Uwagi Polskiej Izby Informatyki i Telekomunikacji do projektu Strategii Cyfryzacji Polski do 2035 r.

Strona	Treść	Uwagi
ROZDZIAŁ: WSTĘP		
3	*Niniejsza strategia stanowi ponadsektorowy dokument strategiczny w dziedzinie informatyzacji państwa, określający nadrzędny cel, jakim jest poprawa jakości życia obywateli poprzez cyfryzację do 2035 r. Jego realizacja możliwa jest tylko dzięki interwencji w szeregu obszarów, wykraczających poza tradycyjnie definiowany dział administracji – informatyzacja[1].* *Zaplanowane do realizacji cele obejmują szerokie spektrum zagadnień, począwszy od kwestii horyzontalnych, poprzez płaszczyznę państwa i jego obywateli, na gospodarce i rozwoju technologii kończąc. Takie podejście pozwoliło na stworzenie nowoczesnej, przekrojowej i odpowiadającej na aktualne wyzwania wizji rozwoju cyfrowego, bazującej na aktualnych trendach europejskich i globalnych, wynikającej z diagnozy aktualnego stanu informatyzacji państwa oraz odpowiadającej na formułowane oczekiwania społeczne.* *[1] Ustawa o działach administracji rządowej z dnia 11 września 2024 r. (Dz.U. z 2024 r. poz. 1370).*	W założeniach strategia nie dotyczy tylko działu informatyzacja administracji – co będzie miało znaczenie w kolejnych formułowanych opiniach dotyczących strategii. **Wnosimy, aby także inne działy administracji (gospodarki, nauki, edukacji, itp.) w sposób bardziej bezpośredni uczestniczyły w przygotowaniu tego dokumentu oraz realizacji podanych w nim celów?** Innymi słowy, plany w zakresie cyfryzacji w innych resortach powinny być włączone do Strategii.
6	Wizja	Wizja opiera się na założeniu, że dostawcą elementów dotyczących spełnienia wizji jest administracja publiczna, wizja nie wskazuje na tym etapie współpracy wszystkich zaangażowanych stron: administracji publicznej na szczeblu rządowym i samorządowym, trzeciego sektora, instytucji biznesowych oraz instytucji naukowych. Wizja wskazuje na stymulowanie adopcji

Strona	Treść	Uwagi
		rozwiązań a nie na wypracowywaniu usług wraz z uczestnikami rynku. Wizja nie wskazuje, że rynek cyfrowy to w znaczącym stopniu usługi realizowane przez ten rynek, gdzie dziś w dużym stopniu korzystamy z rozwiązań kreowanych poza granicą polski, przez wielkich dostawców technologicznych, którzy współpracują z własnymi rządami. **Przede wszystkim, w zakresie wizji postulujemy – na podstawie analizy potencjałów krajowych, w tym dotychczasowej realizacji Krajowych Inteligentnych Specjalizacji oraz otoczenia konkurencyjnego Polski – wybranie obszarów gospodarki cyfrowej, w których Polska miała ambicje budowy silnej pozycji.** Obszary te powinny mieć potencjał do istotnego konkurowania na rynkach globalnych. Niezależnie od wybranych konkretnie obszarów, w naszej ocenie wartością samą w sobie, będzie skupienie się na realizacji konkretnej agendy, operacjonalizacji planu, budżetowania itp. Cele powinny być przeglądane i ewentualnie rewidowane cyklicznie.
7	Wybrane cele na 2035 roku: 1. Wszystkie kluczowe usługi dostępne są przez aplikację mobilną. 2. Państwowe systemy i rejestry są w pełni interoperacyjne. 3. 20 mln Polek i Polaków aktywowało portfel tożsamości cyfrowej. 4. Płatności elektroniczne są dostępne w całej administracji. 5. 50% firm i 80% urzędów wykorzystuje technologie sztucznej inteligencji. 6. Wszystkie istotne incydenty cyberbezpieczeństwa są zgłaszane terminowo. 7. W każdym zakątku kraju jest zasięg szybkiego internetu. 8. 85% Polek i Polaków posiada przynajmniej podstawowe	**Podanie celów na rok 2035, bez podania celów cząstkowych w kolejnych latach (tzw. road map) jest dużą wadą tej Strategii.** Niektóre z tych wybranych celów powinno być zrealizowanych jak najszybciej – np. zapewnienie działania bezpiecznych systemów teleinformatycznych (jeżeli w ciągu 2-3 lat nie zapewni się prawie 100% cyberbezpieczeństwa oraz 90% redukcji oszustw natury teleinformatycznej to użyteczność cyfryzacji poważnie spadnie – będzie zbyt niebezpieczna dla obywateli. Należy też ze względu na obecną sytuację geopolityczną przygotować jak najszybciej dla wszystkich systemów teleinformatycznych (aplikacji) administracji rozwiązania zastępcze przy uszkodzeniach sieci oraz braku prądu, a nawet ewakuacji ludności. Dodatkowo 10 lat w rozwoju teleinformatyki, to prawie okres, gdzie wielu zmian nie można przewidzieć. Podkreślamy więc potrzebę gotowości do bieżącej analizy otoczenia jej realizacji oraz dokonywania korekt obranych trajektorii działania. Dodatkowe uwagi: • Żaden z celów nie dotyczy rozwoju polskich przedsiębiorstw w zakresie dostarczania usług cyfrowych. • Większość celów dotyczy tylko rozwoju i finansowania usług publicznych. • Cel 5 w praktyce jest sztuczny. • Cel 7 sformułowany jest zbyt ogólnie. Należy doprecyzować jak szybki internet będzie

Strona	Treść	Uwagi
	kompetencje cyfrowe. 9. Moc obliczeniowa dostępna dla naukowców jest przynajmniej dziesięciokrotnie większa niż dziś. 10. Wszystkie placówki ochrony zdrowia wymieniają się dokumentacją medyczną w formie elektronicznej.	dostępny, w jakiej technologii, dla jakiego % gospodarstw domowych, % użytkowników, % powierzchni
ROZDZIAŁ DIAGNOZA		
	Zdublowane diagnozy	Postulujemy połączenie części diagnostycznych zawartych w aktualnym rozdziale „Analiza SWOT" z diagnozami odnoszącymi się w innych częściach do tych samych obszarów. Z perspektywy czytelników dokumentu aktualny podział jest niepotrzebny i utrudnia odbiór treści i wniosków w nim zawartych. Diagnoza powinna znaleźć się w jednym rozdziale lub być zintegrowana z poszczególnymi obszarami strategii.
9-16		Dotyczy opisanych diagnoz na podstawie DESI, eGovernment Benchmark, DPA, DGI, Deklaracji Berlińskiej oraz badania Eurobarometru. Stwierdzamy, że do tych diagnoz opracowywanych przez różne instytucje należy podchodzić z dużym krytycyzmem, gdyż nie zawsze prezentują aktualne dla Polski (zresztą zapewne dla innych krajów również) oceny. Powodem jest brak jednolitych merytorycznie aktualnych danych, na podstawie których wyznaczana jest ocena dla danego kraju, a tym samym miejsce w danym rankingu. Czasem, niestety, również oceniający nie są w pełni rzetelni i dokonują ekstrapolacji części danych na podstawie danych historycznych lub porównawczych. **Dlatego też proponujemy dopisanie działania Ministerstwa Cyfryzacji na rzecz zapewnienia rzetelności tych indeksów w kolejnych latach**. Aby to było możliwe, MC powinno zadbać o gromadzenie aktualnych danych dotyczących cyfryzacji w Polsce i udostępnianie ich instytucjom opracowującym te diagnozy. Warto też dokonywać weryfikacji wyznaczanych indeksów, ewentualnie żądając ich poprawienia. Oczywistym jest, że te Indeksy (chociaż nie całkiem rzetelne) mają wpływ na postrzeganie danego rynku teleinformatycznego oraz poziomu informatyzacji/cyfryzacji danego kraju.

Strona	Treść	Uwagi
ROZDZIAŁ: WYZWANIA I TRENDY		
20	Brak jasnego powiązania zdiagnozowanych wyzwań i trendów z działaniami i wskaźnikami.	W naszej ocenie dla każdego z określonych obszarów „wyzwań i trendów" należy przypisać konkretne działania, które zostaną podjęte w reakcji na nie.
20	Wyzwania i trendy: Nacisk na suwerenność technologiczną. Postępująca rywalizacja przekłada się na dążenie do przywracania unijnej i krajowej produkcji kluczowych komponentów technologicznych oraz upraszczania łańcuchów dostaw. Suwerenność technologiczna jest istotna dla dalszego rozwoju, w tym utrzymania zdolności produkcyjnych w UE. Niemniej suwerenności technologicznej UE równolegle towarzyszy pogłębiająca się współpraca UE z państwami pozaeuropejskimi o zbliżonych wartościach i filozofii rozwoju cyfrowego (tzw. like-minded). Zauważalna jest konwergencja technologiczna i regulacyjna między tymi ośrodkami na świecie.	Bardzo ważny akapit, który powinien być wzięty pod uwagę w strategii – gdzie działania krajowe powinny kłaść nacisk na przywracanie krajowych produkcji kluczowych komponentów, jakimi są między innymi krajowe produkty i usługi teleinformatyczne.
21	Wyzwania i trendy: Zaburzenia konkurencji wobec dominacji dużych platform technologicznych, których pozycja rynkowa zmniejsza zasięg kontroli rządów i stanowi istotne wyzwanie z perspektywy regulacyjnej. Jest ono tym większe, że wiele z najistotniejszych platform (społecznościowych czy handlowych) ma pochodzenie poza unijne. Państwo musi angażować się w działania na rzecz	W naszej ocenie państwo musi angażować się w działania na rzecz zapewniania równego pola gry dla wszystkich uczestników rynku, szczególnie w przypadku świadczenia zbliżonych funkcjonalnie usług. Odnotowujemy jednocześnie, że z zawartej w Strategii diagnozy nie wynikają konkretne działania lub wskaźniki. Wydaje się, że powinno to zostać uzupełnione.

	zapewniania równego pola gry dla wszystkich uczestników rynku.	
ROZDZIAŁ: ANALIZA SWOT		
26	*W zakresie rozwoju cyfrowych usług publicznych (i prywatnych), Polska radzi sobie relatywnie dobrze*.	Analiza bierze w nawias usługi prywatne – nie stawiając tego zagadnienia jako jeden z istotnych punktów strategii. W dalszej części jasno widać, że e-usługi są traktowane jako usługi publiczne. Natomiast warto wskazać, że przeciętna osoba w wieku produkcyjnym korzysta z e-usług prywatnych wielokrotnie więcej niż z usług publicznych. Dysproporcja w podejściu do sfery publicznej i prywatnej jest także szczególnie zauważalna w zakresie zaprojektowanych wskaźników realizacji Strategii, których zdecydowana większość odnosi się do administracji publicznej.
27	Analiza SWOT *Cyfrowe państwo*	• Brak w silnych stronach – dużego doświadczenia krajowego we wdrażaniu takich usług jak e-commerce (np. Allegro), bankowość elektroniczna, duża akceptacja płatności elektronicznych (BLIK), • Brak w słabych stronach – współpracy publiczno-prywatnej, brak nadzoru nad usługami cyfrowymi, nastawienie administracji rządowej, że musi budować wszystko sama, brak umiejętności budowy porozumień w zakresie państwa • Zagrożenie: Konkurowanie administracji z rynkiem rodzimych dostawców, rozumienie rynku teleinformatycznego (ICT) jako dostawcy produktów (technologii).
30	Infrastruktura – wymaga usunięcia lub poważnej modyfikacji	W naszej ocenie diagnoza oraz SWOT zawierają treści o charakterze oceny subiektywnej i poważnie dyskusyjne**. Uważamy je za wręcz krzywdzące dla znaczenia, wysiłku i obciążenia branży. Szczególnie, że są istotnie wybiórcze.** **Uważamy, że powinny zostać sformułowane ponownie w drodze dialogu z udziałem reprezentacji różnych środowisk telekomunikacyjnych.** W szczególności: • Zupełnie pomięty został wysiłek prywatnego sektora telekomunikacyjnego, który mimo realnego spadku wartości rynku wciąż prowadzi wielomiliardowe inwestycje w rozwój sieci. Uznano jedynie sukces „środków unijnych oraz regulacji". Tym samym administracja publiczna przypisuje sobie pełen sukces związany z szybkim rozwojem szybkich sieci światłowodowych i ruchomych. W żaden sposób nie zauważono, że regulacje i środki unijne nie miałyby żadnego

		znaczenia, gdyby nie wysiłek rynku, także finansowy. Projekty unijne nie istnieją bowiem bez własnego wkładu finansowego. Pominięto także inwestycje czysto prywatne. Trzeba przy tym podkreślić jak ogromną część wartości rynku operatorzy inwestują w infrastrukturę corocznie. W raporcie za 2023 r. Prezes UKE wskazał, że *wartość rynku telekomunikacyjnego wyniosła w 2023 r. 43,1 mld zł* podczas gdy *na inwestycje telekomunikacyjne wydano 11,1 mld zł, z czego 9,8 mld zł (88,1%) stanowiły wydatki na infrastrukturę*. • Wyzwania zostały spłaszczone do „alternatywnych technologii dostępowych", które nie zostały nazwane, stymulacji popytu oraz „nowych infrastruktur". • Sformułowanie „skarżących się od lat na malejące przychody" należy usunąć lub rozwinąć w sposób merytoryczny. Operatorzy nie „skarżą się" tylko wskazują na proste fakty. W PL od 15 lat nominalna wartość rynku telekomunikacyjnego oscyluje w okolicach 40 mld zł. Skumulowana inflacja w tym okresie wyniosła ponad 67%. 40 mld zł dziś to mniej niż 24 mld zł w 2009 r. W ujęciu realnym wartość rynku spada. W efekcie operatorom coraz ciężej jest pozyskać kapitał niezbędny do dalszych inwestycji. Przyczyn tego stanu jest wiele, choć przede wszystkim warto wskazać dwie – z jednej strony bardzo niskie ceny usług wymuszone wysoką konkurencyjnością mocno nasyconego rynku, a z drugiej wysokie koszty wynikające wprost z polityki regulacyjnej instytucji krajowych i unijnych. • Spadająca wartość rynku nie jest specyfiką tylko Polski. Wg raportu Draghiego kapitalizacja sektora spadła o 41% w latach 2015-2023 do ok 270 mld EUR, w porównaniu ok 650 mld EUR w USA. Skalę pokazuje porównanie do największych platform (Alphabet, Amazon, Apple, Meta, Microsoft), która wyniosła 8,7 biliona USD. • Wskazanie na oddzielanie infrastruktury od usług jako szansy dla rynku nie jest adekwatne. Zjawisko to, które faktycznie występuje, jest przede wszystkim odpowiedzią właśnie na spadającą wartość rynku oraz potrzeby zwiększania możliwości inwestycyjnych wobec bardzo trudnej sytuacji rynkowej. Jest to raczej przesłanka do oceny elastyczności rynku próbującego sprostać ciągle rosnącym wymaganiom, a nie długoterminowym silnik wzrostu. • Nieuprawniona jest kategoryczna ocena konsolidacji na rynku, która jest oceniona a priori jako zjawisko negatywne. Należy ją usunąć lub przeformułować. Przede wszystkim należy wskazać, że każda większa konsolidacja podlega restrykcyjnym zasadom oceny organów regulacyjnych na poziomie krajowym lub europejskim. To do tych organów należy ocena konsolidacji na konkurencję i konsumentów oraz wprowadzenie ew. mechanizmów zabezpieczających. Z

		drugiej strony strategia zupełnie pomija wnioski płynące z raportów Draghiego i Letty. W naszej ocenie powinny być one bezwzględnie wzięte pod uwagę. Wskazano w nich, że sektor telekomunikacyjny w UE ma ok 450 mln użytkowników, ale brakuje mu skali. W UE jest 34 operatorów mobilnych (351 MVNO) w porównaniu z 3 w USA (70 MVNO) oraz 4 w Chinach (16 MVNO). W zakresie sieci stacjonarnych tylko średni unijny operator obsługuje zaledwie 5 mln użytkowników, podczas gdy w USA to 107 mln i 467 mln w Chinach. Skutkiem tego przychody na klienta oraz wydatki kapitałowe są ponad połowę mniejsze niż USA i Japonii. Według raportu Letty, inwestycje per capita wynosiły 104 EUR w UE, w Japonii 260 EUR, 150 EUR w USA i 110 w Chinach. Obraz ten jest jednocześnie zupełnie nieproporcjonalny wobec sytuacji w Polsce. Wg raportu Prezesa UKE Polsce dostęp stacjonarny świadczy 2225 przedsiębiorców. Uśredniając na jednego operatora przypada ledwie kilkanaście tysięcy obywateli. • Diagnoza pomija zupełnie poziom obciążeń regulacyjnych sektora telekomunikacyjnego, także w szerszym otoczeniu prawa gospodarczego. Zarówno raport Enrico Letty, ale jeszcze mocniej raport Mario Draghi punktują Europę za skutki jej polityki regulacyjnej. Szczególnie wybija się tutaj ogromny formalizm procedur, nadmiar i niespójność regulacji. W raporcie Draghiego przywołano też badanie Business Europe, które pokazało, że w 13 analizowanych aktach znaleziono 169 duplikujących się wymagań, w tym 29% było różnych, a 11% wprost niespójnych. Do tego dochodzi tzw. gold plating, czyli wprowadzanie dodatkowych wymagań na etapie krajowych wdrożeń przepisów. To powoduje, że firma chcąca skalować się poza jednym krajem musi liczyć się, że w każdym kraju UE mogą ją spotkać inne wymagania. W stanach i chinach ta bariera jest zredukowana. Niestety nie mamy dobrych i aktualnych narzędzi do mierzenia kosztów regulacji i ich wpływu na wskaźniki ekonomiczne, konkurencyjność czy innowacje. Raport Draghi szacuje koszt braku harmonizacji na ok 200 mld EUR rocznie. To aż 25% inwestycji niezbędnych do budowy nowego silnika rozwojowego Europy (dodatkowe 750-800 mld rocznie). Potencjał do poprawy jest więc ogromy. Zmiana podejścia do regulacji i przekierowanie wydatkowanych na te cele funduszy na rozwój wydaje się najtańszym pieniądzem po jaki można sięgnąć. Dodatkowo wg Draghi, aż 60% przedsiębiorstw UE widzi je jako barierę inwestycyjną, a dla 55% MŚP to największe wyzwanie. Warunki prowadzenia działalności w UE vs. USA dobrze obrazuje statystyka (Draghi)

		„wyprowadzek" z UE. W latach 2008-2021 aż 30% jednorożców przeniosło się poza UE, głównie do USA. Nieprzypadkowo też wartość inwestycji VC w UE i US dzieli ok 80% przepaść dla każdej fazy rozwoju firm. Uderzające jest też podsumowanie, że unia posiada już ok 100 regulacji odnoszących się do technologii oraz ponad 270 regulatorów, których kompetencje dotyczą sieci cyfrowych. Patrząc szerzej, w latach 2019-2024 w USA przyjęto ok 3,5 tys. aktów legislacyjnych i 2 tys. rezolucji podczas gdy w UE było to ok 13 tysięcy. To jednak nie wszystko, bo mamy przecież legislację krajową. Według raportu Grant Thorton w samym 2023 r. rząd i parlament uchwaliły 34,4 tys. stron nowego prawa, z czego wprowadzono 1604 modyfikacji przepisów dot. działalności gospodarczej przy rekordowo krótkim vacatio legis na poziomie 31 dni. W 1H 2024 zanotowano za to najniższy od 2000 r. wskaźnik na poziomie 4,2 tys. stron nowego prawa – spadek o 79% wobec 1H 2023. Częściowo to zapewne wynik stabilizowania nowego rządu, ale liczymy na utrzymanie tej spadkowej tendencji. Potrzebujemy nowej agendy regulacyjnej, która odważnie ograniczy obciążenia i skupi się na długofalowych celach unijnej gospodarki. Sektory, które zostaną zidentyfikowane jako kluczowe (chociażby 10 sektorów z raportu Draghiego) powinny otrzymać szczególne wsparcie i narzędzia rozwoju. • Koncentracja na niskich cenach jako zjawisku bezwzględnie pozytywnym. Niskie ceny są wynikiem wysokiego poziomu konkurencji oraz regulacji. Dylemat polega natomiast na wyważeniu cen na rynku, a możliwościom inwestycyjnym. Aktualnie postęp do Internetu jest w Polsce o 34% tańszy niż średnia w UE (19,16 EUR vs. 29,16 EUR). Jeszcze większe odchylenie widać w przypadku przychodu z usług telefonii komórkowej – przy cenie o 55% niższej za 1 minutę od średniej unijnej, ARPU wynosi tylko 50% unijnej średniej (5,5 EUR – najniższa wartość w UE (sic!) – vs. 11,1 EUR). Wg Eurostat od 2014 średnie ceny dóbr konsumpcyjnych wzrosły o 27%. Tymczasem ceny usług telekomunikacyjnych spadły o 3,3%. W Polsce sytuacja jest jeszcze trudniejsza, bo średni poziom cen usług łączności w Polsce był w roku 2023 o 47% niższy od średniego poziomu w UE, a w krajach Zachodniej Europy był on 2-3 krotnie wyższy niż w Polsce. • Z perspektywy polityk unijnych i użytkowników skutki to m.in.: ○ Utrzymanie luki inwestycyjnej wobec niezbędnych do 2030 w UE wydatków: 114 mld EUR

		na FTTH, 33,5 mld EUR na 5G i 26 mld EUR na łączność na korytarzach transportowych – w sumie 174 mld EUR (WiK Consult dla KE, Draghi szacuje na 200 mld) ○ Niski poziom konkurencyjności europejskich telekomów wobec globalnych liderów rynku telekomunikacyjnego oraz cyfrowego. ○ Ryzyko zapchania się niedoinwestowanej sieci i ograniczenia możliwości świadczenia usług cyfrowych za jej pośrednictwem. Bez silnego rynku telekomunikacyjnego i niezawodnej i odpornej łączności nie będzie podstaw do wzrostu w innych – cyfrowo zależnych – sektorach. To jest zaś kluczowe, bo wzrost ruchu w sieci generuje ciągłą potrzebę inwestowania. Tylko w latach 2019-2022 wzrost ruchu w sieciach ruchomych i stacjonarnych wyniósł odpowiednio 90 i 138%.
	Analiza SWOT *Infrastruktura*	• Silne strony ○ Dodanie: Wysoki poziom inwestycji w sieci telekomunikacyjne (wymienione w NPS). ○ Doświadczenie w zakresie dysponowania środkami publicznymi powinno trafić do „słabych stron" ze względu na niski stopień rozdysponowania środków na budowę sieci w ramach FERC i KPO. ○ Brak w silnych stronach punktu, który wyróżnia polski rynek – duży udział hurtowych dostawców dostępu do sieci umożliwiających użytkownikowi końcowemu wybór dostawcy usług. <u>Zagrożenia:</u> • Słabe strony ○ „Niewielki popyt na łącza o najwyższych przepływnościach" – należałoby ten punkt skorygować, ponieważ większym problemem jest ogólnie niska saturacja sieci budowanych ze środków publicznych i komercyjnych, ograniczająca tempo dalszych inwestycji. Dodanie: ○ Wysoki poziom regulacji na poziomie unijnym i krajowym. ○ Nieprzejrzyste regulacje na poziomie UE, dające dowolność interpretacji na niekorzyść operatorów – szczególnie przypadek zakazu świadczenia usług Zero Rate na bazie Rozporządzenia o otwartym internecie (niekorzystne wyroki ETS zaskoczyły BEREC, który uważał, że co do zasady takie usługi są dopuszczalne). ○ Utrzymanie presji cenowej na usługi regulowane (jak np. stawki MTR), połączenia wewnątrzunijne, stawki roamingowe, które powodują permanentne obniżenie

		wartości rynku. ○ Niewystarczająca skala prowadzonej działalności. ○ Niskie ARPU i wyczerpujące się możliwości inwestycyjne sektora. ○ Podwyższony poziom wrażliwości infrastruktury i usług telekomunikacyjnej na naruszenia ciągłości działania oraz naruszenia autentyczności, dostępności lub integralności danych. ○ Prawne, administracyjne, finansowe i techniczne bariery dla dalszego usprawnienia procesu inwestycyjnego (wymienione w NPS). ○ Popyt gospodarstw domowych na usługi o lepszej jakości rosnący wolniej niż rozwój infrastruktury (wymienione w NPS). ○ Słaby popyt na wyższe przepustowości w firmach braki kompetencyjne, niska świadomość i inne trudności we wdrażaniu rozwiązań wymagających wyższych przepustowości. (wymienione w NPS). ○ Niejednorodna praktyka organów administracji publicznej uczestniczących w procesie inwestycyjnym. (wymienione w NPS). ○ Brak umiejętności dialogu z dostawcami infrastruktury – sprowadzony jedynie do nadzoru formalnego. ○ Brak współpracy rynkowej przy standaryzacji na poziomie krajowym. ○ Brak umiejętności realizacji wspólnych inicjatyw w partnerstwie publiczno-prywatnym, nastawionych na rozwój. Zmiana: ○ Nieprawidłowa/niepełna diagnoza: „Ograniczona innowacyjność telekomów”: Po pierwsze uznajemy, że w przypadku analizy dot. infrastruktury wskazanie na „niską innowacyjność telekomów” jest nieadekwatne. Wręcz przeciwnie, w zakresie usług telekomunikacyjnych operatorzy aktywnie wykorzystują najnowocześniejsze technologie zarówno w obszarze sieci stacjonarnej i ruchomej. Ograniczona innowacyjność jest wypadkową wprowadzonych regulacji, które ograniczają telekomy w możliwości wprowadzania innowacyjnych usług (np. monetyzacji danych), co nie występuje w przypadku firm świadczących podobne funkcjonalnie usługi, ale bez gorsetu regulacyjnego. Późne rozdysponowanie pasma 5G w Polsce, co było wynikiem działania administracji publicznej, w porównaniu z innymi krajach, hamowało telekomy we wprowadzeniu nowych usług opartych o tę

		technologię, które są już dostępne w krajach zachodnich czy azjatyckich. Warto przypomnieć, że w przypadku wdrażania sieci 4G polskie firmy były jednymi z liderów szybkiego pokrycia kraju wówczas nową generacją sieci. ○ Zainteresowanie w Polsce innowacyjnymi usługami ze strony klientów jest niższe niż w innych krajach, z racji niższego dyspozycyjnego dochodu. Szanse: ○ Usunięcie: trend rozdzielania infrastruktury od usług (opis powyżej) ○ Dodanie: Zwiększanie skali prowadzonej działalności Upraszczanie ram regulacyjnych i usuwanie barier inwestycyjnych Efektywna gospodarka widmem radiowym (wymieniona w NPS) Wprowadzenie mechanizmów wsparcia odporności infrastruktury i usług Poprawa spójności regulacji na poziomie europejskim Zagrożenia: Usunięcie: ○ Przebijająca się narracja o konieczności konsolidacji rynku telekomunikacyjnego (opis powyżej). W naszej ocenie więcej argumentów przemawia za ujęciem tego w kategorii szans. Dodanie: ○ Utrzymywanie barier i nadmiernych kosztów regulacyjnych ○ Rozwój cyberprzestępczości zagrażającej bezpieczeństwu, integralności i nienaruszalności transmisji danych w nowoczesnych sieciach szerokopasmowych. (wymienione w NPS) ○ Dalszy spadek globalnej wartości przychodów z tytułu świadczenia usług dostępu do internetu (wymienione w NPS) ○ Słabe przygotowanie polskich firm, zwłaszcza MŚP, do funkcjonowania w Przemyśle 4.0. Brak innowacyjności może spowodować, że Polska stanie się rynkiem zbytu dla zagranicznych technologii. (wymienione w NPS) ○ Utrzymujące się rozbieżności w stosowaniu prawa przez organy administracji publicznej uczestniczące w procesie inwestycyjnym. (wymienione w NPS) ○ Brak mechanizmów pozwalających na obniżenie kosztów utrzymania sieci na terenach

		wykluczonych. (wymienione w NPS) ○ Starzenie się populacji zwiększające barierę popytową. (wymienione w NPS) ○ Utrudnione wdrażanie nowoczesnych usług 5G, z uwagi na podsycanie obaw społecznych dotyczących rozwoju infrastruktury mobilnej i powiązanej z tym emisji PEM. (wymienione w NPS) Brak odpowiednich porozumień transgranicznych z państwami spoza UE zarówno w zakresie koordynacji transgranicznej pasma 700 MHz, jak i ewentualny brak decyzji dotyczący zwolnienia przez te państwa pasma na potrzeby bezprzewodowych usług szerokopasmowej łączności elektronicznej. (wymienione w NPS)
32	Cyberbezpieczeństwo	Postulujemy dodatkowe wskazanie na obszar regulacji cyberbezpieczeństwa. Z jednej strony służą one zwiększeniu odporności podmiotów. Z drugiej, z uwagi na falę jednocześnie wprowadzanych oraz krzyżujących się regulacji podmioty są dodatkowo obciążane koniecznością spełniania wymogów regulacyjnych dla podobnej działalności, ale mających źródło w różnych przepisach. Regulacje te mogą być jednocześnie niespójne między sobą oraz na poziomie poszczególnych krajów UE, także z uwagi na goldplating. To generuje także bariery dla rozwoju firm, w tym transgraniczności. • Należy także uwzględnić szerszy temat odporności infrastruktury i usług, w tym krytycznych. Jest to obszar szerszy niż samo cyberbezpieczeństwo i dotyczy ciągłości dostaw usług niezbędnych dla usług cyfrowych, w tym telekomunikacji i prądu oraz wody.
33	Analiza SWOT *Cyberbezpieczeństwo*	Silne strony: ○ Rewizji wymaga wskazanie na duży zasób specjalistów. Wręcz przeciwnie identyfikowany jest niedobór specjalistów z obszaru cyberbezpieczeństwa co powoduje też wysokie koszty takich usług. Było to także przyczyną wprowadzenia świadczenia teleinformatycznego w uKSC. Słabe strony: ○ Brak programu edukacyjnego w zakresie cyberbezpieczeństwa na wszystkich poziomach edukacji szkolnej i uniwersyteckiej. Niewystarczające finansowanie budowy odporności, w tym cyberbezpieczeństwa w administracji i firmach. ○ Rosnący poziom obciążenia regulacyjnego. ○ Wysoki poziom współzależności wpływu ataków w łańcuchach dostaw. Zagrożenia: ○ Zmiany klimatyczne powodujące występowanie silnych zjawisk pogodowych zagrażających

		utrzymaniu ciągłości działania kluczowej infrastruktury.
ROZDZIAŁ: CELE I CZYNNIKI UMOŻLIWIAJĄCE ICH REALIZACJĘ		
37	Za kluczowe priorytety uznajemy **również rozwój polskiej gospodarki cyfrowej** (a także wykorzystanie technologii cyfrowych do rozwoju innych branż) i jej konkurencyjności, budowanie sprawności administracji w oparciu o technologie oraz zabezpieczenie praw polskich obywateli w domenie cyfrowej.	Zwracamy uwagę na ten akapit - uważamy, że rozwój polskiej gospodarki cyfrowej jest nadrzędnym priorytetem, który będzie motorem realizacji innych priorytetów. W tym miejscu priorytetem powinna się stać umiejętność Państwa do adaptacji usług i rozwiązań kreowanych przez polski sektor teleinformatyczny, tak aby wspierać jego rozwój i korzystać w rozwiązaniach publicznych.
37/38	Realizacja celów i warunków	Nie znalazła się wśród realizacji celów i warunków: • Zapewnienie partnerstwa z sektorem krajowych usług i dostawców rozwiązań informatycznych (IT) • Wpieranie innowacyjności krajowych produktów, rozwiązań i usług IT, promowanie rozwoju • Standaryzacja rozwiązań rozumiana jako dialog techniczny pomiędzy przedsiębiorstwami i z ich uczestnictwem • Używanie rozwiązań dostępnych na rynku zamiast budowania własnych rozwiązań w strukturach administracyjnych
ROZDZIAŁ: OBSZARY HORYZONTALNE		
40/41	Komunikacja elektroniczna	Postulujemy uzupełnienie diagnozy o planowany rozwój sieci ruchomej wynikający z realizacji zobowiązań inwestycyjnych określonych w wydanych decyzjach dla pasma C oraz planowanych decyzji dla pasm 700/800 MHz. Wskazują one, że m.in. do 2028 r. dostępność usług ruchomych o szybkości 120 Mb/s z opóźnieniem do 10 ms będą na poziomie 99% HH. Obszar kraju ma być z kolei pokryty w 90% z szybkością 95 Mb/s. Dalsze wymagania dot. pokrycia korytarzy transportowych. Podobnie, nie wzięto pod uwagę realizowanych obecnie inwestycji w zakresie sieci światłowodowych w ramach programów KPO/FERC, które doprowadzą do minimalizacji liczby „białych plam" w zakresie dostępu stacjonarnego o szybkościach „gigabitowych". Jest to szczególnie istotne z perspektywy rozważania alternatywnych rozwiązań, takich jak

		satelitarne. W naszej ocenie znaczenie rozwiązań satelitarnych – jakkolwiek istotnych w skrajnie oddalonych obszarach oraz jako łączność zapasowa – jest w dokumencie znacząco przeskalowane. Technologii tej poświęca się nieproporcjonalnie więcej uwagi niż faktycznie kluczowych na rynku rozwiązaniom światłowodowym oraz 4/5G, które zapewniają także wyższą jakość i niższe ceny.
40/41	Komunikacja elektroniczna	Postulujemy uzupełnienie opisu obszaru komunikacji elektronicznej o odwołanie do obowiązków na rzecz państwa realizowanych przez operatorów telekomunikacyjnych. W uwagach szeroko odnosiliśmy się do rynkowej sytuacji sektora telekomunikacyjnego. Wskazywaliśmy na konieczność ograniczenia presji regulacyjno-legislacyjnej oraz działań na rzecz wzmacniania potencjału inwestycyjnego oraz odporności. Są one konieczne dla zapewnienia sektorowi cyfrowego szybkich i niezawodnych łączy mogących sprostać coraz szybciej rosnącym wolumenom ruchu w sieciach. Musimy jednocześnie podkreślić, jaki zakres obowiązków – m.in. w zakresie szeroko rozumianego bezpieczeństwa – wykonują już obecnie przedsiębiorcy telekomunikacyjni. NA gruncie PT/PKE obowiązkiem przedsiębiorców powyżej 10 mln zł przychodów jest przygotowanie i uzgodnienie planu działania w sytuacji szczególnych zagrożeń. Dotyczy on zasad współpracy z jednostkami publicznymi, w szczególności w zakresie utrzymywania ciągłości działania oraz jej odtwarzania, a także nieodpłatnego udostępniania urządzeń telekomunikacyjnych na potrzeby akcji ratowniczych. Prezes UKE może także nałożyć dodatkowe obowiązki w drodze decyzji. Dalej idące wymagania obowiązują także na gruncie ustawy o zarządzaniu kryzysowym w zakresie w jakim obiekty infrastruktury telekomunikacyjnej stanowią infrastrukturę krytyczną. W tym zakresie operatorzy przygotowują odpowiednie plany oraz realizują zadania związane ze szczególną ochroną. Operatorzy realizują także obowiązki związane z wysyłką Alertu RCB. Operatorzy mogą być też przedmiotem szczególnego zainteresowania na wypadek stanów nadzwyczajnych. Dotyczy to gotowości na działania związane z treściami w komunikacji elektronicznej, a także gospodarowaniem majątkiem i zarządzaniem świadczeniem usług. Operatorzy wykonują także szeroki zakres obowiązków na rzecz różnych organów państwa w zakresie blokowania domen uznawanych na szkodliwe. Obowiązkiem jest też zapobieganie nadużyciom w komunikacji elektronicznej. Poza powyższym istnieje także szeroki katalog wymagań wynikających z nowego PKE, a także związanych z ochroną konsumentów, bezpieczeństwem produktów, czy szeroko rozumianym ESG. W diagnozach odnoszących się do rynku komunikacji elektronicznej należy także uwzględniać, że

		wymagania oraz poziom obciążeń jest istotnie zróżnicowany wobec różnych podmiotów w nim uczestniczących. Równe pole gry powinno znaleźć więc się wśród konkretnych działań przewidywanych w strategii. Jednocześnie, w projektowaniu nowych zadań oraz narzędzi wsparcia należy proporcjonalnie uwzględniać wkład już wnoszony przez poszczególne podmioty w rozwój całego sektora cyfrowego.
42	Cel 1. Komunikacja elektroniczna - odporność	Podobnie jak już wskazywaliśmy wyżej (SWOT) należy uzupełnić opis o wyzwania związane z odpornością komunikacji elektronicznej. Postulowane jest wprowadzenie działania polegającego na utworzeniu: Funduszu Odporności Infrastruktury Cyfrowej. Dotychczasowe działania dot. wzmocnienia cyfrowej odporności na poziomie UE skupione były na wprowadzeniu szerokiego pakietu legislacyjnego, składającego się m.in. z dyrektyw NIS2 i CER oraz rozporządzeń CSA, DORA i CRA, a także szeregu dokumentów o charakterze poza-legislacyjnym. Z perspektywy przedsiębiorstw sama ta regulacyjna ofensywa oznacza bardzo poważne trudności we właściwym zrozumieniu nowych obowiązków, ich wzajemnych zależności oraz dostosowaniu prowadzonej działalności. Szczególnie, że nowe ramy są wprowadzane bez zapewnienia faktycznych narzędzi wsparcia, także finansowego. Aktualne ramy cyfrowego bezpieczeństwa były jednocześnie tworzone na potrzeby czasów pokoju. Tymczasem sytuacja geopolityczna jasno wskazuje, że niezbędne jest zapewnienie najwyższego możliwego poziomu odporności, który będzie dostosowany do cybernetycznych, fizycznych, hybrydowych oraz militarnych zagrożeń dla infrastruktury i usług cyfrowych. Coraz silniej uwzględniane muszą być też ryzyka związane ze zmianami klimatycznymi, skutkującymi katastrofalnymi zjawiskami pogodowymi, zakłócającymi ciągłość infrastruktury cyfrowej, a także niezbędnych jej dostaw energii elektrycznej. Ostatnie tragiczne powodzie w Polsce i Hiszpanii wyraźnie pokazują skalę wyzwań na jakie trzeba być przygotowanym. Jak pokazują doświadczenia ostatnich konfliktów zbrojnych – obok zupełnie podstawowej sfery militarnej – warunkiem dla utrzymania funkcjonowania państwa, gospodarki i ludności cywilnej jest zapewnienie ciągłości działania najważniejszych usług, świadczonych zazwyczaj przez podmioty cywilne i prywatne. Jak najdłużej muszą pozostać dostępne kanały publicznej komunikacji, usługi bankowe, dostawy podstawowych mediów oraz produkcja i handel. Oznacza to też utrzymanie miejsc pracy i działania firm. Z racji tego, że cyfryzacja jest już obecna we wszystkich sektorach, zatrzymanie pracy kluczowych systemów oznaczałoby paraliż całego

		państwa i gospodarki. Spójne spostrzeżenia zawarte w opracowaniach Mario Draghiego, Enrico Letty i Sauli Niinistö podkreślają pilną potrzebę strategicznych reform w europejskim krajobrazie telekomunikacyjnym. Poprzez wspieranie inwestycji, zachęcanie do konsolidacji, reformowanie ram regulacyjnych i priorytetowe traktowanie innowacji i odporności Europa może zwiększyć swoją konkurencyjność na globalnej arenie telekomunikacyjnej. W kontekście odporności, najdokładniej wątek ten rozwija raport „Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness"[1]. Bazuje on na kilku założeniach ramowych tj. nowy krajobraz zagrożeń, bezpieczeństwo jako fundament, kompleksowe przygotowanie i ciągłość działania przy najgorszych scenariuszach, odwaga i szybkość w nowym podejściu strategicznym. W ramach szerokiego spojrzenia na odporność UE wskazano na usługi, dla których krytyczne jest utrzymanie ciągłości działania, w tym usługi telekomunikacyjne i cyfrowe. **Odporność kluczowym elementem budżetu UE** Również ww. raport premiera Sauli Niinistö wskazuje na konieczność uwzględnienia finansowania zadań w obszarze gotowości i odporności. W pierwszej kolejności wskazano na uwzględnienie diagnozy ryzyk w negocjacjach MFF po 2028 oraz zintegrowanie wątku gotowości w budżetem UE. W ramach polityki spójności środki powinny być kierowane na działania wzmocnienie wobec różnego rodzaju katastrof i kryzysów. Proponowane jest też stworzone dedykowanego Europejskiego Funduszu Gotowości, który miałby stanowić spójny pakiet działań służący budowie w pełni odpornej UE. Na cele cywilne, w tym infrastruktury krytycznej, przeznaczony miałby być nowy „Securing Europe Facility". Ogólnie cele odpornościowe mają stanowić ok 20% budżetu UE. **Luka finansowa w obszarze odporności** Wszystkie przedsiębiorstwa sektora cyfrowego, w tym telekomunikacyjnego inwestują w zachowanie ciągłości działania – zarówno na poziomie środków technicznych (lokalizacja obiektów, ich konstrukcja, zasilanie) jak i organizacyjnych (procedury, certyfikacja, ludzie). Działania te mogą być podejmowane w granicach odpowiednich do możliwości finansowych w ramach danego podsektora. Ich ramy wyznaczają wymagania prawne (o ile istnieją), odpowiedzialność kontraktowa oraz ochrona wizerunku. Podobnie jednak jak w innych obszarach istnieją granice możliwego zaangażowania finansowego.

[1] https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

		Są one wyznaczane przez wymagania bardzo konkurencyjnego rynku, w którym wciąż dominują warunki cenowe. Przedsiębiorstwa, których istotą jest utrzymanie na rynku i rozwój muszą ważyć zakres inwestycji w obszarze odporności. Jest to zjawisko analogiczne do innych obszarów. Przykładowo przedsiębiorstwa telekomunikacyjne, bez dodatkowego wsparcia nie są w stanie samodzielnie realizować inwestycji na obszarach tzw. „białych plam", gdzie warunki inwestycyjne nie zapewniają zwrotu z perspektywy rozsądnego inwestora prywatnego. Podobnie jak w przypadku takich inwestycji, także w obszarze odporności istnieje istotna luka inwestycyjna, której pokrycie będzie wymagało uruchomienia narzędzi finansowania. W aktualnych warunkach rozdrobnionego, wymagającego ogromnych inwestycji w jakość, pojemność i zasięg sieci, a jednocześnie wysoce konkurencyjnego rynku o niskich cenach usług, podjęcie takich wyzwań będzie niemożliwe bez dodatkowego wsparcia. Jeśli więc cen osiągnięcia najwyższego poziomu odporności na wszelkie scenariusze zostanie uznany za jedną flagowych inicjatyw kolejnego budżetu UE konieczne będzie określenie ram dla pomocy publicznej w tym obszarze. W pierwszej kolejności powinny zostać wprowadzone nowe kategorie pomocy zwolnionej z notyfikacji do rozporządzenia GBER - w celu sprawnego udzielania pomocy przez kraje członkowskie. Ramy pomocy powinny też zostać określone na poziomie programów centralnych KE. **Odporność infrastruktury cyfrowej jest już wspierana** W 2024 r. australijski rząd powołał dwa programy dotyczące odporności, które funkcjonują w ramach szerokiego planu „Better Connectivity Plan". Pierwszy „Telecommunications Disaster Resilience Innovation"[2] zakłada m.in. wsparcie dla hybrydowego zasilania obiektów telekomunikacyjnych wykorzystującego połączenie OZE, paliw płynnych, akumulatorów; mobilnych generatorów. Uruchamiając ten program Minister Łączności wskazał trafnie: "*Access to telecommunications coverage during a natural disaster can be the difference between life and death and the Albanese Government's investment will help to save lives. While no network is ever 100 per cent disaster-proof, the Government is determined to do what we can to boost the resilience of our telecommunications networks when Australians need*

[2] https://minister.homeaffairs.gov.au/MurrayWatt/Pages/funding-delivered-strengthen-telco-resilience-during-disasters.aspx

		them most.”. Drugim programem jest “Mobile Network Hardening Program”[3], którego celem jest modernizacja sieci na obszarach słabo zaludnionych poprzez wsparcie operatorów w poprawie odporności infrastruktury. Aktualnie trwa 3. runda naboru projektów. Dotychczas realizowane były inicjatywy tj. zasilanie zapasowe, nowe generatory, poprawa odporności transmisji sygnału, akumulatory zapasowe, wzmocnienie obiektów na wypadek pożarów), odbudowa obiektów. W Kanadzie prowadzone są prace analityczne dot. poprawy odporności infrastruktury telekomunikacyjnej[4], które odwołują się m.in. do doświadczeń Australii. Podobne analizy scenariuszy prowadzono w Niemczech.[5] **Propozycja – Europejski Funduszu Odporności Infrastruktury Cyfrowej** Za niezbędną uważamy pełną koncentrację na adekwatnym przygotowaniu UE, a w szczególności jej krajów granicznych. Do tego konieczne będzie przyjęcie silnych paradygmatów, w tym dot. odporności europejskich przedsiębiorstw, ram pomocy publicznej oraz celów strategicznych Unii. Nieodzowne będzie wprowadzenie mechanizmów wsparcia finansowego dla ponadstandardowego zwiększania odporności kluczowych infrastruktur cyfrowych. Konieczne jest też przyjęcie wspólnego, solidarnego wysiłku całej UE niezależnie od tego jaka odległość dzieli dane państwo od granic z potencjalnymi agresorami. Postulujemy więc przede wszystkim **stworzenie Europejskiego Funduszu Odporności Infrastruktury Cyfrowej.** Może on funkcjonować w ramach wieloletnich ram finansowych lub na wzór Funduszu Odbudowy i Rozwoju. Może zostać powołany jako nowy filar przyszłego CEF – CEF DIGITAL RESILIENCE. Powinien on bazować na analizie zagrożenia oraz wskazywać na kluczowe reformy oraz obszary inwestycji. W zakresie odporności infrastruktury telekomunikacyjnej przedstawiamy poniższe obszary kluczowe: • Redundancja lądowych połączeń międzynarodowych oraz krajowych sieci szkieletowych. Wsparcie powinno objąć inicjatywy mające na celu wzmocnienie ciągłości działania sieci, w tym związane z ich zasilaniem (wyższe poziomy gwarancji zasilania z sieci, magazyny,

[3] https://www.grants.gov.au/Go/Show?GoUuid=d4484970-c328-493d-ba03-36497a14887c
[4] https://crtc.gc.ca/eng/publications/reports/gartner2024.html
[5] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Strategiepapier_Resilienz_eng.pdf?__blob=publicationFile&v=2

		instalacje OZE). • Zwiększenie odporności sieci ruchomych, m.in. poprzez wsparcie dla realizacji dosyłu światłowodowego oraz niezawodnego zasilania. • Wspieranie projektów mogących ograniczać wpływ zakłóceń sygnału radiowego (zarówno w sieciach telekomunikacyjnych, jak i satelitarnych) oraz fizycznych ataków, w tym z użyciem dronów. • Inicjatywy służące zabezpieczeniu danych, w tym w lokalizacjach alternatywnych, o niskim poziomie zagrożenia fizycznymi lub militarnymi atakami.
42	Koordynatorzy szerokopasmowi	**Dobra współpraca z samorządami jest jednym z podstawowych warunków dla realizacji zadań inwestycyjnych w terenie. Niezrozumiałe jest przyjęcie bardzo odległego terminu realizacji w 2026 r. Wnioskujemy o zmianę daty realizacji na 2025. Szczególnie, że podstawy prawne do wdrożenia tego narzędzia są już gotowe.**
45	*Cel 3: Usługi telekomunikacyjne są powszechnie wykorzystywane wśród społeczeństwa, administracji i biznesu*	Brak w budowaniu realizacji celu: o Utworzenia ścisłej współpracy z dostawcami usługi sieciowych umożliwiającej synchronizację działań – poprzez standaryzacje, wspólne projekty rozwojowe, tworzenie jednolitego przekazu, koordynację mechanizmów transformacji o Finansowanie krajowych rozwiązań badawczych w zakresie rozwoju sieci.
45	Wsparcie finansowe i organizacyjne podmiotów zaangażowanych w wdrażania sieci ruchomych nowej generacji dzięki utworzeniu Funduszu Zastosowań Sieci Mobilnych (5G i 6G), w ramach którego możliwa będzie współpraca instytucji publicznych z instytutami badawczymi, uczelniami i przemysłem w celu rozwoju zastosowań dla sieci mobilnych wraz zapewnieniem odpowiednich środków na ten cel.	Może zamiast tworzenia nowego Funduszu lepiej umieścić to odpowiednio na liście priorytetów NCBiR (jeśli chodzi o R&D) lub programów wsparcia PARP (gdy podejście bardziej wdrożeniowe) Warto spojrzeć, jak do takich projektów związanych z 5G od kilku lat podchodzi niemiecki rząd (np. programy tamtejszego Ministerstwa Gospodarki i Ochrony Klimatu). **5G i 6G wymagają zupełnie innych spojrzeń. Pierwszy temat to już „chleb codzienny", drugi - to pierwsze lata nowego wyścigu technologicznego.**
46	System satelitarny	Postulujemy rozważenie, czy nie byłoby bardziej zasadnym, by Polska zamiast budować swój własny system satelitarny, wdrażać pod niego systemy komunikacji kwantowej, budować autonomiczne operacje czy algorytmy do sterowania czy optymalizacji oraz monitorowania ziemi etc., była aktywnym uczestnikiem w stworzeniu europejskiego systemu satelitarnego, np. w

		ramach ESA, który zapewniłby większą innowacyjność i cyberbezpieczeństwo, niższe koszty finansowe dla Polski niż budowa własnego systemu satelitarnego oraz większą konkurencyjność z skali globalnej. Stworzenie przez każdy z krajów członkowski w ramach EU osobnego systemu satelitarnego spowoduje rozdrobnienie tego rynku oraz większe zaśmiecenie przestrzeni kosmicznej. Nad stworzeniem infrastruktury na rzecz odporności, wzajemnych połączeń i bezpieczeństwa drogą satelitarną w UE systemu składającego się z ponad 290 satelitów na różnych orbitach i powiązanego segmentu naziemnego w celu świadczenia usług rządowych do 2030, pracuje już konsorcjum SpaceRISE (IRIS2).
47	Kompetencje przyszłości	W diagnozie dla kompetencji przyszłości są prezentowane zbiorczo wszystkie kategorie kompetencji, które powinny być wyraźniej rozdzielone, gdyż tylko wtedy można dokładniej określić możliwości i potrzeby, jakie powinny być uwzględnione w Strategii Cyfryzacji. Możemy wyróżnić następujące kategorie kompetencji: **Kompetencje rozwoju teleinformatyki.** W tej kategorii mamy osoby, które zostały wykształcone na studiach I oraz II stopnia w dyscyplinie informatyka (dziedzinie nauk matematycznych) lub w dyscyplinie informatyka techniczna i telekomunikacja (dziedzinie nauk technicznych) na kierunkach informatycznych, teleinformatycznych, telekomunikacyjnych oraz pokrewnych. Absolwenci studiów uniwersyteckich nabywają umiejętności w zakresie architektury i rozumienia funkcjonalności urządzeń cyfrowych (komputerów, itp.) oraz logicznego myślenia i teorii obliczeń w projektowaniu złożonych algorytmów wraz z ich implementacją w postaci oprogramowania, oraz systemów informatycznych i aplikacji. Absolwenci studiów technicznych nabywają umiejętności projektowania i wykonywania sprzętu cyfrowego (komputerów, sterowników, modemów, smartfonów, itp.) oraz projektowania i implementacji algorytmów oprogramowania systemowego, systemów teleinformatycznych oraz aplikacji użytkowych. Uzyskując dyplom informatyka lub inżyniera informatyka, teleinformatyka, telekomunikacji są przygotowani do eksploatacji istniejącego sprzętu cyfrowego i oprogramowania oraz do jego rozwoju. Wg GUS[6] w roku akademickim 2023/2024 mieliśmy 14 tys. absolwentów technologii teleinformacyjnych (chyba bez informatyków z uniwersytetów). Znacznie więcej było tych absolwentów w poprzednich latach. Przy tym trzeba uwzględnić, że około 10% rozpoczynających studia, rezygnuje

[6] https://stat.gov.pl/obszary-tematyczne/edukacja/edukacja/szkolnictwo-wyzsze-w-roku-akademickim-20232024,8,10.html

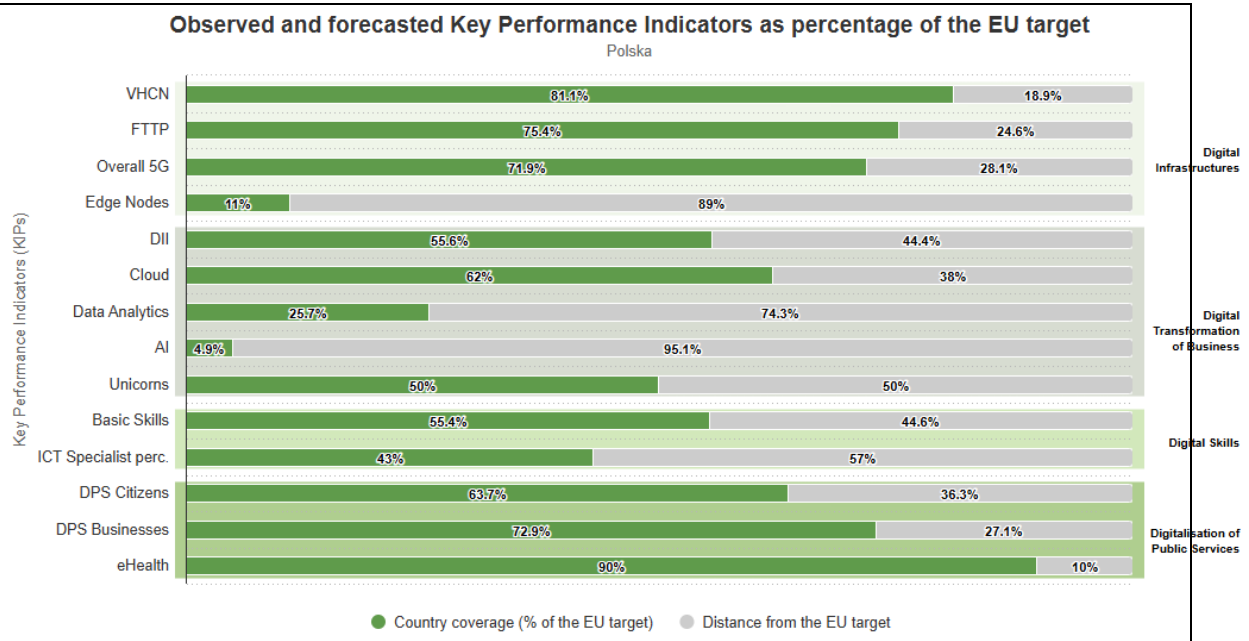
		z nich w trakcie, często skuszonych dobrymi finansów ofertami pracy. Przy poszukiwaniu możliwości zwiększenia naboru kandydatów musimy brać pod uwagę dwa czynniki. Pierwszy z nich wynika z natury genetyki, gdy talenty formułowania bardziej złożonych algorytmów ma jedynie niewielki procent młodzieży (podobnie jak talent muzyczny czy wokalny) w danej populacji – grupie kandydatów na studia. Wraz z drugim czynnikiem – niżem demograficznym będziemy w najbliższym czasie dysponować znacznie mniejszą grupą dobrych kandydatów i kandydatek na studia informatyczne. Trzecim czynnikiem są znaczne braki w dobrej kadrze nauczającej, gdyż poziom wynagrodzeń uczelnianych jest znacznie niższy od średnich wynagrodzeń w przemyśle teleinformatycznym – co nawet przy zmniejszonej liczbie kandydatów ma istotne znaczenie na przyszłość – brak kandydatów na asystentów oznacza bowiem potem ograniczenia w badaniach rozwojowych oraz wyższej kadry naukowej. Z braku istnienia wpisu zawodów informatyk oraz inżynier informatyk w Klasyfikacji Zawodów i Specjalności, oraz braku możliwości oszacowania liczby zatrudnionych informatyków wg klasyfikacji PKD (informatycy są zatrudniani we wszystkich działach PKD) nie dysponujemy dobrymi szacunkami, ilu mamy aktywnych zawodowych informatyków w kraju. Coraz większa ich część jest wykorzystywana przez ośrodki zwalczania cyberzagrożeń oraz przez służby i wojsko. Wielu z nich, często najzdolniejszych wyjeżdża za granicę, głównie do USA, do pracy dającej nie tyle większe wynagrodzenie, ile większe możliwości rozwoju zawodowego. Większość z nich tracimy bezpowrotnie. W jakimś stopniu możemy ich zastąpić obecnie informatykami (zawodowymi programistami) z Białorusi i Ukrainy, ale nie jest zbyt dobre rozwiązanie. Pozostaje jeszcze oszacowanie, rzeczywiście ilu informatyków będziemy potrzebować w najbliższych latach, gdy obecnie notujemy objawy recesji przemyśle teleinformatycznym. **Kompetencje zastosowań teleinformatyki.** W tej kategorii mamy osoby, które mają się zajmować specjalistycznym zastosowaniem produktów i usług teleinformatycznych w określonych tematach. Specjalistami tymi mogą być zawodowi informatycy, absolwenci studiów Informatyki Stosowanej oraz osoby o innych zawodach technicznych, matematycy, fizycy, chemicy oraz ekonomiści i z wielu kierunków humanistycznych (prawnicy, socjologowie, psychologowie), a także nawet medycy i muzycy (STEM). Konieczne jest przy tym douczenie ich na szkoleniach lub studiach podyplomowych podstaw teleinformatyki przez informatyków, a informatyków podstaw z dziedzin, dla których ma być zastosowane rozwiązania teleinformatyczne. Z racji powszechnego zastosowania rozwiązań teleinformatycznych praktycznie w całej gospodarce, sektorze finansowym oraz w administracji i edukacji, a także w medycynie, sądownictwie, bezpieczeństwie

		państwa liczba specjalistów teleinformatyki, według szacunków UE, w Polsce powinna być rzędu miliona. W tym przypadku możliwe i pożądane jest znaczące zwiększenie liczby specjalistek teleinformatyki, korzystając z ich zawodowego wykształcenia. Jednocześnie konieczne jest stałe analizowanie, jak bardzo obecne i przyszłe zastosowania systemów SI mogą ograniczyć lub zwiększyć liczby aktywnych specjalistów i specjalistek teleinformatyki. Należy też uwzględnić potrzeby zapewnienia podstawowego bezpieczeństwa systemów teleinformatycznych oraz służb i wojska w przypadku prowadzenia działań obronnych lub walki z klęskami żywiołowymi. **Kompetencje użytkowania teleinformatyki.** [częściowo z wykorzystaniem tekstu ze Strategii] W tej kategorii mamy wszystkich polskich obywateli w wieku od 7 do 90+ lat. Pomijamy najmłodsze pokolenie, które ma już do czynienia z użytkowaniem smartfonów i tabletów od 2-3 lat, oczywiście pod kontrolą (nie zawsze) rodziców. Pokolenie młodzieży szkolnej od 7 do 18 lat użytkuje sprzęt cyfrowy i wiele aplikacji bez problemu, jednakże brakuje im krytycyzmu co do oceny rzetelności i jakości kontentu oraz etycznych zasad użytkowania. Są też narażeni na zagrożenia na cyberataki i oszustwa internetowe. Brakuje im też umiejętności korzystania z zasobów informacyjnych w samodzielnym uczeniu się. Tutaj znaczącą rolę powinna mieć edukacja szkolna, nie tylko na przedmiocie informatyka, ale praktycznie na każdym z przedmiotów. W grupie dorosłych według danych Eurostatu, w 2023 r. tylko 44% polskich obywateli posiadało co najmniej podstawowe (średnia UE - 56%), a 20% – ponadpodstawowe umiejętności cyfrowe (średnia UE - 27%). Deficyt kompetencji cyfrowych jest przede wszystkim widoczny wśród osób starszych (w wieku 65-74 lata), gdzie 87% nie posiadało nawet podstawowych umiejętności cyfrowych (średnia UE - 72%) i w grupie wiekowej 55–64 lat, w której takie osoby stanowiły 76% (średnia UE - 56%), podobnie jak wśród rolników i osób z niepełnosprawnościami - 77%. Odnotowano także spore dysproporcje wśród osób zamieszkujących miasta i wsie: odsetek mieszkańców terenów wiejskich z co najmniej podstawowymi kompetencjami cyfrowymi wyniósł 33% (średnia UE - 47%), o 22 punkty procentowe mniej niż w przypadku osób zamieszkujących miasta. Kompetencje cyfrowe powinny umożliwić obywatelom zrozumienie i odnalezienie się w środowisku wykorzystującym technologie w niemal każdym aspekcie życia. Osoby o niskich umiejętnościach cyfrowych znacznie bardziej narażone są na dezinformację i nieumiejętne weryfikowanie informacji otrzymanych drogą cyfrową – są narażeni na cyberoszustwa oraz cyberataki. Osoby dorosłe w wieku produkcyjnym powinny być obowiązkowo doszkalane w umiejętnościach teleinformatycznych pożądanych w wykonywaniu zadań ich pracy zawodowej. Należy też stworzyć możliwość szkolenia całej populacji dorosłych (w tym seniorów) w

		umiejętnościach korzystania z teleinformatyki w życiu prywatnym oraz w kontaktach z administracją państwową. Szczególną uwagę należy zwrócić na umiejętność racjonalnego i rozumnego korzystania z systemów AI, upraszczających korzystanie z rozwiązań i zasobów teleinformatycznych.
	Kompetencje przyszłości – **Wymagania dla zwiększania kompetencji cyfrowych**	1. Utrzymanie wyodrębnionego przedmiotu informatyka w programie szkoły podstawowej oraz średniej. W programie nauczania tych przedmiotów powinna być zwrócona uwaga na nabywanie umiejętności poprawnego korzystania ze sprzętu cyfrowego oraz aplikacji użytkowych wraz z dbałością o bezpieczeństwo ich użytkowania. 2. Wprowadzenie na każdym z przedmiotów szkolnych odpowiednich aplikacji wspomagających tematycznie program nauczania wraz z umiejętności wykorzystania systemów SI. 3. Utrzymanie przedmiotu informatyka rozszerzona w programie szkoły średniej z wprowadzeniem prawa do zdawania informatyki na egzaminie maturalnym. 4. Wspomaganie organizacji konkursów oraz olimpiad matematyczno-informatycznych, szczególnie w szkołach średnich dla wyodrębnienia uczniów i uczennic mających zdolności matematyczno-informatyczne. 5. Zwiększenie liczby miejsc na studiach o kierunkach informatycznych oraz pokrewnych (bezpieczeństwo systemów teleinformatycznych, modelowanie systemów SI, itp.) poprzez dofinansowywanie kosztów prowadzenia tych zajęć – kontrowersyjne, gdyż brak jest możliwości różnicowania wynagrodzeń pracowników dydaktycznych. 6. Zwiększenie liczby miejsc na studiach na kierunkach zastosowania teleinformatyki oraz włączenie przedmiotu zastosowania teleinformatyki na każdym prowadzonym kierunku studiów. 7. Utworzenie z finansowaniem centrów naukowo-badawczych w dziedzinie teleinformatyki – np. rozwój metod bezpieczeństwa systemów teleinformatycznych, rozwój modelowania oraz generowania specjalistycznych systemów SI, rozwój metod identyfikacji i weryfikacji osób (w tym ich akceptacji dokumentów), rozwój nowych form przetwarzania informacji (w tym urządzenia mechaniki kwantowej), itp. Tego typu centra mają dostarczyć gospodarce nowe rozwiązania teleinformatyczne, ale też mają zatrzymać najlepsze kadry specjalistów teleinformatyki. 8. Obserwowanie działalności oraz czasowe zapraszanie na uczelnie lub do centrów badawczych naszych profesjonalnych naukowców z informatyki. 9. Wprowadzenie do Klasyfikacji Zawodów i Specjalności zawodu informatyk i inżynier

		informatyk oraz stała analiza statystyczna aktywnych zawodowo profesjonalistów teleinformatyków (informatyków, inż. informatyków, teleinformatyków oraz telekomunikacji). 10. Zwiększanie zatrudnienia specjalistów teleinformatyki – zawodowych informatyków oraz z innych zawodów, przyuczonych do wykorzystania rozwiązań teleinformatycznych w różnych dziedzinach gospodarki, finansów oraz administracji. W tym przypadku możliwe jest znaczące zwiększenie liczby kobiet zaangażowanych w wykorzystywaniu teleinformatyki. 11. Zweryfikowanie jakości nauczania (treści oraz umiejętności prowadzących) wszystkich szkoleń i studiów podyplomowych w przyuczaniu osób z innymi niż teleinformatyczne zawodami do pracy jako specjaliści teleinformatyki. [lepiej, aby nie było casusu Collegium Humanum]. 12. Stałe weryfikowanie jakości i dostępności oraz użyteczności wszystkich aplikacji teleinformatycznych udostępnianych przez administrację publiczną i samorządową do wykorzystania przez obywateli (z uwzględnieniem osób młodych, pracujących zawodowo, starszych oraz z niepełnosprawnościami, itp.). Utrzymywanie klasycznych procedur administracyjnych dla osób nie „akceptujących" rozwiązań teleinformatycznych. 13. Wprowadzenie wymogu na opracowanie dla każdej aplikacji teleinformatycznej wersji możliwych do ograniczonego (ale skutecznego) użytkowania w warunkach niezwyczajnych (braku prądu, klęsk żywiołowych, katastrof, stanu zagrożenia lub wojny). Konieczne jest odpowiednie rozpropagowanie tych rozwiązań zastępczych.
54	Cel 4: Pracownicy administracji publicznej posiadają kompetencje cyfrowe niezbędne do świadczenia e-usług publicznych o najwyższym poziomie dojrzałości oraz efektywnego działania administracji.	Proponujemy dopisać punkt: d) *d) Uporządkowanie nomenklatury nazewnictwa stron internetowych JST wraz z unifikacją komunikacji elektronicznej e-mail.* Przykładowo: urzad@krakow.gmina.pl, podatki@piaseczno.gmina.pl, kultura@nowawola.gmina.pl
	a) Zapewnienie dostępu do wysokiej jakości szkoleń, warsztatów praktycznych oraz pakietów kursów e-learningowych, zakończonych ewaluacją zdobytych kompetencji, np. w modelu mikropoświadczeń, m.in. w obszarach świadczenia cyfrowych usług publicznych, identyfikacji elektronicznej, zarządzania cyfryzacją, cyfryzacji procesów,	W naszej opinii, to bardzo dobry pomysł, jednak by zachęcić pracowników JST mikropoświadczenia powinny być uznanymi certyfikatami w Polsce i/lub świecie. W innym wypadku będzie to tylko zaświadczenie wydane przez ministerstwo lub inną jednostkę publiczną. Szkolenia zakończone dodatkowym egzaminem powinny mieć wyższą wartość rynkową, przez co powinno być zachęcające do pogłębiania wiedzy lub wręcz obligatoryjne. Ponadto w kontekście AI należałoby oprócz promowania open source stworzyć np. białą listę rozwiązań Trustworthy AI w oparciu o rozwiązania światowe, licencjonowane, gwarantujące rzeczone „trustworthy". Dla JST potrzebne też są konkretne rekomendacje lub wręcz szablony dokumentów, będące wymaganiami na systemy w oparciu o AI. Dobrym pomysłem była też tzw. architektura referencyjna, która miała

	cyberbezpieczeństwa, sztucznej inteligencji, systemów chmurowych, zarządzania i analizy danych oraz otwierania danych, inteligentnych miast i wsi (smart city i smart village), open-source (otwarte oprogramowanie) w administracji, zarządzania dostępnością cyfrową i jej wdrażaniem itp.;	być wykonana w NASK oraz projekty pilotażowe w wybranych miastach różnych wielkości
	b) wprowadzenie systemowego wsparcia dla pracowników administracji chcących się przekwalifikować do zawodu specjalisty ICT	Przekwalifikowanie się pracowników administracji na specjalistów teleinformatyki powinno dotyczyć analizy danych i wsparcia JST w tworzeniu departamentów analiz danych i strategii miasta. Takie departamenty potrzebują urzędników wykształconych do pracy z danymi i platformami lowcode/nocode obsługującymi te dane.
	c) wprowadzenie w administracji publicznej prymatu kształcenia własnych kadr w obszarach zdiagnozowanych potrzeb ICT (np. cyberbezpieczeństwo, sztuczna inteligencja).	Najpilniejsze potrzeby to praca z danymi. Nie można mówić o AI bez danych, które je zasilają, w tym przede wszystkim danymi miejskimi.
56	Cel 6: Polskie przedsiębiorstwa posiadają kompetencje cyfrowe kluczowe do efektywnego prowadzenia biznesu, utrzymania pozycji konkurencyjnej na rynku i strategicznego rozwoju firmy przy wykorzystaniu rozwiązań cyfrowych	Brak realizacji celu poprzez Budowanie dialogu publiczno-prywatnego, w ramach którego kompetencje polskich przedsiębiorstw będą wykorzystywane przez sektor publiczny (zamiast ich kanalizowania poprzez konkurowanie rządu z biznesem w dostarczeniu usług cyfrowych). Według naszej oceny zaniedbano rozwój i cyfrową transformację podmiotów gospodarczych, i w niewystarczający sposób promowano strategiczne elementy Europejskiej Strategii Danych ogłoszonej w 2020 roku. Komisja Europejska w ostatnim raporcie oceniającym postępy Polski na drodze do osiągnięcia celów Dekady Cyfrowej 2030 wskazuje, że mimo odnotowania postępów nadal bolączką w naszym kraju są kompetencje cyfrowe pracowników i wdrażanie przez przedsiębiorstwa zaawansowanych technologii, takich jak sztuczna inteligencja czy narzędzia do analizy danych.

		 *Źródło: Komisja Europejska, Cyfrowa Dekada 2024, raporty krajowe – Rzeczpospolita Polska*
60	*Rozwijanie krajowych rozwiązań i standardów kryptograficznych (w tym w zakresie kryptografii postkwantowej), a także inicjowanie programów i projektów badawczo-rozwojowych i innowacyjnych w tym zakresie, aby Polska dokonała bezpiecznej migracji do kryptografii postkwantowej oraz mogła wykorzystać technologie kwantowe na rzecz bezpieczeństwa państwa;*	Działanie wymaga nie tylko straszenia, ale zrozumienia ryzyk, opracowania strategii wyboru zagrożeń, przygotowania planów, itp. Proponujemy jasne odwołanie się do zaleceń KE dot. kryptografii postkwantowej: https://digital-strategy.ec.europa.eu/pl/news/commission-publishes-recommendation-post-quantum-cryptography Punkt wydaje się prezentować stan wiedzy sprzed kilku lat. Temat PQC jest na liście priorytetów EU Horizon, instytucje badawcze i firmy mogą aplikować o środki na projekty wdrożeniowe. Migracja do PQC powinna w dużym stopniu dokonać się do 2030 - kto w branży ICT tego nie zrobi będzie po prostu zapóźniony technologicznie. Standardy PQC zostały opublikowane przez NIST w 08'2024, jest też lista rezerwowa. Raczej nie ma więc już miejsca na pracę u podstaw, tzn. wymyślanie nowych algorytmów (może poza wąskimi niszami). Więc zamiast inicjować programy i

		projekty badawcze raczej trzeba skupić się na wsparciu już w pełni produkcyjnych projektów / inicjatyw wdrożeniowych.
64-65	*1.4 Koordynacja cyfrowej transformacji kraju. Wciąż brakuje kompleksowej, spójnej i uporządkowanej informacji na temat stanu informatyzacji podmiotów publicznych i ich efektów.* *Cel 1: Wymiana informacji na temat stanu cyfryzacji jednostek administracji publicznej oraz realizowanych przez nie przedsięwzięć informatycznych jest sprawna i efektywna*	Dokument utożsamia cyfryzację kraju z cyfryzacją administracji publicznej. Brak odniesienia się w strategii do faktu, że cyfryzacja dotyczy wielu aspektów funkcjonowania obywatela i przedsiębiorstwa nie pozwala na zauważenie, że skuteczna transformacja kraju, w tym także transformacja obszaru podmiotów publicznych jest ze sobą związana. Przykładem tutaj jest fakt, braku kompleksowej i uporządkowanej wiedzy o stanie informatyzacji podmiotów publicznych, ale także brakuje wiedzy o informatyzacji w szkolnictwie i nauce, transformacji cyfrowej firm, poziomie użycia usług cyfrowych przez obywateli w obszarze usług zaufania. Brakuje zdefiniowania wskaźników, które powinniśmy badać jako społeczeństwo informacyjne w obszarach życia i funkcjonowania.
66	*Cel 2: Projekty informatyczne są realizowane i zarządzane w sposób skoordynowany, przejrzysty i efektywny*	Cel nie zauważa, że wiele projektów w Polsce skupia się tylko na budowaniu kolejnych rozwiązań w podmiotach publicznych, często rozwiązania są bliźniaczo podobne, wykorzystują te same funkcjonalności, jednakże wielokrotnie skupione na dostarczeniu sprzętu i kodu potrzebnego do realizacji przedsięwzięcia. W ramach celu nie wskazano, że koordynacja przedsięwzięć w zakresie informatyzacji sektora publicznego powinna: • Wprowadzić politykę re-użycia danych i usług dostępnych na rynku wewnętrznym, w którym nie buduje się rozwiązań, dla których istnieją na rynku wewnętrznym usługi, w szczególności, jeżeli podlegają one nadzorowi państwa • zapewnić używanie standardów polskich PKN, europejskich ETSI i CEN oraz międzynarodowych w przedsięwzięciach, włączyć projekty tworzone w Polsce w procesy standaryzacyjne, w tym także uczestniczyć jako państwo w procesie standaryzacji
67	*Cel 3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa.*	Architektura informacyjna państwa nie bazuje na standardach technicznych, administracja publiczna wdraża standardy własne dalekie od normalizacji technicznej, w którą powinno się zaangażować na poziomie Polskiego Komitetu Normalizacyjnego. Wykorzystanie standardów technicznych i potencjału, który jest związany z funkcjonowaniem norm technicznych pozwala na znaczące zmniejszenie kosztu budowy rozwiązań i w sposób naturalny angażuje sektor prywatny w możliwość dostarczenia rozwiązań. Cel powinien określić, że Architektura Informacyjna Państwa oparta powinna być o przyjęte krajowe, europejskie lub międzynarodowe normy a państwo powinno być zaangażowane w proces normalizacji w przypadku braku wymaganych norm. Jednocześnie normalizacja pozwala na przeniesienie części nadzoru do procesów audytowych i

		certyfikacji, gdzie państwo może korzystać z jednolitego sposobu nadzoru nad rozwiązaniami technicznymi w zakresie IT.
69	*Cel 4: Dyplomacja cyfrowa jest skuteczna i efektywnie koordynowana.* *b) Rozwinięcie w urzędzie obsługującym ministra właściwego ds. informatyzacji kompetencji w zakresie pozyskiwania inwestycji zagranicznych w nowoczesne technologie w Polsce i promowania polskich technologii cyfrowych na świecie oraz przeznaczenie odpowiednich zasobów na ten cel. Pozwoli to m.in. na rozwijanie zdolności w zakresie zapewnienia suwerenności technologicznej w kooperacji z partnerami międzynarodowymi;*	Realizacja celu związanego z promocją polskich rozwiązań technicznych i technologii wymaga od ministra właściwego ds. informatyzacji zaangażowania się w rozwój polskiego rynku IT także na poziomie wewnętrznym, głównie poprzez dialog z rynkiem, wskazanie, że rynek to zarówno nauka, rozwój technologii, rozwój usług, normalizacja i patenty. Dziś minister ds. informatyzacji o czym świadczy treść strategii nie widzi rynku, ponieważ jego kompetencje są związane głównie z administracją publiczną.
ROZDZIAŁ: PAŃSTWO		
72	*2.1 E-usługi publiczne* *Diagnoza – jak jest?*	**Rozdział ten powinien być napisany ponownie we współpracy z ekspertami zajmującymi się identyfikacją tożsamości oraz podpisami elektronicznymi.** Diagnoza pominęła fakt jak dużą rolę w transformacji cyfrowej kraju miały banki, dostarczając zarówno mechanizmów identyfikacji użytkowników jak i interfejsu dla wielu usług publicznych takich jak wnioski 500+/800+. Ten przykład pokazuje jak ważna jest koordynacja działań z podmiotami, które obsługują klienta/petenta na co dzień. Na ile zamiast budować kolejne systemy po stronie administracji nie dałoby się wykorzystać potencjału tych, którzy realizują procesy z użytkownikiem oraz mają już znaczące doświadczenie w opracowywaniu interfejsów łatwych w obsłudze dla użytkowników. Jednocześnie w diagnozie zawarto sugestie dotyczące braku jednolitego interfejsu do składania podpisu i pieczęci, należy wskazać, że podstawowym brakiem nie jest interfejs użytkownika natomiast brak jednolitych ram akceptacji podpisów elektronicznych w Polsce, wspieranych przez administrację międzynarodowych standardów w ramach interfejsów API oraz brak testów interoperacyjności. Tworzenie interfejsu użytkownika dla podpisów stworzy nową barierę w rozwoju usług publicznych, poprzez brak akceptacji dostawców podpisu (tak jak się to dzieje dziś),

		brak możliwości dołączania nowych portfeli cyfrowej tożsamości do podpisywania, brak możliwości integracji z innymi usługami, ograniczenie do jednego scenariusza wymyślonego przez urzędników.
73	*brak jednego punktu dostępu do e-usług publicznych dla obywatela, przedsiębiorców i administracji zapewniającego jednolity interfejs i sposób uwierzytelnienia użytkownika oraz zapewniającego funkcjonalności podpisu cyfrowego i pieczęci elektronicznej;*	Cel wskazuje na konieczność budowania kolejnego obywatel.gov.pl lub ePUAP, natomiast budowanie jednego punktu dostępu do usług jest obarczone ryzykiem niedostosowania do potrzeb, rozwoju i narzędzi. Przykładem jest fakt, że żaden system administracji publicznej nie dostosował się do funkcjonujących od 6 lat na rynku zdalnych kwalifikowanych podpisów elektronicznych – uniemożliwiając korzystanie z nich. Powodem jest to, że podążanie cyfrowe wymaga inwestycji i bieżącej współpracy z użytkownikiem. W tym zakresie państwo nie zauważa potencjału integracji różnych usług z systemami państwa, tak żeby one mogły stanowić interfejsy do usług państwowych, a konkurując ze sobą stawiały na innowacyjność i łatwość dostępu, adresowanie potrzeb użytkowników. Integracja z identyfikacją i podpisami powinna być realizowana na poziomie sytemu integracyjnego z innymi usługami a nie na poziomie interfejsu użytkownika, który powinien móc być wybrany przez użytkownika z wachlarza rozwiązań.
73	*wdrożenie różnorodnych narzędzi (platform) realizacji e-usług publicznych, które nie są zbudowane w oparciu o jednolite standardy umożliwiające uwzględnienie specyficznych potrzeb użytkowników e-usług, m.in.*	W katalogu narzędzi brakuje narzędzi do akceptacji złożonych podpisów elektronicznych, które byłyby oparte o europejskie standardy oraz przyjętą krajową politykę podpisu elektronicznego – która by ustaliła zasady akceptacji podpisów elektronicznych na poziomie krajowym. Aktualnie państwo nie potrafi w usługach publicznych akceptować podpisów elektronicznych opartych o kwalifikowane certyfikaty zagraniczne oraz nie akceptuje wszystkich wymaganych przepisami europejskimi formatów podpisu. W wielu usługach państwowych jedyną opcją jest złożenie podpisu zaufanego, który nie spełnia standardów europejskich.
73	*brak e-usług publicznych akceptujących transgraniczne metody uwierzytelnienia;*	Problemem akceptacji transgranicznej identyfikacji elektronicznej jest oparcie prawie wszystkich usług publicznych o konieczność identyfikacji numerem PESEL, w tym zakresie bardzo brakuje jednolitej strategii w zakresie posługiwania się PESEL, sposobów realizacji usług w przypadku, gdy brakuje PESEL lub dysponujemy innymi identyfikatorem. Całość może dotyczyć szerszego zakresu architektury systemów administracji publicznej, które nie potrafią realizować usług bez numeru PESEL.
75	*a) Wdrożenie jednego punktu dostępu do e-usług publicznych dla obywateli, przedsiębiorców i administracji. Zapewniać on będzie jednolity interfejs uspójniający dostępne kanały komunikacji realizacji e-usług;*	Konieczność poza interfejsem ustalenia jednolitych ram integracji usług zewnętrznych (świadczonych jako proxy) także przez podmioty prywatne dla usług publicznych, gdzie użytkownik nie musi korzystać z interfejsu państwowego dla zrealizowania usługi.

75	*c) Dostosowanie wymaganych i kluczowych e-usług publicznych do wymogów krajowego i europejskiego portfela tożsamości cyfrowej, będącej certyfikowanym, uznawanym środkiem identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa;*	To jest bardzo ważny cel, natomiast jego realizacja powinna opierać się o realizację celu jakim jest utworzenie jednolitych ram integracji z portfelem cyfrowej tożsamości oferowanymi przez nie usługami z możliwością korzystania z usług i informacji dostarczanych przez portfel tożsamości cyfrowej w sposób elastyczny – uwzględniający wykorzystania w usługach potwierdzeń atrybutów pochodzących z różnych publicznych i prywatnych usług, jednocześnie korzystanie z atrybutów wymaga stworzenia krajowych repozytoriów schematów dla rozpoznawalnych atrybutów, brak takich schematów na poziomie krajowym będzie skutkował powstawaniem schematów lokalnych, których interoperacyjność będzie bardzo trudna.
75	*e) Organizacja systemowego wsparcia podmiotów świadczących e-usługi publiczne w uspójnieniu działań w zakresie zapewnienia jednolitego dostępu do e-usług oraz środków identyfikacji elektronicznej.*	Wsparcie i koordynacja powinny dotyczyć zarówno podmiotów świadczących bezpośrednio e-usługi jak i podmiotów wspierających świadczenie tych usług – w tym pośredników.
76	*Cel 2: Wdrożone jednolite narzędzia służące realizacji e-usług publicznych ułatwiają interakcję podmiotów świadczących e-usługi z ich użytkownikami.*	Realizacja celu w strategii jest oparta o budowanie narzędzi i rozwiązań, brakuje standaryzacji technicznej, opartej o funkcjonowanie ciał standaryzujących w tym Polskiego Komitetu Normalizacyjnego, uczestnictwo w standaryzacji na poziomie europejskim, ustanawianie w porozumieniu z rynkiem standardów publicznie dostępnych. Możliwe, że ustanowieni reguł i sfinansowanie publicznej dostępności standardów mających zasadnicze znaczenie dla rozwoju administracji publicznej.
76	*b) Zwiększenie zakresu e-usług publicznych świadczonych przy wykorzystaniu jednolitych platform realizacji e-usług;*	Realizacja celu powinna uwzględniać funkcjonowanie platformy integracyjnej dla usług świadczonych przez podmioty trzecie, powstanie ram dopuszczania podmiotów zewnętrznych do platformy integracyjnej w tym także jednolitych modeli współpracy z rynkiem w zakresie świadczenia usług za pośrednictwem podmiotów niepublicznych, w tym także rozwój piaskownicy integracyjnej, w której innowacyjne i zewnętrzne usługi mógłby być testowane
76	*f) Wdrożenie mechanizmów bezpiecznego przesyłania dokumentów elektronicznych, w tym przy wykorzystaniu systemu e-Doręczeń;*	Należy zwrócić uwagę, że system doręczeń elektronicznych, to jest sieć współpracy dostawców doręczeń elektronicznych spełniających standard i w tym zakresie należy szeroko współpracować z rynkiem, a mechanizmy tworzyć w sposób znormalizowany w ramach krajowej normalizacji, która pozwoli na transparentność procesu i brak wykluczenia podmiotów. **Niedopuszczalnym jest realizowanie rozwoju doręczeń elektronicznych poprzez narzucanie rozwiązań bez współpracy i dialogu z rynkiem.** Usługi publiczne powinny integrować się na zasadzie otwartych interfejsów ze wszystkimi dostawcami doręczeń elektronicznych, na zasadach podobnych jak dziś płatności integrują się ze

		wszystkimi bankami i schematami płatniczymi.
78	*Cel 3: Rozwiązania horyzontalne zapewniają optymalizację świadczonych e-usług publicznych*	Konieczne jest wdrożenie: • jednolitych mechanizmów opartych o publiczne API w zakresie integracji usług publicznych z doręczeniami elektronicznymi • jednolitych mechanizmów opartych o publiczne API w zakresie integracji usług publicznych z usługami kwalifikowanego podpisu elektronicznego w tym także usługami podpisu zdalnego oraz opartego o podpis składany z użyciem europejskiego portfela tożsamości cyfrowej • jednolitego mechanizmu opartego o publiczne API pozwalającego na walidację kwalifikowanych i zaawansowanych podpisów elektronicznych, które spełniają politykę podpisu elektronicznego akceptowanego w usługach publicznych • budowy katalogu schematów i polityk dla tworzenia elektronicznych poświadczeń oraz warunków ich prawidłowego rozpoznawania
81	*f) Ustawowe umocowanie systemu EZD RP oraz powołanie Operatora EZD odpowiedzialnego za rozwój systemu EZD RP, bezpłatne wsparcie wdrożeniowe I utrzymaniowe EZD RP świadczone na rzecz podmiotów realizujących zadania publiczne.*	Zmonopolizowanie rozwoju platformy typu EZD poprzez wspieranie tylko jednolitego rozwiązania EZD RP może skutkować ograniczeniem rozwoju i brakiem konkurencyjności rynku. W tym zakresie należy rozważyć, czy w oparciu o otwarty kod EZD RP nie zbudować ekosystemu EZD RP pozwalającego rozwijanie się na zasadzie licencji europejskiej wielu rozwiązań rozszerzających funkcjonowanie EZD RP. W tym zakresie konieczne byłoby ze strony państwa koordynowanie repozytorium kodu, testowanie oraz promowanie społeczności firm rozwijających kod EZD RP w sposób innowacyjny i dostosowany do potrzeb.
83	*b) Pełne wdrożenie i upowszechnienie elektronicznych doręczeń (e-Doręczeń) zarówno w relacjach z podmiotami publicznymi, jak i między podmiotami niepublicznymi;*	Doręczenia elektroniczne wymagają współpracy pomiędzy dostawcami usługi publicznej RDE oraz kwalifikowanych RDE w zakresie nie tylko przekazywania usług między sobą, ale jednolitego modelu integracji z usługami publicznymi. Strategia powinna obejmować zwiększenie współpracy z rynkiem kwalifikowanych usług doręczeń, ponieważ jedynym sposobem, aby usługi niepubliczne korzystały powszechnie z doręczeń pomiędzy sobą jest obsługa ich przez w ramach usług kwalifikowanych. Strategia także powinna obejmować rozszerzenie dostępności usługi doręczeń w szczególności tam, gdzie formalne bezpieczeństwo komunikacji może wspierać bezpieczne transakcje – np. pomiędzy pracownikiem a pracodawcą, pomiędzy konsumentem a dużymi dostawcami usług przez internet (usługi telekomunikacyjne, sklepy internetowe, usługi ubezpieczeniowe), a także obowiązek obsługi przez doręczenia pracowników przez pracodawców.

83	*c) Wprowadzenie obowiązku integracji e-usług z e-Doręczeniami, co zapewni obywatelom jedno miejsce, w którym będą mieli zgromadzoną całą korespondencję z urzędami, bez względu na to, z którego serwisu udostępniającego e-usługi korzystali.*	Integracja z doręczeniami musi objąć nie tyko publiczną usługę, ale także możliwość integracji usług kwalifikowanych, ponieważ brak jednolitego wypracowanego na zasadzie normalizacji API uniemożliwi obsługę osób, które korzystają z usługi kwalifikowanej
85	Stworzenie narzędzia AI do tworzenia przejrzystego prawa.	W naszej ocenie zadanie to wymaga doprecyzowania. W zakresie wymiaru sprawiedliwości niewątpliwie narzędzia AI powinny być wykorzystywane jako wsparcie wymiaru sprawiedliwości np. w automatyzacji żmudnych operacji (np. pobieranie danych, tworzenie podsumowań, szablonów pism). Wątpliwości istnieją natomiast w zakresie postulatu tworzenia przez nie „przejrzystego" prawa. Pomijając kwestie formalne wynikające z zasad prowadzenia procesu legislacyjnego należy podkreślić szczególną wagę pracy człowieka. Technologie AI, w szczególności GenAI, mogą halucynować, cechować się stronniczością (ang. bias), co mogłoby wpłynąć niekorzystnie na takie przepisy. W naszej ocenie narzędzia AI mogą być stosowane jako narzędzie pomocnicze, w tym analityczne pomocne w wyszukiwaniu potencjalnych niespójności pomiędzy przepisami.
86	*Brak jest powszechnie obowiązującego i jawnego standardu API dla systemów teleinformatycznych służących do realizacji zadań publicznych, który ułatwiałby i przyspieszał integrację rozwiązań cyfrowych, przyczyniając się do zwiększenia interoperacyjności, w tym dostępności i jakości zasobów informacyjnych państwa.*	Brakuje przejrzystego mechanizmu, który pozwoliłby, aby opracowywane API powstawało przy uczestnictwie rynku, w oparciu o doświadczenia podmiotów i w oparciu o uznane standardy. Narzucenie API nie rozwiąże problemu.
87	*Cel 1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne*	Cel powinien zostać uzupełniony o normalizację i standaryzację. W tym zakresie konieczne jest włączenie w działania Polskiego Komitetu Normalizacyjnego, zaangażowanie się poprzez utworzenie komitetu do spraw normalizacji w administracji publicznej, budowanie rozwiązań w zakresie przejrzystego procesu normalizacyjnego, finansowanie normalizacji i budowanie siły normalizacji poprzez finansowanie normalizacji z pieniędzy publicznych
89	*Cel 2: Udostępnianie wysokiej jakości danych z rejestrów publicznych i publicznych*	Wśród realizacji celów brakuje realizacji zobowiązania rozporządzenia eIDAS udostępniania danych rejestrowych na potrzeby kwalifikowanych usług elektronicznego potwierdzenia atrybutów, a

	systemów teleinformatycznych odbywa się w sposób bezpieczny i zautomatyzowany	także szerszego modelu udostępniania danych w ramach europejskiego portfela cyfrowej tożsamości. Realizacja wymagań powinna zostać określona w celu - *„Umożliwienie wymiany danych rejestrowych z wykorzystaniem europejskiego portfela tożsamości cyfrowej poprzez ustanowienie jednolitych zasad dostępu do danych rejestrowych oraz utworzenie repozytorium krajowych schematów poświadczeń pozwalających na jednolite krajowe ramy wydawania i weryfikacji poświadczeń atrybutów."*
91	*2.4 Cyfrowa tożsamość* *Diagnoza – jak jest?*	W diagnozie zabrakło kilku aspektów: • Należy wskazać, że możliwość wyboru przez użytkownika środka identyfikacji, z którego może skorzystać, jest ważnym aspektem dostępności i wspiera rozwój rynku. • Głównym motorem dostępności środków identyfikacji elektronicznej są bankowe środki identyfikacji, które pozwoliły szybko dostarczyć rozwiązanie do wielu uczestników rynku, jednocześnie pozwoliły użytkownikom wybrać rozwiązanie optymalne do ich potrzeb. • Państwo nie daje możliwości łatwego i szybkiego podłączania się do profilu osobistego i profilu mObywatel identyfikacji elektronicznej przez podmioty prywatne – proces jest złożony i długotrwały. • Podłączenie przez węzeł krajowy narusza ustanowione w UE zasady nielinkowalności i braku śledzenia użycia środków identyfikacji elektronicznej • Państwo nie rozpoznaje zarówno krajowych jak i zagranicznych kwalifikowanych podpisów elektronicznych w usługach publicznych i nie rozpoznaje wszystkich wymaganych przepisami formatów podpisów elektronicznych. Warto wskazać, że w diagnozie pominięto funkcjonującą z powodzeniem pieczęć elektroniczną zarówno w podmiotach publicznych jak i gospodarczych. • Nie ustanowiono ram pozwalających na integrację rozwiązań podpisu elektronicznego z usługami publicznymi, nie stosuje się międzynarodowych standardów API pozwalających na integrację podpisów zdalnych • Państwo skupiło się na rozwoju usług administracji publicznej, natomiast świadomie ograniczało możliwość rozwoju usług kwalifikowanych np. poprzez uniemożliwianie rejestracji w krajowych usługach kwalifikowanych zdalnie – bez konieczności fizycznej obecności. • Aktualnie istnieje coraz więcej naruszeń bezpieczeństwa systemów administracji publicznej poprzez posługiwanie się cudzym profilem zaufanym i podpisem zaufanym,

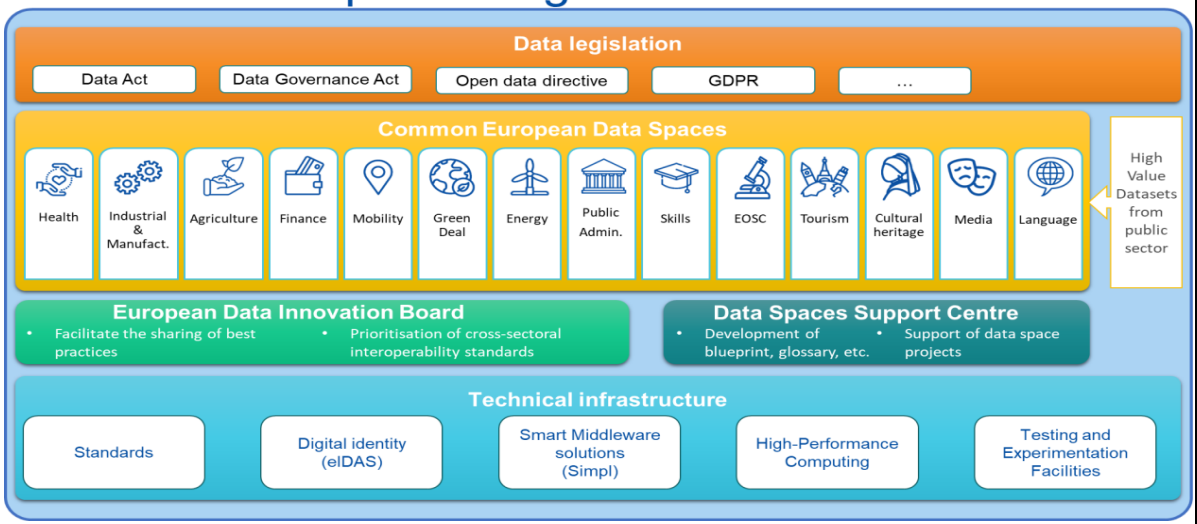
		środki te nie są monitorowane a jednocześnie pojawiają się nowe formy ataku na administrację publiczną oraz środki publiczne za pomocą przejętych profili zaufanych, w tym zakresie państwo nie zarządza ryzykiem i nie odpowiada na bieżące zagrożenia. • W zakresie cyfrowej tożsamości nadzór ministra właściwego jest realizowany nad usługami, które sam świadczy, wobec czego w rzeczywistości następuje konflikt interesu związany z prawidłowym rozwojem narzędzi i świadczeniem roli nadzorczej. • Nie jest prawdą, że nie istnieją narzędzia do składania podpisów wielokrotnych pod dokumentami, natomiast brakuje polityki akceptacji takich podpisów, wobec czego składane są w różny sposób z wykorzystaniem różnych narzędzi. • Wskazując rozwiązanie europejskiego portfela tożsamości cyfrowej pominięto fakt, że portfele mogą być wydane bezpośrednio, w oparciu o upoważnienie lub uznawane przez państwo członkowskie – innymi słowy nie muszą być dostarczone przez Ministra Cyfryzacji. Ten fakt wymaga szerokiej współpracy nie tylko z potencjalnymi dostawcami wewnątrz administracji, ale także innymi podmiotami zaangażowanymi już dziś w dostarczanie narzędzi dla cyfrowej tożsamości. Ten fakt może mieć także wielkie znaczenie dla udostępnienia portfela dla przedsiębiorstw.
92	*Polska posiada dwa notyfikowane środki identyfikacji elektronicznej: profil zaufany i profil osobisty, jednak ich praktyczne użycie w usługach online innych państw członkowskich jest nieznaczne.*	W naszej opinii powinien być notyfikowany trzeci środek identyfikacji: Profil mObywatel. Nie było realizowanej żadnej promocji ani kampanii informacyjnej o możliwości wykorzystania środków identyfikacji transgranicznie. Problem też nie dotyczy tylko Polski, inne kraje UE też nie promują znacząco identyfikacji elektronicznej na poziomie transgranicznym. Dodatkowo strategia powinna uwzględniać „poświadczenie obywatela" (Person Identification Data - PID) wystawiane przez administrację publiczną, jako dodatkowy środek identyfikacji, który może stanowić dodatkowe źródło uwierzytelnienia obywatela i może być przechowywane z zachowaniem najwyższych środków bezpieczeństwa w certyfikowanym prywatnym cyfrowym portfelu tożsamości.
93	*a) Utworzenie w ramach publicznego systemu identyfikacji elektronicznej środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej osobę prawną;*	Utworzenie środka identyfikacji dla osoby prawnej powinno być związane z europejskim portfelem cyfrowej tożsamości i zintegrowane z nowymi wymaganiami, stworzenie samego środka bez tej integracji może w rzeczywistości być nieużyteczne, ze względu na brak automatyzmu i powiązania z nowoczesnymi usługami. Tworzenie osobnego środka dla osoby fizycznej reprezentującej osobę prawną w rzeczywistości będzie miało zastosowanie tylko dla ograniczonego zakresu spraw, należy wskazać, że reprezentacja w podmiotach związana jest z zakresem uprawnień oraz pełnomocnictwami.

		Aktualnie rozwijane w ramach tzw. Large Scale Pilots wskazują na konieczność ustanowienia schematów uprawnień i pełnomocnictw dla osób fizycznych reprezentujących osoby prawne. Jednocześnie należy odejść od proponowanych w latach wcześniejszych rejestru pełnomocnictw – ponieważ nie może on mieć zastosowania biznesowego – ze względu na nieadekwatność do wymagań obrotu gospodarczego.
93	*d) Utworzenie narzędzia zapewniającego możliwość łatwego i wygodnego składania podpisów elektronicznych niezależnie od ich rodzaju i formatu dokumentu w przypadku wieloosobowej reprezentacji osoby prawnej ("wielopodpis");*	Tworzenie narzędzia przez podmioty publiczne dla składania podpisów wielokrotnych wydaje się powielaniem rozwiązań dostępnych na rynku, które spełniają wymagania norm technicznych. W Polsce nie opracowano zasad (polityki) tworzenia i akceptacji podpisów elektronicznych, wobec czego nie istnieje skoordynowany model pozwalający na wykorzystanie rozwiązań dostępnych na rynku. Należy się skupić na wypracowaniu krajowych zasad (polityki) i ew. opracowaniu na zasadzie otwartego kodu rozwiązań referencyjnych. Ustanowienie zasad na poziomie krajowym opartych o polskie lub europejskie normy pozwoli także na certyfikowanie rozwiązań zamiast budowy rozwiązania, które może nie sprostać wyzwaniom rynku.
93	*e) Udostępnienie europejskiego portfela tożsamości cyfrowej do użytku osób prawnych.*	Samo udostępnienie portfela, bez wsparcia i rozwoju krajowych inicjatyw związanych z jego akceptacją nie rozwiąże problemu. Portfel osób prawnych potrzebuje szerokiej akceptacji w usługach publicznych i prywatnych, możliwość jego zasilania potwierdzeniami atrybutów związanymi z prowadzoną działalnością – np. koncesjami, referencjami, potwierdzeniami bankowymi, poświadczeniami w zakresie zabezpieczenia społecznego i podatków. Jednocześnie wymaga to otwartości i zbudowania krajowych ram pozwalających na zasilanie portfela poświadczeniami pochodzącymi z rynku prywatnego i wykorzystywanych w sektorze prywatnym. Jednocześnie wymaga to łatwości udostępniania portfela firmowego różnym stronom ufającym bez zbędnego bagażu biurokracji.
94	*Cel 2: Podpisy elektroniczne są dostępne I powszechnie używane, a ich weryfikacja jest prosta i niezawodna bez względu na format dokumentu i rodzaj podpisu*	Pierwszym elementem umożliwiającym realizację celu jest odbudowanie współpracy z kwalifikowanym dostawcami usług zaufania, w celu współpracy i wytworzenia krajowych polityk związanych z akceptacją podpisów elektronicznych. Dotychczasowa polityka państwa oparta na ignorowaniu rynku i samodzielnej budowie rozwiązań podpisu elektronicznego i pozwala adresować wyzwań rynku i uniemożliwia rozwój.
94	*a) Rozwój narzędzi do podpisywania i weryfikowania dokumentów podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym;*	Cel wymaga najpierw zbudowania krajowej strategii funkcjonowania podpisów elektronicznych, tak aby nie były budowane rozwiązania, które obciążają budżet państwa natomiast ich zastosowanie jest ograniczone. W związku z tym należy postawić na ustanowienie krajowych wymagań (polityk) tworzenia i akceptacji podpisów elektronicznych, które by powstały wraz z

		rynkiem dostawców usług podpisu. Rozwój narzędzi do podpisywania i weryfikacji powinien oznaczać wspieranie interoperacyjności rozwiązań opartych o uznane normy techniczne, wspieranie API dostępu do usług podpisu, certyfikację rozwiązań. Konieczne jest wspieranie testów jakościowych w zakresie weryfikacji podpisów elektronicznych i zgodność aplikacji do weryfikacji podpisów z wymaganiami norm. Powinny powstać krajowe rekomendacje w zakresie implementacji rozwiązań podpisu w usługach publicznych, uwzględniające akceptację podpisów kwalifikowanych opartych o certyfikaty pochodzące z innych krajów UE, w tym także rekomendacje w zakresie akceptacji podpisów niezawierających numeru PESEL.
94	*b) Rozpowszechnienie informacji o korzyściach wynikających z korzystania z możliwości składania i weryfikowania podpisów elektronicznych w ich systemach, w tym wspierających realizację e-usług publicznych, poprzez integrację z komponentem węzła podpisu.*	Wskazano w celu mechanizm – węzeł podpisów – nie ujmowany nigdzie w innych celach.
94		W celach brakuje – ustanowienie ram pozwalających na akceptację podpisów nie zawierających numeru PESEL, ramy dla podpisów kwalifikowanych stosowanych przez urzędników
94		Zasady tworzenia dokumentów zawierających podpisy elektroniczne w podmiotach publicznych zostały opracowane w latach 2005-2008, od tego czasu nie uległy zmianie. Technologicznie się zmieniło bardzo dużo, a nie zostały wpracowane na poziomie krajowym rekomendacje i nowe standardy, które ułatwiłyby korzystanie z podpisów elektronicznych w usługach publicznych. Wymagany jest przegląd i ustanowienie nowych rekomendacji dla podpisywania dokumentów.
94		Brak powszechności podpisu elektronicznego jest związany z niską dostępnością środka identyfikacji elektronicznej na poziomie wysokim jakim jest profil osobisty oraz brakiem wsparcia krajowego dostawców podpisu w zakresie potwierdzania tożsamości. Celem powinno być utworzenie jednolitych ram potwierdzenia tożsamości dla wszystkich podpisów akceptowanych przez podmioty publiczne. Pomysłem może być także utworzenie ram pozwalających na zdalne odblokowywanie profilu osobistego w dowodzie osobistym bez konieczności chodzenia do urzędu. Taki model pozwoliłby na znaczące ułatwienie w posługiwaniu się profilem osobistym w usługach publicznych.

95	*a) Budowa oraz wdrożenie modelu szerokiego wykorzystywania warstwy elektronicznej dowodu osobistego oraz certyfikatów elektronicznych związanych z wykonywanym zawodem w systemach teleinformatycznych;*	Niezrozumiałe jest powiązanie w jednym punkcie certyfikatu związanego z wykonywanym zawodem z dowodem osobistym. Wydaje się, że powinny to być osobne punkty, ponieważ dowód osobisty co do zasady jest narzędziem związanym z osobą i nie powinno się łączyć codziennego używania dowodu osobistego jako narzędzia w sprawach służbowych. Certyfikat związany z wykonywanym zawodem raczej powinien być elektronicznym potwierdzeniem atrybutu, który może funkcjonować w oparciu o portfele cyfrowej tożsamości.
95	*Dodanie do węzła krajowego środka identyfikacji o wysokim poziomie bezpieczeństwa, jakim będzie europejski portfel tożsamości cyfrowej;*	Należy zwrócić uwagę, że europejski portfel cyfrowej tożsamości powinien mieć możliwość funkcjonowania bez węzła, w oparciu o bezpośrednią komunikację strony ufającej z portfelem. Ten model związany jest z utworzeniem znaczących usprawnień w zakresie wydawania certyfikatów stronom ufającym i dostępności także polskiej implementacji portfela poza węzłem krajowym.
95	*c) Dodanie do węzła krajowego historii użycia środków identyfikacji elektronicznej;*	Cel jest sprzeczny z założeniami funkcjonowania środków identyfikacji elektronicznej określonych rozporządzeniem eIDAS i jest sprzeczny z wymaganiami braku śledzenia użycia środka a także braku możliwości łączenia kolejnych transakcji i identyfikacji portfelem (linkowalność). Historia użycia środka może jedynie być zbierana po stronie użytkownika usługi i nie może być dostępna dla stron trzecich. Środki identyfikacji elektronicznej co do zasady nie służą dostarczeniu wartości dowodowej w transakcji a jedynie dostarczeniem informacji, zabezpieczenie informacji dowodowej jest domeną usług zaufania. Realizacja celu w rzeczywistości jest sposobem inwigilacji użycia środka identyfikacji przez obywatela i może naruszać jego zaufanie do środków.
96	*c) Udostępnienie nieodpłatnych kwalifikowanych podpisów elektronicznych w europejskim portfelu tożsamości cyfrowej dla osób fizycznych, przynajmniej do użytku nieprofesjonalnego;*	Obowiązkiem portfela jest umożliwienie złożenia kwalifikowanego podpisu elektronicznego do celów nieprofesjonalnych. Zapis może sugerować naruszenie konkurencyjności poprzez szerokie udostępnienie rozwiązania finansowanego z pieniędzy publicznych, które nie będzie respektowało rozwoju usług. Wymaganej jest wprowadzenie ram, które pozwolą na możliwość składania takiego podpisu darmowego ze strony użytkownika, natomiast w sposób, który pozwoli na rozwój usług i rynku.
97	*2.5 Chmura obliczeniowa*	W diagnozie i celach brakuje odniesienia się do zapewnienia przestrzeni dla rozwoju chmury obliczeniowej, która powinna wspierać także powstawanie lokalnych komponentów chmury pozwalającej na przetwarzanie danych jak najbliżej miejsca ich powstawania oraz na rozwój infrastruktury chmurowej w sposób efektywny energetycznie.
102	*2.6 Otwarte dane i wymiana danych Diagnoza*	Dane postrzegane są obecnie jako podstawowy czynnik rozwoju ekonomicznego w każdej dziedzinie. Bez odpowiedniej jakości danych nie ma mowy o rozwoju sztucznej inteligencji, która definiuje na nowo strategię rozwoju krajów, przedsiębiorstw i obywateli. Bez narzędzi służących

		ponownemu wykorzystaniu danych w oparciu o suwerenne decyzje podmiotów niemożliwy jest jakikolwiek rozwój we współczesnym świecie, stąd według naszej oceny nowa polityka państwa oparta na danych powinna znaleźć się w centrum strategii cyfryzacji kraju. Doceniamy dotychczasowe osiągnięcia polskiej administracji w obszarze dostępu do otwartych danych pochodzących z projektów krajowych i unijnych. Na uwagę zasługuje fakt, że w rankingu dostępności do danych „OURdata Index" wśród krajów OECD Polska zajmuje trzecie miejsce, zaraz za Koreą Południową i Francją. Podobnie w unijnej klasyfikacji otwartości danych „Open Data in Europe" Polska wraz z Francją zajmuje pierwsze miejsce w Europie, wyprzedzając znajdujące się na drugim miejscu Estonię i Ukrainę, oraz Hiszpanię na miejscu trzecim. Pozycję Polski potwierdza także ranking „Open Data Inventory" prowadzony przez Open Data Watch, gdzie nasz kraj znajduje się na miejscu drugim, za Singapurem, a przed krajami północnej Europy Danią, Finlandią i Norwegią. W opinii Polskiej Izby Informatyki i Telekomunikacji należy w szczególności podnieść nakłady i zainicjować projekty, które pozwolą na dynamiczny rozwój gospodarki cyfrowej, w skali nie mniejszej od tej, którą osiągnięto w obszarze projektów skierowanych na administrację oraz obywateli. Ku naszemu rozczarowaniu w ostatnich blisko pięciu latach, czyli od ogłoszenia w lutym 2020 roku „Europejskiej strategii w zakresie danych", nie odnotowaliśmy na poziomie krajowym żadnych znaczących inicjatyw zmierzających do włączenia naszej gospodarki do jednolitej europejskiej przestrzeni danych. Tymczasem łączne nakłady Komisji Europejskiej i państw członkowskich na zbudowanie wspólnych przestrzeni danych w sektorach gospodarczych szacuje się na ponad 3,5 miliarda Euro.
104	*Cel 1: Administracja publiczna świadomie działa na rzecz otwartości danych*	W realizacji celu brakuje inwentaryzacji posiadanych zasobów danych, ujednolicenia sposobu ich opisywania, zmniejszenia redundancji danych, powstania narzędzia pozwalającego monitorować połączenia, ustalenia spójnego sposobu korzystania przez podmioty niepubliczne z otwartych danych
105	*Cel 2: Otoczenie prawne w obszarze zarządzania danymi sprzyja rozwojowi ekosystemu wymiany danych.* Ustanowienie przyjaznego środowiska legislacyjnego dla dzielenia się danymi z pobudek altruistycznych oraz wymiany danych w relacjach B2B oraz B2G, (w tym przyjęcie	Podstawowym instrumentem aktu w sprawie zarządzania danymi, który wynika z przyjętej w 2020 roku europejskiej strategii w zakresie danych, jest zbudowanie europejskich przestrzeni danych mających służyć zbudowaniu jednolitego rynku danych, z zachowaniem suwerenności podmiotów europejskich, i jednocześnie pozwalając na zbudowanie bezpiecznych relacji w oparciu o zaufanie do podmiotów gospodarczych uczestniczących w wymianie danych. Wstępnie zidentyfikowano kilkanaście sektorów, w których kluczowym elementem rozwoju jest zbudowanie platformy do współdzielenia danych, są to m.in. przemysł, rolnictwo, zdrowie, finanse, energetyka i inne.

	przepisów krajowych służących stosowaniu Aktu w sprawie zarządzania danymi i Aktu w sprawie danych);	 *źródło: Komisja Europejska, DG-CNECT* Przy czym należy zauważyć, że w oparciu o przyjęty model i prace normalizacyjne rozwijane są przestrzenie danych także w innych, kluczowych obszarach europejskiej gospodarki, takich jak motoryzacja czy przemysł kosmiczny i lotnictwo. Co więcej przyjęty model pozwala na osiągnięcie interoperacyjności pomiędzy przestrzeniami danych z różnych sektorów i wymianę/współdzielenie danych w oparciu o relacje zaufania pomiędzy tymi obszarami. W ten sposób uniknąć można syndromu silosowości i korzystać z danych do osiągania wspólnych korzyści poszczególnych sektorów. Należy zaznaczyć, że bez wdrożenia jednolitej przestrzeni danych niezwykle trudno będzie sprostać wyzwaniom współczesnego świata oraz zapewnić zgodność z wymogami regulacyjnymi Unii Europejskiej. Takie inicjatywy jak regulacje w obszarze cyfrowego paszportu produktu, monitorowania i raportowania łańcucha dostaw, obliczania śladu węglowego, czy śledzenia produkcji żywności, są nie do zrealizowania bez wdrożenia koncepcji wspólnych przestrzeni danych. W ostatnich latach drogą wytyczaną przez Komicję Europejską podążają inne kraje, które odgrywają znaczącą rolę w światowych łańcuchach produkcji (np. Japonia, Chiny czy Brazylia). Międzynarodowe organizacje normalizacyjne (ISO/IEC, IEEE, CEN-CENELEC, ETSI) opracowują

		standardy obiegu i zarządzania danymi.
ROZDZIAŁ: LUDZIE		
126	*3.3. Branże kreatywne*	
126	*Diagnoza*	Cieszy nas ujęcie branż kreatywnych w Strategii oraz zauważenie, iż „Mierzenie wpływu tego sektora na rozwój państwa nie może (…) być mierzone jedynie wskaźnikami gospodarczym" oraz że „branże kreatywne mają duże znaczenie kulturotwórcze i edukacyjne, sprzyjając jednocześnie innowacyjności". Należy podkreślić, że branże kreatywne odgrywają istotną rolę w unijnej, w tym polskiej gospodarce przyczyniając się do wzrostu PKB, zatrudnienia oraz eksportu. Wg raportu EUIPO z 2022 r. w latach 2017–2019 *„sektory intensywnie korzystające z praw własności intelektualnej wygenerowały 29,7% wszystkich miejsc pracy w UE (…) oraz wygenerowały ponad 47% unijnego PKB o łącznej wartości 6,4bln EUR. (…) Podczas gdy państwa takie jak Niemcy, Francja, Włochy i Niderlandy przodują w tworzeniu nowych praw własności intelektualnej, inne państwa, w tym Węgry, Polska i Estonia, również w dużym stopniu korzystają z podziału pracy w sektorach intensywnie korzystających z praw własności intelektualnej*."[7] Sektor kreatywny stanowi dynamiczny element gospodarki o dużym potencjale wzrostowym, a jego rozwój może generować nowe miejsca pracy w obszarach o wysokiej wartości dodanej. Sekcja Strategii poświęcona branżom kreatywnym skupia się przede wszystkim na e-sporcie i sektorze gier wideo. Są to z pewnością obszary o dużym potencjale ekonomicznym i kulturotwórczym, których rozwój powinien być wspierany przez państwo (vide Cele 1 i 2 tej sekcji). **Jednak w naszej ocenie nie mniej ważne są też inne sektory, takie jak przemysł filmowy i muzyczny, media, branża wydawnicza oraz nie wymieniony bezpośrednio w strategii sektor rozrywki i dostępu do treści twórczych.** Mimo że wskazując na kilka istotnych zagrożeń dla rozwoju branż kreatywnych autorzy Strategii wymienili m.in. niesprzyjające i skomplikowane regulacje prawne oraz wzrost konkurencji międzynarodowej, w ocenie członków Izby zagrożenia te nie zostały adekwatnie zaadresowane w Strategii w szczególności w *Celu 3 Branże kreatywne są wspierane w procesie rozwoju*. Regulacje

[7] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/IPR-intensive_industries_and_economic_in_EU_2022/summary/2022_IPR_Intensive_Industries_ExSum_pl.pdf

		prawne mają istotny wpływ na biznesowe funkcjonowanie polskich branż kreatywnych i na ich realne możliwości przeciwstawiania się rosnącej presji konkurencyjnej z zagranicy. Niestety w Polsce mamy z jednej strony do czynienia z nadmiernie opresyjnymi przepisami w porównaniu do przepisów innych państw członkowskich UE wynikających z niektórych unijnych dyrektyw (np. w zakresie przepisów dot. reklam w ustawie o radiofonii i telewizji, czy też wymogu odprowadzania tantiem od reemisji i VoD w krajowym prawie autorskim), z drugiej zaś strony z brakiem wdrożenia od wielu lat unijnych przepisów umożliwiających skuteczne egzekwowanie w przestrzeni cyfrowej praw autorskich (art. 8.3. dyrektywy info-soc), które to prawa mają fundamentalne znaczenie dla funkcjonowania branży kreatywnej. Od lat obserwujemy coraz większą obecność kultury i treści kreatywnych w przestrzeni cyfrowej oraz umożliwiania dostępu do takich treści nie tylko w warstwie cyfrowej (np. audiobooki, e-booki), lecz szerzej poprzez sieć internet (np. wirtualne wystawy, serwisy streamingowe). Także konkurencja o pieniądze, czas i uwagę odbiorców kultury i informacji w coraz większym stopniu stopniowo przenosi się do świata cyfrowego i internetu. Prawo i polityka państwa muszą za tymi procesami nadążać i właściwie na nie reagować. Tymczasem pod wieloma względami polski system prawny nie tylko nie stwarza sprzyjających warunków do rozwoju branż kreatywnych (np. poprzez stworzenie systemu zachęt podatkowych stymulujących produkcję i koprodukcję filmową w naszym kraju – pozytywnym wzorem mógłby być system węgierski oferujący m.in. 30% ulgi podatkowej na produkcje filmowe), lecz wręcz tworzy bariery przekładające się bezpośrednio na gorsze warunki konkurowania i prowadzenia działalności w tym sektorze przez podmioty podlegające polskiemu prawu. Jeżeli na problem braku równoważnych warunków konkurencyjnych dla polskich podmiotów w porównaniu do podmiotów zarejestrowanych w innych państw członkowskich nałożymy jeszcze bardzo silną presję konkurencyjną ze strony działających w Polsce globalnych podmiotów nie podlegających europejskiej jurysdykcji, widzimy realną potrzebę podjęcia przez państwo działań w przestrzeni prawnej celem wsparcia polskiego rynku kreatywnego. Wśród istotnych ograniczeń i barier w tym sektorze należałoby wskazać także braki kompetencyjne: niewystarczające umiejętności w zakresie cyfryzacji wśród twórców i kadr zarządzających, brak dostępu do nowoczesnych technologii w mniejszych miejscowościach oraz ograniczony dostęp do kapitału inwestycyjnego i funduszy publicznych.
131	*Cel 3. Branże kreatywne są wspierane*	W świetle powyższych uwag odnotowujemy uwzględnienie w Celu 3 tej sekcji Strategii:

	w procesie rozwoju	• punktu „a" *Dotacje i granty na rozwój projektów kreatywnych, umożliwiające artystom i firmom rozwijanie nowych projektów i technologii* oraz • punktu „g": *Wzmocnienie przepisów dotyczących ochrony własności intelektualnej, co zapewni twórcom lepszą ochronę ich prac i zachęci do innowacji* jednak apelujemy o szersze potraktowanie w Strategii problemu niesprzyjających regulacji prawnych i warunków konkurencyjnych, jak też konieczności wsparcia innowacji i transformacji cyfrowej. Sugerujemy: • dodanie kolejnego punktu: *Wprowadzenie systemu zachęt podatkowych dla sektora kreatywnego celem stymulacji jego innowacyjnego rozwoju i konkurencyjności,* • następującą zmianę brzmienia punktu „g": *Rewizja i wzmocnienie polskich przepisów dotyczących ochrony praw własności intelektualnej w przestrzeni cyfrowej pod kątem ich zgodności z normami i praktykami europejskimi, co zapewni twórcom lepszą ochronę ich prac oraz zachętę do innowacji.* • następującą zmianę punktu b) *Wsparcie rozwoju programów edukacyjnych i szkoleń, które kształcą w zakresie kreatywności, nowych technologii i zarządzania projektami kreatywnymi, a także współpraca z uniwersytetami i szkołami wyższymi w celu rozwijania programów nauczania dostosowanych do potrzeb branż kreatywnych z uwzględnieniem m.in. projektów pilotażowych, wykorzystania blockchain do zarządzania własnością intelektualną w świecie cyfrowym, automatyzacji w produkcji medialnej, legalnego wykorzystania AI w procesie twórczym.*
ROZDZIAŁ: BIZNES I TECHNOLOGIE		
138	*4.1 Cyfrowa transformacja przedsiębiorstw*	Cyfrowa transformacja przedsiębiorstw nie może być zrealizowana bez współpracy z rynkiem dostawców usług i rozwiązań dla przedsiębiorstw, są to usługi księgowe, platformy i rozwiązania. Istnieje obawa, że działania państwa mające na celu transformację cyfrową przedsiębiorstw zmniejszą potencjał rozwojowy firm, które tym się zajmują na rodzimym rynku. Jednocześnie należy zauważyć, że dziś główny rozwój firm i przedsiębiorstw jest oparty o rozwiązania teleinformatyczne, które nie powstają na rodzimym rynku – w szczególności sprzęt oraz oprogramowanie systemowe.
141	*d) Wprowadzenie instrumentu „Cyfrowy start dla biznesu", który wspierałby nowopowstałe*	Start dla biznesu powinien być oparty o krajowe rozwiązania dla biznesu, promować ich używanie i rozwój, być realizowane w taki sposób, w którym inkubator nowych biznesów buduje potencjał

	firmy w rozwoju cyfrowym. Pakiet ten zawierałby propozycje rozwiązań, cyfryzujących procesy biznesowe już na początku działania firmy I ułatwiających jej prowadzenie – np. oprogramowanie biurowe, księgowe I finansowe, zarządzania relacjami z klientami oraz dokumentami, programy do komunikacji i współpracy, oprogramowanie cyberbezpieczeństwa, ewentualnie systemy planowania zasobów przedsiębiorstwa;	biznesów świadczących rozwiązania i usługi krajowo.
142-179		We wszystkich opisywanych celach brakuje instytucji, która ma inicjować i odpowiadać za realizację danego celu oraz wskazania terminu i opisu kluczowych punktów weryfikujących postęp w realizacji danego celu (road map). Bez tych ustaleń proponowana Strategia nie ma szans na realizację. Mając na uwadze strategiczną rolę jednolitej europejskiej przestrzeni danych rekomendujemy powołanie krajowego Punktu Wsparcia Rozwoju Przestrzeni Danych, na wzór prowadzonego przez Komisję Europejską projektu Data Spaces Support Center. Zespół takiego centrum wsparcia mógłby korzystać z doświadczeń nielicznych podmiotów z Polski, które biorą udział w projektach europejskich, takich jak CloudFerro w przestrzeniach danych geosatelitarnych, czy Poznańskiego Centrum Superkomputerowo-Sieciowego w dziedzinie danych sektora rolniczego. Oferujemy wsparcie naszych ekspertów prowadzących w Izbie komitet Gaia-X i zaangażowanych w opracowanie nowych standardów w ISO/IEC i CEN-CENELEC z ramienia Polskiego Komitetu Normalizacyjnego.
146	*4.2 Sztuczna inteligencja - Diagnoza*	Gorąco popieramy wyróżniony w diagnozie postulat dotyczący regulacji, w pełni zgodny ze stanowiskiem Izby: **„Ważne jest wdrożenie tych regulacji w sposób sprzyjający innowacjom, równoważący troskę o godną zaufania, bezpieczną AI, z zadbaniem o rozwój i wdrażanie innowacji w przedsiębiorstwach. Ta równowaga powinna przejawić się zarówno w podejściu instytucjonalnym (rola i zakres działania polskich organów nadzoru współpracujących z europejskim Biurem ds. AI), jak i w systemie finansowania inwestycji”** W tym kontekście pragniemy zwrócić uwagę, że w przekonaniu Izby przedstawiony do konsultacji projekt regulacji w tym zakresie (ustawa dotycząca Komisji Rozwoju i Bezpieczeństwa Sztucznej

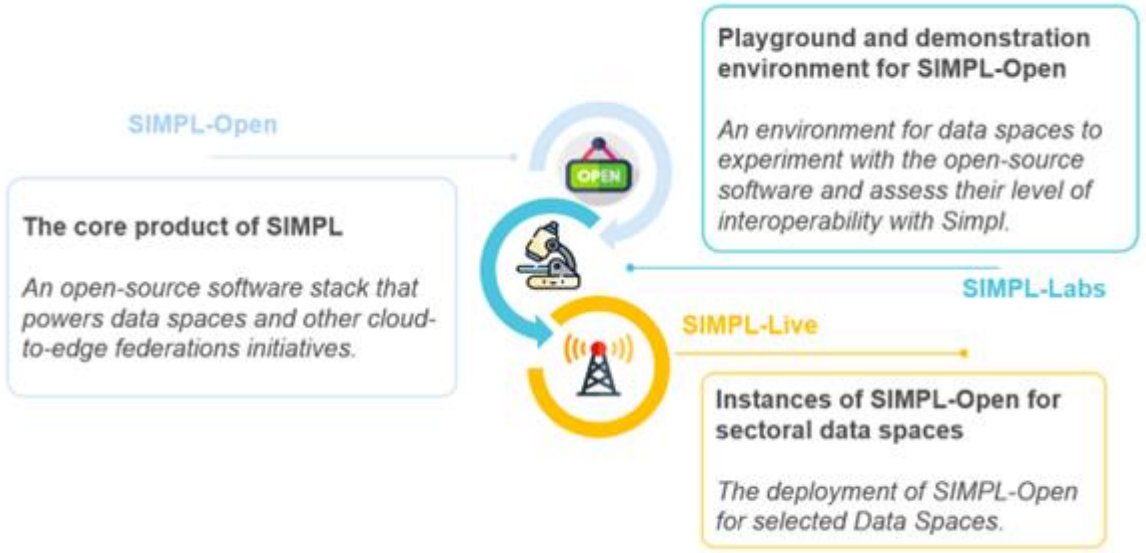
		Inteligencji) nie w pełni odzwierciedla postulaty strategii i rodzi wiele obaw o negatywne skutki, jakie mogłaby ona mieć w zaproponowanym kształcie na innowacyjność przedsiębiorstw.
		Izba popiera postulat dotyczący potrzeby aktualizacji polityki publicznej dotyczącej rozwoju sztucznej inteligencji w Polsce, w tym *wskazanie obszarów strategicznych dla rozwoju gospodarki, w których AI powinna być wdrażana priorytetowo*. Uważamy równocześnie, że postulowana w strategii potrzeba zapewnienia spójności i koordynacji na szczeblu rządowym nie może oznaczać sprzeczności z nadrzędną wartością wolności gospodarczej. Chodzi więc o zapewnienie właściwych warunków i zasobów (w tym kapitału i wiedzy) pozwalającym na wykorzystanie innowacyjnego potencjału AI+ i podjęcia ryzyka innowacji przez podmioty świadomie zabiegające o zwiększanie przewagi konkurencyjnej dzięki technologii.
		Strategia zakłada, że nowa polityka zostanie przygotowana w oparciu o cztery filary: innowacje, inwestycje, edukację oraz wdrożenia. Wobec braku precyzyjnej definicji tych filarów w strategii pragniemy zwrócić uwagę, że kluczowymi zagadnieniami dla realizacji strategii – zwłaszcza w kontekście wskazanych dalej celów są: • Inkubacja nowych produktów i usług AI+ realizujących wyzwania rozwojowe „*strategicznych obszarów gospodarki*" – a więc również szybkie i skuteczne zdefiniowanie tych wyzwań poprzez projekty R&B łączące naukę, przedsiębiorców i sektorowych liderów adopcji innowacji. • Skalowanie produktów, które osiągną fazę dopasowania do rynku (*market fit*) w oparciu o referencyjne wdrożenia poprzez pomoc w kreowaniu popytu i obecności na rynku globalnym. To wyzwanie dla dyplomacji technologicznej jest dzisiaj słabo wspierane przez państwo.
149	Cel 1: Rozwój gospodarki, przemysłu cyfrowego, dobrostanu społecznego i autonomii człowieka jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji	Jednym z postulowanych zadań prowadzących do celu jest „wyłonienie instytucji wiodącej w zakresie badań nad AI oraz koordynacja współpracy instytucji badawczych zajmujących się badaniami w zakresie sztucznej inteligencji wchodzących w skład ekosystemu podmiotów zajmujących się tą tematyką". Zdaniem Izby założenie o centralizacji tego procesu (jedna instytucja) jest nierealistyczne wobec szerokiego zakresu celu, obejmującego tak zróżnicowane obszary, o dużej wewnętrznej różnorodności problemów, wyzwań i możliwych interwencji. O ile implementacja całej strategii powinna być koordynowana przez strukturę reprezentującą wielu interesariuszy to działania prowadzące do celu nr 1 muszą być w pragmatyczny sposób zdecentralizowane i zorganizowane.

		Zdaniem Izby właściwą drogą do tego celu jest (1) powołanie programów transformacji dla obszarów o najwyższym priorytecie – np. w gospodarce mogą to być sektory o wysokim udziale w PKB, eksporcie, rynku pracy, znaczeniu krytycznym i poddane presji modernizacyjnej. Izba pozytywnie ocenia tutaj propozycję studium „SMART" jako wzorzec do tego typu działań. „Operatorami" tych transformacji – po zdefiniowaniu celów i wyzwań – muszą być jednak podmioty posiadające kompetencje i zasoby do realizacji procesów inkubacji i skalowania, które są podstawą osiągania rezultatów o jakie – jak rozumiemy – chodzi w ramach tego celu. Uważamy za mało realne, aby tego typu działania mogła skutecznie pełnić jedna instytucja rządowa.
149	a) Stworzenie zgodnego z przepisami unijnymi oraz przyjaznego dla przedsiębiorczości systemu nadzoru nad modelami i systemami AI, dzięki czemu obywatele, konsumenci i firmy będą miały świadomość oraz pewność, że rozwiązania AI używane na rynku i w administracji publicznej są bezpieczne, zgodne z przepisami i etyką;	W ocenie Izby zaproponowane cele strategii powinny być w pełni spójne z uchwalonymi przez Unię Europejską przepisami rozporządzenia – Aktu o Sztucznej Inteligencji. Biorąc pod uwagę instytucjonalny podział kompetencji pomiędzy Urząd ds. AI (AI Office) oraz właściwe organy krajowe (przedstawiony projekt ustawy przewidujący utworzenie Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji zwracamy uwagę, że sformułowanie powinno odnosić się do systemu nadzoru nad systemami AI. Ponadto istotne jest, żeby prawodawca krajowy nie rozszerzał zakresu obowiązków przewidzianych w unijnym rozporządzeniu, które w sposób wyważony uwzględnia perspektywę zarówno ochrony praw podstawowych w związku z konkretnymi zastosowaniami AI, jak i potrzebą zapewnienia modelu regulacyjnego, który nie hamuje innowacji.
149	f) Stworzenie albo wyłonienie podmiotu odpowiedzialnego za bezpieczeństwo AI na światowym poziomie, którego zadaniem będzie badanie najnowszych zagrożeń związanych z szybkim rozwojem tej technologii, a także wsparcie w nadzorze nad bezpieczeństwem zastosowań AI. Jego działalność będzie wiązała się z jednej strony z bezpiecznym użytkiem i przyszłym rozwojem AI, z drugiej – z cyberbezpieczeństwem rozwiązań AI i zabezpieczeniem przed cyberatakami z wykorzystywaniem tej technologii. Instytucja będzie prowadziła globalną współpracę z innymi instytucjami tego typu;	Zwracamy uwagę na konieczność uspójnienia koncepcji z proponowanym obecnie w projekcie ustawy o systemach sztucznej inteligencji rozwiązaniem dot. utworzenia jednej instytucji odpowiedzialnej za nadzór nad systemami sztucznej inteligencji. O ile Akt o sztucznej inteligencji nie przesądza właściwości tylko jednego organu krajowego w sprawach związanych z AI, struktura instytucjonalna powinna być przejrzysta i jasna zarówno dla przedsiębiorców, jak i innych zainteresowanych podmiotów (obywateli, NGOs, administracji publicznej, organów unijnych, innych państw członkowskich). Jeśli zadaniem podmiotu odpowiedzialnego miałoby być wsparcie w nadzorze nad bezpieczeństwem zastosowań AI, jego rola powinna zostać zdefiniowana w ustawie o systemach sztucznej inteligencji.

151	Cel 2: Realizacja i finansowanie R&D oraz wdrożeń sztucznej inteligencji odbywa się w sposób efektywny i transparentny	Działania zakładają „stworzenie mechanizmu koordynacji obecnych funduszy, konkursów i sposobów ich realizacji, aby uniknąć duplikacji działań i nieefektywnego wydatkowania środków inwestycyjnych wraz z koniecznością centralizowania agendy badawczej, rozwojowej oraz wdrożeniowej". Postulat ten rodzi poważne obawy Izby. W istocie sprawne finansowanie powinno dotyczyć w pierwszej kolejności inkubacji (co może a nawet powinno obejmować pilotażowe wdrożenia innowacji) oraz globalnego skalowania produktów, które przeszły test rynkowy. Procesy te powinny być raczej w pragmatyczny sposób decentralizowane poprzez budowanie portfeli innowacji dla potrzeb określanych w poszczególnych obszarach realizacji celu nr 1. Z tego typu zadaniami dobrze poradzi sobie ekosystem bazujący na doświadczeniach finansowania prywatno-publicznego Krajowego Funduszu Kapitałowego, pod warunkiem dostosowania jego reguł działania do specyfiki projektów AI+. Takie działanie powinno zostać przewidziane w strategii. Efektywność inwestycji nie rodzi się z ograniczeń biurokratycznych, jest pochodną efektywności funduszy inwestycyjnych jakie powinny rozwijać się wokół największego źródła finansowania B+R jakim jest niewątpliwie w Polsce grupa PFR oraz potencjalnie – w zakresie zgodności polskiej i europejskiej polityki rozwoju – Europejski Fundusz Inwestycyjny - EIF). Postulowana w działaniu (b) priorytetyzacja w finansowaniu opracowywania, komercjalizacji i wdrażania innowacji, w tym adaptacji i wykorzystania technologii sztucznej inteligencji przez startupy, administrację publiczną, MŚP i duże przedsiębiorstwa wymaga odpowiedniego zdefiniowania programów i zasad działania funduszy inwestycyjnych wykorzystujących fundusze publiczne tak, aby w budowaniu swoich portfeli uwzględniały w sposób zrównoważony cele jakościowe (rodzaj produktów) oraz finansowe. Należy przy tym podkreślić, że nadmierne ideologizowanie procesów inwestycyjnych (nadmierny nacisk na cele jakościowe niezależnie od ryzyka inwestycyjnego) byłoby skrajnie nieodpowiedzialne biorąc pod uwagę eksperymentalny charakter i niską dojrzałość wielu obszarów rozwiązań AI. Postulat „50% finansowania krajowego dla projektów związanych ze sztuczną inteligencją współfinansowanych z funduszy unijnych" jest niejasny. Co do zasady projekty realizowane w ramach systemu finansowania innowacji mają poziomy dofinansowania od 50% do 80% (w zależności od wielkości firmy). Fundusze dla startupów w ekosystemie PFR mają możliwość udziału kapitału publicznego na poziomie 80%, a w przypadku funduszy Enterprise Venture (EV) należących do spółek skarbu państwa nawet 100%. Wydaje się, że problemem jest raczej struktura inwestycji, brak dobrych instrumentów finansowania operacyjnego dla startupów i niski generalnie apetyt na ryzyko zasobnych funduszy EV spółek s.p.

		Jeżeli chodzi o punkt g) (wdrożenie i upowszechnienie polskiego dużego modelu językowego w modelu open-source, z typem licencji pozwalającej na jego wykorzystanie na rynku oraz dalsze udoskonalanie oraz dobrej jakości zbioru danych językowych dla polskiego rynku), to w ocenie PIIT konieczne jest dalsze uszczegółowienia idei oraz eksperckiej dyskusji nt. modelu finansowania. Dla zastosowań realizowanych w języku polskim takie rozwiązanie wydaje się, że byłoby przydatne. Platformy LLM mają sensowne możliwości monetyzacji w ekosystemach największych globalnych spółek technologicznych, które wiedzę i rozwiązania z takich rozwiązań wykorzystują w szerokim portfelu usług i relacji rynkowych. Same w sobie pozostają rozwiązaniami o ogromnym apetycie na kapitał i finansowanie bieżące zapewniające im trwałość mimo przynoszonych strat (OpenAI, które skonsumowało 15 mld USD inwestycji, zakończyło rok 2023 stratą 0,5 mld USD, przy przychodach ok 4 mld USD). Na tej skali działania Polski z całą pewnością nie stać.
	4.3 Inne technologie przełomowe	
153	Zwiększenie liczby węzłów w systemach przetwarzania brzegowego stało się jednym z celów polityki UE do 2030, dostarczających rynkowi bodźców do optymalizacji sieci przetwarzania danych.	Przetwarzanie brzegowe (edge computing) było obszarem zainteresowania biznesu / branży ICT kilka lat temu. Wydaje się jednak, że nie oferowało nic wystarczająco przełomowego, aby odnieść rynkowy sukces. Co więcej - ze swojej natury przetwarzanie brzegowe będzie mnie optymalne energetycznie niż w scentralizowanych centrach danych, co powoduje istotną sprzeczność z celami efektywności energetycznej. A już z pewnością edge computing przestał być czymś przyszłościowym i przełomowym.
157	Cel 3: Technologie internetu rzeczy są wykorzystywane w kluczowych sektorach gospodarki i w ośrodkach miejskich i wiejskich Co umożliwi realizację celu: a) Opomiarowanie akwenów, w szczególności głównych rzek i jezior celem monitorowania jakości wody, poziomu wód i publiczne udostępnianie tych danych mieszkańcom i obywatelom; b) Rozwój sieci monitorowania poziomu smogu w miastach i miasteczkach w celu diagnozy jakości powietrza. Opomiarowanie głównych szlaków komunikacyjnych w celu monitorowania ruchu i optymalizacji	Podpunkty od a) do d) Samo opomiarowanie nie jest wystarczające, bez platform analizujących dane z czujników to rozwiązanie jest sztuką samą dla siebie (warstwą prezentacyjną). Przykładem jest ostatnia powódź, gdzie dane z czujników i predykcji wykonane przez Polskie Wody oraz IMGW różniły się o 1 metr w wysokości fali.

	transportu; c) Budowa farm demonstracyjnych zawierających najnowsze rozwiązania internetu rzeczy (IoT), na przykład czujniki wilgotności gleby w każdym województwie, celem edukacji i wdrożenia IoT w sektorze rolniczym; d) Zbudowanie 1000 węzłów przetwarzania brzegowego celem efektywnego przetwarzania danych zbieranych z urządzeń IoT;	
157	e) Zbudowanie platformy smart city w modelu open source dostępnej dla mniejszych miasteczek i wsi w celu popularyzacji rozwiązań inteligentnych miast i wsi w mniej skomunikowanych regionach, przy zapewnieniu ochrony prywatności mieszkańców.	Taka platforma została już wykonana ze środków Digital Europe i prywatnych partnerów w 2015 roku (w sumie około 500 mln euro) i jest rozwijana jako Fiware Open Source (fiware.org) i promowane w ramach OASC (Open Agile Smart Cities, w których są również polskie miasta). Jednak platforma ta oprócz wpinania komponentów IoT i wizualizacji wielu źródeł danych nie zapewnia większych zdolności analitycznych niezbędnych jako gotowe narzędzie dla JST. Proponujemy wykorzystanie platformy Fiware stworzonej za pieniądze UE i dedykowanych narzędzi analitycznych z tzw. białej listy wypracowanej w dialogu MC i światowych liderów w tej domenie (rekomendacje lub certyfikacje Ministerstwa Cyfryzacji lub np. NASK).
169	4.6 Open source Cel 1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie.	Należy rozważyć, jak ma to miejsce w innych krajach członkowskich Unii Europejskiej, powołanie ośrodka OSPO (Open Source Program Office) definiującego strategię na poziomie krajowym i promującego stosowanie wolnego i otwartego oprogramowania tak w administracji publicznej, jak i wśród podmiotów gospodarczych. Koordynacją tych działań na poziomie europejskim zajmuje się Open Source Observatory (OSOR) w ramach programu Interoperable Europe. W ramach wdrażania strategii i tworzenia wspólnych przestrzeni danych, Komisja Europejska finansuje powstające w modelu otwartym oprogramowanie pośredniczące (middleware) w ramach platformy SIMPL (Smart middleware platform). Według naszej oceny oprogramowanie to może z powodzeniem zostać wykorzystane w ramach działań Centralnego Ośrodka Informatyki, Centrum e-Zdrowia, czy powstające we współpracy z NASK Krajowego Centrum Przetwarzania Danych. Podobnie warto rozważyć wykorzystanie powszechnie stosowanego protokołu dla przestrzeni danych i innych komponentów budowanych w modelu otwartym przez społeczność skupioną w europejskiej organizacji Eclipse Foundation.

		 *źródło: Komisja Europejska*
171	4.7. Cyfrowa i zielona transformacja	Z zadowoleniem przyjmujemy obecność wątku wpływu rozwoju teleinformatyki i cyfryzacji na klimat i środowisko w konsultowanym dokumencie. Bez wątpienia rozwój technologiczny i postępująca digitalizacja gospodarki przekładają się na podwyższone zapotrzebowanie na transfer danych i efektywność infrastruktury teleinformatycznej, a co za tym idzie – energię. W tym kontekście konsultowany dokument słusznie zwraca uwagę na kwestię efektywności energetycznej. Zaskoczenie budzi jednak brak odniesienia do kluczowej potrzeby – rozwoju niskoemisyjnych i zeroemisyjnych źródeł energii. Działania efektywnościowe, choć istotne, nie rozwiążą problemu negatywnego wpływu teleinformatyki na klimat związanego z emisjami pochodzącymi z energii elektrycznej i paliw potrzebnych do zasilania i zapewnienia ciągłości działania niezbędnych systemów. Aby sprostać temu wyzwaniu, niezbędne jest wspieranie rozwoju odnawialnych źródeł energii, zarówno wielkoskalowych, aby poprawić dostępność mocy OZE na rynku energii i zwiększyć udział nisko- i zeroemisyjnej energii w miksie krajowym, jak też w mniejszej skali, jak chociażby rozwiązania off-grid, zarówno w modelu inwestycyjnym, jak i as a service.

		W zakresie efektywności energetycznej, kluczowa jest gotowość na dialog z uczestnikami rynku teleinformatycznego. Już dziś funkcjonuje wiele dobrych praktyk, które mogą i powinny stać się podstawą do wspólnego wypracowania rekomendacji i w rezultacie standardów, o których w kontekście zapewniania usług teleinformatycznych wspomina projekt „Strategii…". Aby się o tym przekonać, wystarczy przejrzeć raporty pozafinansowe, które publikuje wielu uczestników rynku teleinformatycznego w Polsce. Zasadnym wydaje się sformułowanie platformy dialogu w tym zakresie, łączącej praktyków – przedsiębiorstwa wdrażające praktyki dekarbonizacyjne, ekspertów rządowych, regulatorów. Warto też podkreślić, że wszelkie rekomendacje i wytyczne przyjmowane na szczeblu krajowym powinny być spójne z obowiązującymi regulacjami europejskimi i w maksymalnym stopniu wykorzystywać już istniejące mechanizmy, aby wykorzystać efekt synergii i unikać dublowania procesów. Co szczególnie istotne, podobnie jak w przypadku energii odnawialnej, rozwój efektywności energetycznej w kontekście usług cyfrowych potrzebuje konkretnego wsparcia, również z perspektywy finansowej. Aby osiągnąć zamierzony w „Strategii…" cel niezbędne jest opracowanie modelu finansowania inwestycji dekarbonizujących infrastrukturę teletechniczną. Znaczenie teleinformatyki w transformacji gospodarki, wielokrotnie podkreślane w konsultowanym dokumencie sprawia, że wsparcie dekarbonizacji tego sektora przełoży się na bardziej zrównoważoną transformację Polski.
Tabela 1 – wskaźniki efektywności Strategii		
183	*Komunikacja elektroniczna*	Brakuje wskaźnika dotyczącego stacjonarnych usług dostępu do sieci umożliwiających świadczenie usług 1 Gb/s.
ROZDZIAŁ: FINANSOWANIE		
189	Doprecyzowanie źródeł finansowania	• Postulujemy wprowadzenie bardziej skonkretyzowanego planu finansowego. • W zakresie Funduszu Szerokopasmowego postulujemy precyzyjne wskazanie, że będzie on przeznaczany na cele związane z jego powołaniem tj. dotyczące rynku telekomunikacyjnego, z którego jest finansowany. • Postulujemy rozwinięcie założeń do negocjacji przyszłego budżetu wieloletniego UE ze wskazaniem głównych celów w obszarze cyfrowym. Wskazujemy na ochronę i promocję inwestycji prywatnych, w szczególności ograniczenie skomplikowanych i kosztownych zmian regulacyjnym celem zwiększenia potencjału inwestycyjnego.

189	Przykładowe programy wsparcia	Dla porównania **w innych krajach środki publiczne przeznaczane na technologie przełomowe są znaczące**: • W 2023 r. rząd niemiecki zapowiedział, że publiczne inwestycje w AI zostaną zwiększone dwukrotnie do prawie 1 mld EUR w ciągu najbliższych 2 lat[8]. • W 2021 powstał w Niemczech 10-letni „Fundusz Przyszłości" ("Zukunftsfonds, "Future Fund"), w ramach którego rząd ma przeznaczyć 10 mld EUR, a wraz z partnerami prywatnymi i publicznymi zostanie uruchomione min. 30 mld EUR na finansowanie innowacyjnych startupów związanych z przełomowymi technologiami[9]. Do końca 2023 r zostało już zainwestowane 3,3 mld EUR z tego funduszu[10]. W 2024 r rząd niemiecki zapowiedział zwiększenie tego funduszu o 1,6 mld EUR[11] • Ze środków publicznych finansowany jest w Niemczech również rozwój 6G, np. na projekty R&D z 6G przeznaczono 700 mln EUR ze środków Ministerstwa Nauki i Badań w ramach rządowego "Funduszu Przyszłości"[12] • We Francji w I 2023 rząd zapowiedział uruchomienie finansowania projektów R&D rozwijających technologie i zastosowania 5G, 6G i sieci nowej generacji, że wstępnie planowanym budżetem na kolejne lata w wysokości 750 mln EUR[13] w ramach budżetu France 2030. • Również w Japonii rząd stworzył fundusz w wysokości 450 mln USD na R&D w obszarze 6G w celu przyspieszenia innowacyjności tej technologii[14]. • W Kanadzie rząd planuje finansowanie wprowadzania przez MŚP nowych innowacyjnych zastosowań GenAI i AI w celu zwiększenia produktywności firm w ramach pakietu $2,4 mld inicjatyw związanych z AI: ○ *Deputy Prime Minister and Minister of Finance, on behalf of the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry, announced the*

[8] https://www.reuters.com/technology/germany-plans-double-ai-funding-race-with-china-us-2023-08-23/
[9] https://www.kfw.de/About-KfW/Newsroom/Latest-News/Pressemitteilungen-Details_643072.html
[10] https://startupport.de/en/future-fund-first-evaluation-of-the-package-of-measures-for-start-ups/
[11] ibidem
[12] https://www.gtai.de/en/r-d-640954!marketsContent?channel=red_gtai_germanyinvestmentnews&newsletterId=640962
[13] https://www.telecoms.com/5g-6g/french-government-issues-750-million-call-for-6g-projects
[14] Źródło: IDATE, 2024

		*launch of two programs to grow Canada's AI ecosystem by supporting the development of new generative AI applications and **enabling AI adoption among SMEs to increase productivity**. **These programs are part of a $2.4 billion package of AI-focused initiatives announced in Budget 2024** to accelerate job growth, boost productivity and ensure AI is used responsibly.* ▪ *First, the Regional Artificial Intelligence Initiative (RAII) will invest **$200 million** to help bring new AI technologies to market and help accelerate AI adoption by SMEs and sectors across the country.* ▪ *Second, the AI Assist Program is investing **$100 million** to help innovative Canadian SMEs that are building or actively incorporating generative AI and deep learning solutions into their core products and services.*[15] • Do rozważenia powinno być wprowadzenie **zachęt inwestycyjnych dla firm do inwestowania oraz R&D** w nowe technologie digitalne, a zwłaszcza przełomowe np. poprzez ulgi podatkowe. • W rozdziałach nt. zwiększenia kompetencji wśród uczniów, studentów i nauczycieli w zakresie nowych technologii brakuje informacji nt. **przeznaczenia na to dodatkowych środków z budżetu dla sektora edukacyjnego oraz modelu finansowania**: ○ Do rozważenia finansowanie dostępu przez szkoły/uczelni do szerszej gamy rozwiązań IT (nie tylko darmowego), e-szkoleń (w tym z VR/AR), tworzenia na uczelniach laboratoriów związanych z najnowszymi technologiami, w tym 6G, AI, kwantowymi oraz dostęp do piaskownic technologicznych. ▪ Np. Rząd niemiecki planował w 2023 stworzenie 150 nowych laboratoriów uniwersyteckich dla badań nad AI[16] • Dostęp i finansowanie e-szkoleń z wyspecjalizowanych rozwiązań ICT dla uczniów i studentów jako element poszerzenia oferty edukacyjnej publicznych jednostek oraz zamknięcia luki kompetencyjnej pracowników oświaty.

[15] https://www.canada.ca/en/innovation-science-economic-development/news/2024/10/federal-government-launches-programs-to-help-small-and-medium-sized-enterprises-adopt-and-adapt-artificial-intelligence-solutions.html

[16] https://www.reuters.com/technology/germany-plans-double-ai-funding-race-with-china-us-2023-08-23/