https://www.bbn.gov.pl/pl/wydarzenia/459,Seminarium-Infrastruktura-krytyczna-w-Polsce-w-Palacu-Prezydenckim.html
23.04.2024, 08:41

Seminarium "Infrastruktura krytyczna w Polsce" w Pałacu Prezydenckim

9 września 2002 roku w Pałacu Prezydenckim odbyło się seminarium pt. "Infrastruktura krytyczna w Polsce", zorganizowane przez Biuro Bezpieczeństwa Narodowego i Telekomunikację Polską S.A.

Seminarium otworzył szef BBN, minister Marek Siwiec, który zwracając się do zebranych, powiedział m.in.:

"Dzisiejsze spotkanie odbywa się w dosyć szczególnych okolicznościach, na dwa dni przed rocznicą ataku terrorystycznego na Stany Zjednoczone 11 września. Niewątpliwie to, co wydarzyło się w USA rok temu, jest memento i inspiracją do mówienia o zagrożeniach, tworzy wymóg przewidywania przyszłości w sposób bardziej kreatywny, niekonwencjonalny, z mniejszą ilością stereotypów, jak to zwykliśmy - mówię tu o politykach - robić przed 11 września.

Na tej sali spotkali się profesjonaliści, ludzie, których zaprosiła Telekomunikacja Polska oraz Biuro Bezpieczeństwa Narodowego. Jesteśmy w gronie osób, które zawodowo zajmują się przekazywaniem informacji, ich gromadzeniem i przetwarzaniem. Chciałem wszystkich państwa serdecznie powitać, podziękować za przybycie, a szczególnie gorąco chciałem powitać naszych partnerów z zagranicy, którzy współpracują z Biurem Bezpieczeństwa Narodowego. Grono mamy więc bardzo reprezentatywne.

Czy mówimy o zagrożeniach realnych, czy może o zagrożeniach abstrakcyjnych? Pamiętajmy przez cały czas trwania dzisiejszej konferencji, że rok temu z zimną krwią zamordowano ponad trzy tysiące ludzi, spalono trzy tysiące ludzi. Pamiętajmy też, że jeśli ktoś był w stanie dokonać tego czynu, wykorzystując w nim wszystkie zdobycze technologii, wykorzystując wszystkie zdobycze wolności i demokracji, korzystając też z niemałych zasobów finansowych - jest w stanie dokonać jakiegokolwiek innego aktu agresji, aktu zniszczenia. Zamordowano ludzi, ale tak naprawdę cios wymierzony był w funkcjonowanie najsilniejszego państwa na świecie. W związku z tym wyzwanie, które stawiamy sobie dzisiaj, dyskusja o ochronie infrastruktury krytycznej, jest zadaniem praktycznym, to nie jest zadanie wirtualne.

Obrona infrastruktury krytycznej, fizycznych i wirtualnych systemów o zasadniczym znaczeniu dla funkcjonowania gospodarki i rządu, nie jest nowym obszarem działalności państwa. Jednak wraz z rozwojem Internetu oraz powiązanych z nim wirtualnych infostrad polityka państwa odnośnie do tego problemu musi ulec redefinicji. Istnieje potrzeba elastycznego, ewolucyjnego podejścia, które umożliwi wykorzystanie zarówno publicznych, jak i prywatnych zasobów w celu ochrony bezpieczeństwa państwa. Założeniem dzisiejszej konferencji jest właśnie wypracowanie takiego podejścia, a także zainicjowanie prac nad przygotowaniem wspólnej strategii państwa dotyczącej ochrony infrastruktury krytycznej.

Jak wykazały wydarzenia 11 września 2001 roku, żadne państwo nie może czuć się bezpiecznie wobec tego typu zagrożeń. Polska, jako inicjator konferencji na temat zwalczania terroryzmu, czuje się szczególnie predystynowana do napełnienia wtedy formułowanych założeń treścią. Zgodnie z postanowieniami przyjętymi przez szefów państw biorących udział w konferencji warszawskiej, zagadnienia związane z ochroną infrastruktury

krytycznej są również częścią zadań, które powinny zostać podjęte w ramach kampanii działań przeciwko terroryzmowi.

Postęp technologiczny oraz nowoczesne technologie teleinformatyczne wpływają na zmianę uwarunkowań polityki bezpieczeństwa państwa. Nie ma dzisiaj systemów zamkniętych, państw - enklaw. Powstanie globalnej wioski informacji sprawiło, że należy teraz zwrócić większą uwagę na bezpieczeństwo informacyjne. Informacja stała się zasobem strategicznym gospodarki, podstawowym dobrem, którym dysponuje państwo i społeczeństwo. Celem przyszłego ataku mogą być nie tylko obiekty wojskowe, ale również na przykład centra informacyjne i kluczowe sieci teleinformatyczne oraz system finansowy państwa.

Ochrona infrastruktury informatycznej oraz telefonicznej jest o tyle istotna, że skutki wirtualnego ataku mogą być katastrofalne. Choć takie zagrożenie może się wydawać z perspektywy Polski odległe, to pamiętajmy, że czasy zmieniają się o wiele szybciej niż ludzie, i konstruując jakąkolwiek strategię bezpieczeństwa, myślą musimy wybiegać co najmniej o dekadę lub jeszcze dalej naprzód. Niezbędne jest też partnerstwo sektora prywatnego i państwowego w celu wspólnego zabezpieczenia infrastruktury krytycznej.

Proponuję, żeby wysiłek uszczelnienia istniejących już zabezpieczeń oraz wytworzenia spójnego systemu ochrony infrastruktury krytycznej opierał się na trzech filarach: zapobieganiu, ochronie oraz reakcji.

Dziękuję Państwu za przybycie! Jesteście Państwo gośćmi prezydenta RP Aleksandra Kwaśniewskiego. Pałac Prezydencki jest miejscem, które dobrze służy otwartej i szczerej dyskusji. Do takiej dyskusji zachęcam!".

Po wystąpieniu ministra Marka Siwca uczestnicy seminarium wysłuchali referatów poświęconych infrastrukturze kryzysowej, które wygłosili:

- prezes TP S.A. Marek Józefiak: "*Rola operatora narodowego w integracji infrastruktury krytycznej*";
- Kenneth Watson (USA): "*Infrastruktura krytyczna - doświadczenia USA po 11 września*";
- dyr. Robert Kośla (Agencja Bezpieczeństwa Wewnętrznego): "*Infrastruktura krytyczna w Polsce*";
- Karl F. Rauscher (USA): "*Co się wydarzyło w systemie telekomunikacyjnym USA po 11 września*".
