Cyberdefence 24

aut. Tomasz Fastyn 28.03.2017

NATO I KANADA BUDUJĄ STRATEGIĘ CYBEROBRONY WSCHODNIEJ FLANKI

Wojska kanadyjskie, które rozpoczną niedługo stacjonowanie na Łotwie w ramach misji NATO, rozlokują też na wschodniej flance pododdziały specjalizujące się w walce w cyberprzestrzeni. Jak pisze SC Magazine, Sojusz Północnoatlantycki zamierza jasno określić granice działań innych krajów i charakter odpowiedzi na cyberataki.

W najbliższych tygodniach jednostki kanadyjskiego wojska, które pojawią się na terytorium Łotwy w ramach obrony wschodniej flanki przez sojusznicze armie NATO, będą wzmacniać nie tylko potencjał konwencjonalny, ale też cybernetyczny. Mimo uznania przez wszystkie kraje Paktu Północnoatlantyckiego cyberprzestrzeni jako kolejnego obszaru działań wojskowych, nie ma nadal jednej strategii reakcji na ataki hakerów.

Zgodnie z informacjami przekazanymi przez Paula Rutherforda, dowódcy połączonego komponentu cyberbezpieczeństwa (Joint Forces Cyber-Component – z ang.) za pośrednictwem CBC NEWS wraz z pododdziałami zmechanizowanymi, na Łotwie pojawią się te odpowiedzialne za działania w cyberprzestrzeni. Komentatorzy wskazują, że jednostki NATO będą skupiać się na działaniach defensywnych i ochronnych, natomiast środki ofensywne będą co najmniej ograniczone.

Podjęcie kontrakcji o charakterze ofensywnym byłoby możliwe przede wszystkim w wypadku niebezpiecznego ataku hakerskiego na dużą skalę (np. bezpośrednio zakłócającego systemy wojskowe). Oprócz tego należałoby jednak określić z całą pewnością, kto jest sprawcą włamania czy zakłócania. W chwili działania hakerów na ogół nie wiadomo kto za nie dokładnie odpowiada, cyberprzestępcy maskują swój ruch za pomocą licznych i różnorakich serwerów proxy. W dodatku wojsko nie zawsze jest w stanie zweryfikować, czy atakujący działał jedynie kierując się chęcią zysku, czy na polecenie administracji państwowej.

Część komentatorów wskazuje, że m.in. dzięki działaniom na wschodniej flance i zdobywanym cały czas doświadczeniom NATO zdoła opracować strategię odpowiedzi na działania rosyjskich hakerów. Jednym z rozwiązań, które mogłyby potencjalnie zostać wzięte pod uwagę jest prowadzenie ataków „hack back", czyli ataku cybernetycznego na urządzenie z którego dokonano ataku. To do pewnego stopnia rozwiązuje problem rozpoznania źródła zagrożenia, aczkolwiek jak na razie nie ma oficjalnych sygnałów o podejmowaniu tego typu kroków w ramach NATO.

Innym istotnym elementem powinno być prowadzenie aktywnych działań informacyjnych - otwarte demaskowanie kłamstw, a być może także pokazywanie korupcji i błędów władz potencjalnego przeciwnika. Z drugiej strony, problemem dla NATO prawdopodobnie będzie różny stopień woli poszczególnych państw członkowskich do podejmowania zdecydowanych działań ofensywnych (tak samo, jak w wypadku operacji konwencjonalnych).

Czytaj też: USA: Ogromny wyciek danych z Pentagonu