https://www.bbn.gov.pl/pl/wydarzenia/6346,Szef-BBN-dla-informatora-RCB-Polska-musi-miec-mozliwosc-kontruderzenia-w-cyberpr.html
2021-09-20, 19:20



23.01.2015

# Szef BBN dla informatora RCB: Polska musi mieć możliwość kontruderzenia w cyberprzestrzeni

**Rozmowa z szefem BBN Stanisławem Koziejem dla publikacji Rządowego Centrum Bezpieczeństwa CIIP-focus na temat zagrożeń w cyberprzestrzeni, doświadczeń innych państw oraz Doktryny Cyberbezpieczeństwa RP. "- Rola sił zbrojnych w cyberbezpieczeństwie jest oczywiście bardzo duża, wręcz podstawowa w dziedzinie cyberobrony państwa. Siły zbrojne muszą zapewnić sobie bezpieczne funkcjonowanie, ale oczekuje się także od nich, aby stanowiły potencjał państwa, mogący zapobiec agresji w cyberprzestrzeni skierowanej wobec różnych elementów państwa, prywatnych firm i obywateli. Muszą mieć więc zdolności ofensywne, kontruderzeniowe" - mówi w rozmowie szef BBN.**

**Jakie są Pana zdaniem największe zagrożenia z cyberprzestrzeni, które mogą dotknąć RP oraz związane z nimi wyzwania i trudności dla Polski?**

*Szef BBN, Stanisław Koziej*: Musimy pamiętać, że nie tylko instytucje państwa i podmioty prywatne, ale i społeczeństwo staje się coraz bardziej zależne od cyberprzestrzeni. Można postawić tezę, że w cyberprzestrzeni będą istniały takie same zagrożenia jak w świecie realnym. Zarówno zagrożenia dla państwa jako całości – rywalizacja miedzy państwami, presja polityczno-militarna, zastraszanie, aż do ataków destrukcyjnych, zakłócających funkcjonowanie – jak i zwykła przestępczość, np. kradzieże danych, pieniędzy. Jednym z wyzwań jest także przeniesienie się protestów społecznych do cyberprzestrzeni. Szczególnie narażone są też firmy prywatne. Możemy tu mówić np. o wykradaniu danych, kopiowaniu produktów, itp.

**Czyli z tymi zagrożeniami, które tak naprawdę nie są nowe, ma się zmierzyć Doktryna Cyberbezpieczeństwa RP. Czy może Pan przybliżyć jej projekt?**

Doktryna jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego. Określa ona cele w dziedzinie cyberbezpieczeństwa. Stanowi też podstawę ideową, wspólny mianownik dla podejmowanych przez instytucje państwa działań. Stworzenie w Polsce takiego jednolitego podejścia do spraw cyberbezpieczeństwa powinno umożliwić dobre przygotowanie konkretnych już dokumentów wdrażających. Jak np. Polityka Ochrony Cyberprzestrzeni RP, ale nie tylko. Uważam, że Polityka nie obejmuje całości spraw związanych z cyberbezpieczeństwem. Dotyczy przede wszystkim sfery cywilnej i publicznej. Wydaje się, że oprócz Polityki pojawi się potrzeba opracowania dokumentu dotyczącego np. cyberobrony. Ministerstwo Obrony Narodowej z pewnością taki plan będzie przygotowywało.

Co więc charakterystyczne dla Doktryny, to kompleksowe, zintegrowane podejście. Konieczne jest połączenie w jeden całościowy system wielu wymiarów: cyberochrony i cyberobrony; wymiarów – wojskowego i cywilnego. Kolejną kwestią jest połączenie sfery publicznej i prywatnej. Bezpieczeństwa prywatnych podmiotów, przedsiębiorstw, instytucji, nie można uregulować aktami urzędowymi, tak jak można to zrobić w stosunku do administracji. Tutaj Doktryna proponuje korzystanie z katalogu „dobrych praktyk", zachęcanie do współpracy sektorów prywatnego i publicznego. No i to wszystko jeszcze uzupełnione wymiarem obywatelskim, indywidualnym. Państwo musi oferować obywatelom pomoc, wsparcie, edukację, zachęty, czy też musi wykorzystywać inicjatywy obywatelskie.

**Wspomniał Pan o wymiarze obywatelskim i stwierdził, że tej sfery nie można uregulować tak jak administracji i trzeba szerzej spojrzeć na zaangażowane podmioty. Jednym z krajów, który ciężko doświadczył tych zagrożeń, zarówno w sferze ochrony i obrony, jest Estonia. Jednym z pomysłów , który tam się pojawił jest ochotnicza cyber armia, czyli Estońska Liga Obrony Cybernetycznej. Jak ta koncepcja się Panu podoba, czy jest ona do zrealizowania na polskim gruncie, czy doktryna wspomina o tego typu łączeniu sił zarówno administracji , jak i stowarzyszeń, fundacji, think-tanków?**

- Pracując w BBN nad projektem Doktryny wykorzystaliśmy także doświadczenia innych państw, w tym m.in. Estonii. Staramy się zachęcać zarówno obywateli, jak i struktury państwa do współpracy, współdziałania, co łączy się ze wspomnianym wykorzystywaniem inicjatyw obywatelskich. W Polsce jest podatny grunt na tego typu działania, co stało się szczególnie widoczne w kontekście kryzysu bezpieczeństwa w Europie i rosyjskiej agresji na Ukrainę. Widać, że obywatele w większym stopniu niż to było rok czy dwa lata temu, poczuwają się do osobistego angażowania w zapewnienie bezpieczeństwa Państwa, w tym także cyberprzestrzeni. Niedawno miałem możliwość obserwowania ćwiczeń organizacji proobronnych w Ostrowcu Świętokrzyskim, gdzie pojawił się także element działań w cyberprzestrzeni.

**Elementem, o którym Pan wspomina jest cyberobrona. Czy mógłby Pan zarysować, jak wyobraża Pan sobie rolę sił zbrojnych w ochronie cyberprzestrzeni. Jak powinna wyglądać współpraca ze sferą cywilną ochrony cyberprzestrzeni i jednocześnie z podmiotami gospodarczymi. Czy nie wydaje się Panu że w sytuacji krytycznej przedsiębiorcy powinni liczyć na pomoc armii?**

Rola sił zbrojnych w cyberbezpieczeństwie jest oczywiście bardzo duża, wręcz podstawowa w dziedzinie cyberobrony państwa. Siły zbrojne muszą zapewnić sobie bezpieczne funkcjonowanie, ale oczekuje się także od nich, aby stanowiły potencjał państwa, mogący zapobiec agresji w cyberprzestrzeni skierowanej wobec różnych elementów państwa, prywatnych firm i obywateli. Muszą mieć więc zdolności ofensywne, kontruderzeniowe.

Polska musi mieć zdolność odwetowej operacji w cyberprzestrzeni. I to, moim zdaniem, jest jedno z wyzwań, przed jakimi stoją dzisiaj wszystkie państwa. Mechanizm ten dobrze pokazały ostatnie wydarzenia, gdzie Korea Północna, która prawdopodobnie – co jest niezwykle trudne do udowodnienia – zastraszyła dużą firmę, spotkała się ze zdecydowaną odpowiedzią. Musimy pamiętać – co pokazuje historia wojen – że sama obrona jest niewystarczająca. Trzeba mieć zdolności zarówno obronne, jak i ofensywne. I dlatego w Doktrynie wskazujemy na konieczność

budowania nie tylko potencjału obronnego, ale także zdolności kontruderzeniowych.

Oczywiście siły zbrojne nie mogą pełnić roli głównego koordynatora spraw cyberbezpieczeństwa w państwie. Tutaj dostrzegamy konieczność stworzenia systemu koordynacji podnadresortowej w zakresie cyberbezpieczeństwa. Zwracaliśmy na to uwagę już wcześniej m.in. w Strategicznym Przeglądzie Bezpieczeństwa Narodowego czy Białej Księdze. Widzimy konieczność utworzenia na szczeblu Rady Ministrów instytucji, która zajmowałaby się całościowym patrzeniem na wszystkie wymiary bezpieczeństwa, w tym na cyberbezpieczeństwo. Wskazujemy np. w Białej Księdze, że powinno to być swego rodzaju Rządowe Centrum Bezpieczeństwa Narodowego, z kompetencjami znacznie szerszymi niż tylko z zakresu zarządzania kryzysowego. Być może to jest kierunek, w którym powinniśmy iść. Bo jeśli chcemy całościowo, ponadresortowo regulować funkcjonowanie państwa w cyberprzestrzeni, to musi powstać instytucja państwa za to odpowiedzialna. Musimy także przygotować ludzi odpowiedzialnych za cyberbezpieczeństwo, uruchamiać nowe kierunki studiów. Jednym słowem tworzyć kompetencje narodowe w tej dziedzinie. Jedną z najważniejszych, bardzo specjalistycznych kompetencji, które musimy w kraju rozwijać jest kryptografia.

**Jak długo będzie trwało wdrożenie Doktryny cyberbezpieczeństwa RP?**

Jest to proces, który się nie kończy. Natomiast najważniejszy jest początek tego procesu, początek budowania zintegrowanego systemu, o którym mówimy. Na pewno Doktryna cyberbezpieczeństwa da pewien impuls. Wydaje się, że nadal będą budowane „wyspy" cyberbezpieczeństwa, o których teraz mówi się w teorii. Chciałbym, żeby już w przyszłym roku powstała instytucja, która mogłaby spinać w całość to, o czym mówimy, która zapewni ponadresortową zdolność realnego działania. Ze względu na wybory, 2015 r. jest trudny. Ale mam nadzieję, że jeżeli nie w 2015 to w 2016 r. takie instytucje powstaną – zarówno o charakterze politycznym, jak i o charakterze sztabowym. Bez tego trudno sobie wyobrazić realne nadążanie za szybko wzrastającymi potrzebami cyberbezpieczeństwa.

**Czy w związku z potrzebą tych wszystkich zmian widzi Pan konieczność skorzystania przez prezydenta z własnej inicjatywy ustawodawczej?**

Prezydent z pewną inicjatywą już wystąpił. Myślę tu o wprowadzeniu do ustawy o stanach nadzwyczajnych kategorii cyberprzestrzeni. Drugi krok prezydenta to właśnie Doktryna, która powinna dać impuls do działania. Natomiast praktyczne regulowanie życia państwa w cyberprzestrzeni jest jednak kompetencją rządu. Rząd może dużo tu zrobić nawet bez regulacji ustawowych. Mam na myśli tworzenie rozwiązań ponadresortowych. Ale jeżeli będą konieczne regulacje prawne, na przykład do zapewnienia systemowej współpracy sektora publicznego z sektorem prywatnym, to być może ze strony prezydenta taka inicjatywa się pojawi, ale pierwszy ruch należy do rządu.

**Dziękujemy bardzo.**

*Źródło: rcb.gov.pl*

---