

"PODSTAWOWYM ZADANIEM PAŃSTWA JEST ZAPEWNIENIE BEZPIECZEŃSTWA OBYWATELI, KTÓRZY KORZYSTAJĄ Z CYBERPRZESTRZENI" [SCF2019]

"Tego typu spotkania są bardzo cenne, bo pozwalają nam na budowanie relacji, które są niezbędne, jeśli chcemy myśleć o sprawnym systemie cyberbezpieczeństwa w Polsce" – powiedział Minister Marek Zagórski, inaugurując wydarzenie Strategic Cyber Forum organizowane przez portal CyberDefence24.pl. Podczas wydarzenia uczestnicy wysłuchali wystąpień Ministra Cyfryzacji Marka Zagórskiego, Ministra Pawła Słocha, Szefa Biura Bezpieczeństwa Narodowego oraz gen. bryg. rez. Rami Efrati, założyciela i byłego szefa Wydziału Cywilnego Izraelskiego Narodowego Biura Cybernetycznego w Kancelarii Premiera Izraela.

Strategic Cyber Forum, które odbyło się 1 października w Warszawie, zgromadziło 320 uczestników. Wysłuchali oni 3 wystąpień wprowadzających, wzięli również udział w 2 otwartych debatach oraz 2 zamkniętych spotkaniach w formule Chatham House.

W ramach wydarzenia spotkali się najważniejsi przedstawiciele administracji rządowej, Sił Zbrojnych RP, zarządów największych spółek ze strategicznych branż a także eksperci i reprezentanci instytutów badawczych. Wydarzenie poruszało aktualne problemy i wyzwania bezpieczeństwa: związane ze znaczeniem przywództwa strategicznego, budowy efektywnego systemu cyberbezpieczeństwa, ochrony infrastruktury krytycznej oraz współpracy prywatno – publicznej i cywilno – wojskowej.

W ramach wystąpienia otwierającego Minister Marek Zagórski zwrócił uwagę na wagę wydarzenia, które pozwala na budowę relacji umożliwiających zorganizowanie sprawnego systemu cyberbezpieczeństwa w Polsce. Ponadto w swoim wystąpieniu odniósł się do uchwalonej w zeszłym roku ustawy o krajowym systemie cyberbezpieczeństwa. W jego opinii, dokument zdefiniował nie tylko zadania dla poszczególnych instytucji działających w ramach administracji państwowej, ale również biznesu. Minister podkreślił jednocześnie konieczność stałego umacniania cyberbezpieczeństwa za który odpowiedzialność ponoszą wszyscy uczestnicy systemu – „odpowiedzialność biorą nie tylko administracja, rząd, poszczególne służby, w którym każdy podmiot ma poczucie odpowiedzialności za bezpieczeństwo swojej firmy, sektora, w konsekwencji za nasze wspólne bezpieczeństwo" – stwierdził w ramach inauguracji spotkania.

Czytaj też: [„Bez rodzimych rozwiązań IT nie będzie bezpieczeństwa infrastruktury krytycznej” \[SCF2019\]](#)

Minister podkreślił, że budowanie sprawnego systemu cyberbezpieczeństwa jest zadaniem kompleksowym. „To nie jest tylko odpowiedzialność i zadanie instytucji, poszczególnych CERTów, ale to jest także zadanie polegające na współpracy, wymianie informacji, na wymianie także rozwiązań i

budowaniu tych rozwiązań” – stwierdził.

„Żadna firma nie jest w stanie funkcjonować w tym zakresie odrębnie, tak samo jak żadne państwo nie jest się w stanie kompleksowo zabezpieczyć” – podkreślił minister, dodając jednocześnie, że współpraca na poziomie międzynarodowym jest „szalenie istotna”.

Minister wskazał również, że w całym systemie na końcu zawsze okazuje się, że najsłabszym jego elementem jest człowiek. „Potrzebna jest nam wiedza, a także zrozumienie wśród mediów i biznesu. Potrzebne są nam kompetencje na poziomie poszczególnych firm, ale również potrzebne nam są kompetencje i świadomość całego społeczeństwa” – stwierdził. „Chciałbym prosić, aby aspekt dobrej komunikacji i dobrej edukacji był także obecny w dyskusjach (debat w trakcie wydarzenia – przyd. red.)”.

"System obrony cyberprzestrzeni wymaga skoordynowania z pozostałymi komponentami systemu bezpieczeństwa" - stwierdził Paweł Soloch, Szef Biura Bezpieczeństwa Narodowego w swoim wystąpieniu. Podkreślił również, że zdolność do szybkiej reakcji na pojawiające się w przestrzeni bezpieczeństwa wyzwania i zagrożenia uznawane za nowe wymaga całościowego spojrzenia na bezpieczeństwo państwa oraz oparcia się na zintegrowanym systemie zarządzania bezpieczeństwem narodowym. Warto podkreślić, że szef BBN zapewnił, że Prezydent RP Andrzej Duda, dostrzega konieczność zachowania bezpieczeństwa funkcjonowanie państwa również w obszarze cyberprzestrzeni.

Konieczność dalszego budowania zdolności do zapewnienia bezpiecznego funkcjonowania państwa w cyberprzestrzeni dostrzega prezydent RP (...) Tylko całościowe spojrzenie na bezpieczeństwo państwa w oparciu o zintegrowany system zarządzania bezpieczeństwem narodowym zapewni zdolność do szybkiej reakcji na pojawiające się nowe wyzwania i zagrożenia

- Paweł Soloch, Szef Biura Bezpieczeństwa Narodowego

Paweł Soloch w ramach wystąpienia potwierdził również konieczność przygotowania dokumentu - ustawy o zarządzaniu bezpieczeństwem narodowym, który w zwartych ramach scaliłby wszystkie systemy mające służyć bezpieczeństwu narodowemu. Jak wskazał bezpieczeństwo państwa w cyberprzestrzeni jest obecnie jednym z najczęściej omawianych globalnych wyzwań. Dlatego też Szef BBN jako reprezentant Prezydenta RP zaliczył bezpieczeństwo obywateli korzystających z cyberprzestrzeni za jedno z podstawowych zadań państwa. Podkreślił konieczność ochrony ich prywatności, danych osobowych, godności a także mienia, również w cyberprzestrzeni.

"Podstawowym zadaniem państwa jest zapewnienie bezpieczeństwa obywateli, którzy korzystają z cyberprzestrzeni" - podkreślił w trakcie wystąpienia.

Jak wskazał jednak, niezwykle istotna jest oprócz własnego przygotowania przez struktury państwowe również działalność na poziomie międzynarodowym. Z uwagi na globalny charakter zagrożenia niezbędne jest, aby kwestie bezpieczeństwa z zakresu cyberbezpieczeństwa były traktowane jednakowo w całym regionie. Dlatego też podkreślił rolę pracy i działań Polski w ramach V4, Bukaresztańskiej Dziewiątki, UE oraz NATO.

W ramach wystąpienia, Minister Soloch zaznaczył również, że współodpowiedzialność za bezpieczeństwo państwa w cyberprzestrzeni spoczywa również na podmiotach sektora prywatnego.

"Izrael jest jednym z nielicznych państw na świecie, gdzie za cyberbezpieczeństwo odpowiada bezpośrednio premier" powiedział generał brygady rezerwy Rami Efrati - założyciel i były szef wydziału cywilnego izraelskiego Narodowego Biura Cybernetycznego w Kancelarii Premiera Izraela.

Rami Efrati zaczął swoje wystąpienie od podkreślenia, że Izrael od dawna prowadzi dialog na temat cyberbezpieczeństwa z rządem Polski. "Minister Okoński wielokrotnie odwiedził Tel Awiw. Wynika to z tego, że Polacy traktują problem cyberbezpieczeństwa bardzo poważnie" - stwierdził w trakcie wystąpienia.

W swojej dalszej części wystąpienia przybliżył system Izraela. Podkreślił, że już w 2003 roku, długo przed jakimkolwiek państwem na świecie, Tel-Awiw dostrzegł problem cyberbezpieczeństwa infrastruktury krytycznej i zaczął go traktować jako zagrożenie dla bezpieczeństwa narodowego. Przełomowa zmiana w systemie cyberbezpieczeństwa Izraela dokonała się w styczniu 2012 roku — powiedział w trakcie wystąpienia Efrati. Mówił także, że Premier Netanjahu zdecydował się powołać nową strukturę: Narodowe Biuro Cybernetyczne, które obecnie nazywa się Narodowym Dyrektoriatem Cyberbezpieczeństwa. "Nazwa nie jest tu jednak najważniejsza. Często wizytując różne kraje, pytam się, kto jest odpowiedzialny za cyberbezpieczeństwo i nie dostaje odpowiedzi" - podkreślił Efrati. Izraelski generał dodał, że w tym objawia się wyjątkowość Izraela, ponieważ jest to jedno z nielicznych państw na świecie, gdzie za cyberbezpieczeństwo odpowiada bezpośrednio premier. Netanjahu zdaje sobie sprawę z powagi zagrożeń w cyberprzestrzeni.

Rami Efrati podkreślił, że Izrael nie chce być numerem 1, "bo wtedy każdy z nas będzie chciał nas atakować i sprawdzić nasze systemy zabezpieczeń. Chcemy jednak być w czołówce 5 państwa o najwyższym stopniu bezpieczeństwa" - dodał.

Jednocześnie Efrati wskazał, że Polska ma pewną przewagę nad Izraelem, wskazując na Ustawę o Krajowym Systemie Cyberbezpieczeństwa. Izrael takiego dokumentu jeszcze nie posiada. Brak takiej legislacji wynika z tego, że Izrael chciał działać, najszybciej jak się tylko da.