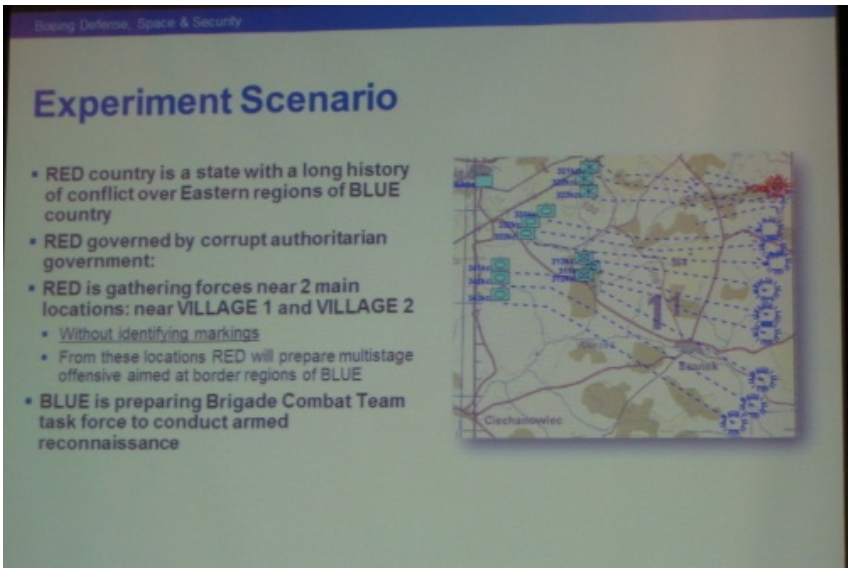
Polska doktryna cyberbezpieczeństwa państwa

#Strategia i polityka 7 listopada 2014

Szef Biura Bezpieczeństwa Narodowego (BBN), Stanisław Koziej, po raz pierwszy podał do publicznej wiadomości informację o pracach nad projektem polskiej doktryny cyberbezpieczeństwa państwa podczas międzynarodowej konferencji – Zagrożenia w cyberbrzestrzeni – bezpieczeństwo ponad granicami. Imprezę, która wczoraj odbyła się po raz drugi, wspólnie zorganizowały Zarząd Targów Warszawskich i Agencja Lotnicza Altair – wydawca magazynu RAPORT-wto.



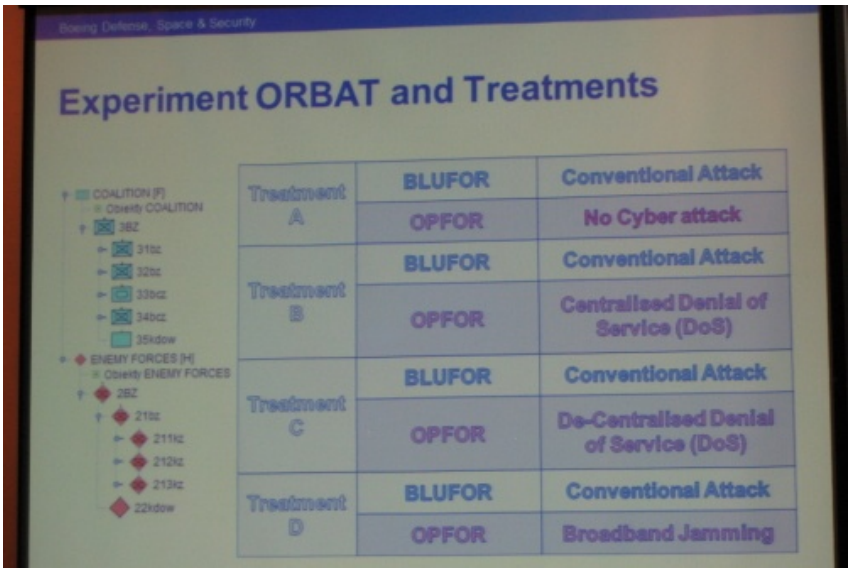
Militarna gra symulacyjna – wojna w cyberprzestrzeni. Na początku założono, że działania prowadzą przeciwko sobie dwie formacje – batalion Czerwonych – atakującego państwa autorytarnego i brygadowa grupa bojowa Niebieskich – prowadząca rozpoznanie bojem zaatakowanego terenu przygranicznego

Konferencja w warszawskim hotelu Marriott – połączona z wystawą najnowszego sprzętu kryptologicznego i rozwiązań do prowadzenia działań w cyberprzestrzeni – zgromadziła czołówkę instytucji odpowiedzialnych za bezpieczeństwo informatyczne państwa – z BBN, Ministerstwem Administracji i Cyfryzacji, Narodowym Centrum Kryptologii MON, Agencją Bezpieczeństwa Wewnętrznego i Policją na czele. Stała się ona kolejnym – po ubiegłorocznej pierwszej edycji – największym w Polsce forum wymiany myśli, poglądów i nowoczesnych idei technologicznych, a także sceną debaty na temat wszelkich działań w cyberprzestrzeni. W tym także działań wrogich – godzących w bezpieczeństwo państwa i w dobro jego obywateli.

Szef BBN, Stanisław Koziej, w swoim wprowadzeniu do dyskusji zaprezentował zarys rodzącego się dokumentu podstawowego – projektu polskiej doktryny cyberbezpieczeństwa państwa. Według jego słów ma to być *sektorowy dokument wykonawczy* do najnowszej, zatwierdzonej właśnie przez prezydenta Bronisława Komorowskiego Strategii Bezpieczeństwa Narodowego (zastępuje ona dokument z 2007). Jak oświadczył Koziej, projekt cyberdoktryny przygotowany zostanie do końca

2014, 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 ma 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.



Starcie doskonale wyposażonych i posiadających znaczną przewagę Niebieskich przeciwko intruzom (Czerwonym) postanowiono rozegrać w kilku wariantach. Głównie jednak testując zastosowanie przez Czerwonych konwencjonalnych zasad walki i działań prowadzonych z użyciem narzędzi wojny cybernetycznej i bezwzględnego starcia radioelektronicznego (zagłuszanie i aktywny atak na środki dowodzenia i łączności)

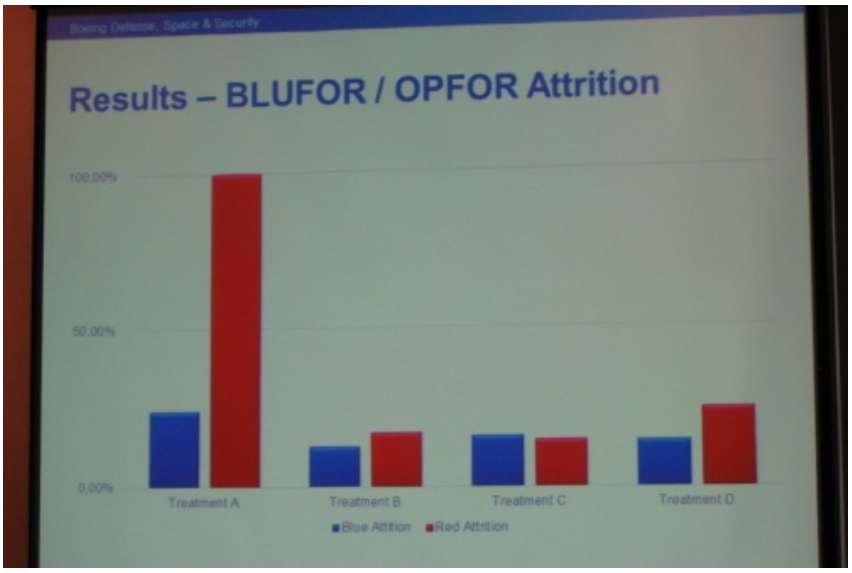
Stanisław Koziej ujawnił po raz pierwszy kształt nowego dokumentu. Doktryna zawierać ma cztery grupy zagadnień. Po pierwsze – określać ma cele o charakterze operacyjnym i przygotowawczym na polu cyberbezpieczeństwa. Ma to być rozwinięcie pojęciowe podstawowego celu strategicznego ujętego w najnowszej Strategii Bezpieczeństwa Narodowego, jakim jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej (tj. państwa, społeczeństwa, podmiotów prywatnych i obywateli) w cyberprzestrzeni.

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

Po trzecie – identyfikować najważniejsze *zadania operacyjne* dla zapewnienia cyberbezpieczeństwa, jakie powinny być stawiane 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 – zaakcentował Koziej

Po czwarte – rekomendować działania mające na celu *przygotowanie*(tj. doskonalenie, rozwój, transformację) systemu cyberbezpieczeństwa, z uwzględnieniem *podsystemu zarządzania sprawami cyberobrony oraz publicznych i prywatnych ogniw wykonawczych*.



Bilans starcia intruzyjnego batalionu Czerwonych z działającą w przewadze brygadową grup bojową Niebieskich w różnych wariantach zastosowania środków broni radioelektronicznej i walki w cyberprzestrzeni. W wersji A – konwencjonalnej walki – Czerwoni nie mają najmniejszych szans, a ich straty sięgają 100%, co oznacza fizyczną eliminację intruzów. W pozostałych wariantach z zastosowaniem przez Czerwonych elektronicznych i cybernetycznych środków paraliżowania przewagi Niebieskich – straty się wyrównują, a zwycięzcę trudno zdecydowanie wyłonić / Rysunki: Boeing Phantom Works i Wojskowa Akademia Techniczna

Szef BBN pokreślił, że w tym kontekście szczególnego znaczenia nabiera kształcenie kadr i rozwijanie narodowych kompetencji na polu kryptologii. Co jest wspólną powinnością Narodowego Centrum Kryptologii MON i warszawskiej Wojskowej Akademii Technicznej.

Efektem ubiegłorocznej pierwszej konferencji *Zagrożenia w cyberbrzestrzeni – bezpieczeństwo ponad granicami* (Cyber Security 2013 – wnioski dla Polski , 2013-10-29) stało się nawiązanie współpracy między doświadczalnym centrum innowacyjnych technologii korporacji Boeing – znanym jako Phantom Works i warszawskiej Wojskowej Akademii Technicznej. Współpraca przyniosła pierwszą na tę skalę przeprowadzoną w Polsce militarną grę symulacyjną, która przynieść miała odpowiedź na pytanie – w jaki sposób zastosowanie zaawansowanych narzędzi wojny w cyberprzestrzeni wpłynąć może na przebieg konwencjonalnego starcia między konkretnymi wydzielonymi jednostkami wojskowymi. Scenariusz i wyniki symulacji za pomocą wspólnych narzędzi badawczych omówili na tegorocznej konferencji w Warszawie Andrew McMahon, Chief Engineer Strategic Development & Experimentation Phantom Works Boeinga i prof. Andrzej Najgebauer z Instytutu Systemów Informatycznych WAT.

Powiązane wiadomości
