Armia IT, czyli amerykańska cyberofensywa

16 listopada 2022

Pojawiają się kolejne informacje o atakach cybernetycznych prowadzonych przeciwko Rosji przez mitycznych „ochotników – hakerów” z Ukrainy. Tymczasem ostatnie publikacje pokazują, że za wszystkimi tymi działaniami niekoniecznie stoją Ukraińcy. I niekoniecznie też ochotnicy.

NSA w Estonii

31 maja w Tallinie odbyła się już czternasta edycja konferencji „Cyber Conflict”. Jej organizatorem jest powołane w 2008 roku w ramach Sojuszniczego Dowództwa ds. Transformacji NATO Centrum Doskonalenia Współpracy Obrony Cybernetycznej (ang. Cooperative Cyber Defense Center for Excellence). Choć ten znajdujący się w Estonii ośrodek jest strukturą akredytowaną przy NATO, w jego skład wchodzić mogą również kraje spoza sojuszu. W sierpniu 2021 roku akces do niego zgłosiła Ukraina, która w marcu 2022 roku uzyskała status członka wspierającego.

Tym razem szczególnym echem wśród uczestników odbił się wywiad udzielony przez amerykańskiego generała Paula Nakasone, szefa Dowództwa Sił Cybernetycznych Stanów Zjednoczonych i jednocześnie dyrektora Agencji Bezpieczeństwa Narodowego (NSA, ang. National Security Agency). Sama NSA, przynajmniej od czasów informacji ujawnionych przez Edwarda Snowdena, rozszyfrowywana bywa jako No Such Agency („nie ma takiej agencji”), bo jej sposób funkcjonowania jest kompletnie nieznany opinii publicznej, w tym amerykańskiej.

Cybernetyczne działania ofensywne

Wywiad z Nakasone przeprowadził brytyjski kanał Sky News, którego dziennikarze uznali NSA za najpotężniejszą na świecie strukturę zajmującą się wojnami cybernetycznymi. W rozmowie amerykański dowódca potwierdza wprost, że kierowana przez niego agencja przeprowadziła szereg „operacji ofensywnych, obronnych i informacyjnych" przeciwko Rosji na rzecz Ukrainy. Mówił o tym zresztą już dużo wcześniej. Jeszcze w 2018 roku podkreślał , że agencja pod jego kierownictwem prowadzić będzie cybernetyczne działania ofensywne nie tylko w imieniu samego Waszyngtonu, lecz także „w imieniu partnerów Stanów Zjednoczonych".

Daleko idąca wypowiedź Nakasone dla Sky News sprawiła, że w Białym Domu postanowiono się z niej tłumaczyć. Jej wymowę próbowała złagodzić Karine Jean-Pierre, rzeczniczka prasowa administracji Joe Bidena. Stwierdziła ona, że generałowi chodziło wyłącznie o wsparcie Ukrainy, choć przyznała, że ramy tej pomocy ulegają rozszerzeniu. Jean-Pierre na pytanie o to, czy ofensywne działania cybernetyczne nie stanowią zaprzeczenia polityki nieangażowania się w bezpośredni konflikt Stanów Zjednoczonych z Rosją, oznajmiła, że „my tak nie uważamy. Mówiliśmy już o tym. Nasi eksperci ds. cyberbezpieczeństwa mówili tu o swoim stanowisku. Nic się nie zmieniło. Także odpowiedź brzmi: nie".

Armia IT czy przykrywka dla zachodnich operacji?

Pogłoski o współpracy amerykańsko-ukraińskiej w sferze cybernetycznej już wcześniej wywołały zaniepokojenie szefa amerykańskiej Centralnej Agencji Wywiadowczej (CIA), Williama Burnsa. Stwierdził on, że działania cybernetyczne przeciwko Rosji stanowią przejaw nieodpowiedzialności, są niebezpieczne, a Ukraina znakomicie – jak dodał – radzi sobie sama z

wyzwaniami wywiadowczymi.

Niektórzy tymczasem uznają, że tzw. wojska IT Ukrainy w rzeczywistości służą za przykrywkę do działań służb i podmiotów zachodnich skierowanych przeciwko Rosji. Wprawdzie wszelkie przecieki na ten temat są zazwyczaj ściśle kontrolowane i neutralizowane, lecz w kilku przypadkach udało się ujawnić zaangażowanie struktur amerykańskich i brytyjskich, np. w działania hakerskie. Oficjalnie, kolejne cyberataki mają być jednak rzekomo popełniane przez hakerów-ochotników z Kijowa.

Wiadomo jednak, że powszechnie dostępny materiał instruktażowy dla ukraińskiej „armii IT" dostępny jest nie tylko na jej oficjalnym profilu w Telegramie, lecz także w Google Docs. A narzędzie do przeprowadzania ataków DDoS, Death by 1000 needles (db1000n), odnaleźć można w repozytorium GitHub. To ostatnie należy do pracownika firmy Cyberhaven w kalifornijskim Palo Alto, Bogdana Iwaszko. Oficjalnie jego pracodawca zajmuje się bezpieczeństwem sieci komputerowych.

Operacje hunt forward

Najwięcej ciekawych danych na temat działań Amerykanów po stronie ukraińskiej znaleźć można jednak w publikacji brytyjskiej BBC z 30 października. Czytamy tam, że jeszcze na początku grudnia 2021 roku na Ukrainę trafiła „niewielka grupa amerykańskich wojskowych z młodą major na czele". Miała ona przeprowadzić rekonesans przed konfliktem na większą skalę.

Jak powiedział BBC gen. William Hartman, dowodzący Narodowymi Cybernetycznymi Siłami Ekspedycyjnymi Stanów Zjednoczonych, „Przeanalizowała ona sytuację i powiedziała, że grupa powinna zostać. Natychmiast otrzymaliśmy sygnał, że 'teraz na Ukrainie jest inaczej'. Zamiast wycofania zespołu, jeszcze go wzmocniliśmy". Grupa rozrosła się liczebnie do 40 osób, stając się największą tego rodzaju misją amerykańską na świecie. W styczniu 2022 roku amerykańscy specjaliści mieli tam już zająć

„kluczowe pozycje” w sferze działań cybernetycznych.

W terminologii amerykańskiej misje tego rodzaju zwane są hunt forward, czyli myśliwymi. Nakasone mówi o hunt forward operations (operacjach łowieckich). Ich celem jest badanie sieci komputerowych państwa, na terenie którego działają i odnajdywanie ich słabych miejsc, które może wykorzystać przeciwnik.

Od 2018 roku amerykańskie misje tego rodzaju znalazły się w dwudziestu krajach partnerskich – w Europie, na Bliskim Wschodzie i w regionie Azji-Pacyfiku. Nie ma wśród tych państw Francji, Niemiec czy Wielkiej Brytanii. Jak nietrudno zgadnąć, wynika to nie tylko z faktu, że wiele z nich posiada własne systemy cyberbezpieczeństwa, ale również z obaw przed przekazaniem Amerykanom zbyt wielu informacji i tym samym wpływów na ich krajowe sieci.

Eksperci ostrzegają

Rozwijana przez Amerykanów cyberarmia Ukrainy budzi niepokój nie tylko w państwach Ukrainie nieprzychylnych czy krytycznych wobec Waszyngtonu. „Struktura wojsk IT i ich wzrastająca rola tworzy mnóstwo nowych problemów dla społeczności międzynarodowej w sferach, takich jak zastosowanie prawa międzynarodowego w cyberprzestrzeni, normatywne zachowanie krajów, uderzenia w infrastrukturę cywilną, etyka firm sektora IT z siedzibami poza Ukrainą, by wymienić tylko niektóre z nich. Większość, a może nawet wszystkie te kwestie nie dostrzegane są przez środowisko akademickie i kręgi bezpieczeństwa informacyjnego, a także przez decydentów politycznych w krajach członkowskich Unii Europejskiej i NATO” – czytamy w raporcie Centrum Studiów nad Bezpieczeństwem Federalnej Wyższej Szkoły Technologicznej w Zurichu. Problem zauważają na razie tylko szwajcarscy eksperci. Politycy zamykają na niego oczy, kierując się wyłącznie „ukraińską” poprawnością polityczną.

Autorstwo: Mateusz Piskorski
Źródło: MyslPolska.info