Cyberdefence 24

aut. Jacek Raubo 06.02.2016

WIĘCEJ PIENIĘDZY DLA PENTAGONU NA DZIAŁANIA W CYBERPRZESTRZENI

Amerykanie uznają cyberbezpieczeństwo za jeden ze strategicznych priorytetów obronności państwa w XXI w. Dlatego też w projekcie nowego budżetu Pentagonu zakłada się podniesienie wydatków na ten cel. Ma to zwiększyć defensywną i ofensywną siłę USA w cyberprzestrzeni.

Departamentowi Obrony (DoD) USA zależy na szybkim zwiększeniu zdolności obronnych państwa w sferze cyberprzestrzeni. Dotychczasowe oceny i analizy zagrożeń nie napawają optymizmem na przekór stereotypowej wizji „wielkiej cyberpotęgi", w którą zdawali się wierzyć amerykańscy decydenci. Dlatego też różne instytucje wojskowe i powiązane z DoD, a zaangażowane w cyberbezpieczeństwo, będą mogły liczyć na dopływ znacznych środków finansowych z budżetu państwa.

Według zapewnień sekretarza obrony Ashtona Cartera w roku fiskalnym 2017 w budżecie DoD planuje się przeznaczyć prawie 7 miliardów dolarów właśnie na sferę cyberbezpieczeństwa. Szacuje się, że w perspektywie najbliższych pięciu lat amerykański podatnik przeznaczy ze środków federalnych już niemal 35 miliardów na cyberaktywność sił zbrojnych. Przy czym w strukturze przyszłych wydatków DoD USA na cyberbezpieczeństwo coraz głośniej mówi się o przesunięciu punktu ciężkości z inwestycji w hardware na wydatki na software.

Tak gwałtowny wzrost w budżecie DoD wydatków na cyberbezpieczeństwo wynika z dążenia do stworzenia odpowiednio zabezpieczonych sieci wojskowych. Chodzi tu m.in o szersze wykorzystanie technologii sieci sterowanych programowo (SDN – Software Definied Networks). Opracowanie odpowiedniej, przeznaczonej dla wojska, architektury SDN, miałoby ograniczyć przyszłym przeciwnikom możliwość przeprowadzania skutecznych cyberataków na sieci wojskowe. Na potencjalne zyski, związane z rozwijaniem podobnych rozwiązań w ramach programów DoD, zwrócił uwagę przede wszystkim gen. Alan R. Lynn, będący obecnie dyrektorem Agencji Obronnych Systemów Informacyjnych (DISA). Generał jest również przewodniczącym Joint Force Headquarters – DoD Information Networks.

Jednak Amerykanie nie ukrywają, że cyberobrona to tylko jeden z dwóch elementów w ramach inwestycji. Zgoła nowy impuls rozwojowy stanowić będą wydatki na zwiększenie zdolności ofensywnych w sferze cyberbezpieczeństwa. Ashton Carter zaznacza przy tym, że dofinansowane zostaną zarówno szkolenia operatorów odpowiadających za uderzenia na obce systemy, jak i same narzędzia oraz infrastruktura. Bliższych szczegółów dotyczących konkretnych inwestycji można się spodziewać się jeszcze w lutym, w ramach procedury prezentacji założeń budżetu DoD przez administrację prezydencką. Ale i w tym kontekście zwraca się uwagę na możliwość szerszego zastosowania architektury sieci sterowanych programowo, których zadaniem jest zapewnienie możliwości mobilnego poruszania się na współczesnym polu cyberwalki. Na atuty ofensywnego wykorzystywania rozwiązań budowanych w oparciu o sieci SDN zwrócił uwagę m.in. inny przedstawiciel agencji DISA John Hickey.

Odwołując się od odtajnionej w ramach „sprawy Edwarda Snowdena” dyrektywy prezydenckiej w zakresie cyberoperacji należy podkreślić znaczenie działań ofensywnych. Mają one być wykorzystywane do wspierania w niekonwencjonalny sposób działań zmierzających do realizacji celów i zabezpieczenia interesów USA na całym świecie. Szczególnie w przypadku, gdy przeciwnik nie bierze pod uwagę, że może być obiektem amerykańskich operacji tego typu. Dotyczyć to może oczywiście podmiotów państwowych, ale i niepaństwowych jak różne organizacje terrorystyczne np. Daesh. Można więc śmiało założyć, że część pieniędzy posłuży do rozwoju narzędzi w stylu słynnego już Stuxnet.

Tak czy inaczej, istnieje przekonanie, nie tylko wśród najwyższych amerykańskich dowódców i dyrektorów najważniejszych instytucji zajmujących się problematyką cyberbezpieczeństwa, że wyzwania w sferze cyberprzestrzeni i technologii informacyjnych powinny znaleźć się wysoko na liście priorytetów państwa. Mówił o tym niedawno chociażby James R. Clapper, stojący na czele wywiadu narodowego. Wskazał on, że począwszy od 2013 r. to właśnie cyberzagrożenia zepchnęły terroryzm z pierwszego miejsca na liście zagrożeń. Przy czym - jego zdaniem - kluczowe jest przygotowanie się nie tyle na jeden szeroko zakrojony atak na infrastrukturę krytyczną państwa, co raczej na wiele rozproszonych prób uderzenia w różne sfery aktywności USA, zwłaszcza związane z funkcjonowaniem biznesu i podstawami ekonomicznymi państwa.

Amerykanie zdają sobie sprawę jak mocno ich państwo jest obecnie zależne od aktywności w cyberprzestrzeni. Dlatego DoD oprócz własnych agencji i struktur nadal zamierza inwestować chociażby w centra specjalnie utworzone w Dolinie Krzemowej i Bostonie. W opinii szefa Pentagonu Ashtona Cartera, USA muszą być przygotowane na reagowanie nie tylko w środowiskach dotychczas typowych dla sił zbrojnych – na lądzie wodzie i w powietrzu - ale również w cyberprzestrzeni w zakresie wojen elektronicznych. Państwo musi bowiem być zdolne nie tylko do prowadzenia współczesnych operacji militarnych, ale również myśleć o konfliktach przyszłości.