aut. Andrzej Kozłowski 28.02.2018

WSPÓŁPRACA NATO I UE INTENSYWNIE SIĘ ROZWIJA (CSBXL18)

27 lutego w Brukseli podczas CYBERSEC – Brussels Leaders Foresight odbył się panel zatytułowany Defence Stream: EU and NATO Cyber Affairs – Joint Transatlantic Effort in Cyberdefence. Moderatorem był komandor porucznik Wiesław Goździewicz, a w dyskusji wzięli udział: Urmas Paet – członek Parlamentu Europejskiego, autor raportu poświęconego cyberobronie, ambasador Sorin Ducaru były asystent sekretarza generalnego ds. nowych wyzwań bezpieczeństwa w NATO, George Sharkov z Ministerstwa Obrony Bułgarii, Diana Kelley z Microsoftu i Thomas Goodman z Raytheona.

Komandor Goździewicz rozpoczął prezentację od przypomnienia głównych decyzji podjętych przez NATO w obszarze cyberbezpieczeństwa. Pierwszy raz dyskutowano o tym problemie w Bukareszcie w 2007 roku po ataku na Estonię. Przełomowy był jednak szczyt w 2014 w Walii, kiedy NATO stwierdziło, że cyberatak może zostać uznany za atak zbrojny oraz, że prawo konfliktów zbrojnych ma zastosowanie do cyberprzestrzeni. W 2016 roku w Warszawie uznano cyberprzestrzeń za kolejną domeną operacyjną NATO, która musi być broniona z taką samą skutecznością jak morze, ląd i powietrze. Stworzono również mechanizm Cyber Defence Pledge, który umożliwia ocenienie postępów poszczególnych państw w obszarze cyberbezpieczeństwa. Postanowiono również o podpisaniu deklaracji o współpracy strategicznej między Unią Europejską a NATO w odniesieniu do obszaru cyberbezpieczeństwa i zagrożeń hybrydowych. NATO i UE podpisały również porozumienie o współpracy technicznej pomiędzy CERTami.

Goździewicz przypomniał, że w listopadzie ministrowie obrony państw NATO postanowili o stworzeniu Centrum Operacji NATO w Cyberprzestrzeni (NATO's Cyber Operations Center). Pierwszy raz od czasu szczytu w Lizbonie państwa Sojuszu zdecydowały o rozbudowie struktury dowódczej w celu walki z cyberzagrożeniami. Postanowiono również, że Sojusz powinien zintegrować zdolności w cyberprzestrzeni z planowaniem wspólnych operacji (Joint Operation NATO). Ostatnio podczas spotkania w bazie sił lotniczych w Rammstein jednym z głównych tematów dyskusji były zasady angażowania się w operacje w cyberprzestrzeni oraz w jaki sposób integrować je z tradycyjnymi zdolnościami. Na szczycie w maju prawdopodobnie dojdzie do potwierdzenia postanowień szczytu z Walii i Warszawie oraz będzie to okazja do pierwszego przeglądu w ramach Cyber Defence Pledge. Po tym wstępie komandor porucznik zadał pytanie o przyszłość współpracy w obszarze cyberprzestrzeni między UE a NATO.

Jako pierwszy odpowiedział na nie Urmas Paet, który powiedział, że współpraca pomiędzy obiema instytucjami cały czasy się rozwija. Początkowo nie było wspólnego zrozumienia problemu, ale to uległo zmianie. Z pewnością krokiem naprzód będzie utworzenie wspólnych struktury obronnych, które nie mogą funkcjonować bez cyberobrony.

Ambasador Sorin Ducaru przypomniał o porozumieniu na mocy, którego obie organizacje wymieniają dane wywiadowcze, z dużym naciskiem na informacje dotyczące zagrożeń w cyberprzestrzeni. Z

pewnością trzeba wzmocnić współpracę jeśli chodzi o reagowania kryzysowe. NATO ma swój własny mechanizm, który corocznie sprawdza na ćwiczenia. W ostatnich brali przedstawiciele Unii Europejskiej. Z pewnością rozwinięcie Cyber Tool Box jest pozytywnym sygnałem i przyczyni się do usprawnienia współpracy.

George Sharkov z bułgarskiego ministerstwa obrony podkreślił, że cyberbezpieczeństwo jest jednym z głównych priorytetów prezydencji jego kraju w Radzie UE. Zwrócił on uwagę na kwestie współpracy publiczno-prywatnej, cyber higieny oraz utworzenia minimalnych wymagań odnośnie cyberbezpieczeństwa. Dobrym krokiem w tym kierunku może być dyrektywa NIS. Podkreślił, też istnieje różnych graczy w sektorze prywatnym i fakt, że zbyt często uwaga skupia się tylko na największych przedsiębiorstwach. Przytoczył atak NotPetya, który skierowany był na małą firmę na Ukrainie odpowiedzialną ze usług podatkowej. Małe i średnie przedsiębiorstwa są o wiele bardziej podatne. Kończąc swoją wypowiedź Skarkov zarekomendował utworzenie wstępnego planu wspólnego reagowania UE i NATO na incydenty i sytuacje kryzysowe. Przedstawiciel bułgarskiego MONu zwrócił uwagę na fakt, że infrastruktura krytyczna nie jest zarządzana przez ministerstwa obrony i dlatego NATO nie może zajmować się jej ochroną i tutaj pojawia się szansa dla Unii Europejskiej.

Diana Kelley z Microsoftu podkreślała konieczność dzielenia się informacjami o znalezionych podatnościach. Nie może być takie sytuacji – jej zdaniem, że rządy wykorzystuję luki w oprogramowaniu jako potencjalną broń i nie informują producentów oprogramowania. Thomas Goodman z Raytheona dodał, że najważniejsza jest odporność na ataki oraz odpowiednie przygotowanie.

Komandor porucznik Goździewicz zadał pytanie do Urmasa Peata o treść raportu, który obecnie przygotowuje dla Parlamentu Europejskiego poświęconego cyberbezpieczeństwu. Raport obecnie oczekuje na opinie i komentarze ze stronnych innych grup politycznych. Powinien zostać poddany pod głosowanie i przyjęty w czerwcu. Jest jasnym sygnałem dla klasy politycznej, że cyberbezpieczeństwo jest ważnym aktualnym, problemem, który jest dyskutowany Dokument zwraca m.in. uwagę na dyplomację publiczną w obszarze cyberprzestrzeni, konieczność otwartości na sektor prywatny, bez którego pełnej współpracy nie będzie możliwe zbudowanie efektywnego i skutecznego systemu cyberbezpieczeństwa. Konieczna jest również współpraca międzyinstytucjonalna. Ostrzegał, że najpoważniejsze cyberataki mogą zakończyć się śmiercią ludzi. Niestety współpraca między pojedynczymi krajami jest trudna, a co dopiero kooperacja w ramach całej UE czy poza nią.

Ostatnią dyskutowaną kwestią jest rola technologii chmurowych. Przedstawicielka Microsoftu wymieniła liczne zalety jej stosowania . Podkreśliła też, że należy zwracać uwagę na jej odporność na ataki. Tego problemu dotyczyło też pytanie z publiczności od przedstawiciela Ministerstwa Obrony Belgii, który zapytał czy atakowanie serwerów Microsoftu, na których znajduje się chmura NATO, jest legalne. Komandor porucznik Goździewicz powiedział, że w momencie kiedy obiekty cywilne są wykorzystywane przez wojskowych tracą swoją ochronę w prawie konfliktów zbrojnych i mogą stać się celem ataków, które są legalne w świetle prawa międzynarodowego.

Na sam koniec Ambasador Ducaru powiedział, że największym problemem dowódców na polu walki nie jest brak informacji, ale fakt, że nie można im ufać. Potrzebne jest wykorzystanie algorytmów AI w celu sprawdzenia prawdziwości danych.

Organizatorem wydarzenia był Instytut Kościuszki.