**aut. Andrzej Kozłowski** 27.02.2018

# NATO POTRZEBUJE INTEGRACJI ZDOLNOŚCI W CYBERPRZESTRZENI (CSBXL18)

**27 lutego w Brukseli podczas CYBERSEC – Brussels Leaders Foresight miała miejsce rozmowa pomiędzy ambasadorem Sorinem Ducaru, który był asystentem sekretarza generalnego ds. nowych wyzwań bezpieczeństwa w NATO i Jamie Shea, który obecnie kieruje pracami Kwatery Głównej, związanymi z nowymi zagrożeniami dla bezpieczeństwa. Tematem rozmowy była gotowość NATO do walki z zagrożeniami w cyberprzestrzeni.**

**Ambasador Sorin Ducaru: Jak zmieniał się krajobraz zagrożeń?**

Jamie Shea: Pierwszy raz z zagrożeniami w cyberprzestrzeni mieliśmy do czynienia podczas wojny w Kosowie, kiedy hakerzy przypuścili ataki na strony internetowe Sojuszu. Obecnie poziom zagrożeń jest o wiele większy i obejmuje systemy uzbrojenia, ochronę wrażliwych danych itp.

**Ostatnio byliśmy świadkami publicznej atrybucji ataków NotPetya i WannaCry przez kilka państw.**

Ataki pokazują wielką siatkę światowych połączeń i współzależności. WannaCry niezwykle szybko zainfekował wiele komputerów z ponad 100 państw na całym świecie.

Niestety problemem jest, że publiczne instytucje używają starego oprogramowania. Nie mają żadnej strategii czy budżetu na modernizację. NotPetya był ukierunkowany na paraliż ukraińskiego systemu podatkowego, ale byliśmy świadkami tego, że konsekwencje były światowe, a przypadkowymi ofiarami firmy z innych państw.

**Jak ważna jest atrybucja polityczna? Przed 2016 rokiem była bardzo rzadko stosowana. Dlaczego więcej członków NATO publicznie nie przypisuje ataków do konkretnych państw?**

Publicznie przypisując ataki podważamy kulturę bezkarności za cyberataki. Służby wywiadowcze są stanie przypisać ataki do konkretnego kraju. W przypadku NotPetya potrzebne było 6 miesięcy pracy wywiadowczej żeby zebrać dowody i wskazać sprawcę. Wcześniej unikano publicznej atrybucji ataków, ponieważ załatwiano sprawy po cichu, żeby nie eskalować napięcia na arenie międzynarodowej.

NotPetya był przykładem bardzo dobrej współpracy wywiadowczej i to nie tylko między państwami NATO. Musimy pamiętać, że Sojusz nie ma własnych zdolności wywiadowczych. Polega w tym obszarze jak i innych sferach na zdolnościach poszczególnych państwa. Atrybucja ataków polega na zastosowaniu środków odstraszających i nie tylko w cyberprzestrzeni.

**Jaka jest świadomość sytuacyjna w NATO?**

Na początku byliśmy dobrzy w analizie cyberataków kilka tygodniu po ich wykryciu. Nie byliśmy w stanie ich przewidywać. Obecnie utworzyliśmy nowe komórki w NATO w celu szybszego przekazywania informacji. W cyberprzestrzeni opieramy bardziej niż w innych obszarach na zewnętrznych źródłach informacjach. Przykładowo UE może wcześniej wykryć ataki i dzięki współpracy my również możemy się o tym dowiedzieć. Bardzo dobrą inicjatywa jest NATO Industry Cyber Partnership, która była bardzo użyteczna w trakcie NotPetya. Dzięki temu otrzymujemy informacje z różnych źródeł.

**Jak NATO radzi sobie z pozyskiwanie nowych technologii, rozwijaniem zdolności oraz procedurami zamówień?**

W cyberprzestrzeni mamy 4 główne czynniki, które decydują o jakości i skuteczności: ludzi, procesy, technologie i władze i musimy je odpowiednio zintegrować. Z wykształcenia jestem historykiem i lubię odwoływać się do przykładu z 1940 roku, kiedy Niemcy pokonały Francję. Nie dlatego, że mieli lepszą technologię czy większą armię, ale dlatego, że lepiej zintegrowali swoje siły zbrojne. Podobnie sytuacja wygląda w cyberprzestrzeni, jeżeli mamy świetną technologię, ale słabych ludzi to nie będziemy skuteczni i odwrotnie.

Odnośnie procedur zamówień i kupowania nowego sprzętu. W przypadku klasycznego uzbrojenia jak czołgi i samoloty, zakup dokonywany jest na 20- 30 lat. Jest to niemożliwe w odniesieniu do technologii IT.

**Jak państwa są przygotowane do wypełniania zobowiązań wynikających z CyberDefence Pledge. Następny szczyt NATO, który będzie miał miejsce w maju 2018 wydaję się perfekcyjnym miejscem, żeby dokonać podsumowania?**

To był wielki sukces. Wcześniej temat ten był utajniony. Musimy pamiętać, że najsłabsze ogniwo – państwo z najsłabszym systemem cyberbezpieczeństwa może narazić cały sojusz. Przykładowo rozmieszczone wojska NATO w kraju-gospodarcza mogą zostać pozbawione elektryczności, jeżeli infrastruktura energetyczna nie jest odpowiednio chroniona. Cyber Defence Pledge umożliwia wyszukanie potencjalnych słabości w operacjach NATO. Ponadto państwo zobaczą jak dobre lub słabe są w zabezpieczeniu własnych sieci i systemów teleinformatycznych. Dlatego uważam, że ocena ta będzie ważna dla NATO, ale jeszcze ważniejsza dla poszczególnych państw.

**W Warszawie postanowiono o uznaniu cyberprzestrzeni za nowy rodzaj pola walki, takiego samego jak powietrze, ląd i morze. Sojusz musi osiągnąć taką samą skuteczność obrony. Jak przebiega proces operacjonalizacji?**

Każdy konflikt będzie miał swój początek w cyberprzestrzeni, dlatego odporność naszych systemów komputerowych na ataki jest najważniejsza. Ponadto nasza obrona musi być ciągła i obecna 24 godziny 7 dni w tygodniu. W przypadku konfliktu zbrojnego, cyber „bombardowanie” będzie miało miejsce cały czas.

Odporność naszych systemów i umiejętność utrzymywania obrony cały czas nie jest jednak wystarczająca. Musimy mieć też umiejętność odpowiedzi. Wprawdzie NATO postanowiło nie rozwijać swoich zdolności ofensywnych, ale członkowie Sojuszu mogą to jak najbardziej robić. Musimy również podkreślić, że odpowiedź nie musi być tylko w cyberprzestrzeni. Może mieć charakter polityczny, ekonomiczny albo nawet klasyczny – kinetyczny. NATO musi posiadać szereg narzędzi umożliwiających odpowiedź oraz sposoby ich skutecznego egzekwowania.

Organizatorem wydarzenia był Instytut Kościuszki.