aut. Szymon Palczewski 15.02.2019

WZMOŻONA AKTYWNOŚĆ US CYBER COMMAND

Gen. Paul Nakasone, szef US Cyber Command, w przygotowanych uwagach dla senackiej Komisji Sił Zbrojnych sprecyzował działania oraz filozofię dowództwa, które w ostatnim czasie wykazywało wzmożoną aktywność.

Ponadprzeciętna aktywność Cyber Command wynika z kliku zmian. Jedną z nich jest nowe podejście Stanów Zjednoczonych do cyberprzestrzeni. W tym obszarze należy wskazać na skuteczniejsze konkurowanie z przeciwnikami, którzy aktywnie podejmują działania o charakterze asymetrycznym.

Paul Nakasone zauważył, że cyberprzestępcy korzystają z danych osobowych, kradną własność intelektualną oraz prowadzą szeroko rozumiane kampanie, których skutki mają strategiczny wpływ zarówno na cały naród, jak i sojuszników. W jednym z wywiadów dla Joint Force Quarterly stwierdził, że w przeciwieństwie do sfery nuklearnej, w której przewaga strategiczna wynika z posiadania zdolności lub dużych zasobów, w cyberprzestrzeni wykorzystanie wirtualnych zdolności ma strategiczne konsekwencje. Swoje stanowisko tłumaczył – „(przyp. red. przeciwnicy) aktywnie uczestniczą w komunikacji sieciowej, próbują kraść dane i wpływać na nasze systemy uzbrojenia. Tak więc przewagę zyskują ci, którzy utrzymują ciągły stan działania".

W przygotowanych uwagach dla senackiej Komisji Sił Zbrojnych Paul Nakasone podkreślił, że zgodnie z nową filozofią (znaną jako „defend forward"), Departament Obrony podejmie działania przeciwko tym, którzy dopuścili się ataku na Stany Zjednoczone. Obraną ideę określa się jako aktywną walkę z hakerami prowadzoną za granicą, a nie w ramach wewnątrzkrajowych struktur. Działania tego typu polegają na uzyskaniu dostępu do sieci oraz systemów przeciwników lub ich infrastruktury w celu poznania planu działania nieprzyjaciela.

Jak to działa w praktyce? Paul Nakasone nakreślił, w jaki sposób amerykanie wspierali dowództwo europejskie, Departament Bezpieczeństwa Wewnętrznego, Federalne Biuro Śledcze, aby zapewnić bezpieczeństwo wyborów w połowie 2018 roku. Działania te obejmowały utworzenie małej grupy rosyjskiej w ramach NSA, a także ścisłą współpracę z dowództwem europejskim oraz samymi państwami. „Stworzyliśmy stałą obecność w cyberprzestrzeni, aby monitorować działania przeciwników i opracować narzędzia, a także taktykę w celu udaremnienia wysiłków wroga" – tłumaczy szef Cyber Command.

Po drugie, dowództwo wspiera także bieżące operacje DoD w sferze fizycznej przeciwko grupom terrorystycznym. „Wykorzystujemy możliwości z zakresu cyberprzestrzeni w celu poprawy ochrony sił, wzmocnienia inteligencji, zrozumienia oraz ukształtowania środowiska informacyjnego, a także zakłócenia operacji, dowodzenia i kontroli, w tym propagandy kilku grup powstańczych i terrorystycznych" – zaznaczył Paul Nakasone.