aut. Andrzej Kozłowski 13.07.2018

CYBERBEZPIECZEŃSTWO CORAZ MNIEJ WAŻNE DLA NATO? [ANALIZA]

Zgodnie z prognozami szczyt NATO nie przyniósł zaskakujących zmian w polityce bezpieczeństwa Sojuszu w cyberprzestrzeni. Tak jak oczekiwano, potwierdzono ustalenia poprzednich szczytów – w Newport i Warszawie oraz poinformowano o konieczności dalszej integracji działań w środowisku wirtualnym z operacjami prowadzonymi na lądzie, morzu, w powietrzu i przestrzeni kosmicznej. W deklaracji końcowej potwierdzono również utworzenie Dowództwa NATO ds. Operacji w Cyberprzestrzeni. Zaskakująco niewiele powiedziano jednak o cyberbezpieczeństwie w porównaniu do szczytów w Wali i Polsce.

W każdej deklaracji ze szczytu NATO, wymienia się zagrożenia z którymi Sojusz musi się mierzyć. W Brukseli uznano, że do głównych problemów bezpieczeństwa zaliczyć można m.in. cyberataki, wojnę hybrydową oraz kampanie dezinformacyjne. Podkreślono również niestabilność środowiska bezpieczeństwa oraz brak możliwości przewidzenia nadchodzących zmian. Zaakcentowano rosnące zagrożenie ze strony aktorów niepaństwowych, szczególnie płynące z cyberprzestrzeni. Te sformułowania nie powinny dziwić, poprawnie identyfikują najważniejsze zmiany w środowisku bezpieczeństwa. Bez właściwego rozpoznania zagrożeń, trudno mówić o skutecznym i efektywnym ich przeciwdziałaniu.

NATO zapowiedziało również podjęcie konkretnych działań w środowisku wirtualnym. Jednym z nich jest usprawnienie mechanizmu wczesnego wykrywania zagrożeń oraz usprawnienie procesu dzielenia się danymi wywiadowczymi w obszarze zagrożeń w środowisku wirtualnym. Nie ma ważniejszej kwestii w cyberprzestrzeni niż wymiana informacji oraz szybkość wykrywanie zagrożeń, najlepiej zanim zdąża się one rozprzestrzenić i zainfekować znaczną liczbę sieci i systemów.

W deklaracji końcowej podkreślono również, że cyberataki są coraz częstsze, bardziej zaawansowane oraz niszczycielskie. NATO będzie kontynuowało proces przygotowania się do działania w tym, wciąż nowym środowisku bezpieczeństwa, w którym ataki dokonywane są zarówno przez państwa jak i aktorów niepaństwowych. Podkreślono również, że cyberobrona jest nieodłącznym elementem kolektywnej obrony Sojuszu. NATO musi również z taką sama efektywność działać w cyberprzestrzeni jak na lądzie, w powietrzu i morzu oraz wzmocnić odstraszanie w przestrzeni wirtualnej.

Członkowie Sojuszu zgodzili się zintegrować swoje krajowe zasoby w cyberprzestrzeni z operacjami i misjami NATO. Potwierdzono również wykorzystanie wszystkich zdolności, w tym w cyberprzestrzeni do odstraszania, obrony oraz przeciwdziałania wszystkim rodzajom cyberataków. Zapis ten jest efektem uznania cyberprzestrzeni za pełnoprawne środowisko prowadzenia działań wojennych i wynikająca z tego konieczność dostosowania własnych zasobów i zdolności do działania w nim.

W deklaracji potwierdzono również, kontynuowanie prac nad rozwojem środków, które zwiększą skuteczność identyfikacji napastników oraz pozwolą wprowadzić środki, które będą ich odstraszały. Podkreślono też, że członkowie Sojuszu mogą wskazywać publicznie państwa, które stoją za

cyberatakami oraz odpowiadać na niej w zorganizowany i skoordynowany sposób. Zaznaczano, jednak że atrybucja pozostanie prerogatywą państw członkowskich. Punkt też odwołuje się do działań Stanów Zjednoczonych i Wielkiej Brytanii, które to publicznie oskarżały państwa odpowiednio: Rosję i Koree Północną o dokonywanie cyberataków.

W Brukseli odniesiono się również do kontynuowania i pełnej implementacji Cyber Defence Pledge, czyli wzmocnienia zdolności w cyberprzestrzeni każdego z państwa. Jest to niezwykle istotne w celu wzmocnienia odporności (resilience), która jest postrzegana w Sojuszu jako kluczowa oraz podniesienia kosztów cyberataku. Zapis ten wskazuje na próby wprowadzenia elementów doktryny odstraszania w środowisku wirtualnym.

NATO potwierdziło również zobowiązania do działania w cyberprzestrzeni zgodnie z obowiązującymi prawem międzynarodowymi i zapisami wynikającymi z karty Narodów Zjednoczonych. Sojusz zamierza również uczestniczyć w pracach nad utrzymaniem pokoju w środowisku wirtualnym oraz zwiększenia bezpieczeństwa w cyberprzestrzeni poprzez działania ukierunkowane na promowanie stabilności i zmniejszenie ryzyka wybuchu konfliktu. Praktycznie wszystkie państwa NATO podzielają pogląd, że obecne prawo międzynarodowe, a w szczególności prawo konfliktów zbrojnych może być stosowane w cyberprzestrzeni. Dlatego zapis ten nie jest żadną niespodzianką tylko potwierdzeniem pozycji na której stoi NATO od samego początku .

Zapowiedziano również dalszy rozwój współpracy z przemysłem oraz światem nauki ze wszystkich państw Sojuszu w celu utrzymania przewagi technologicznej oraz wprowadzania innowacji. Nie określono jednak czy chodzi o program NATO Industry Cyber Partnership czy o coś nowego. Zarówno sektor prywatny jak i świat nauki jest absolutnie kluczowy w cyberprzestrzeni, dlatego zwiększenie współpracy jest niezwykle ważne.

Jedną z oczekiwanych decyzji było ogłoszenie stworzenia Centrum Operacji w Cyberprzestrzeni z siedzibą w Brukseli. Celem tej instytucji będzie koordynacja działań operacyjnych NATO w cybeprzestrzeni oraz budowanie tzw. świadomości sytuacyjnej. O tym pomyśle, mówił wcześniej sekretarz stanu Jens Stoltenberg oraz dyskutowali ministrowie obrony państw NATO podczas spotkania w Brukseli w maju. Szef sekcji cyberobrony Sojuszu Północnoatlantyckiego Christian-Marc Liflände r w wywiadzie dla Cyberdefence24.pl argumentował, że powołanie tej struktury stanowi odpowiedź na deklarację ze szczytu w Warszawie, podczas którego NATO uznało cyberprzestrzeń za kolejną sferę działań operacyjnych. Sojusz zamierza realizować cyberobronę nie tylko z perspektywy technicznej czy obrony sieciowej, lecz i z punktu widzenia zabezpieczenie własnych misji w tym obszarze. Zdaniem Liflände ra Sojusz musi przejść z zabezpieczenia informacji do zabezpieczenia misji. Innymi słowy od ochrony informacji technicznych do możliwości operowania w tej sferze. Oznacza to również, że istotne zmiany muszą zostać wprowadzone w strukturze organizacyjnej.

Kwestie cyberbezpieczeństwa włączono równie do pomocy Tunezji i Jordanii. Zapis ten jest przejawem rosnącego znaczenia cyberbezpieczeństwa dla sił zbrojnych a pomoc w zwiększeniu ochrony systemów i sieci jest obecnie standardowym elementem pomocy wojskowej.

Tekst deklaracji nie zaskakuje i pokrywa się z tym o czym pisałem w prognozie dotyczącej szczytu NATO. W tekście końcowym nie znalazły się propozycje amerykańskich ekspertów z Center for a New American Security (CNAS), co akurat nie powinno dziwić. Szanse, że NATO sięgnie po ich rady były niewielkie.

Bardziej zaskakujący jest brak w deklaracji zapisów o współpracy z Unią Europejską w obszarze cyberbezpieczeństwa. Ten ważny element poprzedniego szczytu w Warszawie został tu pominięty, co jest o tyle dziwne, ponieważ obie instytucje coraz bliżej ze sobą współpracują i podobnie rozumieją problem.

Analiza deklaracji szczytu pozwala dojść do wniosku, że rola cyberbezpieczeństwa dla NATO maleje. Nic bardziej mylnego. Po prostu zmienił się nacisk z głośnych i szeroko komentowanych decyzji politycznych na wdrażanie zmian operacyjnych oraz na szczeblu taktycznym, które nie są opisywane w deklaracjach NATO ze szczytu