OPINIA Rady ds. Cyfryzacji do projektu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 to kluczowy dokument wyznaczający priorytety i kierunki działań na rzecz zapewnienia cyberbezpieczeństwa w Polsce w najbliższych latach. Będzie on wpływać w istotny sposób także na rozwój cyfryzacji kraju, w tym na rozwój sieci 5G. O ile ogólne założenia *Strategii* oceniamy jako słuszne i niezbędne do rozwoju cyfrowej i bezpiecznej gospodarki, to w naszej ocenie szczegółowy zakres dokumentu powinien zostać doprecyzowany.

Stoimy na stanowisku, że cyberbezpieczeństwo kraju, jego gospodarki i obywateli to w dzisiejszych czasach ważny priorytet działań władz publicznych. Aby zapewnić je na odpowiednim poziomie, potrzebne są znaczne nakłady finansowe. Niestety ani projekt *Strategii*, ani uzasadnienie do tego projektu nie wskazują poziomu nakładów finansowych niezbędnych dla osiągnięcia tego celu, ani konkretnych źródeł finansowania. Wskazano jedynie, że podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Konkretne koszty realizacji poszczególnych działań mają być określone dopiero w *Planie działań na rzecz wdrożenia Strategii*, który będzie przedstawiony Radzie Ministrów do akceptacji w terminie do 6 miesięcy od przyjęcia S*trategii*.

W dokumencie w pozycji „źródła finansowania" znajduje się zapis, że "*Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego*". Teza ta nie znajduje odzwierciedlenia w rzeczywistości. Przeciwnie - skala problemu i wyzwań wymaga alokowania i przeznaczenia znacznych środków budżetowych na budowanie odporności cybernetycznej, a także zabezpieczenia ich w ramach negocjowania funduszy unijnych. Ta potrzeba powinna bardzo wyraźnie wybrzmieć w *Strategii.*

Strategia również nie zawiera żadnych miar pozwalających ocenić stopień jej realizacji, przez co w niewielkim stopniu staje się dokumentem praktycznie wyznaczającym cele dla podmiotów wszystkich sektorów. Dopiero *Plan działań na rzecz wdrożenia Strategii* będzie wskazywał m.in. na oczekiwane efekty wynikające z realizacji poszczególnych zadań w ramach realizacji celów szczegółowych. Uważamy to za mankament dokumentu klasy „strategii", który takie miary winien proponować.

W naszym przekonaniu dokument w niewystarczającym stopniu odnosi się do stwierdzonego w niezależnych badaniach niskiego poziomu cyberbezpieczeństwa urzędów administracji samorządowej i samorządowych jednostek organizacyjnych. Wobec skali i zagrożeń, jakie wiążą się z nieprzygotowaniem jednostek samorządu terytorialnego do sprostania wyzwaniom cyberzagrożeń, jego zapewnienie – w naszym przekonaniu – stanowić winno odrębny cel szczegółowy *Strategii*.

Strategię sformułowano na dużym poziomie ogólności, co utrudnia ocenę jej kompletności i adekwatności do wyzwań. W dużym stopniu pomija ona kwestie infrastrukturalne, w tym

związane ze strukturą i charakterem podmiotów kluczowych z punktu widzenia realizacji *Strategii* i zapewnienia właściwego poziomu cyberbezpieczeństwa RP.

Cel główny opisany w projekcie *Strategii*, jak i towarzyszący mu nieprecyzyjnie sformułowany w tłumaczeniu na język polski przypis, nie obejmuje wszystkich ważnych strategicznie wymiarów. Dlatego postulujemy rozszerzenie definicji celu głównego o m. in. działania prewencyjne, działania zapewniające zdolność do reakcji na zmaterializowane zagrożenia, a także o ochronę infrastruktury cyfrowej i procesów cyfrowych, a nie tylko informacji.

Cel główny w zakresie zapewnienia cyberbezpieczeństwa obywateli ograniczony wyłącznie do lepszej ochrony ich informacji pomija istotny element niezakłóconego dostępu obywateli do informacji za pośrednictwem systemów teleinformatycznych. W efekcie, w celach szczegółowych potraktowano marginalnie działania związane ze zwiększeniem odporności na ataki mające na celu wpływanie na obywateli za pomocą nieprawdziwych informacji lub innych narzędzi wojny psychologicznej stanowiących element wojny hybrydowej toczonej w cyberprzestrzeni. Niewystarczająco opisano także ewentualne działania mające na celu zapobieganie pozbawiania obywateli dostępu do informacji prawdziwych, a usuwanych z przyczyn politycznych z cyberprzestrzeni przez podmioty prywatne z powołaniem się na ich wewnętrzne zasady i regulaminy pod pretekstem walki z nienawiścią lub podobnymi pretekstami.

Cele szczegółowe projektu *Strategii* nie odnoszą się do niektórych sektorów gospodarki narodowej, które powinny być przedmiotem szczególnej troski z punktu widzenia zapewnienia cyberbezpieczeństwa i odporności na ataki cybernetyczne, takich jak szeroko rozumiany sektor energii (w tym energetyka, paliwa, gaz) i inne sektory krytyczne w tym dostarczające obywatelom podstawowe media (w tym wodociągi), telekomunikacyjny, finansowy (w tym instytucje finansowe, fin-techy, obrót pieniężny).

W *Strategii* nie zapisano żadnych konkretnych działań, które odnoszą się do tych sektorów.

Ich pominięcie uniemożliwia realizację celu głównego w zakresie zwiększenia poziomu ochrony informacji m.in. w sektorze prywatnym. Projekt Strategii przewiduje jedynie dokonanie przeglądu regulacji sektorowych i szczególnych bez określenia kierunków przeglądu i ewentualnych zmian regulacyjnych dotyczących poszczególnych sektorów, w tym infrastruktury krytycznej oraz traktowanie bezpieczeństwa najważniejszych sektorów gospodarki ze szczególnym uwzględnieniem sektora energii oraz operatorów infrastruktury krytycznej i usług kluczowych w ramach celu szczegółowego 1.

W opisie celu szczegółowego 1. czytamy, że: *„z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków zmian i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK,*

CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa." W ramach realizacji postulatu o współpracy publiczno-prywatnej należy w tym miejscu dopuścić także konsultacje z podmiotami zewnętrznymi, w tym z sektorem prywatnym i organizacjami pozarządowymi.

W celu tym projekt *Strategii* zakłada również, że „*rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych*". Naszym zdaniem dokument powinien bardziej precyzyjnie określić i opisać docelowy model współpracy centrum i jednostek samorządu terytorialnego w zakresie budowania odporności i zdolności, a także zapobiegania incydentom.

Pozytywnie należy ocenić wskazanie konieczności doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G oraz wprowadzenie zmian prawnych umożliwiających odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa. Z uwagi na czasowy zakres dokumentu rekomendowane jest natomiast wzięcie pod uwagę także technologii 6G, dlatego postuluje się rozważenie zapisu "5G i sieci komórkowych kolejnych generacji".

W ramach celu szczegółowego 3 – zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa – nie wskazano wprost na włączenie w te działania polskiego przemysłu obronnego, co wydaje się, że jest pewnym brakiem ze względu na specyfikę przedsiębiorców przemysłu obronnego w odróżnieniu od przedsiębiorców prowadzących działalność na rynku cywilnym.

Jednocześnie postuluje się dokonanie zmian w opisie celu w punkcie 7.1, poprzez następującą modyfikację:

> „Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania urządzeń oraz oprogramowania systemowego i użytkowego, a także realizacji usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego cyberbezpieczeństwo, co bezpośrednio przełoży się na realizację celów związanych z transformacją cyfrową gospodarki i na zwiększenie jej konkurencyjności. Sektor cyberbezpieczeństwa, w ramach sektora teleinformatycznego, może także stać się siłą napędową wzrostu gospodarczego."

Proponuje się także wyróżnienie dwóch typów działań, które mogą zostać podejmowane przez polskie uczelnie, dotyczących rozwoju zasobów technologicznych i ludzkich, poprzez modyfikację stosownego fragmentu:

> „Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa w zakresie rozwoju zasobów technologicznych. Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące rozwojowi zasobów ludzkich z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych."

W punkcie projektu *Strategii*, który dotyczy stymulowania badań i rozwoju w obszarze cyberbezpieczeństwa, pominięte zostały technologie, które niewątpliwie zmienią krajobraz cyberbezpieczeństwa. Są nimi informatyka kwantowa oraz sztuczna inteligencja. Dlatego powinny one zostać dołączone do zapisu tego punktu. Postulujemy zatem następującą zmianę:

> „W związku z dynamicznie rozwijającym się rynkiem informatycznym, w szczególności w związku z perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6, a także w związku z rozwojem idei Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0, jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy technologii komputerów kwantowych oraz sztucznej inteligencji, a tym samym zwiększenia ilości przetwarzanych danych, zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa. W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze, mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami."

W dalszej części opisu omawianego celu szczegółowego napisano, że „w obliczu dynamicznie rozwijających się technologii związanych m.in. z Internetem Rzeczy należy zwrócić szczególną uwagę na konieczność zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (Security by Design)". Zasadnym wydaje się, że jako podobną zasadę przyjąć należy także ochronę danych i prywatności czyli Privacy by Design.

Postulujemy następującą modyfikacje tego zapisu: „W obliczu dynamicznie rozwijających się technologii związanych m.in. z Internetem Rzeczy należy zwrócić szczególną uwagę na konieczność zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (*Security by Design*), a także ochronę danych i prywatności (*Privacy by Design*). Rząd RP będzie promował i wspierał podejście uwzględniające bezpieczeństwo i ochronę danych i prywatności już od etapu projektowania."

W ramach celu szczegółowego 4. – budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa – wskazano m.in., że podnoszenie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP będzie realizowane poprzez stworzenie i wdrożenie takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników, a także opisano

mechanizmy mające zapobiegać utracie pracowników o wysokich kompetencjach przez sektor administracji publicznej na rzecz sektora prywatnego. Nie wskazano natomiast, jak zapobiegać utracie wykształconych w Polsce specjalistów w wyniku emigracji do innych krajów, ani mechanizmów powrotu do Polski specjalistów, którzy uprzednio wyemigrowali z Polski i uzyskali kwalifikację za granicą.

W zakresie celu szczegółowego 5, w punkcie „Aktywna współpraca międzynarodowa" na poziomie operacyjnym i technicznym należy konsekwentnie wspomnieć o potrzebie wypracowania wspólnych procedur działania także w ramach współpracy krajów Trójmorza.

Projekt *Strategii* nie zawiera bezpośrednich odniesień do realizowanego obecnie procesu zapewnienia obywatelom dowodów osobistych z warstwą elektroniczną i związanych z tym potencjalnych możliwości zwiększenia bezpieczeństwa obrotu z wykorzystaniem elektronicznych nośników tożsamości.

We wstępie do projektu *Strategii* nie nawiązano do wymiaru obronnego, który obejmuje dokument w dalszej swojej części. Dla zapewnienia spójności konieczne jest zatem rozszerzenie opisu przesłanek o związane z uwarunkowaniami nowoczesnego pola walki, zarówno w zakresie świadomości sytuacyjnej (informacja), jak i zdolności obronnych i defensywnych (zależnych od sprawnie funkcjonujących sieci i systemów IT). W związku z tym proponowane brzmienie punktu 1. projektu Strategii „Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo" powinien – naszym zdaniem - otrzymać brzmienie:

> „Rozwój społeczny i gospodarczy, a także bezpieczeństwo (militarne) w coraz większym stopniu zależne są od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Dynamiczny rozwój systemów informacyjnych, a także zwiększanie wydajności centrów przetwarzania danych, służą rozwojowi gospodarki, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych, a także warunkują zdolności obronne państw. Z wykorzystaniem technologii cyfrowych budujących cyberprzestrzeń, tworzone są i kształtowane relacje społeczne, a usługi w sieci Internet stały się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej i geopolitycznej."

Podobnie o aspekt bezpieczeństwa narodowego należałoby rozwinąć punkt 4.1. Strategii „Wizja". Proponujemy następujące jego brzmienie:

> „Pomyślny rozwój Polski, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym i aktywność społeczna oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa, jak i bezpieczeństwo Państwa są związane ze sprawnym i niezakłóconym działaniem systemów informacyjnych i środków komunikacji elektronicznej. Dlatego w ramach działań zaplanowanych w Strategii do roku 2024 rząd RP będzie systematycznie wzmacniał i rozwijał Krajowy System Cyberbezpieczeństwa. Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych, prowadzenie

badań naukowych, tak aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń i usług cyfrowych. Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz poprzez budowę zaufania pomiędzy poszczególnymi sektorami rynkowymi a administracją publiczną."

Z tego samego względu należy – w naszym przekonaniu - zmodyfikować punkt 9.1. celu szczegółowego 5, który wymienia instytucje istotne z punktu widzenia wzmocnienia polskiej pozycji międzynarodowej poprzez dodanie Ministra Obrony Narodowej obok ministra właściwego ds. informatyzacji oraz Ministra Spraw Zagranicznych.

W uzasadnieniu do projektu wskazano, że projekt nie będzie miał wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców. Powyższe stwierdzenie pozostaje w sprzeczności z częścią zapisów projektu Strategii (w celu głównym jest m.in. mowa o sektorze prywatnym bez ograniczenia go wyłącznie do dużych przedsiębiorców, w celu szczegółowym 3. jest mowa m.in. o stwarzaniu warunków dla rozwoju przedsiębiorstw jak i start-upów).

Józef Orzeł
Przewodniczący Rady
/podpisano elektronicznie/