https://www.bbn.gov.pl/pl/wydarzenia/6351,Doktryna-cyberbezpieczenstwa-RP-Dokument-na-rzecz-skutecznosci.html
19.04.2024, 01:39

25.01.2015

“Doktryna cyberbezpieczeństwa RP. Dokument na rzecz skuteczności”

Przedstawiamy artykuł szefa BBN Stanisława Kozieja oraz Marcina Skowrona na temat Doktryny cyberbezpieczeństwa Rzeczypospolitej Polskiej. Tekst opublikowany został 25 stycznia br. na portalu Wszystko Co Najważniejesze.

“Doktryna cyberbezpieczeństwa RP. Dokument na rzecz skuteczności”

Stanisław Koziej, Marcin Skowron

Pojawienie się ogólnoświatowej sieci komputerowej w ciągu zaledwie kilkunastu lat zrewolucjonizowało nasze życie. Internet przyczynił się do gigantycznego postępu technologicznego i zmienił sposób postrzegania świata.

Jak każda rewolucja, także i ta stała się źródłem zarówno wielkich szans, jak i potencjalnego ryzyka. Za przenoszonymi do sieci tradycyjnymi ludzkimi aktywnościami, podążyły tradycyjne zagrożenia - od tych dotykających pojedynczego obywatela, po zakłócające funkcjonowanie całych państw, armii i społeczeństw. Niestety, o wiele trudniej było przenieść do wirtualnej rzeczywistości tradycyjne narzędzia służące radzeniu sobie z nimi.

Polska – jak większość państw – stoi dziś przed wyzwaniem zapewnienia sobie możliwie bezpiecznego funkcjonowania w cyberprzestrzeni. Oczywiście na co dzień wiele instytucji, służb i przedsiębiorstw profesjonalnie dba o cyberbezpieczeństwo w obszarach swojej odpowiedzialności. Brakuje jednak spójnego, skoordynowanego, systemowego podejścia do cyberbezpieczeństwa, dotyczącego wszystkich obszarów funkcjonowania państwa i obywateli. A właśnie w taki wielowymiarowy sposób powinniśmy je traktować.

Rozpoczynając budowę systemu, wpływającego na tak wiele podmiotów i obszarów, potrzebujemy wspólnego mianownika, jednego punktu wyjścia podejmowanych działań. Musimy uzgodnić, gdzie widzimy ryzyka, gdzie szanse. Jakie cele chcemy osiągnąć i jakich potrzebujemy do tego narzędzi. To właśnie był cel, który przyświecał opublikowanej przed kilkoma dniami Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej. Pierwszego w Polsce dokumentu o takim charakterze.

Nie chcielibyśmy tu przedstawiać jej treści, raczej zachęcić do przeczytania Doktryny. Tym bardziej, że problem bezpieczeństwa w sieci dotyczy zapewne każdego odbiorcy tego tekstu – jako że jest on publikowany właśnie w internecie... Warto natomiast zwrócić uwagę na kilka wątków wyróżniających Doktrynę. Propozycji nowych, czy

tych szczególnie istotnych z punktu widzenia myślenia o bezpieczeństwie.

Po pierwsze, należy zaznaczyć, że Doktryna nie jest dokumentem opracowanym wyłącznie przez Biuro Bezpieczeństwa Narodowego. W ramach prac nad nią udało nam się zaprosić do dobrej i konstruktywnej współpracy liczne instytucje, resorty i służby, przedstawicieli środowiska akademickiego, prywatnych przedsiębiorców (firm informatycznych, telekomunikacyjnych, instytucji finansowych) i organizacji pozarządowych. Taka formuła była szczególnie cenna, ponieważ problem cyberbezpieczeństwa dotyczy, w różnym stopniu, wszystkich powyższych aktorów. A konkretne rozwiązania – aby były skuteczne – muszą być wypracowywane wspólnie. W Doktrynie znalazło to odbicie w licznych postulatach dotyczących publiczno-prywatnej współpracy, takich jak tworzenie mechanizmów wymiany informacji o zagrożeniach, przekazywanie sektorowi prywatnemu opracowanych na poziomie państwa dobrych praktyk i standardów bezpieczeństwa czy kooperacji przy tworzeniu projektów legislacyjnych.

Przechodząc do drugiego zagadnienia należy zaznaczyć, że nie chcemy tu zabrzmieć alarmistycznie, a jedynie przedstawić określony sposób myślenia. Zapewnianie bezpieczeństwa obywateli przez państwo zawsze wiązało się z ponoszonymi przez nich kosztami. To zupełnie naturalne. Wchodząc dziś na pokład rejsowego samolotu, godzimy się na kontrolę, która czasem narusza prywatność, ponieważ mamy świadomość, że dzieje się to w imię naszego bezpieczeństwa. Problem ten dotyczy też funkcjonowania w cyberprzestrzeni. Być może nawet w większym stopniu, ponieważ trochę przywykliśmy do tego, że sieć jeszcze niedawno była swego rodzaju „Dzikim Zachodem" – terytorium nie do końca uregulowanym.

Temat zapewnienia równowagi pomiędzy środkami bezpieczeństwa a swobodami obywatelskimi w Doktrynie pojawia się już na samym początku. Dalej zwraca ona uwagę chociażby na fakt, że wprowadzanie konkretnych mechanizmów zabezpieczających państwo, instytucje i obywateli, może spotykać się ze społecznym sprzeciwem, powodowanym obawami o naruszania wolności osobistych czy gospodarczych. Doktryna podkreśla w tym zakresie wagę dialogu i konsultacji społecznych, które z jednej strony są dla obywateli szansą jak najlepszego zrozumienia istoty problemu i proponowanych rozwiązań, a z drugiej, zapewniają potrzebną kontrolę społeczną.

Kolejne z zagadnień podniesionych w Doktrynie było dotychczas pewną tajemnicą poliszynela. Zapewnienie przez państwo bezpiecznego funkcjonowania w cyberprzestrzeni nie może wiązać się jedynie z tworzeniem systemów czysto defensywnych. Państwo musi mieć możliwość tzw. aktywnej obrony – czyli zwalczania źródeł zagrożeń, zakłócania ich i niszczenia. Chcąc być bezpiecznymi musimy posiadać także zdolności do uderzeń odwetowych czy prowadzenia cyberkonfliktu (jako jednego z podstawowych elementów współczesnych wojen). Tym bardziej, że zdolności te, same w sobie mogą odstraszyć agresora. Takim potencjałem muszą dysponować siły zbrojne i powinien to być jeden z priorytetów ich rozwoju.

Po części łączy się z tym następny ujęty w Doktrynie postulat, jakim jest konieczność inwestowania w narodowe rozwiązania w dziedzinie cyberbezpieczeństwa, także w dziedzinie kryptologii, oraz zapewnienie sobie pełnego panowanie nad informatycznymi systemami wykorzystywanymi na rzecz bezpieczeństwa. Krytyczne znaczenie ma to oczywiście w przypadku środków łączności wykorzystywanych przez władze państwa, a także sprzętu wojskowego i uzbrojenia. Trudno sobie wyobrazić sytuację, w której nasz potencjał miałby opierać się na systemach informatycznych obcej produkcji, do których nie mielibyśmy pełnego zaufania. Czyli mówiąc wprost, nie dysponowalibyśmy kodami źródłowymi ich oprogramowania.

Podobnych problemów, które dotychczas nie były szerzej poruszane, znalazło się w Doktrynie znacznie więcej. Tym bardziej zachęcamy do zapoznania się z jej treścią.

Na koniec jeszcze jedna rzecz. Rozpoczynając prace nad Doktryną stanęliśmy przed dylematem - czy naszym celem powinno być zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, czy też zapewnienie bezpieczeństwa

cyberprzestrzeni RP? Chociaż problem brzmi dość akadamicko, w praktyce okazał się bardzo istotny z punktu widzenia filozofii myślenia o bezpieczeństwie. Jednak wspominamy o tym, ponieważ konieczność odpowiedzi na to zasadnicze pytanie pokazała, na jakim byliśmy etapie myślenia o budowie narodowego systemu cyberbezpieczeństwa. Dziś znajdujemy się o wiele dalej. Liczymy także, że publikacja „cyberdoktryny" będzie impulsem i podstawą do tworzenia coraz to bardziej zaawansowanych i skutecznych rozwiązań.

***

Źródło: wszystkoconajwazniejsze.pl
