FAE Policy Paper
nr 21/2014

Andrzej KOZŁOWSKI

Izrael jako cybermocarstwo

Mimo niewielkich rozmiarów terytorium i małego potencjału ludnościowego, Izrael powszechnie uważany jest za mocarstwo oraz jedno z państw o największym potencjale defensywnym i ofensywnym w cyberprzestrzeni. W raporcie przygotowanym w 2011 roku przez firmę McAfee, zajmującą się bezpieczeństwem komputerowym, Izrael uzyskał ocenę 4.5 w pięciostopniowej skali. Co decyduje o fenomenie cyberbezpieczństwa Izraela i czy możliwe jest przeniesienie ich rozwiązań na polskie podwórko?

Otoczony przez wrogo nastawione państwa arabskie i uznawany za jednego z głównych przeciwników świata muzułmańskiego – Izrael od początku swojego istnienia kładł szczególny nacisk na politykę bezpieczeństwa. Zdawano sobie sprawę, że każda przegrana wojna doprowadzi do anihilacji narodu żydowskiego i będzie powtórką Holokaustu. Żydzi rozwinęli sprawne siły zbrojne, gotowe do odparcia prawie każdego niebezpieczeństwa. Nie mogąc się równać ze swoimi adwersarzami potencjałem demograficznym, musieli bazować na przewadze technologicznej. Dotyczy to również nowego środowiska bezpieczeństwa, jakim jest cyberprzestrzeń. Jest ona szczególnie ważna dla praktycznie każdego aspektu funkcjonowania państwa izraelskiego, od gospodarki opartej na nowoczesnych technologiach, przez agendy rządowe, a kończąc na społeczeństwie korzystającym z dobrodziejstw, które daje np. Internet. Przetrwanie Izraela coraz bardziej zależy więc od zbudowania skutecznej cyberobrony.

Rosnące zagrożenie

Izrael był jednym z pierwszych uczestników tzw. konfliktu w cyberprzestrzeni. Już w 1999 roku, wraz z wybuchem Drugiej Intifady, walki przeniosły się w to dotąd nieznane środowisko. Rok później w odpowiedzi na porwanie przez Hezbollah izraelskich żołnierzy, hakerzy włamali się na strony tej organizacji terrorystycznej, palestyńskich władz oraz innych organizacji terrorystycznych. Na odpowiedź ze strony Palestyńczyków nie trzeba było długo czekać. Ofiarą ich ataku typu *e-mail bombing*, polegającego na zablokowaniu skrzynek poczty elektronicznej masowym zalewem wiadomości, padł Kneset oraz witryny izraelskiej administracji rządowej.

Obie strony konfliktu umieściły również w sieci narzędzia do przeprowadzania prostych ataków typu DDoS, pozwalających na czasowe zablokowanie dostępu do stron internetowych. Jedno z ugrupowań sympatyzujących ze stroną palestyńską przygotowało nawet czterofazowy plan wojny internetowej. Pierwsze uderzenie miało obejmować uderzenie na izraelskie serwery rządowe, drugie – atak na obiekty mające znaczenie dla finansów państwa, jak np. banki. Trzecie polegało na uderzeniu w głównych dostawców usług internetowych. Faza ostatnia przewidywała zmasowany atak na wszystkie serwisy handlu elektronicznego, co miało doprowadzić do poważnych strat finansowych. Planowano również przypuścić uderzenie na cele zagraniczne.

Początkowe ataki były nieszkodliwe i polegały raczej na cyberwandaliźmie, jednak ich skala w latach 2000–2003 ciągle rosła, wykryto 548 poważnych operacji skierowanych przeciwko domenom izraelskim. Zwiększał się również poziom zaawansowania szkodliwego oprogramowania, tworzonego przez adwersarzy Izraela. Powodowało to, że wzrost zagrożenia w cyberprzestrzeni traktowano coraz poważniej. Obecnie szacuje się, że co minutę przeprowadzanych jest około 1000 cyberataków. Większość z nich to niegroźne wybryki wandali, sympatyzujących ze sprawą palestyńską. Rośnie jednak zagrożenie ze strony obcych państw, a w szczególności szybko zbrojącego się w cyberprzestrzeni Iranu oraz organizacji cyberprzestępczych.

Strategia

Jeśli chodzi o strategie i doktryny Izraela w cyberprzestrzeni, to pozostają one utajnione i niewiele o nich wiadomo. Jest to znacząca różnica w porównaniu do państw Zachodu, gdzie większość dokumentów tego typu jest jawna.

Przywiązanie wagi do operacji w cyberprzestrzeni i nadanie im dużego znaczenia jest zgodne z głównym założeniem izraelskiej doktryny, kładącej nacisk na jakość kosztem ilości. W 2009 roku izraelski szef sztabu powiedział, że cyberprzestrzeń to miejsce wojny strategicznej. Izrael poprzez działania w środowisku wirtualnym realizuje trzy niżej wymienione cele:

- Odstraszanie – zaawansowane zdolności prowadzenia działalności w cyberprzestrzeni pozwalają na skuteczne odstraszanie od agresji potencjalnych przeciwników. Sukcesy

ofensywne Izraela w cyberprzestrzeni, ujawnione przez światowe media, tylko ten obraz utrwalają.

- Ostrzeganie – rozwinięte zdolności cyberszpiegowskie pozwalają na zebranie wielu istotnych informacji na temat ruchów i zachowań potencjalnego przeciwnika, dzięki czemu zaskoczenie Izraela będzie praktycznie niewykonalne. Jednocześnie silne zabezpieczenia przez obcą penetracją powodują, że izraelskie wrażliwe dane będą skutecznie chronione.
- Mnożnik siły – rozwinięte zdolności w cyberprzestrzeni mogą przechylić szalę zwycięstwa w konwencjonalnej wojnie na stronę izraelską

Cyberwojna jest traktowana przez Izraelczyków jako alternatywa do działań konwencjonalnych, która jednakże ze względu na brak konsekwencji i trudność w wykryciu sprawcy może być wykorzystywana znacznie częściej.

Izraelska cyberobrona

Izrael bardzo wcześnie rozpoczął prace nad kształtowaniem swojej cyberobrony. W 1997 roku opracowano projekt *Tehila*, zakładający ochronę infrastruktury rządowej poprzez zapewnienie bezpiecznego dostępu do Internetu oraz zabezpieczenie stron rządowych. Rok później w życie weszło prawo definiujące systemy komputerowe o kluczowym dla państwa znaczeniu. W 2002 Izrael sporządził listę 19 najważniejszych obiektów infrastruktury krytycznej. Wśród nich znalazły się m.in. elektrownie, system bankowy czy systemy zaopatrzenia w wodę.

Do bardzo ważnych inicjatyw zaliczyć należy stworzenie w 2010 roku planu zatytułowanego „Narodowa inicjatywa na rzecz rozwoju cyberprzestrzeni", którego głównym celem jest wyniesienie Izraela do grona pięciu państw dysponujących największym potencjałem w środowisku wirtualnym. Plan ten został stworzony we współpracy między praktycznie wszystkimi instytucjami zainteresowanymi rozwojem cyberbezpieczeństwa. Izraelski rząd przydzielił również dodatkową kwotę 22 milionów dolarów, które mają zostać przeznaczone na badania i rozwój w latach 2013-2015.

Kolejnym istotnym aspektem jest kapitał ludzki. Młodzi ludzie o patriotycznym nastawieniu, rozumiejąc zagrożenie płynące z sieci, coraz częściej podejmują studia z zakresu

cyberbezpieczeństwa. Stają się tym samym niezwykle użyteczni, tak dla wojska, jak i struktur cywilnych, a coraz większa liczba uniwersytetów oferuje im możliwość pogłębiania wiedzy w tej dziedzinie poprzez otwieranie nowych kierunków.

Bardzo istotnym aspektem izraelskiej cyberobrony jest silna, rozbudowana pozycja prywatnego sektora IT, a w szczególności firm odpowiedzialnych za bezpieczeństwo w Internecie. Już od samego początku *boomu* związanego z popularnością komputerów osobistych Izrael zajmował jedno z czołowych miejsc, jeśli chodzi o rozwój technologii. To właśnie w latach 80. w laboratorium w Hajfie powstał chip 8088, który stał się kluczowym elementem PC. Izraelscy inżynierowi wnieśli również olbrzymi wkład w rozwój procesorów Pentium, procesorów wielordzeniowych, oszczędnych jednostek zasilających przenośne komputery oraz wielu innych technologii. Najwięksi potentaci Internetowi, poczynając od Microsoftu, poprzez IBM, a na Google kończąc, posiadają jednostki badawcze w Izraelu. Podobna sytuacja występuje w odniesieniu do cyberbezpieczeństwa. Kiedy temat ten stał się niezwykle popularny, wyżej wymienione przedsiębiorstwa sektora IT dokonały natychmiastowych inwestycji w izraelskie firmy, zajmującą się tą problematyką.

Ostatnim pomysłem w zakresie budowy zintegrowanego centrum cyberobrony jest stworzenie międzynarodowego cybercentrum w południowej części miasta Ber Szawa. Wszystkie wojskowe i rządowe instytucje odpowiedzialne za działania w świecie wirtualnym mają zostać przemieszczone w ten rejon, który leży w sąsiedztwie uniwersytetu Ben-Guriona oraz niedawno zbudowanego centrum przemysłu IT. Odzwierciedla to filozofię Izraelczyków, którzy wierzą, że skuteczne połączenie sektora prywatnego z publicznym, wsparte przez środowisko akademickie, gwarantuje zbudowanie skutecznej cyberobrony.

Izrael aktywnie włącza się również w budowanie międzynarodowych porozumień dotyczących bezpieczeństwa w cyberprzestrzeni, popierając wszystkie propozycje mające na celu uregulowanie działań w przestrzeni wirtualnej. Jest też stroną Konwencji Budapesztańskiej o cyberprzestępczości.

Wciąż jednak problemem pozostaje podatność prywatnych przedsiębiorstw, jak również przeciętnych użytkowników sieci, na ataki w cyberprzestrzeni. Izrael nie jest tutaj odosobniony, z tym wyzwaniem nie może sobie jak na razie poradzić nikt na świecie. Żadna z rządowych agencji nie została bezpośrednio wyznaczona do ochrony tych podmiotów.

Może być to szczególnie groźne dla gospodarki Izraela, która jest w dużej mierze zależna od zdolności eksportowych biznesu i przemysłu. Problem ten próbowały rozwiązać największe przedsiębiorstwa z sektora obronnego, poprzez ustanowienie w swoich strukturach jednostek odpowiedzialnych za cyberobronę. Nie zapobiegło to jednak poważnej kradzieży informacji, która nastąpiła w 2014 roku. Chińscy hakerzy włamali się do trzech firm zbrojeniowych, wykorzystując luki w ich zabezpieczeniach, i skradli dane dotyczące najnowszego systemu przeciwrakietowego „Żelazna Kopuła".

Izraelskie zdolności ofensywne

Izraelskie zdolności ofensywne w cyberprzestrzeni postrzegana są jako jedne z najbardziej zaawansowanych na świecie, a dwie operacje przeprowadzone przez hakerów z tego kraju zapisały się w historii konfliktów w cyberprzestrzeni. Pierwsza z nich miała miejsce w 2007 roku, kiedy to w ramach operacji *Orchard* zniszczono syryjski reaktor nuklearny. Do zneutralizowania syryjskiej obrony przeciwlotniczej wykorzystano tradycyjne metody walki radioelektronicznej, jak również zaawansowane złośliwe oprogramowanie, które umożliwiło izraelskim samolotom niepostrzeżenie dotrzeć w rejon reaktora. Sytuacja ta doskonale ilustruje, jak operacje w cyberprzestrzeni mogą być wykorzystywane jako tzw. mnożnik siły, zwielokrotniając zniszczenia powstałe w wyniku użycia konwencjonalnych środków walki.

Drugą operacją, która zapisała się w historii konfliktów w cyberprzestrzeni, było użycie robaka *Stuxnet* – niezwykle skomplikowanego oprogramowania stworzonego we współpracy z amerykańską Agencją Bezpieczeństwa Narodowego do sparaliżowania irańskiego programu nuklearnego. Był to pierwszy przypadek, kiedy program komputerowy był w stanie wyrządzić szkody w świecie materialnym, niszcząc wirówki wzbogacania uranu w ośrodku w Natanz.

Izrael nie przestaje jednak zadziwiać w wynajdywaniu innowacyjnych rozwiązań ofensywnych w cyberprzestrzeni. W 2010 roku stworzono jednostkę cyberkomandosów. Należą do nich osoby, które przeszły standardowe szkolenie dla jednostek specjalnych w Izraelskich Siłach Obronnych, a później zostały dodatkowo wyszkolone w przeprowadzaniu skomplikowanych ataków w cyberprzestrzeni. Ich przeznaczeniem jest

przenikanie do obcych państw i wykonywanie cyberataków z ich terytorium lub pomaganie komandosom w kradzieży nowoczesnej technologii czy radzeniu sobie z najbardziej zaawansowanymi zabezpieczeniami. Jednostka ta podlega Departamentowi Wywiadu Wojskowego.

Struktura sił odpowiedzialnych za działalność w cyberprzestrzeni

Za działania Izraela w cyberprzestrzeni odpowiada wiele rozmaitych organizacji. Trudno jest wskazać jedną dominującą, ale wydaje się, że główną rolę zaczyna odgrywać powołane w 2011 roku Narodowe Biuro ds. Cyberprzestrzeni. Główne cele można podzielić na trzy części:

- Tworzenie strategii oraz doktryn działania w cyberprzestrzeni w kooperacji z instytucjami odpowiedzialnymi za obronę,
- Rozwijanie infrastruktury oraz promowanie Izraela jako lidera na polu cyberbezpieczeństwa poprzez zwiększone inwestycje w kapitał ludzki oraz wspieranie badań nad różnymi aspektami cyberbezpieczeństwa,
- Zajęcie pozycji lidera w generalnym działaniach ukierunkowanych na zapewnienie cyberbezpieczeństwa – takich, jak regulowanie rynku usług bezpieczeństwa, stworzenie infrastruktury bezpieczeństwa narodowego poprzez odpowiednie przepisy legislacyjne oraz przeprowadzanie ćwiczeń i współpracę międzynarodową z partnerami.

Biuro ma działać głównie w skali makro i zajmować się cyberbezpieczeństwem na poziomie strategicznym. Istnieje jednak wiele innych instytucji zajmujących się działalnością Izraela w środowisku wirtualnym, bardziej na poziomie taktycznym, pełniąc wyspecjalizowane role. Prymat wiedzie tutaj „Jednostka 8200", działająca w ramach Izraelskich Sił Obronnych (IDF). Skupia się ona na trzech aspektach działania w świecie wirtualnym: ofensywie, defensywie i zbieraniu informacji. To właśnie ona stała za stworzeniem robaka *Stuxnet*. Ważną rolę od końca lat 90. odgrywa również *Shin Bet*, odpowiedzialny za ochronę systemów rządowych, infrastruktury krytycznej oraz danych gospodarczych. Nie można również zapomnieć o roli pełnionej przez *C4I Corps*, który odpowiedzialny jest za komunikację oraz przygotowanie i zarządzanie zasobami

cyberobrony. W ramach ten instytucji rozwinięto programy treningowe „Kursy z Cyberobrony", skierowane do żołnierzy, którzy po krótkim, acz intensywnym kursie mieliby być gotowi to przeprowadzania zadań o charakterze ofensywnym. W 2009 roku w celu poprawy jakości i zwiększenia skuteczności współpracy wywiadowczej pomiędzy C4I i Wywiadem Wojskowym, powołano Centrum Kodowania i Bezpieczeństwa Informacji. Instytucja ta odpowiada za dostarczanie informacji o rozwoju technologicznym potencjalnych przeciwników Izraela w świecie wirtualnym. Dodatkowo zajmuje się tworzeniem szyfrów dla sieci IDF, *Shin Betu* i *Mossadu*.

Ostatnią, powołaną w 2011 roku, instytucją odpowiedzialną za cyberbezpieczeństwo jest Narodowa Grupa Zadaniowa do działań w cyberprzestrzeni (*National Cybernetic Taskforce*). Była to odpowiedź na sugestie zawarte w raporcie przygotowanym przez panel ekspertów od cyberbezpieczeństwa, sugerującym znaczne wzmocnienie ochrony krytycznej. Licząca niespełna 80 osób, odpowiedzialna jest głównie za prowadzenie działań o charakterze defensywnym, ochronę głównych sieci przed atakami hakerów oraz pomoc prywatnym przedsiębiorstwom w przeciwdziałaniu szpiegostwu. Nie można jednak wykluczyć, że odpowiada też za operacje zaczepne. Do pozostałych jej funkcji zaliczyć należy koordynowanie współpracy w trójkącie rząd-uniwersytety-sektor prywatny. W planach pozostaje stworzenie specjalnych programów nauczania poświęconych cyberbezpieczeństwu rozpoczynających się na poziomie szkoły średniej.

Zakończenie

Znaczenie cyberbezpieczeństwa dla Izraela zostało dobrze zilustrowane w wypowiedzi jednego z doradców ds. bezpieczeństwa premiera Izraela Benjamina Netanjahu, który wyraził opinię, że cyberbezpieczeństwo to coś więcej, niż tylko ochrona informacji czy danych, to przede wszystkim ochrona kluczowych sektorów dla funkcjonowania państwa.

Efektywna współpraca pomiędzy przemysłem, światem akademickim i sektorem publicznym jest jednym z fundamentów skutecznej izraelskiej obrony w cyberprzestrzeni. Mimo, iż ich przedstawiciele mają różne cele oraz kulturę pracy, to udaje się im znaleźć wspólne rozwiązania. System prawny umożliwia skuteczny nacisk na sektor prywatny co do środków, które powinien podjąć w celu zabezpieczenia systemów o znaczeniu krytycznym.

Niewątpliwe jednak wciąż jest jeszcze wiele do zrobienia, szczególnie jeśli chodzi o wsparcie administracji rządowej dla sektora prywatnego. Analizując sytuację Izraela należy jednak pamiętać o specyficznym położeniu tego kraju i przyzwyczajeniu ludzi do konieczności poświęcania się w imię bezpieczeństwa. Jeśli Izraelczycy zgodzili się np. na prawo budowlane nakazujące wyposażenie każdego nowego domu w schron, tak teraz łatwiej jest im przystać na regulacje rządzące konfliktem w środowisku wirtualnym. Nie można zapominać też o ogromnym znaczeniu sektora IT w rozwoju technologii komputerowej w ogóle, a teraz skupiającym się na cyberbezpieczeństwie. Przeniesienie takich rozwiązań do innego kraju, jak np. Polski, jest bardzo mało prawdopodobne.

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 21/2014

Izrael jako cybermocarstwo

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.