Cyberdefence 24

aut. Andrzej Kozłowski 06.06.2019

GEN. MOLENDA: NIE MOŻNA BAZOWAĆ TYLKO NA OPERACJACH OBRONNYCH W KONFLIKCIE W CYBERPRZESTRZENI [ESD]

Generał Molenda podczas czwartej edycji Exatel Security Days wygłosił prezentację pt. „Przygotowania do konfliktu w cyberprzestrzeni", w której to przedstawił jakie działania musi podjąć Wojsko Polskie, żeby przygotować się do prowadzenia działań w cyberprzestrzeni.

Swoje wystąpienie rozpoczął od przypomnienia zgromadzonym, że kiedyś hakerzy łamali zabezpieczania, żeby zademonstrować swoje umiejętności, dzisiaj chodzi tylko o pieniądze i dane, które stały się walutą XXI wieku.

Cyberprzestrzeń jest jedyną przestrzenią, w której operują wojska, zbudowaną przez człowieka – podkreślił generał. Dodał, że przestrzeń ta, to nie tylko Internet, ale również Internet rzecz, smart city, smart home itp. Molenda stwierdził, iż powiedział, że smart znaczy podatny.

W dalszej części prezentacji ostrzegał przed cyfrowym Pearl Harbour, jednocześnie podkreślając, że zmiana w spojrzeniu na cyberkonflikty dokonała się po Stuxnecie, który zainfekował ośrodek wzbogacania uranu w Natanaz i pokazał, że działania w cyberprzestrzeni mogą wpływać na inne środowisko.

Molenda wyjaśnił, że kiedy następuje atak to wszystkie oczy kierują się na wojsko, w szczególności jeśli incydent jest poważny. Podkreślił, iż jest już jednak wtedy za późno i trzeba aktywnie działać wcześniej. Zaznaczył też, że kwestią nie jest czy w ogóle dojdzie do cyberataku, tylko kiedy.

Generał podkreślił, że wojsko przygotowuje się przede wszystkim do czasu wojny. Budowanie zdolności w cyberprzestrzeni - 5 domenie operacyjnej jest czymś oczywistym, skoro robimy to w pozostałych, takich jak ląd, morza i oceany czy powietrze. NATO w końcu uznało cyberprzestrzeń za kolejny obszar prowadzenia działań wojskowy w 2016 roku podczas szczytu w Warszawie – przypomniał generał.

Molenda podkreślił, że wciąż dyskutowany tematem jest czy armia powinna przygotować się tylko i wyłącznie do obrony własnych systemów i sieci teleinformatycznych czy może jej działania powinny być szersze i obejmować również obronę systemów przemysłu. Dlatego tak istotne jest określenie, w jakich sieciach wojsko może operować w czasie pokoju.

Stany Zjednoczone wyodrębniły następujące rodzaje operacji w cyberprzestrzeni:

- Operations of Defence Networks
- Offensive Cyberspace Operations
- Defence Cyberspace Operation

W swojej ostatniej strategii „Departament of Defence Cyber Strategy 2018”, Departament Obrony przedstawił koncepcję Defence Forward, czyli działań wyprzedzających. Jest to typ aktywnej obrony, który polega na ciągłej obecności w sieciach i systemach przeciwnika, co pozwala na rozpoznanie jego infrastruktury i odpowiednią reakcję, jeżeli przygotowuje się do podjęcia działań ofensywnych – podkreślił generał Molenda. Zaakcentował również konieczność prowadzenia operacji ofensywnych w cyberprzesteń, podkreślając, że nie można bazować tylko i wyłącznie na działań defensywnych.

Generał Molenda powiedział, że inspiracji do tego, jak przygotować się do konfliktu w cyberprzestrzeni należy szukać u klasyków, przy czym nawiązał do „Sztuki wojny” Sun Tzu. Chiński mistrz stwierdził, że znajomość siebie i swoich wrogów, pozwala pomyślnie przetrwać sto bitew. Dlatego kluczowe jest poznanie swoich słabości. W cyberprzestrzeni jest to jeszcze bardziej istotne i wiąże się z koniecznością poznania swoich systemów oraz systemów przeciwnika. Musimy wiedzieć, czym dysponujemy, w jaki sposób próbuje się nas atakować, co pozwoli lepiej przygotować się do potencjalnego konfliktu.

Molenda podkreślił, że tworzenie zdolności do operowania w cyberprzestrzeni można porównać do budowy samolotu w czasie lotu. Musimy cały czas wzmacniać bezpieczeństwo systemów komputerowych a jednocześnie prowadzić monitoring 24/7.

Generał kończąc swoją prezentację podkreślił, że od lutego i rozpoczęcia tworzenia WOC, otrzymał ponad 500 CV osób zainteresowanych służbą dla państwa.