PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 68 (1305), 10 lipca 2015 © PISM

Polityka NATO w cyberprzestrzeni: obrona i odstraszanie

Artur Kacprzyk

Wobec narastających zagrożeń w cyberprzestrzeni NATO przyjęło na szczycie w Walii przełomową deklarację o możliwości przywołania art. 5 w razie najpoważniejszych cyberataków. W związku z nadchodzącym szczytem w Warszawie implementacja wzmocnionej polityki cyberobrony wymaga jednak nie tylko określenia form i sposobów wspólnej reakcji na różne rodzaje cyberataków, lecz także wzmocnienia zdolności obronnych samych sojuszników i dalszego rozwijania narzędzi NATO służących temu celowi.

Zagrożenia w cyberprzestrzeni. Ataki w cyberprzestrzeni stają się coraz liczniejsze i bardziej zaawansowane. Większość włamań do systemów NATO i sieci rządowych to obecnie akty cyberszpiegostwa, ukierunkowanego głównie na pozyskiwanie informacji, tak jak odkryta w kwietniu br. kradzież danych ok. 4 mln pracowników federalnych USA z bazy Rządowej Agencji ds. Personelu (OPM). Również w kwietniu potwierdzono kradzież 5 mln dolarów z konta linii lotniczych Ryan Air, co stanowi przykład działalności motywowanych finansowo grup cyberprzestępczych, regularnie atakujących sektor prywatny i osoby indywidualne. Powszechne są też akty cyberwandalizmu (m.in. blokowanie dostępu do stron internetowych, zmiana ich treści, niszczenie danych), dokonywane przez indywidualnych hakerów oraz grupy sympatyzujące lub współpracujące z państwami czy organizacjami terrorystycznymi. Przykładowo, w styczniu br. hakerzy zamieścili materiały propagandowe Państwa Islamskiego na kontach społecznościowych Centralnego Dowództwa (CENTCOM) USA, kierującego operacjami militarnymi na Bliskim Wschodzie.

W przyszłości destrukcyjne cyberataki mogą jednak posłużyć także do zdestabilizowania czy zastraszenia krajów NATO w czasie pokoju lub do wsparcia działań militarnych przeciwko Sojuszowi. Zdolności tego typu rozwijają potencjalni przeciwnicy NATO, m.in. Rosja i Iran, a konflikty w Gruzji (2008) i na Ukrainie (2014–2015) świadczą o postępującej koordynacji operacji wirtualnych i konwencjonalnych. Głównymi celami najdotkliwszych ataków byłyby sieci wojskowe i systemy cywilnej infrastruktury krytycznej. Przejęcie nad nimi kontroli lub usunięcie i zmanipulowanie danych może sparaliżować systemy dowodzenia i łączności, czy też pozbawić społeczeństwa dostępu do usług sektora energetycznego, finansowego i telekomunikacyjnego.

Choć do tej pory nie odnotowano ataków skutkujących paraliżem najistotniejszych dla państwa sektorów, stratami w ludziach czy rozległymi zniszczeniami fizycznymi, to środki potrzebne do tego rodzaju działań stają się coraz bardziej zaawansowane. Świadczą o tym doniesienia o paraliżu syryjskiej obrony przeciwlotniczej przez izraelski cyberatak przed nalotem na reaktor jądrowy al-Kibar w 2007 r. czy usunięcie danych z 30 tys. komputerów firmy naftowej Aramco, ujawniające luki w systemach infrastruktury krytycznej Arabii Saudyjskiej. Przykładem istnienia „cyberbroni" jest zwłaszcza robak Stuxnet, który został użyty przeciwko irańskiemu ośrodkowi atomowemu Natanz i rzekomo zniszczył ok. 1000 wirówek do wzbogacania uranu.

Trudne początki cyberobrony NATO. Głównym zadaniem NATO jest ochrona własnych sieci informatycznych oraz wsparcie sojuszników w budowie narodowych zdolności cyberobrony, służących zabezpieczeniu sieci, wykrywaniu ataków, zapewnieniu funkcjonowania sieci w razie ataku, oraz przywróceniu sprawności systemów po włamaniach. Wsparcie NATO polega m.in. na ułatwianiu wymiany dobrych praktyk i informacji, ustalaniu wspólnych standardów ochrony sieci krajowych o kluczowym znaczeniu dla realizacji operacji NATO i na organizacji cyberćwiczeń. W zakresie obrony własnych sieci Sojusz podejmował działania jeszcze przed przyjęciem pierwszej polityki cyberobrony

NATO z 2008 r., powołując w 2002 r. Zespół Reagowania na Incydenty Komputerowe (NCIRC), który osiągnął pełną zdolność operacyjną w 2014 r. W 2012 r., rok po uaktualnieniu polityki cyberobrony, ustanowiono też dwa sześcioosobowe zespoły szybkiego reagowania (RRT), które mogą być rozmieszczane za zgodą Rady Północnoatlantyckiej w celu wsparcia krajów będących obiektem poważnych ataków.

Przyjęta na szczycie w Walii we wrześniu 2014 r. wzmocniona polityka cyberobrony wciąż zakłada, że za ochronę sieci narodowych odpowiedzialni są sami sojusznicy, jednak mogą liczyć na szersze niż do tej pory wsparcie NATO. Jest ono konieczne, gdyż wiele krajów, zwłaszcza mniejszych, nie rozwinęło odpowiednich zdolności ze względu na redukcję budżetów obronnych i brak zaplecza eksperckiego. Z kolei niechęć największych sojuszników do przekazywania poufnych informacji (nt. oceny zagrożeń i posiadanych zdolności) utrudnia przygotowanie do współdziałania w trakcie kryzysu, w tym kompleksowe włączenie działań cyberobrony do planów operacji obrony terytorialnej i reagowania kryzysowego.

Dlatego nowa polityka kładzie nacisk na zintensyfikowane ćwiczenia z wykorzystaniem wirtualnego poligonu w Estonii, służące budowie sojuszniczego zaufania i interoperacyjności. Wzmocnieniu ma ulec pomoc konsultacyjna i edukacyjna, m.in. ze strony Centrum Doskonalenia Obrony Cybernetycznej (CCD CoE) w Tallinie. NATO ustala także cele rozwoju środków cyberobronnych państw członkowskich w ramach procesu planowania obronnego. Za obiecujący sygnał należy uznać rozpoczęcie przez trzy grupy państw prac nad wspólnymi zdolnościami w ramach projektów inicjatywy Smart Defence: platformy wymiany informacji nt. złośliwego oprogramowania (MISP), rozwoju wielonarodowych zdolności cyberobrony (MN CD2) oraz edukacji i szkolenia (MN CD E&T).

Nowe priorytety NATO obejmują też ściślejszą współpracę z partnerami międzynarodowymi, zwłaszcza z UE, która rozwija własną politykę cyberbezpieczeństwa. Istotne znaczenie będzie również miała wzmocniona kooperacja z sektorem przemysłowym w ramach rozpoczętej we wrześniu 2014 r. inicjatywy NICP (NATO Industrial Cyber Partnership). Jej realizacja jest ważna pod kątem opracowania nowych zdolności cyberobronnych dla NATO, ale też ze względu na to, że to firmy prywatne są operatorami znacznej części infrastruktury krytycznej. Stąd niezbędne jest przygotowanie do współdziałania w razie ataków (m.in. poprzez wymianę informacji o zagrożeniach).

Problemy odstraszania w cyberprzestrzeni. Rozwijane przez NATO zdolności cyberobrony stanowią również środek odstraszania, ponieważ mogą przekonać agresora, że atak będzie nieskuteczny (tzw. *deterrence by denial*). Jednak wielu sojusznikom brak odpowiednich zdolności defensywnych, dlatego potencjalni agresorzy wciąż mogą zdecydować się na uderzenie, którego ewentualne niepowodzenie nie będzie miało dla nich poważnych konsekwencji. Dzięki deklaracji, że cyberatak może uruchomić wspólną reakcję NATO, Sojusz wzmacnia zatem drugą formę odstraszania, tzw. odstraszanie przez odwet (*deterrence by punishment*), aby przekonać przeciwników, że nawet udany atak spotka się z dotkliwą odpowiedzią.

Deklaracja walijska nie definiuje jednak jasno, jak dotkliwy cyberatak doprowadzi do uruchomienia artykułu 5 i zaznacza, że decyzja o zbiorowej odpowiedzi będzie podejmowana przez Radę Atlantycką w zależności od danego przypadku (*case by case*). Wskazuje także, że skutki cyberataków mogą być porównywalne do efektów uderzeń konwencjonalnych. To sformułowanie jedynie sugeruje, że NATO zareaguje na straty ludzkie i zniszczenia fizyczne, pozostawia zatem jeszcze większe wątpliwości co do możliwości reakcji na uderzenie o poważnych konsekwencjach w sferze wirtualnej (jak paraliż systemu bankowego).

Niejasność polityki odstraszania w domenie cyberprzestrzeni jest jednak logicznym krokiem Sojuszu, mającym na celu utrzymanie nieprzyjaciół w niepewności co do tego, czy zareaguje on na ich działania. Przyjęcie określonego progu odpowiedzi mogłoby zasygnalizować sprawcom mniej dotkliwych ataków, że pozostaną bezkarni. Poza tym, odpowiedź na agresję wymaga ustalenia sprawcy, który będzie starał się ukryć swój udział. W części przypadków źródło ataku może być jasne, zwłaszcza że tylko państwa dysponują zapleczem ludzkim i materialnym niezbędnym do przeprowadzenia najbardziej destrukcyjnych uderzeń, które nastąpiłyby najprawdopodobniej podczas poważnych napięć politycznych. Niewykluczone jednak, że w niektórych sytuacjach kraje NATO nie będą miały pewności, czy ataku dokonało dane państwo, czy np. sympatyzujący z nim hakerzy.

Sojusznicy powinni zatem nie tyle zmieniać treści polityki odstraszania, ile określić swoistą wewnętrzną doktrynę cyberobrony, ustalając, jakie ataki muszą wywołać odpowiedź NATO i jaka będzie jej forma. Państwa najprawdopodobniej nie będą skłonne do użycia sił konwencjonalnych, jeśli cyberatak nie doprowadzi do rozległych zniszczeń fizycznych i strat ludzkich. Sposobem odpowiedzi na mniej dotkliwe, ale wciąż poważne ataki mogą być działania cyberofensywne, polegające na wtargnięciu do sieci agresora w celu sparaliżowania lub uszkodzenia systemów będących źródłem zagrożenia czy innych zasobów informatycznych. Jednak stworzenie wspólnych sił cyberofensywnych NATO nie jest możliwe, ponieważ wiązałoby się ono z kontrowersjami prawnymi (m.in. zdolności cyberofensywne mogą zostać wykorzystane w potajemnych operacjach militarnych, a skutki użycia siły w cyberprzestrzeni mogą dotknąć także systemy niebędące celem ataków, prowadząc do niekontrolowanych i nieproporcjonalnych zniszczeń) i niechęcią państw do udostępniania tajnych i kosztownych technologii cyberofensywnych. Niemniej liczne kraje Sojuszu posiadają i rozwijają takie środki, zwłaszcza USA, których cyberstrategia oficjalnie pozwala na prowadzenie działań ofensywnych. NATO powinno więc rozpocząć dialog o możliwościach i mechanizmach użycia sił cyberofensywnych przez poszczególne kraje w ramach obrony zbiorowej, chociaż priorytetem musi pozostać budowa zdolności obronnych. Odstraszanie nie powstrzyma bowiem wielu ataków o mniejszej skali – wandalizmu, przestępczości czy szpiegostwa – ani większych działań podczas otwartego konfliktu zbrojnego.