Komentarz KBN

Nr 5 (60) / 2020 15 marca 2020 r.

Nowa strategia działań USA w cyberprzestrzeni – potencjalne konsekwencje „obrony wyprzedzającej”

Dominika Dziwisz

W wywiadzie udzielonym 9 stycznia 2020 r. stacji telewizyjnej 13ABC prezydent Donald Trump powiedział, że Stany Zjednoczone są jedynym światowym cybermocarstwem, ale jak do tej pory nie pokazały arsenału swoich możliwości. Zapowiedział, że jeśli USA zostaną zaatakowane w cyberprzestrzeni, odpowiedź będzie dla przeciwnika bardzo bolesna. Ta i inne wypowiedzi amerykańskiego prezydenta pozostają w zgodności z nową wizją działania Dowództwa Cybernetycznego Stanów Zjednoczonych (United States Cyber Command – USCYBERCOM) z 2018 r. oraz aktywną strategią Pentagonu, która została wyrażona w koncepcjach „stałego zaangażowania” (*persistent engagement*) oraz „obrony wyprzedzającej” (*defend forward*).

Donald Trump i zmiana podejścia do cyberobrony

Przed 2018 r., kiedy Biały Dom wydał zgodę na ofensywne operacje w cyberprzestrzeni, USCYBERCOM (utworzone już w 2009 r.) prezentowało postawę defensywną. Opracowana za prezydentury Baracka Obamy Strategia działania w cyberprzestrzeni nie zawierała żadnych zapisów o traktowaniu cyberprzestrzeni jako domeny prowadzenia działań wojennych.

Administracja Donalda Trumpa promuje bardziej zdecydowane podejście i działania ofensywne. 20 września 2018 r. opublikowano pierwszą od 15 lat Narodową Cyberstrategię Stanów

Zjednoczonych. Treść dokumentu wyraźnie wskazuje na zainteresowanie zarówno wojskową cyberobroną, jak i zdolnościami ofensywnymi w obszarach od infrastruktury krytycznej po eksplorację kosmosu i ochronę własności intelektualnej. Nowe zadania Departamentu Obrony i USCYBERCOM najdobitniej opisał doradca ds. bezpieczeństwa narodowego John Bolton: „USA będzie działać ofensywnie, w tym celu będziemy identyfikować, przeciwdziałać, zakłócać, ograniczać i powstrzymywać zachowania w cyberprzestrzeni, które są destabilizujące i sprzeczne z interesami narodowymi". Również w 2018 roku opublikowano cyberstrategię Departamentu Obrony, w której potwierdzono kontynuację „ofensywnego kroku naprzód" w operacjach w cyberprzestrzeni. Jest to szczególnie widoczne w nowej koncepcji doktrynalnej – „obrony wyprzedzającej".

Nowa wizja działania USCYBERCOM

W porównaniu z wcześniejszymi dokumentami, nowa wizja zaprezentowana przez USCYBERCOM pod tytułem „Achieve and Maintain Cyberspace Superiority" jest bardziej spójnym i szczegółowym planem działania w cyberprzestrzeni mającym na celu utrzymanie przewagi USA. To także jawna deklaracja, że Departament Obrony przyjmuje bardziej zdecydowane podejście do ochrony sieci amerykańskich, co stanowi istotną różnicę w stosunku do poprzedniego myślenia o cyberbezpieczeństwie.

Pierwszą zasadniczą zmianą jest uznanie, że większość cyberoperacji celowo pozostaje poniżej progu „zbrojnej agresji", a cyberprzestrzeń jest obszarem nieustannej rywalizacji. W tej „nowej normalności" przeciwnicy rozszerzają swoje wpływy bez uciekania się do fizycznej agresji. Prowokują i zastraszają bez obawy o konsekwencje prawne lub wojskowe. Dlatego administracja Trumpa uznaje, że szczególnie niebezpieczne dla USA są zorganizowane, wyrafinowane kampanie w cyberprzestrzeni podważające amerykańską potęgę dyplomatyczną, gospodarczą i militarną.

Ponadto Departament Obrony podważa skuteczność odstraszania w cyberprzestrzeni. W konsekwencji USCYBERCOM będzie traktować priorytetowo działania ofensywne w celu zakwestionowania zdolności przeciwnika poprzez trwałe, zintegrowane operacje. Ciągłe zaangażowanie zmusza przeciwników, po pierwsze, do zmniejszenia skali i skutków złośliwych działań, bo powstrzymanie lub zapobieganie wszelkim niepożądanym działaniom nie jest możliwe; po drugie, do przesunięcia zasobów w celu obrony i ograniczenia ataków. Podejście do zabezpieczenia interesów narodowych USA poprzez „strategię stałego zaangażowania" oznacza, że USA starają się przewidywać i wykorzystywać słabości przeciwników, jednocześnie podważając ich możliwości ofensywne. Innymi słowy, Stany Zjednoczone będą konsekwentnie prowadzić do konfrontacji z przeciwnikami w cyberprzestrzeni, zamiast czekać, aż ci zaatakują sieci amerykańskie. Jest to także zapowiedź tego, że USCYBERCOM będzie stale badać i sprawdzać zagraniczne sieci w celu wykrycia szkodliwych działań.

Najważniejsza zmiana podejścia do obrony cyberprzestrzeni wiąże się z wprowadzeniem koncepcji „obrony wyprzedzającej", czyli wyjścia obrony poza wyłącznie amerykańskie sieci i zwalczanie zagrożeń zanim dotrą one do USA. Uznano, że wcześniej zbyt często zajmowano się przeciwnikami w sieciach USA, zamiast zatrzymywać ich przed wejściem. Dlatego nowe

podejście pozwala USCYBERCOM na opuszczenie sieci Departamentu Obrony i atakowanie przeciwników w ich własnych sieciach.

Teoria a praktyka działania

Wymienione powyżej koncepcje strategiczne wzbudzają uzasadnione obawy. Zasadnicze pytanie, na które Pentagon nie udzielił dotychczas odpowiedzi sprowadza się do metod realizacji „obrony wyprzedzającej", które mają zmienić zachowanie przeciwnika i utrzymywać napięcie poniżej progu wymuszającego interwencję zbrojną.

Aktualna napięta sytuacja między USA a Iranem może być testem nowych metod działania. Po tym jak 3 stycznia 2020 r. Amerykanie zabili irańskiego generała Kasema Sulejmaniego, eksperci bezpieczeństwa poważnie rozważają możliwość irańskiego odwetu w cyberprzestrzeni. Po atakach z 2010 r. na irańskie instalacje nuklearne z wykorzystaniem robaka komputerowego „Stuxnet", Teheran zaczął intensywnie inwestować w rozwój zdolności do cyberobrony i ataku. Dzisiaj Iran ma na koncie ataki z wykorzystaniem wyrafinowanego arsenału broni cyfrowej i jest powszechnie uznawany za jedno z państw z największymi możliwościami atakowania w cyberprzestrzeni jako piątej domenie operacji militarnych.

Faktem jest, iż Iran nieustannie sprawdza słabości niektórych wrażliwych systemów amerykańskich, a także strategicznych celów regionalnych, jak przedsiębiorstwa naftowe i gazowe w Arabii Saudyjskiej, Zjednoczonych Emiratach Arabskich i Bahrajnie. Sponsoruje także tworzenie złośliwego oprogramowania, które jest stosowane w atakach takich jak „odmowa usługi" (DDoS), czy ransomware, a także kradzież danych uwierzytelniających, ukierunkowanych na niedostatecznie chronione cele przemysłowe i w sektorze publicznym. „Aby przeprowadzić znaczący atak trzeba poświęcić czas i wysiłek, aby go zaprojektować i wykonać perfekcyjnie", mówi Lotem Finkelstein z Cyber Threat Intelligence. Dodaje: „Jeśli Iran kiedykolwiek zaatakuje poprzez cyberprzestrzeń, spodziewamy się, że będzie to w momencie i miejscu, które działają na ich korzyść. Oznacza to, że wszyscy musimy dziś podjąć niezbędne przygotowania".

W ciągu ostatnich miesięcy Biały Dom i Kongres wprowadziły i usprawniły wiele programów, aby pomóc cybersiłom w uprzedzaniu zagrożenia w sieciach na całym świecie. Jeden z zapisów w zeszłorocznym projekcie ustawy o polityce obronnej daje Pentagonowi uprawnienia do działania w zagranicznych sieciach. Wśród wyszczególnionych w projekcie wrogich państw znajduje się Iran, który prowadzi aktywne, systematyczne i ciągłe kampanie ataków na rząd lub ludność USA.

Wnioski

Nowe amerykańskie koncepcje strategiczne są w fazie testowania i wydarzenia najbliższych miesięcy pozwolą ocenić ich skuteczność. Można przypuszczać, że konsekwencje nowej polityki cyberbezpieczeństwa USA mogą być dwojakiego rodzaju.

Pierwszy scenariusz zakłada, że dzięki operacjom w cyberprzestrzeni faktycznie można ograniczyć działania kinetyczne w trzech podstawowych wymiarach prowadzenia wojny, czyli utrzymać je poniżej progu, którego przekroczenie wymuszałoby zastosowanie zbrojnej

odpowiedzi. Można przyjąć, że operacje kinetyczne jedynie utrudniają działanie przeciwnika, a najbardziej dotkliwe w skutkach ataki realizowane są w piątym wymiarze wojennym: cyberprzestrzeni. Każdy bezpośredni cyberatak może doprowadzić do fizycznej reakcji zbrojnej. Zatem dużo bardziej prawdopodobne są subtelniejsze ataki, trudne do przypisania konkretnemu krajowi. W tym scenariuszu eskalacja konfliktu jest eskalacją działań w cyberprzestrzeni. Siły kinetyczne, nadal, pozostają w odwodzie. Taka ścieżka daje czas na niezbędne negocjacje, zanim zgodnie z obserwacją Clausewitza państwa przejdą do kontynuowania polityki innymi środkami.

Alternatywny scenariusz przewiduje, że amerykańska „obrona wyprzedzająca" spotka się ze zdecydowaną, kinetyczną odpowiedzią wrogiego kraju. Obecnie trudno sobie wyobrazić jakiekolwiek państwo wypowiadające konwencjonalną wojnę Stanom Zjednoczonym Ameryki. W dobie gospodarki opartej na wiedzy, a nie na surowcach, żaden liczący się kraj nie jest zainteresowany zagarnięciem chociażby Alaski. Tym niemniej, obserwujemy wzrost znaczenia wojen hybrydowych. Są one nastawione na osiągnięcie pewnych celów politycznych, a takim może być zniechęcenie USA do podejmowania działań w cyberprzestrzeni. I choć sama cyberprzestrzeń odgrywa w nich ważną rolę, jest tylko jednym z obszarów prowadzenia działań. Zaangażowane są również środki konwencjonalne. W wypadku takiego rozwoju wydarzeń pozostajemy już tylko o krok od rozpoczęcia konfliktu w każdym wymiarze wojennym. Dlatego Departament Obrony powinien włożyć więcej pracy w zrozumienie, jakie rodzaje celów lub efektów ataków mogą przypadkowo doprowadzić do eskalacji konfliktu poza cyberprzestrzeń.

„Obrona wyprzedzająca" daje nadzieję na to, że pewna część konfliktów zostanie przeniesiona w piątą domenę prowadzenia wojny. Działania tam przeprowadzane zwykle nie zagrażają bezpośrednio życiu ludzkiemu. Efektywność tej strategii zależy od tego, jak dobrze Departament Obrony przygotuje się do tego zadania.