

Uwagi Polskiej Izby Informatyki i Telekomunikacji do projektu Strategii Cyfryzacji Państwa

Lp.	Część Strategii	Obszar Strategii	Cel Strategii	Treść uwagi (w przypadku odnoszenia się do działań zawartych w celach proszę podać literę a), b), c), itd.)
	I Wstęp	Wybierz element.	Wybierz element.	Strategia Cyfryzacji Państwa traktuje suwerenność cyfrową jako kluczowy element rozwoju kraju, podkreślając, że intensywne inwestowanie w cyfryzację oraz zwiększenie poziomu suwerenności cyfrowej nie jest już kwestią wyboru, lecz koniecznością, bez której pozycja Polski wyraźnie osłabnie. Na poziomie Unii Europejskiej wzrasta znaczenie suwerenności cyfrowej i konieczności przenoszenia produkcji kluczowych komponentów stosu technologicznego do Europy, a także zwiększenia niezależności infrastruktury cyfrowej od największych globalnych graczy. Suwerenność technologiczna (cyfrowa) to zdolność państwa lub wspólnoty – jak UE – do autonomicznego kształtowania rozwoju w domenie cyfrowej oraz korzystania z technologii zgodnie z własnymi wartościami i interesami. Nie oznacza izolacjonizmu, lecz polega na swobodzie w wyborze, łączeniu i przechodzeniu między technologiami i rozwiązaniami, które najlepiej odpowiadają potrzebom państw lub wspólnoty oraz zapewnieniu dostępu do szerokiego wachlarza rozwiązań przy jednoczesnej redukcji zależności od zewnętrznych podmiotów i zachowaniu kontroli np. nad miejscem przechowywania danych, ich szyfrowaniem i dostępem do danych. Tak rozumiana suwerenność technologiczna prowadzi do wzmacniania odporności gospodarczej, informacyjnej i militarnej. Suwerenność technologiczna to projekt polityczny, gospodarczy i cywilizacyjny, który powinien być realizowany. Jego celem jest utrzymanie przez Europę i Polskę zdolności do samostanowienia w erze cyfrowej, w oparciu o wspólne wartości, zdolności

				technologiczne i współpracę – nie zaś poprzez protekcjonizm. Stanowi ona fundament nowoczesnej, bezpiecznej i konkurencyjnej gospodarki, otwartej na współpracę z międzynarodowymi partnerami na uczciwych warunkach. Możliwość czerpania najlepszych technologii i świadomego wyboru przez administrację powinno prowadzić do eliminacji klauzul abuzywnych i tych utrudniających zmianę dostawcy technologii, promować interoperacyjność i podejmować dalsze prace zmierzające do zwiększania przenoszalności danych. Wolność wyboru jest jednym z elementów suwerenności w wymiarze technologicznym. Ten wybór będzie stanowił o silnym sektorze publicznym.
	II Wizja	Wybierz element.	Wybierz element.	W ocenie PIIT, choć w części Wizja mówi się o wyzwaniach dotyczących budowania suwerenności cyfrowej, to w zbyt małym stopniu podkreślona została potrzeba wpływania Polski na kształt dyskusji o suwerenności na poziomie europejskim. Ambicją polskiego państwa powinno być zwiększanie wpływu na kształt europejskich polityk i potencjału całego kontynentu. Skupianie się w zbyt dużym stopniu na lokalnej perspektywie i odwoływanie się do sytuacji innych państw głównie przez pryzmat wyścigu o prym lidera w jakiejś dziedzinie, działa na naszą niekorzyść. Istotnym elementem Strategii powinno być nakreślenie ambicji w zakresie kształtowania prawa na poziomie unijnym, gdyż znaczenie na arenie międzynarodowej buduje się nie tylko poprzez konkurencję, ale także przez współpracę. Warto aby diagnoza (analiza SWOT) została uzupełniona o punkt dotyczący wpływu Polski na politykę i prawodawstwo europejskie. Z kolei przy nakreślaniu celów należy wskazać bardziej szczegółowo, jak Polska zamierza walczyć w instytucjach europejskich w ciągu najbliższych 10 lat o kwestie dla nas kluczowe. „Zwiększenie zaangażowania” i „aktywna współpraca”, to sformułowania zdecydowanie zbyt ogólne. Cenne byłoby również wskazanie w poszczególnych obszarach konkretnych celów do osiągnięcia w zakresie polityki europejskiej (np. w zakresie komunikacji elektronicznej powinno to być w naszej ocenie zapewnienie

				środków na rozbudowę i zwiększenie odporności infrastruktury cyfrowej w nowej perspektywie finansowej). Postulujemy zatem ujęcie tego aspektu zarówno w Wizji, jak i w dalszych częściach dokumentu.
	II Wizja			Fundamentem cyfryzacji państwa jest cyfryzacja strategicznych sektorów gospodarki. W tym kontekście, istotne jest uwzględnienie elementu łączności telekomunikacyjnej przy planowaniu projektów publicznych, które mają znaczenie strategiczne dla bezpieczeństwa państwa lub dla podniesienia poziomu ucyfrowienia gospodarki. Postulujemy planowanie rozwoju dedykowanych systemów łączności w konkretnych sektorach gospodarki (takich jak specjalistyczne systemy łączności GSM-R i FRMCS dla transportu kolejowego, budowa dedykowanych sieci łączności dla służb publicznych – <i>Public Protection and Disaster Relief</i>, dla sektora energetyki, zapewnienie łączności w obiektach infrastrukturalnych dual-use, jak tunele, dworce kolejowe i inne budowle służące za schrony, etc). Realizacja znacznej części tych projektów nie leży w gestii Ministerstwa Cyfryzacji, tylko innych instytucji publicznych, a co za tym idzie, konieczna jest współpraca Ministerstwa z tymi instytucjami, w celu optymalnego planowania i zarządzania istniejącymi zasobami. Projekty publiczne mogą być realizowane przy udziale sektora prywatnego, tak by zapewnić państwu kontrolę nad strategicznymi obszarami, jednocześnie unikając niepotrzebnego dublowania infrastruktury telekomunikacyjnej i wykorzystać istniejący na rynku know-how. Doceniamy wskazanie w dokumencie <i>Strategii Cyfryzacji Państwa</i> obszarów, w których współpraca poszczególnych instytucji publicznych jest konieczna do osiągnięcia wyznaczonych celów cyfryzacji. Postulujemy jednak, by dokument <i>Strategia Cyfryzacji Państwa</i> uwzględniał także cele do osiągnięcia na poziomie międzyresortowym, w których Ministerstwo Cyfryzacji występuje w roli

				konsultacyjnej w aspekcie łącznościowym, a inne instytucje odpowiadają za realizację danego projektu. Pozwoliłoby to na spójniejsze zarządzanie rozwojem łączności i odpowiadało na zdiagnozowaną już przez Ministerstwo słabą stronę w analizie SWOT Cyfrowego Państwa – silosowości administracji publicznej.
	II Wizja	Wybierz element.	Wybierz element.	Postulujemy uzupełnienie Wizji o jednoznaczne wskazanie, że celem Strategii jest nie tylko adopcja technologii i rozwoju kluczowych sektorów gospodarki, lecz również wzmacnianie pozycji konkurencyjnej polskich firm technologicznych i eksport usług cyfrowych , wraz z zapowiedzią wyboru priorytetowych specjalizacji.
	III Diagnoza	Wybierz element.	Wybierz element.	Lit g) W tej części strategia wspomina, że „największe globalne firmy technologiczne (...) muszą uczciwie kontrybuować do rozwoju państwa, również w obszarze podatkowym”. Zgadza się z tym stwierdzeniem, przy czym nie odczytujemy go jako sugestii, że przedsiębiorstwa nie płacą zgodnie z prawem, wymaganych od nich podatków. Międzynarodowe firmy technologiczne w sposób znaczący kontrybuują zarówno do budżetu państwa, jak i do rozwoju gospodarki. Sektor gospodarki cyfrowej w Polsce stanowi dziś ok. 10 proc. PKB i daje pracę ok. 1,5 mln osób. W ujęciu podatku jako procentu przychodu, wpływy CIT z działalności firm technologicznych są porównywalne do przedsiębiorstw z innych branż. Co więcej, tworząc miejsca pracy dla wysoko wykwalifikowanej kadry inżynierskiej kontrybuują do gospodarki wysokimi wynagrodzeniami, które przekładają się na konsumpcję, jak i świadczeniami, które zasilają budżet ZUS. Wiele międzynarodowych firm technologicznych ma swoje oddziały w Polsce, które współpracują z szeroką gamą lokalnych dostawców, tworząc dodatkową wartość poprzez swoje łańcuchy dostaw. Oprócz bezpośredniego wpływu na gospodarkę, obecność międzynarodowych firm technologicznych w Polsce, poprzez liczne i często bezpłatne szkolenia oraz współpracę z wiodącymi polskimi uczelniami,

				przyczynia się do rozwoju umiejętności cyfrowych zarówno w społeczeństwie, jak i wśród polskich przedsiębiorstw. Należy również wspomnieć, że wiele polskich przedsiębiorstw aktywnie korzysta z usług oferowanych przez międzynarodowe firmy technologiczne. Począwszy od powszechnie znanych usług, np. pakiety biurowe, poczta e-mail czy komunikatory i mapy, po bardziej zaawansowane narzędzia. Dla wielu małych i średnich przedsiębiorstw, kluczowym w dotarciu do klient jest reklama online. Według badania European Public Policy Partnership, 40 proc. ankietowanych w Polsce przedsiębiorstw uważa, że reklama online pozwala im konkurować z większymi i bardziej rozpoznawalnymi markami.
	IV Wyzwania i trendy	Wybierz element.	Wybierz element.	W Strategii trafnie zidentyfikowano wyzwania związane z dominacją globalnych platform cyfrowych, jednak nie przypisano im konkretnych działań ani mierników. Wnosimy o doprecyzowanie, w jaki sposób państwo zamierza realizować zasadę równego pola gry oraz wspierać konkurencyjność krajowych podmiotów.
	V Analiza SWOT	Wybierz element.	Wybierz element.	Analiza SWOT w ograniczonym stopniu uwzględnia dorobek i potencjał polskiego sektora prywatnego, w szczególności w obszarach takich jak e-commerce, bankowość cyfrowa, płatności elektroniczne czy usługi software'owe. Postulujemy uzupełnienie analizy o te elementy oraz o ryzyko konkurowania administracji publicznej z rynkiem.
	V Analiza SWOT	1.1 Komunikacja elektroniczna	Wybierz element.	Uwagi PIIT dotyczące analizy SWOT w zakresie komponentu „Infrastruktura techniczna” (poprzednio: „Infrastruktura”) zostały uwzględnione tylko częściowo. Podtrzymujemy potrzebę wprowadzenia następujących modyfikacji: Projekt wciąż wskazuje na trend rozdzielania infrastruktury od usług jako szansa dla rynku (już nie w tabeli, ale wciąż we wstępie), mimo postulatu PIIT usunięcia traktowania go jako trwałego motoru rozwoju. Proponujemy zmianę zdania we wstępie „Szansą na zwiększenie środków na inwestycje oraz na poszerzenie pola działalności operatorów telekomunikacyjnych (od lat

				zwracających uwagę na malejące przychody) jest trend oddzielania infrastruktury od usług (w Polsce widoczny zarówno w sieciach ruchomych jak i stacjonarnych)" na „Silną stroną polskiego rynku telekomunikacyjnego jest jego elastyczność, uwidoczniła m.in. przez trend oddzielania infrastruktury od usług (w Polsce widoczny zarówno w sieciach ruchomych jak i stacjonarnych), który umożliwił części operatorów telekomunikacyjnych zwiększenie środków na inwestycje, a tym samym poszerzenie pola działalności.", co jest spójne z obecnym kształtem tabeli SWOT. • Silne strony: ○ Nie dodano do „Silnych stron” rynku cech sugerowanych przez PIIT: wysokiego udziału hurtowego dostępu, dojrzałości modeli hurtowych. ○ 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. • Szanse: ○ W projekcie wskazano jako szansę zwiększoną dostępność do usług satelitarnych o coraz lepszych parametrach jakościowych (co jest faktem), jednak Strategia w żadnym miejscu nie wskazuje na zagrożenia związane z silną koncentracją na rynku usług satelitarnych, co może okazać się bardzo istotnym zjawiskiem w świetle rozwoju technologii mobilnych-satelitarnych (D2D). ○ Brakuje pozycji: ▪ Efektywna gospodarka widmem radiowym (ważne np. w kontekście dyskusji o górnej części pasma 6 GHz czy bliższego współdziałania państw członkowskich przy rozwiązywaniu problemów zakłóceń ze strony państw trzecich).
--	--	--	--	--

				▪ Wprowadzenie mechanizmów wsparcia odporności infrastruktury i usług. • Zagrożenia: ○ Nie wskazano na obciążenia regulacyjne sektora (koszty regulacji i brak harmonizacji UE). ○ Nie jest jasne, co autorzy mieli na myśli pisząc o „nierównomiernym dostępie do infrastruktury”. Jeśli stwierdzenie to odnosi się do różnic w podejściu różnych JST i innych podmiotów publicznych na terenie kraju do udostępniania swojej infrastruktury technicznej, to należy to uściślić. W przeciwnym wypadku PIIT postuluje wykreślenie tej pozycji. ○ Nowy projekt nadal ujmuje „propozycję paneuropejskiej konsolidacji” jako zagrożenie, wbrew postulatowi neutralności i case-by-case kontroli organów konkurencji. PIIT podtrzymuje przy tym, że zagrożeniem dla rynku jest niewystarczająca skala prowadzonej działalności. ○ Brakuje pozycji: ▪ Słabe przygotowanie polskich firm, zwłaszcza MŚP, do funkcjonowania w Przemysle 4.0. Brak innowacyjności może spowodować, że Polska stanie się rynkiem zbytu dla zagranicznych technologii. ▪ Starzenie się populacji zwiększające barierę popytową. ▪ Brak mechanizmów pozwalających na obniżenie kosztów utrzymania sieci na terenach wykluczonych. ▪ Nie uwzględniono interesów narodowych związanych z utrzymaniem pasma dla naziemnej telewizji i radiofonii. Operatorzy sieci komórkowych (MNO) stoją na stanowisku, że po 2030 roku dalsze utrzymywanie obecnego sposobu
--	--	--	--	--

				wykorzystywania pasma poniżej 700 MHz (tj. zakres 600 MHz i poniżej) nie będzie adekwatne w świetle ewolucji preferencji obywateli co do sposobu pozyskiwania informacji. Pasma zasięgowe będą kluczowe dla zapewnienia odpowiedniej jakości usług świadczonych przy wykorzystaniu ruchomych sieci telekomunikacyjnych na obszarach nieurbanizowanych, co jest istotne także z punktu widzenia bezpieczeństwa. W związku z tym stanowisko Polski w ramach dyskusji o przyszłości pasma wykorzystywanego obecnie przez naziemną telewizję powinno być elastyczne i dostosowane do zmieniających się tendencji technologicznych. ▪ Natomiast zdanie odrębne w tej kwestii przedstawia Emitel, który uważa, że Strategia pomija znaczenie pasma UHF wykorzystywanego przez naziemną telewizję cyfrową oraz pasm przeznaczonych dla radiofonii (FM/DAB+). Brak jednoznacznej identyfikacji tych zakresów jako zasobów o strategicznym znaczeniu z punktu widzenia bezpieczeństwa informacyjnego, odporności państwa oraz pluralizmu mediów stanowi ryzyko. W sytuacji trwających na poziomie UE dyskusji o przyszłym wykorzystaniu pasma UHF i pojawiających się koncepcji jego redystrybucji na potrzeby komunikacji mobilnej lub satelitarnej, brak odniesienia do interesów narodowych w tym obszarze może prowadzić do ich marginalizacji w polityce widmowej.
	VI Cele i czynniki	Wybierz element.	Wybierz element.	Strategia wskazuje cele horyzontalne, jednak nie rozdziela w sposób jednoznaczny celów i działań kierowanych do administracji publicznej od tych adresowanych do

	umożliwiające ich realizację			sektora prywatnego. Postulujemy wyraźne rozdzielenie tych dwóch logik (państwo – rynek), w tym osobne nazwanie celów, narzędzi interwencji i odpowiedzialności instytucjonalnej.
	VI Cele i czynniki umożliwiające ich realizację	Wybierz element.	Wybierz element.	Cele strategiczne zostały sformułowane wyłącznie na rok 2035. Brakuje celów pośrednich oraz mapy drogowej (roadmapy) umożliwiającej monitorowanie postępów i korektę działań w trakcie realizacji Strategii. Wnosimy o uzupełnienie dokumentu o kamienie milowe i etapy realizacji.
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Wybierz element.	W zakresie opisu obszaru horyzontalnego – komunikacji elektronicznej rola sektora wciąż jest niedoceniana. Infrastruktura telekomunikacyjna oraz działalność operatorów mają fundamentalne znaczenie dla bezpieczeństwa państwa. Przedsiębiorcy realizują szereg obowiązków, które potwierdzają ich kluczową rolę (planowanie działania na wypadek szczególnych zagrożeń, nieodpłatne udostępnianie urządzeń telekomunikacyjnych na potrzeby akcji ratowniczych, realizacja zadań związanych z ochroną infrastruktury krytycznej, wysyłanie Alertów RCB, blokowanie domen uznawanych za szkodliwe, przeciwdziałanie nadużyciom w komunikacji elektronicznej, gotowość do działań w stanach nadzwyczajnych). Także skupianie się wyłącznie na łączności satelitarnej jako zasobie podwójnego zastosowania wypacza obraz i nieuzasadnione zawęża perspektywę. Infrastruktura zlokalizowana na terytorium Polski jest nie tylko strategicznym zasobem, ale także elementem podlegającym ścisłej kontroli i ochronie, co czyni ją bardziej pewną i dostępną niż zasoby satelitarne. Dodatkowo należy podkreślić, że naziemna infrastruktura radiofoniczna i telewizyjna – utrzymywana i rozwijana przez operatorów krajowych stanowi kluczowy komponent krajowej infrastruktury krytycznej, zapewniający odporne, powszechne i niezależne od zagranicznych podmiotów kanały dystrybucji informacji. W przeciwieństwie do łączności satelitarnej, infrastruktura naziemna: 1) jest w całości zlokalizowana i kontrolowana na terytorium Polski,

				2) funkcjonuje niezależnie od czynników geopolitycznych, 3) umożliwia natychmiastowe dotarcie do całego społeczeństwa w sytuacjach kryzysowych (komunikaty bezpieczeństwa, ostrzeganie publiczne), 4) charakteryzuje się wysoką odpornością fizyczną i redundancją, 5) stanowi fundament pluralizmu i bezpieczeństwa informacyjnego państwa. Z tych względów Strategia powinna wyraźnie wskazywać naziemną radiofoniczno-telewizyjną infrastrukturę nadawczą jako strategiczny zasób państwa, równorzędny wobec innych technologii łączności, oraz przewidzieć działania wzmacniające jej odporność, modernizację i stabilność regulacyjną.
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Cel 1	W odniesieniu do zasięgu sieci mobilnych w Strategii stwierdzono: „W przypadku wdrażania technologii 5G za sprawą przeprowadzonego w 2023 roku postępowania aukcyjnego na częstotliwości pasma 3,6 GHz nastąpiła znacząca poprawa i obecnie (2025 r.), według danych UKE, ponad 90% gospodarstw domowych w Polsce znajduje się w zasięgu sieci 5G”. W ocenie PIIT to zdanie zawiera daleko idące uproszczenia i może wprowadzać odbiorców w błąd. Aukcja z 2023 r. oczywiście była kluczowa dla wdrażania technologii 5G w Polsce, ale poprawa zasięgu sieci 5G nie wynikała z procesu selekcyjnego, lecz z inwestycji, które poczynili operatorzy. Co więcej, pasmo 3,6 GHz nie jest pasmem zasięgowym, jak np. pasmo 700 MHz rozdyskrebowane dopiero w 2025 r. Bliższe prawdy byłoby stwierdzenie, że do 90% pokrycia sieciami 5G w Polsce doszliśmy tak późno, gdyż pasma pionierskie 5G nie były w Polsce dostępne znacznie dłużej niż w innych państwach członkowskich UE. W związku z tym postulujemy nadanie temu zdaniu brzmienia: „Za sprawą inwestycji operatorów mobilnych, którzy na skutek przeprowadzonych w latach 2023 i 2025 roku aukcji uzyskali możliwość korzystania z pasm pionierskich dla technologii 5G (3,6 GHz i 700 MHz), nastąpiła znacząca poprawa zasięgu usług w

				tej technologii. Obecnie (2025 r.), według danych UKE, ponad 90% gospodarstw domowych w Polsce znajduje się w zasięgu sieci 5G”. Dodatkowo zwracamy uwagę, że rozwój sieci mobilnych – choć kluczowy – nie może być analizowany w oderwaniu od infrastruktury naziemnej radiofonii i telewizji, infrastruktury radionawigacyjnej oraz infrastruktury radiolokacyjnej która również pełni funkcję krytycznego kanału komunikacji z obywatelami i istotną rolę w bezpieczeństwie Państwa. Wysoki zasięg technologii 5G nie zastępuje potrzeby utrzymania i modernizacji ogólnokrajowej infrastruktury nadawczej, wykorzystywanej m.in. do rozpowszechniania komunikatów bezpieczeństwa oraz zapewniania powszechnego dostępu do informacji. W związku z tym postulujemy, aby w Celach i działaniach towarzyszących rozwojowi sieci mobilnych równolegle uwzględnić potrzebę wzmacniania infrastruktury naziemnej, w tym jej odporności, redundantnych ścieżek transmisji i stabilności regulacyjnej, co ma bezpośrednie znaczenie dla interesu publicznego oraz bezpieczeństwa państwa.
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Cel 1	Autorzy projektu Strategii zauważają, że: „<i>Konieczne jest (...) sformułowanie odpowiedzi na problem spadającej (w ujęciu realnym) wartości rynku, przekładający się na ograniczenie zdolności inwestycyjnych przedsiębiorstw telekomunikacyjnych.</i>” Niestety projekt nie proponuje takiej odpowiedzi. Z pewnością nie jest nią uchwalenie nowelizacji Megaustawy, która może mieć istotne znaczenie dla likwidowania barier w szeroko pojętym procesie budowlanym, ale nie wpłynie na zwiększenie opłacalności samego prowadzenia działalności telekomunikacyjnej. Ta może wzrosnąć dzięki obniżaniu kosztów świadczenia usług (na co państwo ma wpływ poprzez obniżanie obciążeń fiskalnych). W związku z tym wnosimy o określenie dodatkowego celu pośredniego (1.1.5.) albo rozszerzenie celu 1.1.1. o następujące działania:

				1) na poziomie europejskim aktywne zabieganie o pełną harmonizację ram regulacyjnych dla sektora i zasad ochrony konsumenta na całym rynku cyfrowym (w ramach prac nad DNA czy innymi aktami). 2) uruchomienie mechanizmu umowy inwestycyjnej i skierowanie środków z Funduszu Szerokopasmowego na realną działalność inwestycyjną (o tym więcej w kolejnym punkcie). 3) obniżenie albo co najmniej zamrożenie opłat związanych z prowadzeniem działalności telekomunikacyjnej (opłaty za numerację, roczne opłaty za częstotliwości, opłaty za wydanie pozwolenia radiowego). 4) wycofywanie opłaty telekomunikacyjnej w związku ze zmianą zakresu wyzwań związanych z regulacją rynków cyfrowych i sytuacją regulacyjną przedsiębiorców komunikacji elektronicznej. 5) promowanie długich okresów rezerwacji częstotliwości i korzystanie z mechanizmu przedłużania rezerwacji 15-letnich. 6) ograniczenie i uspoźnienie obowiązków przedsiębiorców telekomunikacyjnych w zakresie raportowania (dodatkowo lepsze wykorzystywanie danych, którymi dysponuje administracja). 7) uwzględnienie w polityce inwestycyjnej i regulacyjnej państwa konieczności utrzymania i modernizacji infrastruktury naziemnej radiofonii i telewizji, będącej elementem krajowej infrastruktury krytycznej. W kontekście problemu spadającej wartości rynku telekomunikacyjnego oraz ograniczonych możliwości inwestycyjnych przedsiębiorstw, szczególnego znaczenia nabiera stabilność i przewidywalność regulacyjna dotycząca operatorów świadczących usługi rozpowszechniania programów radiowych i telewizyjnych. Niezbędne jest zapewnienie, aby mechanizmy inwestycyjne – takie jak umowa inwestycyjna czy środki Funduszu Szerokopasmowego – mogły obejmować nie
--	--	--	--	--

				tylko inwestycje w łączność mobilną i szerokopasmową, ale również projekty wzmacniające odporność i niezawodność infrastruktury nadawczej , która pełni kluczową rolę w systemie komunikacji kryzysowej, bezpieczeństwa informacyjnego oraz powszechnego dostępu do treści publicznych.
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Cel 1	W ocenie PIIT wciąż aktualny pozostaje postulat zapewnienia dedykowanego finansowania inwestycji zwiększających odporność sieci telekomunikacyjnych - przede wszystkim zaś sieci mobilnych. W obliczu zagrożeń wynikających ze zmian klimatu (gwałtowne zjawiska pogodowe) i niepewnej sytuacji geopolitycznej (wojna w Ukrainie) zwiększenie gwarancji niezawodności sieci telekomunikacyjnych powinno być priorytetem państwa. O niezbędności i pilności problemu świadczą ostatnie ataki hybrydowe na infrastrukturę krytyczną w Polsce. Starania państwa nie powinny skupiać się wyłącznie na poprawie bezpieczeństwa tej infrastruktury, która należy do podmiotów kontrolowanych przez państwo – np. kolei. To, że większość rynku telekomunikacyjnego należy do prywatnych właścicieli z pewnością nie jest okolicznością, która czyni z infrastruktury telekomunikacyjnej dobro o mniej krytycznym znaczeniu. W interesie państwa jest zapewnienie jak najlepszych warunków do wzmacniania jej odporności. Choć operatorzy dbają o jakość swojej sieci w granicach swoich możliwości finansowych, to potrzeby przekraczają dostępne środki. Biorąc pod uwagę skalę obciążeń fiskalnych nałożonych na przedsiębiorców, które wzrastają w związku z podwyżkami licznych opłat przewidzianych w PKE, w pełni zasadne jest zapewnienie, że pobierane z tego tytułu środki wrócą na rynek w celu wsparcia niezbędnych inwestycji. W tym kontekście PIIT wnosi o: wskazanie wprost na potrzebę uruchomienia przewidzianego już w przepisach PKE mechanizmu umowy inwestycyjnej, także w odniesieniu do inwestycji

				odpornościowych (nie tylko czysto zasięgowych) oraz rozszerzenia zakresu działań finansowanych z Funduszu Szerokopasmowego o inwestycje odpornościowe; wprowadzenie kluczowego wskaźnika realizacji tego celu poprzez wskazanie roku, od którego oba instrumenty zaczną być faktycznie stosowane w celu poprawy odporności sieci (w ocenie PIIT powinno to nastąpić nie później niż w 2027 r.).
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Cel 3	Postulujemy rozszerzenie działań przewidzianych w celu 1.1.3. o takie, które odnoszą się do zwiększenia popytu na usługi szybkiego internetu: łączenie informacji na temat nowych funkcji mObywatela czy innych elektronicznych usług publicznych z informacjami o rozwoju sieci światłowodowych (w szczególności: lokalne akcje informacyjne we współpracy z JST, na terenie których funkcjonują sieci budowane z wykorzystaniem środków publicznych); rozszerzenie aktualnego modelu ulgi PIT na internet, w sposób promujący wykorzystanie sieci najwyższych przepływności, także dla osób, które korzystały z tej ulgi w przeszłości.
	VI Cele i czynniki umożliwiające ich realizację	1.1 Komunikacja elektroniczna	Cel 4	Zgodnie z lit. c na realizację celu 1.1.4. mają wpłynąć: <i>„Nowe inwestycje i innowacje dla rozwoju i rozbudowy krajowego potencjału w zakresie szybkiej telekomunikacji, opartej na satelitach i naziemnej infrastrukturze, w szczególności sieciach komórkowych nowych generacji (5G/6G) dla świadczenia przez operatorów efektywnych kosztowo, wysokiej jakości telekomunikacyjnych usług szerokopasmowych”</i>. W ocenie PIIT z przytoczonego fragmentu można wyczytać, że celem Ministerstwa Cyfryzacji jest m.in. finansowe wsparcie inwestycji w zakresie sieci 5G. W związku z tym podkreślamy znaczenie umowy inwestycyjnej jako jednego z narzędzi, które mogą zwiększyć krajowy potencjał.

				Ponadto wnosimy o dodanie punktu dotyczącego podejmowania działań zmierzających do zadbania o istnienie skutecznej konkurencji na rynku usług satelitarnych. Z punktu widzenia Polski i Europy kluczowym celem jest uniknięcie stworzenia nowych obszarów zależności od dostawców z państw trzecich. Istotne znaczenie ma więc z jednej strony budowanie lokalnych alternatyw (biorąc pod uwagę skalę przedsięwzięcia – przede wszystkim na poziomie europejskim), a także monitorowanie sytuacji rynkowej pod kątem nadmiernej koncentracji na rynku szybkiej transmisji satelitarnej. Dodatkowo postulujemy, aby działania podejmowane w ramach celu 1.1.4. uwzględniały także wzmocnienie i modernizację krajowej infrastruktury naziemnej radiofonii i telewizji, która – obok sieci mobilnych – stanowi fundament krajowego potencjału w zakresie odpornej i niezależnej komunikacji elektronicznej. Infrastruktura ta, utrzymywana przez wyspecjalizowanych operatorów takich jak Emitel, pełni kluczową rolę w zapewnianiu powszechnego dostępu do informacji, w tym w kontekście bezpieczeństwa państwa, komunikacji kryzysowej i ciągłości działania instytucji publicznych. W związku z tym uważamy za zasadne, aby mechanizmy wsparcia inwestycyjnego obejmowały także projekty modernizacyjne i odpornościowe dotyczące sieci nadawczych, co pozwoli na zrównoważony rozwój wszystkich elementów infrastruktury o strategicznym znaczeniu.
	VI Cele i czynniki umożliwiające ich realizację	1.3 Cyberbezpieczeństwo	Wybierz element.	Z uwagi na trwające prace nad nową Strategią Cyberbezpieczeństwa RP na lata 2025-2029 sugerujemy, aby cele przewidziane w Strategii Cyfryzacji zostały określone w sposób spójny ze strategią specjalistyczną, czyli Strategią Cyberbezpieczeństwa. Tymczasem już na gruncie celów ogólnych Strategia Cyfryzacji wymienia:

				Cel 1.3.1: Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny Cel 1.3.2: Cyberprzestępczość jest skutecznie zwalczana Cel 1.3.3: Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności Cel 1.3.4: Krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiada rozwinięty potencjał i cechuje się wysokim stopniem suwerenności technologicznej Cel 1.3.5: Kadry podmiotów krajowego systemu cyberbezpieczeństwa oraz społeczeństwo posiadają świadomość cyberzagrożeń oraz wiedzę i kompetencje w zakresie cyberbezpieczeństwa Cel 1.3.6: Polska posiada silną pozycję międzynarodową w obszarze cyberbezpieczeństwa Strategia Cyberbezpieczeństwa (projekt) posługuje się zaś niemal identycznie, ale jednak inaczej zdefiniowanymi celami: Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa. Cel szczegółowy 2. Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni. Cel szczegółowy 3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej. Cel szczegółowy 4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa. Cel szczegółowy 5. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców.
--	--	--	--	--

				Cel szczegółowy 6. Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa. Same działania definiowane w ramach tych celów są już jednak inne na poziomie projektów Strategii Cyfryzacji i Strategii Cyberbezpieczeństwa. Np. dla pierwszego celu w jednej strategii zdefiniowano 6 działań, a w drugiej 5. W drugim celu jedna strategia przewiduje 4 działania, druga 6. Z perspektywy spójności i przejrzystości ww. strategii zasadnym jest, aby posługiwały się identycznym zestawem generalnych celów i działań, przy czym to Strategia Cyberbezpieczeństwa powinna określać szczegółowy sposób ich realizacji. Zastrzegamy przy tym, że nie jest jeszcze powszechnie znany końcowy tekst Strategii Cyberbezpieczeństwa więc być może zostało to już zmodyfikowane, a tym samym niniejsza uwaga będzie nieaktualna.
	VI Cele i czynniki umożliwiające ich realizację	1.3 Cyberbezpieczeństwo	Cel 4	Strategia uznaje, że celem jest, aby krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiadała rozwinięty potencjał i cechowała się wysokim stopniem suwerenności technologicznej. Wzmocnienie suwerenności technologicznej ma nastąpić poprzez realizację działań prowadzących do stworzenia polskich rozwiązań cyberbezpieczeństwa (sprzętowych i programowych), co pozwoli na budowę krajowych kompetencji technologicznych i przemysłowych. Planuje się również rozwijanie krajowych rozwiązań i standardów kryptologicznych (w tym w zakresie kryptografii kwantowej i postkwantowej) w celu zapewnienia, aby Polska dysponuje suwerennym potencjałem kryptologicznym. Zgadza się, że elementem suwerenności jest zwiększenie lokalnych kompetencji i technologii. Jednak apelujemy, aby nie traktować suwerenności niewykluczająco.

				Wąsko pojmowana polityka suwerenność cyfrowa stawiająca na protekcyjizm z natury rzeczy generuje znaczne koszty ekonomiczne i paradoksalnie może osłabiać, a nie wzmacniać bezpieczeństwo, odporność i zdolność kraju do innowacji. Szybkie tempo rozwoju sztucznej inteligencji oraz zmieniający się globalny krajobraz cyberbezpieczeństwa tylko potwierdzają niezawodność współpracy w celu utrzymania przewagi technologicznej i zapewnienia długoterminowej odporności. Współpraca z partnerami na poziomie UE czy NATO jest niezbędna, aby Polska mogła sprostać wyzwaniom ze strony Rosji, Chin i ich strefy wpływów. W zakresie rozwijania krajowych rozwiązań i standardów kryptologicznych, apelujemy o udział polskiej administracji w międzynarodowych pracach standaryzacyjnych, tak aby polskie rozwiązania były zgodnie z najlepszymi praktykami międzynarodowymi. W ostatnim okresie aktywność legislacyjną w tym zakresie zapowiedziała Komisja Europejska. Warto ukierunkować polskie aktywności na tę inicjatywę. Skupienie się na polskich rozwiązaniach, może doprowadzić do sytuacji niezgodności podejść, co może skutkować zmniejszeniem bezpieczeństwa oraz zwiększeniem barier regulacyjnych.
	VI Cele i czynniki umożliwiające ich realizację	1.4 Koordynacja cyfrowej transformacji kraju	Cel 2	W ramach koordynacji transformacji cyfrowej planuje się przygotowanie rozwiązań, które będą wspierać uwzględnianie wymogów suwerenności i bezpieczeństwa w postępowaniach zakupowych na rozwiązania ICT w administracji publicznej, a także promować polskich dostawców i dostawców z państw UE. Zwracamy uwagę na potencjalną niezgodność takich zapisów z prawem UE oraz jego dyskryminacyjny charakter. Sugerujemy, aby inspirację czerpać z Cloud Sovereignty Framework, które w październiku opublikowała Komisja Europejska. Takie podejście może zagwarantować bezpieczeństwo, które można zdefiniować przez bardzo konkretne wskaźniki.
	VI Cele i czynniki	2.4 Cyfrowa tożsamość	Wybierz element.	W przedstawionym rozdziale wskazano dążenie do budowy Europejskiego Portfela Tożsamości Cyfrowej, które ma zapewnić możliwość składania kwalifikowanego

	umożliwiające ich realizację			podpisu elektronicznego dostępnego za darmo co najmniej do użytku nieprofesjonalnego. W uzupełnieniu znajdziemy także informację, że <i>ułatwienie składania zdalnych kwalifikowanych podpisów elektronicznych we wszystkich krajowych usługach publicznych jest ważne także z tego powodu, że kwalifikowane podpisy elektroniczne, w odróżnieniu od podpisu zaufanego i podpisu osobistego – nie mają ograniczeń formalnoprawnych w ich zastosowaniu i są ważne zarówno z usługach publicznych jak prywatnych w całej Unii Europejskiej</i> Wskazując przy tym cel określony w pkt 2.4.2, gdzie czytamy: <i>Obywatel będzie mógł używać wszystkich trzech rodzajów podpisów elektronicznych w usługach publicznych (kwalifikowany podpis elektroniczny, podpis osobisty, podpis zaufany,</i> nasuwa się pytanie, po co Skarb Państwa ma utrzymywać 3 równoległe rozwiązania podpisu elektronicznego w Polsce. Warto nadmienić, że wskazana „kompleksowa inwentaryzacja istniejących mechanizmów” pozwoli na pokazanie realnej mnogości sektorowych takich „narzędzi podpisowych” w Polsce. Obywatel nie powinien w ogóle zastanawiać się jaki rodzaj podpisu elektronicznego wybierze, ponieważ mechanizmy podpisu powinny być zaszyte w procesach udostępnianych obywatelowi. Wraz z obligatoryjnym wprowadzeniem Europejskiego Portfela Tożsamości Cyfrowej z możliwością składania kwalifikowanego podpisu elektronicznego należy rozważyć docelowe wycofanie się Państwa z wykorzystywania innych rodzajów podpisów elektronicznych które posiadają ograniczenia formalnoprawne. Bardzo ważnym zagadnieniem poruszonym w tym samym punkcie jest weryfikacja (walidacja) złożonych podpisów. Tu warto podkreślić, że obecnie tylko kwalifikowany podpis elektroniczny jest automatycznie weryfikowany na zgodność z wymaganiami eIDAS w kwalifikowanych usługach walidacji. Dodatkowo warto także podkreślić, że wyłącznie w przypadku kwalifikowanego podpisu elektronicznego można automatycznie w usłudze walidacji potwierdzić poprawność oraz status prawny
--	------------------------------	--	--	--

				weryfikowanego (akceptowanego) podpisu. Kwalifikowany podpis, jak i kwalifikowana usługa walidacji są realizowane w ramach ekosystemu usług zaufania UE zbudowanego zgodnie z wymaganiami eIDAS jednolicie obowiązującymi w państwach członkowskich. Każdy inny rodzaj podpisu nie jest tak uniwersalnym instrumentem, gdyż swój status i skutek prawny wywodzi albo z przepisów lokalnych, albo z deklaracji dostawcy rozwiązania lub stron transakcji. Dlatego realizacja idei powszechnego obrotu elektronicznego na jednolitym europejskim rynku cyfrowym wymaga odchodzenia od rozwiązań niestandardowych o zasięgu lokalnym, czy wręcz resortowym. Połączenie bezpieczeństwa kwalifikowanej usługi składania podpisu z kwalifikowaną usługą jego walidacji daje holistyczne zabezpieczenie przed fraudami dotyczącymi naruszenia integralności dokumentów i niezaprzeczalności procesu składania podpisu. Rosnąca ilość fraudów dotyczących podpisanych dokumentów, stawia usługę walidacji jako kluczową w zapewnieniu holistycznej ochrony cybersec.
	VI Cele i czynniki umożliwiające ich realizację	2.5 Chmura obliczeniowa	Wybierz element.	Z niezrozumieniem przyjmujemy fragment dotyczący „nierównowagi na niekorzyść instytucji sektora publicznego”. Naszym zdaniem nierównowaga bierze się z zapóźnienia technologicznego administracji publicznej, która ciągle nie wdrożyła nowoczesnych narzędzi, takich jak chmura obliczeniowa. Chmura jest podstawą nie tylko dla nowoczesnych i łatwo skalowalnych usług publicznych, ale też i warunkiem koniecznym dla rozwoju sztucznej inteligencji. W odniesieniu do suwerenności danych, chociaż lokalizacja danych może wydawać się prostym rozwiązaniem problemów związanych ze zgodnością i bezpieczeństwem w chmurze obliczeniowej, często jest to błędne podejście. Może stwarzać fałszywe poczucie bezpieczeństwa, a nawet wprowadzać nowe wyzwania. Lekcja z Ukrainy dobitnie pokazała skalę potencjalnych zagrożeń. Zamiast wskazywać na konieczność lokalizacji danych, korzystniej skupić się na:

				1. Kontroli rezydencji danych: - Rzeczywista kontrola nad lokalizacją danych: Współcześni dostawcy chmury oferują zaawansowane mechanizmy kontroli rezydencji danych, umożliwiające klientom precyzyjne określenie, gdzie ich dane są przechowywane, nawet do konkretnego regionu lub strefy dostępności. Zapewnia to zgodność z lokalnymi przepisami i regulacjami bez potrzeby ścisłej lokalizacji danych. 2. Domyślnym szyfrowaniu: - Ochrona danych na wszystkich etapach: Wiodący dostawcy chmury oferują domyślne szyfrowanie danych w spoczynku, w użyciu i w tranzycie. Oznacza to, że dane są chronione niezależnie od ich fizycznej lokalizacji, co sprawia, że argument za lokalizacją danych traci na znaczeniu. - Zaawansowane techniki szyfrowania: Dostawcy chmury inwestują znaczne środki w zaawansowane technologie szyfrowania, często przewyższające możliwości pojedynczych organizacji. Zapewnia to solidną ochronę danych przed nieautoryzowanym dostępem i cyberzagrożeniami. 3. Ograniczeniu polityk bezpieczeństwa: - Szczegółowa kontrola dostępu do danych: Ograniczenia polityki bezpieczeństwa danej organizacji pozwalają administratorom zdefiniować szczegółowe mechanizmy kontroli dostępu i polityki bezpieczeństwa dla swojego środowiska chmurowego. Gwarantuje to, że tylko upoważniony personel ma dostęp do poufnych danych, niezależnie od miejsca ich przechowywania. - Egzekwowanie zgodności: Te zasady można skonfigurować w celu egzekwowania zgodności z określonymi wymogami prawnymi, takimi jak RODO lub HIPAA, co dodatkowo zmniejsza potrzebę lokalizacji danych. 4. Kontroli usług VPC: - Bezpieczny obwód danych: Kontrola usług VPC tworzy bezpieczne środowisko wokół zasobów chmury, zapobiegając eksfiltracji danych i nieautoryzowanemu
--	--	--	--	--

				dostępowi. Stanowi to dodatkową warstwę bezpieczeństwa, niezależnie od lokalizacji danych. • Zarządzanie danymi i kontrola: Kontrola usług VPC umożliwia organizacjom definiowanie jasnych granic dostępu do danych i ich udostępniania, zapewniając zgodność i zmniejszając ryzyko naruszenia danych. Podsumowując: • Lokalizacja danych może być kosztownym i nie efektywnym podejściem do rozwiązywania problemów związanych z zgodnością i bezpieczeństwem. Współcześni dostawcy chmury oferują szereg zabezpieczeń uwzględniających wymogi suwerennościowe, które zapewniają większą elastyczność, skalowalność i bezpieczeństwo bez ograniczeń związanych ze ścisłą lokalizacją danych. • Podobne podejście przyjęła Komisja Europejska opublikowanym w październiku Cloud Sovereignty Framework.
	VI Cele i czynniki umożliwiające ich realizację	2.5 Chmura obliczeniowa	Cel 1	Strategia w celu f) postuluje stworzenie ambasad danych, zlokalizowanych poza granicami kraju jednostek umożliwiających składowanie kluczowych danych i informacji z rejestrów publicznych i teleinformatycznych systemów państwowych oraz zapewnienie ciągłości działania tych rejestrów i systemów w przypadku wystąpienia sytuacji kryzysowych na terytorium RP. Co do zasady zgadzamy się z takim podejściem, wskazujemy jednak na jego kosztowność. Jeżeli Polskę dotknie sytuacja kryzysowa wymagająca transferu danych, to lepszym rozwiązaniem będzie wykorzystanie komercyjnie dostępnej infrastruktury chmury publicznej, nawet kosztem suwerenności, niż utrzymywanie pustych centrów danych. Dodatkowo w celu h) strategia przewiduje przyjęcie rozwiązań legislacyjnych kształtujących warunki korzystnego rozwoju chmury obliczeniowej w Polsce oraz wzmacniających bezpieczeństwa i pewności prawnej w związku z jej wykorzystywaniem. Naszym zdaniem, korzystanie z chmury jest już wystarczająco

				uregulowane. Kolejne regulacje, do tego rzekomo celowane, tylko dodatkowo skomplikują i tak niełatwy krajobraz regulacyjny. Dlatego, rekomendujemy przyjęcie holistycznej polityki „Cloud First”. Niedawna nowelizacja uchwały WIIP jest krokiem w dobrym kierunku, jednak nie uchwała z uwagi na niższą rangę aktu prawnego nie powinna być stanem docelowym. Przyjęcie polityki ‘Cloud First’ na poziomie ustawowym może być ważną dźwignią symulującą adopcję chmury obliczeniowej w sektorze publicznym i potencjalnie innych branżach regulowanych, takich jak opieka zdrowotna i usługi finansowe. Dobre praktyki w zakresie wdrażania chmury istnieją w różnych regionach świata, w tym w Australii (Australijska strategia chmury obliczeniowej z 2014 r.), Wielkiej Brytanii (Polityka „Chmura przede wszystkim” z 2013 r.), Stanach Zjednoczonych (Federalna strategia chmury obliczeniowej z 2011 r.; Strategia „Cloud Smart” z 2018 r.). Skuteczna polityka „Cloud First” zalecałaby, aby usługi chmury publicznej były rozważane w pierwszej kolejności w przypadku infrastruktury IT agencji rządowych i miały pierwszeństwo przed rozwiązaniami wyłącznie lokalnymi i chmurą prywatną – pod warunkiem, że dostawcy usług chmurowych spełniają niezbędne wymogi bezpieczeństwa i międzynarodowe standardy. Poniżej przedstawiamy kluczowe obszary, na których należy się skupić, aby polityka „Chmura przede wszystkim” odniosła sukces: Definiowanie „Cloud First”. Istnieją różne globalne podejścia do definiowania, co „Cloud First” oznacza dla zasad zamówień publicznych w sektorze publicznym. Uważamy, że polityka „Cloud First” powinna wymagać od organizacji publicznych, aby najpierw oceniały chmurę publiczną, zanim rozważą inne rozwiązania przy zakupie usług IT, a także jasno wyjaśniały, jeśli zdecydują się nie korzystać z tej opcji.
--	--	--	--	---

				• Multicloud i chmura hybrydowa. W ramach zamówień publicznych organizacje publiczne byłyby zachęcane do rozważenia strategii multicloud i chmury hybrydowej. • Wymagania dotyczące przenośności. Aby wesprzeć realizację strategii multicloud/lub chmury hybrydowej, rozwiązania obejmujące wymagania migracji i przenoszenia danych muszą zostać uwzględnione w ogólnej ocenie w ramach procesów zamówień publicznych przez organizacje publiczne jako jedno z podstawowych kryteriów. Powyższe może również pomóc w zapewnieniu technicznego rozwiązania chroniącego przed ryzykiem nadmiernej koncentracji (tzw. vendor lock-in). • Rezydencja i klasyfikacja danych. Polityka „Cloud First” musi wyraźnie zabraniać zamawiającym nakładania warunków dotyczących lokalizacji danych w określonej lokalizacji i segmentacji danych, ponieważ postanowienia te byłyby sprzeczne z RODO i rozporządzeniem UE w sprawie swobodnego przepływu danych nieosobowych. Jednak polityka „Cloud First” musi definiować jasne i kompleksowe podejście do klasyfikacji danych, które między innymi mogłoby określić, które typy danych i systemów byłyby uważane za gotowe do migracji do chmury publicznej. • Zrównoważony rozwój środowiska. Zrównoważony rozwój środowiska powinien być traktowany jako obowiązkowe kryterium przez organizacje publiczne wybierające swoich dostawców usług chmurowych. • Zasady prywatności i bezpieczeństwa oraz międzynarodowe standardy. Aby zapewnić agencjom sektora publicznego maksymalną ochronę prywatności i bezpieczeństwa w przypadku outsourcingu do chmury, polityka „Cloud First” może definiować zasady wysokiego poziomu i/lub ramy kontroli oparte na ryzyku, które będą kierować ich procesem wyboru dostawców. Jednym ze sposobów osiągnięcia tego celu byłoby ustalenie minimalnego zestawu
--	--	--	--	---

				uznanych na arenie międzynarodowej standardów, zgodnie z którymi dostawcy muszą posiadać certyfikaty, a także obowiązujących dobrowolnych kodeksów postępowania branżowego. • Współodpowiedzialność. W środowisku chmurowym klienci i dostawcy usług działają w oparciu o model współodpowiedzialności, który musi być podkreślony w polityce „Cloud First”. • Ramy umowne i model zamówień. Polityka „Cloud First” musi zachować elastyczność w odniesieniu do ram umownych, w ramach których organizacje publiczne dokonywałyby zakupów u dostawców. • Walidacja i ocena kosztów. Aby dodatkowo stymulować przyspieszenie wdrażania chmury w sektorze publicznym i zachęcać organizacje publiczne do wprowadzania innowacji i eksperymentowania z rozwiązaniami chmurowymi, polityka „Cloud First” mogłaby pomóc w opracowaniu narzędzi do ustalania i monitorowania celów oszczędności kosztów wynikających z outsourcingu w chmurze, w tym jasnych wskaźników ilustrujących progres osiągany dzięki chmurze. Wskaźniki te nie powinny opierać się wyłącznie na cenie, ale mogłyby obejmować mechanizm oceny oparty na wartości dla potencjalnych rozwiązań outsourcingowych. • Polityka otwartych danych w celu zwiększenia wykorzystania uczenia maszynowego za pośrednictwem chmury. Ponieważ platformy chmurowe ułatwiły dostęp do technologii sztucznej inteligencji (AI) i uczenia maszynowego (ML), umożliwiając firmom i organizacjom sektora publicznego wprowadzanie innowacji w tej dziedzinie, polityka „Cloud First” może stać się ważną dźwignią promującą dostęp do otwartych zbiorów danych rządowych do celów badawczych i szkoleniowych ML poprzez zasady otwartych danych. • Dalsze promowanie wdrażania chmury i podnoszenie kwalifikacji. W ramach wdrażania polityki „Cloud First” organizacje publiczne mogą wyznaczać
--	--	--	--	---

				„Ambasadorów Chmury” w sektorze publicznym, którzy będą pełnić rolę liderów i promować chmurę. Krytyczne znaczenie ma również zaspokojenie potrzeby podnoszenia kwalifikacji pracowników sektora publicznego, których obciążenia pracą zostaną przekształcone za pomocą technologii chmurowych.
	VI Cele i czynniki umożliwiające ich realizację	2.5 Chmura obliczeniowa	Cel 3	Strategia przewiduje, wsparcie dla podmiotów publicznych w nabywaniu, wdrażaniu i wykorzystywaniu systemów i rozwiązań informatycznych w oparciu o usługi chmurowe. Popieramy takie podejście, jednak wskazujemy, że dotychczasowe modele wsparcia były nieefektywne (ZUCH) na co wskazywała np. Najwyższa Izba Kontroli. Warto, aby Strategia wspomniała jak ZUCH miałyby być zreformowane, tak aby 1) uniknąć skomplikowane procedury zakupów usług przez ZUCH, 2) zwiększenia katalogu usług dostępnych w platformie, 3) zwiększenie elastyczności mechanizmów ZUCH tak, aby nadążały za dynamicznie zmieniającymi się modelami rozliczeń w chmurze publicznej (np. pay-as-you-go). Zwracamy też uwagę na potencjalną sprzeczność celów b) dot. Zawierania umów ramowych i uproszczonych umów wykonawczych z pkt. c) dotyczącym reformy ZUCH. Nie jest jasne, którą ścieżką będzie przebiegał proces zakupowy oraz jakie typy usług będzie obejmował.
	VI Cele i czynniki umożliwiające ich realizację	3.3 Branże kreatywne	Wybierz element.	Sektor kreatywny został w Strategii wymieniony, jednak potraktowany głównie w kategorii digitalizacji zasobów kultury i kompetencji cyfrowych. Brakuje celów gospodarczych dotyczących skalowania działalności, eksportu treści i usług cyfrowych oraz wykorzystania AI (np. generatywnej) w przemysłach kreatywnych
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Transport	Transport pojawia się w Strategii jedynie kontekstowo. Brakuje celów sektorowych odnoszących się do cyfryzacji, automatyzacji, logistyki danych czy zastosowań AI. Wnosimy o uzupełnienie Strategii o sektorowe cele dla transportu i powiązanej logistyki.
	VI Cele i czynniki	Gospodarka i technologie	Energetyka	Energetyka jest wskazana jako obszar oddziaływania transformacji cyfrowej, jednak Strategia nie definiuje dla tego sektora żadnych celów ani planu działań w zakresie

	umożliwiające ich realizację			cyfryzacji i zastosowań AI (np. zarządzanie sieciami, prognozowanie, elastyczność popytu). Postulujemy rozważenie energetyki jako jednego z kluczowych sektorów transformacji cyfrowej
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Nauka i B+R	Strategia definiuje cele związane z dostępem do mocy obliczeniowej i danych dla nauki, jednak brak powiązania tego obszaru z sektorową transformacją gospodarki oraz transferem technologii do przemysłu i usług. Proponujemy wzmocnienie wątku komercjalizacji i zastosowań gospodarczych wyników cyfryzacji B+R.
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Przemysł / produkcja	Przemysł nie został w Strategii wyróżniony jako odrębny sektor transformacji cyfrowej. Brakuje odniesienia do przemysłowej transformacji cyfrowej i AI (Industry 4.0/5.0), mimo jej istotnego znaczenia dla produktywności i konkurencyjności gospodarki.
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Sektor usług rynkowych (finanse, handel, e-commerce)	W Strategii nie zdefiniowano celów ani działań dla kluczowych sektorów usługowych gospodarki, takich jak finanse, handel czy e-commerce, mimo ich wysokiego stopnia cyfryzacji i znaczenia dla PKB. Postulujemy uzupełnienie dokumentu o refleksję sektorową w tym zakresie.
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Przemysł cyfrowy / sektor ICT	Strategia nie definiuje mierzalnych celów rozwoju przemysłu cyfrowego (liczby startupów, produktów i usług cyfrowych, w tym AI), ani nie powiązuje ich z kluczowymi sektorami gospodarki. Postulujemy uzupełnienie Strategii o ilościowe cele rozwoju przemysłu cyfrowego, rozumianego jako źródło innowacyjnych produktów i usług dla sektorów takich jak zdrowie, energetyka, transport czy sektor kreatywny.
	VI Cele i czynniki umożliwiające ich realizację	Gospodarka i technologie	Przemysł (manufacturing)	Zarówno Strategia Cyfryzacji Państwa, jak i Polityka rozwoju sztucznej inteligencji nie traktują przemysłu jako pełnoprawnego sektora transformacji cyfrowej i AI. Postulujemy uwzględnienie przemysłu na liście kluczowych sektorów Strategii, z uwagi na jego istotny udział w PKB i eksporcie oraz wysoki potencjał do zastosowań

				AI (AI+), prowadzących do wzrostu produktywności, tworzenia innowacyjnych produktów i rozwoju krajowego przemysłu cyfrowego.
	VI Cele i czynniki umożliwiające ich realizację	4.8 Cyfrowa modernizacja rolnictwa	Wybierz element.	Strategia wskazuje rolnictwo jako sektor wymagający cyfryzacji, jednak cele i działania koncentrują się głównie na modernizacji administracyjnej i informacyjnej. Brakuje odniesienia do transformacji produktywności sektora, wykorzystania AI i analityki danych oraz rozwoju krajowych dostawców rozwiązań cyfrowych dla rolnictwa.
	VI Cele i czynniki umożliwiające ich realizację	4.1 Cyfrowa transformacja przedsiębiorstw	Wybierz element.	Cele w tym obszarze koncentrują się na upowszechnianiu technologii w przedsiębiorstwach, pomijając rozwój polskich dostawców technologii i usług cyfrowych . Proponujemy dodanie celu odnoszącego się wprost do zwiększenia liczby i skali polskich firm dostarczających rozwiązania cyfrowe (w tym AI, software, usługi chmurowe), wraz z adekwatnymi wskaźnikami.
	VII System wdrażania	1.1 Komunikacja elektroniczna	Cel 1	Cel na poziomie 100% (od 2030 r.) w kontekście zapewnienia zasięgu sieci stacjonarnej jest nierealistyczny. Postulujemy ograniczenie się do poziomu 99%, co i tak jest podejściem ambitnym.
	VII System wdrażania	1.1 Komunikacja elektroniczna	Cel 2	Zaproponowane poziomy zasięgu przyjęte dla sieci mobilnych są nieracjonalne. W ocenie PIIT należy je powiązać z poziomami wynikającymi z zobowiązań w rezerwacjach częstotliwości, gdzie docelową wartością dla pokrycia zasięgiem gospodarstw domowych przez każdego z MNO jest 99%. I wartość ta nie dotyczy sieci 5G, ale sieci dowolnej technologii, która zapewnia przepustowość na poziomie 95 Mb/s i opóźnienie na poziomie 10 ms.
	VII System wdrażania	1.1 Komunikacja elektroniczna	Wybierz element.	W nawiązaniu do uwagi zgłoszonej do części 1.1. Komunikacja elektroniczna, PIIT wnosi o wprowadzenie wskaźnika realizacji celu polegającego na uruchomieniu przewidzianego już w przepisach PKE mechanizmu umowy inwestycyjnej, poprzez wskazanie roku, od którego oba instrumenty zaczną być faktycznie stosowane w

				celu poprawy odporności sieci (w ocenie PIIT powinno to nastąpić nie później niż w 2027 r.).
	VIII Finansowanie	Wybierz element.	Wybierz element.	Rozdział „Finansowanie” wskazuje potencjalne źródła środków, lecz nie zawiera ramowego budżetu Strategii, podziału środków na obszary ani priorytetów wydatkowych . Postulujemy uzupełnienie Strategii o syntetyczny plan finansowy, umożliwiający ocenę wykonalności celów
	VIII Finansowanie	Wybierz element.	Wybierz element.	Wnosimy o wskazanie w zakresie źródeł finansowania wprost umowy inwestycyjnej, o której mowa w Prawie komunikacji elektronicznej. W ocenie PIIT bezpośrednia konwersja opłat na inwestycje byłaby stosunkowo prostym i efektywnym sposobem na osiągnięcie celów w zakresie zwiększenia odporności sieci telekomunikacyjnych oraz uzupełnienia zasięgu w najtrudniejszych inwestycyjnie obszarach.

1. Uwagi o charakterze ogólnym

Lp.	Treść uwagi
1	Strategia Cyfryzacji Państwa identyfikuje wybrane sektory gospodarki, jednak tylko w nielicznych przypadkach przekłada to na konkretne cele i działania sektorowe. W obecnym kształcie dokument nie stanowi sektorowej strategii transformacji cyfrowej gospodarki.
2	Brakuje wskazania sektorów priorytetowych dla transformacji cyfrowej i AI oraz dokonania świadomych wyborów strategicznych w tym zakresie. Postulujemy rozważenie wzmocnienia komponentu sektorowego Strategii
3	Transformacja AI w Strategii ma charakter horyzontalny i narzędziowy. Nie przypisano jej do konkretnych sektorów gospodarki jako źródła trwałej przewagi konkurencyjnej.
4	Spójne potraktowanie w Strategii i Polityce AI kluczowych sektorów transformacji cyfrowej oraz transformacji AI zwiększyłoby jej spójność z polityką gospodarczą i przemysłową państwa oraz poprawiło jej użyteczność wdrożeniową

5	Spójność dokumentów strategicznych państwa ma kluczowe znaczenie dla skuteczności polityk publicznych. Strategia Cyfryzacji Państwa oraz Polityka Rozwoju Sztucznej Inteligencji powinny wzajemnie się uzupełniać – zarówno na poziomie wyboru sektorów priorytetowych, jak i definiowania celów oraz instrumentów ich realizacji. Brak spójności utrudnia wdrażanie, osłabia sygnały inwestycyjne dla rynku oraz ogranicza możliwość koncentracji zasobów publicznych na obszarach o największym potencjale rozwojowym. Jednocześnie doświadczenia sektorów, dla których Strategia przewiduje pogłębione podejście (np. rolnictwo), pokazują, że ujęcie sektorowe pozwala przejść od ogólnych deklaracji do konkretnych celów, działań i efektów gospodarczych. Zastosowanie analogicznego podejścia do innych sektorów, w szczególności przemysłu, wydaje się uzasadnione zarówno z perspektywy skali gospodarki, jak i potencjału technologicznego.
---	---