Cyberdefence 24

aut. Piotr Mieszkowski 21.06.2017

POLSKA MA POTENCJAŁ BY STAĆ SIĘ SILNYM KRAJEM W CYBERPRZESTRZENI

W Sejmowej Komisji Obrony kontynuowane są cyklicznie organizowane spotkania o charakterze konferencyjnym, poświęcone najważniejszym kwestiom obrony państwa oraz realizacji zadań w dziedzinie umacniania obronności. W środę odbyło się kolejne, siódme już spotkanie, którego tematem było „Bezpieczeństwo informacyjne państwa - funkcjonowanie w cyberprzestrzeni”.

Przedsięwzięcie w formule Parlamentarnego Forum Obrony Narodowej każdorazowo adresowane jest do posłów i senatorów – członków parlamentarnych Komisji Obrony Narodowej, pozostałych parlamentarzystów, zapraszanych ekspertów oraz pragmatyków z dziedziny bezpieczeństwa narodowego i obronności. Jednymi z gości środowej dyskusji byli prof. Andrzej Zybertowicz, socjolog, doradca społeczny prezydenta RP Andrzeja Dudy oraz dr inż. Janusz Jabłoński, adiunkt na Wydziale Matematyki, Informatyki i Ekonometrii Uniwersytetu Zielonogórskiego i jednocześnie dyrektor ds. badań naukowych w firmie Rublon.

VII Spotkanie Parlamentarnego Forum Obrony Narodowej poprowadził poseł PiS Michał Jach, przewodniczący Sejmowej Komisji Obrony Narodowej. Prelekcję pod tytułem "Zagrożenia a cele strategiczne w zapewnieniu bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni" wygłosił Bogusław Cichoń dyrektor Departamentu Prawa i Bezpieczeństwa Pozamilitarnego, Biura Bezpieczeństwa Narodowego.

Zdaniem dyrektora Cichonia należy sobie przede wszystkim zadać pytanie, czym jest suwerenność w cyberprzestrzeni i jak należy ją zdefiniować. Ekspert BBN postawił także pytanie, co mogłoby spowodować wprowadzenie stanu wojennego w efekcie ataku hakerskiego. Cichoń przypomniał zebranym, że w kwietniu rząd przyjął Krajowe Ramy Polityki Cyberbezpieczeństwa 2017-2022. Równolegle, jak twierdzi - trwają prace nad stworzeniem planu implementacji tej strategii oraz nad dokończeniem ustawy o cyberbezpieczeństwie państwa.

Czytaj też: GLOBSEC 2017: Ustawa o cyberbezpieczeństwie musi wyjść poza ramy implementacyjne dyrektywy NIS

Drugim, ważnym tematem poruszonym podczas forum, było "Tworzenie warunków do budowania systemu cyberbezpieczeństwa państwa". Temat ten przybliżył zebranym Mirosław Maj, doradca ministra obrony narodowej ds. cyberbezpieczeństwa, ekspert w dziedzinie bezpieczeństwa teleinformatycznego oraz ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), współpracownik Rządowego Centrum Bezpieczeństwa, wieloletni kierownik CERT Polska, a także fundator i prezes Fundacji Bezpieczna Cyberprzestrzeń. Według Maja niezwykle ważnym momentem ubiegłorocznego szczytu NATO Summit w Warszawie, było uznanie cyberprzestrzeni jako kolejnego pola działalności wojennej.

Doradca ministra obrony narodowej przypomniał zebranym, że od sierpnia 2016 roku obowiązuje dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, która na terytorium Unii zwana jest Dyrektywą NIS. Wspomniał też, że w Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-2022 rząd stawia na walkę z dystrybucją szkodliwego oprogramowania, włamaniami do systemów teleinformatycznych czy blokowaniem możliwości świadczenia usług. Cel wprowadzonych zmian jest taki, żeby zapewnić wysoki poziom odporności krajowych systemów teleinformatycznych, operatorów kluczowych usług i dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze) na ataki w cyberprzestrzeni.

Mirosław Maj mówił także o konieczności ponadresortowej koordynacji, konieczności łączenia operacji o charakterze cyber z operacjami informacyjnymi oraz konieczności budowania systemu, który nie będzie pokrywał w szczegółach nie tylko kwestie reakcji, ale i odpowiedniego zabezpieczenia. Zdaniem doradcy ministra obrony narodowej, konieczne jest także uwzględnienie w rozwiązaniach legislacyjnych stanów innych niż stan pokoju, w tym wiodącej roli koordynacyjnej MON w stanie kryzysu i wojny. Zwrócił także uwagę na problemy związane z funkcjonowaniem w nieokreślnym do końca stanie „hybrydowym”.

Według Mirosława Maja, Polska ma wystarczającą ilość ekspertów i osób z dużym potencjałem wiedzy w dziedzinie cyberbezpieczeństwa, by móc stworzyć niezbędne zasoby kadrowe, których w tym momencie jeszcze brakuje. Mamy jednak, jak mówił Ekspert i doradca MON, olbrzymi potencjał, by stać się silnym krajem w tej dziedzinie obronności. Maj nawiązał także do wypowiedzi dyrektora Cichonia BBN mówiąc, że w dziedzinie cyberbezpieczeństwa faktycznie jest w Polsce problem z podstawowymi definicjami i usystematyzowaniem dotychczas opracowanej wiedzy.