aut. Andrzej Kozłowski 10.06.2019

WOJSKO POLSKIE POSIADA ZDOLNOŚCI W CYBERPRZESTRZENI. PIERWSZA JEDNOSTKA POWSTAŁA W 2010 ROKU [ESD]

Płk Przybylak w swojej prezentacji zatytułowanej „Operacje militarne w cyberprzestrzeni, czyli jak wojsko realizuje zadania w nowej domenie operacyjnej – wszystko co można Wam o tym powiedzieć" opowiedział o tym jak siły zbrojne działają w cyberprzestrzeni.

Swoje wystąpienie rozpoczął od przytoczenia definicji cyberprzestrzeni z Ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Definicja brzmi następująco

„Cyberprzestrzeń rozumie się jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie, odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sesji) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami."

W dalszej części swojej prezentacji prelegent omówił postanowienia szczytów NATO. W 2002 roku na szczycie w Pradze po raz pierwszy poruszono kwestię cyberbezpieczeństwa i utworzono NATO Computer Incident Response Center(NCIRC). Była to reakcja na pierwsze ataki DDoS podczas wojny o Kosowo 1999. Do kolejnych przełomowych decyzji doszło w Bukareszt 2008. Szczyt miał miejsce kilka miesięcy po atakach na Estonię. Uchwalono wtedy Cyber Defence Management Authority (CDMB). Przełom dokonał się w Lizbonie w 2010 roku, kiedy to cyberbezpieczeństwo było rozpatrywane na poziomie strategicznym. Uznano wtedy, że konieczna będzie wymiana informacji na temat zagrożeń dziejących się w środowisku. 4 lata później w walijskim mieście Newport uznano, że cyberatak może doprowadzić do powołania się na artykuł V. Stwierdzono również, że tylko kolektywna obrona przyniesie pożądane rezultaty. W 2016 roku w Warszawie uznano, że cyberprzestrzeń jest kolejną domeną operacyjną, a cyberatak może implikować odpowiedź w innej domenie. Wciąż również szukamy odpowiedzi czy cyberatak daje możliwości odpowiedzi kinetycznej, czyli krótko mówiąc czy możemy wystrzelić w kierunku atakującego rakietę czy nie. Ostatnie wydarzenia w Izraelu pokazało, że to już się wydarzyło i jednostka cyber Hamasu została unieszkodliwiona przez siły powietrzne.

W 2018 roku w Brukseli w NATO stwierdziło, że struktura dowódcza jest nieadekwatna do dzisiejszych zagrożeń i należy ją zmienić. Specjalistów od cyberbezpieczeństwa jest niewielu, dlatego też dopasowanie struktur do nich i stworzenie im odpowiednich pozycji w hierarchii jest bardzo istotne.

W Wojsku Polskim, pierwsza jednostka zajmująca się operacjami w cyberprzestrzeni powstała w 2010 roku, dlatego już od kilku lat posiadamy pewne zdolności w tym obszarze – podkreślił płk Przybylak.

Wojskowy powiedział, że wojna w cyberprzestrzeni jest pojęciem dyskusyjnym, ale mamy sytuacje kryzysowe.

Mamy procedury i zgodnie z jedną z nich Crisis Response Process (NCRP), hakowanie występuje dopiero w fazie 5 z 6. Pierwsza z nich to ostrzeżenie, następnie dokonywana jest ocena. W fazie 3 mamy opcję odpowiedzi. Faza 4 polega na planowaniu i dopiero 5 faza to wykonanie. Ostatnia to zmiana. Wojsko słynie z planowania, ale ma to sens. Dla swojego dowódcy muszę przedstawić kilka wariantów, które oceniane są przez kilka wskaźników - podkreślił Przybylak. Koszt i efekt to dwa kluczowe. Proces Battle Damage Assesment (BDA) czyli ocena skutków, ma również miejsce w cyberprzestrzeni.

Sama cyberprzestrzeń składa się z warstwy geograficznej, logicznej, fizycznej i socjologicznej. Płk Przybylak powiedział, że walka może odbywać się w warstwie logicznej, ale jej efekty przekładają się na pozostałe warstwy jak np. tożsamości cyfrowe, które można skompromitować. Można również oddziaływać na kable światłowodowe, lotniska czy inne elementy infrastruktury krytycznej w szczególności energetykę, która była już celem ataków.

Operacje w cyberprzestrzeni można podzielić na Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Intelligence, Surveillance & Reconnaissance (ISR) oraz CIS Infrastructure Operations.

Defensive Cyberspace Operations (DCO)

Operacje obronne w cyberprzestrzeni zostały podzielone na Internal Defence Measures (DCO-IDM) i External Defence Measures (DCO-EDM). Pierwsze obejmują operacje we własnych sieciach (środowiskach) zwanych też „blue networks". Drugie zaś dotyczą sieci (środowisk) zewnętrznych, w tym „red networks" (należących do adwersarzy) oraz „gray networks" (pozostałych, w szczególności neutralnych). DCO jest stosowane prokatywnie jeśli mamy symptomy, że coś może się wydarzyć, wtedy trzymamy siły i środki w gotowości. Kiedy jednak stwierdzimy, że doszło do ataku to podejmowane są działania reaktywne – podkreślił płk Przybylak.

Offensive Cyberspace Operations (OCO)

Ofensywne operacje w cyberprzestrzeni dzielą się na Denial Operations (OCO-DA), Manipulation Operations (OCO-MA) oraz Operational Preparation of the Environment. Pierwsze z nich to portfolio działań tzw. 4D, czyli deny, disrupt, degrade, destroy. Dotyczy on przede wszystkim danych i usług. Drugie - tj. OCO-MA - dotyczą oddziaływania na integralność informacji i usług. Trzecie natomiast można przetłumaczyć jako informacyjne przygotowanie obszaru operacyjnego zainteresowania. Innymi słowy - chodzi o działania przygotowujące tak, aby zwiększyć skuteczność działań z grupy pierwszej (OCO-DA) i drugiej (OCO-MA). Rozpatrując OCO należy wziąć pod uwagę, co chcemy zrobić i jakie efekty osiągnąć - dodał prelegent.

Intelligence, Surveillance & Reconnaissance (ISR)

Trzeci rodzaj działań operacyjnych to wywiad, nadzór i rozpoznanie. Jak w poprzednich grupach i tutaj wyróżniamy 3 rodzaje operacji. Pierwszy z nich to non-intrusive collection rozpoznanie – działania bazujące na ogólnodostępnych źródłach (OSINT z ang. pen- source intelligence). Kolejnym jest intrusive collection występujący wtedy, kiedy następuje aktywne oddziaływanie z rozpoznawanym obiektem, np.: skanowanie portów dla protokołu TCP (TCP scan). Trzecim jest podobnie jak w OCO Operational Preparation of the Environment.

CIS Infrastructure Operations – łączność i informatyka

W innym dokumencie tj. NATO High Level Taxonomy for Cyberspace Operations, NATO wyróżniło dodatkowo czwartą grupę operacji w cyberprzestrzeni. Mowa tutaj o CIS Infrastructure Operations. Grupa ta dotyczy głównie Communication&Information Systems Operations czyli - w uproszczeniu - usług ICT. CIS odpowiadają za utrzymanie cyberprzestrzeni i są kluczowe z punktu widzenia wojska.

Operacje w cyberprzestrzeni wymagają dopasowania obecnego prawa międzynarodowego do zmieniającego się obrazu konfliktu.