Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
1. 2.	Uwaga ogólna		Notyfikacja przepisów: W uzasadnieniu projektu podobnie jak dotychczas wskazano, że: *„Projektowana regulacja będzie poddana notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych”.* Prosimy o wyjaśnienie w jakim zakresie prowadzona będzie notyfikacja i czy będzie to zakres wykraczający również poza dotychczas identyfikowaną jako podlegającą zgłoszeniu procedurę ustalania dostawców wysokiego ryzyka.	
3.	Tytuł ustawy		TYTUŁ USTAWY NIE ODPOWIADA JEJ PROJEKTOWANEJ TREŚCI Uwaga/uzasadnienie: Tytuł ustawy nie odpowiada jej treści. Przepisy dot. Strategicznej Sieci Bezpieczeństwa, procedur dystrybucji częstotliwości, spółki Polskie 5G czy powołania funduszu przeznaczonego na rozwój SSB, mimo ich wskazania w zakresie przedmiotowym ustawy, nie powinny być regulowane ustawą, której tytuł wskazuje wyłącznie na regulację krajowego systemu cyberbezpieczeństwa. Zgodnie z par. 16 i nast. rozporządzenia w sprawie zasad techniki prawodawczej tytułowi ustawy przypisuje się istotne znaczenie informacyjne co uzasadnia ustawienie w tym zakresie minimalnych wymagań. W szczególności par. 18 ust. 1 wskazuje, że „*Przedmiot ustawy określa się możliwie najzwięźlej, jednakże w sposób adekwatnie informujący o jej treści*.” Trudno uznać tak w przypadku ustawy o krajowym systemie cyberbezpieczeństwa, do której wprowadzono przepisy dotyczące podmiotów, działań i instytucji pozostających poza zakresem krajowego systemu cyberbezpieczeństwa. Ani bowiem Operator Strategicznej Sieci Bezpieczeństwa, ani Spółka Polskie 5G nie są wskazani jako podmioty KSC.	

			Propozycja: Zmiana tytułu ustawy uwzględniająca rozszerzenie jej zakresu dalece poza regulację dot. krajowego systemu cyberbezpieczeństwa.	
4.	art. 1 pkt 3 lit d		**W art. 1 pkt 3 lit d po pkt 4b dodaje się pkt 4c w brzmieniu następującym:** *„funkcje krytyczne – oznaczają funkcje zawarte w wykazie funkcji krytycznych dla bezpieczeństwa sieci i usług, o którym mowa w art. 66f, które są krytyczne dla bezpieczeństwa produktów ICT, usług ICT i procesów ICT;”* **Uzasadnienie:** Projekt nie przewiduje definicji „*funkcji krytycznych*”, podczas gdy to pojęcie jest istotne z perspektywy wprowadzanych instytucji prawnych, w szczególności postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Z tego względu proponuje się zdefiniowanie tego pojęcia w art. 2 ustawy, poprzez odwołanie do szczegółowego postanowienia odnoszącego się do trybu określania wykazu funkcji krytycznych w proponowanym art. 66f (pkt 49 poniżej). W przypadku braku uwzględnienia uwagi dotyczącej art. 66f (pkt 49 poniżej), proponuje się dodanie pkt 4c w brzmieniu następującym: *„funkcje krytyczne – oznaczają funkcje zawarte w wykazie funkcji krytycznych dla bezpieczeństwa sieci i usług, stanowiącym załącznik nr 3 do ustawy, które są krytyczne dla bezpieczeństwa produktów ICT, usług ICT i procesów ICT zgodnie z wykazem krytycznych aktywów zawartym w 5G Toolbox;”*	
5.	art. 1 pkt 3 lit d		**W art. 1 pkt 3 lit d po pkt 4c dodaje się pkt 4d w brzmieniu następującym:** *„5G Toolbox* – oznacza dokument „Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G” opublikowany w styczniu 2020 roku i jego kolejne wersje. **Uzasadnienie:** Definicja jest skorelowana z propozycją wprowadzenia definicji dla pojęcia funkcji krytycznych w pkt 4 powyżej.	
6.	Art. 1 pkt 13 dot. art. 11 ust. 2 u KSC		Sektorowe CSiRT: Zarządzanie incydentami cyberbezpieczeństwa wymaga bardzo szybkiej reakcji i skoordynowanego działania w kraju. Zwiększanie liczby CSiRT przez wprowadzenie CSiRT’ów	

			sektorowych może mieć negatywny wpływ na sprawne i skuteczne zarządzanie obroną przed cyberatakami na operatorów usług kluczowych. Nie można powielać modelu sektorowych regulatorów (którzy w normalnym trybie ustawodawczym/wykonawczym definiują wymagania dla firm ze swoich sektorów gospodarki) w obszarze zarządzania incydentami cyberbezpieczeństwa, gdzie wymagane jest natychmiastowe działanie kierowane równolegle do różnych sektorów gospodarki oraz centralny punkt zarządzania incydentem i monitorowania skuteczności podjętych środków zaradczych. W naszej ocenie stworzenie obligatoryjnych sektorowych CSiRT'ów odwrotnie niż to jest zakładane, faktycznie osłabiony może zostać krajowy system odporności na cyberataki. Stąd wątek ten wymaga w naszej ocenie dodatkowej dyskusji i rewizji.	
7.	Art. 1 pkt 36 dot. art. 44 uKSC		Dotyczy: *Art. 44. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 do ustawy, do którego zadań należy:* *1) przyjmowanie zgłoszeń o incydentach* *2) reagowanie na incydenty (…)* Nie rozumiemy na czym ma polegać reagowanie na incydenty w wykonaniu CSIRT sektorowego. Pojęcie to nie zostało zdefiniowane w ustawie. Zarządzanie, w tym obsługa incydentu (w tym działania naprawcze oraz ograniczanie skutków incydentów) pozostaje w zakresie odpowiedzialności OUK. Co w takim razie kryje się pod zadaniem w postaci „reagowania". Nie możemy zaakceptować kolejnego podmiotu na rynku z uprawnieniami o charakterze władczym względem UOK.	
8.	Art. 1 pkt 13 dot. art. 11 ust. 2 u KSC		KORZYSTANIE Z SYSTEMU S46 Uwaga/uzasadnienie: Wprowadzenie powszechnego obowiązku raportowania – a więc i korzystania – przez system S46 jest nadmiarowe. Może to generować dodatkowe koszty i obciążenia organizacyjne dla OUK. Zasilenie systemu S46 może być realizowane przez odpowiednie CSIRT sektorowe otrzymujące zgłoszenie. Według zapisów zawartych w projekcie Krajowego Planu Odbudowy, w którym zakładane było finansowanie przyłączenia do S46 ponad 300 jednostek publicznych koszt ten szacowano na ok 180 tys. zł. W uzasadnieniu nie określono przyczyn wprowadzenia obowiązku korzystania przez OUK z systemu S46. Nie oszacowano również kosztów	

			wprowadzenia tych przepisów, w tym dla jednostek budżetowych, ani źródeł ich pokrycia – brak załączonego nowego OSR projektu. Postulaty (częściowo alternatywne): • Pozostawienie dotychczasowego brzmienia przepisu tj. „2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.” Doprecyzowanie, że CSIRT sektorowy przekazuje informacje za pośrednictwem S46. • Ograniczenie obowiązku przekazywania zgłoszeń przez system S46 do podmiotów, które dobrowolnie zawrą porozumienie dot. korzystania z systemu. • Wprowadzenie mechanizmu pełnego finansowania wykonywania działań związanych z przyłączeniem i korzystaniem z systemu S46. • Wyraźne ograniczenie obligatoryjnego i nieodpłatnego korzystania z systemu S46 wyłącznie do obowiązków określonych w art. 11 co byłoby spójne z projektowanym przepisem karnym, który sankcjonuje brak korzystania z S46 wyłącznie w takim zakresie. • Wprowadzenie automatyzacji w zakresie przekazywania informacji poprzez odpowiednie interfejsy maszynowe. • Przeprowadzenie warsztatów w zakresie systemu S46 dla jego potencjalnych użytkowników przed wprowadzeniem zmian przepisów – aktualnie brak jest usystematyzowanej wiedzy nt. działania systemu S46 poza gronem jego bezpośrednich użytkowników.	
9.	Art. 1 pkt 13 dot. art. 11 ust. 3 u KSC		ZAKRES INFORMACJI PRZEKAZYWANY CSIRT SEKTOROWEMU (o ile zostanie utrzymany obowiązek raportowania OUK do CSIRT sektorowego) Dotyczy: *Art. 11 ust. 3 pkt 2* *Operator usługi kluczowej:* *2) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach.;* Należy doprecyzować jaki zakres informacji o rejestrowanych incydentach CSIRT sektorowy może posiadać z wyraźnym zastrzeżeniem, że CSIRT sektorowy nie może mieć dostępu do informacji prawnie chronionych OUK/SOC oraz tych informacji, do których zapewnienia poufności OUK / SOC jest zobowiązany w myśl zawartych umów.	

			Przy wyznaczaniu sektorowych CSiRT'ów nie można dopuścić do sytuacji, w której wyznaczony podmiot będzie działał również komercyjnie i stanowił konkurencję na tym samym rynku, a uprawnienie CSiRTu sektorowego pozwoli mu na dostęp do bardzo szerokiego zakresu informacji stanowiących tajemnicę przedsiębiorstwa. Naruszy to zasadę uczciwej konkurencji na rynku.	
10	Art. 1 pkt 14 dot. art. 14 ust. 5 uKSC		SOC Uwaga/uzasadnienie: W nowym brzmieniu projektowanego przepisu dodana została możliwość realizacji zadań w zakresie SOC, poprzez SOC utworzony na rzecz OUK przez organ tworzący lub nadzorujący. Dalsze przepisy nie wyjaśniają jednak zasad takiej współpracy, ew. odpłatności, odpowiedzialności itp. W tym zakresie wydaje się niezbędne odpowiednie doprecyzowanie.	
11	Art. 1 pkt 14 dot. art. 14 ust. 7 uKSC		SOC – DOSTĘP DO SYSTEMÓW Uwaga/uzasadnienie: Proponowane rozwiązanie polegające na dopuszczeniu dostępu OUK do systemów SOC obsługującego OUK (szczególnie jeśli to zewnętrzny OUK) jest rozwiązaniem, które powinno zostać usunięte lub dalece doprecyzowane. Aktualne brzmienie nakłada zbyt szeroki i niedoprecyzowany obowiązek dopuszczania OUK do kluczowych systemów, które nie muszą i zazwyczaj nie służą do obsługi jedynie jednego podmiotu – szczególnie w zakresie usług dot. monitorowania i wykrywania zagrożeń lub incydentów. Propozycja: Przepisy jeśli zostałyby pozostawione powinny wprost wskazywać, że SOC może odmówić udzielenia dostępu jeśli mogłoby to zagrozić bezpieczeństwu tego systemu lub innych podmiotów przez niego obsługiwanych, w tym w zakresie ewentualnego naruszenia danych lub tajemnic prawnie chronionych. Jednocześnie dostęp taki mógłby być przyznawany jedynie na wniosek OUK, wynikać z zawartej umowy oraz dotyczyć niezbędnego zakresu dotyczącego wyłącznie obsługiwanego OUK.	
12	Art. 1 pkt 15 dot. art. 14a ust. 7 u KSC		SOC – wpis do rejestru Uwaga Aktualna konstrukcja przepisów wydaje się pomijać sytuację, w której SOC *„niepowołany wewnątrz struktury operatora usługi kluczowej ani niebędący stroną umowy o SOC"* mógłby zostać wpisany przez Ministra na wniosek podmiotu prowadzącego taki SOC. Brzmienie przepisów wskazuje, że nie było intencją wykluczenie takiej możliwości.	

			Propozycja: Doprecyzowanie możliwości złożenia wniosku o wpis przez podmiot prowadzący SOC niepowołany wewnątrz struktury operatora usługi kluczowej ani nie będący stroną umowy o SOC.	
13	Art. 1 pkt 15 dot. art. 14a ust. 7 pkt 3 KSC		SOC – korzystanie z systemu S46 Uwaga Wymóg zawarcia porozumienia ws. S46 jest nadmiarowy, nawet uwzględniając założenie korzystania przez OUK z tego systemu. Zakres świadczonych usług SOC może np. nie dotyczyć samego zgłaszania incydentów do czego zobowiązani mieliby zostać OUK, natomiastnormy określające zasady korzystania z systemu, w tym w zakresie porozumień ws. S46, określone są w art. 46 ustawy. Wymóg ten jest faktycznie ukrytą opłatą za wpis do rejestru polegającą na wymuszonym włączeniu do systemu S46, które wg informacji zawartych w uzasadnieniu związane jest z ponoszeniem kosztów przez podmiot przystępujący. Propozycja: Wykreślenie projektowanego pkt 3.	
14	Art. 1 pkt 21 dot. art. 25 i nast. uKSC		ISAC – ograniczone realne zachęty do wykorzystania tej formuły Uwaga Projektowane przepisy dot. ISAC określają zasady wpisu ISAC do rejestru, ramowe zadania oraz kwestie związane z kontrolą czy coroczną sprawozdawczością. Brakuje natomiast przepisów, które w sposób faktyczny zachęcałyby do tworzenia takich jednostek, np. poprzez określenie szczególnych uprawnień podmiotów je tworzących. Na tym etapie identyfikujemy uprawnienie do zawarcia porozumienia wz. korzystania z systemu S46. Istnieje ryzyko, że przy obecnym kształcie projektu, wprowadzenie regulacji dot. ISAC przyniesie skutek odwrotny od zamierzonego, tj. będzie zniechęcać do podejmowania takich inicjatyw. Propozycja: Włączenie ISAC (na zasadzie dobrowolności) z głosem doradczym/opiniodawczym w procesy prowadzone przez organy KSC, tj. w szczególności pełnomocnik lub Kolegium dot. kierunków rozwoju KSC, strategii, szacowania ryzyk, ustalania wysokiego poziomu ryzyka związanego z dostawcami, ocen sprzętu, oprogramowania, procesów ICT.	

15	Art. 1 pkt 22 dot. art. 26 ust. 3 pkt 21 lit a uKSC		Przedsiębiorcy są zaniepokojeni, że CSIRT GOV będzie mógł u nich przeprowadzić testy bezpieczeństwa. Taka operacja wymaga przygotowania po stronie przedsiębiorców oraz poniesienia kosztów. Nie jest jasne, jak będą traktowane wyniki tych testów, a także kto będzie decydował, czy określona podatność ma być załatana i w jakim terminie. Naszą obawę budzi, że administracja otrzyma wgląd w informacje, które są tajemnicą przedsiębiorstwa. Wnosimy zatem o wykreślenie tego uprawnienia CISRTów. Alternatywnie wnosimy o dodanie przepisu, że podmiot zobowiązany powinien mieć możliwość niewyrażenia zgody na wykonanie takiego testu.	
16	Art. 1 pkt 25 dot. art. 25a ust. 11 pkt 1 uKSC		Regulacja zakładająca, że minister właściwy do spraw informatyzacji, na wniosek organu właściwego albo urzędu, może przeprowadzić kontrolę zgodności z prawem działania ISAC wpisanego do wykazu ISAC jest zbyt daleko idąca. Taki przepis raczej nie zachęci przedsiębiorców do tworzenia ISAC. Trzeba wskazać, że celem ISAC jest współpraca, wymiana wiedzy i doświadczeń między firmami. Natomiast ta propozycja legislacyjna pozwala ministrowi na wgląd w działalność podmiotów, które tworzą ISAC. Jak się wydaje, taka ingerencja organu administracji może zniechęcić przedsiębiorców do wymiany informacji.	
17	Art. 1 pkt 25 dot. art. 25a ust. 13 pkt 1 i 2 uKSC		Proponowana regulacja ze względu na swój nadmierny rygoryzm administracyjny z pewnością nie przyczyni się do zwiększenia liczby nowych ISAC w Polsce. Wnosimy zatem o złagodzenie proponowanej sankcji, przynajmniej zrezygnowanie z wykreślenia ISAC z wykazu ISAC.	
18	Art. 1 pkt 32 dot. art. 37 ust. 3 uKSC		Proponowany przepis przewiduje możliwość publikacji w BIP informacji o incydentach istotnych, jakie dotknęły danego przedsiębiorcę. Nie widzimy podstaw do upublicznienia takiej informacji. Poza tym, nie jest zdefiniowana przesłanka niezbędności, o której mowa w projektowanym przepisie. W ocenie Konfederacji Lewiatan wymaga to bliższego określenia. Trzeba tu wyrazić obawę, że bez tej definicji każdy taki incydent istotny będzie publikowany w BIP, co może narazić na szwank reputację przedsiębiorcy	
19	Art. 1 pkt 38 dot. art. 46 uKSC		OBOWIĄZEK KORZYSTANIA Z SYSTEMU S46	

			W art. 46 wprowadzany jest obowiązek OUK do korzystania z systemu S46. Z perspektywy OUK krytyczną kwestią może być zakres korzystania, który wydaje się wymagać doprecyzowania. System S46 ma, według naszych ogólnych informacji, zaimplementowaną w sobie bardzo rozbudowaną metodykę zarządzania ryzykiem. Wprowadzanie danych do tego systemu, wykonywanie tam analizy ryzyk i utrzymywanie aktualności rejestru ryzyk zajmowałoby znacznie więcej czasu niż aktualnie jest poświęcane u operatora usługi kluczowej na analizę ryzyk znacznie większego obszaru spółki, niż tylko usługa kluczowa. Przy budowaniu systemu S46 -w szczególności w przypadku rozszerzenia zakresu jego użytkowników – w naszej ocenie w sposób niewystarczający uwzględniono, że na rynku są firmy, które mają już wdrożone skuteczne metodyki zarządzania ryzykiem i mogłyby wprowadzać do tego systemu tylko wyniki analiz ryzyka przeprowadzonych u siebie. Taką możliwość powinny mieć szczególnie firmy, w których zarządzanie ryzykiem jest corocznie weryfikowane przez zewnętrzne firmy audytorskie. W wypadku właśnie tych firm, wewnętrzne analizy ryzyk i tak będą musiały być dalej wykonywane bo do tego są zobligowane dla utrzymania np. certyfikatów ISO22301 oraz ISO27001. Obowiązkowe korzystanie z systemu S46, w tym zakresie, nałożyłoby jednak na te firmy czasochłonne i nadmiarowe wykonywanie dodatkowej pełnej analizy ryzyka wg. rozbudowanej metodyki zaszytej w S46. Stąd ewentualnie takim zakresem korzystania z systemu S46 powinno być fakultatywne. Niezależnie od powyższego w naszej ocenie kluczowa odpowiedzialność za analizy związane z szacowaniem ryzyka na poziomie krajowym powinna pozostawać przy kluczowych organach KSC. Propozycja: • Wobec OUK należałoby zrezygnować z obowiązkowego korzystania z S46, szczególnie jeśli miałoby to się wiązać z koniecznością ponoszenia dodatkowych kosztów z tym związanych. • W przypadku pozostawienia przepisu należy doprecyzować, że OUK korzysta z systemu w zakresie zgłaszania i obsługi incydentów oraz może korzystać w pozostałych zakresach w zakresie wynikającym z porozumienia. • Jednocześnie, korzystanie z systemu nie powinno wiązać się z ponoszeniem z tego tytułu kosztów lub dodatkowymi zadaniami, przekraczającymi podstawowe zadania OUK lub wpływającymi na swobodę ich realizacji w ramach obowiązujących przepisów. W przypadku występowania takich kosztów należy wprowadzić mechanizmy ich rekompensowania.	

20	Art. 1 pkt 45 dot. art. 64a uKSC		Proponowany przepis przewiduje możliwość publikacji w BIP informacji o incydentach istotnych, jakie dotknęły danego przedsiębiorcę. Nie widzimy podstaw do upublicznienia takiej informacji. Poza tym, nie jest zdefiniowana przesłanka niezbędności, o której mowa w projektowanym przepisie. W ocenie Konfederacji Lewiatan wymaga to bliższego określenia. Trzeba tu wyrazić obawę, że bez tej definicji każdy taki incydent istotny będzie publikowany w BIP, co może narazić na szwank reputację przedsiębiorcy.	
21	**art. 1 pkt 47 lit a**		**W art. 1 pkt 47 lit a dodany do art. 65 ust. 1 pkt 7 otrzymuje brzmienie następujące:** *„7) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka;”* **Uzasadnienie:** Decyzja w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka powinna uwzględniać kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług (por. w tym zakresie argumentację zawartą w pkt **5** poniżej). W konsekwencji projektowany przepis art. 65 ust. 1 pkt 7 powinien być uzupełniony poprzez wskazanie, że przepis ten dotyczy dostawcy sprzętu lub oprogramowania o funkcjach krytycznych. Zmiana skorelowana jest ze zmiana proponowaną w pkt 4 (definicja funkcji krytycznych)	
22	Art. 1 pkt 48 dot. art. 64a uKSC		OCENA WYSOKIEGO RYZYKA – brak konsultacji z podmiotami objętymi skutkami potencjalnych decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka Uwaga W zmodyfikowanej wersji projektu odnotowujemy rezygnację z przygotowywania analizy przez ekspertów, na rzecz analizy dokonywanej przez CSIRT GOV, MON lub NASK. Kwestie instytucjonalne wydają się jednak wtórne wobec merytorycznej jakości dokonywanej analizy. Wciąż jednak zbyt ograniczony jest w naszej ocenie sposób uwzględnienia opinii podmiotów wymienionych w art. 66a tj. tych, których systemów dotyczy ocena oraz tych, których będą dotyczyć skutki ewentualnych decyzji w zakresie uznania dostawcy za dostawcę wysokiego ryzyka. Zauważamy przy tym, że projektowany art. 64a ust. 1 pkt wskazuje, że analizy powinny uwzględniać informacje „*przekazane przez sektor prywatny*”, co jak wnioskujemy miałoby spełniać postulat prowadzenia odpowiednich konsultacji w ramach postępowania przygotowawczego. Dalsze przepisy, a w szczególności projektowany art. 66a ust. 7 określający	

			zakres opinii Kolegium dotyczy już wprost samego dostawcy oraz związanych z nim i jego produktami potencjalnymi zagrożeniami. Nie obejmuje więc wprost badania wpływu decyzji na podmioty zobowiązane do jej stosowania. To co jest jednak kluczowe to fakt, że projektowany art. 66a ust. 9 przewiduje, że w ramach sporządzanej w ramach postępowania opinii uwzględnia się *„analizę, o której mowa w art. 64a ust. 1 i 2, jeżeli przewodniczący Kolegium zlecił jej przeprowadzenie*". Oznacza to, że analiza prowadzona przez CSIRT nie musi zostać zlecona, a tym samym nie musi zostać uwzględniona na etapie formalnego postępowania. W praktyce oznacza to, że także nawet tak ogólnie zarysowane uwzględnienie informacji *„przekazanych przez sektor prywatny*" nie musi mieć miejsca. Faktycznie więc projektowane przepisy dają zaangażowanym w proces oceny organom swobodę w pozyskaniu analiz ekspertów oraz związanych z nimi opinii sektora prywatnego. Podsumowując, dostrzegamy następujące braki w zakresie procesu konsultacyjnego jako elementu postępowania przygotowawczego: • Analizy ekspertów, które mają zawierać element konsultacji z sektorem prywatnym nie są obligatoryjne i nie muszą być przeprowadzone przed wszczęciem formalnego postępowania. • Proces pozyskania informacji z sektora prywatnego nie został opisany w projektowanych przepisach. • Istnieje poważne ryzyko, że w procesie analiz zostanie pominięty głos użytkowników systemów, dla których ryzyko jest badane, a tym samym wyciągnięte zostaną niepełne lub nieprawidłowe wnioski. • Wydaje się, że podmiotami uprawnionymi do przedstawienia informacji w ramach analiz ekspertów powinny być też podmioty inne niż prywatne, ponieważ one również mogą zostać objęte zakresem stosowania decyzji dot. dostawcy uznanego za stwarzającego wysokie ryzyko. **Propozycja:** W pierwszej kolejności przeprowadzenie analizy przez właściwy CSIRT powinno być obligatoryjne dla procedury z art. 66a. Ewentualne kwestie nagłe mogą być rozwiązywane z zastosowaniem projektowanych ostrzeżeń lub poleceń. W zakresie postulatu zwiększenia poziomu konsultacji, poszukując modelu, który wydaje się stanowić dobry kompromis między odpowiednią elastycznością przepisów, a obiektywną potrzebą dokonywania konsultacji w obszarze objętym potencjalnym postępowaniem, chcielibyśmy zwrócić uwagę na znane już rozwiązania przyjęte w Finlandii. Zgodnie z przepisem 244a tamtejszej ustawy o komunikacji elektronicznej organ właściwy przed podjęciem decyzji	

			prowadzi konsultacje z właścicielami lub operatorami sieci i daje im możliwość naprawienia zidentyfikowanych niedociągnięć bezpieczeństwa. Rezygnacja z takich konsultacji i możliwości wprowadzenia działań naprawczych istnieje jedynie w szczególnie pilnych przypadkach. Biorąc powyższe pod uwagę wnosimy o wprowadzenie wymogu przeprowadzenia konsultacji z podmiotami potencjalnie objętymi obowiązkami wynikającymi z decyzji w ramach przygotowania do wydania rozstrzygnięć w ramach oceny dostawcy, ostrzeżeń oraz poleceń zabezpieczających. Rezygnacja z ich przeprowadzenia powinna być możliwa jedynie w szczególnie uzasadnionych przypadkach zagrożenia bezpieczeństwa Państwa i porządku publicznego.	
23	**art. 1 pkt 49 lit b**		**W art. 1 pkt 49 lit b w art. 66 ust. 4 dodaje się pkt 8 w następującym brzmieniu:** *„8) w sprawach określonych w art. 66a ust. 7 – przedstawiciele operatora strategicznej sieci bezpieczeństwa który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie”* Alternatywnie – w razie braku uwzględnienia uwagi zawartej w pkt 5 w zakresie odniesienia decyzji wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB: *„8) w sprawach określonych w art. 66a ust. 7 – przedstawiciele podmiotów wskazanych w art. 66a pkt 1) – 4), które nabywają lub posiadają produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie”* **Uzasadnienie:** Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka prowadzone jest w specyficznym trybie, a skutki decyzji daleko wybiegają poza bezpośrednie konsekwencje dla dostawcy, którego sprzęt lub oprogramowanie podlega ocenie. Prace Kolegium w zakresie opracowania opinii mają kluczowe znaczenie dla tego postępowania. Opinia ta w praktyce będzie stanowić podstawowe uzasadnienie merytoryczne dla decyzji podejmowanej przez organ. Z tego względu kluczowe jest zapewnienie odpowiednio wysokiej jakości merytorycznej analizy.	

			Skład Kolegium ma co do zasady charakter polityczny (art. 66 ust. 1 ustawy). Z tego względu zasadne jest, by udział w procesie analizy – poza członkami Kolegium – zapewniony został także podmiotom eksperckich, aktywnym na rynku i najlepiej znających bieżące uwarunkowania techniczne i rynkowe Z perspektywy ekonomiki postępowania, zasadne jest także uwzględnienie w składzie zespołu pracującego nad opinią, także samego dostawcy, którego postępowanie dotyczy. Umożliwi to bieżące udzielanie wyjaśnień, przedstawianie dokumentów czy dodatkowych informacji. Udział dostawcy umożliwi mu bieżącą korektę w obszarach wiążących się z ryzykiem zakwestionowania oraz przygotowanie się z wyprzedzaniem na ewentualną konieczność podjęcia kroków naprawczych (w razie wydania decyzji o uznaniu za dostawcę wysokiego ryzyka). Proponowana zmiana skorelowana jest z propozycją opisaną w pkt 33.	
24	Art. 1 pkt 50 dot. art. 66a uKSC		OCENA WYSOKIEGO RYZYKA – przesłanki wszczęcia postępowania Uwaga: Za istotne postrzegamy doprecyzowanie okoliczności w jakich Minister może wszcząć postępowanie dot. oceny ryzyka związanego z dostawcą. Przesłanka ta jest określona bardzo szeroko i w naszej ocenie nie określa w sposób wystarczający przyczyn zainicjowania postępowań, które w istotny sposób oddziaływają na prowadzenie działalności w sektorze komunikacji elektronicznej. Propozycja 1: Proponujemy doprecyzowanie, że wszczęcie postępowania może nastąpić w szczególności w przypadku **gdy wystąpił lub istnieje zagrożenie wystąpienia incydentu krytycznego,** który rozumiany jest jako: *incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV*; Bieżące zarządzanie sytuacją związaną z incydentem krytycznym następowałoby w ramach instytucji poleceń lub ostrzeżeń. Procedura oceny i wykluczeń, jako najdalej idąca, stosowana byłaby zgodnie z zasadą proporcjonalności jako ostateczne rozwiązanie wynikające z realnego i potwierdzone zagrożenia o dużej skali i potencjalnym oddziaływaniu.	

			Propozycja 2: W art. 1 pkt 50 przepis art. 66a ust. 1 i 2 otrzymuje brzmienie: „Art. 66a. 1. *Minister właściwy do spraw informatyzacji, w celu ochrony ważnego interesu państwowego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, gdy istnieją konkretne dowody lub uzasadnione podejrzenia, że sprzęt lub oprogramowanie określonego dostawcy zagraża bezpieczeństwu narodowemu, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania o którym mowa w ust. 2, wykorzystywanych przez operatora strategicznej sieci bezpieczeństwa, za dostawcę wysokiego ryzyka, zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka”.* *2. Dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT o funkcjach krytycznych*” Alternatywnie proponuje się, by postępowanie wszczynane było, jeśli zaistnieją **konkretne dowody lub uzasadnione podejrzenia, że określony dostawca zagraża bezpieczeństwu narodowemu.** Aktualnie projektowane brzmienie przepisu nie określa przesłanek wszczęcia postępowania, pozostawiając organowi bardzo dużą dowolność w tym obszarze. W konsekwencji może pojawić się ryzyko wszczynania postępowań bezpodstawowych (nieuzasadnionych) i ponoszenia w związku z tym kosztów obciążających budżet. Przede wszystkim jednak tak szerokie ujęcie będzie negatywnie wpływać na poziom zaufania do właściwego organu przez uczestników rynku – zarówno po stronie producentów sprzętu lub oprogramowania jak i podmiotów je nabywających. Proponowana zmiana zapewni, że prowadzone będą postępowania uzasadnione konkretnymi dowodami na zagrożenia bezpieczeństwa narodowego lub uzasadnionymi (a więc znajdującymi poparcie w danych okolicznościach) podejrzeniami, co zniweluje opisane wyżej ryzyka.	
25	Art. 1 pkt 50 dot. art. 66a uKSC		OCENA WYSOKIEGO RYZYKA – strony postępowania Nowy art. 66a ust. 4 w związku z wyłączeniem stosowania art. 28 KPA zmierza do zawężenia zakresu potencjalnych stron postępowania jedynie do podmiotu wobec, które zostało ono wszczęte, a więc dostawcy. Świadczy o tym również zbyt wąsko określony sposób informowania o wszczęciu postępowania. Ograniczany jest również udział organizacji społecznych o którym mowa w art. 31 KPA.	

			W naszej ocenie podmioty, które będą objęte skutkami wydawanych decyzji mogłyby być stroną postępowania w myśl art. 28 KPA i taką ogólną regulację należałoby utrzymać. Postulujemy więc wykreślenie lub odpowiednią modyfikację projektowanego ust. 4 oraz ograniczeń w zakresie stosowania KPA wskazanych w ust. 3 Brak właściwego zawiadomienia stron może skutkować istotnymi wadami prowadzonego postępowania. Stąd podtrzymujemy nasze propozycje dotyczące zapewnienia, że informacja o wszczęciu postępowania będzie powszechnie dostępna i nie będzie istniało ryzyko, że podmioty posiadające interes prawny lub których obowiązków decyzja może dotyczyć nie miałyby wiedzy o wszczętym postępowaniu administracyjnym, a tym samym nie mogłyby w praktyce korzystać ze statusu strony prowadzonego postępowania. Ponadto postuluje się, by postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dotyczyło dostawcy, który dostarcza sprzęt lub oprogramowanie o funkcjach krytycznych, a nie każdy rodzaj sprzętu. Obecne brzmienie przepisu umożliwia bowiem prowadzenie postępowania także w kontekście sprzętu lub oprogramowania, które nie mają i nie mogą mieć znaczenia dla ochrony bezpieczeństwa. Aktualnie projektowany zakres możliwego postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest niezwykle szeroki i obejmuje w praktyce każdego producenta, dystrybutora lub importera produktów, usług lub procesów ICT lub produktów i usług dla infrastruktury telekomunikacyjnej. W raporcie Grupy Współpracy ds. Bezpieczeństwa Sieci i Informacji z postępów państw członkowskich we wdrażaniu zestawu narzędzi UE w zakresie cyberbezpieczeństwa 5G z lipca 2020 r. wskazano, że zdefiniowanie kluczowych aktywów podlegających ograniczeniom jest jednym z głównych wyznaczników skutecznej realizacji działania strategicznego SM03[1]. W skoordynowanej ocenie ryzyka UE zidentyfikowane zostały najbardziej wrażliwe aktywa (np. funkcje sieci bazowej, funkcje zarządzania siecią i orkiestracji oraz funkcje sieci dostępu) oraz główne kryteria, które należy wziąć pod uwagę przy ocenie wrażliwości różnych aktywów[2]. W myśl powyższego proponowana zmiana doprecyzowuje, że postępowanie powinno dotyczyć sprzętu lub oprogramowania o funkcjach krytycznych – co jest spójne z wytycznymi zawartymi w EU 5G Toolbox[3]. Pozwoli także uchronić się przed zarzutem naruszenia zasady	

[1]https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, s. 11 i 16.
[2] Zob. raport NIS Cooperation Group z 9 października 2019 r. *EU coordinated risk assessment of the cybersecurity of 5G networks*, pkt. 2.20 i 2.21, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.
[3] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, styczeń 2020

			proporcjonalności, którego ryzyko generuje aktualnie projektowane brzmienie przepisu. W kontekście sposobu identyfikowania funkcji krytycznych – por. uzasadnienie do pkt 26. [**podmioty korzystające z rozwiązań ICT o funkcjach krytycznych**] Zgodnie z projektowanym brzmieniem, katalog podmiotów, korzystających ze sprzętu i oprogramowania potencjalnie objętego postępowaniem, obejmować będzie tysiące podmiotów prawa prywatnego i publicznego (operatorzy usług kluczowych, dostawcy usług cyfrowych, jednostki sektora finansów publicznych wymienione w ustawie – w tym jednostki samorządu terytorialnego, itd.). Także w tym zakresie projekt stwarza ryzyko zarzutu naruszenia zasady proporcjonalności. Skoro bowiem ustawodawca zakłada utworzenie operatora strategicznej sieci bezpieczeństwa – OSSB – i powierza mu niezwykle szeroko zdefiniowane zadania, kluczowe dla bezpieczeństwa Państwa (art. 76a ust. 2). – uzasadnione jest, by omawiana regulacja w sprawie uznania za dostawcę wysokiego ryzyka odnosiła się właśnie do OSSB, bez generowana dodatkowych obciążeń dla innych uczestników rynku. Strategiczna sieć bezpieczeństwa jest bowiem stworzona właśnie w celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji (art. 76a ust. 1). Odniesienie postępowania w sprawie uznania za dostawcę wysokiego ryzyka do sprzętu lub oprogramowania, z którego korzysta OSSB, w świetle obszernego katalogu zadań przypisanych OSSB, będzie wystarczające dla zapewnienia podstawowego celu regulacji jakim jest wzmacnianie bezpieczeństwa państwa.	
26	Art. 1 pkt 50 dot. art. 66a uKSC		OCENA WYSOKIEGO RYZYKA – badanie urządzenia lub oprogramowania Postulujemy wprowadzenie jako obligatoryjnego etapu postępowania przeprowadzenie oceny o której mowa w art. 33 KSC, tj. badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Takie badanie powinno dostarczać istotnych informacji z punktu widzenia oceny technicznej.	

27	Art. 1 pkt 50 dot. art. 66a ust. 3 uKSC		**W art. 1 pkt 50 w dodanym art. 66a ust. 3 skreśla się następujący fragment:** *„z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy”.* **Uzasadnienie:** Obecna wersja Projektu ogranicza możliwość udziału na prawach strony innych podmiotów, np. operatorów telekomunikacyjnych (art. 28 k.p.a.), wyklucza możliwość dopuszczenia do udziału w postępowaniu zainteresowanych organizacji społecznych (art. 31 k.p.a.), czy wreszcie uprawnienia strony w zakresie przeprowadzenia czynności dowodowych (art. 79 k.p.a.). Poprzednie wersje Projektu nie przewidywały tak daleko idących ograniczeń dla uczestników postępowania. Proponowane rozwiązanie stanowi daleko idące ograniczenie podstawowych praw przewidzianych dla uczestników postępowania w przepisach powszechnie obowiązujących i może skutkować naruszeniem podstawowych zasad rzetelnego postępowania. W szczególności niepokojący jest projekt wyłączenia stosowania art. 28, 31 i 79 KPA. **Wyłączenie stosowania art. 28 i 31 KPA** Zgodnie z uzasadnieniem Projektu: *„Zawężenie przymiotu strony oraz udziału organizacji społecznej jest koniecznej w celu uniknięcia obstrukcji postępowania i wzmocnić trwałość rozstrzygnięć, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania”.* Takie uzasadnienie nie przekonuje i stwarza bardzo duże ryzyka w kontekście ograniczania sprawiedliwości proceduralnej podmiotów rynku. Powyższa argumentacja może być bowiem zastosowana dla wyłączenia wskazanych przepisów w każdej sprawie, wskazując na konieczność zapewnienia trwałości rozstrzygnięcia i uniknięcia obstrukcji. Tymczasem w szczególności z uwagi na szczególną wagę postępowania w sprawie uznawania za dostawcę wysokiego ryzyka – i jego bardzo daleko idące skutki rynkowe i potencjalnie społeczne, niezbędne jest zapewnienie udziału w postępowaniu podmiotów, na których prawa i obowiązki oddziaływać będzie decyzja, jak również zapewnić udział strony społecznej. Nie sposób nie zauważyć, iż wyłączenie stosowania art. 28 k.p.a. oraz zdefiniowanie nowego pojęcia „strony” w myśl proponowanego brzmienia art. 66a ust. 4 (wskazane w art. 1 pkt 50 projektu) implikuje ryzyko nie tylko zbyt skrajnego ograniczenia, ale także całkowitego wyłączenia możliwości ochrony praw przez podmioty związane decyzją w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka, ale niemieszczące się w pojęciu „strony” w	

			brzmieniu proponowanym przez projektodawcę w art. 1 pkt 50 niniejszego projektu. O ile stosowanie szczególnych względem k.p.a. definicji strony w aktach prawnych regulujących szczegółowe obszary gospodarki jest zjawiskiem występującym w systemie postępowania administracyjnego, o tyle należy zwrócić uwagę na daleko idące, *de facto*, zrównanie pojęcia strony z „podmiotem wobec którego zostało wszczęte postępowanie", które uniemożliwia udział w postępowaniu podmiotom, których prawa i obowiązki będą kształtowane przez wydaną w toku takiego postępowania decyzję. Wbrew zatem stanowi faktycznemu, stroną postępowania będzie tylko podmiot formalnie wskazany jako strona przez organ wszczynający postępowanie, a więc tylko od woli organu wszczynającego postępowanie będzie zależeć, kto będzie stroną postępowania – ze wszystkimi tego procesowymi konsekwencjami, w tym możliwością lub brakiem możliwości ochrony swoich praw. Prawo do rzetelnego postępowania administracyjnego (w szczególności – prawo do przedstawienia swojej argumentacji, do obrony oraz do uczestnictwa w postępowaniu, którego wynik decyduje o prawach bądź obowiązkach) należy wywodzić z wartości konstytucyjnych oraz międzynarodowych – w szczególności z prawa do sądu oraz zasady demokratycznego państwa prawa[4]. Ograniczanie praw podmiotów powinno być każdorazowo badane z perspektywy art. 31 ust. 3 Konstytucji RP, który wskazuje wprost, iż ograniczenia konstytucyjnych wolności i praw nie mogą naruszać samej istoty tych wolności i praw. Proponowane w Projekcie wyłączenie stosowania art. 28 k.p.a. naruszy istotę prawa do korzystania z uprawnień strony oraz prawa do czynnego uczestnictwa w postępowaniu względem podmiotu lub podmiotów będących adresatami obowiązków wynikających z przedmiotowej decyzji. Redukcja tak głębokiej ingerencji w uprawnienia podmiotów posiadających interes prawny w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka byłaby również możliwa przez rozszerzenie statusu strony postępowania także o podmioty wskazane w art. 66b ust. 1 w związki z objęciem ich konsekwencjami wydania decyzji, które projektodawca przedstawia w pkt 1 i 2 powyższego przepisu. Rozwiązanie to również wydaje się słuszne z punktu widzenia ochrony interesów stron oraz chęci uniknięcia obstrukcji postępowania przez projektodawcę, wskazanego w uzasadnieniu projektu. **Wyłączenie stosowania art. 79 kpa** Projekt wyłącza regulację KPA gwarantującą stronie możliwość udziału w postępowaniu dowodowym w odniesieniu do przesłuchania świadków i biegłych czy przeprowadzania	

[4] J. Szremski, Prawo do postępowania administracyjnego i jego elementy jako wartości wynikające z uregulowań konstytucyjnych, międzynarodowych oraz europejskich, Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury, Zeszyt 2 (42)/2021, s. 38.

			oględzin. W połączeniu z pozostałymi ograniczeniami praw proceduralnych (por. uwagi powyżej oraz pkt 7-8, 17-18), strona zostanie faktycznie pozbawiona realnego wpływu na postępowanie i przedstawienie swojej argumentacji. Proponowane rozwiązanie stanowi zaprzeczenie zasad ogólnych postępowania administracyjnego, które mają **umocowanie konstytucyjne**, zwłaszcza przy uwzględnieniu potencjalnej możliwości wyłączenia jawności niektórych dokumentów na podstawie art. 74 kpa. Tak daleko idące ograniczenia nie mają żadnego uzasadnienia – nawet bowiem powołanie się na względy bezpieczeństwa narodowego nie pozwalają na odebranie stronie konstytucyjnego prawa do obrony. **Z tego względu wskazane wyłączenie powinno zostać usunięte.** W praktyce mogą wystąpić okoliczności uzasadniające wyłączenie jawności określonych czynności – w przypadku, gdy takie ujawnienie byłoby sprzeczne z obowiązującym prawem (w szczególności w zakresie informacji niejawnych) lub z prawem międzynarodowym. W żadnym jednak wypadku ograniczenie udziału strony w postępowaniu dowodowym nie powinno być zasadą, a rozstrzygnięcie organu o wyłączeniu możliwości udziału w czynnościach powinno być mieć charakter zaskarżalnego postanowienia na zasadach ogólnych.	
28	Art. 1 pkt 50 dot. art. 66a ust. 4 uKSC		**W art. 1 pkt 50 w art. 66a skreśla się projektowany ust. 4.** **Uzasadnienie:** Proponowana zmiana jest skorelowana z postulatem wykreślenia wyłączenia stosowania art. 28 KPA (por. pkt 5 powyżej). Usunięcie ust. 4 umożliwi bezpośrednie stosowanie przepisów KPA odnoszących się do pojęcia „strony postępowania". Obecna treść art. 66a ust. 4 zawęża pojęcie strony tylko do tego wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Przyjęcie takiej definicji względem art. 28 k.p.a. zawierającego znacznie szersze znaczenie strony może nieść ze sobą wyłączenie możliwości ochrony praw podmiotów, których obowiązki zostaną ukształtowane w wyniku wydania decyzji w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. W tym kontekście por. uwagi do pkt 6 powyżej.	
29	Art. 1 pkt 50 dot. art. 66a ust. 6 uKSC		**W art. 1 pkt 50 w projektowanym art. 66a skreśla się ust. 6** **Uzasadnienie:** Projekt przewiduje we wskazanym punkcie brak obowiązku doręczenia zawiadomienia o wszczęciu postepowania podmiotom spoza UE / EFTA/ Konfederacji Szwajcarskiej, co	

			stanowi istotne odstępstwo od zasad ogólnych kpa. W uzasadnieniu Projektu brak w tym zakresie wyjaśnienia przyczyn przyjętego podejścia. Obecne brzmienie stwarza ryzyko dyskryminacji podmiotów spoza wskazanych regionów (w tym w szczególności podmiotów położonych w Ameryce Północnej lub Azji, w których działa cały szereg dostawców rozwiązań ICT, potencjalnie objętych regulacją). Zważywszy, że projekt przewiduje względem takich podmiotów opublikowanie informacji o postępowaniu jedynie na stronie podmiotowej BIP organu (potencjalnie – wyłącznie w języku polskim), występuje bardzo wysokie ryzyko braku realnej możliwości uzyskania informacji o prowadzanym postępowaniu przez zainteresowany podmiot. Stanowi to zaprzeczenia podstawowej zasady postepowania administracyjnego polegającej na zapewnieniu stronie czynnego udziału w postępowaniu. Może być także sprzeczne z umowami międzynarodowymi, których stroną jest Rzeczpospolita Polska (w szczególności umów popieraniu i wzajemnej ochronie inwestycji, a potencjalnie także Porozumienia o Wolnym Handlu GATT).	
30	Art. 1 pkt 50 dot. art. 66a ust. 7 uKSC		W art. 1 pkt 50 w art. 66a ust. 7 nadaje się następujące brzmienie: *„W przypadku wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka, minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy.”* Uzasadnienie: Wbrew treści uzasadnienia ustawy, zgodnie z obecnym brzmieniem projektu opinia Kolegium nie będzie sporządzana „każdorazowo”, a jedynie w przypadku, w którym postępowanie w sprawie uznania za dostawcę wysokiego ryzyka zostało wszczęte z urzędu. W przypadku wszczęcia postępowania na wniosek przewodniczącego Kolegium, brak jest ustawowej gwarancji zapewniającej, że także w tym wypadku rozstrzygnięcie zostanie poprzedzone pogłębioną analizą wszystkich mających znaczenie okoliczności. Potencjalnie takie rozwiązanie stwarza też ryzyko wykorzystywania wskazanego ograniczenia jako furtki pozwalającej na pominięcie kroku w postaci uzyskania opinii Kolegium. Opinia ta ma tymczasem kluczowe znaczenie z perspektywy rozstrzygnięcia i kształtowania podejścia do cyberzagrożeń.	

			W naszej ocenie, sam fakt wszczęcia postępowania na wniosek przewodniczącego Kolegium nie oznacza jeszcze, że taka analiza została sporządzana, a nawet jeśli tak – nie gwarantuje jej zawartości ani formy sporządzenia, nie wywołuje też żadnych skutków w postępowaniu (teoretycznie – nie musi nawet zostać uwzględniona przez organ wydający decyzję). W odniesieniu do propozycji usunięcia wyłączenia stosowania art. 106 § 5 kpa, to należy przypomnieć, że zgodnie z tym przepisem, zajęcie stanowiska przez ten organ następuje w drodze postanowienia, na które służy stronie zażalenie. Efektem wyłączenia art. 106 § 5 będzie także brak możliwości wniesienia zażalenia na opinię – jej kwestionowanie będzie więc możliwe dopiero na etapie wnoszenia skargi do sądu administracyjnego. Negatywnie wpływać to będzie na ekonomikę procesową i zwiększy ryzyko uchylania decyzji, opartych na opiniach niespełniających wymogów określonych w ustawie, których nie można było zakwestionować na wcześniejszym etapie, bez angażowania drogi sądowej. Wyłączenie w obecnej wersji Projektu stosowania art. 106 § 5 k.p.a. oznacza także brak określenia formy prawnej wydawanej opinii – a w konsekwencji brak możliwości jasnego określenia jej statusu. Niewątpliwie opinia będzie mieć faktyczną wartość dowodową – kluczową dla wydania decyzji, nie jest jednak jasne, by będą stosować się do niej pozostałe przepisy kpa odnoszące się do stanowisk organów wydawanych w toku postępowania administracyjnego. Takie rozwiązanie będzie powodować duże wątpliwości praktyczne w zakresie skutków wydania opinii (lub braku jej wydania w terminie) na przebieg postępowania.	
31	Art. 1 pkt 50 dot. art. 66a ust. 8 uKSC		W celu uzupełnienia zakresu opinii postulujemy: • W zakresie w jakim ocena ma odnosić się do incydentów (pkt 4) zasadne jest wprowadzenie także przesłanki istotności skutku zakłócającego potencjalnego incydentu. • Uzasadnionym byłoby również zasięgnięcie także opinii aktualnych lub potencjalnych podmiotów korzystających z objętych oceną produktów, usług lub procesów ICT. Mogłaby ona wskazać na bezpośrednią ocenę ryzyka w realnie funkcjonujących sieciach i systemach teleinformatycznych. Przedstawienie takiej opinii powinno być ze strony użytkownika dobrowolne. • Postulujemy również, aby elementem analizy było ustalenie zakresu stosowania danych produktów, usług i procesów ICT co będzie miało także podstawowe znaczenie dla określenia stron postępowania dot. oceny. Zakres tych stron będzie bowiem	

			potencjalnie istotnie wykraczał poza samego dostawcę oraz Ministra, a z uwagi na konsekwencje wydawanej decyzji będzie też obejmował podmioty objęte bezpośrednio skutkami wydanej decyzji. **W art. 1 pkt 50 w art. 66a ust. 8 punkt 2 otrzymuje brzmienie:** *„2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:* *a) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności tam gdzie nie zostały zawarte umowy międzynarodowe w zakresie ochrony tych danych między Unią Europejską i tym państwem, lub czy dostawca sprzętu lub oprogramowania przestrzega postanowień rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* *b) struktury własnościowej dostawcy sprzętu lub oprogramowania, w tym z uwzględnieniem informacji o dostawcy z Centralnego Rejestru Beneficjentów Rzeczywistych, zgodnie z przepisami prawa polskiego lub odpowiedniego właściwego rejestru prowadzonego przez państwo członkowskie Unii Europejskiej.* **Uzasadnienie:** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci telekomunikacyjnych, pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci telekomunikacyjnych, w oparciu o niedookreślone kryteria, które nie zawierają rzeczywistych elementów analizy technicznej. Projekt w art. 66a ust. 8 wśród kryteriów oceny wymienia kryteria ocenne i niezwykle szerokie, w szczególności ocenę przepisów prawa regulujących stosunki pomiędzy dostawcą a państwem oraz praktyki stosowania prawa w tym zakresie (art. 66a ust. 8 pkt 2 lit a Projektu). Brak jest wskazówek co do standardu dowodu wymaganego do oceny zagrożeń, wpływu państwa trzeciego, wagi podatności na zagrożenia i incydentów oraz stopnia kontroli procesu produkcji i dostawy (art. 66a ust. 4 Projektu). W naszej ocenie proponowane podejście nie będzie w praktyce możliwe do poddania merytorycznej kontroli. Z uwagi na brak precyzji sformułowań, zakres swobody pozostawiony Kolegium nie znajduje uzasadnienia w świetle celu jakim jest zapewnienie bezpieczeństwa publicznego. Nie daje też wystarczających gwarancji ograniczenia ryzyka dyskryminacji, co będzie wpływało negatywnie na poziom zaufania adresatów regulacji do organów państwa.	

			Proponowane zmiany (wraz ze zmianami opisanymi w pkt 10 poniżej) ograniczają arbitralność regulacji w tym zakresie, jednocześnie zapewniając Kolegium odpowiednio szerokie możliwości weryfikacji. Propozycja są skorelowane ze zmianami proponowanymi w pkt XX w zakresie włączenia w proces analizy podmiotów eksperckich oraz samego zainteresowanego.	
32	Art. 1 pkt 50 dot. art. 66a ust. 8 (uzupełnienie) uKSC		**W art. 1 pkt 50 w art. 66a ust. 8 po punkcie 6 dodaje się następujące postanowienia:** *„7) treści deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, przedkładanej operatorom telekomunikacyjnym oraz aktualizowanej nie rzadziej niż co dwa lata, która powinna w szczególności zawierać:* *a) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;* *b) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;* *c) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej polegające na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;* *d) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;* *e) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;* *f) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;* *g) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa;* *8) zobowiązania do zapewnienia integralności dostarczanych krytycznych składników infrastruktury, a w szczególności w zakresie:*	

			a) możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu; *b) sprawdzenia w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione;* *9) zobowiązania prowadzenia monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;* *10) zobowiązania zatrudniania tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie;* *11) zobowiązania uzyskania przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego;* *12) zobowiązania zapewnienia przez producenta ciągłości dostaw*". **Uzasadnienie:** Projekt znacząco ogranicza ilość kryteriów oceny umożliwiających ocenę sprzętu lub oprogramowania pod względem technicznym bezpieczeństwa infrastruktury, czyli weryfikacji za pomocą mierzalnych technicznych kryteriów, bezpieczeństwa tej infrastruktury (art. 66a ust. 8 pkt 4-6 Projektu). Proponowane aktualnie kryteria nie składają się na systemowe, spójne rozwiązanie i należy obawiać się, że nie będą w praktyce odgrywać istotnej roli w procesie decyzyjnym. Tymczasem zalecenia Komisji europejskiej odnoszące się do wdrażania rozwiązań 5G Toolbox jednoznacznie przewidują, że ocena ryzyka dostawców powinna być niedyskryminująca a „*ocena profili ryzyka dostawców była prowadzona wyłącznie ze względów bezpieczeństwa i na podstawie obiektywnych kryteriów*"[5]. Przedstawione w propozycji uzupełnienia tego artykułu o techniczne kryteria oceny są ze sobą powiązane i tworzą spójny model ochrony bezpieczeństwa infrastruktury. Model ten charakteryzuje się obiektywnością weryfikacji kryteriów i bardzo dużym stopniem profesjonalizacji weryfikacji, gwarantującej poprawność wyników stosowanych kryteriów oceny. Kryteria *pozatechnologiczne*, bardzo często są niedefiniowalne i posługują się niedookreślonymi pojęciami, które są bardzo trudne do zweryfikowania i dokonania oceny. Nie powinny więc odgrywać kluczowej roli w procesie decyzyjny. Proponowane rozwiązania, zgodnie z najlepszymi praktykami, obejmują m.in: • Uzyskanie deklaracji dostawcy odnoszącej się do wszystkich kwestii istotnych z punktu widzenia zapewnienia bezpieczeństwa. Konkretna treść deklaracji powinna być ustalana pomiędzy przedsiębiorcą telekomunikacyjnym a dostawcą lub producentem	

[5] Komunikat z dnia 29 stycznia 2020 r. Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, „*Bezpieczne wdrażanie 5G w UE - Wdrażanie zestawu narzędzi 5G*", COM (2020) 50 final, s. 9, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0050&from=FR.

			w każdym indywidualnym przypadku. W propozycji uzupełnienia przepisu podany jest tylko przykładowy wykaz zawartości deklaracji wiarygodności danego dostawcy lub producenta; • Zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu. • Zapewnienie monitoringu bezpieczeństwa infrastruktury w celu ciągłego identyfikowania zagrożeń i zapobiegania im. Monitoring bezpieczeństwa infrastruktury powinien obejmować wszystkie krytyczne składniki infrastruktury telekomunikacyjnej, a w szczególności te składniki, które przekazują dane osobowe zewnętrznym kontrahentom, np. w związku z roamingiem. Powinny być przygotowane odpowiednie procedury monitoringu bezpieczeństwa. Zatrudnienie odpowiedniego personelu technicznego posiadającego stosowne kompetencje, z uwagi na postępowanie z krytycznymi składnikami infrastruktury i regularnie szkolonego.	
33	Art. 1 pkt 50 dot. art. 66a ust. 10 pkt 1 uKSC		**W art. 1 pkt 50 w art. 66a ust. 10 do punktu 1 dodaje się zdanie w następującym brzmieniu:** *„oraz przedstawiciele operatora strategicznej sieci bezpieczeństwa, który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie*” Alternatywnie – w razie brak uwzględnienia uwagi zawartej w pkt 5 w zakresie odniesienia decyzji wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB: *„oraz przedstawiciele podmiotów wskazanych w pkt 66a pkt 1) – 4), które nabywają lub posiadają produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie*” **Uzasadnienie:** Proces analizy ma charakter krytyczny dla postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Opinia Kolegium stanowi faktyczną podstawę merytoryczną dla wydania decyzji przez właściwy organ. Zasadne jest, by w jej przygotowaniu wzięli udział nie tylko członkowie Kolegium, będącego – z definicji – organem politycznym, ale także podmioty działające na rynku, posiadające odpowiednie doświadczenie merytoryczne i znajomość uwarunkowań rynkowych oraz posiadające szeroką wiedzę w obszarze cyberzagrożeń. Z	

			tego względu proponuje się rozszerzyć katalog podmiotów uczestniczących w procesie o przedstawicieli podmiotu lub podmiotów potencjalnie dotkniętych decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka, jak również właściwe izby gospodarcze lub stowarzyszenia o podobnym profilu. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma specyficzny charakter i wywiera dalekosiężne skutki. Zasadne jest więc także uwzględnienie w składzie zespołu pracującego nad opinią, także samego dostawcy, którego postępowanie dotyczy. Umożliwi to bieżące udzielanie wyjaśnień, przedstawianie dokumentów czy dodatkowych informacji. Udział dostawcy umożliwi mu bieżącą korektę w obszarach wiążących się z ryzykiem zakwestionowania oraz przygotowanie się z wyprzedzaniem na ewentualną konieczność podjęcia kroków naprawczych (w razie wydania decyzji o uznaniu za dostawcę wysokiego ryzyka). Propozycja skorelowana z propozycją zawartą w pkt 21 powyżej.	
34	Art. 1 pkt 50 dot. art. 66a ust. 10 pkt 5 uKSC		**W art. 1 pkt 50 w art. 66a ust. 10 punkt 5 otrzymuje następujące brzmienie:** *„uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji oraz dostawcy sprzętu i oprogramowania, którego dotyczy ta opinia”* **Uzasadnienie:** O treści opinii powinien być poinformowany ten, kogo dotyczy ta opinia, czyli dostawca sprzętu lub oprogramowania, którego dotyczy postępowanie. Zmiana skorelowana jest z propozycjami odnoszącymi się do zwiększenia udziału dostawcy w postępowaniu, w tym w procesie sporządzania opinii, a także z postulatem zwiększenia przejrzystości postępowania w stosunku do dostawcy, którego ono dotyczy. Przekazanie uzgodnionej opinii dostawcy pozwoli mu z wyprzedzeniem poczynić przygotowania do opracowania planu naprawczego lub innych działań niwelujących zidentyfikowane cyberzagrożenia.	
35	Art. 1 pkt 50 dot. art. 66a ust. 10 (uzupełnienie) uKSC		**W art. 1 pkt 50 w art. 66a po ust. 10 dodaje się ust. 10a-10f w następującym brzmieniu:** *10a. W ciągu miesiąca od otrzymania opinii Kolegium, dostawca sprzętu lub oprogramowania, którego dotyczy ta opinia, może przedstawić środki naprawcze i plan naprawczy.*	

			10b. Środki naprawcze powinny wskazywać sposób usunięcia sformułowanych w opinii Kolegium zagrożeń dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. *10c. Plan naprawczy powinien przedstawiać harmonogram realizacji poszczególnych środków naprawczych.* *10d. W przypadku zaakceptowania środków naprawczych i planu naprawczego, Kolegium zmienia ocenę.* *10e. Do czasu zakończenia postępowania w sprawie zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji nie wydaje decyzji o której mowa w art. 66a ust. 11* **Uzasadnienie:** Przepisy Projektu w obecnej wersji nie przewidują żadnych postanowień, które dawałyby możliwość podjęcia właściwych środków naprawczych przez dostawcę, w szczególności umożliwienia takiemu dostawcy usunięcia wskazanych zagrożeń w określonym terminie, Decyzja powinna stanowić *ultima ratio*, czyli być podejmowana dopiero wtedy, gdy inne, mniej dotkliwe, ale możliwe środki naprawcze okazały bezskuteczne. Przepisy Projektu w obecnej wersji nie przewidują żadnych postanowień, które dawałyby możliwość podjęcia właściwych środków naprawczych przez dostawcę sprzętu lub oprogramowania, którego dotyczy postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Zważywszy na daleko idące skutki decyzji – zarówno dla dostawcy, jak i dla jego klientów zobowiązanych do zaprzestania użytkowania rozwiązań objętych decyzją – decyzja powinna stanowić *ultima ratio*, czyli być podejmowana dopiero wtedy, gdy inne, mniej dotkliwe, ale możliwe środki naprawcze okazały bezskuteczne. Wprowadzenie omawianych tu rozwiązań mogłoby zapobiec wydaniu decyzji na podstawie ust. 11, a więc byłoby rozwiązaniem względniejszym zarówno dla dostawców, jak i podmiotów nabywających sprzęt lub oprogramowanie dostawcy. zwłaszcza dla dostawcy i dla operatorów. Biorąc pod uwagę fakt, że wydanie decyzji, na podstawie projektowanego art. 66a ust. 11 będzie stanowić przejaw dużego ograniczenia (o ile nie zupełnego wyłączenia) swobody działalności gospodarczej, to wprowadzenie rozwiązań mniej uciążliwych należy uznać za konieczne w kontekście art. 31 ust. 3 Konstytucji i wywodzonej z tego przepisy zasady proporcjonalności. Prawodawca powinien dążyć do wprowadzenia regulacji, które w jak najmniejszym stopniu ograniczą konstytucyjne wolności i prawa jednostek, a doprowadzą do ochrony tych samych wartości (tu: bezpieczeństwo państwa).	

			Proponowane rozwiązanie jest zbliżone do rozwiązań funkcjonujących w innych państwach członkowskich UE (przykładowo – § 244a fińskiej ustawy o usługach łączności elektronicznej).	
36	Art. 1 pkt 50 dot. art. 66a ust. 11 uKSC		**W art. 1 pkt 50 dodany art. 66a ust. 11 otrzymuje następujące brzmienie:** *„11. Minister właściwy do spraw informatyzacji, w drodze decyzji na okres nie dłuższy niż 24 miesiące, po wcześniejszym jej zaakceptowaniu przez ministra właściwego do spraw rozwoju i technologii, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw obrony narodowej, ministra właściwego do spraw sprawiedliwości oraz wyrażenia pozytywnej opinii przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów, uznaje dostawcę sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi”.* **Uzasadnienie:** Proponowane zmiany odnoszą się do dwóch zagadnień – poszerzenia kręgu podmiotów uczestniczących w wydaniu decyzji o uznaniu za dostawcę wysokiego ryzyka oraz określeniu okresu obowiązywania tej decyzji. W obecnym kształcie decyzja jest podejmowana jednoosobowo przez ministra właściwego do spraw informatyzacji. Z uwagi na wpływ tej decyzji na stosunki międzynarodowe z innymi państwami czy bezpieczeństwo wewnętrzne oraz skomplikowany charakter prawny, powinny uczestniczyć w jej podejmowaniu także inni ministrowie odpowiedzialni za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny, zdrowie i życie ludzi) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia). Będzie to zgodne z analogicznymi rozwiązaniami funkcjonującymi w innych krajach UE. Przykładowo decyzja taka w Niemczech jest podejmowana przy udziale federalnego ministerstwa spraw wewnętrznych, zagranicznych i gospodarki[6]. Pozytywną opinię powinien wyrazić także Prezes Urzędu Ochrony Konkurencji i Konsumentów. Decyzja w sprawie uznania za dostawcę wysokiego ryzyka może bowiem, poprzez ograniczenie możliwości oferowania określonych produktów lub usług przez tego dostawcę, wpływać istotnie na konkurencję na rynku oraz korzystanie z usług przez użytkowników. Konsekwencją takiego – częściowego lub całkowitego – wykluczenia z rynku dostawcy czy dostawców, może być wzrost cen infrastruktury telekomunikacyjnej, a w konsekwencji wzrost cen świadczonych dla indywidulanych klientów usług telekomunikacyjnych.	

[6] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Dziennik Nr 25 z 27.05.2021, s. 1122, https://www.bundesanzeiger-verlag.de/

			Wyłączenie możliwości prowadzenie działalności gospodarczej danego rodzaju (a do tego sprowadzałoby się dla dostawcy wydanie decyzji na podstawie projektowanego art. 66a ust. 11), nie może być przy tym w demokratycznym państwie prawnym bezterminowe. Regulacja powinna w szczególności uwzględniać wpływ bardzo szybkiego rozwoju technologicznego i dynamicznych zmian w zakresie zagrożeń związanych z cyberbezpieczeństwem na aktualność decyzji. Z tego względu w naszej ocenie regulacja powinna wymuszać przegląd aktualnych uwarunkowań, i stosownie do przypadku – dokonanie zmian w wydanej decyzji, wydanie nowej decyzji albo uznanie, że nie zachodzi już potrzeba wydawania w omawianym zakresie kolejnej decyzji. Uregulowania takie występują w innych krajach UE, np. w Austrii	
37	Art. 1 pkt 50 dot. art. 66a ust. 11 uKSC (uzupełnienie)		**W art. 1 pkt 50 w art. 66a po ust. 11 dodaje się ust. 11a-11f w następującym brzmieniu:** *11a. Decyzja, o której mowa w art. 66a ust. 11, powinna wskazywać sposób usunięcia cyberzagrożeń których usunięcie przez dostawcę sprzętu i oprogramowania, spowoduje uchylenie decyzji przez ministra właściwego do spraw informatyzacji.* *11b. W ciągu miesiąca od dnia otrzymania lub ogłoszenia decyzji ministra właściwego do spraw informatyzacji, o której mowa w art. 66a ust. 11, dostawca sprzętu lub oprogramowania, którego dotyczy ta decyzja, powinien przedstawić środki naprawcze i plan naprawczy.* *11c. Środki naprawcze powinny wskazywać sposób usunięcia sformułowanych w decyzji ministra właściwego do spraw informatyzacji zagrożeń dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.* *11d. Plan naprawczy powinien przedstawiać harmonogram realizacji poszczególnych środków naprawczych.* *10e. W przypadku zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji uchyla decyzję.* *11f. Do czasu zakończenia postępowania w sprawie zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji wstrzymuje wykonanie decyzji".* **Uzasadnienie:** W uzupełnieniu propozycji zawartej w pkt 14, proponuje się umożliwienie dostawcy przedstawienie planu naprawczego i środków naprawczych także po wydaniu decyzji. Nie zawsze bowiem przebieg analizy po stronie Kolegium i jego Opinia będą na tyle jasne, by już na etapie sporządzenia opinii możliwe lub zasadne było opracowywanie takich materiałów. Z kolei zaproponowanie po wydaniu decyzji rozwiązań sanacyjnych, podlegających ocenie organu, najpełniej pozwoli urzeczywistnić cel regulacji, jakim jest usuwanie cyberzagrożeń i stałe zwiększanie poziomu bezpieczeństwa państwa, w tym w związku z korzystaniem z dostawców, których rozwiązania ICT wiążą się ze zidentyfikowanymi w postępowaniu ryzykami.	

			Proponowana zmiana zapewnia także, że organ wydając decyzję, będzie wskazywał konkretne uchybienia i konkretne oczekiwania względem dostawcy wysokiego ryzyka. Z jednej strony przyczyni się to do polepszania jakości wydawanych rozstrzygnięć i skłoni organ do opracowania uzasadnienie decyzji dokładnie i precyzyjnie, z drugiej – wzmocni oparty na zaufaniu dialog pomiędzy organem a dostawcę, nakierowany na osiągnięcie celu w postaci minimalizacji ryzyk cybernetycznych.	
38	Art. 1 pkt 50 dot. art. 66a ust. 12 uKSC		Wprowadzenie ustawowej zasady, iż decyzja określona w ust. 8 podlega natychmiastowej wykonalności jest rozwiązaniem zbyt daleko idącym. Ponieważ do decyzji tej mają zastosowanie przepisy KPA wystarczające byłoby odniesienie o możliwości nałożenia rygoru natychmiastowej wykonalności dla przedmiotowych decyzji ale dopiero po przeprowadzeniu analizy czy taki rygor należy nałożyć. Wprowadzenie automatyzmu w tym zakresie ograniczy możliwości działania Ministra wydającego decyzję, o której mowa w ust. 8, który być może nie uznawałby za uzasadnione nadawanie takiego rygoru absolutnie wszystkim decyzjom wydawanym w zakresie uznania dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego. **W art. 1 pkt 50 dodany art. 66a ust. 12 otrzymuje następujące brzmienie:** *„12. Decyzja, o której mowa w ust. 11, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT o funkcjach krytycznych pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka”.* **Uzasadnienie:** Wyłączna zmiana w przepisie art. 66a ust. 12, polega na dodaniu po słowach „*konkretnych procesów ICT*” słów „*o funkcjach krytycznych*”. Zmiana ta powodowana jest koniecznością zapewnienia spójności z pozostałymi propozycjami i jest skorelowana ze zmianami proponowanymi w pkt 4 powyżej.	
39	Art. 1 pkt 50 dot. art.		OCENA WYSOKIEGO RYZYKA – natychmiastowe wykonanie	

	66a ust. 14 uKSC		Sygnalizujemy ogromne ryzyko wiążące się z przyznaniem decyzji niewzruszalnej przez sąd natychmiastowej wykonalności. Decyzja wiąże się bowiem z określonymi realnymi skutkami dla podmiotów, które według aktualnego projektu nie biorą żadnego udziału na etapie poprzedzającym postępowanie administracyjne, we właściwym postępowaniu administracyjnym, przy jednoczesnym braku postępowania odwoławczego. To oznacza, że nie muszą nawet wiedzieć o prowadzonym postępowaniu, a nawet wiedząc to nie mogą uzyskać informacji o jego przebiegu. Należy mieć świadomość, że z perspektywy takich podmiotów decyzja administracyjna wydana wobec dostawcy będzie miała skutki zbliżone do skutków uchwalenia przepisów powszechnie obowiązujących, tj. będzie stanowiła normę nakazującą pewne zachowania podmiotu niebędącego stroną postępowania, ani adresatem decyzji. Pomijając formalne rozważania nad taką konstrukcją należy zapewnić jako minimalne zabezpieczenie praw podmiotów obowiązanych, w tym interesów w toku, aby istniał czas na przygotowanie się do wdrożenia decyzji. Natychmiastowa wykonalność decyzji – jako zasada, nie zaś wyjątek – może ograniczać prawa strony do sprawiedliwego i rzetelnego procesu i stać w sprzeczności z założeniami KPA. Zgodnie z przepisami KPA, rygor natychmiastowej wykonalności może zostać nadany decyzji w przypadku, gdy jest to niezbędne ze względu na ochronę zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony. W każdym jednak wypadku to na organie wydającym decyzję leży obowiązek wskazania – i wykazania występowania – przesłanek uzasadniających zastosowanie tego mechanizmu. Rygor natychmiastowej wykonalności decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (art. 66a ust. 11) przy jednoczesnym wyłączeniu możliwości wstrzymania wykonania zaskarżonej decyzji przez sąd administracyjny (art. 66d ust. 3) praktycznie uniemożliwia jakiekolwiek ograniczanie negatywnych skutków decyzji dla dostawcy i brak możliwości kontroli w tym zakresie prawidłowości decyzji przez sąd. Rygor natychmiastowej wykonalności, w połączeniu z przewidzianym w Projekcie zakazem wstrzymania wykonalności decyzji w sprawie dostawcy wysokiego ryzyka (art. 66d ust. 3 Projektu), doprowadzi do natychmiastowego rozpoczęcia po stronie podmiotu lub podmiotów do tego zobowiązanych zgodnie z art. 66b procesu wycofywania sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Od momentu wydania takiej decyzji będzie musiał rozpocząć się proces usuwania sprzętu dostawcy już wykorzystywanego , a także – co następuje	

			natychmiast – sprzęt od dostawcy nie będzie mógł być nabywany przez podmiot lub podmioty wskazane w ustawie. Dla zaistnienia i w wielu przypadkach skonsumowania takich skutków nie będzie miało znaczenia nawet późniejsze korzystne rozstrzygnięcie sądowe (skoro z uwagi na rygor natychmiastowego wykonania decyzji, sprzęt zostanie usunięty lub nie zostanie już zakupiony). Nadanie rygoru natychmiastowej wykonalności powinien więc następować każdorazowo po rozważeniu przesłanek ustawowych określonych w kpa, a postanowienie w tym zakresie powinno podlegać zaskarżeniu na zasadach ogólnych. W obecnej postaci – zwłaszcza wobec wyłączenia możliwości wstrzymania wykonalności decyzji przez sąd zgodnie z projektowanym art. 66d ust. 3 – środek ten może być sprzeczny z podstawowym – gwarantowanym konstytucyjnie i traktatowo – prawem do sprawiedliwego rozpatrzenia sprawy przez sąd (art. 45 ust. 1 w zw. z art. 31 ust. 3 Konstytucji, art. 47 w zw. z art. 52 ust. 1 i 3 Karty Praw Podstawowych UE i art. 6 w zw. z art. 13 Europejskiej Konwencji Praw Człowieka - EKPC). Postulujemy, aby w decyzji wprowadzany był swoisty „vacatio legis" określający, że decyzja powoduje skutki prawne po adekwatnym do danej sytuacji terminie, który w żadnym przypadku nie powinien być krótszy niż 6 miesięcy. Alternatywnie rekomendowane jest stosowanie zasad ogólnych wynikających z KPA.	
40	Art. 1 pkt 50 dot. art. 66a uKSC		OCENA WYSOKIEGO RYZYKA – przeglądy wydanych decyzji (uwaga alternatywna do pkt 36) W naszej ocenie wydanie decyzji musi podlegać rewizji w czasie. W związku ze zmianą sytuacji stanowiącej podstawę do wydania danego rozstrzygnięcia doprecyzowania w przepisach wymagałoby przynajmniej wprowadzenie okresowych przeglądów wydanych decyzji. W art. 66a dodaje się ust. 16 i 17 w brzmieniu: „16. Kolegium w terminie 2 lat od wydania decyzji, o której mowa w ust. 11 przedstawia Ministrowi właściwemu do spraw informatyzacji aktualizację opinii, o której mowa w ust. 8. 17. W przypadku, gdy w wyniku aktualizacji opinii, przedstawione zostały okoliczności uzasadniające zmianę rozstrzygnięcia w zakresie uznania dostawcy za stwarzającego poważne ryzyko dla bezpieczeństwa narodowego, Minister może zmienić lub uchylić wydaną decyzję."	
41	Art. 1 pkt 50 dot. art.		**W art. 1 pkt 50 dodany w art. 66a ust. 15 otrzymuje następujące brzmienie:** *„15. Od decyzji, o której mowa w ust. 11, przysługuje wniosek o ponowne rozpatrzenie sprawy".*	

	66a ust. 15 uKSC		**Uzasadnienie:** Zasada dwuinstancyjności postepowania ma rangę konstytucyjną (art. 78 Konstytucji RP) i powtórzona została wyraźnie w art. 15 k.p.a. Jak wskazuje doktryna, regulacja wyłączenia dwuinstancyjności na rzecz ponownego rozpatrzenia sprawy to już samo w sobie ograniczenie zasady dwuinstancyjności postępowania[7]. Ustrojodawca przewiduje wprawdzie możliwość ustanawiania wyjątków od tej zasady, jednak w ślad za Trybunałem Konstytucyjnym[8], należy uznać, że *„z art. 78 zd. 1 Konstytucji można zatem wywieść skierowany do prawodawcy postulat takiego kształtowania procedury, aby w miarę możliwości przewidziane w niej było prawo wniesienia przez stronę środka zaskarżenia. Omawiany przepis ma charakter ogólny i zamieszczony został w rozdziale drugim Konstytucji, poświęconym wolnościom, prawom i obowiązkom człowieka i obywatela, w części normującej środki ochrony wolności i praw. Jak wynika z jego brzmienia ma on zastosowanie zarówno do postępowania sądowego, jak i administracyjnego*”. Uzasadnienie Projektu nie wyjaśnia, dlaczego prawa strony postępowania zostały ograniczone poprzez odebranie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy. Należy więc dopuścić możliwość złożenia wniosku o ponowne rozpoznanie sprawy i w ten sposób umożliwić weryfikację - przez ten sam organ – prawidłowości podjętej przez niego decyzji. Jakkolwiek rozpatrzenie sprawy ponownie przez ten sam organ, nie stanowi pełnego urzeczywistnienia zasady dwuinstancyjności postępowania, to jednak jest przyjętym w polskim systemie prawnym rozwiązaniem zapewniającym dodatkową (auto)kontrolę prawidłowości decyzji. Zapewnienie możliwości tej weryfikacji pozwoli potencjalnie na samodzielną rewizję przez organ ewentualnych decyzji nieprawidłowych oraz wymusza ponowną analizę merytoryczna sprawy. Większe gwarancje co do prawidłowości merytorycznej decyzji mogą ograniczyć konieczność składania skargi do sądu administracyjnego i zapewnią wyższy poziom sprawiedliwości proceduralnej względem strony.	

[7] A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, Komentarz aktualizowany do Kodeksu postępowania administracyjnego, LEX/el. 2021, art. 15, teza 3.
[8] Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2002 r., sygn. SK 31/01.

42	Art. 1 pkt 50 dot. art. 66b uKSC		OCENA WYSOKIEGO RYZYKA – okres na wycofanie **Uwagi dot. Wszystkich podmiotów objętych regulacją** Propozycja Z zadowoleniem należy przyjąć wydłużenie okresu czasu w jakim dany sprzęt powinien być wycofany z użytkowania przez wskazane podmioty (7 lat) jednakże samo obligatoryjne nałożenie takiego obowiązku jest rozwiązaniem zbyt daleko idącym. Decyzję w tym zakresie powinien podjąć każdy podmiot indywidualnie po przeprowadzeniu analizy ryzyka. Nie każdy sprzęt lub usługa jest na tyle krytyczny w systemie informatycznym, aby wymagał obligatoryjnej wymiany. Nadal postulujemy więc wprowadzenie obligatoryjności działania w tym zakresie ale dopiero w oparciu o przeprowadzoną przez podmioty analizę ryzyka i tylko w sytuacji gdy z tej analizy będzie wynikała taka konieczność. Dodatkowo podjęcie działań objętych tym przepisem, a raczej brak tych działań jest obwarowane horrendalną karą w wysokości 3% obrotu światowego danej firmy. Wprowadzenie takiej kary przy jednoczesnym obligatoryjnym narzuceniu konieczności podjęcia danych działań bez względu na to, czy takie działanie jest racjonalne czy nie, jest zupełnie nieproporcjonalne. **Uwagi dot. wszystkich podmiotów objętych regulacją (propozycje alternatywne)** Propozycja 1 **W art. 1 pkt 50 dodany art. 66b ust. 1 otrzymuje brzmienie:** *Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 11,* *Operator strategicznej sieci bezpieczeństwa:* *1) nie wprowadza do użytkowania ani nie nabywa typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;* *2) wycofuje z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 10 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 11;* - oraz usuwa się ust. 2-3.	

			Propozycja 2 Alternatywnie – w razie brak uwzględnienia uwagi zawartej w pkt 5 w zakresie odniesienia decyzji wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB: *Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 11, podmioty, o których mowa w art. 66a ust. 1 pkt 1-4:* *1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;* *2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 10 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 11.* **Uzasadnienie:** Proces wymiany sprzętu będzie długotrwały i kosztowny. Będzie wymagać od podmiotu (lub podmiotów) zobowiązanych do uwzględnienia skutków decyzji i rezygnacji z określonego sprzętu i oprogramowania przeprojektowania architektury wykorzystywanej sieci, rozpisania postępowań zakupowych, wybory nowego dostawcy i wreszcie wdrożenia zaplanowanych zmian. Całość procesu będzie stanowić wyzwanie – w szczególności w przypadku, gdyby zakres koniecznej wymiany sprzętu i oprogramowania miał dotyczyć szerokiego katalogu podmiotów – wskazanych w art. 66a ust. 1 pkt 1-4, zarówno prywatnych jak i publicznych, dysponujących różnymi możliwościami finansowymi i kompetencjami umożliwiającymi sprawne przeprowadzenie procesu. Zmiany będą wymagać poniesienia znaczących wydatków. Wymagają one w naszej ocenie wydłużenia okresu wycofania rozwiązań do 10 lat. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz”. Przepis nakazujący wycofywanie sprzętu zakupionego wiele lat wcześniej stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu w oparciu o obowiązujące wówczas przepisy. Tym bardziej więc powinien być uwzględniony postulat przedłużenia okresu wycofywania sprzętu z użytkowania.	

			Zapewnienie stabilności sieci i poprawności nowego wdrażanego rozwiązania będzie na tyle skomplikowane i trudne technicznie, że powinien być on planowany w perspektywie 10 lat. Ponadto w przepisie art. 66b ust. 1 pkt 2 dodano po słowach „*konkretne procesy ICT*" słowa „*o funkcjach krytycznych*" dla zapewnienia spójności ze zmianami proponowanymi w pkt 4 powyżej. **Uwagi dot. wyłącznie przedsiębiorców telekomunikacyjnych** Wśród wszystkich możliwych do objęcia oceną sektorów, jedynie dla sektora telekomunikacyjnego zdecydowano się na określenie w zał. nr 3 listy funkcji krytycznych. W naszej ocenie skoro lista taka powinna być traktowana jako maksymalny zakres decyzji możliwej do wydania w odniesieniu do sektora telekomunikacyjnego. Jednocześnie, jak już wielokrotnie wskazywaliśmy, uważamy, że termin 5 lat na wycofanie typów zasobów wskazanych w decyzji jest zdecydowanie zbyt krótki i powinien wynosić minimalnie 7 lat. **Propozycja 1** - przyjęcie terminu 7 lat dla przedsiębiorców telekomunikacyjnych i dostosowanie przepisów do Toolbox, tj. ograniczenie skutków decyzji do zasobów kluczowych. • Art. 66a ust. 12 otrzymuje brzmienie: *12. Decyzja, o której mowa w ust. 11, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka., <u>z zastrzeżeniem ust. 12a</u>.* • W art. 66a dodaje się ust. 12a w brzmieniu: *12a. W przypadku gdy decyzja dotyczy bezpieczeństwa sieci i usług, może ona obejmować wyłącznie typy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT zawierające się w wykazie zawartym w załączniku nr 3 do ustawy.* • W art. 66b skreśla się ust. 2 wraz z odwołaniem do niego w art. 66b ust. 1 pkt 2. **Propozycja 2 –** przyjęcie terminu 7 lat z możliwością skrócenia go w szczególnie uzasadnionych przypadkach do 5 lat oraz dostosowanie przepisów do Toolbox, tj. ograniczenie skutków decyzji do zasobów kluczowych • Zmiany zawarte w Propozycji 1 powyżej. • W art. 66b dodaje się ust. 1a w brzmieniu:	

			„Minister właściwy do spraw informatyzacji może w odniesieniu do części lub całości decyzji skrócić termin, o którym mowa w ust. 1 pkt 2 do 5 lat jeśli określenie dłuższego terminu rodziłoby bardzo poważne, bezpośrednie zagrożenie dla bezpieczeństwa narodowego, a jednocześnie określenie krótszego terminu nie będzie groziło ryzykiem zakłóceniem ciągłości działania istotnych dla bezpieczeństwa usług lub infrastruktury." **Propozycja 3** **W art. 1 pkt 50 dodany art. 66b ust. 2 otrzymuje następujące brzmienie:** *„2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, wycofują w ciągu 10 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT o funkcjach krytycznych* Uwaga aktualna jedynie w przypadku braku akceptacji propozycji zawartej w pkt 5 dotyczącej ograniczenia decyzji o uznaniu za dostawcę wysokiego ryzyka wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB **Uzasadnienie:** Zmiana w przepisie art. 66b ust. 2, polega na dodaniu po słowach „*konkretne procesy ICT*" słów „*o funkcjach krytycznych*" i przedłużenia okresu wycofania sprzętu do 10 lat. Przepis art. 66b ust. 2 Projektu dotyczy określonej grupy przedsiębiorców telekomunikacyjnych, tj. tych, którzy obowiązani są posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. W uzasadnieniu Projektu wyjaśniono, że jest to grupa ok. 100 podmiotów, czyli znacząca. W tym do tej grupy zaliczają się najwięksi operatorzy telekomunikacyjni. Umowy z dostawcami zawierane są z reguły na długie okresy. Proces wymiany sprzętu będzie więc długotrwały zarówno z uwagi na ilość podmiotów jak i na poziomie indywidualnym, w odniesieniu do poszczególnych podmiotów, zmuszonych do przejrzenia infrastruktury, zaprojektowaniu niezbędnych zmian, przeprowadzenia postępowania zakupowego, wynegocjowania nowej umowy itd.	

			Przedstawiona w załączniku nr 3 do ustawy lista funkcji jest bardzo obszerna. Decyzje odnoszące się do elementów infrastruktury tam wskazanych będą wymuszać bardzo istotne techniczne zmiany w sieci telekomunikacyjnej, wymagające technologicznego przeprojektowania całych sieci – a co za tym idzie, będą wiązać się z koniecznością alokowania w tym celu istotnych kosztów. Konieczność zapewnienia stabilności sieci będzie wymagał zaplanowania skomplikowanego i trudnego technicznie procesu, wymagającego zdecydowanie więcej czasu niż 5 lat. Z tego względu proponowany okres to 10 lat. W tym zakresie por. także uwagi do pkt 20.	
43	Art. 1 pkt 50 dot. art. 66b uKSC		OCENA WYSOKIEGO RYZYKA – <u>Uwzględnienie potrzeb związanych z utrzymaniem zasobów w okresie wycofania</u> **Dostosowanie przepisów dot. skutków oceny do stanowiska wyrażonego m.in. w zestawieniu uwag, gdzie wskazano,** że *„Z kolei decyzja o uznaniu za dostawcę wysokiego ryzyka nie powinna być przesłanką do zakończenia wsparcia eksploatacyjnego przez dostawcę tego sprzętu do momentu wycofania danego sprzętu lub oprogramowania z użytkowania*.”. Aktualny przepis art. 66b ust. 1 pkt 1 przez użycie zwrotu „nie wprowadzają do użytkowania” może w praktyce bardzo poważnie blokować możliwość użytkowania zasobów już zakupionych (np. stany magazynowe, świeże zakupy), a potencjalnie także dokonywania napraw i bieżącej eksploatacji. **Propozycja 1** - usunięcie art. 66b ust. 1 pkt 1 jako zbędnego wobec dalej idącego obowiązku wycofania w określonym terminie. Termin realizacji obowiązku wycofania jest bowiem liczony od decyzji, a nie od wprowadzenia do użytkowania. Jeśli z uwagi na potrzeby eksploatacyjne, a szczególnie utrzymanie ciągłości działania dany podmiot musiałby wprowadzić do użytkowania zasób, który byłby następnie konieczny do usunięcia powinien mieć taką możliwość oraz ponosić koszty i ryzyko takiej decyzji. Jednocześnie, z uwagi na ryzyko uznania takich ewentualnych działań za działanie na szkodę przedsiębiorstwa istnieje bardzo małe prawdopodobieństwo dokonywania nowych, szerszych niż realnie niezbędne zakupów i wdrożeń, mimo wydanej decyzji wskazującej na wysokie ryzyko związane z danym dostawcą. **Propozycja 2 –** alternatywna	

			W art. 66b dodaje się ust. 1a i 1b w brzmieniu *1a. W okresie, o którym mowa w ust. 1 pkt 2 dopuszcza się wprowadzanie do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jeśli zostały zakupione przed opublikowaniem informacji o decyzji, o której mowa w art. 66a ust. 11.* *1b. W okresie, o którym mowa ust. 1 pkt 2 dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w tym w zakresie dokonywania zakupów lub wdrożeń, jeśli jest to niezbędne dla a zapewnienia odpowiedniej jakości i ciągłości świadczonych usług lub dokonywania niezbędnych napraw awarii lub uszkodzeń.*	
44	Art. 1 pkt 50 dot. art. 66b ust. 3 uKSC		W art. 1 pkt 50 dodany art. 66b ust. 3 skreśla się: *„3. Podmioty, o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 i 1598), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 11”.* Uwaga aktualna jedynie w przypadku braku akceptacji propozycji zawartej w pkt 5 dotyczącej ograniczenia decyzji o uznaniu za dostawcę wysokiego ryzyka wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB **Uzasadnienie:** Przepis art. 66b ust. 3 Projektu wprowadza przesłankę dodatkową wykluczenia wykonawcy z postępowania o udzielenie zamówienia, która w stosunku przesłanek przewidzianych już w ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych, a wynikających z dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (dalej „dyrektywa 2014/24/UE”). W sprawie	

			projektowanej regulacji wypowiadał się także MSUE (zob. pismo: https://legislacja.gov.pl/docs//2/12337950/12716624/12716626/dokument487161.pdf), który wskazał, że projektodawca powinien przygotować się na przedstawienie uzasadnienia dopuszczalności tego przepisu w świetle przewidzianych w dyrektywie 2014/24/UE przesłanek pozwalających na wyłączenie jej stosowania, w tym przesłanki odnoszącej się do podstawowych interesów danego państwa członkowskiego w zakresie bezpieczeństwa. Polskie prawo zamówień publicznych stanowi transpozycję art. 57 dyrektywy 2014/24/UE, w którym określono precyzyjnie podstawy wykluczenia wykonawcy. Regulacje zawarte w Projekcie muszą być zgodne z dyrektywą 2014/24/UE, a wśród podstaw wykluczenia zawartych w dyrektywie brak jest podstawy wykluczenia sformułowanej w art. 66b ust. 3 Projektu. Minister ds. UE („MSUE") zwrócił uwagę, że aktualne pozostaje zastrzeżenie, w myśl którego zgodnie z utrwalonym orzecznictwem Trybunału Sprawiedliwości UE wszelkie wyjątki od stosowania przepisów dyrektyw dotyczących zamówień publicznych podlegają wykładni zawężającej. Dotychczas nie przedstawiono argumentacji dotyczącej związku dokonywanych zakupów sprzętu, oprogramowania i usług ze sferą podstawowych interesów państwa w zakresie bezpieczeństwa. Powoduje to uzasadnione wątpliwości co do konieczności i prawidłowości wprowadzenia regulacji w art. 66b ust. 3 Projektu jako odstępstwa od postanowień dyrektywy 2014/24/UE.	
45	Art. 1 pkt 50 dot. art. 66b ust. 4 uKSC		**W art. 1 pkt 50 dodaje się art. 66b ust. 4 w brzmieniu następującym (alternatywnie/uzupełniająco do pkt 43):** *„4. Przepisów ust. 1-3 nie stosuje się, do nabywania i wprowadzania do użytkowania produktów, usług i procesów ICT o funkcjach krytycznych wskazanych w decyzji, o której mowa w art. 66a ust. 11, jeżeli jest to niezbędne do zachowania ciągłości utrzymania funkcjonowania sieci."* **Uzasadnienie:** Dodanie przepisu art. 66b ust. 4 wynika z konieczności zapewnia ciągłości dostaw do bieżącego funkcjonowania operatorów telekomunikacyjnych i pozostałych podmiotów zobowiązanych stosować się do ograniczeń wynikających z decyzji o uznaniu za dostawcę wysokiego ryzyka. Decyzja o uznaniu za dostawcę wysokiego ryzyka nie powinna być przesłanką do zakończenia wsparcia eksploatacyjnego przez dostawcę tego sprzętu. Podmiotowi (lub podmiotom) zobowiązanym do wycofania z użytkowania określonego sprzętu należy zapewnić możliwość realizacji niezbędnych czynności zakupowych,	

			wdrożeniowych i serwisowych odnoszących się do już eksploatowanych produktów, usług lub procesów ICT oraz objętych zakresem decyzji. Brak możliwości realizacji szeroko rozumianych funkcji utrzymania infrastruktury będzie potencjalnie skutkował awariami (także fizycznymi) oraz trudnościami (lub nawet niemożliwością) usuwania luk lub podatności. W konsekwencji wzrośnie prawdopodobieństwo incydentów cyberbezpieczeństwa, w tym przerwanie ciągłości świadczenia usług przez podmiot (lub podmioty) zobowiązany do uwzględnienia skutków decyzji. Proponowana zmiana ma też uzasadnienie w istniejących – nierzadko długoterminowych – umowach z dostawcami, w ramach których zapewniane jest wsparcie dostawcy. Zakończenie korzystania z tych usług, zwłaszcza w trybie nagłym, będzie wymagać potencjalnie renegocjacji umowy lub nawet – ponoszenia przez podmiot lub podmioty zobowiązane do uwzględnienia skutków decyzji, dodatkowych kosztów związanych z wyjściem z zawartej umowy i poszukiwaniem rozwiązań alternatywnych – nie zawsze zresztą dostępnych. W przypadku braku możliwości uwzględnienia proponowanej zmiany w pełnym brzmieniu, proponujemy zachowanie możliwości nabywania z produktów, usług i procesów ICT co najmniej przez okres odpowiadający okresowi wycofania ich z użytku zgodnie z ust. 1 pkt 2) oraz ust. 2) – ze wskazanych wyżej przyczyn związanych z koniecznością zapewnienia bezpieczeństwa eksploatacji wykorzystywanych rozwiązań.	
46	Art. 1 pkt 50 dot. art. 66b ust. 5 – 6 (dodawane) uKSC		**W art. 1 pkt 50 dodaje się art. 66b ust. 5-6 w brzmieniu następującym:** *„5. Podmiot lub podmioty, zobowiązane do wycofania z użytkowania sprzętu lub oprogramowania, na skutek wydania decyzji, o której mowa w art. 66a ust. 11, otrzymują odszkodowanie za koszty związane z wymianą tego sprzętu lub oprogramowania.* *6. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup sprzętu lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów wykazujących poniesione koszty”.* **Uzasadnienie:** Wprowadzenie obowiązku wycofania z użytku sprzętu lub oprogramowania objętego decyzję w sprawie uznania za dostawcę wysokiego ryzyka spowodowuje wysokie koszty dla podmiotu lub podmiotów zobowiązanych do wycofania z użytkowania zakwestionowanych	

			rozwiązań ICT. Koszty te nie będą w żaden sposób zawinione przez te podmioty, a wynikać będą z regulacji o szczególnym charakterze – z założenia mających zastosowanie w sytuacjach wyjątkowych. Zaproponowane regulacje w praktyce oznaczają, że podmioty zobowiązane (w zależności od przyjętej koncepcji – OSSB lub wszystkie podmioty wymienione w aktualnie projektowanym art. 66a ust 1 pkt 1-4) muszą pozbyć się sprzętu lub oprogramowania, które potencjalnie mogłoby być eksploatowane jeszcze przed długi czas – gdyby nie wprowadzono określonych regulacji. Z tego względu uzasadnione jest zdefiniowanie w przepisach rozsądnej rekompensaty dla podmiotów ponoszących tego rodzaju koszty. Warto wskazać przy tym, że podobne rozwiązania wprowadzone zostały m.in. w Finlandii. Propozycja zakłada rekompensatę pochodzącą z budżetu Skarbu Państwa – Prezesa UKE. Z uwagi jednak na fakt, że rekompensata ma związek ze szczególnymi działaniami państwa, związanymi z kluczowymi aspektami bezpieczeństwa, propozycja ogranicza się przy tym do pokrycia wydatków poniesionych na zakup wymienianego sprzętu, bez uwzględnienia innych kosztów związanych z wydaną decyzją (np. przeprowadzenie procesu zakupowego, przeprojektowanie infrastruktury itd.). Z tego względu uważamy, że propozycja jest rozsądna i do pewnego stopnia ma szansę zniwelować negatywne konsekwencje ponoszone przez podmioty, zobowiązane do stosowania się do decyzji.	
47	Art. 1 pkt 50 dot. art. 66d ust. 1 i 2 uKSC		**W art. 1 pkt 50 postanowienia art. 66d ust. 1-2 otrzymują brzmienie następujące:** *„1. Sąd administracyjny rozpatruje skargę na decyzje, o których mowa w art. 66a ust. 11, na posiedzeniu jawnym*. *2. Odpis sentencji wyroku z uzasadnieniem doręcza się ministrowi właściwemu do spraw informatyzacji oraz skarżącemu."* **Uzasadnienie:** W zaproponowanej w Projekcie postaci, przepis art. 66d stanowi odstępstwo od kardynalnych zasad nie tylko procedury administracyjnej (art. 10 oraz art. 142 ustawy p.p.s.a.), ale każdego rzetelnego postępowania, w postaci jego jawności, ustności, prawa do skutecznego wniesienia środka zaskarżenia i generalnie prawa do obrony. Zainteresowany podmiot nie będzie mógł bronić swoich praw, skoro skarga będzie rozpoznawana na posiedzeniu niejawnym i nie będzie on mógł zapoznać się z pełnym uzasadnieniem wyroku. W ten sposób postępowanie to będzie spełniało cechy procesu inkwizycyjnego. Wbrew twierdzeniom w uzasadnieniu Projektu, że strona i tak będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym, czyli	

			nie powinno ucierpieć jej prawo do obrony, nie będzie jednak miała dostępu do dowodów i materiałów postępowania, skoro niejawne będzie posiedzenie i uzasadnienie wyroku. W sposób więc oczywisty jej prawa w tym postępowaniu zostaną ograniczone. Przyjęta w Projekcie konstrukcja w praktyce będzie wyłączać skuteczną obronę oraz możliwość wnoszenia środków odwoławczych do sądu wyższej instancji w celu weryfikacji rozstrzygnięcia sądu pierwszej instancji. Strona nie będzie bowiem posiadała pełnej wiedzy na temat powodów takiego a nie innego rozstrzygnięcia – w szczególności występuje wysokie ryzyko odmowy stronie dostępu do kluczowych elementów ustalonego stanu faktycznego. Wskazujemy, że na wady prawne art. 66d wskazywała także Rada Legislacyjna już w opinii do projektu z dnia 23 lutego 2021 r. W szczególności Rada Legislacyjna podniosła wątpliwość, czy w ogóle jest zgodne z Konstytucją RP odstępowanie od doręczania stronie pełnego uzasadniania wyroku sądu administracyjnego (art. 66d ust. 2). Według Rady, zasadą musi być dostarczanie stronie pełnego uzasadnienia faktycznego decyzji administracyjnej, tak aby strona (będąca adresatem decyzji) mogła w sposób skuteczny – w oparciu o pełną znajomość relewantnych prawnie faktów, które wpłynęły na treść decyzji – zaskarżyć tę decyzję do sądu administracyjnego. Podobnie też wyrok sądu administracyjnego musi w świetle konstytucyjnego prawa do sądu zawierać pełne uzasadnienie doręczane stronie, gdyż w oparciu o to uzasadnienie strona może skutecznie wykorzystać swoje uprawnienia do zaskarżenia tego wyroku na drodze sądowej (w omawianym przypadku: zwłaszcza skargą kasacyjną do Naczelnego Sądu Administracyjnego), a ponadto jest to konieczne dla pogłębiania zaufania obywateli do państwa i stosowanego prawa (art. 2 Konstytucji RP). Wreszcie także w tym obszarze pojawiają się duże wątpliwości co do proporcjonalności proponowanego rozwiązania – z uwagi na niezwykle szerokie ograniczenia praw strony. Przyjęcie w obecnej postaci w Projekcie postanowień art. 66d ust. 1-2 rodzi poważne ryzyko uznania tych przepisów za sprzecznie z Konstytucją RP.	
48	Art. 1 pkt 50 dot. Art. 66d ust. 3 uKSC		Nie wiadomo w jakim celu wprowadzona zastała zasada, że WSA nie może wstrzymać wykonalności decyzji, o której mowa w art. 66a ust. 8, po wniesieniu skargi na tą decyzję. Pozostawienie takiego zapisu może spowodować nieodwracalne starty dla firmy, których dotyczy zaskarżona decyzja	

			W art. 1 pkt 50 postanowienia art. 66d skreśla się ust. 3 **Uzasadnienie:** Przepis, którego dotyczy niniejszy punkt, wyłącza możliwość wstrzymania wykonalności zaskarżonej decyzji przez sąd. Uzasadnienie Projektu nie zawiera szczegółowego wyjaśnienia, poza ogólnym powołaniem się na szczególne interesy bezpieczeństwa państwa, przyczyny zrezygnowania z jednej z zasad ogólnych odnoszących się do wstrzymania wykonalności decyzji. Art. 61 ust. 3 p.p.s.a. reguluje instytucję tzw. ochrony tymczasowej w postępowaniu sądowo-administracyjnym. Celem przewidzianej w art. 61 § 3 p.p.s.a. ochrony tymczasowej jest uchronienie strony skarżącej przed skutkami wykonania zakwestionowanego aktu, które mogą być trudne do odwrócenia, po ewentualnym jego uchyleniu przez sąd (por. postanowienie Wojewódzkiego Sądu Administracyjnego („WSA") w Poznaniu z 25 czerwca 2019 r. sygn. akt IV SA/Po 425/19). Wstrzymanie wykonania zaskarżonej decyzji jest dodatkowym, obok skargi, środkiem ochrony przysługującym skarżącemu. Wyłączenie możliwości wstrzymania przez sąd wykonania decyzji stanowi wyjątek od zasady ogólnej wynikającej z art. 61 § 3 ustawy prawo o postępowaniu przed sądami administracyjnymi („p.p.s.a.")[9], który dotychczas w polskim prawie był stosowany niezwykle rzadko. Ustawowe wyjątki od zasady istnienia możliwości wstrzymania wykonania decyzji powinny być przy tym wprowadzane z najwyższą ostrożnością. Trafny jest pogląd Naczelnego Sądu Administracyjnego („NSA"), zwracający uwagę na konieczność zachowania „*daleko idącej ostrożności*" przy wykonywaniu decyzji ostatecznych przed upływem terminu do ich zaskarżenia, co może doprowadzić do powstania stanów nieodwracalnych[10]. Instytucja wstrzymania decyzji jest stosowana od dawna także w UE. Celem ochrony tymczasowej jest zapewnienie możliwości wstrzymania decyzji, jeżeli zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków. Dokładnie taka sytuacja może nastąpić w następstwie zastosowania rozwiązań proponowanych w Projekcie, tj. w następstwie wydania decyzji mogą powstać już nieodwracalne konsekwencje dla podmiotu, którego dotyczyć będzie taka decyzja. Badanie	

[9] Dz. U. z 2002 r., Nr 153, poz. 1270 ze zm.
[10] Zob. T. Woś red., *Prawo o postępowaniu przed sądami administracyjnymi,* Komentarz do art. 61, LEX 2016 i przywołane tam orzecznictwo.

			przesłanek wstrzymania wykonania decyzji powinno odbywać się w odniesieniu do konkretnej sprawy – to niezwisły sąd bada, czy w świetle indywidualnych okoliczności nad interesami strony przeważa ochrona interesu bezpieczeństwa państwa. Dokonywanie takiej oceny przez ustawodawcę w sposób generalny na etapie projektu ustawy będzie pozbawiać stronę możliwości ochrony jej praw i skutkować pozornością ochrony sądowej. Z tego względu wskazany przepis należy usunąć z Projektu; zastosowanie powinny znaleźć zaś zasady ogólne wynikające z p.p.s.a.	
49	Art. 1 pkt 50 dot. Art. 66f (dodanie) uKSC		**W art. 1 pkt 50 dodaje się art. 66f w brzmieniu następującym:** *„Prezes UKE ustala z odpowiednim CSRIT oraz przedsiębiorcami komunikacji elektronicznej świadczącymi usługi publicznej sieci telekomunikacyjnej oraz ich stowarzyszeniami, producentami i dostawcami infrastruktury telekomunikacyjnej oraz ich stowarzyszeniami, z uwzględnieniem stanowisk ENISA oraz wytycznych wydawanych przez inne właściwe organy Unii Europejskiej, wykaz funkcji oraz komponentów krytycznych dla bezpieczeństwa sieci i usług, i publikuje go na swojej stronie internetowej”,* **Uzasadnienie:** Istotną częścią systemu zapewnienia bezpieczeństwa jest identyfikacja krytycznych obszarów architektury sieciowej. W przypadku bowiem tych elementów infrastruktury należy zastosować wyższy poziom bezpieczeństwa. Składniki są krytyczne w szczególności wtedy, gdy techniczne nieprawidłowości prowadzić mogą do istotnych naruszeń bezpieczeństwa lub naruszeń ochrony danych w znacznym stopniu. Krytyczność danego składnia jest uzasadniona przez te jego funkcje, które mogą doprowadzić do nieprawidłowości technicznych w przypadku awarii. Lista zawarta w załączniku nr 3 („Kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług”) ma więc kluczowe znaczenie – zarówno z perspektywy wymogu wycofania z użytku produktów / usług / procesów przez przedsiębiorców telekomunikacyjnych (obecne brzmienie projektu – art. 66b ust. 2), jak i dla ustalenia zakresu dopuszczalnego zakresu postępowania w sprawie uznania za dostawcę wysokiego ryzyka (por. pkt 5). Zważywszy na wagę tej listy – ale również mając na uwadze dynamicznie zmieniające się okoliczności, zarówno technologiczne jak i podmiotowe – zasadne jest, by nie stanowiła ona załącznika do ustawy. Takie ujęcie uniemożliwia bowiem jej sprawną zmianę w przypadku	

			zmieniających się okoliczności, a de facto uzależnia możliwości stosowanego dostosowania wykazu funkcji krytycznych od możliwości uzyskania porozumienia politycznego umożliwiającego zmianę ustawy. W praktyce innych państw europejskich, analogiczne listy są tworzone przez – lub przy udziale – regulatora rynku telekomunikacyjnego. Zapewniana jest też współpraca z organami odpowiedzialnymi za bezpieczeństwo oraz konsultacje z uczestnikami rynku oraz aktorów społecznych. Lista podlega aktualizacji w zależności od zmieniających się okoliczności. Ponadto zapewniony jest wówczas udział podmiotów, posiadających szeroką wiedzę i doświadczenie, co umożliwia stworzenie wykazu racjonalnego, adresującego cyberzagrożenia a jednocześnie zapewniającego stabilizację rynku rozwiązań ICT. Tytułem przykładu podobne rozwiązania funkcjonują w innych państwach europejskich: **a)** W Finlandii, proces identyfikacji funkcji krytycznych odbywa się przez pryzmat podstawowych funkcji sieciowych opartych o standardy ETSI i specyfikacje techniczne 3GPP, zdefiniowane przez regulatora. Ocena ryzyka dla bezpieczeństwa sieci skupia się na konkretnym sprzęcie stanowiącym element infrastruktury krytycznej, zaś regulator wspierany jest w procesie decyzyjnym przez dedykowane ciało doradcze., składające się z przedstawicieli organów rządowych, operatorów telekomunikacyjnych, głównych dostawców sprzętu i innych interesariuszy **b)** W Austrii środki bezpieczeństwa opracowane w tym kraju mają zastosowanie do produktów bezpośrednio zidentyfikowanych jako komponenty krytyczne w sieci 5G zgodnie z załącznikiem do rozporządzenia dotyczącym bezpieczeństwa sieci wydanego przez austriacki organ regulacyjny Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)[11]. Jednocześnie każdy z operatorów sieci telekomunikacyjnych działających w technologii 5G w Austrii został zobowiązany do regularnego przedkładania deklaracji wiarygodności dotyczącej spełnienia wymogów bezpieczeństwa sieci określonych w załączniku nr 1 do przedmiotowego rozporządzenia.[12] Podobnie jak w przypadku Finlandii, rozwiązanie wdrożone w Austrii odwołuje się do międzynarodowych standardów technicznych 3GPP.	

[11] Załącznik nr 2 do rozporządzenie RTR nr 301: Telekom-Netzsicherheitsverordnung 2020 – TK-NSiV 2020, wydanego zgodnie z § 6 ust. 4, https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_TK-NSiV_2020.de.html.
[12] Załącznik nr 1 do Rozporządzenia – TK-NSiV.

			Wreszcie uznaniowość zaproponowanego wykazu nie wzmacnia zaufania uczestników rynku – w tym uczestników krajowego systemu cyberbezpieczeństwa – do państwa i jego organów. Z niniejszym punktem skorelowany jest pkt 28 przewidujący usunięcie załącznika nr 3 do ustawy. W przypadku bowiem przyjęcia w zaproponowanym brzmieniu art. 66f, załącznik ten będzie zbędny; wykaz kategorii funkcji krytycznych będzie bowiem ustalany w trybie art. 66f.	
50	Art. 1 pkt 52 dot. art. 67a (w całości) uKSC		Przepis ten wprowadza możliwość wydawania ostrzeżeń przez Pełnomocnika. Ostrzeżeniem takim, mającym formę zalecenia działania, objęte są wszystkie podmioty określone w art. 66a ust. 1. Jednak nie do końca wiadomo jakie działania powinien podjąć dany podmiot, do którego skierowane zostało ostrzeżenie ponieważ przepis ten wskazuje, że jedynie operator usługi kluczowej uwzględnia wydane ostrzeżenia podczas procesu szacowania ryzyka. Przepis ten powinien być uzupełniony o wyraźne stwierdzenie, że pozostałe podmioty nie muszą uwzględniać wydanego ostrzeżenia ponieważ dla nich ma ono charakter wyłącznie informacyjny o stwierdzonym możliwym zagrożeniu.	
51	Art. 1 pkt 52 dot. art. 67a ust. 6 uKSC		Proponujemy by ostrzeżenie było publikowane w mediach obligatoryjnie.	
52	Art. 1 pkt 52 dot. art. 67a ust. 8 uKSC		Środki jakie są możliwe przy ostrzeżeniu Pełnomocnika są zbyt szerokie. Wydaje się, że konsekwencją ostrzeżenia nie powinno być narzucenie konieczności stosowania odpowiedniej technologii lub sprzętu. Niepokojące jest, że w projektowanej regulacji nie został wskazany okres na odstąpienie od korzystania z danych rozwiązań teleinformatycznych.	
53	Art. 1 pkt 52 dot. art. 67b ust. 3 uKSC		Wprowadzenie zasady, że każde polecenie zabezpieczające ma rygor natychmiastowej wykonalności jest rozwiązaniem zbyt daleko idącym. Ponieważ do decyzji tej mają zastosowanie przepisy KPA wystarczające byłoby odniesienie o możliwości nałożenia rygoru natychmiastowej wykonalności dla przedmiotowych decyzji ale dopiero po przeprowadzeniu analizy czy taki rygor należy nałożyć. Wprowadzenie automatyzmu w tym zakresie ograniczy możliwości działania Ministra wydającego decyzję, o której mowa w ust. 2, który być może nie uznawałby za uzasadnione nadawanie takiego rygoru absolutnie wszystkim decyzjom wydawanym w	

			zakresie poleceń zabezpieczających. Ponadto rygor natychmiastowej wykonalności oznacza, że dana decyzja powinna być wykonana natychmiast. Możliwości wykonania takiej decyzji mogą być jednak bardzo mocno ograniczone lub wręcz niemożliwe. Szczególnie w zakresie zakazu użytkowania określonego sprzętu lub usługi (o tym poniżej). Efektem natychmiastowego działania decyzji, połączonym z niezwykle wysoką karą za jej niewykonanie może być zupełne zaprzestanie produkcji. Mając na uwadze fakt, iż regulacja dotyczy kluczowych sfer gospodarczych państwa, konsekwencje jakie ona wywoła mogą być nieobliczalne i nienaprawialne.	
54	Art. 1 pkt 52 dot. art. 67b ust. 5 pkt 6 uKSC		W ocenie Konfederacji Lewiatan polecenie zabezpieczające może zabronić przedsiębiorcom korzystania z określonego sprzętu lub oprogramowania, co może być niewykonalne, szczególnie gdy będzie to ważny sprzęt lub krytyczne oprogramowanie. Brakuje tutaj okresu, w jakim przedsiębiorca będzie miał się wycofać z wykorzystywania danego sprzętu lub oprogramowania.	
55	Art. 1 pkt 52 dot. art. 67b ust. 9 pkt 6 uKSC		Wprowadzenie obligatoryjnego zakazu stosowania określonego sprzętu lub usługi może mieć katastrofalne skutki dla przemysłu. Przy zaawansowanych technologicznie liniach produkcyjnych czy systemach zapewnienia jakości może nie być możliwości wykonania takiego polecenia zabezpieczającego, które wprowadzi ww. zakaz. Tym bardziej, że polecenie zabezpieczające mające rygor natychmiastowej wykonalności powinno być wykonane w najszybszym możliwym terminie. Tymczasem w specyficznych systemach produkcji wykorzystujących drogie i trudno dostępne/trudno zamienialne technologie wykonanie polecenia zabezpieczającego może być niemożliwe, nie mówiąc już o szybkim jego wykonaniu. Przepis ten powinien mieć formę zalecenia, a nie sztywnego zakazu lub powinien nakazywać wskazanie przez Ministra alternatywnego rozwiązania, które zabezpieczałoby przed incydentem krytycznym lub go znacznie ograniczało. W obecnym brzmieniu przepis może być niewykonalny „od ręki” (a nawet w krótkim lub średnim okresie czasu), a obwarowany jest horrendalnie wysoką karą w postaci 3% światowego obrotu danej firmy.	
56	Art. 1 pkt 52 dot. art. 67b ust. 13 uKSC		Polecenie zabezpieczające powinno być upubliczniane w sposób szerszy niż tylko dzienniku urzędowym ministra właściwego do spraw informatyzacji. W celu efektywniejszego przekazania takiej informacji zainteresowanym podmiotom jest wykorzystanie środków masowego przekazu.	

57	Art. 1 pkt 53 dot. art. art. 73 ust. 3 pkt 2a i 2b uKSC		Wprowadzenie kar w wysokości 3% światowego obrotu danej firmy jest absolutnie nieuzasadnione. Taka wysokość kary może prowadzić do bankructwa firm, tym bardziej, że kary te nałożone są za brak działań określonych w ww. przepisach, które często są niemożliwe do podjęcia lub ich wprowadzenie w życie może skutkować zatrzymaniem produkcji całego zakładu. Oczywiście kara powinna być proporcjonalnie wysoka do przewinienia i jednocześnie powinna odstraszać od nieodpowiedniego zachowania poszczególnych podmiotów ale nie może stanowić o dalszym funkcjonowaniu całych przedsiębiorstw.	
58	Art. 1 pkt 53 dot. art. 73 ust. 3 (pkt 14-16) uKSC		Wysokość kar pieniężnych zaproponowanych w tym przepisie jest zdecydowanie nieadekwatna do wagi przewinienia. Wnosimy o obniżenie kar, tak aby nie stanowiły tak dotkliwej sankcji dla przedsiębiorcy	
59	Art. 1 pkt 53 dot. art. Art. 73 ust. 3 pkt 2b uKSC		Uwaga techniczna. Wskazany w przepisie art. 67b ust. 2 nie wskazuje podmiotów, które miałyby być objęte sankcją.	
60	Załącznik nr 3		Jak już wielokrotnie sygnalizowaliśmy zakres załącznika nr 3 został zarysowany zbyt szeroko. Odnosząc się do aktualnej treści załącznika musimy wskazać, że z perspektywy przedsiębiorców telekomunikacyjnych nie stanowi on doprecyzowania zakresu możliwych do wydania decyzji, a tym samym trudno nam uznać go jako określenie „essential assets", do których referuje Toolbox 5G. Uznając oczywiście swobodę poszczególnych państw w decydowaniu co do zakresu funkcji uznanych za kluczowe, zauważamy jednak, że wskazany w załączniku zakres funkcji jest tak szeroki, że zdecydowana większość funkcji sieci uznawana jest za krytyczną. Brak przy tym wyjaśnienia czy doprecyzowania jakie kryteria przyjęto podczas badania krytyczności, tj. czy krytyczność ta została faktycznie powiązana z przesłanką wydania decyzji dot. wysokiego ryzyka czyli istnienia poważnego zagrożenia bezpieczeństwa narodowego. Tym samym, mimo przedstawienia treści załącznika nr 3 wciąż aktualne pozostają obawy co do potencjalnego zakresu wydawanych decyzji. Warto przy tym jednak zauważyć, że „luz" decyzyjny, jaki takie podejście zapewnia administracji publicznej, po stronie przedsiębiorców skutkuje wysokim poziomem niepewności otoczenia prawno-regulacyjnego, który to ma istotne znaczenie dla podejmowanych kosztowych i długoterminowych decyzji inwestycyjnych.	

			W naszej ocenie Lista funkcji krytycznych wymaga doprecyzowania, które powinno nastąpić w ramach eksperckich prac grupy podmiotów reprezentujących regulatora rynku telekomunikacyjnego, odpowiednie podmioty zajmujące się bezpieczeństwem państwa, dostawców oraz przedsiębiorców telekomunikacyjnych (także uwaga 49). W naszej ocenie przepisy powinny zawierać bardziej precyzyjne określenia ze wskazaniem konkretnych definicji urządzeń lub funkcji zgodnych ze standaryzacją 3GPP. Podtrzymujemy naszą dotychczasową opinię o potrzebie doprecyzowania przepisów tak, aby ewentualne decyzje dot. dostawców wysokiego ryzyka były ograniczone do faktycznie krytycznych i możliwie precyzyjnie określonych zasobów (a nie tylko funkcji) w zakresie sieci 5G w architekturze Stand Alone. Dodatkowo, podkreślamy, że utrzymanie tak szerokiego zakresu potencjalnych decyzji wzmacnia w istotnym zakresie potrzebę wyraźniejszego potwierdzenia na poziomie ustawy form dialogu między podmiotami przygotowującymi analizy i projekty decyzji, a podmiotami dla których z wydawanych decyzji będą wynikały konkretne obowiązki w zakresie wycofania wskazanych w decyzji zasobów. <u>Propozycja 1</u> W naszej ocenie lista wskazana w zał nr 3 powinna zostać oparta o listę zasobów i funkcji **krytycznych** wypracowaną już w dokumentach unijnych i aktualną, jako pochodzącą z grudnia 2020 r.. Tym samym jako krytyczne powinny zostać wskazane jedynie funkcje sieci rdzeniowej (CORE) oraz zarządzania funkcjami wirtualizacji sieci oraz jej orkiestracji (MANO). Taka lista została przedstawiona na str. 8 dokumentu ENISA z 10/12/2020 r. pt. *5G Supplement - to the Guideline on Security Measures under the EECC*[13].	

[13] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

Table 3: Assets (according to the Coordinated risk assessment)

Categories of elements and functions	Criticality	Examples of key elements
Core network functions	CRITICAL	User Equipment Authentication, roaming and Session Management Functions; User Equipment data transport functions; Access policy management; Registration and authorization of network services; Storage of end-user and network data; Link with third-party mobile networks; Exposure of core network functions to external applications; Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	CRITICAL	
Management systems and supporting services (other than MANO)	MODERATE/HIGH	Security management systems; Billing and other support systems such as network performance
Radio Access network	HIGH	Base stations
Transport and transmission functions	MODERATE/HIGH	Low-level network equipment (routers, switches, etc.); Filtering equipment (firewalls, IPS...)
Internetwork exchanges	MODERATE/HIGH	IP networks external to MNO premises; Network services provided by third parties

Further details about the listed asset categories is available in paragraphs 2.22 - 2.27 of the Coordinated risk assessment.

Przedstawiona w aktualnej treści załącznika nr 3 lista funkcji krytycznych wydaje się być oparta o przyjętą w grudniu 2019 r. we Francji listę zasobów podlegających wydawaniu zezwoleń czasowych. Jednocześnie jednak różni się od niej istotnie poziomem szczegółowości. W szczególności z materiałów z Francji zaczerpnięto jedynie najbardziej ogólne z możliwych określenie funkcji sieci. Zrezygnowano jednak z przypisania im konkretnych nazw funkcji sieci wg standardu 3GPP. Ponadto, pominięto zawarte w rozwiązaniu francuskim precyzyjne wyłączenia, w tym np. wyraźne wyłączenie dla anten pasywnych. **W praktyce usunięto więc zapisy kluczowe dla zrozumiałości przyjętego zakresu funkcji krytycznych. Dlatego też proponujemy zamianę obecnej treści Załącznika 3 na tabelę z dokumentu ENISA z grudnia 2020.**

Propozycja 2
W art. 1 pkt 50 skreśla się pkt 61) (Załącznik nr 3).

			Uzasadnienie: Zmiana skorelowana jest z pkt 27 określającym proponowany tryb określania funkcji krytycznych.	
61	Art. 1 pkt 52 dot. art. 67a I 67b uKSC		POLECENIE I OSTRZEŻENIE – konieczność konsultacji z podmiotami objętymi W zakresie nowych, daleko idących uprawnień Pełnomocnika i Ministra właściwego ds. informatyzacji zauważamy przede wszystkim, że ich skutki mogą być bardzo poważne. Stosowanie tych instrumentów może wpływać na organizację i możliwość prowadzenia działalności przez podmioty nimi objęte. W tym zakresie kluczowe są zalecenia/nakazy w zakresie wdrożeń określonych poprawek bezpieczeństwa, dokonania określonej konfiguracji, odstąpienia od korzystania z określonego sprzętu czy wprowadzenia reguł ruchu sieciowego. Nie zawsze realizacja takich zaleceń/nakazów będzie z perspektywy podmiotu obowiązanego właściwa, proporcjonalna czy nawet możliwa do technicznego wdrożenia. Skutki wydania takich zaleceń lub nakazów mogą dla podmiotu nimi objętego oznaczać brak możliwości utrzymania ciągłości działania, w tym w zakresie funkcji krytycznych. W przypadku operatorów telekomunikacyjnych może to dotyczyć ciągłości działania usług świadczonych także na rzecz kluczowych systemów administracji publicznej lub przedsiębiorstw o istotnym znaczeniu obronno-gospodarczym. Stąd kluczowe jest, aby na etapie analiz o których mowa w art. 67a ust. 2 oraz art. 67b ust. 5 przeprowadzany był także dialog z podmiotami potencjalnie obowiązanymi do stosowania ostrzeżeń lub poleceń w celu ustalenia najwłaściwszej z ich perspektywy ścieżki działania oraz ustalenia technicznych możliwości realizacji planowanych zaleceń/nakazów. Ponadto polecenie lub ostrzeżenie powinny określać adekwatny czas na wdrożenie. Należy wprowadzić także katalog okoliczności umożliwiających podmiotowi do którego zalecenie jest kierowane podjęcie innych niż wskazane działań, ale o podobnym skutku z perspektywy bezpieczeństwa. W szczególności natychmiastowe wykonanie poleceń lub zaleceń powinno być ograniczone jeśli miałoby to spowodować wystąpienie naruszenia obowiązków wynikających z przepisów prawa, ryzyka utraty ciągłości działania świadczonych usług lub wręcz wystąpienie incydentu lub zagrożenia bezpieczeństwa u podmiotu obowiązanego do stosowania polecenia lub ostrzeżenia – szczególnie jeśli możliwe byłyby inne działania mitygujące. O braku możliwości zastosowania polecenia lub ostrzeżenia adresat mógłby informować organ wydający polecenie lub ostrzeżenie. Polecania/zalecenia powinny jednocześnie dotyczyć wyłącznie zakresu w jakim występuje incydent krytyczny.	

62	Art. 1 pkt 53 dot. rozdziału 13a uKSC		FUNDUSZ CYBERBEZPIECZEŃSTWA – niejasne zasady i krąg podmiotowy odbiorców wsparcia W projektowanych przepisach dot. funduszu cyberbezpieczeństwa, finansowanego m.in. z 50% opłat za numerację, wskazano, że kosztami Funduszu będą m.in.: 2) koszty działań związanych ze zwiększeniem poziomu bezpieczeństwa systemów informacyjnych, z wyjątkiem systemów, o których mowa w pkt 3; 3) koszty działań związanych ze zwiększeniem poziomu bezpieczeństwa systemów infrastruktury krytycznej; W zakresie działań dot. bezpieczeństwa systemów informacyjnych ograniczeniem możliwości wsparcia działalności przedsiębiorstw w tym zakresie jest przyjęta formuła dotacji celowej. Wydaje się, że wsparcie (podobnie jak projektowane środki w ramach KPO i FERC) przeznaczane byłyby przede wszystkim na potrzeby administracji publicznej, z pominięciem znaczenia wyzwań cyberbezpieczeństwa po stronie sektora prywatnego. Podobnie w przypadku potencjalnego wsparcia dot. infrastruktury krytycznej. Z uwagi na przewidziany w art. 72a ust. 9 wymóg uzyskania zgody Rady Ministrów w drodze uchwały, zamknięta wydaje się droga do ewentualnego wsparcia podmiotów spoza sektora publicznego. W naszej ocenie stworzenie Funduszu Cyberbezpieczeństwa powinno służyć nie tylko wsparciu podmiotów publicznych, ale proporcjonalnie do ich znaczenia i potrzeb także podmiotów sektora prywatnego, w szczególności jeśli pełnią istotne funkcje w ramach KSC czy infrastruktury krytycznej.	
63	Art. 1 pkt 56 dot. Dział III uKSC		OPERATOR STRATEGICZNEJ SIECI BEZPIECZEŃSTWA – zakres świadczonych usług Kluczowym aspektem planowanego uruchomienia OSSB jest potencjalny wpływ tej inicjatywy na komercyjny rynek telekomunikacyjny i teleinformatyczny. Kierunek dotyczący projektowania i uruchomienia w różnych krajach UE i na świecie systemów w zakresie tzw. Public Protection and Disaster Relief (PPDR) jest powszechnie znany i akceptowany. Możliwość taka powinna i jest rozpatrywana w kategoriach niezbędnego służbom narzędzia służącego zapewnianiu bezpieczeństwa publicznego, które jest kluczowe także z perspektywy ciągłości funkcjonowania podmiotów sektora prywatnego. Jak komunikowaliśmy już dotychczas jest to zakres, który znajduje nasze pełne zrozumienie. Niestety jednak projektowane przepisy dotyczące Operatora SSB wydają się znacznie wykraczać poza zakres ruchomej sieci specjalnej dla służb bezpieczeństwa, a wkraczają wyraźnie w inne	

			zakresy zarówno jeśli chodzi o podmioty, jak i zakres usług mający obejmować także np. kwestie cyberbezpieczeństwa. Stąd w dalszych uwagach postulujemy wyraźnie doprecyzowanie zakresu działania Operatora SSB, które na poziomie szczegółowości i przejrzystości powinno odpowiadać chociażby projektowi ustawy dot. Sieci Łączności Rządowej zaprezentowanej w 2019 r. przez MSWiA, z którego zresztą część zapisów została skopiowana. 1) Należy wykreślić fragment projektowanego art. 76c ust. 1, który wskazuje na możliwość świadczenia usług innych niż usługi telekomunikacyjne, w tym w szczególności dotyczących cyberbezpieczeństwa. W przypadku sieci specjalnej jej bezpieczeństwo powinno być immanentną cechą, a nie świadczone jako odrębna usługa. Zakres działania OSSB powinien być ściśle ograniczony do obszaru telekomunikacji. 2) W art. 76d należy wprost wskazać, że Operator SSB świadczy usługi w zakresie telekomunikacji (głos i dane) jedynie w zakresie w jakim są one bezpośrednio związane z wykonywaniem zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. 3) Zakres usług określonych w art. 76d ust. 2 i 3 wskazuje zakres w jakim Operator SSB ma faktyczną pozycję monopolistyczną. Zakres ten jednocześnie znacząco wykracza w naszej ocenie poza zakres usług świadczonych w sieciach typu PPDR i dotyczy szerokiego portfolio usług telekomunikacyjnych i teleinformatycznych. W naszej ocenie powinien on pozostać regulowany na dotychczasowych zasadach. W przypadku utrzymania planowanych rozwiązań należy dookreślić, że Operator SSB ma obowiązek korzystać z dostępnej, istniejącej infrastruktury telekomunikacyjnej, a nie dublować ją z wykorzystaniem środków publicznych. 4) Należy usunąć określenie Strategicznej Sieci Bezpieczeństwa jako „ruchomej publicznej sieci telekomunikacyjnej”, ponieważ zgodnie z ustawową definicją sieci publicznej, służy ona głównie do świadczenia „publicznie dostępnych usług telekomunikacyjnych”, co pozostaje w sprzeczności z naturą sieci specjalnej. W przypadku świadczenia usług publicznie dostępnych (czyli świadczonych w sieci publicznej), zakres odbiorców tej usługi nie może zostać zawężony do z góry ograniczonego kręgu, tak jak ma to miejsce w art. 76 d projektu ustawy. Zachodzi zatem sprzeczność pomiędzy słusznie zaprojektowanym ograniczeniem katalogu podmiotów uprawnionych do korzystania z usług OSSB (wymagających, jak była wyżej mowa w stanowisku Lewiatana, dalszego jeszcze doprecyzowania) a kwalifikacją tej sieci specjalnej jako publicznej sieci telekomunikacyjnej.	
64	Art. 76a		Operator Strategicznej Sieci Bezpieczeństwa – zasady kontroli działalności	

			Prezes Rady Ministrów jako organ wyznaczający operatora SSB (ewentualne UKE lub organ taki jak ABW) powinien mieć przyznane szczególne uprawnienia do kontroli działalności prowadzonej przez operatora SSB pod katem jej zgodności z przepisami prawa, a także racjonalności i efektywności działania w zakresie gospodarowania mieniem i środkami publicznymi. Operator SSB powinien być zobowiązany do szczegółowego raportowania w zakresie swojej działalności co najmniej raz w roku. Równolegle powinny zostać wprowadzone przepisy umożliwiające odwołanie danego podmiotu z funkcji Operatora SSB w przypadku stwierdzenia naruszeń lub istotnej nieefektywności działania. Mogłoby to następować w szczególności w wyniku prowadzonych kontroli lub oceny przedłożonego sprawozdania.	
65	art. 76c ust. 1		W **art. 76c ust. 1** – dookreślenie zakresu usług świadczonych przez OSSB, który powinien obejmować wyłącznie „zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego". Przy czym usługi świadczone przez OSSB dotyczyć powinny ściśle wykonywania wskazanych wyżej zadań bezpośrednio przez osoby realizujące te zadania w jednostkach organizacyjnych organów i instytucji administracji , w ramach ich kompetencji w tym zakresie.	
66	art. 76d ust. 4 projektu KSC		Zgodnie z projektowanym przepisem, Prezes Rady Ministrów „może zobowiązać" Operatora SSB do świadczenia usług, o których mowa w art. 76c ust. 1 projektu KSC, właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej lub przedsiębiorcom, o szczególnym znaczeniu gospodarczo-obronnym. Zwracamy uwagę, że w przypadku powyższej propozycji, projektodawca posługuje się inną konstrukcją, niż dla świadczenia usług podmiotom wskazanym w art. 76d ust. 1 projektu KSC, w którym to przypadku świadczenie tych usług następuje „na wniosek tych podmiotów". Nie jest przy tym jasne, jakie faktyczne skutki ma „zobowiązanie" przez Prezesa Rady Ministrów operatora SSB do świadczenia usług na rzecz właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej lub przedsiębiorców, o szczególnym znaczeniu gospodarczo-obronnym, w szczególności czy takie zobowiązanie wobec operatora SSB rodzi także „obowiązek" korzystania z tych usług przez w/w podmioty (co nie powinno mieć miejsca). Niezależnie od powyższego zwracamy również uwagę, że zgodnie z art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, również infrastruktura telekomunikacyjna może być także zaliczana do kategorii infrastruktury krytycznej, która obejmuje między innymi systemy łączności. Poszczególne obiekty, instalacje lub urządzenia stanowiące infrastrukturę telekomunikacyjną, należące do przedsiębiorców telekomunikacyjnych, mogą zatem zostać ujęte w wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury	

			krytycznej z podziałem na systemy, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym. Natomiast w przypadku rozporządzenie Rady Ministrów w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym z dnia 3 listopada 2015 r., zawiera ono w swym załączniku wykaz ponad 200 przedsiębiorców, w tym także przedsiębiorców telekomunikacyjnych. W skrajnym przypadku można sobie zatem wyobrazić sytuację, że na bazie projektowanych przepisów zakres podmiotów, którym w praktyce operator SSB może świadczyć usługi telekomunikacyjne, o których mowa w art. 76a ust.1 będzie bardzo istotnie poszerzony, a do korzystania z nich będą zobowiązani nawet sami przedsiębiorcy telekomunikacyjni. W naszej ocenie przepisy te powinny zostać usunięte z projektu ustawy.	
67	art. 76e projektu KSC		Zgodnie z projektowanym przepisem przy zawieraniu umów, o których mowa w art. 76d ust. 6, dotyczących realizacji zadań, o których mowa w art. 76a ust. 1, nie stosuje się przepisów ustawy Prawo zamówień publicznych. Zwracamy uwagę, że w poprzedniej wersji projektu ustawy KSC z marca br. zawarty był przepis (ówczesny art. 56c ust. 2 projektu KSC) odnoszący się do poziomu cen usług świadczonych przez operatora SSB (wtedy operatora SKS), zgodnie z którym cena za usługi świadczone przez operatora sieci komunikacji strategicznej miała być ustalana „z uwzględnieniem zasad handlowych i interesu publicznego". W aktualnej wersji projektu ustawy przepis ten został wykreślony. W zakresie poziomu cen za usługi świadczone przez operatora SSB nie jest przewidziana zatem żadna regulacja, która adresowałaby ryzyko czy to zawyżania czy to zaniżania tych cen. Oznacza to, że na określonym „monopolistycznym" rynku usług świadczonych przez operatora SSB (bo taki monopol projektowana ustawa w praktyce tworzy), operator SSB, wyłączony z reżimu oferowania usług z uwzględnieniem przepisów o zamówieniach publicznych, będzie miał pełną dowolność w zakresie kształtowania poziomu tych cen. Z oczywistych względów sprzyja to nieefektywności w działaniu tego podmiotu. Takie rozwiązanie jest szkodliwe zarówno z punktu widzenia podmiotów zobowiązanych ustawowo do korzystania z tych usług (ryzyko zawyżania cen), jak i innych przedsiębiorców telekomunikacyjnych już działających na rynku, oferujących swoje usługi podmiotom publicznym (ryzyko stosowania przez operatora SSB – w zależności od potrzeby – cen zaniżonych).	
68	Art. 76f		W zakresie szczególnych uprawnień dot. dostępu postulujemy doprecyzowanie przepisu polegające na wskazaniu na obowiązek dostępu do zasobów nieaktywnych w zakresie sieci	

			radiowej (tj. infrastruktury pasywnej), a także doprecyzowanie konieczności uwzględniania adekwatnych cen rynkowych.	
69	Rozdział 2 w dziale III		W projekcie ustawy przedstawione są plany dotyczące regulacji na poziomie ustawowym dot. zasad powołania Spółki Polskie 5G w tym udziału w niej prywatnych podmiotów. Przepisy przewidują, że decydującą rolę w takim podmiocie będą mieli udziałowcy ze strony publicznej (operator SSB i/lub PFR), natomiast podmioty prywatne miałyby bardzo ograniczony wpływ na działalność spółki. W naszej ocenie powołanie takiego podmiotu powinno odbywać się na zasadach rynkowych, w ramach wspólnych, opartych o przepisy ogólne i odpowiednie umowy ustaleń podmiotów tworzących ten podmiot. Stąd uważamy, że rozdział 2 w dziale III pt. 'Spółka Polskie 5G', powinien zostać usunięty w całości.	
70	Rozdział 3 w dziale III		Uwzględniając przedstawione powyżej uwagi dot. postulowanego wykreślenia przepisów w rozdziale 2 w dziale III pt.' Spółka Polskie 5G', odpowiednio powinny zostać wykreślone przepisy dot. sposobu dystrybucji częstotliwości z pasma 700 MHz dla operatorów zawarte w art. 76 p i art. 76r, które to powinny zostać rozdystrybuowane na zasadach ogólnych, zgodnych z ustawą Prawo telekomunikacyjne (i projektowaną ustawą Prawo komunikacji elektronicznej). Niezależnie od tego postulatu podstawowego wskazujemy także, że planowana w przepisach konstrukcja rodzi poważne wątpliwości pod kątem zgodności z art. 45 ust. 1 EKŁE który wskazuje, że *„W należytym stopniu uwzględniając fakt, że **widmo radiowe jest dobrem publicznym, które ma istotną wartość społeczną, kulturalną i ekonomiczną**, państwa członkowskie zapewniają efektywne zarządzanie widmem radiowym do celów dostarczania sieci łączności elektronicznej i świadczenia usług łączności elektronicznej na ich terytorium zgodnie z art. 3 i 4. **Zapewniają** także, **aby przeznaczenie widma radiowego na użytek sieci i usług łączności elektronicznej** i wydawanie ogólnych zezwoleń lub indywidualnych praw do użytkowania takiego widma radiowego przez właściwe organy **odbywały się według obiektywnych, przejrzystych, sprzyjających konkurencji, niedyskryminacyjnych i proporcjonalnych kryteriów**"*.	
71	Art. 76l		W projektowanych przepisach dotyczących następstwa podmiotów pełniących funkcję OSSB doprecyzowania wydają się wymagać zasady dotyczące, w szczególności nabytych przez dotychczasowego OSSB szczególnych uprawnień związanych bezpośrednio z jego funkcją i uprawnieniami jako OSSB (a nie dostępnych na warunkach ogólnych dla przedsiębiorców telekomunikacyjnych), w tym dotyczących nabytego majątku lub uprawnień.	

72	Dodatkowa propozycja		**W przypadku nieuwzględnienia propozycji zawartych w pkt 49 i 60, proponujemy usunięcie z listy stanowiącej Załącznik nr 3 do Projektu postanowienia dotyczącego dotyczące RAN w brzemieniu następującym:** *„3. Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych."* **Uzasadnienie:** Jak wskazano wyżej, aktualna lista wydaje się być przygotowana weryfikacji technicznej i rynkowej. Brak zapewnienia udziału podmiotów rynkowej w jej tworzeniu powoduje poważne wątpliwości co do jej zawartości zaproponowanej w załączniku nr 3 do Projektu. W Załączniku nr 3 do Projektu wymieniona jest usługa obejmująca *Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych (*RAN – *Radio Access Network).* Zgodnie jednak z modelem 3GPP (raport ETSI TR 121 915 V.15.0.0. (2019-10), s. 41) funkcje takie jak UDM (*Unified Data Management*), tj. zarządzanie subskrypcją, dane użytkownika, rejestracja i zarządzanie mobilnością oraz ARPF (*Authentication Credential Repository and Processing Function*), tj. przechowanie danych uwierzytelniających, są elementami architektury sieciowej wymagającymi większego poziomu ochrony niż stacje bazowe. Wspomniany raport ETSI został przywołany w § 3 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych, jako wytyczna dla rozumienia pojęcia „sieci 5G" („*Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) (…)*"). Idąc za wskazanym w Raporcie sposobem rozumienia sieci 5G, należy również konsekwentnie przyjąć podział na elementy krytyczne sieci 5G (takie jak UDM, ARPF) i pozostałe, niekrytyczne elementy sieci 5G, do których należy radiowa sieć dostępowa. Podejście przedstawione w Raporcie ETSI zostało również przyjęte w dokumentach Unii Europejskiej (*Raport on EU Coordinated Risk Assessment for 5G*, s. 16 i 17 i Toolbox, s. 39 i 40), z których również wynika, iż RAN nie stanowi krytycznego elementu sieci. Analogiczne podejście, czyli wyłączenie funkcji dostępowych z kategorii krytycznych elementów sieci 5G, przyjął Rząd polski w lipcu 2019 r. w swoim stanowisku, przygotowanym dla potrzeb stworzenia dokumentu *Raport on EU Coordinated Risk Assessment for 5G* (*Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings*, s. 7).	

			Z uwagi na powyższe, zasadne jest usunięcie z listy zawartej w załączniku nr 3, pozycji odnoszącej się do RAN.	

Konfederacja Lewiatan, KL/402/280/AM/2021