https://www.bbn.gov.pl/pl/wydarzenia/6092,Szef-BBN-musimy-zespolic-wysilki-w-budowaniu-spojnego-systemu-cyberbezpieczenstw.html
2021-02-26, 17:41

06.11.2014

Szef BBN: musimy zespolić wysiłki w budowaniu spójnego systemu cyberbezpieczeństwa

6 listopada br. na międzynarodowej konferencji "Zagrożenia w cyberprzestrzeni - bezpieczeństwo ponad granicami" minister Stanisław Koziej po raz pierwszy publicznie przedstawił założenia opracowywanej w BBN "Doktryny cyberbezpieczeństwa RP". Gotowy dokument będzie rozwijał zapisy, zatwierdzonej w dniu wczorajszym przez Prezydenta Bronisława Komorowksiego Strategii Bezpieczeństwa Narodowego RP. Jego założenia zostały także przyjęte podczas ostatniego posiedzenia Rady Bezpieczeństwa Narodowego.

WYSTĄPIENIE SZEFA BBN

Szanowni Państwo,

Dziękuję za zaproszenie, bo rozmowa o cyberbezpieczeństwie w tak szerokim i zróżnicowanym gronie jest dziś niewątpliwie bardzo potrzebna. Bezpieczeństwo w cyberprzestrzeni to bowiem najnowsza i najbardziej wymagająca dziedzina bezpieczeństwa narodowego, o charakterze wybitnie wielowymiarowym, wielosektorowym: obronnym i ochronnym; cywilnym i wojskowym; rządowym, samorządowym i pozarządowym; publicznym i prywatnym.

Dlatego też najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane, kompleksowe, stwarzające warunki do budowania spójnego systemu cyberbezpieczeństwa, uwzględniającego pożądaną jednolitość koncepcyjną, łączącego te wszystkie wymiary. I taki jest najbardziej ogólny cel Doktryny cyberbezpieczeństwa RP, nad którą obecnie pracujemy.

Nie startujemy od zera. W tej dziedzinie już w Polsce pewne działania zostały podjęte i zrobione. Dotyczy to np. polskiego systemu prawnego – do którego w 2011 r. wprowadziliśmy m.in. kategorię „cyberprzestrzeni” oraz ustanowiliśmy prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia.

W pełni wykorzystujemy dorobek Unii Europejskiej i NATO w tej dziedzinie. W administracji wprowadzono rozwiązania ujęte w Polityce Ochrony Cyberprzestrzeni RP, przyjętej przez Radę Ministrów w 2013 r. Dokument ten dotyczy przede wszystkim ochrony cyberprzestrzeni w wymiarze pozamilitarnym.

W Ministerstwie Obrony Narodowej trwają prace nad rozwiązaniami w zakresie cyberobrony, a prywatne podmioty we własnym zakresie organizują swoje bezpieczne funkcjonowanie w cyberprzestrzeni.

Nadeszła pora, by stworzyć warunki do zespolenia tych wysiłków i jednocześnie nakreślić strategiczne kierunki i ramy budowania zintegrowanego, spójnego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Takie są przesłanki przygotowania projektu doktryny cyberbezpieczeństwa, która w swojej treści jest też sektorowym dokumentem wykonawczym do Strategii Bezpieczeństwa Narodowego. Jej główne założenia zostały już rozpatrzone i przyjęte przez Radę Bezpieczeństwa Narodowego na jej ostatnim posiedzeniu.

Projekt przygotowywany jest na podstawie analiz prowadzonych z udziałem przedstawicieli administracji publicznej, zainteresowanych resortów, urzędów i agend, świata akademickiego, organizacji pozarządowych, a także sektora prywatnego.

Doktryna cyberbezpieczeństwa wskazywać będzie strategiczne kierunki działań na rzecz zapewnienia pożądanego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne, kompleksowe i kompletne podejście do zagadnień cyberochrony i cyberobrony - jako swego rodzaju "wspólny mianownik" dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny i obywateli.

W swojej treści zawiera cztery grupy zagadnień. Po pierwsze – określa cele o charakterze operacyjnym i przygotowawczym w dziedzinie cyberbezpieczeństwa. Rozwija tu podstawowy cel strategiczny ujęty w najnowszej Strategii Bezpieczeństwa Narodowego, jakim jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej (tj. państwa, społeczeństwa, podmiotów prywatnych i obywateli) w cyberprzestrzeni.

Po drugie – zawiera ocenę zagrożeń, ryzyk i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa, w jego wymiarze zewnętrznym i wewnętrznym (międzynarodowym i krajowym): od zwykłych cyberprotestów do cyberwojny.

Po trzecie – identyfikuje najważniejsze zadania operacyjne dla zapewnienia cyberbezpieczeństwa, jakie powinny być podejmowane w sektorze publicznym, prywatnym i obywatelskim. Wśród nich podkreśliłbym szczególne znaczenie działań zmierzających do zapewnienia narodowego panowania informatycznego nad wysoce zinformatyzowanymi systemami o strategicznym znaczeniu, np. nad uzbrojeniem, wszelkimi systemami walki i wsparcia.

I wreszcie po czwarte – rekomenduje działania mające na celu przygotowanie (tj. doskonalenie, rozwój, transformację) systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu zarządzania sprawami cyberobrony oraz publicznych i prywatnych ogniw wykonawczych. Na szczególne podkreślenie zasługuje kształcenie kadr i rozwijanie kompetencji w zakresie narodowej kryptologii.

W sumie doktryna ta będzie mogła stanowić punkt odniesienia i ukierunkowania dla dalszych prac, które tworzyć będą coraz bardziej solidne i niezawodne rozwiązania na rzecz bezpieczeństwa Polski i Polaków w cyberprzestrzeni.

Wierzę, że dzisiejsza konferencja również wniesie swój wkład we wzmacnianie tego bezpieczeństwa. Na to liczę i życzę Państwu owocnych obrad.

***

Konferencja zorganizowana przez Agencję Lotniczą Altair oraz Zarząd Targów Warszawskich objęta została patronatami szefa Biura Bezpieczeństwa Narodowego, Ministerstwa Obrony Narodowej i Ministerstwa Administracji i

Cyfryzacji. Wśród panelistów znaleźli się m.in. podsekretarz stanu w MAiC Roman Dmowski, dyrektor Narodowego Centrum Kryptologii gen. Krzysztof Bondaryk, rektor Wojskowej Akademii Technicznej gen. bryg. Zygmunt Mierczyk czy gen. Adam Sowa, w latach 2008-2012 zastępca dyrektora wykonawczego Europejskiej Agencji Obrony.

Tweetnij