aut. Grzegorz Małecki 01.10.2018

PŁK MAŁECKI: NOWA STRATEGIA CYBERBEZPIECZEŃSTWA POLSKI – FUNDAMENT POLSKIEGO EKOSYSTEMU CYBERBEZPIECZEŃSTWA [KOMENTARZ]

Nowa strategia cyberbezpieczeństwa Polski musi być konkretna i precyzyjna, ale jednocześnie nie może być dokumentem hermetycznym i adresowanym tylko do ekspertów. Powinna być instrumentem komunikacji rządu z obywatelami.

Jednym z najpilniejszych obowiązków rządu wynikających z uchwalonej niedawno ustawy o Krajowym Systemie Cyberbezpieczeństwa jest przyjęcie strategii na najbliższe 5 lat. Zastąpi ona przyjęte w 2017 roku „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022". Konieczność przyjęcia strategii nie wynika jednak wyłącznie z dyspozycji nowej ustawy, ale przede wszystkim determinuje ją niezwykle dynamiczny rozwój środowiska cyberprzestrzeni oraz narastające wyzwania dla bezpieczeństwa państwa i społeczeństw, będące konsekwencją zachodzących w efekcie zmian w całym otoczeniu. Posiadanie aktualnej strategii cyberbezpieczeństwa jest niezbędnym warunkiem świadomego kształtowania polityki państwa w tej dziedzinie, umożliwiającej nadawanie pożądanego kierunku zachodzącym zmianom oraz sprawowanie kontroli nad zjawiskami i procesami determinującymi stan bezpieczeństwa narodowego oraz stanowiącymi istotny element wielu kluczowych sektorów gospodarki, jak również jakości i poziomu życia społeczeństwa.

Ze znaczenia i wagi posiadania własnej, aktualnej strategii cyberbezpieczeństwa zdaje sobie sprawę zdecydowana większość nowoczesnych państw demokratycznych, które od wielu lat przygotowują kolejne, systematycznie aktualizowane wersje takich dokumentów. W mijającym miesiącu najnowszą strategię podpisał amerykański prezydent Donald Trump. W lipcu zarządzenie o rozpoczęciu prac nad nową wersją strategii, zastępującą tę z 2013 roku, przyjęły władze Hiszpanii. Kolejne państwa opracowujące nowe bądź nowelizujące dotychczasowe dokumenty strategiczne, bazują podczas tych prac zarówno na własnych doświadczeniach, jak również na najlepszych praktykach i standardach wypracowanych przez państwa uznane za wiodące w rozwoju technologii oraz systemów cyberbezpieczeństwa. Należy liczyć, że nasze władze pójdą tym samym tropem, korzystając z najlepszych dostępnych rozwiązań, których skuteczność została już zweryfikowana w praktyce.

Przystępując do prac nad strategią należy odpowiedzieć sobie na kilka podstawowych pytań dotyczących kształtu, zakresu, formy, struktury czy zawartości tego dokumentu, które zadecydują o jego praktycznym zastosowaniu i w efekcie spełnieniu celu, jaki przyświeca jego tworzeniu. Zasadniczą jednak kwestią, jaką należy rozstrzygnąć w pierwszej kolejności, jest określenie rzeczywistego odbiorcy, do którego będzie ona adresowana. Najnowsze doświadczenia najbardziej zaawansowanych w dziedzinie cyberbezpieczeństwa państw wskazują, że powinien nim być każdy uczestnik cyberprzestrzeni, czyli przeciętny polski obywatel. Wynika to z faktu, iż cyberprzestrzeń

oddziaływuje na całe społeczeństwo, przez co jej bezpieczeństwo jest uzależnione od zachowania każdego użytkownika. Społeczna świadomość zagrożeń oraz aktywny udział obywateli w inicjatywach i mechanizmach budujących odporność na nie oraz zdolność do zapobiegania i neutralizacji stanowią fundament skutecznego i efektywnego systemu cyberbezpieczeństwa. Strategia budowy i rozwoju takiego systemu musi zakładać masową partycypację społeczeństwa. Jednym z warunków zapewniających ją jest dotarcie z przekazem zawartym w dokumencie do szerokiego odbiorcy. Aby ten cel osiągnąć konieczne jest zapewnienie przyjaznej formy oraz zrozumiałej zawartości. Musi to być zatem dokument atrakcyjny w formie, także graficznej, zwięzły, napisany przystępnym językiem, jasnym i zrozumiałym stylem, o objętości oscylującej wokół 50 stron.

Strategia nie może być hermetycznym dokumentem, adresowanym wyłącznie do ekspertów, poruszającym zagadnienia o charakterze technicznym i specjalistycznym. Powinna być instrumentem komunikacji rządu z obywatelami - uczestnikami cyberprzestrzeni. Za jego pośrednictwem będą oni zarówno uświadamiani i uwrażliwiani na wyzwania związane z rozwojem świata cyfrowego jak również zapoznawani z wynikającymi z tego dla nich obowiązkami. Jednocześnie jednak, obywatel powinien otrzymać informację na temat zobowiązań jakie państwo na siebie przyjmuje w celu zapewnienia bezpiecznej cyberprzestrzeni oraz jakimi środkami zamierza ten cel osiągnąć. Skuteczność strategii będzie w równym stopniu zależna od zawartej w niej merytorycznej koncepcji działań co od zapewnienia ich społecznej recepcji oraz praktycznego wdrażania na poziomie masowych uczestników systemu.

Aby była użyteczna strategia powinna być konkretna i precyzyjna, zarówno jeśli chodzi o cele, jakie ma realizować, jak również w odniesieniu do środków i metod służących ich osiągnięciu. Cele muszą być sformułowane w sposób jednoznaczny oraz być kwantyfikowalne, tak aby każdy odbiorca był w stanie ocenić stopień ich realizacji. Obok jasnych i zrozumiałych celów należy wskazać konkretne kierunki i ścieżki działań, służących ich osiągnięciu oraz środki i metody, w tym mechanizmy i struktury, jakie mają to umożliwić. W tym kontekście szczególnie ważne będzie zaprezentowanie modelu finansowania wydatków państwa przeznaczonych na realizację strategii. Należy także sformułować jasną i spójną koncepcję rozwoju struktur państwa odpowiedzialnych za tworzenie i rozbudowę krajowego systemu cyberbezpieczeństwa.

Nowoczesna strategia powinna cechować się kompleksowym, horyzontalnym i holistycznym podejściem do zagadnienia cyberbezpieczeństwa, będącego w swej istocie dziedziną interdyscyplinarną. Punktem wyjścia do prezentacji założeń strategicznego rozwoju systemu powinno zatem być zaprezentowanie zwięzłej, ale wyczerpującej definicji pojęcia cyberbezpieczeństwa, uwzględniającej jej złożoną naturę oraz szerokie i przekrojowe ujęcie wszelkich aspektów jej funkcjonowania i rozwoju.

Niezwykle istotnym elementem dobrej strategii powinno być precyzyjne wskazanie oraz omówienie dóbr, których ochrona jest jednym z jej celów i zadań, jak również zagrożeń oraz ryzyk, którym są poddane, a także sposobów, w jakich mogą się zmaterializować. Budowa świadomości zagrożeń dla przeciętnego obywatela pochodzących z cyberprzestrzeni oraz zrozumienie mechanizmów zapewniających odporność na nie oraz sposobów postępowania w celu minimalizowania ich negatywnych efektów jest jednym z kluczowych warunków powodzenia strategii. Poświecenie temu zagadnieniu odpowiedniego miejsca w strategii jest jednak tylko jednym z wielu sposobów realizacji tego celu. Znacznie skuteczniejszym jest włączenie problematyki cyberbezpieczeństwa, np. jako osobnego przedmiotu, do programu nauczania w szkołach wszystkich szczebli. Takie działanie powinno zostać zaplanowane w ramach omawianej strategii w możliwie najszybszym terminie.

Odnosząc się do konkretnych postanowień, jakie powinny znaleźć się w strategii, to z cała pewnością punktem wyjścia, otwierającym rozważania na temat planowanych zamierzeń, powinna stać się ocena stanu wyjściowego. Konieczne jest zatem zwięzłe, ale szczere omówienie aktualnego stanu systemu

cyberbezpieczeństwa oraz warunków funkcjonowania cyberprzestrzeni, wskazanie słabości i deficytów, których niwelowanie będzie jednym z celów działań w najbliższych latach, a także mocnych stron i atutów, jakie cechują obecną sytuację, których wzmocnienie i rozbudowa w przyszłosci pozwoli realizować cele strategii. Dopiero dysponując taką bazą wyjściową, w postaci swoistej "fotografii" aktualnego stanu, pozwoli w zrozumiały sposób opisać zamierzenia, jakie państwo polskie stawia przed sobą oraz wskazać środki, metody, formy ich osiągania, przewidziane przez rząd. Warto przy tym pamiętać, żeby formułowane cele do realizacji z jednej strony były osiągalne, z drugiej zaś na tyle konkretne, żeby możliwa była wersyfikacja ich wykonania, czyli aby były rozliczalne. W przypadku materii jaką jest cyberbezprzestrzeń zadanie sformułowania takich celów jest szczególnie trudnym wyzwaniem, zważywszy na niezwykłą dynamikę rozwoju tej dziedziny. Prognozowanie zmian w tym środowisku na czas dłuższy niż 1 rok jest zadaniem niemal niewykonalnym. Nie można zatem wskazać jakiegoś stanu docelowego, jaki oczekujemy osiągnąć za 5 lat. Zamiast tego należy wyznaczyć warunki brzegowe w obszarach uznanych za kluczowe, jakich spełnienie będzie ambicją strategii, wskazując jednocześnie kryteria oceny i parametry o charakterze uniwersalnym, które pozwolą ocenić stopień osiągnięcia celów.

Bardzo ważnym zagadaniem, które koniecznie powinno zostać poruszone w strategii jest kwestia mechanizmów budowy zaufania w cyberprzestrzeni oraz roli państwa w tym zakresie, w szczególności instrumentów, w tym prawnych i instytucjonalnych, niezbędnych do implementacji, w celu osiągnięcia jego poziomu pożądanego z punktu widzenia bezpieczeństwa państwa. Wysoki poziom zaufania pomiędzy uczestnikami cyberprzestrzeni oraz w stosunku do instytucji państwa, zwłaszcza odpowiedzialnych za prawidłowe funkcjonowanie tego środowiska, jest fundamentalnym warunkiem bezpieczeństwa w świecie cyfrowym. Zadanie stworzenia optymalnych warunków, zapewniających pożądany stan należy do państwa. Jednym z obowiązkowych narzędzi jest powołanie wiarygodnej i kompetentnej instytucji, której misji powinno stać się tworzenie i promowanie standardów zachowań i najlepszych praktyk w tej sferze oraz doradztwo i wsparcie dla wszystkich potrzebujących w zakresie budowy skutecznych struktur i mechanizmów obronnych w cyberprzestrzeni. Równolegle konieczne jest gruntowna przebudowa istniejącego systemu reagowania na incydenty komputerowe, w kierunku budowy silnej i wysoce wyspecjalizowanej instytucji rządowej, odpowiedzialnej za przyjmowanie wszystkich zgłoszeń oraz jednocześnie za zapewnienie wsparcia także dla użytkowników prywatnych, także osób fizycznych, dotkniętych atakami komputerowymi. Dzisiejsze rozwiązania w tej sferze są mało efektywne i ograniczone do zbyt małego kręgu podmiotów.

Strategia cyberbezpieczeństwa wydaje się także właściwym miejscem do zaprezentowania koncepcji przeciwdziałania i zwalczania dezinformacji za pośrednictwem i w cyberprzestrzeni. Oczywiście zagadnienie zewnętrznej ingerencji podmiotów państwowych w procesy społeczne i polityczne poprzez manipulację informacją wykracza poza problematykę cyberbezpieczeństwa, jednak należy pamiętać, że cyberprzesterzeń jest jednym z głównych środowisk w jakim ta wojna informacyjna się toczy. Wszelkie strategie, koncepcje czy mechanizmy walki z tym zjawiskiem muszą uwzględniać wykorzystanie elementów tworzących system cyberbezpieczeństwa. Warto zatem juz na samym początku działania te skoordynować.

Nowoczesna narodowa strategia cyberbezpieczeństwa nie może ominąć kwestii budowy i rozwoju polskiego ekosystemu cyberbezpieczeństwa. O korzyściach wynikających z posiadania sprawnego systemu zapewniającego harmonijną współpracę w tej dziedzinie sektora przemysłu, nauki oraz administracji w nie trzeba dzisiaj już nikogo przekonywać. Świat dostarcza licznych przykładów takich ekosystemów i efektów ich działania. Niestety dotychczasowe dokonania w tej dziedzinie w Polsce należy uznać za zawstydzająco skromne. Nie ulega wątpliwości, że zmiana tego stanu w perspektywie najbliższych 5 lat, dzięki potencjałowi naszych ekspertów od zaawansowanych technologii, jest w zasięgu naszych możliwości. Realizacja takiego zadania powinna stać się jednym z priorytetów narodowej strategii cyberbezpieczeństwa na lata 2019 - 2024.