Tabela uwag odnośnie do projektu uchwały Rady Ministrów
w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029

I. Uwagi ogólne

1. Cel główny został zdefiniowany jako "Podniesienie poziomu odporności krajowych podmiotów przez zwiększenie poziomu ochrony informacji oraz zwiększenie zdolności do wykrywania i reagowania na zagrożenia, promowanie wiedzy i dobrych praktyk oraz podnoszenie kompetencji w zakresie cyberbezpieczeństwa w sektorze publicznym (w tym militarnym), prywatnym, a także wśród obywateli." Choć z aprobatą przyjmujemy modyfikację celu w porównaniu z poprzednimi wersjami projektu, nadal dostrzegamy, że skupienie się przede wszystkim na zwiększaniu ochrony informacji i szybkim reagowaniu na incydenty nie jest wystarczające. Współczesne wyzwania wymagają bardziej stanowczego podejścia do kwestii wzmacniania **krajowej infrastruktury ICT**, podnoszenia jakości **usług cyfrowych** oraz zwiększania **bezpieczeństwa produktów cyfrowych**. O ile Cel szczegółowy 3. przewiduje plan podniesienia poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej, o tyle jesteśmy zdania, że kwestie wysoce odpornej infrastruktury ICT powinny stanowić nadrzędny cel Strategii.
2. W 1. celu szczegółowym „Rozwój krajowego systemu cyberbezpieczeństwa", punkt 5.1. odnosi się do doskonalenia tego systemu, koncentrując się jednak głównie na omówieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa. Warto zastanowić się, czy dokument o strategicznym charakterze, jakim jest Strategia Cyberbezpieczeństwa, powinien w tak dużym stopniu skupiać się na opisywaniu samej regulacji (która wynika z prawodawstwa unijnego i powinna być już dawno zaimplementowana w krajowym porządku). Wydaje się, że w tym obszarze uzasadnione byłoby przyjęcie bardziej ambitnego i przyszłościowego podejścia – wykraczającego poza ramy obowiązującego ustawodawstwa – z uwzględnieniem kierunków dalszego rozwoju, nowych wyzwań i innowacyjnych, krajowych rozwiązań systemowych.
3. W opisie celów w kontekście UKSC słusznie wskazano potrzebę sformalizowania funkcjonowania Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), które w dalszej perspektywie ma zostać przekształcone w centralną instytucję odpowiedzialną za zapewnianie cyberbezpieczeństwa na poziomie krajowym. Warto jednak zauważyć, że w zapisach dotyczących utworzenia tej instytucji brakuje doprecyzowania jej przyszłej właściwości – w szczególności tego, czy jej odpowiedzialność będzie obejmować wyłącznie obszar cywilny, czy też również wojskowy. Takie rozróżnienie jest istotne z punktu widzenia efektywnego planowania kompetencji oraz struktury organizacyjnej. Ponadto, w dokumentach pojawiają się rozbieżności co do zakresu działania planowanej instytucji – w niektórych fragmentach mówi się o funkcji koordynacyjnej, w innych natomiast o zarządzaniu cyberbezpieczeństwem. Z uwagi na horyzontalny charakter cyberbezpieczeństwa, centralne zarządzanie wszystkimi jego aspektami może być trudne do zrealizowania w praktyce. Dlatego

zasadne byłoby doprecyzowanie, czy planowana instytucja będzie pełniła funkcję koordynacyjną, czy też zostanie jej przypisana szersza rola zarządcza – co wiązałoby się z koniecznością bardziej złożonych rozwiązań.

4. O ile wdrożenie w Polsce NIS2 zostało bardzo szczegółowo opisane w Strategii, o tyle istotna z punktu widzenia infrastruktury krytycznej Dyrektywa CER wydaje się nieco pominięta. Jesteśmy zdania, że wymieniona jedynie raz w tekście dyrektywa zasługuje na szersze potraktowanie, ze względu na to, iż od wdrożenia tej regulacji zależeć będzie rzeczywisty poziom odporności na zakłócenia podstawowych funkcji państwa (wraz z ustawą o ochronie ludności).
5. Z uznaniem odnosimy się do planów rozwijania narodowego komunikatora przeznaczonego dla administracji publicznej. Uważamy jednak, że zapowiedź „podejmowania **działań w kierunku** zastępowania komercyjnych rozwiązań komunikacyjnych rozwiązaniami udostępnianymi przez instytucje państwowe" stanowi krok niewystarczający wobec aktualnych wyzwań. W obliczu niestabilności globalnego ładu politycznego i gospodarczego – związanej m.in. z agresywną polityką Federacji Rosyjskiej, ryzykiem eskalacji konfliktów w Azji Południowo-Wschodniej czy rosnącą niepewnością w relacjach transatlantyckich – oraz w kontekście dynamicznego rozwoju technologii, poziom zagrożeń cybernetycznych pozostaje wyjątkowo wysoki. W naszej ocenie, w administracji publicznej w komunikacji o charakterze profesjonalnym należy niezwłocznie zastąpić rozwiązania komercyjne systemami zapewnianymi przez państwo. Dodatkowo, kluczowe znaczenie ma budowanie świadomości wśród przedstawicieli najwyższych władz państwowych co do skali i charakteru zagrożeń. W tym kontekście niezbędne wydaje się wprowadzenie jasnych zasad, zakazujących prowadzenia korespondencji służbowej za pośrednictwem prywatnych kanałów komunikacji.
6. Strategia nie podejmuje wprost istotnego zagadnienia dotyczącego poziomu samowystarczalności państwa w zakresie cyberbezpieczeństwa – zarówno w kontekście technologii, jak i zdolności operacyjnych. Brakuje więc szerszej refleksji nad tym, w jakich obszarach kooperacje z sektorem prywatnym są lub będą niezbędne. Choć dokument wspomina o partnerstwie z PwCyber oraz o wspieraniu polskich podmiotów, warto zauważyć, że nie uwzględniono szerszego wachlarza istniejących modeli współpracy oraz możliwości ich rozwoju. Strategia mogłaby w tym kontekście zawrzeć propozycję ustanowienia inicjatywy, która – w perspektywie krótko- lub średnioterminowej – określiłaby zasady, cele i warunki rozwijania partnerstw publiczno-prywatnych w obszarze cyberbezpieczeństwa z podmiotami z Polski i UE. Tego rodzaju podejście mogłoby wzmocnić zarówno krajowy potencjał technologiczny, jak i operacyjny, jednocześnie wspierając polski sektor innowacyjny.

II. Uwagi szczegółowe

Tabela uwag odnośnie do projektu uchwały Rady Ministrów
w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029

Lp.	Podmiot zgłaszający uwagę/ propozycję zmian	Jedn. red. projektu/ str. uzasadnienia/ część OSR	Treść uwagi/propozycji zmiany	Stanowisko Ministra Cyfryzacji
uwagi/propozycje zmian do projektu uchwały				
1.				
2.				
3.				
uwagi/propozycje zmian do projektu załącznika do uchwały				
4.		7.1 / str. 28	Proponujemy wprowadzenie w podrozdziale pt. „Podniesienie poziomu odporności systemów informacyjnych” następującego akapitu: *Z uwagi na zależność ciągłości działania systemów informacyjnych pomiędzy dostawcami niektórych kluczowych usług podejmowane będą działania w zakresie stworzenia mechanizmów wymiany informacji pomiędzy podmiotami z sektorów dostaw energii elektrycznej, wody oraz usług telekomunikacyjnych. Ich celem będzie stworzenie bezpiecznych narzędzi opartych o otwarte API umożliwiających wymianę informacji o pracach planowych, wyłączeniach, modernizacjach i awariach.* Wprowadzenie takiego mechanizmu będzie miało istotne znaczenie dla planowania i podejmowania działań podmiotów zależnych od ciągłości dostaw kluczowych mediów, w tym przygotowywania i alokowania zasobów rezerwowych lub	

			stosowania mechanizmów zastępczych pozwalających na utrzymanie ciągłości funkcjonowania.	
5.		7.1 / str. 28 12 / str. 44	Proponujemy wprowadzenie w podrozdziale pt. „Podniesienie poziomu odporności systemów informacyjnych" lub rozdziale „Finansowanie" następującego akapitu: *„Z uwagi na kluczowe znaczenie wzmacniania odporności po stronie kluczowych przedsiębiorstw, w tym z sektorów telekomunikacji, energetyki czy dostaw wody, podjęte zostaną prace nad stworzeniem mechanizmów wsparcia dedykowanych inwestycjom w poprawę odporności takich podmiotów, ze szczególnym uwzględnieniem zagrożeń klimatycznych, militarnych i fizycznych. W szczególności w ramach alokacji środków europejskich z aktualnej i przyszłej perspektywy finansowej. W ramach prac podjęte zostaną także działania zapewniające możliwość udzielania pomocy publicznej w tych obszarach, w tym poprzez włączenie zagadnień odporność dużych firm z kluczowych sektorów do katalogu wyłączeń blokowych w rozporządzeniu GBER."* Z uwagi na rosnący poziom zagrożenia konieczne jest podjęcie działań także wobec podmiotów gospodarczych, działających na rynku konkurencyjnym wśród których istnieje luka finansowa w zakresie inwestycji mogących podnosić ponadstandardowo poziom bezpieczeństwa, szczególnie w obszarach wyjątkowego narażenia, jak obszary wschodnie lub szczególnie narażone na klęski żywiołowe.	

6.		5.3 / str. 18	Pkt. 5.3. pt. Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania administracji państwowej, bezpieczeństwa narodowego i ochrony ludności W tym podrozdziale został opisany System Bezpiecznej Łączności Państwowej. Wiąże się z nim działanie 1.3 w tabeli na str. 50-51. Zawiera ona wskazanie podmiotów odpowiedzialnych za realizację oraz terminy wykonania. W naszej ocenie Strategia Cyberbezpieczeństwa powinna zostać ograniczona jedynie do wskazania, na fakt, że realizacja zadań w zakresie SBŁP oraz systemów alarmowania i powiadamiania będzie realizowana na podstawie ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej. Zadania te mają już więc swoją podstawę prawną do realizacji w postaci przepisów powszechnie obowiązujących, a także wydanego na jej podstawie Programu Ochrony Ludności i Obrony Cywilnej zatwierdzonego już przez Radę Ministrów. Tenże program zawiera już opis tych zagadnień, a także wskazuje podmioty odpowiedzialne – działanie nr 5 w tabeli na str. 48. Tym samym, aby uniknąć sytuacji, w której te same zadania są adresowane w dwóch dokumentach przyjmowanych na poziomie Rady Ministrów, za właściwe uznajemy, że właściwym dokumentem dla ujęcia tego zagadnienia jest Program Ochrony Ludności i Obrony Cywilnej. Proponujemy więc: • Modyfikację opisu SBŁP poprzez zawarcie odwołania do ustawy oraz Programu, a także usunięcie zapisów	

			wskazujących na planowane działania, które powinny być ujmowane w Programie (akapit 4) • Usunięcie tego zadania z tabeli wdrożeniowych	
7.		6.1 / str. 21 i nast.	Proponujemy wprowadzenie w podrozdziale 6.1. pt. *„Wprowadzenie regulacji skuteczniej pozwalających zwalczać cyberprzestępczość*" następującego akapitu: *„Z uwagi na szeroki zakres planowanych rozwiązań dot. zwalczania cyberprzestępczości oraz ich potencjalnie istotnego wpływu na szereg podmiotów zobowiązanych do realizacji nowych wymagań dot. współpracy z organami planowane jest powołanie zespołów tematycznych, których zadaniem będzie wypracowanie modelowych rozwiązań prawnych przed ich skierowaniem na ścieżkę legislacyjną. Ma to na celu zbudowanie rozwiązań skutecznych, ale jednocześnie proporcjonalnych i niewiążących się z nadmiernym obciążeniem sektora przedsiębiorstw. Podobne podejście będzie stosowane w stosownych przypadkach w wypracowywaniu rozwiązań omówionych w podrozdziale 6.5, w tym w szczególności w zakresie rejestracji kart SIM."* Popieramy kierunkowo wprowadzanie rozwiązań poprawiających bezpieczeństwo w cyberprzestrzeni, w szczególności pod kątem działalności oszukańczej negatywnie oddziałującej zarówno na konsumentów, jak i podmioty w sposób legalny oferujący swoje usługi i produkty. Odnotowujemy jednocześnie, że część z tych wymagań może wiązać się z koniecznością zmian po stronie przedsiębiorstw, jak np. udostępnianie danych, blokowanie stron lub treści, działania związane z nadużyciami w komunikacji elektronicznej czy dot. kart SIM. Poniżej do części z nich odnosimy się także szczegółowo. W tym miejscu sygnalizujemy jedynie, że	

			postulowanym kierunkiem jest aby operacyjne rozwiązania zostały wypracowane w drodze dialogu przez ekspertów ze wszystkich zaangażowanych środowisk. Za konieczne uważamy bowiem, aby rozwiązania te nie stawały się nieproporcjonalnym obciążeniem administracyjnym.	
8.		7.1 / str. 28 8.1 / str. 34-35	Popieramy wprowadzenie rozwiązań umożliwiających szybkie reagowanie na potrzeby związane z zapobieganiem incydentom lub przeciwdziałaniu zagrożeniom w instytucjach publicznych. Przyjmujemy do wiadomości, że może to wiązać się ze stosowaniem nadzwyczajnych trybów zakupowych. Postulujemy jednak wprowadzenie do Strategii jasnych zapisów wskazujących, że zostaną określone jasne kryteria dla stosowania trybów nadzwyczajnych oraz sposób procedowania gwarantujący minimalne przynajmniej zasady efektywności i konkurencji w wydatkowaniu środków publicznych. Zauważamy również, że dla części z takich sytuacji możliwe jest wyprzedzające zawarcie – w normalnych trybach – umów (np. umów ramowych) umożliwiających świadczenie usług dopiero po zaktualizowaniu się przesłanek, np. ataku na systemy informacyjne. Przede wszystkim podkreślamy, że nadzwyczajne tryby nie mogą służyć obchodzeniu normalnych, konkurencyjnych procedur zakupowych, ale być jedynie ostatecznym narzędziem, które jest faktycznie konieczne do podjęcia.	
9.		7.1 / str. 28	W zakresie planowanych do wprowadzenia wymagań cyberbezpieczeństwa, w tym w zakresie certyfikacji lub kryptografii uważamy ten kierunek za słuszny. Kluczowe jednak jest, aby wymagania te powstawały z uwzględnieniem aktualnych możliwości rynku, w tym dojrzałości samego systemu certyfikacji. Istotne jest więc, aby formułowane wymagania nie stawały się nadmiarowe lub ograniczające, w szczególności dla podmiotów krajowych.	

10.		7.1 / str. 29	Poza odwołaniem do bezpieczeństwa kabli podmorskich podkreślamy także zagadnienia bezpieczeństwa lądowych połączeń międzynarodowych. W przypadku wprowadzania narzędzi wspierających dla rozwoju kabli podmorskich, adekwatne narzędzia powinno się wprowadzać wobec kabli lądowych. Jest to szczególnie istotne wobec Polski, której połączenia z najbliższymi sąsiadami bazują właśnie na kablach lądowych.	
11.		9.2 / s. 38	Proponujemy wprowadzenie w podrozdziale pt. „Rozwój świadomości i wiedzy obywateli i przedsiębiorców z zakresu cyberbezpieczeństwa" następującego akapitu: *„Z uwagi na zagrożenia w sferze informacyjnej, które mogą także wywoływać skutki w obszarze bezpieczeństwa kluczowych usług oraz ciągłości działania kluczowych dla państwa procesów podejmowane będą także działania mające na celu walkę z dezinformacją, szczególnie w dziedzinie nowoczesnych technologii. Promowana będzie wiedza oparta o dorobek naukowy, w tym krajowym instytutów badawczych oraz ośrodków akademickich*". Przykładem tego typu działań jest dezinformacja w zakresie sieci 5G, która może negatywnie oddziaływać na ogólną percepcję społeczną i adopcję nowych technologii, a w skrajnych przypadkach skutkować opóźnianiem jej wdrażania czy nawet fizycznymi atakami na obiekty infrastrukturalne. Podobnie jest z technologiami OZE lub energetyką jądrową. Z uwagi na istotny interes państwa, a także szeroko rozumiany wpływ na funkcjonowanie cyberprzestrzeni kwestie te powinny zostać uwzględnione w Strategii.	
12.				
13.				
14.				

Tabela uwag odnośnie do projektu uchwały Rady Ministrów
w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029

uwagi/propozycje zmian do uzasadnienia				
15.				
16.				
17.				
uwagi/propozycje zmian do Oceny Skutków Regulacji				
18.				
19.				
20.				

KL/351/119/AM/2025