https://www.bbn.gov.pl/pl/wydarzenia/5198,Wyzwanie-dla-panstwa-to-zintegrowac-system-cyberbezpieczenstwa.html
2021-09-21, 04:08

25.01.2014

Wyzwanie dla państwa to zintegrować system cyberbezpieczeństwa

25 stycznia br. minister Stanisław Koziej był gościem dwudniowego zjazdu Akademii Młodych Dyplomatów zorganizowanego przez Europejską Akademię Dyplomacji. Podczas wystąpienia na sesji głównej szef BBN mówił o wyzwaniach i zagrożeniach dla Polski związanych z funkcjonowaniem w cyberprzestrzeni.

Minister Koziej przyznawał, że cyberbezpieczeństwo jest jeszcze dziedziną, w której państwo uczy się działać: - *Dziś jesteśmy na początku drogi budowania systemu cyberbezpieczeństwa i zagadnienie to stanowi nowe wyzwanie zarówno dla analityków, jak i dla samych instytucji państwowych.* Na przykład sam termin cyberprzestrzeni jest różnie interpretowany, a w polskim ustawodawstwie skonkretyzowany został dopiero przed dwoma laty, przy okazji prezydenckiej nowelizacji ustaw o stanach nadzwyczajnych.

Zobacz prezentację

Jednym z problemów radzenia sobie przez państwo z problematyką cyberbezpieczeństwa, jest fakt, że ma ono charakter transsektorowy, dotyczy funkcjonowania wszystkich resortów, ale też sektora prywatnego i obywateli. Tym samym istnieją trudności w skoordynowaniu wysiłków państwa dotyczących budowy systemu cyberbezpieczeństwa.

Dyskutowanym rozwiązaniem problemu jest m.in. powierzenie odpowiedzialności za koordynację Ministerstwu Administracji i Cyfryzacji. Jednak według szefa BBN takie podejście w praktycznym funkcjonowaniu może okazać się niewystarczająco skuteczne. Biuro Bezpieczeństwa Narodowego przy okazji prac nad Strategicznym Przeglądem Bezpieczeństwa Narodowego postulowało, że sprawą koordynacji wysiłków związanych z umacnianiem systemu bezpieczeństwa państwa, w tym także cyberbezpieczeństwa, powinny się zająć struktury ponadresortowe (rządowy komitet ds. bezpieczeństwa narodowego oraz obsługująca go ponadresortowa instytucja, np. Rządowe Centrum Bezpieczeństwa o poszerzonych kompetencjach w stosunku do stanu obecnego). Takie rozwiązanie BBN proponuje rządowi.

Podczas wystąpienia szef BBN mówił także, że problematyka cyberbezpieczeństwa dyskutowana była na każdym etapie prac w ramach Strategicznego Przeglądu Bezpieczeństwa Narodowego. Na etapie definiowania celów

operacyjnych rozważano m.in. dwojakie podejście do kwestii cyberbezpieczeństwa: jako zapewnienie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej oraz jako zapewnienie bezpieczeństwa Rzeczypospolitej w cyberprzestrzeni. Dla potrzeb formułowania dokumentów strategicznych przyjęto drugą definicję celu.

W wyniku prac nad Przeglądem określono również cele preparacyjne, czyli związane z przygotowaniem odpowiednich zasobów państwa. Według szefa BBN takim celem powinno być zbudowanie zintegrowanego systemu cyberbezpieczeństwa. Obejmowałby on zarówno określenie jasnego podziału zadań, zapewnienie środków czy chociażby stworzenie polskiej myśli kryptologicznej. Na pytanie czy Polska będzie rozwijać również środki do działań ofensywnych w cyberprzestrzeni, szef BBN stwierdził, że zarówno środki o charakterze defensywnym jak i ofensywnym są niezbędne i każde państwo takie tworzy. Szczególnie mocno podkreślił konieczność inwestowania w rozwój narodowej kryptologii, w tym zwłaszcza własnych kadr w tej dziedzinie.

Mówiąc o polskich działaniach szef BBN zwrócił uwagę, że problemy dotyczące funkcjonowania w cyberbezpieczeństwa mają także charakter międzynarodowy. Toczy się np. dyskusja czy normy prawne związane z działalnością w geoprzestrzeni, można odnosić bezpośrednio do cyberprzestrzeni. Jest to chociażby istotne w przypadku gwarancji bezpieczeństwa udzielanych przez NATO w przypadku agresji na terytorium państwa członkowskiego i dylematu czy atak w cyberprzestrzeni można traktować jako taką agresję.

Tweetnij