Stanowisko Rady do Spraw Cyfryzacji w sprawie projektu strategii cyfryzacji – wersja projektu z dnia 4 października 2024 r. z dnia 14 października 2024 r. skierowane do Ministra Cyfryzacji.

W nawiązaniu do przedstawionego projektu strategii ds. cyfryzacji (wersja z dnia 4.10.24; dalej „projekt strategii"), w imieniu Rady ds. Cyfryzacji pragnę przedstawić Panu uwagi mające na tym etapie opiniowania tego dokumentu głównie charakter kierunkowy, zawierające sugestie oraz wskazówki strategiczne względem opiniowanego dokumentu, o zasadniczym znaczeniu z punktu widzenia istoty projektowanego dokumentu przez Ministerstwo Cyfryzacji.

W opinii Rady ds. Cyfryzacji, zaprezentowany projekt strategii ma bardzo dobrą strukturę, jednak w wielu miejscach jest niespójny, a jego lektura prowadzi do przekonania, iż jest to zbiór propozycji zgłaszanych przez różnych interesariuszy – widać to m.in. po tym, że różne fragmenty projektu strategii posiadają zróżnicowany poziom szczegółowości, niektóre obszary są opisywane bardzo szczegółowo, zawierają konkretne projekty, na które w naszej opinii nie powinno być miejsca w dokumencie o charakterze strategicznym, zaś niektóre są opisane pobieżnie lub zupełnie ogólnie (przykład rozdział poświęcony innym technologiom przełomowym), a w niektórych rozdziałach brak jest zaznaczenia kluczowej dla rozwoju kraju tematyki.

Ponadto, należy zwrócić uwagę, iż cały dokument jest zbyt obszerny jak na strategię o charakterze parasolowym, dlatego też w naszej opinii warto byłoby przeredagować projekt strategii, usunąć niektóre fragmenty, uspójnić opisy poszczególnych rozdziałów, zaś niektóre fragmenty mogłyby stanowić załączniki do opiniowanego dokumentu. Dokument strategiczny, o charakterze strategii parasolowej, powinien być zwięzły, zawierać zwarte sformułowania w zakresie celu głównego, priorytetów, celów strategicznych, celów operacyjnych i inicjatyw strategicznych służących realizacji celów. Nie powinien schodzić do poziomu projektów (np. tak jak to ma miejsce w przypadku projektu „Kronika"). Dokument ten powinien również zawierać informację o hierarchii strategii (np. strategia cyfryzacji jako strategia główna oraz strategie obszarowe – np. strategia cyberbezpieczeństwa, która jest w trakcie nowelizacji). Strategia główna powinna odsyłać do strategii obszarowych – w tej chwili w dokumencie tym brak jest informacji na ten temat i brak odwołań do strategii obszarowych.

Jednocześnie, pragnę poinformować Pana Premiera, iż w kwietniu br. członkowie Rady ds. Cyfryzacji przygotowali szereg materiałów inspiracyjnych dla Departamentu Projektów i Strategii, prowadzącego koordynację prac nad projektem strategii, z których – po zapoznaniu się z treścią projektu strategii wygląda na to, że żadne z tych sugestii i propozycji nie zostały uwzględnione. Oczywiście, materiały te były materiałami inspiracyjnymi, jednak wiele wskazanych w nich propozycji mogłoby być wykorzystane w

projekcie strategii, zwłaszcza pragnę zwrócić uwagę na materiał dotyczący tematyki cyberbezpieczeństwa, czy edukacji cyfrowej, gdzie wskazano wiele naprawdę ciekawych, ale i kompleksowych propozycji.

Poniżej przedstawiam uwagi do poszczególnych punktów projektu strategii. W przypadku zainteresowania Pana Premiera, informuję, iż członkinie i członkowie Rady ds. Cyfryzacji są gotowi na przedstawienie uwag szczegółowych, jednak będę wdzięczna za wyraźne wskazanie przez Pana Premiera takiej potrzeby i takiego oczekiwania względem Rady.

1. Wstęp

Z fragmentu zawartego we wstępie, cyt.: „Niniejsza strategia uwzględnia i poszerza cele zarysowane w ramach wspomnianego programu. Obejmuje ona obszary nieuwzględnione w unijnych celach, ma też bardziej odległy, sięgający 2035 r., horyzont czasowy." [….] „Biorąc pod uwagę zasady zarządzania strategicznego oraz tempo rozwoju technologicznego, planujemy regularną ewaluację i aktualizację dokumentu. Zastąpi on Program Zintegrowanej Informatyzacji Państwa i będzie stanowić podstawę strategiczną dla wydatkowania europejskich funduszy przeznaczonych na cyfryzację, a tym samym będzie wyznaczał kierunek negocjacji obejmujących nadchodzącą perspektywę finansową."

Nie jest jasne czym jest ta strategia? Autor pisze, że ta strategia „uwzględnia i poszerza cele zarysowane" w cyfrowej dekadzie i „obejmuje obszary nieuwzględnione w unijnych celach, ma też bardziej odległy, sięgający 2035 roku horyzont czasowy", ale nie jest jasne i nie wynika to z treści całej strategii, że te wszystkie cele wymienione w cyfrowej dekadzie zostały uwzględnione w projekcie strategii, nadto dalej mowa jest o tym, że projekt strategii „zastąpi Program Zintegrowanej Informatyzacji Państwa i będzie stanowić podstawę strategiczną dla wydatkowania europejskich funduszy przeznaczonych na cyfryzację…" – zatem pytanie czym jest ta strategia cyfryzacji z punktu widzenia rządu oraz administracji? Czy jest road-mapą dla programowania funduszy UE na cyfryzację? Czy w istocie jest dokumentem strategicznym, strategią parasolową (a więc ponadsektorową) i faktycznie nowoczesną strategią mówiącą o tym jaki jest cel główny tej strategii, jakie są jej priorytety, cele strategiczne, celów operacyjne oraz inicjatyw strategiczne, służące realizacji tych postawionych sobie (nam Polakom, Polsce) celów.

2. Diagnoza i analiza SWOT

Diagnoza powinna stanowić dokument odrębny, np. załącznik do strategii cyfryzacji, gdyż zajmuje zbyt wiele miejsca w projekcie strategii, powodując że dokument staje się zbyt obszerny jak na dokument o charakterze strategicznym, a nadto w części „Obszary horyzontalne" wskazuje się w każdym z poszczególnych punktów właśnie diagnozę sytuacji (tj. diagnoza – jak jest? Może warto nazwać ten punkt „Stan obecny", a niekoniecznie diagnoza?). Diagnozę, jeśli byłaby ona załącznikiem do strategii, można i warto byłoby

uzupełnić o badania krajowe, wskazujące np. jakie zagrożenia w kontekście rozwoju gospodarczego, transformacji cyfrowej i ogólnie cyfryzacji dostrzegają Polki i Polacy, badania realizowane przez krajowe instytucje oraz jednostki badawczo-rozwojowe, dotyczące np. kwestii technologii, innowacyjności (co ściśle łączy się zarówno z rozwojem technologicznym, a tym samym z cyfryzacją) – powinno to dotyczyć zarówno obywateli, jak i przedsiębiorców. Warto również zwrócić uwagę w diagnozie na strukturę gospodarczą i społeczną Polski (np. struktura przedsiębiorstw w Polsce – warto uwzględnić tutaj raporty realizowane przez Polską Agencję Rozwoju Przedsiębiorczości, lub opracowania na temat kluczowych inteligentnych specjalizacji Polski, co wskazuje na pożądane obszary koncentracji uwagi i środków sektora publicznego; diagnoza struktury społecznej – index DESI to jedno, ale także specyficzne dla naszego kraju kwestie powinny być uwzględnione, jak np. kwestia demografii).

Wiele ciekawych sugestii, które mogłyby być uwzględnione również w diagnozie, zostały przekazane przez Radę ds. Cyfryzacji w kwietniu tego roku do Departamentu Projektów i Strategii. Na przykład w materiale przygotowanym przez RDC dotyczącym zagadnienia cyberbezpieczeństwa były wskazane informacje na temat diagnozy właśnie w tym obszarze, zaś w projekcie strategii w rozdziale opisującym diagnozę kompletnie brak diagnozy cyberbezpieczeństwa w oparciu o raporty np. europejskiej agencji ENISA.

Należy również wskazać, iż w diagnozie powinny być uwzględnione informacje, które nawiązują do obszarów horyzontalnych, bo to odpowiada na pytanie po co my to robimy? Dlaczego są takie a nie inne obszary horyzontalne, dlaczego to jest ważne? W tej chwili tego brakuje, a diagnoza opiera się na unijnych raportach.

3. Wyzwania i trendy

Pierwszy akapit w tym rozdziale nawiązuje do diagnozy i niejako jest diagnozą sytuacji, więc niewiele wnosi do punktu „wyzwania i trendy". Ponadto jak w przypadku rozdziału Diagnoza, proponujemy, aby opis wyzwań i trendów również umieści w załączniku do strategii.

Ponadto warto zastanowić się nad dodaniem nawet minimalnego słownika pojęć – należy tu przede wszystkim wyjaśnić co mamy na myśli pisząc cyfryzacja i jaki jest związek tego pojęcia z pojęciem informatyzacja, którym posługujemy się m.in. w aktach prawnych, w szczególności mamy tu na myśli ustawę o informatyzacji działalności podmiotów publicznych, która ma stanowić podstawę prawną dla niniejszej strategii cyfryzacji. Dodatkowo, jedynie w tym rozdziale używa się pojęcia TIK – warto uspójnić treść projektowanej strategii również w obszarze pojęciowym.

Rozdział poświęcony jest zagadnieniom globalnym, ale bez wskazania żadnych relacji do sytuacji Polski (za wyjątkiem p. 6). Warto, nawet w skrócie, wskazać jaka jest sytuacja Polski. Warto także zachować lub wskazać na istotność niektórych trendów – jeśli

wymieniony jest „Wzrost znaczenia cyberbezpieczeństwa” to ma to fundamentalne znaczenie dla dzisiejszego życia i aktywności Polaków i polskich przedsiębiorstw. Z drugiej strony „Niezakończony proces tworzenia jednolitego unijnego rynku cyfrowego” ma jednak dużo mniejszy wpływ na działania. Dodatkowo ostatni akapit projektu strategii cyt.: „efektywna implementacja wniosków….” Itd. – ten punkt mógłby stanowić jedno z wyzwań „trapiących” administrację, a więc mityczna już „silosowość administracji” oraz kwestia kompetencji cyfrowych urzędników.

Rozdział ten należy dopracować, gdyż cała strategia cyfryzacji powinna odpowiadać na wskazane w tym rozdziale trendy i wyzwania i zawierać w sobie (w poszczególnych rozdziałach) odniesienia do poszczególnych wyzwań (tak jak zresztą i do wniosków z diagnozy). Ponadto, w rozdziale tym nie jest jasne co dla autora jest trendem, a co wyzwaniem (czyli swego rodzaju „kłopotem”, z którym coś należy zrobić, np. w ramach właśnie tej strategii cyfryzacji).

4. Analiza SWOT

W analizie SWOT jest pomieszanie słabych stron z wyzwaniami, szans z mocnymi stronami – należy zastanowić się jakie są przyczyny, jakie skutki. Analiza, która została przygotowana przez PIE, nie była konsultowana z interesariuszami i to należy uznać za słaby punkt, ponieważ szanse, zagrożenia, słabe strony i mocne strony określone w dokumencie nie uwzględniają perspektywy wszystkich uczestników cyfrowego ekosystemu, a jedynie własną analizę autorów. Uprzednia konsultacja tej analizy (jeszcze przed etapem konsultowania całego projektu strategii cyfryzacji) mogłaby potencjalnie stanowić wartość poznawczą dla Ministerstwa Cyfryzacji.

Analiza SWOT, podobnie jak rozdziały Diagnoza oraz Wyzwania i Trendy, mogłyby być załącznikami do strategii cyfryzacji, zaś sam dokument strategiczny z powodzeniem może zaczynać się od Wstępu – opisu idei i podejścia, wartości, a następnie Wizja i cele strategii.

Ponadto, proponujemy ewentualne rozważenie uzupełnienia analizy SWOT o następujące elementy:

Cyfrowe państwo – zagrożenia: silosowość, brak koordynacji, brak wspólnych standardów; szanse: partnerstwo z biznesem i korzystanie z najlepszych rozwiązań rynkowych, rozwój lokalnego rynku ICT, zatrzymanie talentów.

Kompetencje – słabe strony: niski poziom wiedzy nauczycieli/wykładowców IT, brak nauczycieli IT z odpowiednim wykształceniem i wiedzą; szanse: zatrzymanie talentów, inwestycje w obszarze high value /R&D; zagrożenia: brain-drain, brak inwestycji w R&D.

Cyberbezpieczeństwo – szanse: jeden ośrodek koordynujący cyberbezpieczeństwo – wyłoniony z pośród najlepszych kompetencyjnie i organizacyjnie (nie powinniśmy tworzyć

kolejnych instytucji, biorąc pod uwagę ograniczone zasoby kompetencyjne oraz budżet na ich utrzymanie); zagrożenia: post quantum cryprtograpy.

5. Obszary horyzontalne

- ### Koordynacja cyfrowej transformacji kraju

W kwestii koordynacji należy wskazać (jako jeden z przykładów), iż w projekcie strategii cyfryzacji nie ujęto odniesienia do ważnych zagadnień zawartych w Polityce Cyfrowej Transformacji Edukacji. Polityka ta została przyjęta w dniu 12 kwietnia br. przez Radę Ministrów i stanowi politykę publiczną, określającą podstawowe uwarunkowania, cele i kierunki rozwoju kraju w wymiarze społecznym, gospodarczym i przestrzennym w dziedzinie edukacji. Jest ona dokumentem komplementarnym wobec projektowanej strategii cyfryzacji, gdyż kompleksowo traktuje cyfryzację edukacji w latach 2024-35. W Polityce tej m.in. jest mowa o konieczności podjęcia działań dotyczących efektywnego przygotowania nauczycieli, w szczególności współpracy MEN z MNiSW w zakresie zmiany systemu kształcenia i doskonalenia w zakresie kompetencji cyfrowych, a także rozprowadzenia internetu po budynkach szkolnych i zapewnienia finansowania ciągłego utrzymania wyposażenia szkół w sprzęt komputerowy na wysokim poziomie, które to działania są domeną Ministerstwa Cyfryzacji. W związku z tym w przedmiocie koordynacji należy wskazać, że wszystkie polityki oraz strategie „sektorowe", które dotyczą kwestii cyfryzacji, uzupełniają się, a realizacja celów cyfrowych jest monitorowania również w ramach realizacji projektowanej strategii cyfryzacji, w której powinny być wyraźnie oznaczone odniesienia do tych polityk / strategii (jak właśnie m.in. Polityka Cyfrowej Transformacji Edukacji, czy też nowa Strategia Cyberbezpieczństwa).

Dodatkowo w kwestii koordynacji cyfrowej transformacji kraju należałoby uwzględnić:

- wątek administracji zdecentralizowanej – rola samorządów w tym procesie jest olbrzymia,
- wątek regulacji dotyczących obszarów cyfrowych, w tym koordynacji regulacji implementujących regulacje unijne.

- ### Komunikacja elektroniczna

Fragment „Kontynuacja wsparcia finansowego dla przedsiębiorców telekomunikacyjnych dla rozwoju infrastruktury…" – wydaje się, że wobec bieżących doświadczeń z wydatkowaniem tego typu środków oraz problemami z tym związanymi należałoby zaplanować nowe sposoby pobudzania inwestycji w obszarze białych plam, a także rozważyć wsparcie innych potrzeb w zakresie rozwoju infrastruktury telekomunikacyjnej, np. w celu zapewnienia bezpieczeństwa (w tym cyberbezpieczeństwa) infrastruktury szerokopasmowej, czy wzmocnienia jakości usług świadczonych w sieciach mobilnych najnowszej generacji poprzez zapewnienie światłowodowego dosyłu.

Fragment „Likwidowanie barier prawnych i systemowych dla rozwoju sieci telekomunikacyjnych poprzez nowelizację tzw. Megaustawy i integrację prawa krajowego z unijnym rozporządzeniem Gigabit Infrastructure Act" – sektor wielokrotnie wskazywał na szereg barier inwestycyjnych i rozwojowych, które do dziś nie zostały rozwiązane. Potrzebne są działania o charakterze deregulacyjnym idące znacznie dalej niż zintegrowanie Megaustawy z Gigiabit Infrastructure Act, obejmujące nie tylko obszar inwestycyjny, ale również inne aspekty prowadzonej działalności. Jedną z konkretnych propozycji, jaka została skierowana do Ministerstwa Cyfryzacji w ostatnim czasie, jest wspólne z branżą przygotowanie "Porozumienia sektorowego na rzecz przyspieszenia cyfryzacji Polski", którego celem byłoby określenie inicjatyw i zadań zmierzających właśnie do zlikwidowania barier prawnych i systemowych i odblokowania potencjału rozwojowego sektora telekomunikacji oraz w rezultacie wsparcia ambitnych celów państwowych postawionych w projektowanej strategii. Taka inicjatywa mogłaby być elementem działań planowanych w ramach realizacji Celu 1 określonego w przedmiotowym rozdziale.

Fragment „Wspieranie rozwoju samorządowych i prywatnych sieci 5G." – jak najbardziej obszar ten zasługuje na pełne wsparcie, jednakże określony sposób działania jest tak enigmatycznie opisany, że zupełnie nie wiadomo, jakie działania się pod tym kryją. Strategia powinna być tak określona, żeby było wiadome przynajmniej jakiego rodzaju wsparcie to będzie, np. finansowe, edukacyjne, legislacyjne itp.

Fragment „Wprowadzenie programu tzw. bonów łączności – zestawu zachęt ekonomicznych dla użytkowników końcowych do korzystania z usług." – oczywiście odpowiednio zaprojektowany program może się przyczynić do zwiększenia popytu tam, gdzie on obecnie nie występuje i gdzie potencjalną barierą jest bariera finansowa. Jednakże, biorąc pod uwagę planowany rozmiar interwencji to nie będzie to duży program, który zasadniczo zmieni obraz korzystania z usług. Brakuje rozwiązania systemowego.

W zakresie łączności większość celów to są cele na maksymalnie najbliższe dwa lata, są mało ambitne, natomiast niektóre stanowią działania polegające na „egzekwowaniu od rynku", co będzie źle odebrane przez branżę ICT.

- Kompetencje przyszłości

**W kwietniu br. RDC przygotowała materiał inspiracyjny dla Departamentu Projektów i Strategii pod kątem planowanych prac nad projektem strategii cyfryzacji. Materiał ten został ponownie przekazany Panu Premierowi w czerwcu jako stanowisko Rady ds. Cyfryzacji/zespołu roboczego ds. edukacji cyfrowej i kompetencji cyfrowych – Postulaty w zakresie rozwoju kompetencji cyfrowych.*

Ponadto, brakuje jako celu/priorytetu stałego podnoszenia kompetencji cyfrowych nauczycieli/wykładowców (nie tylko ICT).

- Cyberbezpieczeństwo

**W kwietniu 2024 r. zespół roboczy ds. Cyberbezpieczeństwa Rady ds. Cyfryzacji przygotował i przekazał Departamentowi Projektów i Strategii materiał inspiracyjny do strategii cyfryzacji w zakresie cyberbezpieczeństwa.*

W odniesieniu do projektu strategii w rozdziale dotyczącym cyberbezpieczeństwa o ile zrozumiały jest cel zapewnienia bezpieczeństwa obywatelom, to równie ważny byłby cel zapewnienia bezpieczeństwa przedsiębiorcom.

Należy wprost napisać, iż cyfryzacja się nie uda bez dojrzałego cyberbezpieczeństwa.

Cyberbezpieczeństwo jest obszarem horyzontalnym, a więc oprócz głównego rozdziału o cybeerbezpieczeństwie, w innych rozdziałach jest wzmiankowane cyberbezpieczeństwo, ale nie zawsze konsekwentnie, np. cele dot. obszaru zielonej transformacji cyfrowej, cyfrowego zdrowia czy sztucznej inteligencji nie zawierają odniesień do cyberbezpieczeństwa lub nie są wyraziście potraktowane (pozytywny przykład: przestrzeń kosmiczna). Należy zatem przyjąć jednolite podejście do uwzględniania cyberbezpieczeństwa w całej projektowanej strategii.

<u>Współpraca sfery cywilnej i wojskowej w cyberbezpieczeństwie:</u>

a. Obszar cyberbezpieczeństwa można podzielić na dwie sfery: cywilną oraz wojskową/militarną. W niniejszym opracowaniu skupiono się na sferze cywilnej cyberbezpieczeństwa. Jednak należy zauważyć, że w obecnych czasach i dającej się przewidzieć przyszłości sfera cywilna musi współpracować ze sferą militarną w dziedzinie cyberbezpieczeństwa, zarówno w kontekście krajowym, jak i międzynarodowym.
b. Jeśli chodzi o współpracę ze sferą militarna w cyberbezpieczeństwie, to jest ona uwzględniona (w niewielkim zakresie w porównaniu z innymi zagadnieniami – np. e-sportem) tylko w aspekcie międzynarodowym, ale nie w krajowym. Należy nadać wyższy priorytet współpracy cywilno-wojskowej w strategii, w szczególności w aspekcie krajowym.
c. We wstępie autorzy piszą o wojnie przeciwko UA ale w samej strategii nic lub prawie nic nie ma o tym aspekcie – np. brak jest odniesień i celów związanych z działaniami wobec dziejącej się już obecnie wojny hybrydowej.

<u>Aspekt międzynarodowy</u>

a. W projekcie strategii w obszarze cyberbezpieczeństwa dominuje podejście prawie wyłącznie krajowe – nie ma zbyt wiele na temat nadchodzących unijnych regulacjach: CRA, CSoA, CER i inne, a jest to poważne wyzwanie.
b. Jeśli jest mowa o suwerenności, to wyłącznie w aspekcie krajowym (a nie np. w aspekcie UE, czy krajów tzw. like-minded).
c. Cel dotyczący pozycji międzynarodowej w cyber jest bardzo skromny.
d. Współpraca cyber w sieciach UE/międzynarodowych nie wygląda, aby była priorytetem.

Czasem cele mylone są ze środkami realizacji:

a. Przykładowo, samo powołanie agencji cyberbezpieczeństwa jest wskazywane jako cel, a nie jest to cel tylko środek realizacji jakiegoś celu;
b. Nie jest też jasne, czy taka inicjatywa dotyczy wyłącznie sfery cywilnej, czy wraz z militarną?
c. Należałoby zacząć od zdefiniowania wszystkich zadań podmiotów uKSC (oraz wynikających z innych przepisów, takich jak DORA, e-IDAS, CER itd.) i do tego dopasować optymalną architekturę krajowego systemu cyberbezpieczeństwa. Potrzebna dogłębna analiza funkcjonowania krajowego systemu, w tym pod kątem przyszłych wyzwań, w tym związanych z nowymi regulacjami. Dobrze działające mechanizmy zachować i rozwinąć, brakujące stworzyć, gorzej działające ulepszyć.

Brak uwzględnienia w strategii tematyki zwalczania i przeciwdziałania cyberprzestępczości – bez ustanowienia celów dotyczących zwalczania cyberprzestępczości w obszarze cyberbezpieczeństwa strategia jest niekompletna.

Należy popracować nad wskaźnikami efektywności: przykładowo w obszarze cyberbezpieczeństwa są trzy:

- powołanie agencji, gdy samo powołanie nie może być traktowane jako wskaźnik efektywności,
- chmura niejawna – też nie jest wskaźnikiem (może nią być np. liczba podmiotów korzystająca z chmury),
- system certyfikacji cyber – prawidłowa inicjatywa strategiczna, ale samo ustanowienie nie jest dobrze określonym wskaźnikiem efektywności.

Przykładowe cele i wskaźniki w cyberbezpieczeństwie – do wykorzystania:

Systemowy wzrost dojrzałości cyberbezpieczeństwa – propozycja celów i inicjatyw do osiągnięcia:

i. Polska w pierwszej trójce krajów UE i w pierwszej piątce krajów like-minded we wszystkich uznanych międzynarodowych rankingach/indeksach cyberbezpieczeństwa i cyber defense;

ii. Krajowa, cykliczna ocena funkcjonowania dojrzałości w oparciu o Cybersecurity Index ENISy i regularnie przeprowadzane ćwiczenia na poziomie krajowym i sektorowym;

iii. Opracowanie rozwiązania systemowego wspierającego wzrost świadomości i stosowania zasad cyberhigieny z wykorzystaniem kampanii, szkoleń i poradników; system powinien być skalowalny – wraz z cyklicznym pomiarem na bazie ustanowionej metodyki;

6. Rozdział Państwo (eUsługi publiczne, Cyfryzacja procesów administracyjnych i postępowań sądowych, Systemy i rejestry, Cyfrowa tożsamość, Chmura obliczeniowa, Otwarte dane i wymiana danych)

- Zagadnienia związane z interoperacyjnością zajmują nieproporcjonalnie dużo miejsca w treści projektu strategii. Interoperacyjność pojawia się wielokrotnie jako panaceum na rozwój e-usług państwa, jako ugruntowana metoda strategicznego zarządzania informatyzacją państwa, cel przy informatyzacji rejestrów, która ma zredukować obciążenia administracyjne (co samo w sobie jest dyskusyjną tezą). Interoperacyjność ma nawet wspomagać technologie przełomowe i technologie kosmiczne. Jednocześnie, jeśli interoperacyjność ma aż tak fundamentalny charakter, to dlaczego nie widać jej w analizach SWOT? Dlaczego nie jest wskazany, jako np. słaba strona, brak kompetencji w zakresie interoperacyjności. Ponadto, dlaczego interoperacyjność występuje jako zagadnienie wyłącznie w dyskusji poświęconej systemom administracji publicznej? Czyżby przedsiębiorstwa, w tym także te największe, nie przykładały aż takiej wagi do zagadnienia? W tym kontekście proponujemy zachowanie odpowiedniej proporcji obecności tematu interoperacyjności w projekcie strategii i ograniczenie dyskusji o tym zagadnieniu do jej operacyjnego charakteru, gdyż interoperacyjność – w porównaniu z zagadnieniami cyberbezpieczeństwa, transformacji cyfrowej gospodarki, kompetencji – nie jest elementem strategicznie zmieniającym Polskę.
- eDoręczenia – brak nawiązania do rozwiązań obszarowych/dziedzinowych, które są sprawne i którymi obywatele już posługują się – należy stworzyć pomost pomiędzy tym co już dobrze funkcjonuje, a co jest planowane.
- W warunkach konwergencji technologicznej oraz postępującego procesu ujednolicania systemu sieci dystrybucji powstała potrzeba stworzenia jednego, nowoczesnego, kompletnego miejsca w Internecie, które byłoby rzeczywiście pierwszym miejscem kontaktu użytkownika (społeczeństwa) z informacją posiadaną przez sektor publiczny. Na taką potrzebę wskazywała strategia Państwa, zgodnie z którą celem cyfryzacji

zbiorów instytucji kultury w Polsce było nie tylko zabezpieczenie ich w postaci wysokojakościowych kopii cyfrowych, ale również umożliwienie użytkownikom jak najszerszego dostępu do zasobów całości polskiego dziedzictwa narodowego poprzez tworzenie dostępnych poprzez Internet zasobów archiwów, bibliotek, muzeów oraz repozytoriów cyfrowych. Zadaniem państwa jest budowa systemu publicznego dostępu do wiarygodnego i kompleksowego indeksu zasobów cyfrowych w Polsce (zasoby instytucji publicznych oraz podmiotów prywatnych), traktując ten projekt jako uzupełniający do istniejących już platform udostępniania zasobu cyfrowego a nie tworzenie zcentralizowanego systemu udostępniania danych (instytucje kultury nie mają obowiązku udostępniania zasobów w ramach re use, a tym bardziej podmioty prywatne). Natomiast nie ma rozwiązań pozwalających na indeksację zasobów. Należy podkreślić znaczenie własności prywatnej w sieci i poszanowanie praw cyfrowych obywateli i przedsiębiorców. W koncepcji projektu istotne jest wyraźne podkreślenie, że w aspekcie definicyjnym rozróżnić należy instytucje „dostępu dodanych ” oraz „ponownego wykorzystywania”. Szczególnie istotne jest rozróżnienie pomiędzy realizacją prawa dostępu do informacji sektora publicznego (access to public sector information) a dalszą eksploatacją informacji pozyskanych w ten sposób (re-use of public sector information). Ponowne wykorzystanie oparte zostało na regułach o wymiarze gospodarczym i społecznym. W kontekście udostępniania zasobu danych cyfrowych powinna mieć zastosowanie zasada access to public sector information, z kolei w stosunku do samej treści cyfrowej powinna mieć zastosowanie reguła re-use of public sector information. Zasadę dostępu do danych powinno się realizować w ramach kanałów wymiany metadanych i materiałów, których kontynuacja powinna następować w ramach bieżącej współpracy międzysektorowej. W tym celu należy wykorzystywać istniejące już repozytoria cyfrowe partnerów, a nie opierać się na jednym, nieefektywnym rozwiązaniu.

- Udostępnianie informacji

  Głównym celem wymiany informacji jest bardziej potwierdzenie i wyliczenie sytuacji niż faktyczna analiza i dzielenie się nimi. Niektórzy eksperci przyznali również, że dla mniejszych organizacji i podmiotów o niższym cyberbezpieczeństwie złożoność przetwarzania wszystkich informacji udostępnianych za pośrednictwem ISAC może być czasami trudna. Dlatego analiza oraz dzielenie się informacjami jest jednym z głównych wyzwań w budowaniu ekosystemu ISAC w Europie. W większości krajów UE wymiana informacji między członkami ISAC odbywa się w sposób sformalizowany na podstawie umowy lub umowy o członkostwo. Umowy te obejmują sposoby wymiany i rodzaje informacji, które należy wymienić. Członkowie ISAC wymieniają się informacjami o zagrożeniach, incydentach, podatnościach, środkach łagodzących, a także o najlepszych praktykach i narzędziach. Najpopularniejszym narzędziem wymiany informacji jest

specjalna sieć portal / platforma (według określonego szablonu) i zaszyfrowane wiadomości e-mail. Najważniejszą i skuteczną metodą są bezpośrednie spotkania. Wśród ISAC powszechną praktyką jest tworzenie tzw. „kręgów zaufania". Niektóre informacje (np. szczegóły techniczne dotyczące incydentów) mogą być jednak szeroko udostępniane wszystkim członkom. Dodatkowo tworzy się też wewnętrzny krąg, w którym udostępnione informacje są bardziej szczegółowe. Zwykle osoby zaangażowane w taki wewnętrzny krąg to zespół zarządzający (lub komitet sterujący) z dobrą znajomością organizacji i wysokim (wyższym) poziomem wzajemnego zaufania. W większości ISAC informacje są weryfikowane, zanim zostaną przekazane wszystkim członkom. W ISAC, które nie mają takiego mechanizmu, zwykle informacje są dostarczane za pośrednictwem listy mailingowej, aby wszyscy członkowie mogli zobaczyć, kto je posiada i kto je dostarczył.

Projekt strategii nie zawiera elementów związanych z budowaniem ISAC, które są coraz bardziej popularne i wykorzystywane jako skuteczne narzędzie w zwalczaniu cyberataków w obszarze miedzy sektorowym.

7. Rozdział Ludzie (Cyfrowe prawa, Przeciwdziałanie dezinformacji, Cyfrowe zdrowie, Branże kreatywne, Nauka)

- ISAC i Dezinformacja

Kluczowym elementem działań organizatorskich w obszarze cyberbezpieczeństwa jest budowanie sieci powiązań i wymiany danych, która stanowiłaby międzysektorowe wsparcie w walce z cyberzagrożeniami, w tym z dezinformacją. Takie działania wymagają jednak polityki wzajemnego zaufania i lojalności, co w kulturze pracy i organizacji w środowisku UE stanowi istotny problem. Podstawą takiej koordynacji działań jest wymiana informacji i szybkość działania. Organizacje działają lepiej w sytuacji identyfikacji i definiowania zagrożeń, kiedy są lepiej poinformowane o napastnikach i metodach ataku. Jednym z instrumentów wykorzystywanych w zapewnieniu cyberbezpieczeństwa jest Information Sharing and Analysis Center (ISAC), czyli Centrum Wymiany i Analizy Informacji.

Walka z dezinformacją stanowi ważny element zapewnienia cyberbezpieczeństwa. Nie tylko sieci stanowią przedmiot ataków, ich zawartość również jest narażona na manipulację i próby wpływu. Centrum Wymiany Informacji i Analiz to w założeniu zaufana jednostka sektorowa, która może zapewnić bezpieczną zdolność operacyjną oraz określa wymagania dotyczące koordynacji, udostępniania informacji i analizy w przypadku incydentów. Z jednej strony ISAC może służyć jako zasób branżowy, dzięki któremu można gromadzić kluczowe informacje o zdarzeniach i problemach związanych z cyberbezpieczeństwem w danej branży oraz identyfikować, komunikować się i analizować potencjalne skutki takich problemów dla danego sektora. Z drugiej strony

powstanie ISAC niekoniecznie musi wiązać się z realizacją działań jedynie w określonej branży. Koordynacja może dotyczyć wspólnych przedsięwzięć czy wspólnych celów związanych potrzebą zapewnienia ochrony systemowej. Wspólnym mianownikiem dla działań partnerów w obszarze cyberbezpieczeństwa jest często charakter strategiczny ich usług, stanowiących ważny element na mapie infrastruktury krytycznej państwa. Rozwój ekosystemu ISAC w Europie zależy od uwarunkowań kulturowych różnych członków i ogólnego poziomu zaufania między podmiotami publicznymi i prywatnymi – jeśli mamy do czynienia z partnerstwem publiczno-prywatnym (PPP). Z tego powodu w krajach, w których zaufanie nie jest wystarczające, warto najpierw rozpocząć opracowywanie struktur PPP, a następnie przekształcić je w ISAC. Dzieje się tak, ponieważ wymiana informacji o incydentach, zagrożeniach i podatnościach jest bardzo wymagająca, a poziom zaufania między podmiotami jest tu niezwykle istotny. Ponieważ kluczowe usługi wymagają budowania tego typu organizacji w celu wzmocnienia cyberbezpieczeństwa, takie podmioty jak ISAC, skupiające wyłącznie partnerów z sektora publicznego, także są potrzebne, a nawet wymagane.

Interesującym rozwiązaniem w warunkach polskich mogłoby być utworzenie specjalnego ISAC (Information Sharing and Analysis Center), którego głównym obszarem wymiany byłyby doświadczenia i informacje związane z działaniami dezinformacyjnym. Taka konstrukcja mogłaby przyczynić się do stworzenia warunków zaufania międzysektorowego, ale także koordynacji aktywności dezinformacyjnych różnych inicjatyw i organizacji działających w sektorze publicznym. ISAC jest formą partnerstwa, którego funkcjonowanie w krajowym systemie cyberbezpieczeństwa ma uregulować ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z zawartymi tam propozycjami do zadań ISAC ma należeć w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów. Na poziomie krajowym oczekuje się, że ISAC tworzone jako inicjatywy dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Sformułowanie Zaufane Środowisko Cyfrowe (ang. Trusted Digital Environment) nawiązuje do wymaganego wysokiego poziomu bezpieczeństwa obszaru, jakim jest środowisko cyfrowe odnoszące się do działań dezinformacyjnych. Wykorzystywanie wyłącznie bezpiecznego środowiska cyfrowego i wymiany danych stanowi podstawę do budowy zaufania pomiędzy partnerami biznesowymi, biznesem i klientami, a także państwem i obywatelami w walce dezinformacyjnej. Bez wzajemnego zaufania do środowisk cyfrowych utrzymywanych przez poszczególnych interesariuszy, nie jest możliwa transformacja cyfrowa, a tym samym dalsza dynamiczna walka z dezinformacją.

ISAC Dezinfo ma na celu stworzenie warunków do wymiany doświadczeń związanych z bezpieczeństwem szerokiego spektrum rozwiązań obejmujących cyfrowe zasoby

informacyjne i wyciągania wniosków w zakresie ustanowienia optymalnych przyszłych kierunków transformacji cyfrowej uwzględniającej kwestie cyberbezpieczeństwa w obszarze dezinformacji. Udział partnerów, którzy posiadają cyfrowe zasoby informacyjne (dane) stwarza możliwość prowadzenia wspólnej misji społecznej.

- Część z e- sportem koniecznie do konsultacji Ministerstwa Zdrowia, patrząc na wyniki zdrowia, czy kondycji sportowej młodzieży.
- W całym rozdziale kompletnie brak odniesienia m.in. do następujących elementów:

a. rozwijania miękkich kompetencji przyszłości, jako bazy dla rozwijania "technicznych" kompetencji cyfrowych;

b. uwzględnienia postępującego kryzysu zdrowia psychicznego młodzieży, który jest ważnym kontekstem dla zmian w edukacji;

c. uwzględnienia braków w edukacji samych nauczycieli i potrzeby zmiany metod dydaktycznych (np. praca projektowa; działania zorientowane na kształtowanie empatii i krytycznego myślenia), jako warunków powodzenia zmian w edukacji;

d. potrzeby dokonania przeglądu e-usług, serwisów internetowych i elementów Wspólnej Infrastruktury Informatycznej Państwa pod kątem bezpieczeństwa danych, ochrony prywatności obywateli oraz zagrożeń wynikających z zależności od komercyjnych dostawców;

e. potrzeby wprowadzenia przemyślanego, spójnego dla wszystkich systemów modelu zarządzania danymi (w szczególności ram prawnych i technologicznych pozwalających na łączenie i analizowanie danych pochodzących z różnych źródeł i systemów);

f. wprowadzenia śladowalności i rozliczalności zapytań o dane w ramach administracji, aby ograniczyć i ścigać przypadki nieautoryzowanego dostępu oraz konstruowania e-usług i serwisów dla obywateli w taki sposób, by obywatel mógł sprawdzić historię zapytań o jego dane;

g. rozwiązania (sygnalizowanego w diagnozie) problemu niedostatecznej dostępności danych i narzędzi do analizy społecznych zachowań na potrzeby tworzenia polityk publicznych (np. poprzez pozyskiwanie danych z sektora prywatnego);

h. dostrzeżenie, na poziomie diagnozy i stawianych celów, zagrożenia jakim jest nieprzemyślane (tj. bez refleksji nad tym, jaki problem próbujemy rozwiązać i czy projektowane rozwiązanie jest niezbędne i proporcjonalne) rozwiązań technologicznych przez państwo; konkretną procedurą, która może rozwiązać ten problem, są obowiązkowe i publikowane oceny wpływu projektowanego systemu na prawa człowieka (Fundamental Rights Impact Assessment);

i. poważnego potraktowania wyzwań związanych z suwerennością cyfrową (na poziomie dużych celów);

j. poważnego potraktowania zagrożeń dla praw cyfrowych związanych z modelem biznesowym dominujących platform internetowych (w szczególności śledzeniem i profilowaniem użytkowników na potrzeby reklamy oraz projektowaniem algorytmów rekomendujących treści tak, by za wszelką cenę utrzymać zaangażowanie użytkownika).

- Ponadto, w projekcie strategii podkreśla się znaczenie zawodów w obszarze IT. Cyfryzacja to nie tylko informatyzacja. W środowisku cyfrowym muszą pojawiać się nowe zawody i nowe funkcje, i tym samym nowe kompetencje z uwzględnieniem wyrównywania szans dla kobiet, które mogą uzupełniać luki w obszarach coraz bardziej zautomatyzowanych. Nauki ścisłe i informatyka nie wypełniają pełnego zapotrzebowania na zmianę w myśleniu o cyfrowym rozwoju państwa.

8. Rozdział biznes i technologie (Cyfrowa transformacja przedsiębiorstw, Sztuczna inteligencja, Inne technologie przełomowe, Technologie kosmiczne, Finansowanie i wsparcie innowacji, Open source, Cyfrowa i zielona transformacja, Rolnictwo)

- W projekcie strategii należy podkreślić znaczenie współpracy w oparciu o mechanizm partnerstwa publiczno-prywatnego. Jest to istotne zwłaszcza w dobie kryzysu gospodarczego, wobec oczywistej konieczności cięć wydatków budżetowych. Współpraca sektora publicznego i sektora prywatnego w takich okolicznościach wydaje się niezbędna, jest bowiem dyktowana względami interesu publicznego. W związku rozwojem nowych technologii w procesie realizacji różnych zadań publicznych powstaje potrzeba coraz nowszych inwestycji infrastrukturalnych, zwłaszcza w dziedzinie komunikacji elektronicznej. Jedynie nowatorskie podejście do inwestycji może zaspokoić narastające potrzeby w tworzeniu nowoczesnej kultury cyfrowej.
- Partnerstwo publiczno-prywatne, poza tym, że jest elastyczną i bezpieczną formą powierzania wykonywania zadań publicznych podmiotom prywatnym, stanowi także sposób na zaangażowanie kapitału prywatnego w realizacje istotnych celów publicznych. Forma ta jest nowoczesnym instrumentem władz publicznych służącym wypełnianiu jej obowiązków wobec społeczeństwa. Zwłaszcza w tak szybko rozwijającej się dziedzinie, jaką jest kultura cyfrowa, stanowi atrakcyjny sposób na realizację wytyczonych celów. Może przyczynić się do obniżenia kosztów publicznych i osiągnięcia zamierzonego celu za pomocą nowoczesnych środków (także nowatorskich sposobów zarządzania, działań marketingowych i technik public relations). Zaś jeśli planowana działalność jest niedochodowa, dzięki wynagrodzeniu ze środków publicznych PPP może być atrakcyjne dla podmiotu prywatnego, a jednocześnie stanowić efektywne

rozwiązanie dla realizacji celów interesu publicznego, poprzez wykorzystanie do realizacji zadań publicznych infrastruktury, wiedzy fachowej i zasobów ludzkich, którymi dysponują podmioty prywatne.

- Bardzo zdawkowo została potraktowana w projekcie strategii tematyka dotycząca technologii przełomowych, ze szczególnym naciskiem na te kwantowe. Technologie kwantowe stanowią ważny element obecnej działalności MC (inwestycje w zakup hardware, zaangażowanie merytoryczne, współpraca z MNiSW i MRiT, popularyzacja wiedzy o technologiach kwantowych wśród tysięcy studentek i profesjonalistek w ramach Perspektywy Women in Tech Summit oraz realizowana tam ministerialna "Ścieżka kwantowa - Meet quantum)". W projekcie strategii powinna być mocno zaznaczona konieczność podjęcia działań, które przygotują Polskę na wyzwanie kwantowe i zapowiedzieć powstanie osobnej strategii (road mapy) w tym obszarze, co było komunikowane przez członków RDC zarówno kierownictwu Ministerstwa Cyfryzacji, jak i bezpośrednio Departamentowi nadzorującemu ten obszar.

9. Wskaźniki realizacji

- Zaproponowane wskaźniki realizacji w całym projekcie strategii to stricte wskaźniki ilościowe, brak jest natomiast wskaźników jakościowych (brak informacji na temat podniesienia jakości, albo wykorzystania proponowanych narzędzi, np. usługi ezd będą, ale czy będą umiejętności korzystania z nich); Wskaźniki wskazują, że strategia nie jest całościowo przemyślana, tylko jest zbiorem wkładów – to bardzo widać w całym dokumencie (np. powołanie danej instytucji to jest wskaźnik, a nie cel).

Jednocześnie, sugerujemy już na tym etapie przemyślenie kwestii sposobu promowania strategii oraz szerokiego informowania społeczeństwa o niej, jej celach, założeniach, priorytetach oraz spodziewanych efektach realizacji. W tym celu już w tym momencie Ministerstwo Cyfryzacji mogłoby opracować zarys planu komunikacji, z uwzględnieniem zaangażowania środowisk społeczno-gospodarczych.

W imieniu Rady ds. Cyfryzacji, będę zobowiązana Panie Wicepremierze za odniesienie się do prezentowanego stanowiska oraz propozycji Rady, jak również poinformowanie Rady o tym, jakie są dalsze planowane działania Ministerstwa w przedmiotowym zakresie.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji