Instytut
Mikromakro

Warszawa 7 października 2016 roku

Komentarz fundacji Instytut Mikromakro do dokumentu „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020 zaprezentowanej przez Ministra Cyfryzacji do konsultacji

Piotr Rutkowski
wiceprezes zarządu

Zadania poszczególnych organów władzy publicznej

Ref. 3.1. Wymiar strategiczny.

Strategia dosyć swobodnie interpretuje zadania poszczególnych organów władzy publicznej (BBN, min. sprawiedliwości, ABW, minister obrony narodowej, minister spraw wewnętrznych i administracji, komendant główny Policji, minister cyfryzacji) w zakresie cyberbezpieczeństwa, nie odnosząc ich do zadań określonych w ustawach kompetencyjnych, ale dodając na końcu każdemu obowiązek współpracy z pozostałymi „uczestnikami systemu". W tym systemie minister cyfryzacji ma pełnić „rolę usługową, nie wchodząc w kompetencje" innych. To dosyć niejasna właściwość w obowiązującym systemie konstytucyjnym.

Wątpliwości ma rozstrzygnąć zapowiedź przyszłej ustawy o krajowym systemie bezpieczeństwa. Jednak dla strategii jest to kwestia o znaczeniu fundamentalnym, tym bardziej że w podsumowującym podrozdział akapicie znalazła się oczywista konkluzja o wymogu koordynacji inicjatyw w zakresie cyberbezpieczeństwa.

Jak ma wyglądać funkcja koordynacyjna ministra cyfryzacji, którą określi wprowadzająca Strategię uchwała rady ministrów, jeżeli właściwy w sprawach cyberbezpieczeństwa minister cyfryzacji, sam deklaruje ograniczenie koncepcji swojej roli wobec innych instytucji do usługowej? (I jak to się ma do obecnej organizacji, gdzie Narodowe Centrum Bezpieczeństwa, które ma być wg strategii „na szczycie hierarchii podmiotów zaangażowanych w krajowy system bezpieczeństwa" działa w ramach NASK, który jest nadzorowany przez ministra cyfryzacji).

Można też odnieść wrażenie, że na razie kwestia podziału właściwości poszczególnych organów władzy publicznej w systemie cyberbezpieczeństwa państwa jest opisana raczej na poziomie operacyjnym, a nie strategicznym. Tym nie mniej narzuca się wiele pytań, na które powinna próbować odpowiedzieć strategia:

1. Jak powinna być zorganizowana koordynacja i współpraca w obowiązującym systemie podziału władzy pomiędzy poszczególnymi ministrami (zespół zadaniowy, tak jak obecnie, komitet rady ministrów, zespół międzyresortowy, inne)?

2. Czy i jak rozdzielić sferę cywilną i wojskową? Strategia przypisuje np. MON kompetencje w zakresie organizacji „aktywnej obrony i działań ofensywnych" (zdaje się, że to jest to samo), ale nie sygnalizuje, czy ten specyficzny sposób działań przeniesie się na sferę cywilną, która np. w obszarze infrastruktury krytycznej może być głównym celem cyberataków.
3. Jak ma być rola BBN, w tym Doktryny Cybeberbezpieczeństwa RP?

Zaznaczam, że tylko przykłady zagadnień, do rozstrzygnięcia których należałoby znaleźć na użytek Strategii ścieżkę dojścia.

Na końcu podrozdziału jest wzmianka o modelu współpracy administracji, biznesu i nauki. Model ten jest dokładniej omówiony w rozdziale 6, ale w części strategicznej dokumentu stosowny byłby komentarz, jakie jest strategiczne znaczenie tego rodzaju współpracy, szczególnie w zakresie partnerstwa publiczno-prywatnego i dlaczego państwo musi taką współpracę podjąć. To ma bardzo istotne znaczenie, gdyż ta na razie ta postulowana współpraca właściwie nie ma jeszcze precedensu w innych dziedzinach aktywności państwa.

Współpraca międzynarodowa

Strategia dosyć ogólnie traktuje temat współpracy międzynarodowej, wymieniając takie fora jak Unia Europejska, ONZ, NATO, OBWE. Wymiar polityczny, który tu podkreślono narzucałby konieczność udziału MSZ w gronie podmiotów zaangażowanych w ochronę cyberprzestrzeni RP, które wymienia rozdział 1.

Kwestia kto co koordynuje sprawy zagraniczne, czy minister cyfryzacji konsultując z ministrem spraw zagranicznych, czy minister spraw zagranicznych z pomocą merytoryczną ministra cyfryzacji, powinna być rozstrzygana na zasadach ogólnych, podobnie jak pozostałe obszary polityki zagranicznej. Minister cyfryzacji i tym razem zastrzega sobie we własnych kontaktach ostrożnie prawo do decyzji o charakterze roboczym, a także rolę pomocniczą, która nie wkracza w kompetencje innych podmiotów. Byłoby pewnie trudno wyobrazić sobie np. zastępowanie ministra obrony narodowej lub jednostek organizacyjnych sił zbrojnych we współpracy wojskowej z NATO lub EDA. Tak samo trudne byłoby wyręczać Policję w relacjach z Europolem (NC3).

Z drugiej strony minister cyfryzacji organizując centrum kompetencji państwa w sprawach cyberbezpieczeństwa powinien dysponować przynajmniej mechanizmem komunikacji z instytucjami prowadzącymi własną politykę kontaktów międzynarodowych. To niezbędne, by mieć w nią wgląd zarówno pod praktycznym kątem analizy zagrożeń, jak i w związku wpływem przedsięwzięć międzynarodowych na organizację krajowego systemu cyberbezpieczeństwa.

Ponadto z racji horyzontalnego charakteru problematyki zagrożeń z cyberprzestrzeni, na poziomie rządu powinien zostać utwierdzony mechanizm wymiany informacji o inicjatywach podejmowanych na forach międzynarodowych obsługiwanych przez ministrów (podległe im jednostki organizacyjne), którzy nie są wskazani, jako uczestniczący w stałym zespole instytucji centralnych, zajmujących się organizacją ochrony cyberprzestrzeni. Tego rodzaju potencjalnie „umykające" inicjatywy mogą się pojawiać w każdej dziedzinie (kultura, transport, budownictwo, infrastruktura, energetyka, sport, media). Między innymi właśnie z powodu takich okoliczności, praktycznie użyteczna byłaby pośrednia rola ministra spraw zagranicznych, który z klucza powinien wiedzieć o zagranicznych kontaktach organów administracji rządowej.

Strategia nie wymienia niektórych istotnych instytucji międzynarodowych, które już dzisiaj koordynują współpracę międzynarodową takich, jak ENISA , NC3 (Europol), Interpol, organizacje standaryzacyjne dla telekomunikacji i internetu, pomimo że w nich Polska uczestniczy, a w przypadku

ENISA, agencji unijnej wiodącej w sprawach cyberbezpieczeństwa, dzieje się to za pośrednictwem nadzorowanego przez ministra cyfryzacji NASK. Nie wspomniano np. o bardzo istotnych dla kształtowania systemu bezpieczeństwa praktycznych inicjatywach, jak międzynarodowe ćwiczenia ochrony cyberprzestrzeni, organizowane przez ENISA.

O ile w poprzednich wersjach strategii temat transpozycji dyrektywy NIS był nadmiernie eksploatowany, to w strategii jest wspomniany tylko w kontekście utworzenia w ministerstwie cyfryzacji punktu kontaktowego.

Współpraca z organizacjami pozarządowymi

Strategia nominalnie wymienia potrzebę podejmowania współpracy z organizacjami pozarządowymi. Hasło pojawia się nawet w tytule rozdziału 6, ale potencjał organizacji pozarządowych nie został poddany żadnej głębszej analizie, ani skomentowany. Wśród celów wspomniano tylko, że tak samo jak w przypadku ośrodków akademickich i sektora prywatnego współpraca może dotyczyć zarządzania wiedzą i stymulowania innowacji w dziedzinie cyberbezpieczeństwa w Polsce. Tam gdzie dokument omawia zadania ministra cyfryzacji, dowiadujemy się, że może też chodzić o edukację związaną z cyberbezpieczeństwem. Nie spróbowano np. rozpoznać, czym istniejące organizacje już się zajmują. Przykładowo, fundacje i stowarzyszenia, które na polskim rynku deklarują statutowe działania związane z problematyką cyberbezpieczeństwa państwa na poziomie strategicznym (Fundacja Bezpieczna Cyberprzestrzeń, Instytut Kościuszki, Fundacja im. Kazimierza Puławskiego oraz nasza fundacja Instytut Mikromakro) powstawały niezależnie. Łączy je aspiracja działania w formie think tanków. Każda specjalizuje się w nieco innej problematyce, więc chyba konkurujemy z sobą w minimalnym zakresie. Często udaje nam się wręcz łączyć siły we wspólnej trosce o bezpieczeństwo Polski. Organizujemy konferencje, konwersatoria, spotkania wybranych środowisk, powstają raporty analityczne. Z zasady oczekujemy patronatu urzędów właściwych w sprawach bezpieczeństwa państwa, ale żadna z naszych inicjatyw nie zastępuje aktywności instytucji rządowych, tylko je uzupełnienia i mam nadzieję przyczynia się do lepszego rozumienia strategicznie rozumianej problematyki bezpieczeństwa.

Forum ds. Cyberbezpieczeństwa i organizowane w jego ramach grupy robocze są według koncepcji Strategii potrzebnym zapleczem eksperckim. Można zakładać, że posłuży ono głównie do działań programowanych przez ministra cyfryzacji, w tym dając płaszczyznę wymiany informacji „pomiędzy interesariuszami". Niezależne inicjatywy podejmowane przez organizacje pozarządowe będą pogłębiać potencjał współpracy i współdziałania tworzony przez to Forum.

Warto może też zauważyć w tym miejscu, że krajowy system bezpieczeństwa, stanowiący główny jak się wydaje wątek Strategii, efektownie prezentowany w kilku miejscach w formie graficznej, jest systemem reagowania na incydenty. To warstwa operacyjna. Nie uwzględnia on roli forów planowania i wymiany informacji na poziomie strategicznym, które miałyby wspomagać procesy decyzyjne, polityczne, legislacyjne, standaryzacyjne. Przy okazji proponowany system w zasadzie nie przewiduje inicjatyw niezależnych, np. komercyjnych usługowych centrów reagowania.

Partnerstwo publiczno-prywatne (współpraca z komercyjnym sektorem prywatnym)

Ref podrozdział 6.2

Strategia powinna wyraźniej podkreślać wartość współpracy w ramach partnerstwa publiczno-prywatnego, bo w prezentowanym ujęciu wygląda to zwykłą na relację zamawiający – dostawca, uzależnioną od nakładów, które państwo jest w stanie przeznaczyć na poprawę stanu bezpieczeństwa systemów informacyjnych.

Tymczasem trzeba zwrócić uwagę na oczywisty fakt, że firmy prywatne od dawna są centrami kompetencji w sprawach cyberbezpieczeństwa (podobnie jak jest ogólniej ze wszystkimi nowymi technologiami). Ich potencjał polega nie tylko na zdolności wypełniania wymogów zamówień publicznych, ale zdolnościach badawczo rozwojowych, a od jakiegoś czasu również na gotowości oferowania usług z zakresu cyberbezpieczeństwa. Niektóre mają również zweryfikowane doświadczenia współpracy z krajowymi władzami bezpieczeństwa.

Chodziłoby zatem o dopracowanie i wdrażanie mechanizmów bezpiecznego transferu wiedzy pomiędzy sektorem prywatnym, a instytucjami administracji rządowej. Również wzajemnej. W tym też znaczeniu uzupełniona koncepcja programu „złota setka" może obejmować nie tylko dosyć w sumie ryzykowny mechanizm wyławiania z rynku edukacyjnego zdolniejszych specjalistów, którzy podejmą pracę w administracji, zamiast atrakcyjnych wyzwań komercyjnych.

Chodziłoby o umowy z firmami, również międzynarodowymi, które mają programy współpracy z rządem, dającymi rękojmię bezpieczeństwa i gwarantującymi dostęp do ekspertów, których wiedzę już rzetelnie zweryfikowało doświadczenie zawodowe.

Współpraca z przemysłem obejmuje również doskonalenie mechanizmów planowania, standaryzacji i oceny ryzyka z przedsiębiorcami kwalifikowanymi jako operatorzy infrastruktury krytycznej, operatorzy usług kluczowych lub wszyscy inni przedsiębiorcy, którzy dysponują wrażliwymi z punktu widzenia bezpieczeństwa systemami informacyjnymi. W tym przypadku nie chodzi tylko o mechanizmy reagowania i przeciwdziałania, o których w Strategii sporo, ale wymianę informacji i doświadczeń na temat bezpieczeństwa systemów informacyjnych stosowanych w gospodarce.

Współpraca z sektorem nauki, badań i rozwoju

Ref. podrozdział 6.3

Przedstawiona w Strategii koncepcja współpracy z uczelniami i jednostkami sektora badań i rozwoju , w tym finansowania projektów badawczych za pośrednictwem NCBiR wygląda konserwatywnie, nie gwarantując osiągnięcia spektakularnych efektów. Niewiele jest tu np. miejsca na wspieranie innowacyjności, w tym tak zwanych tzw. start-upów, które często powstają niezależnie od tradycyjnej infrastruktury badawczej.

Trzeba by tu też zwrócić uwagę, że kwestie cyberbezpieczeństwa są ważnym komponentem europejskiego programu wsparcia badań Horyzont 2020, należą do najważniejszych wątków unijnej strategii Digital Single Market oraz są też częścią wielu sektorowych programów rozwoju gospodarczego. Podobnie jest ze wspominanymi w strategii tematami takimi jak inteligentne miasta, internet rzeczy, bezpieczeństwo chmury itp.

Jeżeli mowa o polskiej Strategii, to należałoby usilnie dążyć do podnoszenia kompetencji krajowych jednostek badawczych poprzez wzmacnianie zdolności współpracy w różnego rodzaju międzynarodowych projektach, w tym również wykorzystując mobilność osób ze świata nauki. To pomaga podnosić i weryfikować rzeczywiste kompetencje badawcze, a wielu przypadkach również zdolność współpracy z przemysłem.

Załącznik: wybrane kwestie o charakterze redakcyjnym

Akceptowalny poziom bezpieczeństwa

Ref. rozdział 1 str.4

Pewną wątpliwość już na wstępie budzi samo sformułowanie celu strategii, jakim ma być osiągnięcie „akceptowalnego" poziomu bezpieczeństwa. Razem ze wskazanymi „zdolnościami" brzmi on jak ostrożny plan minimum, odnoszący się do wybranych krytycznie istotnych systemów informacyjnych.

To jasne, że zakres i szybko ewoluujący charakter, czy to obecnych, czy też hipotetycznych zagrożeń z cyberprzestrzeni nie pozwala nam twierdzić, że potrafilibyśmy uniknąć problemów z bezpieczeństwem. Nawet przy zastosowaniu znacznych nakładów i specjalnych środków prawnych. Nie powinniśmy jednak wobec kwestii bezpieczeństwa tworzyć ograniczeń jakościowych.

W kwestii bezpieczeństwa fizycznego, nie powiedzielibyśmy przecież, że służby porządku publicznego (Policja) mają zapewnić akceptowalny poziom bezpieczeństwa w przestrzeni publicznej. Chcemy się po prostu czuć w mieście bezpiecznie. Poza prawem publicznym i prywatnym, wdrażaniem technicznych standardów, kształtowaniem się wzorców kulturowych i zachowań społecznych w edukacji i rodzinie, składają się na to też działania państwa, w tym zadania prewencyjne policji oraz skuteczne ściganie naruszeń i przestępstw.

Podobnie powinno być z bezpieczeństwem cyberprzestrzeni. Skala zagrożeń stała się tak znaczna, że państwo musi podjąć odpowiedzialność za bezpieczeństwo również w tej sferze, tym bardziej że technologie informacyjne mają obecnie zastosowanie we wszystkich obszarach aktywności państwa, gospodarki i obywateli.

Państwo w granicach swych kompetencji ma zatem tworzyć warunki zapewniające poczucie bezpieczeństwa obywatelom i podmiotom gospodarczym. Z oczywistym zastrzeżeniem, że poczucie bezpieczeństwa jest czymś całkowicie subiektywnym, a granice kompetencji państwa określa konstytucja i ustawy.

Internet

Ref. cele strategii str.4

W proponowanym określeniu celu jest błąd logiczny. Jeżeli celem państwa ma być „zapewnienie zdolności do…niezakłóconego dostępu do korzystania w sieci internet" to w tym konkretnym punkcie nie trzeba już dodawać zastrzeżenia, że „w sytuacji gdy realizacja wymienionych aktywności zależna jest od cyberprzestrzeni". Ten fragment wymaga przeredagowania.

Podmiotowy zakres strategii

Ref. podrozdział – zakres strategii str.5

Podmiotowy zakres strategii to obywatele, przedsiębiorcy, pracownicy administracji publicznej, operatorzy usług kluczowych.

Zamiast zdania „ Strategia będzie oddziaływała…." lepiej brzmiałoby tu zdanie

„Strategia uwzględnia zróżnicowanie priorytetów różnych grup użytkowników technologii informacyjnych i usług…"

Informacja niejawna

ref. akapit 2 podrozdziału „zakres strategii" str. 5

Relacja Strategii wobec reżimu ochrony informacji niejawnej jest określona w sposób niewłaściwy. Ramy prawne dla ochrony informacji niejawnej tworzy ustawa, a nie „strategia", więc nie można ich bezpośrednio zestawiać. Z drugiej strony, nie należy separować kompetencji ABW i SKW w zakresie ochrony informacji niejawnej od koncepcji strategicznych państwa. Należałoby je raczej dopasować, nie naruszając autonomii służb specjalnych w sprawach bezpieczeństwa informacyjnego państwa.

Można to wyjaśnić w sposób następujący, zastępując komentowany akapit:

Strategia nie dotyczy systemu ochrony informacji niejawnych uregulowanego ustawą, procedurami i wymaganiami stosowanymi na jej podstawie pod nadzorem służb ochrony państwa. Strategia będzie jednak uzupełniać i wzmacniać ten system.

Wymiar strategiczny

Ref. Uwarunkowania wewnętrzne – wymiar strategiczny str. 9

Mówimy o wymiarze strategicznym, gdzie należy zacząć od planowania wyzwań i zadań, zanim zostaną podjęte działania. Konstytucja ma rangę nadrzędną wobec innych przepisów. Proponowałbym zatem zamienić pierwszy akapit zdaniem:

Art. 5 Konstytucji nakłada na państwo powinność zapewnienia bezpieczeństwa wszystkim obywatelom. Zadania związane z cyberbezpieczeństwem rozkładają się zatem na wiele organów władzy publicznej, zgodnie z ich konstytucyjnymi właściwościami i zadaniami określonymi w ustawach.

Ref. str.10 pkt 4 lit.b
Albo albo - aktywna obrona i działania ofensywne to zdaje się to samo. Aktywna obrona (termin z doktryny amerykańskiej) to wygodny eufemistyczny synonim działań ofensywnych.

Uwarunkowania międzynarodowe
Ref. rozdz. 3.2 str.12

Opis współpracy międzynarodowej pojawia się w dokumencie dwa razy. Raz w kontekście uwarunkowań (podrozdział 3.2.), drugi raz w kontekście zadań. Chyba niepotrzebnie, bo zawartość się powtarza, a w pierwszej wersji jest zbyt lakoniczna. Usunięcie pierwszego opisu wiąże się z usunięciem podtytułu 3.1. – uwarunkowania wewnętrzne.

Dyrektywa NIS

Ref. podrozdział 4.1.1. Rola ministra pkt 6)

Usunąć słowa „zwanej dalej „Dyrektywą" ponieważ dyrektywa NIS nie jest dalej w tekście omawiana (chyba że uwarunkowania wdrażania dyrektywy zostaną omówione)