Konferencja Naukowa

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 7 sierpnia 2020 r.

GŁÓWNA I UBOCZNA DZIAŁALNOŚĆ PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

PROF. DR HAB. GRAŻYNA SZPOR

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

Termin cyberbezpieczeństwo

Czy wspierać wprowadzanie terminu cyberbezpieczeństwo do aktów prawnych i dokumentów urzędowych?

- przeciw – termin modny ale niejednoznaczny, niejasna podstawa uprawnień i obowiązków potencjalnie niekorzystna dla ich konkretyzowania i egzekwowania [wyeliminowany z NIS]
- za – fakty dokonane: jest definicja prawna, termin zbiorczy dla wielu innych terminów systemu normatywnego [prawnego] i normalizacyjnego, nieatrakcyjne alternatywy
- jeśli także: w literaturze naukowej – tak, w edukacji – tak, w nazewnictwie jednostek organizacyjnych – tak, w języku potocznym - tak
- to łącznie czyni mało prawdopodobną eliminację terminu mimo mankamentów

Konkluzja:

- użyteczne określenie zbiorcze celu o rosnącej wadze
- należy uzgodnić zakres pojęcia postulując korektę definicji ustawowej z uwzględnieniem dyrektywy oraz zestawić i adekwatnie objaśnić inne elementy siatki pojęciowej obejmującej zachowania normatywnie postulowane i realnie obserwowane zorientowane na wspólny cel

Zasadność wyodrębniania działalności w zakresie cyberbezpieczeństwa

- Ułatwić realizację zadań publicznych wyznaczonych podmiotom krajowego systemu cyberbezpieczeństwa

- Przezwyciężyć - przez spójną politykę publiczną i prawo - bariery w działalności gospodarczej

PRAWNE KRYTERIA WYODRĘBNIANIA DZIAŁALNOŚCI W ZAKRESIE CYBERBEZPIECZEŃSTWA

- KRYTERIUM PRZEDMIOTOWE – art. 2 pkt 4. ustawy z 5.07.2018 z 5.07.2018 o krajowym systemie cyberbezpieczeństwa [definicja]
- „cyberbezpieczeństwo – odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne
- KRYTERIUM PODMIOTOWE – art. 4 ustawy z 5.07.2018 o krajowym systemie cyberbezpieczeństwa [dwudziestopunktowe wyliczenie podmiotów określonych indywidualnie lub rodzajowo]

- KRYTERIUM POSTULOWANE – Polska Klasyfikacja Działalności

Kryteria strukturyzacji podmiotów krajowego systemu cyberbezpieczeństwa

1. Adresaci działań

- Podmioty administrujące podnoszące poziom cyberbezpieczeństwa innych podmiotów
- Podmioty zobowiązane w interesie publicznym do dbałości o własne cyberbezpieczeństwo [poza systemem: inne dbające o własne cyberbezpieczeństwo]
- Podmioty wspierające: realizujące usługi na rzecz innych podmiotów krajowego systemu cyberbezpieczeństwa

2. Znaczenie cyberbezpieczeństwa wśród celów i zadań

- główne
- uboczne

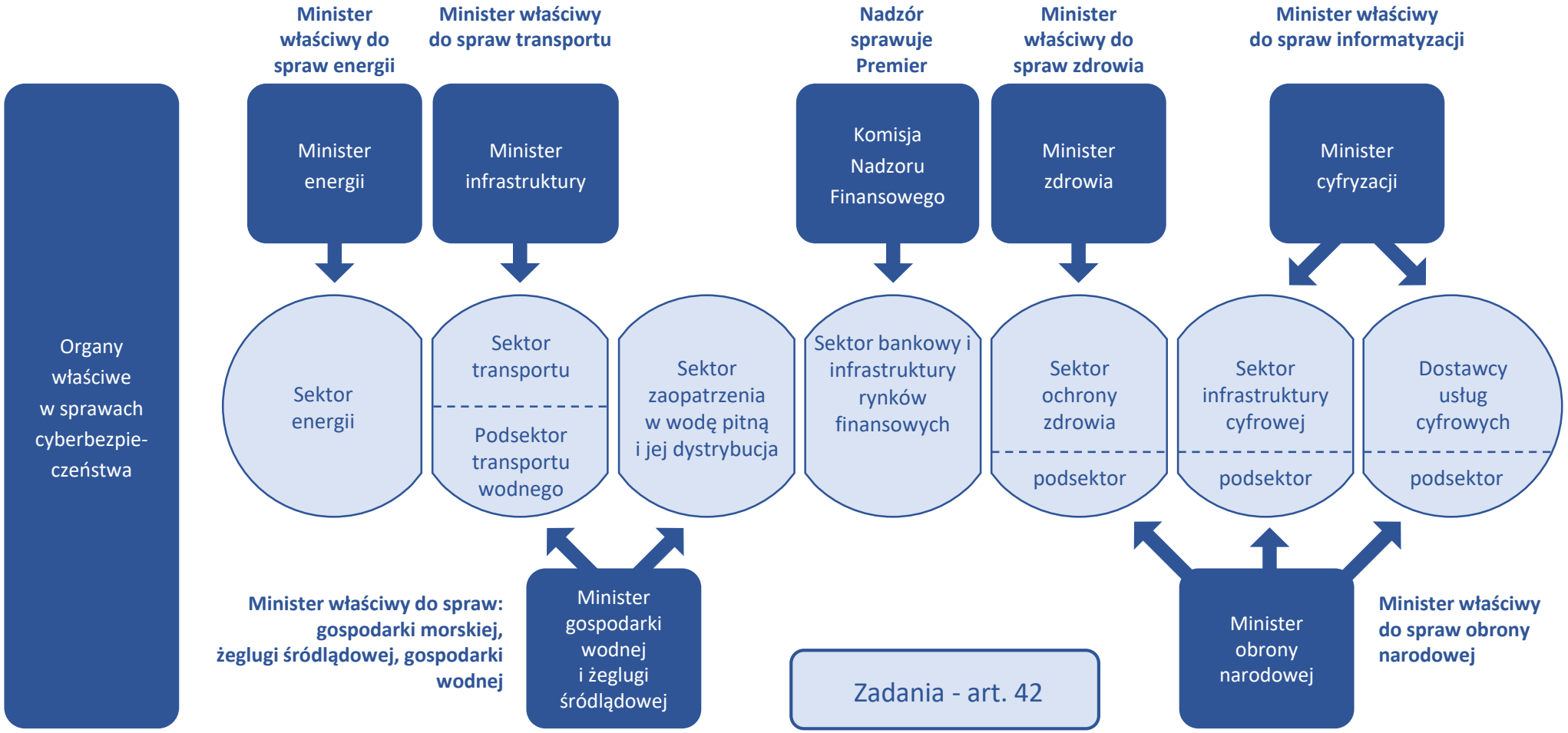
Podmioty administrujące – główna działalność w zakresie cyberbezpiczeństwa

[podnoszące poziom cyberbezpieczeństwa innych podmiotów]

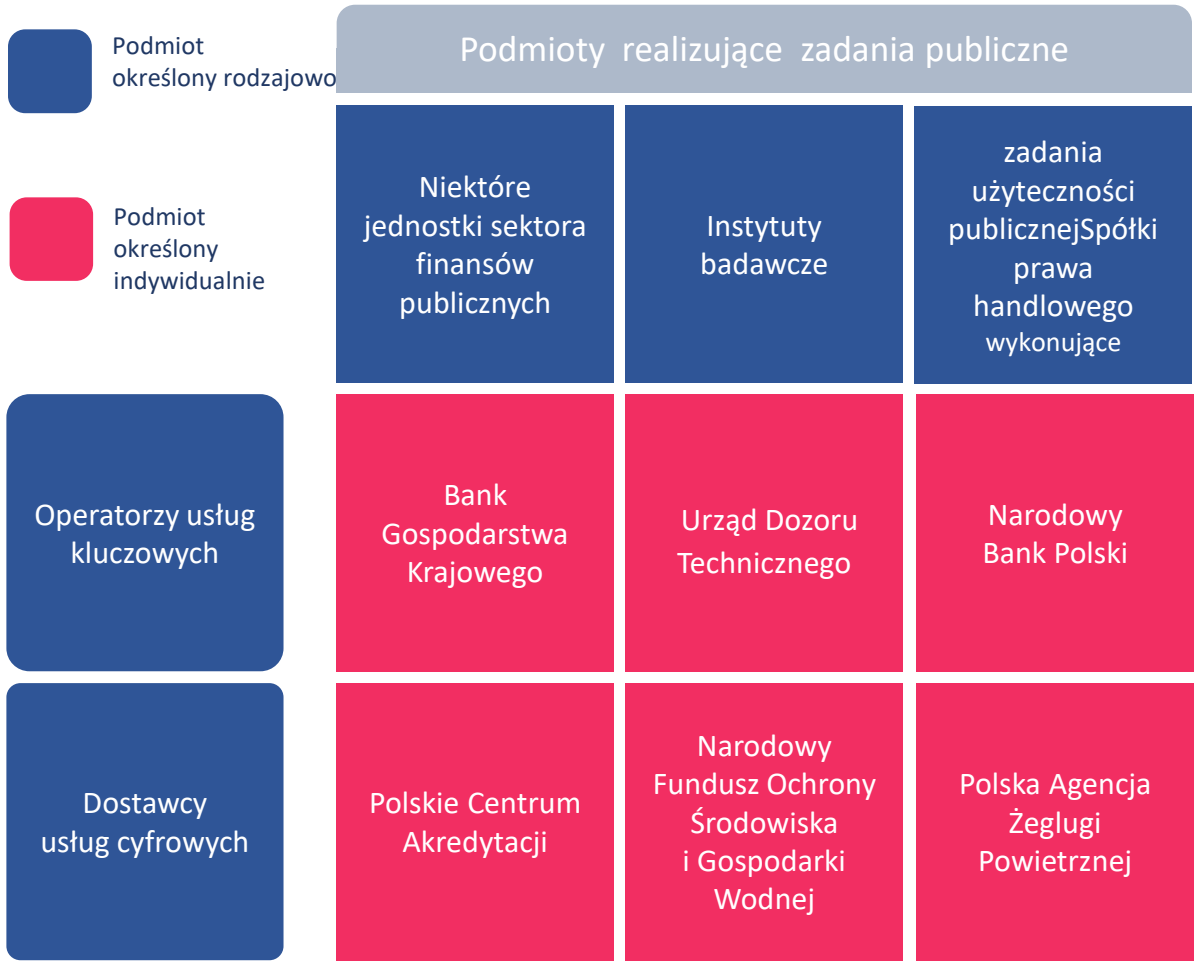
Organy właściwe w sprawach cyberbezpieczeństwa

podnoszące poziom cyberbezpieczeństwa innych podmiotów

dla których cyberbezpieczeństwo jest ubocznym przedmiotem działalności



Podmioty KRC zobowiązane w interesie publicznym do dbałości o własne cyberbezpieczeństwo co stanowi uboczny element działalnosci



Podmioty wspierające pozostałych uczestników KSC – których działalność główna albo uboczna odnosi się do cyberbezpieczeństwa

Podmioty świadczące usługi z zakresu cyberbezpieczeństwa

- Spełniają warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej
- Dysponują pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi
- Stosują zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów
- Podstawa prawna: Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

Operatorzy usług kluczowych w celu realizacji swoich zadań mogą zawierać z tymi podmiotami umowy

Wnioski:

- Ustanowić lub lepiej wykorzystać istniejące instrumenty prawne generalne i indywidualne dla wzmocnienia kapitału ludzkiego w zakresie cyberbezpieczeństwa
- poprzez: działalność naukowo-badawczą, edukacyjną i optymalizującą zatrudnienie
- kierowaną łącznie do: kadr sektora cyberbezpieczeństwo i kadr rozproszonych w podmiotach dla których działalność w zakresie cyberbezpieczeństwa jest dodatkowa
- w szczególności: wyodrębnić sektor cyberbezpieczeństwo w klasyfikacji działalności [PKD]
- stworzyć ramy organizacyjne współdziałania rad sektorowych w zakresie dotyczącym cyberbezpieczeństwa w sektorach i zapewnić koordynację.