Cyberdefence 24

aut. Andrzej Kozłowski 18.11.2020

DYREKTOR NCBC: WOJSKA OBRONY CYBERPRZESTRZENI Z PEŁNĄ ZDOLNOŚCIĄ OPERACYJNĄ DO 2025

Wojska Obrony Cyberprzestrzeni mają osiągnąć pełną zdolność operacyjną w 2025 roku - zapowiedział generał Karol Molenda podczas posiedzenia Komisji Obrony Narodowej. Obecnie kluczowe jest pozyskanie odpowiednich ekspertów do jednostki.

Tematem wtorkowego (17.11.2020 r.) posiedzenia Komisji Obrony Narodowej była kwestia bezpieczeństwa teleinformatycznego Sił Zbrojnych RP i systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych RP oraz omówiono proces formowania Wojsk Obrony Cyberprzestrzeni. Ministerstwo było reprezentowane na posiedzeniu komisji przez wiceszefa MON Wojciecha Skurkiewicza oraz gen. Karola Molendę, dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz pełnomocnika Ministerstwa Obrony Narodowej ds. utworzenia Wojsk Obrony Cyberprzestrzeni. Na prośbę Skurkiewicza oba punkty posiedzenia zostały rozpatrzone łącznie, jako powiązane ze sobą.

Sekretarz stanu w Ministerstwie Obrony Narodowej Wojciech Skurkiewicz rozpoczął od stwierdzenia, że na przestrzeni lat obserwujemy rozwój informatyzacji, wszystkich obszarów naszego życia. Obszar IT jest coraz mocniej obecny w różnych gałęziach przemysłu, ale również na praktycznie każdym kroku w życiu obywateli. "Mamy również powszechne oczekiwania, że organy państwa będą brały udział w zabezpieczeniu użytkowników" – podkreślił Skurkiewicz. Jego zdaniem powszechna dostępność nowoczesnych technologii niesie ze sobą cale mnóstwo zagrożeń i nienotowanych wcześniej wyzwań, nie tylko dotyczących bezpieczeństwa wewnętrznego, ale i międzynarodowego. Sekretarz stanu ostrzegał przede wszystkim przed wykorzystaniem cyfryzacji przez Rosję, co określił mianem głównego rodzaju zagrożeń w tej części Europy. Moskwa w 2000 roku wskazała na cyberprzestrzeń jako elementy wojny informacyjnej, tak aby wykorzystać informacje do wpływania na świadomość społeczną. Skurkiewicz podkreślił, że w Rosji od 20 lat kształci się ekspertów od bezpieczeństwa informacji, którzy zasilają zarówno aparat bezpieczeństwa jak i aparat administracji państwowej.

Sekretarz stanu w MON podkreślił również, że Rosja wspierała swoje działania konwencjonalne operacjami w cyberprzestrzeni, co miało miejsce w Gruzji w 2008 roku oraz na Ukrainie w 2014 roku. Sytuacja ta zmusiła do reakcji NATO, które uznało w 2014 roku, że cyberatak może stanowić podstawę do powołania się na artykuł V Traktatu Waszyngtońskiego. Dwa lata później podczas szczytu Sojuszu w Warszawie uznano cyberprzestrzeń za jedną z domen operacyjnych, stwierdzając, że jest to strefa zainteresowań i wpływu państw, które podejmują swoje działania w celu osiągniecia pożądanych efektów.

NATO wprowadziło również Cyber Defence Pledge, na mocy którego każde państwo członkowskie powinno rozwijać swoje zdolności defensywne w cyberprzestrzeni. Skurkiewicz dodał, że MON

podejmuje liczne przedsięwzięcia informacyjne oraz szkoleniowe. Najważniejsza była jednak konsolidacja zasobów resortu obrony w zakresie struktur odpowiedzialnych za zapewnienie cyberbezpieczenstwa. W ten sposób stworzono NCBC, które bazuje na Narodowym Centrum Kryptologii. W 2018 roku uruchomiono program Cyber.mil. Jego głównym celem było przyciągnięcie do struktur młodych i zdolnych osób. Niestety, specjalistów z zakresu cyberbezpieczenstwa na rynku jest bardzo niewielu, dlatego tak ważne jest zwiększenie osób posiadających odpowiednie kompetencje. Z tego powodu zwiększono liczbę studentów WAT na specjalnościach: informatyka, kryptologia i cyberbezpieczeństwo. Kończąc swoją wypowiedź Skurkiewicz podkreślił, że ochrona cyberprzestrzeni Polski wymaga działań w sferze wojskowej oraz potrzeba stabilnych fundamentów umożliwiających realizację zadań MON w ramach Krajowego Systemu Cyberbezpieczeństwa.

Generał brygady Karol Molenda, dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), omówił stan formowania się Wojsk Obrony Cyberprzestrzeni (WOC). Zaznaczył, że koncepcja ich utworzenia jest niejawna. Posłowie zasiadający w komisji mogą się za nią zapoznać bardziej szczegółowo w kancelarii tajnej Sejmu. "Cyberprzestrzeń stała się przestrzenią oddziaływania różnych adwersarzy i prowadzenia działań, których celem jest pozyskanie informacji lub ich zakłócenie" – rozpoczął generał. "NATO zauważyło ten problem i w 2016 roku cyberprzestrzeń została zdefiniowana jako kolejna domena operacyjna, gdzie trzeba się przygotować do obrony, podobnie jak ma to miejsce w powietrzu, na lądzie i na morzu" - dodał Molenda. Jednocześnie podkreślił, że to jedyna domena zbudowana przez człowieka i która stale podlega modyfikacji.

„Jeżeli samolot zostanie zestrzelony to właściwości powietrza nie ulegną zmianie. Jeśli pewne działania w cyberprzestrzeni się odbywają, to jest ona korygowana i zmieniana chociażby przez aktualizacje używanych aplikacji” – wyjaśnił różnice generał. W cyberprzestrzeni mamy coraz to nowsze urządzenia, funkcjonalności oraz zasoby. "To niekończący się proces, a nie jednolity zastany stan" – dodał Molenda.

Prowadzenie działań w cyberprzestrzeni ma na celu uzyskanie pewnych efektów defensywnych jak i ofensywnych. "Prowadzona jest działalność rozpoznawcza właściwości systemów teleinformatycznych przeciwnika" - dodał. Wyjaśnił również, że w ramach NATO Cyber Defence Pledge Polska zobowiązała się do zbudowania kompetencji i zdolności prowadzenia operacji w cyberprzestrzeni, które można podzielić na kilka typów. Przede wszystkim wyróżnić można: CyberOps polegające na przełamywaniu zabezpieczeń i właściwości sprzętu, aby dostać się do celu oraz InfoOps, czyli operacji informacyjnych z wykorzystaniem cyberprzestrzeni, które może wpłynąć na postawy użytkowników – wyjaśnił generał. Dodał, że duża liczba ataków wykorzystuje socjotechnikę, czyli działania informacyjne, którą są wstępem do działań CyberOps.

Generał Molenda podkreślił, że w ostatnim roku udało się określić zasoby, którymi dysponuje wojsko w obszarze kryptologii i cyberbezpieczeństwa. „Zauważyliśmy, że część jednostek odpowiedzialnych za cyberbezpiezceństwo i kryptografię jest rozrzucanych po całych siłach zbrojnych” – podkreśla generał. Przywołuje również przykład Inspektoratu Informatyki, dla którego priorytetem była funkcjonalność a nie bezpieczeństwo. Znowu dla Narodowego Centrum Kryptologii priorytetem było właśnie bezpieczeństwo. Instytucja ta tworzyła szyfratory i monitorowała sieć. Dyrektor NCBC wyjaśnia, że były dwie jednostki na tym samym poziomie, które miały odmienne zadania. Dlatego trzeba było je skonsolidować i tak powstało NCBC, któremu podlega również 6 regionalnych centrów informatyki, odpowiadających za cyberbezpieczeństwo w przydzielonych obszarach. "Jest również jednostka logistyczna: Centrum Zasobów Cyberprzestrzeni oraz Centrum Operacji Cyberprzestrzeni na podstawie której będzie budowany WOC" – wyjaśnił generał. "Obecnie każdy laptop oraz inny element infrastruktury informatycznej został zakupiony i skonfigurowany przez NCBC" - podkreśla generał.

Gen. Molenda poinformował, że formowanie Wojsk Obrony Cyberprzestrzeni zajmie około czterech do pięciu lat. Jak wyjaśnił, ma na myśli „pełną zdolność do działania w pełnym spektrum

cyberprzestrzeni”. Dodał, że obecnie zakończony jest pierwszy etap formowania takich zdolności. Według dyrektora NCBC w 2025 r. ma funkcjonować „dowództwo, z pełnym (FOC - full operational capability, pełna zdolność operacyjna) jeżeli chodzi o cyberprzestrzeń, z certyfikowanym dowództwem i certyfikowanymi zespołami”.

Omawiając powołany przez resort CSIRT MON (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni) ocenił, że jest on już na poziomie „75 proc. ukompletowania”.

Mówiąc o drugim etapie formowania nowych wojsk gen. Molenda wskazał na konieczność pozyskiwania kadr oraz pracy nad poprawę ich współdziałania. Istotnym problemem, którzy trzeba będzie rozwiązać jest również aspekt prawny, czyli zdefiniowanie w jakich sytuacjach żołnierze mogą realizować działania w cyberprzestrzeni. Dyrektor NCBC dodał, że w obecnej chwili budowane są zdolności na czas wojny, ale większość działań w cyberprzestrzeni toczy się jednak w czasie pokoju i dlatego przygotowujemy się do ich prowadzenia.

Na koniec posiedzenia Molenda powiedział, że tworzone są już kolejne zespoły cyberbezpieczeństwa w Regionalnych Centrach Informatyki, które w regionach swojej odpowiedzialności będą utrzymywać sieci komputerowe pod „względem funkcjonalności i bezpieczeństwa”. Powstaje też „laboratorium”, które ma testować sprzęt pod kątem „potencjalnych podatności” i „zabezpieczania” na potrzeby Sił Zbrojnych.