Pułaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warszawa, 17.07.2015 r.

Autor: Andrzej Kozłowski

Nowa strategia Departamentu Obrony w cyberprzestrzeni

Pod koniec kwietnia 2015 roku nowo wybrany sekretarz obrony Ashton Carter ogłosił drugą w historii strategię Pentagonu w cyberprzestrzeni. Prezentacja strategii odbyła się w Dolinie Krzemowej, sercu amerykańskiego sektora IT. Opublikowany dokument zastąpił strategię z 2011 roku.

Strategia Pentagonu 2011

W 2011 roku Departament Obrony opublikował częściowo odtajnioną, liczącą niespełna 13 stron, „Strategię działania w cyberprzestrzeni". Strategia wyznaczała 5 inicjatyw. Pierwsza z nich zakładała traktowanie środowiska wirtualnego jako kolejnego obszaru działań wojennych obok lądu, morza, powietrza i przestrzeni kosmicznej. Wiązało się to z budową odpowiednich jednostek i struktur do operowania w cyberprzestrzeni, co doprowadziło do utworzenia Dowództwa Operacji w Cyberprzestrzeni (US CYBERCOM) podległego Dowództwu Strategicznemu Stanów Zjednoczonych. Druga inicjatywa polegała na przyjęciu nowych koncepcji obrony, która kładła nacisk na „cyberhigienę", rozumianą jako rozsądne korzystanie z oprogramowania komputerowego oraz ulepszenie metod walki z wewnętrznym zagrożeniem. Wdrożono również koncepcję aktywnej cyberobrony, polegającej na wciągnięciu w pułapkę atakującego i dokonania kontrataku. Trzecia kwestia zakładała współpracę z agencjami rządowymi, przede wszystkim z Federalnym Biurem Śledczym (FBI) i Departamentem Krajowym oraz z sektorem prywatnym w zakresie wymiany informacji.

> *. Po raz pierwszy bezpośrednio wskazano możliwość przeprowadzenia operacji o charakterze ofensywnym w cyberprzestrzeni oraz określono ich potencjalne cele. Ataki miałyby być wymierzone we wrogie systemy dowodzenia i wojskową infrastrukturę krytyczną, w celu sparaliżowania komunikacji przeciwnika, a operacją dowodzić ma US CYBERCOM, a nie jak poprzednio Agencja Bezpieczeństwa Narodowego (NSA).*

Czwarty punkt obejmował działania na arenie międzynarodowej, głównie w odniesieniu do poprawy zdolności NATO operowania w środowisku wirtualnym. Ostatnia inicjatywa polegała na zwiększeniu potencjału Stanów Zjednoczonych w cyberprzestrzeni poprzez inwestycję w technologie i kapitał ludzki.

Strategia Pentagonu z 2011 roku nie wspominała nic o zdolnościach ofensywnych, stanowiła podsumowanie doktryn i dokumentów strategicznych poszczególnych jednostek wojskowych, które zostały opracowane wcześniej. Zdaniem profesora Thomasa M. Chena, autora publikacji dla United States Army War College, była ona zbyt ogólna, nie miała jasno zdefiniowanych priorytetów i wizji strategicznej oraz nie przedstawiała planów wprowadzenia w życie zawartych w niej rozwiązań.

Strategia Pentagonu 2015

Nowa strategia wychodzi naprzeciw oczekiwaniom krytyków poprzedniego dokumentu. Jest bardziej szczegółowa, a także jasno artykułuje główne zadania Pentagonu w cyberprzestrzeni, które mają polegać na:

- obronie sieci, systemów i informacji Departamentu Obrony;
- obronie Stanów Zjednoczonych oraz interesów amerykańskich przed najbardziej destrukcyjnymi cyberatakami;
- gotowości do udzielenia wsparcia w cyberprzestrzeni dla operacji wojskowych.

Poza jasno wyodrębnionymi celami, strategia identyfikuje główne zagrożenia dla cyberbezpieczeństwa Stanów Zjednoczonych, odchodząc od niezwykle popularnej koncepcji apokaliptycznego ataku w środowisku wirtualnym, często porównywanego do japońskiego nalotu na Pearl Harbour. Jako główne zagrożenia wskazano na kradzież własności intelektualnej (obwiniając o to Chiny) oraz na ataki o niskim stopniu natężenia, wymierzone przeciwko pojedynczym osobom i przedsiębiorstwom. Wymieniono także problem proliferacji cyberbroni, spowodowany dynamicznym rozwojem czarnego rynku uzbrojenia tego typu.

Strategia, podobnie jak jej poprzedniczka, wyznacza 5 głównych inicjatyw strategicznych. Dokument zakłada budowę siły i zdolności do przeprowadzania operacji w cyberprzestrzeni oraz przewiduje podjęcie działań ukierunkowanych na zatrudnienie młodych

i utalentowanych ekspertów w tej dziedzinie, przeprowadzenie szkoleń, budowę zaplecza technicznego oraz wsparcie Narodowej Inicjatywy na rzecz Edukacji w cyberprzestrzeni (National Initative for Cyberspace Education). Drugi cel strategiczny uwzględnia obronę sieci Departamentu Obrony, zabezpieczenie danych Pentagonu oraz zmniejszenie ryzyka płynącego ze środowiska wirtualnego w operacjach wojskowych. W ramach tej inicjatywy główne zadania dotyczą poprawy efektywności sieci wojskowych, wymiany informacji o szkodliwym oprogramowaniu oraz przeciwdziałaniu wewnętrznym zagrożeniom. Punkt trzeci porusza problem obrony Stanów Zjednoczonych i ich interesów przed najgroźniejszymi cyberatakami, zdolnymi do wyrządzenia poważnych szkód. Cel ten ma być zrealizowany przez usprawnienie systemu przewidywania ataków, współpracę z innymi instytucjami federalnymi, a także rozwój innowacyjnych zdolności obronnych. Czwarta inicjatywa zakłada zapewnienie Pentagonowi zdolności kontroli eskalacji konfliktów w cyberprzestrzeni. Odbywać się ma to poprzez integrację operacji przeprowadzanych w środowisku wirtualnym z tymi, które mają miejsce na klasycznym polu bitwy. Ostatni punkt dotyczy wzmacniania międzynarodowych organizacji i partnerstwa z wybranymi sojusznikami na Bliskim Wschodzie, Azji oraz państwami członkowskimi NATO. Istotnie jest również osobne nawiązanie do dialogu z Chinami.

Strategia wskazuje podmioty odpowiedzialne za wykonywanie tych zadań. Cyber Mission Force, które są wciąż w fazie rozwoju, dzielą się na 4 zespoły, z których każdy realizuje inne cele:

- National Mission Teams – ochrona Stanów Zjednoczonych przed atakami w cyberprzestrzeni,
- Cyber Protection Teams – skupia się na ochronie sieci Pentagonu,
- Combat Mission Teams – zapewnienie wsparcia dla dowództw regionalnych,
- Support Teams – dostarcza informacji i analiz.

Dwa elementy wyróżniają nowy dokument Pentagonu na tle poprzednich strategii. Po raz pierwszy bezpośrednio wskazano możliwość przeprowadzenia operacji o charakterze ofensywnym w cyberprzestrzeni oraz określono ich potencjalne cele. Ataki miałyby być wymierzone we wrogie systemy dowodzenia i wojskową infrastrukturę krytyczną, w celu sparaliżowania komunikacji przeciwnika, a operacją dowodzić ma US CYBERCOM, a nie jak poprzednio Agencja Bezpieczeństwa Narodowego (NSA).

Drugim elementem jest powrót do koncepcji odstraszania. Początkowo Pentagon odrzucał taką opcję, uważając, że jest ona nieadekwatna do środowiska wirtualnego. Obecnie jednak bliska współpraca wywiadu z sektorem prywatnym ma uczynić atrybucję ataku jak najbardziej możliwą. Ponadto planuje się wdrożenie koncepcji „odstraszania przez odmowę korzyści", polegającej na stworzeniu odpornych systemów komputerowych, doprowadzających atakującego do frustracji.

Wnioski i rekomendacje

1. Nowa strategia Stanów Zjednoczonych kontynuuje i rozszerza zapisy i osiągnięcia poprzedniej. Jednakże nie ogranicza się tylko do definiowana celów strategicznych, ale przedstawia również szczegółowe rozwiązania, które mają zapewnić ich realizację, czego brakowało w poprzednim dokumencie.

2. Stany Zjednoczone powróciły do koncepcji odstraszania, co może świadczy o wierze we własne możliwości śledzenia i zidentyfikowania podmiotu atakującego. Przekonanie to wydaje się jednak błędne, ostatni poważny atak hakerski, wskutek którego napastnicy przejęli dane osób zatrudnionych w wywiadzie oraz siłach zbrojnych pokazuje, że zdolności atrybucji ataku są niewystarczające. Najbardziej znany przypadek identyfikacji atakującego – chińskiej jednostki wojskowej 61398 odpowiedzialnej za operacje szpiegowskie w cyberprzestrzeni – zajął prywatnej firmie Madiant kilka lat. Pokazuje to, że koncepcja odstraszania w środowisku wirtualnym ma ograniczone szanse powodzenia.

3. Oficjalne przyznanie się Amerykanów w dokumencie strategicznym do prowadzenia operacji ofensywnych w cyberprzestrzeni stanowi przełom. Mogą wystąpić jednak problemy w postaci atakowania obiektów podwójnego użytku (cywilnego i militarnego) oraz braku reguł użycia sił w środowisku wirtualnym. Zapisy strategii potwierdzają tezę o militaryzacji cyberprzestrzeni.

4. Zdecydowanie wzrasta rola sił militarnych w zabezpieczeniu kluczowych amerykańskich instytucji w cyberprzestrzeni oraz sektora prywatnego. Administracja Baracka Obamy zmniejszyła znaczenia utrzymywania względnej równowagi między sektorem cywilnym i wojskowym utrzymywanej przez poprzednie administracje.

5. Wymienienie konieczności nawiązania dialogu z Chinami świadczy o znaczeniu tego gracza w środowisku wirtualnym. Nie wydaje się to jednak możliwe w najbliższej

przyszłości. Obie strony wzajemnie oskarżają się o prowadzenie zaawansowanych operacji szpiegowskich w środowisku wirtualnym i trudno przypuszczać, żeby Chiny albo Stany Zjednoczone ich zaprzestały. Wprawdzie strony prowadzą dialog na temat cyberbezpieczeństwa, to jednak dotyczy on głównie spraw mniej kontrowersyjnych, jak np. walki ze spamem.

6. Nowa strategia Pentagonu pokazuje, że prowadzenie operacji o charakterze ofensywnym w cyberprzestrzeni staję się normą. Również polskie siły zbrojne powinny podjąć odpowiednie działania do stworzenia takich zdolności, uwzględniając m.in. tworzenie własnego złośliwego oprogramowania czy sieci botnet. W szczególności trzeba pamiętać, że polityka bezpieczeństwa NATO w świecie wirtualnym była i jest pod silnym wpływem amerykańskich rozwiązań, dlatego posiadanie ofensywnych zdolności w cyberprzestrzeni będzie niewątpliwe atutem Polski w Sojuszu Północnoatlantyckim.

7. Polska w ramach NATO powinna dołączyć do Projektu Rozwoju Wielonarodowych Zdolności Cyberobronnych (Multinational Cyber Defence Capability Development Project), w skład którego wchodzą Holandia, Rumunia, Dania, Norwegia i Kanada. Są to państwa posiadające rozwinięty system cyberobrony. Inicjatywa ta ma na celu usprawnienie dzielenia się wrażliwymi informacjami, zwiększenie świadomości o zagrożeniach i potencjalnej działalności hakerów oraz wspólną pracę nad ulepszeniem istniejących systemów cyberobrony.

Autor: *Krzysztof Kozłowski, Research Fellow Fundacji im Kazimierza Pułaskiego*

Fundacja im. Kazimierza Pułaskiego jest niezależnym think tankiem specjalizującym się w polityce zagranicznej i bezpieczeństwie międzynarodowym. Głównym obszarem aktywności Fundacji Pułaskiego jest dostarczanie analiz opisujących i wyjaśniających wydarzenia międzynarodowe, identyfikujących trendy w środowisku międzynarodowym oraz zawierających implementowalne rekomendacje i rozwiązania dla decydentów rządowych i sektora prywatnego.

Fundacja w swoich badaniach koncentruje się głównie na dwóch obszarach geograficznych: transatlantyckim oraz Rosji i przestrzeni postsowieckiej. Przedmiotem zainteresowania Fundacji są przede wszystkim bezpieczeństwo, zarówno w rozumieniu tradycyjnym jak i w jego pozamilitarnych wymiarach, a także przemiany polityczne oraz procesy ekonomiczne i społeczne mogące mieć konsekwencje dla Polski i Unii Europejskiej.

Fundacja Pułaskiego skupia ponad 40 ekspertów i jest wydawcą analiz w formatach: „Stanowiska Pułaskiego", „Komentarza Międzynarodowego Pułaskiego" oraz „Raportu Pułaskiego". Fundacja wydaje też „Informator Pułaskiego", będący zestawieniem nadchodzących konferencji i spotkań eksperckich dotyczących polityki międzynarodowej. Eksperci Fundacji regularnie współpracują z mediami.

Fundacja przyznaje nagrodę "Rycerz Wolności" dla wybitnych postaci, które przyczyniają się do promocji wartości przyświecających generałowi Kazimierzowi Pułaskiemu tj. wolności, sprawiedliwości oraz demokracji. Do dziś nagrodą uhonorowani zostali m.in.: profesor Władysław Bartoszewski, profesor Norman Davies, Aleksander Milinkiewicz, prezydent Lech Wałęsa, prezydent Aleksander Kwaśniewski, prezydent Valdas Adamkus, Javier Solana, Bernard Kouchner i Richard Lugar.

Fundacja Pułaskiego posiada status organizacji partnerskiej Rady Europy.

www.pulaski.pl