak, jakie dokładnie informacje udało się wykraść. O zaangażowaniu Teheranu w całą operację najlepiej świadczy fakt, że strona NewsOnAir.org została zarejestrowana w Iranie, a w kodzie oprogramowania szpiegowskiego znaleziono słowa w języku perskim. To pierwszy ujawniony przypadek irańskiego szpiegostwa w cyberprzestrzeni.

Reżim w Teheranie stara się również wykorzystać swoje cyberzdolności w propagandowy sposób. Najlepszym przykładem na takie działanie jest katastrofa

Izraela przeciwko Hamasowi w strefie Gazy w 2013 roku. Od tego czasu kolejne baterie „Kopuły" coraz skuteczniej chronią tereny południowego Izraela, narażone na nieustanny ostrzał rakietowy z obszaru Gazy i Płw. Synaj.

amerykańskiego drona RQ-170, zbudowanego w technologii *stealth*. Ten bezzałogowy aparat latający rozbił się na terytorium Iranu po utracie łączności z bazą. Zdaniem władz Iranu, było to spowodowane udaną akcją hakerską. Nie istnieją jednak przekonujące dowody na poparcie tej tezy, zaś zdaniem Pentagonu, katastrofa była spowodowana awarią sprzętu.

Za sukcesem irańskich operacji o charakterze ofensywnym w cyberprzestrzeni stoi połączenie następujących elementów: wiedzy oraz zdolności dość licznej grupy informatyków pracujących dla rządu, z doświadczeniem oraz umiejętnościami społeczności irańskich hakerów, którzy identyfikują się z reżimem i jego celami. Dodatkowo nawiązano liczne kontakty ze zwykłymi cyberprzestępcami, hakerami oraz specjalistami od bezpieczeństwa informacyjnego z państw byłego Związku Radzieckiego, a w szczególności z Rosji. Za zaoferowane pieniądze zgodzili się oni pracować nad wzmocnieniem zdolności ofensywnych Islamskiej Republiki Iranu w cyberprzestrzeni.

Działalność irańskich hakerów w cyberprzestrzeni nie ogranicza się tylko i wyłącznie do przeprowadzania bezpośrednich ataków. Szkolą oni również inne grupy hakerskie, które prowadzą szkodliwą działalność w cyberprzestrzeni wymierzoną we wrogów Iranu. Najlepszym przykładem jest Syryjska Armia Elektroniczna – ugrupowanie hakerów powiązane z popieranym przez Teheran prezydentem Syrii Baszarem al-Assadem. Zasłynęli oni m.in. zhakowaniem konta na *twitterze* amerykańskiej agencji Associated Press. Umieścili na nim fałszywe informacje o rzekomym zamachu w Białym Domu, w wyniku którego ranny miał zostać sam prezydent B. Obama. „News" ten, zanim został usunięty i sprostowany, spowodował wielomilionowe straty na światowych giełdach oraz uświadomił znaczenie cyberbezpieczeństwa dla współczesnego świata.

Irańscy hakerzy wspomagali również Hezbollah w utworzeniu oddziałów tej organizacji, operujących w świecie wirtualnym, a zajmujących się głównie zbieraniem informacji w sieci oraz promocją własnych wartości i idei w mediach społecznościowych.

Zakończenie

Iran w przeciągu ostatnich cztrerech lat znacznie zmodernizował i powiększył swój potencjał obronny i ofensywny w cyberprzestrzeni, co zaskoczyło wielu zachodnich ekspertów. Według raportu izraelskiego *The Institute for National Security Studies*, Iran

z kraju będącego w trzeciej lidze cyberbezpieczeństwa awansował do światowej czołówki, tworząc skuteczny system cyberobrony. Nie jest on może na tyle zaawansowany, żeby przeciwstawić się atakowi z wykorzystaniem skomplikowanego oprogramowania w stylu *Stuxnetu*, ale należy sobie zadać w tym miejscu pytanie, czy jakiekolwiek inne państwo dysponuje skutecznymi zdolnościami obronnymi przed takim programem.

Irańczykom udało się również wyeliminować zagrożenie płynące ze strony grup opozycyjnych, mogących wykorzystać Internet do szerzenie destabilizacji i prób obalenia władzy. Także w działaniach ofensywnych Iran osiągnął duże sukcesy, skutecznie atakując strony internetowe amerykańskich banków czy przeprowadzając zaawansowaną operację przeciwko przedsiębiorstwu naftowemu w Arabii Saudyjskiej, potwierdzając w ten sposób opinie ekspertów wysoko oceniających irański potencjał w cyberprzestrzeni. Działania Iranu są przy tym różne od akcji Chin, które specjalizują się w kradzieży własności intelektualnej czy też od zachowania Rosji, wykorzystującej cyberprzestępców. Teheran stara się stworzyć zdolności odwetowe w cyberprzestrzeni, przeciwdziałając w ten sposób sankcjom i innym wrogim aktom ze strony państw Zachodu. Rozwijając swoje zdolności w środowisku wirtualnym, Iran rekompensuje słabość konwencjonalnych sił zbrojnych. Cyberprzestrzeń staje się środowiskiem coraz bardziej intensywnego konfliktu, a państwa Bliskiego Wschodu inwestują coraz większe środki w rozwój swoich cyberzdolności, co spowoduje, że ten sposób prowadzenia działań wojskowych będzie tylko zyskiwał w miarę upływu czasu na znaczeniu.

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 18/2014

Hakerzy ajatollahów

Autor: Andrzej Kozłowski

Ekspert Fundacji *Amicus Europae* oraz Instytutu Kościuszki. Członek redakcji pisma „Stosunki Międzynarodowe”.
Doktorant na Wydziale Studiów Międzynarodowych i Politologicznych UŁ. W kręgu jego zainteresowań znajdują się cyberbezpieczeństwo, region Kaukazu Południowego oraz polityka bezpieczeństwa i zagraniczna USA.

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.