https://www.bbn.gov.pl/pl/wydarzenia/3256,Szef-BBN-dla-Onetpl-Cyberbezpieczenstwo-w-stanach-nadzwyczajnych.html
24.04.2024, 08:17

25.07.2011

Szef BBN dla Onet.pl: Cyberbezpieczeństwo w stanach nadzwyczajnych

Zachęcamy do zapoznania się z tekstem ministra Stanisława Kozieja dotyczącym cyberbezpieczeństwa, opublikowanym przez portal Onet.pl.

Publikacja Onet.pl

Prezydent Bronisław Komorowski skierował do Sejmu projekt nowelizacji ustaw o stanach nadzwyczajnych, proponujący uzupełnienie ich o regulacje dotyczące uwzględniania w nich problematyki działań w cyberprzestrzeni. Parlament rozpoczął prace nad projektem na wspólnym posiedzeniu komisji Obrony Narodowej, Spraw Zagranicznych oraz Administracji i Spraw Wewnętrznych. Jutro (26.07.2011 r.) czeka nas merytoryczna debata nad projektem w specjalnie do tego celu powołanej podkomisji. To niewątpliwie dobra decyzja i ważne wydarzenie w procesie transformacji polskiego systemu bezpieczeństwa narodowego. Bo sprawy przygotowania państwa i jego struktur do działania w cyberprzestrzeni należą z pewnością do priorytetowych.

Z tego względu bardzo pożądana byłaby także szersza, publiczna dyskusja nad nimi. Warto byłoby rozpocząć ją od refleksji najogólniejszej. Otóż era rewolucji informacyjnej, w którą już na całego weszliśmy, wymaga od nas – mam na myśli całe państwo, poszczególne jego segmenty i każdego obywatela z osobna – umiejętności organizowania się do życia i funkcjonowania w jakościowo zupełnie nowym środowisku, jakim jest środowisko informacyjne, a w nim jego szczególny wymiar, jakim jest cyberprzestrzeń. Powoli uświadamiamy sobie, że w zasadzie wszystko, co zwykliśmy do tej pory robić w tradycyjnej rzeczywistości (w "realu") może mieć i będzie miało swoje odpowiedniki (a niekiedy wręcz wypierające "oryginał" zamienniki) w cyberprzestrzeni. Już dawno do cyberprzestrzeni przeniosła się większość zadań łączności i komunikacji międzyludzkiej (w torbach listonoszy jest coraz mniej listów). Finanse, handel, usługi, administracja, nauka, edukacja, kultura itp., itd. – to obszary ludzkiej aktywności w coraz większym stopniu obejmujące cyberprzestrzeń.

Dotyczy to w całej rozciągłości także spraw bezpieczeństwa. Zauważmy, że ludzkość przez wieki nauczyła się organizować sobie bezpieczeństwo w geoprzestrzeni, czyli na lądzie, morzu, w powietrzu, a ostatnio człowiek opanowuje do tego celu także przestrzeń kosmiczną. Cyberprzestrzeń jest jednak czymś jakościowo zupełnie innym. Jest tym środowiskiem, z którym dopiero się oswajamy. Ale logika i doświadczenie historyczne podpowiadają, że będziemy musieli w niej rozwiązywać analogiczne problemy, z jakimi mamy do czynienia w tradycyjnej geoprzestrzeni.

Obrazowo mówiąc, gdybyśmy do całej dotychczasowej teorii i praktyki bezpieczeństwa w geoprzestrzeni przystawili cybernetyczne lustro, to powinniśmy zobaczyć w nim cybernetyczne odbicie wszystkich znanych nam już dotychczas kategorii bezpieczeństwa: różnych rodzajów zagrożeń, ryzyk, szans i wyzwań, koncepcji strategicznych, metod operacyjnych i taktycznych itp. Jednym słowem: musimy w owej cyberprzestrzeni

zorganizować system bezpieczeństwa tak samo, w takim samym zakresie, jak w geoprzestrzeni. Musimy skorygować, uzupełnić, a gdzie trzeba, opracować nowe strategie, plany operacyjne i programy preparacyjne (przygotowawcze). To ilustruje ogrom wyzwań i zadań, przed jakimi stoimy.

Wiemy, że aby taki proces wystartował i mógł być prawidłowo realizowany przez państwo i jego instytucje, potrzebne są podstawy prawne. Bez nich wszakże nic w państwie dziać się nie może. I to właśnie jest główną przesłanką inicjatywy Prezydenta. Zapoczątkować proces tworzenia takich podstaw.

Celem bezpośrednim prezydenckiego projektu ustawy jest stworzenie podstaw prawnych do uwzględniania problematyki cyberprzestrzeni w przygotowaniu się państwa na ewentualność działania w takich sytuacjach szczególnych zagrożeń, przy takiej ich skali i natężeniu, w których Konstytucja przewiduje możliwość wprowadzenia jednego ze stanów nadzwyczajnych: stanu klęski żywiołowej, stanu wyjątkowego lub stanu wojennego.

Dlaczego akurat od tego, od stanów nadzwyczajnych, zaczynamy? Dlaczego tutaj wybraliśmy punkt startu? Przecież te problemy występują nie tylko w sytuacjach nadzwyczajnych (szczególnych zagrożeń), ale także w różnych bieżących sytuacjach kryzysowych, a nawet w zwyczajnym, codziennym życiu. Otóż przesądziło o tym następujące, pragmatyczne rozumowanie.

Po pierwsze: jest to problematyka w pewnym sensie szczególnie bliska Prezydentowi. To w jego kompetencjach leży wprowadzanie stanu wojennego i wyjątkowego. To on kieruje obroną państwa w stanie wojennym. Czuje się więc w jakiś sposób odpowiedzialny także za regulacje prawne w tym zakresie.

Po drugie: wystartować trzeba jak najszybciej. Wyzwania narastają. Inne państwa już nas wyprzedziły: niektóre mają nawet bardzo rozwinięte strategie i doktryny bezpieczeństwa w cyberprzestrzeni, organizują potrzebne instytucje, przygotowują siły i środki. NATO rozpoczęło budowę systemu cyberobrony. Powinniśmy w tym uczestniczyć. Im więc szybciej wprowadzimy kategorię cyberprzestrzeni do obiegu prawnego w dziedzinie bezpieczeństwa narodowego, tym lepiej. Tym szybciej struktury państwa będą mogły przejść już do praktycznego działania planistycznego i organizacyjnego.

Po trzecie wreszcie: ustanowienie regulacji dotyczących ewentualnego działania w stanach nadzwyczajnych nie pociąga za sobą bezpośrednich kosztów finansowych. Względy finansowe nie będą więc hamulcem w sposób naturalny wydłużającym proces legislacyjny.

W ten sposób kategoria cyberprzestrzeni może znaleźć się najszybciej, jak tylko można, w obiegu prawnym. Nie pozostaniemy zbytnio w tyle za innymi podmiotami i za potrzebami w ramach sojuszu północnoatlantyckiego. Furtka do dalszych koniecznych kroków zostanie otwarta dla legislatorów, decydentów, planistów i organizatorów w sferze bezpieczeństwa.

Ta logiczna kalkulacja może mieć swój sens praktyczny oczywiście pod warunkiem, że Parlament ją podzieli i bez zbędnej zwłoki rozpatrzy i uchwali przedłożony projekt ustawy.

W konkretnej treści projektu można wyróżnić dwa główne obszary regulacji.

Po pierwsze definiuje się w nim cyberprzestrzeń jako kategorię bezpieczeństwa. Rozumie się ją jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Oczywiście definicji cyberprzestrzeni jest wiele: od najbardziej ogólnych, wręcz filozoficznych, do bardzo wąsko praktycznych. Nic dziwnego, bo to nowa kategoria i sposób jej opisu dopiero się kształtuje. W ustawie przyjęto podejście umiarkowanie praktyczne do zdefiniowania cyberprzestrzeni, aby maksymalnie ułatwić wykorzystywanie jej w praktycznych pracach wdrożeniowych (decyzjach, planach i

programach). Definiuje się ją zatem jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

Nie wnikając w nadmierne teoretyzowanie należy jednak podkreślić, że w odróżnieniu od przestrzeni naturalnej (geoprzestrzeni) cyberprzestrzeń jest przestrzenią zbudowaną przez człowieka (sztuczną) i istniejącą tylko poprzez jego aktywność. Można wręcz powiedzieć, że działanie w cyberprzestrzeni jest jednocześnie jej tworzeniem. Albo inaczej - działanie w cyberprzestrzeni odbywa się poprzez jej kształtowanie. To coś takiego, jakby działalność w geoprzestrzeni wyrażała się np. w ciągłym przesuwaniu gór lub zmianie głębokości mórz.

Tę specyfikę, tę odmienność cyberprzestrzeni, warto dobrze sobie uświadomić, aby należycie, odpowiednio do tej specyfiki, planować i organizować działania w tej szczególnej przestrzeni.

Po drugie projekt ustawy doprecyzowuje, konkretyzuje charakterystykę przesłanek ewentualnego wprowadzenia któregoś ze stanów nadzwyczajnych przez uwzględnienie dodatkowo skutków i możliwości działań w cyberprzestrzeni.

Najistotniejszą jest zmiana opisu przesłanek wprowadzenia stanu wojennego przez doprecyzowanie pojęcia „zewnętrzne zagrożenie państwa". Do tej pory domyślnie rozumieliśmy je jako zagrożenia przychodzące do nas z zewnątrz, spoza naszego terytorium, z zagranicy.

Jeśli jednak tą kategorią chcemy objąć także cyberzagrożenia, to wystarczającym punktem odniesienia nie może być terytorium, z którego nadchodzi zagrożenie, ale tym punktem odniesienia musi być wyłącznie podmiot, który to zagrożenie stwarza, niezależnie od tego, gdzie pojawia się impuls tego zagrożenia.

Dlatego proponuje się doprecyzowanie, że zewnętrzne zagrożenie państwa – to celowe działania destrukcyjne (godzące w niepodległość, niepodzielność terytorium lub w ważny interes gospodarczy Rzeczypospolitej Polskiej, a także zmierzające do uniemożliwienia lub zakłócenia wykonywania przez organy państwowe ich funkcji) podejmowane przez zewnętrzne w stosunku do państwa polskiego podmioty, w tym także działania podejmowane przez nie w cyberprzestrzeni.

Konieczność takiego podejścia do definiowania zagrożeń zewnętrznych wynika z nowej jakości współczesnych zagrożeń. Niekoniecznie muszą one odnosić się tylko do terytorium państwa. Agresywne cele wobec państwa mogą być dzisiaj osiągane poprzez destrukcyjne oddziaływanie na jego ważne interesy gospodarcze (np. zagrożenia energetyczne) lub poważne zdezorganizowanie funkcjonowania organów państwa (np. masowy atak cybernetyczny).

Przyjęte w projekcie podejście wynika także z lawinowego, pod wpływem rewolucji informacyjnej, narastania sieciowości i asymetryczności we współczesnym środowisku bezpieczeństwa. Zauważmy, że pod tym względem działania w cyberprzestrzeni, w tym stwarzane w niej zagrożenia, są co do swej istoty bardzo podobne np. do działań i zagrożeń stwarzanych przez globalne sieci terrorystyczne.

Wymownym przykładem może być atak terrorystyczny na Stany Zjednoczone 11 września 2001 roku. To, że atak ten uznany został za atak zewnętrzny, wynika z faktu, że wykonała go Al-Kaida, choć wyprowadzony został z terytorium Stanów Zjednoczonych i do tego jeszcze wykonany przy pomocy amerykańskich środków. Proponowane zatem w ustawie o stanie wojennym doprecyzowanie ma więc nie tylko logiczne, ale także praktyczne uzasadnienie.

Biorąc pod uwagę, że zagrożenia terrorystyczne znalazły swoje odzwierciedlenie we wszystkich ustawach o stanach nadzwyczajnych, logiczne jest, aby także w podobny sposób potraktować cyberzagrożenia. Dlatego w ustawach o stanie klęski żywiołowej i o stanie wyjątkowym proponuje się uzupełnienia, że katastrofa naturalna

lub awaria techniczna oraz zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego mogą być spowodowane także zdarzeniami lub celowymi działaniami w cyberprzestrzeni.

Takie ujęcie nie tylko dostosowuje podstawy decyzji o ewentualnym wprowadzeniu stanu nadzwyczajnego do mogących rzeczywiście zaistnieć przesłanek, ale także daje impuls do rozpoczęcia przeglądu i uaktualnienia planów działania w sferze bezpieczeństwa (planów zarządzania kryzysowego, operacyjnych planów funkcjonowania na czas zagrożenia i wojny, programów przygotowań obronnych itp.) na wszystkich szczeblach struktury państwa (od centrum, przez województwa, aż do samorządów gminnych), z uwzględnieniem potrzeb i możliwości pojawiających się w cyberprzestrzeni.

W zakończeniu warto podkreślić, że projekt ustawy był szeroko konsultowany z właściwymi organami administracji rządowej oraz omawiany na posiedzeniach Rady Bezpieczeństwa Narodowego. Zyskał poparcie uczestników tych gremiów. Dlatego wypadałoby mieć nadzieję, że pomyślnie zdoła przebrnąć przez procedurę legislacyjną jeszcze w tej kadencji Parlamentu.

Autor: Stanisław Koziej
Źródło: Onet.pl
