**Zestawienie uwag zgłoszonych w trakcie konsultacji publicznych**

**Uwagi od podmiotów:**

Osoba fizyczna 1, FILIPIAKBABICZ Kancelaria Prawna (adw. Michał Babicz, dr Łukasz Pilarczyk, adw. dr. Piotr Karlik), STRATPOINTS, NOKIA, Konfederacja Lewiatan (KL), SEQRED, Krajowa Izba Komunikacji Ethernetowej (KIKE), Związek Banków Polskich (ZBP), Polska Izba Komunikacji Elektronicznej (PIKE), Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczne (PTI), Fundacja INFO OPS Polska, Instytut Bezpieczeństwa i Strategii (IBiS), Fundacja Bezpieczna Cyberprzestrzeń (FBC), Izba Gospodarcza Gazownictwa (IGG), Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT), Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa (SKOK), Instytut Kościuszki (IK), Osoba fizyczna 2.

(W kolumnie „Jednostka redakcyjna, do której wnoszone są uwagi” w nawiasach podano rzeczywiste punkty odnoszące się do PSC.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nazwa projektu dokumentu: **projektu uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024** | | | | | | |
| **L.p.** | **Podmiot wnoszący uwagę** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Fragment tekstu opiniowanego** | **Treść uwagi wraz z propozycją zmian zapisu** | **Stanowisko MC** | **Stanowisko podmiotu wnoszącego uwagę po konferencji uzgodnieniowej** |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 1.2 (5.2) | Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie realizowane poprzez uruchomienie w roku 2021 przez ministra właściwego do spraw informatyzacji systemu teleinformatycznego wspierającego[[1]](#footnote-1):  1) współpracę podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa,  2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,  3) zgłaszanie i obsługę incydentów,  4) szacowanie ryzyka na poziomie krajowym,  5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.  **6) zbieranie informacji na temat zagrożeń występujących już w przeszłości oraz wyciąganie wniosków a także ulepszanie już wdrożonych rozwiązań.** | Osoba fizyczna 1 proponuje dodać punkt 6:  **6) zbieranie informacji na temat zagrożeń występujących już w przeszłości oraz wyciąganie wniosków a także ulepszanie już wdrożonych rozwiązań.** | **Wyjaśnienie**  Zakres funkcjonalności S46 określa ustawa o KSC. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 1.3 (p 5.3) | Niezbędna jest budowa **odseparowanego,** odpornego na cyberzagrożenia systemu wymiany informacji dla potrzeb administracji publicznej | Osoba fizyczna 1 proponuje dodać zwrot **„odseparowanego”** | **Wyjaśnienie**  Odseparowanie systemu zawiera się w ogólnej odporności na cyberzagrożenia. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 1.4 (p 5.4) | ze szczególnym uwzględnianiem **zarządzania ciągłością działania** | Osoba fizyczna 1 proponuje zamienić zwrotem **„weryfikowanej okresowo ciągłości działania.”** | **Wyjaśnienie**  Okresowe weryfikowanie wpisuje się w zarządzanie ciągłością działania. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 1.6 (p 5.6) | wymagane są sprawne**, odseparowane** i zaufane kanały | Osoba fizyczna 1 proponuje dodać zwrot **„odseparowane”** | **Uwaga nieuwzględniona**  Zaufane kanały z założenia są odseparowane. Nie ma potrzeby uszczegółowiania. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 1.6 (p 5.6) | operatorzy usług kluczowych, dostawcy usług cyfrowych, **branża bankowa,** dostawcy usługi dostępu do Internetu | Osoba fizyczna 1 proponuje dodać zwrot **„branża bankowa”** | **Wyjaśnienie**  Sektor bankowy jest już częścią ksc. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:   1. **użytkowników,** 2. aplikacji, 3. urządzeń mobilnych, 4. stacji roboczych, 5. serwerów i sieci, 6. modeli chmur obliczeniowych. | Osoba fizyczna 1 proponuje dodać jako pierwszy punkt:   1. **„użytkowników”** | **Wyjaśnienie**  Zakres Narodowych Standardów Cyberbezpieczeństwa określać będzie uchwała WIIP.  Przedstawiony zbiór wymagań jest zbiorem otwartym. Obejmie również użytkowników. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 2.2 (p 6.2) | uruchomienie, **testy,** bieżące utrzymanie, serwisowanie oraz naprawy. | Osoba fizyczna 1 proponuje dodać zwrot **„testy”** | **Wyjaśnienie**  Testy powinny zawierać się w bieżącym utrzymaniu |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 2.2 (p 6.2) | Jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń, są okresowe audyty. Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz specyfikę poszczególnych sektorów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów. | Osoba fizyczna 1 Branża energetyczna ze względu na ogromną ilość urządzeń OT, będzie audytowana inaczej niż np. branża administracji publicznej. Rekomenduje stworzyć podział ze względu na "rodzaj" branż. | **Uwaga uwzględniona**  Jest to już zaznaczone w Strategii. „Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz **specyfikę poszczególnych sektorów.”** |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 2.3 (p 6.3) | Kolejnym środkiem oceny bezpieczeństwa są okresowe testy (w tym testy penetracyjne), które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. | Osoba fizyczna 1 Większość testów penetracyjnych bazuje na "znanych" podatnościach. | **Uwaga uwzględniona**  Nie sposób testować odporność systemu na nieznane zagrożenia np. ataki z użyciem luk 0-day z racji specyfiki tych luk. |  |
|  | Osoba fizyczna 1 | Uwaga o cel szczegółowy 3.4 (p 7.4) | rozpoznawanie zagrożeń, ochronę i **obronę systemów teleinformatycznych** | Osoba fizyczna 1 proponuje zamienić zwrotem **„i zapobieganie zagrożeniom”** | **Wyjaśnienie**  Zastosowano termin „zwalczanie źródeł zagrożeń” jako wystarczający. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga ogólna |  | FILIPIAKBABICZ Kancelaria Prawna: brak odwołań do jakichkolwiek danych czy analiz pozwalających na powiązanie przedstawionych kwestii z ich rzeczywistym obrazem | **Uwaga nieuwzględniona**  Niniejszy dokument ma charakter strategiczny i postulatywny. Kwestie analityczne nie są w nim poruszane. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga ogólna |  | FILIPIAKBABICZ Kancelaria Prawna: Duża część zapisów stanowi bezpośrednie powtórzenie tych zawartych w dokumencie pt. „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej”, który został opracowany jeszcze w 2017 r. a więc przed uchwaleniem Dyrektywy NIS oraz ustawy o KSC | **Uwaga nieuwzględniona**  Strategia jest kontynuacją i rozszerzeniem działań rządu RP z poprzednich lat. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga ogólna |  | FILIPIAKBABICZ Kancelaria Prawna: Nie odwołuje się do obecnego stanu cyberbezpieczeństwa państwa i stanowi jedynie teoretyczny, całkowicie abstrakcyjny zbiór postulatów | **Uwaga nieuwzględniona**  Niniejszy dokument ma charakter strategiczny i postulatywny. Kwestie analityczne nie są w nim poruszane.  Do obecnego stanu cyberbezpieczeństwa odwołują się inne dokumenty o charakterze analitycznym i prawnym (np. ustawa o KSC). |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o treść Kontekstu Strategicznego (p. 2) |  | FILIPIAKBABICZ Kancelaria Prawna: brak propozycji lub chociaż założeń planowanych działań wynikających z analiz istniejącego ryzyka | **Uwaga nieuwzględniona**  Kontekst strategiczny z definicji nie powinien zawierać planowanych działań. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o treść Kontekstu Strategicznego (p. 2) |  | FILIPIAKBABICZ Kancelaria Prawna: strategia powinna, na pewnym poziomie ogólności, wskazywać najbardziej pożądane środki realizacji zakładanych celów | **Uwaga nieuwzględniona**  Strategia wskazuje na kierunki interwencji rządu RP.  Konkretne działania wraz z harmonogramem ich realizacji zostaną określone w Planie działań. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o treść Kontekstu Strategicznego (p. 2) | „realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni […] rząd będzie w pełnie respektować prawo do prywatności oraz stać na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa” | FILIPIAKBABICZ Kancelaria Prawna: zagadnienia te zostały w sposób identyczny określone w dokumencie pt. „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej. Wobec braku rozwinięcia tej kwestii trudno odnieść się do niej w sposób konstruktywny. Należy zatem przyjąć, że zapis ten stanowi swoistą deklarację niezobowiązującą. | **Uwaga nieuwzględniona**  Strategia jest kontynuacją i rozszerzeniem działań rządu RP z poprzednich lat. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwagi o treść Zakresu Strategii (p. 3) | Strategia uwzględnia, w szczególności:  1) cele i priorytety państwa w zakresie cyberbezpieczeństwa,  2) podmioty zaangażowane we wdrażanie i realizację Strategii,  3) środki służące realizacji celów Strategii,  4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym,  5) podejście do oceny ryzyka,  6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,  7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa | FILIPIAKBABICZ Kancelaria Prawna: Dalsza analiza postanowień Strategii w żaden sposób nie potwierdza tego stwierdzenia. Zapis ten stanowi jedynie machinalne powtórzenie treści art. 69 ust. 2 KSC. Nie tylko nie ma bowiem konkretnych rozważań na ten temat w całej Strategii, ale także brak jakichkolwiek odniesień do wymienionych tutaj kwestii | **Uwaga nieuwzględniona**  Delegacja ustawowa, w tym zakres strategii, są jasno określone w ustawie o ksc. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.1 (p 5.1) | Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.” | FILIPIAKBABICZ Kancelaria Prawna: Strategia jedynie określa, jak ma wyglądać proces ewentualnych zmian ustawodawczych, natomiast w ogóle nie wskazuje, aby jakieś działania nowelizacyjne, np. w zakresie przepisów przewidujących odpowiedzialność karną za cyberprzestępstwa, już obecnie były do podjęcia | **Uwaga nieuwzględniona**  Konkretne działania, w tym także legislacyjne, będą określone w Planie działań. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.4 (p 5.4) | rząd podejmie działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. Ponadto, rząd będzie wspierał te podmioty w reagowaniu na incydenty poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych. | FILIPIAKBABICZ Kancelaria Prawna: Należałoby oczekiwać, że w ramach Strategii zostaną wskazane co najmniej środki służące realizacji tych celów. Brak zdefiniowanych podstawowych zagrożeń i ich prawdopodobieństwo wystąpienia przy odwołaniu się do wcześniejszych incydentów. | **Uwaga nieuwzględniona**  Konkretne działania wraz z harmonogramem ich realizacji zostaną określone w Planie działań. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.5 (p 5.5) | Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych. | FILIPIAKBABICZ Kancelaria Prawna: nic nie wiadomo nawet o ogólnym zarysie takiego systemu, ani o jego podstawowych założeniach. Potrzebny jest wynikający z tego przynajmniej ogólny schemat proponowanych działań. | **Uwaga nieuwzględniona**  „Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 roku.” (p 5.5) |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.6 (p 5.6) | Wdrożone zostaną, skierowane do społeczeństwa, programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób dotkniętych przestępstwem. | FILIPIAKBABICZ Kancelaria Prawna: Dyrektywa NIS wprost wymaga od Strategii, aby obejmowała ona także: „wskazówki odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących strategii w zakresie bezpieczeństwa sieci i systemów informatycznych” – nie wystarczające jest zatem stwierdzenie, że dane programy informacyjne powstaną – do czego ogranicza się Strategia. Niezbędne jest jeszcze określenie, co właściwie mają one zawierać (poza elementami podstawowymi), a tego już Strategia nie czyni. | **Uwaga nieuwzględniona**  Nie wydaje się uzasadnionym, aby doprecyzować treść programów na poziomie strategicznym. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.6 (p 5.6) |  | FILIPIAKBABICZ Kancelaria Prawna: Dyrektywa NIS, jak i KSC nakazują strategii odniesienie się do „programów edukacyjnych, informacyjnych i szkoleniowych” – wymienienie trzech kategorii tych programów oznacza, że każdy z ich rodzajów powinien się różnić od pozostałych i do każdego indywidualnie powinna się odnosić Strategia, ta jednak pomija programy szkoleniowe. | **Wyjaśnienie**  Odnosi się do tego pkt 8.1. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.6 (p 5.6) | Biorąc pod uwagę dużą dynamikę przestępstwa w cyberprzestrzeni i związana z tym konieczność podejmowania czynności operacyjnych i procesowych niezbędne jest wprowadzenie przepisów umożliwiających przetwarzanie dokumentów procesowych w postaci elektronicznej i przesyłanie ich w takiej postaci. | FILIPIAKBABICZ Kancelaria Prawna: trudno jest ustalić, o jakie konkretnie dokumenty może chodzić. Nie wiadomo także dlaczego akurat ten aspekt prowadzenia postępowań został uznany za tak dalece istotny, że został wpisany do Strategii. Całkowicie pominięta została także kwestia tego, że już od paru lat zarówno w sądach jak i w prokuraturach funkcjonują systemy informatyczne. | **Wyjaśnienie**  Zgodnie z informacjami od partnerów rządowych jest to obszar wymagający regulacji. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 1.6 (p 5.6) |  | FILIPIAKBABICZ Kancelaria Prawna: Nie bez znaczenia byłoby także wprowadzenie zmian w strukturach organizacyjnych Komend Wojewódzkich, tak aby doszło do realnego, a nie jak to ma obecnie jedynie pozornego, wyspecjalizowania odpowiednich komórek w zakresie walki z cyberprzestępczością. Podobne działania powinny zostać podjęte również w prokuraturach, które jak dotąd nie wyodrębniły ze swojej struktury dedykowanych komórek do walki z cyberprzestępczością | **Uwaga nieuwzględniona.**  Konkretne działania wraz z harmonogramem ich realizacji zostaną określone w Planie działań. |  |
|  | FILIPIAKBABICZ Kancelaria Prawna | Uwaga o cel szczegółowy 3.1 (p 7.1) | Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa. Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz **studiów doktoranckich** i podyplomowych. | FILIPIAKBABICZ Kancelaria Prawna: od 2018 r., na mocy ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668) na uczelniach wyższych funkcjonują **szkoły doktorskie**, a studia doktoranckie jako takie zostały zlikwidowane. | **Uwaga uwzględniona** |  |
|  | STRATPOINTS | Uwaga o dodanie celu szczegółowego |  | **Cel szczegółowy:** Tworzenie i rozwijanie zdolności obrony cybernetycznej w okresie pokoju i wojny oraz warunków do rażenia przeciwnika.   1. Implementacja najnowocześniejszych technologii teleinformatycznych do wojska, zdolnych przeprowadzić atak cybernetyczny na potencjalnego przeciwnika lub odeprzeć atak na instytucje wojskowe i państwowe w okresie pokoju i wojny 2. Stworzenie krajowego systemu kryptologicznego 3. Wypracowanie warunków interoperacyjności krajowych wojsk cybernetycznych z NATO i odpowiednikami w innych państwach sojuszniczych 4. Współdziałanie z podmiotami, instytucjami i służbami tworzącymi krajowy system bezpieczeństwa | **Uwaga nieuwzględniona**  Podane punkty są zawarte w Strategii w różnej formie w p 7.4, 9.1 czy 9,2.  Krajowy System Kryptologiczny – istnieje już Narodowe Centrum Cyberbezpieczeństwa zajmujące się m.in. kryptografią |  |
|  | STRATPOINTS | Uwaga o cel szczegółowy 2.3 (p 6.3) | W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. bug-bounty. | Korzystanie z modelu bug-bounty jest ryzykowne. Dajemy dostęp hakerom do systemów, które mogą zostać rozpoznane. Nie ma przy tym pewności, że osoba (lub co gorsza wroga agencja) zgłosi lukę. Może ją bez rozgłosu wykorzystać do własnych celów. Ponadto program taki zakłada wysokie wynagrodzenia za znalezienie luk, natomiast projekt nie przewiduje dodatkowych nakładów finansowych poza stosunkowo niewielkimi uchwalonymi w ustawie. | **Uwaga nieuwzględniona**  Kwestie używania tzw. bug bounty oraz testów penetracyjnych zostały określone w art. 269b i c Kodeksu karnego. |  |
|  | STRATPOINTS | Uwaga o cel szczegółowy 3.4 (p 7.4) | Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych oraz zwalczanie źródeł zagrożeń. | Pełne spektrum działań militarnych w zakresie cyberbezpieczeństwa poza rozpoznaniem zagrożeń, ochroną i obroną oraz zwalczaniem zagrożeń powinno przewidywać również **działania ofensywne**. | **Uwaga nieuwzględniona**  Zostało zawarte „zwalczanie źródeł zagrożeń” (p 7.4). |  |
|  | STRATPOINTS | Uwaga o cel szczegółowy 4.1 (p 8.1) | W celu utrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, podjęte będą działania w celu zbliżenia zarobków tych pracowników do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym”. | Nie bardzo wiadomo jaki mechanizm zostanie zastosowany w instytucjach państwowych np. takich jak wojsko. Aby wyrównać zarobki żołnierza cyberspecjalisty należałoby mu dać dodatek w wysokości kilku tysięcy procent. Czy będzie zarabiał więcej niż generał dowódca dywizji, w której pełni służbę. Poza tym, nie przewiduje się zwiększonych środków. W tabeli środki finansowe jest stwierdzenie „Nie powodują dodatkowych skutków finansowych”. | **Uwaga nieuwzględniona**  Strategia, jako uchwała, nie może być źródłem wydatków publicznych. Kwestie polityki kadrowej i wynagrodzeniowej są w zakresie poszczególnych jednostek w ramach obowiązujących przepisów. |  |
|  | NOKIA | Uwaga o treść wstępu |  | NOKIA: Sugerujemy wprowadzenie odnośnika do infrastruktury krytycznej już we wprowadzeniu | **Uwaga nieuwzględniona**  Jest to strategia cyberbezpieczeństwa, w której wielokrotnie pojawia się kwestia infrastruktury krytycznej, w tym kierunki działań związane z zapewnieniem interoperacyjności obu systemów. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o treść kontekstu strategicznego | rząd będzie w pełni respektował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa. | NOKIA: Nie tylko ‘respektował’, ale też powinien ‘**gwarantować**’ prawo do prywatności | **Uwaga uwzględniona** | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o treść wizji (p 4.1) | standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń, **wsparcia i utrzymania sieci** i usług cyfrowych. | NOKIA: Proponuje dodać zwrot „**wsparcia i utrzymania sieci**” | **Uwaga nieuwzględniona**  Niepotrzebne wyszczególnianie. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o treść celu głównego (p 4.2) | zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, **prywatnym** | NOKIA: Proponuje zamienić zwrot „**prywatnym**” na „**działalności gospodarczej**” | **Uwaga nieuwzględniona**  Termin „sektor prywatny” jest szerszym pojęciem. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.1 (p 5.1) | w szczególności świadczących usługi **publicznych** chmur obliczeniowych | NOKIA: Proponuje dodanie zwrotu „**publicznych**” | **Uwaga nieuwzględniona**  Nie zawężamy tylko do chmur publicznych. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.1 (p 5.1) | Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnych w cyberprzestrzeni. | NOKIA: Sugerujemy, że legislacja w dziedzinie narzędzi podwójnego zastosowania powinna odbyć się na poziomie ogólnoeuropejskim (tak jak na poziomie europejskim regulowany jest eksport dóbr podwójnego zastosowania) | **Uwaga nieuwzględniona**  Część z tych regulacji pozwala na działania na poziomie krajowym. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.1 (p 5.1) | Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie **okresowe** monitorowanie zjawisk tam zachodzących | NOKIA: Proponuje zmianę zwrotu z „**okresowe**” na „**ciągłe**” | **Uwaga uwzględniona** | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.2 (p 5.2) | Organy właściwe, odpowiedzialne za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe | NOKIA: W jakiej procedurze organy te będą wyznaczone? | **Wyjaśnienie**  Już są wyznaczone w KSC – rozdz. 8, art. 41 | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.2 (p 5.2) | w których świadczone są usługi kluczowe i usługi cyfrowe | NOKIA: Sugerujemy wypracowanie definicji/katalogu usług kluczowych | Wyjaśnienie  Usługi kluczowe są wskazane w Załączniku nr 1 do ustawy o ksc. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.2 (p 5.2) | powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli. | NOKIA: Czy sektor prywatny automatycznie przyjmie/zaakceptuje standardy wprowadzone przez administrację publiczną? | **Wyjaśnienie**  Standardy te będą opracowane z należytą dokładnością i starannością, aby ich jakość stanowiła zachętę dla sektora prywatnego. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.5 (p 5.5) | Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 roku. | NOKIA: Bardzo ważny punkt - w miarę możliwości postulujemy jak najszybsze (jeszcze przed 2020) wypracowanie takiej metodyki i narzędzi | **Uwaga częściowo uwzględniona**  Prace są prowadzone, a Harmonogram prac nad NPC został już ustalony. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 1.6 (p 5.6) | W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych **oraz zapewnienie ‘łańcucha zaufania’**. | NOKIA: Proponuje dodanie zwrotu „**oraz zapewnienie ‘łańcucha zaufania’**” | **Uwaga nieuwzględniona**  Ten termin wymaga dopracowania i nie jest właściwym umieszczanie go na poziomie strategicznym. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 2.1 (p 6.1) | w komitetach technicznych, **Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, a także w zainteresowanych podmiotach publicznych i prywatnych, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm i standardów na konkretne rekomendacje w zakresie ich wdrażania.** | NOKIA: Dla systemów/produktów dla których istnieją odpowiednie normy międzynarodowe (np. 3GPP) powinny być one bezpośrednio przyjęte. Sugerujemy zatem przeformułowanie:  **PKN we współpracy z ośrodkami akademickimi…** **powinien skatalogować istniejące normy międzynarodowe dla poszczególnych kategorii oraz przyjąć konkretne rekomendacje w zakresie ich wdrażania.** | **Uwaga nieuwzględniona**  Propozycja jest niezgodna z systemem normalizacji. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 2.1 (p 6.1) | dotyczących w szczególności bezpieczeństwa:   1. aplikacji, 2. urządzeń mobilnych, 3. stacji roboczych, 4. serwerów i sieci, 5. modeli chmur obliczeniowych, 6. **wsparcie i utrzymanie sieci/systemów teleinformatycznych** | NOKIA: Proponuje dodać:  **6) wsparcie i utrzymanie sieci/systemów teleinformatycznych** | **Uwaga nieuwzględniona**  Katalog nie jest zamknięty. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 2.2 (p 6.2) |  | NOKIA: Proponujemy dodać paragraf o konieczności weryfikowania poziomu zaufania dostawców infrastruktury, uwzględniając podatność owych dostawców na wpływy państw trzecich | **Uwag nieuwzględniona**  Nie jest to w zakresie Strategii. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 2.2 (p 6.2) | Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów **i systemów** (w szczególności oprogramowania, urządzeń i usług). | NOKIA: Proponuje dodać zwrot „**i systemów**”. | **Uwaga nieuwzględniona**  Wyliczenie w nawiasie: „(**w szczególności** oprogramowania, urządzeń i usług)”. Ponadto nie jest to katalog zamknięty. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 2.2 (p 6.2) | Efektem tych działań będzie uzyskanie na poziomie krajowym zdolności do wspierania polskich **oraz europejskich** producentów którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE. | NOKIA: Proponuje dodać zwrot „**oraz europejskich**” | **Uwaga nieuwzględniona**  Cel wyjaśniony w dalszej części zdania. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o cel szczegółowy 3.1 (p 7.1) | poprzez stwarzanie warunków dla rozwoju przedsiębiorstw **działających w Polsce** | NOKIA: Proponuje dodać zwrot „**działających w Polsce**” | **Uwaga nieuwzględniona**  Nie jest konieczne doprecyzowanie, że chodzi tylko o działające w Polsce przedsiębiorstwa. | **Przyjęte wyjaśnienie.** |
|  | NOKIA | Uwaga o dodanie p 7.5 w celu szczegółowym 3 |  | NOKIA: Proponujemy nowy element strategii (7.5.) skupiony poprawie cyberbezpieczeństwa sektora Public Safety (bezpieczeństwa publicznego) | **Uwaga nieuwzględniona**  Uwaga wymaga dodatkowych wyjaśnień lub propozycji zapisów. Do wyjaśnienia na konferencji uzgodnieniowej. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 1.1 (p 5.1) | jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych. | KL: Usługi świadczone przez dostawców usług cyfrowych różnią się zasadniczo, tak w definicjach (użytkownik, incydent, itp.), jak i w modelach biznesowych oraz wpływie świadczonych usług na infrastrukturę kluczową. Identyczne podejście do wszystkich podmiotów jest niekorzystne i nieadekwatne do poziomu świadczonych usług. KL sugeruje dokonanie wyodrębnienia poszczególnych subsektorów i stosowanie różnych miar i wymogów, tak aby były realnie dopasowane do specyfiki konkretnego obszaru | **Uwaga nieuwzględniona**  Kwestia dostawców usług cyfrowych jest uregulowana w ustawie o ksc. Z uwagi na fakt, że usługi cyfrowe nie są w myśl NIS usługami kluczowymi, są objęte obecnie innymi, słabszymi reżimami prawnymi. Kwestia doprecyzowania obowiązków dostawców usług cyfrowych może być rozpatrywana jedynie na forum europejskim. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 1.4 (p 5.4) | Analogicznym reżimem objęci zostaną dostawcy usług cyfrowych, jednak rząd ma pełną świadomość międzynarodowej specyfiki tych podmiotów oraz konieczności zapewnienia takich regulacji, które będą sprzyjały rozwojowi rynku cyfrowego w Polsce | KL: Równanie standardów w zakresie ciągłości działania dla wszystkich dostawców usług cyfrowych może być krzywdzące i nadmiarowe w przypadku dostawców, których działanie nie ma bezpośredniego wpływu na inne sektory (z naciskiem na infrastrukturę kluczową). Wymogi dotyczące chociażby dostawców internetowych czy też firm świadczących usługi z zakresu chmur obliczeniowych nie mogą być takie same jak dla internetowych platform handlowych. Wynika to z różnej specyfiki odbiorców usług, kaskadowości incydentu i jego eskalacji na inne sektory, norm czasowych i ilościowych. | **Uwag nieuwzględniona**  W tym fragmencie mówi się o „**minimalnych** wymaganiach w zakresie cyberbezpieczeństwa”. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 1.5 (p 5.5) | Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych. | KL: Przyjęcie jednej metodyki szacowania ryzyka stanowi bardzo duże ryzyko dla swobody organizacji pracy i planowania, a także nadzoru nad procesami w organizacjach. Na rynku istnieje kilka uznanych metodyk szacowania ryzyka, co więcej są one zależne od skali, rodzaju prowadzonej działalności, zasięgu firmy, itp. W praktyce dużo zależy od przyjętego know how firmy, posiadanych narzędzi (także licencyjnych) a wpływa to na prowadzenie pentestów, wdrażanie nowych projektów, a także zależy od tego czy zarządzanie ryzykiem odbywa się tylko w kontekście rynku lokalnego, czy stanowi np. filię międzynarodowej korporacji, która posiada własne standardy szacowania ryzyka. Przyjęcie jednej metodyki szacowania ryzyka nawet w kontekście jednego sektora (dostawca usług kluczowych) jest obarczone ogromnym ryzykiem, które może wpłynąć negatywnie na prowadzenie i rozwój działań biznesowych. | **Uwaga nieuwzględniona**  Metodyka musi być spójna aby oszacować ryzyko na poziomie krajowym. Konieczne jest zapewnienie porównywalności wyników, co będzie miało wpływ na opracowanie wspólnego krajowego planu zarzadzania ryzykiem. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 1.6 (p 5.6) | Zwiększenie efektywności czynności procesowych i operacyjnych wymaga podjęcia i poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. | KL: zachodzi ryzyko nadmiernego ujawniania danych klientów i przekazania ich danych podmiotom trzecim, nawet jeśli nie są przedmiotem ich zainteresowania | **Uwaga nieuwzględniona**  Dostęp do danych i tajemnic branżowych jest regulowany ustawowo. Strategia nie zmienia tego. Jednocześnie pragnę wskazać iż korzystanie z ekspertów i biegłych jest normalnych elementem działania organów ścigania. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 1.6 (p 5.6) | Wdrożone zostaną, skierowane do społeczeństwa, programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe. | KL: każdy z dostawców usług cyfrowych ma nieco inną specyfikę naruszeń incydentów, które mogą dotyczyć ich klientów. Dla internetowych platform handlowych jest to niezwykle ważne zagadnienie. Co do zasady zgadzamy się, że osoby (klienci) dotknięci przestępstwem powinni mieć zapewnioną odpowiednią obsługę, a także wsparcie. Jednocześnie KL zwraca uwagę na fakt, iż narzucanie sposobów postępowania może zaburzyć procesy biznesowe oraz być nierealne technicznie we wskazanej formie z uwagi na architekturę systemów informatycznych. | **Uwaga nieuwzględniona**  Zapisy nie wpłyną na procesy biznesowe firm. Postepowania będą prowadzone zgodnie z zasadami ustawowymi. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 2.1 (p 6.1) | opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:  1) aplikacji,  2) urządzeń mobilnych,  3) stacji roboczych,  4) serwerów i sieci,  5) modeli chmur obliczeniowych. | KL: Podobnie jak przy próbie wdrożenia wspólnej metodyki ryzyka, tutaj również pojawia się niebezpieczeństwo niepełnego uwzględniania specyfiki rynku, architektury systemów informatycznych, know how firmy, stosowanych systemów, narzędzi, urządzeń, czy też modeli licencyjnych. Zachodzi realne ryzyko, iż przyjęcie sztywnych standardów będzie prowadzić do utrudnienia w prowadzeniu działalności oraz świadczeniu usług. KL postuluje za wprowadzeniem wysoce ogólnych zaleceń, co doprowadziłoby do tego, iż poszczególne obszary podlegałyby ochronie, bez wskazywania konkretnych metodyk działania, sposobów wdrażania, testowania i audytowania rozwiązań dotyczących aplikacji, urządzeń mobilnych, stacji roboczych, serwerów, sieci czy chmur obliczeniowych. | **Uwaga nieuwzględniona**  NSC będą dobrowolne w stosowaniu. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 2.3 (p 6.3) | Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz specyfikę poszczególnych sektorów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów. | KL: Patrząc przez pryzmat form unifikacji standardów i rozwiązań teleinformatycznych oraz proceduralno-procesowych, próba ujednolicania podejścia do testowania bezpieczeństwa i ujednolicenia audytów pod kątem norm i praktyk sektorowych (wypracowanych zgodnie z sugestią wcześniej) docelowo może osłabić poziom bezpieczeństwa, ponieważ z czasem zachodzi ryzyko powtarzalności audytów. Samo prowadzenie audytów, ażeby ich wyniki były łatwo porównywalne, będzie wymagać każdorazowo podobnego zakresu obszary podjętego badaniu. Samo usztywnianie metodyki audytów wpłynie negatywnie na działalność firm zewnętrznych świadczących usługi audytorskie i pentesterskie, obniży konkurencyjność usług pod kątem zakresu oraz stylu prowadzonych działań, co więcej będzie dużym wyzwaniem dla firm spoza Polski. | **Uwaga nieuwzględniona**  Unifikacja nie będzie absolutna. Zdajemy sobie sprawę z różnic branżowych. Chodzi o porównywalność w danych grupach (usługi kluczowe w danym sektorze etc.). | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga o cel szczegółowy 2.3 (p 6.3) | W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty[[2]](#footnote-2).* | KL: specyfika programów bug bounty zachęca społeczeństwo do testowania zabezpieczeń firm. W skrajnych przypadkach ilość prowadzonych testów może wpłynąć negatywnie na ciągłość działania firmy, bezpieczeństwo jej zasobów, jest również dużym wyzwaniem organizacyjnym oraz budżetowym do podjęcia wprowadzenia „bug bounty”. Programy „bug bounty” są narzędziem podnoszącym poziom bezpieczeństwa, o ile firma je prowadząca jest gotowa zapewnić ogrom środków koniecznych do ich utrzymania. Pod żadnym pozorem nie można obligować do wdrażania bug bounty. Jest to obecnie określone jako propagowanie, jednakże ta definicja sugeruje pewnego rodzaju upowszechnianie i zalecanie wdrażania tego typu programów. KL sugeruje zneutralizowanie tego sformułowania. | **Uwaga nieuwzględniona**  Nie będzie obligatoryjnych programów bug bounty. Jest to nierealne i niepożądane. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga ogólna |  | KL sugeruje, aby przed przyjęciem strategii przygotowane i przekazane do konsultacji zostały szczegółowego zapisy lub chociaż założenia planowanych do nowelizacji aktów prawnych. Jedynie taki sposób procedowania umożliwi nam rzeczowe odniesienie się do istotnych dla nas zagadnień wpływających bezpośrednio na działalność podmiotów gospodarczych | **Uwaga nieuwzględniona**  Akty prawne będą procedowane zgodnie z procesem legislacyjnym. | **Przyjęte wyjaśnienie.** |
|  | Konfederacja Lewiatan | Uwaga ogólna |  | KL: analizując tekst przedstawionego do konsultacji projektu strategii, w komparycji również do innych przyjętych już przez Rade Ministrów dokumentów rządowych, w tym strategii i programów rozwoju, KL zauważa, iż uszczegółowienia i doprecyzowania wymagają obszary takie jak:   * Diagnoza stanu obecnego, która powinna jasno określać punkt wyjścia, słabe i mocne strony, szanse i zagrożenia i jako taka stanowić punkt wyjścia dla propozycji konkretnych działań * Konkretne i mierzalne cele strategii, dookreślone w zakresie terminu i podmiotu odpowiedzialnego za ich realizację * Plan finansowy, który chociaż w zarysie powinien określać koszty realizacji celów, zakresów obciążeń, jakie zostaną nałożone na sektor przedsiębiorstw w wyniku realizacji strategii i przyjęcia planowanych w niej aktów prawnych, a także jasno sprecyzowane źródła finansowania | **Uwaga nieuwzględniona**  Szczegółowe działania wraz z harmonogramem ich realizacji, źródłami finansowania oraz miernikami realizacji, będą wskazane w Palnie działań. | **Przyjęte wyjaśnienie.** |
|  | SEQRED | Uwaga ogólna |  | SEQRED: Podmioty podlegające KSC powinny posiadać procesy oraz narzędzia (klasy Threat Intelligence) umożliwiające ciągłe pozyskiwanie informacji z zewnętrznych źródeł o zagrożeniach dla organizacji | **Uwaga nieuwzględniona**  Tworzone systemy: S46 oraz NPC dają możliwość do bieżącej wymiany informacji. |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.2 (p 5.2) | Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego | SEQURED: Sugerujemy doprecyzowanie w jakiej formie/jakimi mechanizmami będą realizowane rekomendacje oraz działania Rządu | **Uwaga nieuwzględniona**  Szczegółowe działania wraz z harmonogramem ich realizacji, źródłami finansowania oraz miernikami realizacji, będą wskazane w Palnie działań. |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.2 (p 5.2) | w tym wprowadzenie minimalnych wymagań bezpieczeństwa dla sieci i systemów teleinformatycznych używanych przez administrację publiczną. Standaryzacja i wymagania cyberbezpieczeństwa, opracowane | SEQURED: Od standaryzacji bezpieczeństwa bardziej właściwym rozwiązaniem jest rekomendowanie dobrych praktyk oraz podejścia normatywnego. W przypadku wykrycia podatności w ustandaryzowanym mechanizmie zabezpieczeń podatność ta będzie dotyczyła całego kraju. | **Uwaga nieuwzględniona**  Mowa jest o **minimalnych wymaganiach.** |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.2 (p 5.2) | Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych, inicjowanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni. | SEQURED: Należy rozważyć wprowadzenie obowiązku okresowego przeprowadzania testów/analiz typu Red Teamining w szczególności przez podmioty objęte Ustawą o Krajowym Systemie Cyberbezpieczeństwa, służące wypracowywaniu możliwych scenariuszy ataków na infrastrukturę, walidację stosowanych zabezpieczeń (potwierdzenie odporności) a w następstwie ew. wdrożenie adekwatnych zabezpieczeń. | **Uwaga nieuwzględniona**  Przepisy ustawy o KSC umożliwiają zespołom CSIRT przeprowadzanie badań systemów lub urządzeń, a także w uzasadnionych przypadkach wydawanie rekomendacji. |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.4 (p 5.4) | Technologie informatyczne (IT)[[3]](#footnote-3) wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT)[[4]](#footnote-4). | SEQURED: Podmioty podlegające Ustawie o Krajowym Systemie Cyberbezpieczeńśtwa powinny przed zakupem (lub zmianą) sprzętu/technologii/oprogramowania przeprowadzać analizę podatności rozwiązania w oparciu o Cybersecurity Bill of Materials  Zwracamy uwagę, że podmioty te wdrażając lub dostarczając usługi korzystają z zakupionych rozwiązań/technologii od swoich partnerów. Należy dążyć do tego aby rozwiązania te przed ich zakupem podlegały każdorazowo analizie składników (Cybersecurity Bill of Materials) wykorzystywanych do budowy tego rozwiązania:  - biblioteki firm trzecich  - flagi kompilacji  - predefiniowane konta użytkowników  - klucze kryptograficzne  Należy zwrócić uwagę, że obecnie nie istnieją na rynku mechanizmy pozwalające wymusić na producencie rozwiązania/dostawcy technologii stosowania dobrych praktyk (predefiniowane konta i hasła użytkowników znalazły się w rozwiązaniach wiodących producentów urządzeń automatyki przemysłowej). | **Uwaga nieuwzględniona**  PL jest członkiem UE, a tym samym obowiązuje nas prawo europejskie.  Przyjęty Akt o Cyberbezpieczeństwie zakłada opracowanie wspólnych europejskich programów certyfikacji cyberbezpieczeństwa. |  |
|  | SEQRED | Uwaga o cel szczegółowy 2.1 (p 6.1) | zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:  1) aplikacji,  2) urządzeń mobilnych,  3) stacji roboczych,  4) serwerów i sieci,  5) modeli chmur obliczeniowych.  **6) oprogramowanie wbudowane dla urządzeń automatyki oraz IoT** | SEQURED: sugeruje dodanie do listy  **6) oprogramowanie wbudowane dla urządzeń automatyki oraz IoT** | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.2 (p 5.2) | W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej, która już w bliskiej przyszłości rozpocznie korzystanie z nowych form przetwarzania i przechowywania informacji m.in. poprzez wykorzystywanie usług chmury obliczeniowej, niezbędne będzie przygotowanie zaleceń i promowanie dobrych praktyk podnoszących odporność na potencjalne cyberzagrożenia. | SEQURED: Należy rozważyć wprowadzenie okresowego przeprowadzania testów/analiz typu Red Teamining, służące wypracowywaniu możliwych scenariuszy ataków na infrastrukturę, walidację stosowanych zabezpieczeń (lub potwierdzenie odporności) a w następstwie ew. wdrożenie adekwatnych zabezpieczeń. | **Wyjaśnienie**  Strategia nie wyklucza tego typu rozwiązań. |  |
|  | SEQRED | Uwaga o cel szczegółowy 2.2 (p 6.2) | Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług). | SEQURED: Zwracamy uwagę, że sama ocena i certyfikacja może być niewystarczająca. Certyfikacji będzie podlegała konkretna wersja oprogramowania wbudowanego (firmware). Należy zwrócić uwagę, że istnieją przykłady dystrybucji złośliwie zmienionej wersji firmware przy zachowaniu identyfikacji istniejącej poprawnej wersji. Wobec tego ocena powinna być prowadzona w kontekście każdej zmiany. | **Uwaga nieuwzględniona**  Istnieją modele certyfikacji uwzględniające częste aktualizacje. |  |
|  | SEQRED | Uwaga o cel szczegółowy 1.2 (p 5.2) | W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty[[5]](#footnote-5)* | SEQURED: Sugerujemy weryfikację zastosowanego pojęcia bug-bounty - cechą charakterystyczną programów bug-bounty jest zapewnienie wynagrodzenia lub uznania za znalezioną podatność. | **Uwaga nieuwzględniona**  Kwestie używania tzw. bug bounty oraz testów penetracyjnych zostały określone w art. 269b i c Kodeksu karnego. |  |
|  | SEQRED | Uwaga o cel szczegółowy 3.3 (p 7.3) | Ponadto we współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze | SEQURED: Sugerujemy rozszerzenie o współpracę z polskimi firmami, które podsiadają odpowiedni potencjał w zakresie oceny i analizy zabezpieczeń (potwierdzone zgłoszeniami podatności do producentów rozwiązań). | **Uwaga częściowo uwzględniona**  Potrzeba bliskiej współpracy z sektorem prywatnym jest opisana w celu 3.2 |  |
|  | SEQRED | Uwaga o cel szczegółowy 4.2 (p 8.2) | Edukacja w zakresie cyberbezpieczeństwa powinna być dostępna na jak najwcześniejszym etapie dostępu dzieci i młodzieży do usług cyfrowych – najlepiej jeśli byłaby prowadzona przed wejściem świat cyfrowy, a w praktyce często wymagana jest na etapie kształcenia wczesnoszkolnego. Uwzględniając tematykę bezpiecznego korzystania z cyberprzestrzeni zakłada się ciągłe doskonalenie podstaw programowych nauczania w ramach różnych kierunków kształcenia. Konieczne jest wprowadzenie systemowych działań doszkalających dla nauczycieli. | SEQURED: Proponujemy ogłaszanie konkursów i realizację zadań w zakresie programów podnoszenia świadomości cyfrowej przez organizacje pozarządowe.  Zwracamy również uwagę, że te działania mogłyby być prowadzone również dla rodziców/opiekunów dzieci uczęszczających do danej szkoły. | **Wyjaśnienie**  Taka forma realizacji tego punktu nie jest wykluczona. |  |
|  | KIKE | Uwaga ogólna |  | KIKE: Zdaniem Izby brakuje dokładnego i konsekwentnego wskazania we wstępie Strategii rodzajów podmiotów, do których jest ona adresowana i dla których porządkuje lub wyznacza nowe zadania i obowiązki. Na samym początku Strategii wskazuje się, że jest kierowana do rządowej i samorządowej administracji państwowej oraz do operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych. W dalszych jej częściach mowa jest z kolei także o dostawcach dostępu do sieci Internet czy też o wszystkich operatorach sieci telekomunikacyjnej. Z uwagi na to, że Strategia zakłada nałożenie na szereg podmiotów obowiązków związanych z cyberbezpieczeństwem, konieczne jest precyzyjne określenie podmiotów, których dotyczą zadania i obowiązki w niej określone. | **Uwaga nieuwzględniona**  Strategia określa kierunki interwencji oraz cele strategiczne rządu RP. W Strategii nie mogą być określone obowiązki dla podmiotów innych niż adm. rządowa. Tylko w drodze aktów prawa powszechnego mogą zostać określone obowiązki dla innych podmiotów.  Natomiast konkretne działania wraz ze wskazaniem podmiotów oraz harmonogramem ich realizacji będą określone w Planie działań. | **KIKE zadeklarowało chęć udziału w ewentualnych konsultacjach do Planu działań.** |
|  | KIKE | Uwaga ogólna |  | KIKE: Potrzebne jest określenie wprost czy w Strategii przewiduje się nowe zadania dla przedsiębiorców telekomunikacyjnych (w tym dostawców dostępu do sieci Internet ISP). W tym względzie KIKE pragnie zaznaczyć, że obecne regulacje w polskim prawie telekomunikacyjnym były wprowadzone niedawno i są wystarczające. | **Uwaga nieuwzględniona**  Praw i obowiązki operatorów są określone w przepisach prawa m.in. w Prawie telekomunikacyjnym. | **Przyjęte wyjaśnienie.** |
|  | KIKE | Uwaga ogólna |  | KIKE: W Strategii położono kilkukrotnie nacisk na kluczową rolę telefonii mobilnej 5G. Już to tylko wskazuje, że Strategia jednak przewiduje (przynajmniej pośrednio) jakąś rolę dla operatorów telekomunikacyjnych choć tylko mobilnych. W opinii Izby, jeżeli założeniem Strategii jest tworzenie w Polsce cyberprzestrzeni wyłącznie w oparciu o telefonię mobilną, to jest to założenie błędne. Pominięcie w dokumencie sieci stacjonarnej, zwłaszcza kablowej najnowszej generacji (światłowodowej) jest sprzeczne z dotychczasowymi strategiami i działaniami Rządu RP. Zarówno sektor rządowy jak i prywatny w ostatnich latach dokonał ogromnych inwestycji w sieci światłowodowe i wykluczenie tej infrastruktury z planów dot. cyberprzestrzeni jest nieracjonalne. | **Uwaga częściowo uwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | Zmiana w zapisie: „…szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa **w zakresie mobilnej telekomunikacji”.** |
|  | KIKE | Uwaga ogólna |  | KIKE: Jest możliwe, że po analizie stanu budowy sieci 5G, Rząd w celu wykonania Strategii rozpocznie program dofinansowania budowy tych sieci telekomunikacyjnych co znacząco naruszy zarówno konkurencję na rynku telekomunikacyjnym, jak również zburzy plany inwestycyjne sektora prywatnego (zwłaszcza korzystającego z unijnego wsparcia budowy sieci światłowodowych w obszarach słabo rozwiniętych). | **Uwaga nieuwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | **Przyjęte wyjaśnienie.** |
|  | KIKE | Uwaga ogólna |  | KIKE: Zgodnie z programem rządowym ośrodki naukowe oraz szkolnictwa są właśnie wyposażane w nowoczesne sieci światłowodowe (OSE) i wyposażanie ich zgodnie z zapowiedziami Strategii w sieci 5G oznaczałoby marnotrawstwo tych środków. | **Uwaga nieuwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | **Przyjęte wyjaśnienie.** |
|  | KIKE | Uwaga ogólna |  | KIKE: Strategia w kilku miejscach wyraźnie wskazuje, że jednym z jej celów jest zapewnienie wolności w sieci Internet oraz otwartość Internetu. Jednocześnie w dokumencie zapowiadana jest walka z dezinformacją, w tym z fake newsami. Zdaniem Izby, oba te cele sprawiają wrażanie wzajemnie się wykluczających. Zrozumienie tych celów Strategii uniemożliwia to, że oprócz ogólnych haseł na ten temat, nie wskazuje się jakie działania są planowane. Czy Rząd przewiduje walkę z cenzurą w Internecie czy też odwrotnie cenzurowanie Internetu w zakresie fake newsów. Zdaniem Izby temat ten powinien zostać bardziej uszczegółowiony co do kierunków jakie Rząd zamierza obrać oraz jakie podmioty mają się zająć tymi działaniami. | **Wyjaśnienie**  Walka z fake newsami i dezinformacją jest konieczna.  Natomiast wszelkie konkretne działania będą wskazane w *Planie działań na rzecz wdrożenia Strategii.* | **Przyjęte wyjaśnienie.** |
|  | KIKE | Uwaga ogólna |  | KIKE: Biorąc pod uwagę wcześniejsze plany Rządu, kiedy to przymierzano się do nałożenia na operatorów obowiązki monitorowania i blokowania określonych treści w Internecie, według Izby jest wręcz niezbędne uszczegółowienie w Strategii szczegółowych zadań oraz podmiotów zobowiązanych do realizacji tych zadań. | **Uwaga nieuwzględniona**  Strategia jest dokumentem ramowym.  Wszelkie konkretne działania będą wskazane w *Planie działań na rzecz wdrożenia Strategii.* |  |
|  | KIKE | Uwaga ogólna |  | KIKE: Jednym z kluczowych elementów Strategii są szkolenia w zakresie cyberbezpieczeństwa wśród niższego i średniego szczebla urzędników państwowych oraz wśród sektora prywatnego. Tymczasem jest to założenie niewystarczające. Doświadczenie wskazuje, że w pierwszej kolejności szkolenia lub warsztaty w zakresie cyberbezpieczeństwa powinni przechodzić wyżsi rangą urzędnicy szczebla centralnego i samorządowego. Podniesienie świadomości i kompetencji dot. cyberbezpieczeństwa wśród kadry kierowniczej jest najlepszą gwarancją, że kwestia ta zostanie właściwie zaadresowana, a nie zostanie zmarginalizowana lub w ogóle zarzucona. Z tego względu, Izba sugeruje uzupełnienie Strategii o warsztaty i szkolenia z cyberbezpieczeństwa dla wyższej rangi urzędników państwowych i to w dodatku w pierwszej kolejności. | **Uwaga nieuwzględniona**  Kwestia ta jest opisana w strategii: cel szczegółowy 4. | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Strategia nie wskazuje w wyraźny sposób podmiotów, do których jest kierowana. Z jednej strony we wstępie Strategii wskazuje się, że jest adresowana tylko do administracji państwowej (rządowej i samorządowej), a także operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych. W dalszych częściach dokumentu mowa jest z kolei także o dostawcach dostępu do sieci Internet czy też o wszystkich operatorach sieci telekomunikacyjnej. Z uwagi na to, że Strategia zakłada nałożenie na szereg podmiotów obowiązków związanych z cyberbezpieczeństwem, konieczne jest precyzyjne określenie podmiotów, których ona dotyczy w zakresie nakładania na nich obowiązków. | **Uwaga nieuwzględniona**  Strategia określa kierunki interwencji oraz cele strategiczne rządu RP. W Strategii nie mogą być określone obowiązki dla podmiotów innych niż adm. rządowa. Tylko w drodze aktów prawa powszechnego mogą zostać określone obowiązki dla innych podmiotów.  Natomiast konkretne działania wraz ze wskazaniem podmiotów oraz harmonogramem ich realizacji będą określone w Planie działań. | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Strategia kładzie silny nacisk na wykorzystanie dla cyberbezpieczeństwa przyszłej sieci mobilnej 5G. Już te twierdzenia wskazują, że Strategia ma jakieś zadania dla operatorów telekomunikacyjnych, których jednak w żaden sposób nie precyzuje. Należy jednak przede wszystkim zwrócić uwagę, że całkowicie pominięta zostaje za to sieć stacjonarna (kablowa), w tym najnowocześniejsza jej wersja oparta na łączach światłowodowych czy na systemie DOCSIS 3.0. Jest to niezrozumiałe działanie Ministerstwa Cyfryzacji, gdyż jest sprzeczne z innymi strategiami rządowymi kładącymi znaczny nacisk na rozwój i wykorzystanie sieci światłowodowej. | **Uwaga nieuwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Obawy Izby związane są także z tym, że w celu wykonania Strategii, Rząd rozpocznie ogromne dofinansowanie budowy sieci 5G naruszając konkurencję na rynku oraz zakłócając proces unijnego wsparcia budowy sieci światłowodowych w obszarach słabo rozwiniętych. Wybudowanie sieci 5G ze wsparciem publicznym w obszarach, w których dopiero co wybudowano sieci światłowodowe ze środków unijnych, spowodowałoby ogromne straty finansowe. | **Uwaga nieuwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Warto zwrócić uwagę, że sama Strategia przewiduje wykorzystanie w cyberbezpieczeństwie ośrodków naukowych oraz szkolnictwa oczywiście przy udziale sieci 5G. Tymczasem zgodnie z programem rządowym (Ogólnopolska Sieć Edukacyjna) ośrodki te są właśnie wyposażane z nowoczesne sieci światłowodowe i wyposażanie ich teraz zgodnie zapowiedziami Strategii w sieci 5G oznaczałoby marnotrawstwo już wykorzystanych środków finansowych. | **Uwaga nieuwzględniona**  Sieci mobilne i bezprzewodowe powstają w oparciu o uzupełnienie dla sieci łączności przewodowej .  Sieci bezprzewodowe adresuje wymagania w zakresie mobilności i celem systemów bezprzewodowych jest opracowanie scenariuszy wspierających użytkowników. | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Strategia w kilku miejscach wskazuje, że jednym z jej celów jest zapewnienie wolności w sieci Internet oraz jej otwartość. Dodatkowo zapowiadana jest walka z dezinformacją, w tym z fake newsami. Niestety oprócz tych generalnych haseł Strategia nie wskazuje jakie działania w tym zakresie będą podejmowane (walka z cenzurą w Internecie czy też odwrotnie cenzurowanie Internetu). Co więcej, nie jest wskazane jakie podmioty mają się zająć tymi działaniami. | **Wyjaśnienie**  Walka z fake newsami i dezinformacją jest konieczna.  Natomiast wszelkie konkretne działania będą wskazane w *Planie działań na rzecz wdrożenia Strategii.* | **Przyjęte wyjaśnienie.** |
|  | PIKE | Uwaga ogólna |  | PIKE: Biorąc pod uwagę wcześniejsze działania Rządu, kiedy to projektowano nałożenie na operatorów obowiązków monitorowania i blokowania określonych treści w Internecie, według Izby jest niezbędne uszczegółowienie w Strategii szczegółowych zadań oraz podmiotów zobowiązanych do realizacji tych zadań. | **Uwaga nieuwzględniona**  Wszelkie konkretne działania będą wskazane w *Planie działań na rzecz wdrożenia Strategii.* | **Przyjęte wyjaśnienie.** |
|  | ZBP | Uwaga o cel szczegółowy 1.2 (p 5.2) | Niezbędne jest wdrożenie systemowych rozwiązań pozwalających na wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do zagrożeń i incydentów. | ZBP: Z treści dokumentu nie wynika jednak, czy rozwiązania te będą dotyczyły również międzysektorowej wymiany informacji. W ocenie Związku, w celu skutecznej obsługi incydentów, konieczne jest wprowadzenie możliwości bezpośredniej, horyzontalnej wymiany informacji pomiędzy operatorami usług kluczowych oraz dostawcami usług cyfrowych różnych sektorów. Aktualnie taka wymiana informacji napotyka na szereg barier prawnych. | **Uwaga częściowo uwzględniona**  Stąd też konkretne działania: tworzenie systemu S46 oraz NPC. | **Przyjęte wyjaśnienie.** |
|  | ZBP | Uwaga o cel szczegółowy 3.1 (p 7.1) | Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych. | ZBP: odpowiednie szkolenia powinny być wdrażane już na wcześniejszych etapach edukacji, co najmniej od szkoły średniej (na barkach tego typu szkolnictwa opiera się w szczególności niższy szczebel administracji systemami IT). W ocenie Związku, rozważenia wymaga również uruchomienie programów promujących tematykę cyberbezpieczeństwa także w szkołach podstawowych. Jest to pokolenie, które będzie wchodziło dopiero na rynek pracy i podejmowało decyzje o dalszej karierze. | **Uwaga nieuwzględniona**  Jest to opisane w celu szczegółowym 4. | **Przyjęte wyjaśnienie.** |
|  | ZBP | Uwaga o cel szczegółowy 2.3 (p 6.3) | W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty[[6]](#footnote-6).* | ZBP: wskazać natomiast należy, że aby zrealizować ten cel, poza zmianami dokonanymi w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, konieczne jest dokonanie analizy innych obowiązujących przepisów i na tej podstawie wprowadzenie regulacji dających możliwość realnego prowadzenia testów tego typu, w szczególności w obszarze infrastruktury państwowej. Ponadto kwestia ta rodzi szereg pytań dotyczących w szczególności tego, czy elementy infrastruktury krytycznej również będą testowane w modelu bug-bounty, a także jaki będzie dobór podmiotów mogących dokonywać tego rodzaju testów. | **Uwaga częściowo uwzględniona**  Propozycje konkretnych działań – w tym także na poziomie legislacyjnym – zostaną określone w Planie działań. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Strategia nie operuje wysokością środków finansowych oraz ilościowymi miernikami stawianych celów. Istnieje zatem ryzyko, że dokument w niewielkim stopniu może wpłynąć na poprawę poziomu bezpieczeństwa cybernetycznego. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. | **PIIT zadeklarował chęć udziału w ewentualnych konsultacjach do Planu działań.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Sugerujemy zwięzłe, obiektywne omówienie aktualnego stanu systemu cyberbezpieczeństwa oraz warunków funkcjonowania cyberprzestrzeni, wskazanie słabości i deficytów, których niwelowanie będzie jednym z celów działań w najbliższych latach, a także mocnych stron i atutów, jakie cechują obecną sytuację, których wzmocnienie i rozbudowa w przyszłości pozwoli realizować cele strategii. Dopiero dysponując taką bazą wyjściową, w postaci swoistej "fotografii" aktualnego stanu, pozwoli to w zrozumiały sposób opisać zamierzenia, jakie państwo polskie stawia przed sobą oraz wskazać środki, metody, formy ich osiągania, przewidziane przez rząd. | **Uwaga nieuwzględniona**  Niniejszy dokument nie ma charakteru analitycznego. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: W naszej ocenie należy przeprowadzić i przedstawić analizę pod kątem m.in.:   * efektów dotychczasowych strategii i planów w zakresie cyberbezpieczeństwa; * efektów dotychczasowych działań legislacyjnych, w szczególności z uwzględnieniem poruszanych w projekcie ustaw o krajowym systemie cyberbezpieczeństwa oraz zarządzaniu kryzysowym; * kluczowych interesariuszy obszaru cyberbezpieczeństwa, w tym użytkowników indywidualnych i instytucjonalnych, administracji publicznej, w tym samorządowej (np. raport NIK w tej sprawie), producentów oprogramowania i urządzeń wykorzystywanych  w ekosystemie teleinformatycznym, w którym mogą wystąpić zagrożenia cyberbezpieczeństwa, dostawców usług świadczonych za pośrednictwem sieci internet, dostawców usług szerokopasmowych, cyberprzestępców, służb, policji, prokuratury,  oraz sądów. | **Uwaga nieuwzględniona**  Niniejszy dokument nie ma charakteru analitycznego. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Istotną przesłanką, wymagającą uwzględnienia w strategii, jest pojawienie się nowego podejścia do kształtowania polityki zagranicznej państw dysponujących zaawansowaną technologią informatyczną. Kontrola dostępu do kluczowych elementów technologii może być wykorzystywana do kształtowania relacji międzypaństwowych (Chiny – technologia 5G, USA – systemy operacyjne), a przez to kształtowania bezpieczeństwa gospodarczego innych krajów, znacznie wykraczającego poza cyberprzestrzeń. Element prowadzenia polityki zagranicznej przy pomocy reglamentowania dostępu do kluczowych technologii informatycznych może w określonym zakresie wpływać na krajową politykę prowadzenia prac badawczo-rozwojowych. Podstawą do opracowania tematyki badań powinien być przeprowadzony audyt technologii wykorzystywanych przez instytucje państwowe. Audyt powinien wskazać jakie technologie mają zastosowanie w poszczególnych obszarach (obronność, energetyka, finanse, służba zdrowia itp.) oraz jakie jest ryzyko związane z wystąpieniem ograniczenia dostępu do technologii z powodu występującej w danym roku sytuacji geopolitycznej. Audyt taki powinien być prowadzony raz do roku. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: W wyniku przeprowadzonego audytu powinny być typowane rozwiązania technologiczne, których pozyskanie w toku prac badawczo-rozwojowych jest istotne z punktu istotnego interesu bezpieczeństwa państwa, pomimo tego, że pozyskane rozwiązanie nie jest rozwiązaniem innowacyjnym na skalę światową i jest w zasięgu możliwości naszego kraju. Elementem ważniejszym od samej innowacyjności powinno być zapewnienie możliwie jak najwyższej i uzasadnionej ekonomicznie suwerenności cyfrowej. | **Uwaga nieuwzględniona**  Strategia zakłada przeprowadzanie audytów oraz wyraźnie wskazuje na ich istotne znaczenie. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: projekt Strategii nie ustala żadnych zobowiązań i mierników pozwalających ocenić sukces jej wdrożenia. Zarazem projekt Strategii nie zawiera żadnych wyraźnie wskazanych środków finansowych do wydatkowania przez państwo na cyberbezpieczeństwo. Strategia powinna stawiać sobie pewne cele, które mierzalnie można ocenić | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: w projekcie strategii nie zostały określone koszty jej wdrożenia oraz źródła pokrycia tych kosztów. Z jednej strony dokument strategiczny o charakterze wdrożeniowym powinien przewidywać zakres obciążenia budżetu państwa wobec działań koniecznych do wykonywania po stronie organów administracji publicznej. Z drugiej natomiast strony, mając niewątpliwy wpływ na gospodarkę i przedsiębiorców powinien przynajmniej szacować te koszty i oceniać wpływ na dotychczasowe prowadzenie działalności gospodarczej. Taka ocena powinna zostać dokonana przynajmniej szacunkowo lub kierunkowo | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc.  Ponadto kwestie finansowania mogą być elementem dyskusji w związku z nowelizacja ustawy o ksc. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: postulujemy rozważenie możliwości stworzenia odpowiedniego funduszu albo innej formuły, w ramach której mogłyby być finansowane i wspierane wdrożenia rozwiązań cyberbezpieczeństwa w przedsiębiorstwach i samorządach. | **Uwaga nieuwzględniona**  Uzasadnienie jw. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Powyżej sygnalizowane zagadnienia uzasadniają w naszej ocenie przyjęcie modelu realizacji strategii, w którym szczegółowe rozwiązania będą opracowywane we współpracy z podmiotami, których mają dotyczyć. W tym celu utrzymana może być dotychczas stosowana dla niektórych zagadnień formuła grup roboczych lub wprowadzenie modelu uszczegółowionych konsultacji z otwartą grupą potencjalnie zainteresowanych nowymi regulacjami podmiotów. | **Uwaga nieuwzględniona**  Strategia jest dokumentem rządowym i obowiązki z niej wynikające wiążą członków Rady Ministrów. Nie zawiera ona obowiązków dla innych podmiotów. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: zaznaczamy, odnosimy wrażenie, że w istotnym stopniu miałoby dochodzić do zacierania granic i zakresu obowiązków pomiędzy operatorami usług kluczowych, infrastruktury krytycznej i usług cyfrowych. Kwestia ta wymaga istotnego wyjaśnienia i doprecyzowania, szczególnie, że aktualnie są to różne zakresy opisane w różniących się niekiedy w sposób istotny reżimach prawnych. | **Uwaga nieuwzględniona**  Ich obowiązki są zawarte i rozróżnione m.in. w ustawie o KSC | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: W naszej ocenie, adresatem nowych obowiązków i wymagań w zakresie bezpieczeństwa powinni być także dostawcy ww. sprzętu i oprogramowania. W tym kontekście, uwzględniając komunikowane już założenia wyrażone w stanowisku Polski przekazanym do Komisji Europejskiej w zakresie bezpieczeństwa sieci 5G, jednym z takich wymagań w kontekście potencjalnie wymaganej dywersyfikacji sprzętu uzasadniony byłby obowiązek zapewnienia wzajemnej kompatybilności  i interoperacyjności. | **Uwaga nieuwzględniona**  Reguluje to rozporządznie UE 2019/881 (Cyber Security Act). | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Zasadnicza wadą projektu Strategii jest także to, że w nikłym stopniu odnosi się on do kluczowych zjawisk związanych z rozwojem nowoczesnych technologii i dynamicznie rozwijającym się rynkiem informatycznym w najbliższych latach takich jak:   * Rozwój Internetu Rzeczy (IOT); * Sztuczna Inteligencji (uczenie maszynowe) (AI); * Mobilne sieci szerokopasmowe 5 generacji (5G); * Przemysł 4.0 * Chmura obliczeniowej; * Megadane (Big Data); * Telewizja i radio cyfrowe; * Dystrybucja treści multimedialnych w Internecie,   czy przechodzeniem w sieci Internet z protokołu IPv4 na IPv6. (Kwestie te poruszono śladowo  w kontekście potrzeby rozwoju badan naukowych w pkt. 7.2 Strategii).  W naszym przekonaniu, przynajmniej kilka z nich, wymaga szerszego omówienia ze względu na zagrożenia dla cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Wszystkie te elementy znajdują swoje miejsce w strategii.  . | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o Kontekst Strategiczny | Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni, a także zwiększyć poziom ochrony informacji w systemach informacyjnych poprzez standaryzację zabezpieczeń. Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań  o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. | PIIT: Czy celem nie powinien być także nie zakłócany poważnymi incydentami, rozwój Polski, w tym gospodarki i społeczeństwa, także w tych dziedzinach, które dziś nie są objęte bezpośrednio regulacjami wynikającymi z UKSC np. media, nauka i badania, kultura narodowa, rozwój MŚP etc.  Co zresztą autorzy podkreślają w innej części tzn. w WIZJI (pkt 4 Strategii). | **Uwaga nieuwzględniona**  Część z tych obszarów jest już regulowana m.in. w ustawie o KSC lub ustawach szczegółowych. Nie wydaje się zasadnym pisać o wszystkim. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.1 (p 5.1) | Zmiany przepisów regulujących funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa będą również wynikały z praktyki funkcjonowania na szczeblu europejskim Dyrektywy Parlamentu Europejskiego i Rady […] Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej  w sprawie zmiany przepisów samej Dyrektywy NIS, tak aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych. | PIIT: Zapowiadana jest zmiana regulacji prawnych w skali UE dot. chmury i dot. operatorów usług cyfrowych, ale bez wskazania kierunków tych zmian. Mowa jest jedynie o konieczności doprecyzowania obowiązków. Czy możemy wskazać najważniejsze przyczyny takiej potrzeby? Należy pamiętać także że rozwiązania chmurowe są istotna częścią technologii 5G  i niezbędnym elementem rozwoju przemysłu 4.0. | **Uwaga nieuwzględniona**  Opisane zmiany wynikają z praktyki funkcjonowania europejskiego systemu cyberbezpieczeństwa. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.2 (p 5.2) | Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie realizowane poprzez uruchomienie w roku 2021 przez ministra właściwego do spraw informatyzacji systemu teleinformatycznego wspierającego:  1) współpracę podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa,  2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,  3) zgłaszanie i obsługę incydentów,  4) szacowanie ryzyka na poziomie krajowym,  5) ostrzeganie o zagrożeniach cyberbezpieczeństwa. | PIIT: Wydaje się ze za generowanie rekomendacji (pkt.2) powinien odpowiadać określony podmiot a nie System Teleinformatyczny, choć można i należy zakładać, że część z nich będzie generowana automatycznie wg określonych algorytmów. | **Uwaga nieuwzględniona**  S46 ma działać na podstawie zasilających go danych i odpowiedniego silnika analitycznego. W tym zakresie będzie w stanie generować niektóre rekomendacje (np., dotyczące patchy). Nie zwalnia to Ministra Cyfryzacji, jako odpowiedzialnego za ten system, z realizacji tych obowiązków. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.2 (p 5.2) | Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych, inicjowanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni. | PIIT: Czy musimy pisać w Polskiej Strategii, że będziemy ćwiczyli w ramach sił zbrojnych wyłącznie operacje defensywne? Wydaje się ze nie powinniśmy wykluczać możliwości ćwiczenia operacji ofensywnych w przypadku odpowiedzi na agresję, a przynajmniej potencjalny agresor nie powinien czuć się bezkarny i sądzić, że jesteśmy przygotowywani, jako państwo, tylko do działań defensywnych. | **Uwaga nieuwzględniona**  Ten zapis jest elementem uzgodnień z MON i pozostaje do ich decyzji. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.4 (p 5.4) | Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. | PIIT: Z pkt. 5.4 Strategii wynika ze rząd posiada już analizy dot. operatorów telekomunikacyjnych w budowie sieci 5G – chętnie byśmy się z nimi zapoznali jako środowisko firm zainteresowanych budową sieci 5G i operatorów telekomunikacyjnych, zwłaszcza że analizy te mają być podstawą do tworzenia zmian prawnych, jak wskazuje Strategia. | **Uwaga nieuwzględniona**  Analizy krajowe są częścią analiz europejskich i zostaną razem z nimi upublicznione. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.4 (p 5.4) |  | PIIT: zwraca w szczególności uwagę na potrzebę stosowania otwartych standardów w budowie sieci 5G jako niezbędnego elementu zapewnienia cyberbezpieczeństwa w sieciach 5G. | **Uwaga częściowo uwzględniona**  Rozpoczęły się prace nad stworzenie wspólnego europejskiego podejścia do technologii 5G – jednym z elementów były własnej krajowe oceny ryzyka. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.4 (p 5.4) | grupy Współpracy Dyrektywy NIS, a także w ramach współpracy transatlantyckiej z brytyjskimi  i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych | PIIT: Mamy nadzieje, że kontakty te będą prowadzić także do wzajemnego uznawania standardów  i certyfikatów. | **Wyjaśnienie**  Zależy od treści porozumień o współpracy. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.4 (p 5.4) | grupy Współpracy Dyrektywy NIS, a także w ramach współpracy **transatlantyckiej z brytyjskimi i amerykańskimi instytucjami** stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych | PIIT: Grupy Współpracy Dyrektywy NIS, a także w ramach współpracy **z międzynarodowymi instytucjami** stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych. | **Uwaga nieuwzględniona**  Strategia ma na celu skupienie się na wskazanych podmiotach. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.5 (p 5.5) | Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 roku. | PIIT: Metody szacowania ryzyka – czy powinna być jedna – wzorcowa metoda stosowana w całym sektorze publicznym? Dlaczego nie wykorzystać w tym celu jednej zeznanych i sprawdzonych wcześniej metodyk? | **Uwaga nieuwzględniona**  Metodyka musi być spójna aby oszacować ryzyko na poziomie krajowym. Konieczne jest zapewnienie porównywalności wyników, co będzie miało wpływ na opracowanie wspólnego krajowego planu zarzadzania ryzykiem. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.6 (p 5.6) | Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. | PIIT: znaczne efekty można także osiągnąć przez współpracę z NGO’s policji i prokuratury np. współpracy Stowarzyszenia Sygnał czy BSA w zwalczaniu kradzieży własności intelektualnej poprzez organizacje wspólnych szkoleń, konferencji, opracowywanie metodyk zwalczania przestępczości określonego typu. | **Wyjaśnienie**  Taka współpraca nie jest wykluczana przez Strategię. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.6 (p 5.6) |  | PIIT: Brakować zdaje się opisu działań, jakie będzie podejmowała Polska na arenie międzynarodowej  w stosunku do podejrzewanych o popełnienie cyberprzestępstw, tak pojedynczych osób z innych krajów, jak i zorganizowanych grup przestępczych oraz grup sponsorowanych przez instytucje rządowe i siły zbrojne państw prowadzących ofensywne działania w cyberprzestrzeni, ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw.  W Strategii szeroko opisano działania na rzecz współpracy, współdziałania, wymiany informacji, reagowania na incydenty. Nie ma nic na temat dążenia Polski do skutecznego ścigania tych przestępstw, a przecież wszelkie działania ofensywne w cyberprzestrzeni są prowadzone z terytoriów innych państw. W Strategii nie znajdziemy odpowiedzi na to jak Polska poradzi sobie ze ściganiem przestępstw cyber prowadzonymi na arenie międzynarodowej, czy nawet w kraju. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 1.6 (p 5.6) |  | PIIT: Nie zostały zaadresowane ani zaznaczone wielokrotnie sygnalizowane kwestie nadużyć (tzw. fraudów) na rynku telekomunikacyjnym, polegające na wprowadzaniu klientów w błąd, podszywaniu się pod innego przedsiębiorcę, manipulowaniu podczas zawierania umowy. Obecnie w praktyce każdy przedsiębiorca telekomunikacyjny samodzielnie realizuje działania w zakresie zwalczania nadużyć telekomunikacyjnych, dzięki czemu wypracowane zostają własne metody działania, na które składają się stosowane procedury, technologie oraz zespoły pracownicze. Wdrażanie indywidualnych działań nie jest jednak wystarczające wobec braku odpowiednich rozwiązań systemowych i prawnych. | **Uwaga nieuwzględniona**  Strategia nie reguluje prawa karnego. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących  w szczególności bezpieczeństwa:  1) aplikacji,  2) urządzeń mobilnych,  3) stacji roboczych,  4) serwerów i sieci,  5) modeli chmur obliczeniowych. | PIIT: Wprowadzenie specyficznych wymagań dla sektora publicznego poprzez Narodowe Standardy Cyberbezpieczeństwa, może być wykorzystywane do wprowadzania preferencji dla określonych dostawców zaopatrujących sektor publiczny i ograniczaniu konkurencji. Obecnie państwo chętnie powierza kluczowe zadania w zakresie wytwarzania systemów informatycznych podmiotom kontrolowanym lub zarządzanym przez państwo bez przestrzegania zasad konkurencji np. w drodze stanowienia prawa. Tworzenie Narodowych Standardów Cyberbezpieczeństwa bez powiązania z międzynarodowymi może prowadzić do pogorszenia jakości specyficznie polskich rozwiązań  i wymagań. Nie ma mowy o żadnej konkurencyjności rozwiązań i poprawianiu cyberbezpieczeństwa, jeżeli mają je realizować imiennie wskazywane podmioty. Budzi to poważne wątpliwości co do bezpieczeństwa przyjmowanych rozwiązań. Przypominamy także że art.67 Ustawy o Krajowym Systemie Cyberbezpieczeństwa przewiduje wydawanie, przez Prezesa Rady Ministrów, wiążących wytycznych dla sektora publicznego w zakresie Cyberbezpieczeństwa który stanowi swoisty bufor bezpieczeństwa. Istnienie tych regulacji nie uzasadnia wprowadzanie nowych opartych o bliżej niedoprecyzowane Narodowe Standardy Cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  NSC będą nieobowiązkowe i technologicznie neutralne. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych  i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność. Pozyskiwanie nowych technologii dla rozwoju rodzimych przedsięwzięć będzie realizowane poprzez udział w inicjatywach międzynarodowych kładących nacisk na innowacyjność, w drodze współpracy dwustronnej oraz w ramach organizacji międzynarodowych, w tym w ramach planowanego przez Komisję Europejską i Państwa Członkowskie Europejskiego Centrum Kompetencji Cyberbezpieczeństwa. | PIIT: O ile pozyskiwanie technologii z zagranicy jest oczywiście uzasadnione, to jednak rolą państwa powinno być przede wszystkim wymierne inwestowane w rodzime polskie nowe rozwiązania, gdyż kompetencje cyberbezpieczeństwa powinny być cechą, własnością i know how o narodowym charakterze. Państwo powinno finansować wytwarzanie rodzimych polskich rozwiązań, a nie przerzucać zagadnienie finansowania takich przedsięwzięć na środki unijne, które wymagają przeważnie programów z realizacją w zespołach wielonarodowych, niekoniecznie wskazanych  w kontekście cyberbezpieczeństwa. Wydaje się rzeczą oczywistą, że koniecznym warunkiem rozwoju i zapewnienia cyberbezpieczeństwa w Polsce jest posiadanie odpowiednich zasobów zarówno zatrudnionych w polskich podmiotach,  jak i w zagranicznych oddziałach firm znajdujących się w Polsce. | **Uwaga nieuwzględniona**  Cel szczegółowy 3 opisuje kierunki interwencji rządu RP w kontekście wzmacniania polskiego potencjału. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 2.2 (p 6.2) | Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego organu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług  i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa | PIIT: Wyznaczenie krajowego organu to zdecydowanie za mało by projekt się udał. Istnieje przede wszystkim potrzeba zapewnienia mu odpowiednich środków finansowych i narzędzi do prowadzenia badań. | **Wyjaśnienie**  Akt o Cyberbezpieczeństwie wymaga od państw członkowskich określonych działań, w tym utworzenie ww. organu. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga ogólna |  | PIIT: Niedostateczne uwzględnienie współpracy publiczno-prywatnej w zakresie cyberbezpieczeństwa. Uważamy, że programy oceny i certyfikacji (jak opisane w pkt. 6.2. Strategii) stanowią wyłącznie wymaganie formalne, natomiast warunkiem rzeczywistego podniesienia cyberbezpieczeństwa będzie stworzenie faktycznych ram współpracy. Naszym zdaniem z punktu widzenia Strategii należałoby określić przynajmniej (Propozycja poniżej):   1. Listę producentów i dostawców usług cyfrowych o kluczowym znaczeniu dla cyberbezpieczeństwa RP w latach 2019-2024. Obecność na liście musi wynikać  z powszechności stosowania określonych rozwiązań i/lub z funkcji istotności takich rozwiązań dla działania państwa. 2. Określenie strategicznych celów współpracy z tymi dostawcami. W szczególności powinno to dotyczyć sposobów wymiany informacji istotnej dla cyberbezpieczeństwa, podniesienia wiedzy i umiejętności związanej z cyberbezpieczeństwem rozwiązań tych dostawców  w administracji (por. cel szczegółowy 8.1.) oraz innych aspektów współpracy. 3. Wskazanie i zapewnienie odpowiednich zasobów oraz właściwego centrum współpracy dla wszystkich wybranych producentów i dostawców. 4. Określenie zasad współpracy międzynarodowej w ramach współdziałania z tymi samymi producentami i dostawcami w wielu krajach UE. 5. Określenia zasad współpracy w/w dostawców z polskimi podmiotami istotnymi dla cyberbezpieczeństwa państwa (np. operatorami usług kluczowych) wdrażającymi technologie tych dostawców. Przykładem mogą być minimalne warunki suportu technicznego jakie odbiorca musi mieć zapewnione przy wdrożeniu, przy jednoczesnym zachowaniu zasady neutralności technologicznej zapisanej w ustawie o informatyzacji, tzn. brak dyskryminacji takiego podmiotu komercyjnego wynikający z faktu, że inne rozwiązanie, gdzie suport nie jest wymagany staje się automatycznie tańsze i bardziej atrakcyjne. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 3.2 (p 7.2) | Zbudowanie mechanizmów współpracy między sektorem publicznym  i prywatnym | PIIT: W pkt. zatytułowanym „zbudowanie mechanizmów współpracy między sektorem publicznym  i prywatnym” zawarta jest sugestia, że takie mechanizmy dopiero musza być budowane tzn., że ich jakoby nie ma.  Po pierwsze: pewne mechanizmy istnieją np. konsultacji projektów przepisów, spotkań tematycznych, udziału w konferencjach obu sektorów, etc. Rada ds. cyfryzacji także w pewnym stopniu służy tym celom choć naszym zdaniem z niedostateczna reprezentacja sektora prywatnego/biznesowego. Dobrym przykładem na współprace sektorów jest praca grup roboczych nad wdrożeniem ustawy  o krajowym systemie cyberbezpieczeństwa i wypracowywane w jej ramach opinie i opracowania. | **Uwaga uwzględniona częściowo.**  Zmiana w zapisie – nastawienie na rozwój współpracy. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o cel szczegółowy 3.2 (p 7.2) | Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie inicjowania  i prowadzenia projektów w dziedzinie cyberbezpieczeństwa. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym będzie promować polski biznes na arenie międzynarodowej | PIIT: Chcielibyśmy zapytać także o jakich powstających formach europejskiej współpracy publiczno-prywatnej jest mowa w tym pkt? | **Wyjaśnienie**  Np. Horyzont 2020, CEF, wkrótce DEP. | **Przyjęte wyjaśnienie.** |
|  | PIIT | Uwaga o Zarządzanie Strategią (p 10) | Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. | PIIT: Występuje niespójność - sam projekt uchwały Rady ministrów w par. 3 zobowiązuje Ministra właściwego do corocznego przedstawiania sprawozdania. | **Wyjaśnienie**  Przegląd to nie to samo co informacja roczna. | **Przyjęte wyjaśnienie.** |
|  | PTI | Uwaga o cel szczegółowy 1.5 (p 5.5) | Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych | PTI: Czy sformułowanie to oznacza, że operatorzy infrastruktury krytycznej, usług kluczowych i dostawcy usług cyfrowych będą zobligowani do szacowania ryzyka wg nowej jednolitej metodyki? Podmioty te w większości przypadków obecnie przeprowadzają szacowanie ryzyka wykorzystując uznane powszechnie standardy (np. ISO). Nie jest jasne czy wspomniana w Strategii *wspólna metodyka statycznego i dynamicznego szacowania ryzyka* będzie w jakiś sposób powiązana z międzynarodowymi standardami, czy też to będzie zupełnie nowa metodyka? | **Wyjaśnienie**  Metodyka musi być spójna aby oszacować ryzyko na poziomie krajowym. Konieczne jest zapewnienie porównywalności wyników, co będzie miało wpływ na opracowanie wspólnego krajowego planu zarzadzania ryzykiem. |  |
|  | PTI | Uwaga o cel szczegółowy 2.1 (p 6.1) | 2. Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń | PTI: należy mieć na uwadze, że istnieje już szereg uznanych międzynarodowych standardów związanych z cyberbezpieczeństwem. PTI postuluje dodanie zapisu, że Narodowe Standardy Bezpieczeństwa będą powiązane z uznanymi standardami międzynarodowymi. Ma to na celu zapewnienie odpowiedniego poziomu standardów narodowych i nie wprowadzanie nowych specyficznych i niszowych rozwiązań polskich. | **Uwaga nieuwzględniona**  O ile nie jest to wykluczone, nie jest to też miejsce na taki zapis. |  |
|  | PTI | Uwaga o cel szczegółowy 4.1 (p 8.1) | W celu utrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, podjęte będą działania w celu zbliżenia zarobków tych pracowników do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym.  Równocześnie rząd RP przygotuje i wdroży systemowe rozwiązanie w celu zapewnienia merytorycznego wsparcia dla podniesienia kompetencji pracowników jednostek administracji samorządowej w zakresie cyberbezpieczeństwa. | PTI: Proponowane zapisy naszym zdaniem wydają się niewystarczające w sytuacji rosnącego deficytu pracowników związanych z szeroko rozumianym obszarem cyberbezpieczeństwa. Rekomendujemy wprowadzenie systemowych rozwiązań pozwalających na ocenę i weryfikację kompetencji zawodowych związanych z obszarem cyberbezpieczeństwa, np. narodowego systemu certyfikacji kwalifikacji zawodowych z obszaru cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | PTI | Uwaga ogólna |  | PTI: Za istotny mankament Strategii uważamy brak mierników umożliwiających ilościową ocenę skuteczność jej realizacji. Brak określenia mierników niesie ryzyko, że Strategia nie będzie prowadziła do istotnej poprawy poziomu cyberbezpieczeństwa lub że poziom poprawy pozostanie nieznany. Nasuwa się też pytanie czy przewiduje się jakiś sposób oceny poziomu cyberbezpieczeństwa poszczególnych podmiotów oraz szacowanie zmian poziomu bezpieczeństwa w czasie. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. |  |
|  | PTI | Uwaga ogólna |  | PTI: 5. Nie jest zrozumiałe dlaczego w projekcie Strategii zwrócono niewielką uwagę na najnowsze rozwiązania techniczne mające coraz większy związek z cyberbezpieczeństwem. Obejmują one takie obszary jak:  a. Sztuczna inteligencja (głębokie uczenie i uczenie maszynowe);  b. Big Data;  c. Chmury obliczeniowe;  d. Internet Rzeczy (IoT);  e. 5G.  Naszym zdaniem obecna Strategia Cyberbezpieczeństwa powinna przewidywać zarówno zagrożenia płynące ze strony ww. technologii, jak i korzyści, które można osiągnąć wykorzystując takie technologie jak np. sztuczna inteligencja, Big Data czy też Internet Rzeczy do zwiększenia poziomu cyberbezpieczeństwa państwa. | **Uwaga nieuwzględniona**  Nie jest zasadne opierać Strategię na zagadnieniach stricte technologicznych. |  |
|  | Fundacja INFO OPS Polska | Uwaga o treść wstępu | a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej.“ | IOP: W zakresie wskazanym w dokumencie, poprzez dedykowanie odpowiedzialności podmiotów na poziomie operacyjnym zajmujących się cyberbezpieczeństwem, sformułowanie nie precyzuje odpowiedzialności za bezpieczeństwo wirtualnego środowiska informacyjnego rozumianego jako środowisko poznawcze oddziałujące na użytkowników cyberprzestrzeni. Wraz z rozwojem systemów teleinformatycznych i nawyków poznawczych użytkowników cyberprzestrzeni wymiar wirtualny środowiska informacyjnego (środowisko informacyjne funkcjonuje w trzech wzajemnie zależnych wymiarach: fizycznym, wirtualnym, poznawczym/kognitywnym) stanowi coraz większy udział w procesie oddziaływania na procesy poznawcze odbiorców we współczesnym świecie. Z uwagi na powyższe, w związku z wykorzystaniem wirtualnego środowiska informacyjnego do prowadzenia działań manipulacyjnych przy wykorzystaniu informacji, powstał nowy sektor działalności podmiotów zajmujących się bezpieczeństwem środowiska informacyjnego, w tym wirtualnego środowiska informacyjnego rozumianego jako środowisko poznawcze. Rozwój usług typu IERT (Information Operation Emergency Response Team) zbliżonych zakresem odpowiedzialności do procedur i zakresu usług CERT (o innej, technicznej specyfice) lecz prowadzących działania na rzecz kontroli i bezpieczeństwa środowiska informacyjnego są elementem/aktorem realizującym działania operacyjne w wymiarze wirtualnym środowiska informacyjnego (cyberprzestrzeni) na rzecz jego bezpieczeństwa. Z uwagi na powyższe poddajemy pod ocenę zmianę treści z obecnej na:  “a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem **i bezpieczeństwem wirtualnego środowiska informacyjnego** w sferze operacyjnej.“ | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o treść wstępu | W działaniach tych uczestniczą pojedyncze osoby, zorganizowane grupy przestępcze oraz grupy sponsorowane przez instytucje rządowe i siły zbrojne państw prowadzących **ofensywne działania w cyberprzestrzeni, ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw**. | IOP: nie uwzględniono działań ofensywnych, wywiadowczych prowadzonych poprzez wirtualne środowisko informacyjne przy wykorzystaniu systemów teleinformatycznych. Metodyka rozpoznania oparta na dedykowanych ścieżkach rozpoznania (cyberszpiegostwa) realizowanych przy użyciu rozpoznania i podejścia poprzez narzędzia i metodykę operacji informacyjnych, w tym psychologicznych realizowanych w wirtualnym środowisku informacyjnym stanowi równorzędny w stosunku do integralności i poufności informacji systemóœ teleinformatycznych obszar ryzyka i jest stosowany w działaniach wywiadowczych przez wrogie Polsce ośrodki państwowe. Z uwagi na powyższe poddajemy pod ocenę zmianę treści z obecnej na:  W działaniach tych […] ofensywne działania w cyberprzestrzeni, **w tym w wirtualnym środowisku informacyjnym** ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw. | **Uwaga nieuwzględniona**  Kwestie militarne są do decyzji MON. |  |
|  | Fundacja INFO OPS Polska | Uwaga o treść Zakresu Strategii | Strategia uwzględnia, w szczególności:  1) cele i priorytety państwa w zakresie cyberbezpieczeństwa, **w tym bezpieczeństwa wirtualnego środowiska informacyjnego.** | IOP proponuje dodanie zwrotu: „**w tym bezpieczeństwa wirtualnego środowiska informacyjnego**” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o cel szczegółowy 1.6 (p 5.6) | W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym (w tym działań o charakterze hybrydowym **z uwzględnieniem operacji manipulacyjnych, informacyjnych, psychologicznych realizowanych poprzez wirtualne środowisko informacyjne**) | IOP: Z uwagi na szeroką, niesprecyzowaną definicję sformułowania “zdarzeń o charakterze terrorystycznym ( w tym działań o charakterze hybrydowym)” należy zauważyć iż metodyka specjalistycznych operacji manipulacyjnych towarzyszących w/w zagrożeniom jest realizowana poprzez wirtualne środowisko informacyjne. Niejednokrotnie z uwzględnieniem fizycznego wymiaru środowiska informacyjnego poprzez środki aktywne, w tym: inspirację, prowokację, mistyfikację, etc, oddziałujących wtórnie na wymiar wirtualny środowiska informacyjnego poprzez systemy teleinformatyczne. IOP proponuje dodanie:  „**z uwzględnieniem operacji manipulacyjnych, informacyjnych, psychologicznych realizowanych poprzez wirtualne środowisko informacyjne**” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o cel szczegółowy 3.1 (p 7.1) | Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa, **bezpieczeństwa środowiska informacyjnego, komunikacji strategicznej operacji informacyjnych, w tym psychologicznych**. Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych | IOP proponuje dodanie: „**bezpieczeństwa środowiska informacyjnego, komunikacji strategicznej operacji informacyjnych, w tym psychologicznych**.” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o cel szczegółowy 3.3 (p 7.3) | ochronę procesów demokratycznych przed zakłóceniami z wykorzystaniem cyberzagrożeń, **w tym (lub) i, wirtualnego środowiska informacyjnego** | IOP: Z uwagi na uwzględnienie ochrony procesów demokratycznych przed zakłóceniem z wykorzystaniem cyberzagrożeń, w związku z niesprecyzowanym zakresem pojęciowym cyberzagrożeń i z uwagi na brzmienie uzasadnienia zawarte wcześniej IOP proponuje dodanie:  „**w tym (lub) i, wirtualnego środowiska informacyjnego**” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o cel szczegółowy 3.4 (p 7.4) | Siły Zbrojne RP, jako podstawowy element systemu obronnego państwa […] oraz zwalczanie źródeł zagrożeń, **w tym działania na rzecz bezpieczeństwa środowiska informacyjnego.** | IOP proponuje dodać: „**w tym działania na rzecz bezpieczeństwa środowiska informacyjnego**” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | Fundacja INFO OPS Polska | Uwaga o cel szczegółowy 4.3 (p 8.3) | W obliczu coraz liczniejszych zagrożeń […] świadomości obywateli w kontekście **weryfikacji autentyczności informacji oraz reagowania na próby jej zakłócenia.** | IOP z uwagi na wcześniejsze wnioskowanie oraz w związku iż wskazany zakres nie uwzględnia faktu, iż dezinformacja rozumiana jako informacja , zwłaszcza w kategoriach obszaru kształtowania kontroli odbitej jako środka aktywnego może być informacją prawdziwą, w tym informacją niepodlegającą weryfikacji, lub informacją spójną z prowokacją, inspiracją, mistyfikacją (kwalifikowanymi jako środki aktywne) należy zauważyć iż zawężanie pojęcia na rzecz “weryfikacji autentyczności informacji” stosowane w dokumencie może być niewystarczające dla celów zwiększenia odporności społecznej na procesy manipulacyjne. IOP proponuje zmianę zwrotu na:  „**rozwijanie świadomości obywateli w kontekście weryfikacji informacji, w tym zwiększanie świadomości społecznej w zakresie procesów manipulacji środowiskiem informacyjnym**” | **Uwaga nieuwzględniona**  Proponowana zmiana jest niezgodna terminologicznie z innymi dokumentami rządowymi oraz ustawami. |  |
|  | IBiS | Uwaga ogólna |  | IBiS: Dokument pozbawiony jest cech wizjonerskich, ma charakter zachowawczy i jest zdecydowanie zbyt skoncentrowany na kwestiach technicznych i taktyczno-operacyjnych. Zaplanowane działania cechują się minimalizmem i brakiem ambicji. Strategia pozbawiona jest także całościowej, długofalowej wizji obejmującej aktywność wszystkich segmentów administracji państwowej, w odniesieniu do całej cyberprzestrzeni publiczne} i prywatnej. Zamiast tego koncentruje się na wybranych fragmentach, ujętych w ustawie o Krajowym Systemie Cyberbezpieczeństwa (w swej większości mających charakter publiczny, w szczególności rządowy), które wszakże nie obejmują swym zasięgiem całej cyberprzestrzeni. | **Uwaga nieuwzględniona**  Strategia jest dokumentem ramowym, określającym kierunki działań rządu RP. | **.** |
|  | IBiS | Uwaga ogólna |  | IBiS: Strategia stawia na kontynuację, nie dostrzegając, że obecny stan polskiej rzeczywistości w zestawieniu z gwałtownie narastającymi wyzwaniami technologicznymi i cywilizacyjnymi, wymaga od państwa działań o skali i charakterze przełomowym. Dynamicznie rozwijająca się cyberprzestrzeń wymaga celów i środków o charakterze rewolucyjnym, a nie ewolucyjnym. Budowa, znajdującego się na początkowym etapie rozwoju Krajowego Systemu Cyberbezpieczeństwa (ustawa w tej sprawie stanowi dopiero pierwszy krok), tworzy niewyobrażalne szanse dla rozwoju innych dziedzin państwa, gospodarki i społeczeństwa Strategia zdaje się tej okoliczności nie dostrzegać. | **Uwaga nieuwzględniona**  Przyjęto model ewolucyjny. |  |
|  | IBiS | Uwaga dot. celów |  | IBiS: Zarówno cel główny jak i cele szczegółowe są sformułowane nieprecyzyjnie i wymagają gruntownej korekty, tak aby jednoznacznie komunikować odbiorcom zamiary rządu. W obecnej postaci informują jedynie ogólnie o intencjach odnośnie planowanych działań, a nie stanu rzeczy do jakiego mają one doprowadzić, Krótko mówiąc nie informują one o celach, a jedynie o środkach, bez wskazania czemu służyć ma ich zastosowanie. Muszą one być sformułowane tak aby możliwa była ocena stopnia ich realizacji, a więc powinny być mierzalne, ale jednocześnie realistyczne, czyli wykonalne oraz precyzyjne i jednoznaczne. Ważnym elementem jest także możliwie precyzyjne określenie czasu w jakim oczekuje się ich spełnienia. Ani cel główny ani żaden z celów szczegółowych nie zawiera takich informacji. | **Uwaga nieuwzględniona**  Konkretne działania wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | IBiS | Uwaga o treść celu główny | Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. | IBiS: Odbiorca nie otrzymuje informacji ani na temat stopnia przyrostu odporności, ani metodologii jej pomiaru, ani czasu w jakim ma on nastąpić. Konieczne jest przyjęcie przez organ kształtujący praktyczny wymiar wdrożenia strategii jakiejkolwiek metodologii pozwalającej na ocenę poziomu cyberbezpieczeństwa poszczególnych instytucji | **Uwaga nieuwzględniona**  Ocena bezpieczeństwa instytucji leży w kompetencjach i odpowiedzialności tej instytucji. Wspomniane zapisy dotyczą ogólnej oceny sytuacji w skali kraju. |  |
|  | IBiS | Uwaga o cel główny |  | IBiS: Osobna kwestia jest niezwykle minimalistyczne ujęcie głównego celu strategii państwa na okres 5 lat i ograniczenie go wyłącznie do sfery publicznej. Zupełnie niezrozumiała jest abdykacja rządu z odpowiedzialności za sferę niepubliczną i zawężenie celu rządu wyłącznie do "promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji". Abstrahując od tego, że promowanie wiedzy i dobrych praktyk nie może być celem, a jedynie działaniem - środkiem do celu, to sprowadzenie roli Państwa do promotora wiedzy i dobrych praktyk oznacza pozostawienie dużej części cyberprzestrzeni poza zakresem zainteresowania, a zatem możliwości oddziaływania państwa. Jest to rozwiązanie sprzeczne ze standardami wypracowanymi w państwach uznanych za wiodące w dziedzinie budowy narodowych systemów cyberbezpieczeństwa | **Uwaga nieuwzględniona**  Opisane działania są elementem celu m.in. celu szczegółowego 4 - Budowanie świadomości i kompetencji społecznych w zakresie cyber-bezpieczeństwa |  |
|  | IBiS | Uwaga o Zarządzanie Strategią (p 10) | Koordynatorem wdrażania Strategii jest minister właściwy do spraw informatyzacji. | IBiS: Wskazanie w strategii jako koordynatora, moderatora i audytora wdrażania założeń strategii w postaci ministra właściwego ds. cyfryzacji uznać należy za mało praktyczne i nieefektywne, ponieważ do jego odpowiedzialności należeć będzie tworzenie warunków do systematycznego budowania nowych możliwości wynikających z cyberprzestrzeni do rozwoju polski, jak też do systematycznej poprawy warunków życia naszego społeczeństwa. Nie może on w tej sytuacji pełnić wobec siebie roli audytora w tym obszarze. | **Uwaga nieuwzględniona**  Koordynator to nie audytor. |  |
|  | IBiS | Uwaga o cel szczegółowy 1.1 (p 5.1) | W ramach realizacji Strategii uregulowane zostaną kwestie współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny. | IBiS: W naszej ocenie poza ustaleniem systemu i zasad takiej wymiany powinna odbywać się ona z wykorzystaniem instytucjonalnej struktury, która także w swoich zadaniach będzie miała koordynowanie prac wdrażających strategię oraz ustalanie norm związanych z zapewnieniem bezpieczeństwa infrastruktury IT jak też tworzenie procedur jej bezpiecznego wykorzystania we współdziałaniu z właściwymi instytucjami. Struktura ta wzięłaby na siebie ciężar podniesienia efektywności funkcjonowania Krajowego Systemu Bezpieczeństwa otrzymując dla swojego działania niezbędne środki i narzędzia pozwalające na zaangażowanie w jej prace wysokiej klasy specjalistów. Źródła i sposób zapewnienia finansowania jej działania na oczekiwanym poziomie powinny zostać wskazane w dokumentach strategii. Jej powstanie, jako kluczowego elementu budowy cyberbezpieczeństwa, powinna uwzględniać Strategia.  Organ ten powinien podlegać bezpośrednio premierowi rządu. Umożliwi mu to bardziej skuteczne działanie w ramach współpracy z innymi resortami i ośrodkami, jak też da możliwość skutecznej współpracujący z komórkami sił zbrojnych i służb specjalnych oraz policji. Szczególne znaczenia ma to w przypadku koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny w zakresie cyberbezpieczeństwa. Posiadając wymiar ponad resortowy miałby możliwość skutecznego koordynowania prac wdrażających strategię, jak też ustalanie norm związanych z zapewnieniem bezpieczeństwa infrastruktury IT współdziałając w tym zakresie z PKN. 0dpowiadałby za tworzenie procedur jej bezpiecznego wykorzystania we współdziałaniu z właściwymi instytucjami oraz, w oparciu o posiadaną wiedzę, inicjowanie ich nowelizacji z uwagi na dynamiczny rozwój cyberprzestrzeni. Tworzenie nowej, wyspecjalizowanej instytucji dawałoby nadzieję na przyznanie jej funduszy i określenie zasad finansowania pozwalających na opracowanie siatki płac dającej szansę na przyciągnięcie wybitnych specjalistów, jak też dających szansę na realne wdrożenie znajdujących się w strategii celów szczegółowych szczególnie w odniesieniu do:   * Planowanego wsparcia udzielanego jednostkom terytorialnym, * Wsparcia operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług i udzielaniu im założonej w Strategii pomocy. * Stworzenia wyspecjalizowanego pionu zatrudniającego wybitnych specjalistów posiadających kompetencje umożliwiające skuteczne kształtowanie i koordynowanie działań służących realizacji celu opisanego w punkcie 5.6 Strategii. | **Uwaga nieuwzględniona**  Strategia nie może powoływać i finansować nowych struktur.  Jest to materia o charakterze ustawowym. |  |
|  | IBiS | Uwaga o cel szczegółowy 1.1 (p 5.1) | jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, **w szczególności świadczących usługi** **chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych.** | IBiS: Z uwagi na założenie, że będą one coraz częściej wykorzystywane jako model przetwarzania danych dla usług kluczowych. W naszej ocenie celowym jest wprowadzenie zapisów stawiających wymóg oceny czy systemy informacyjne wspierające realizację usługi kluczowej powinny przetwarzać i przechowywać dane w chmurze. W przypadku systemów IT wspierających bezpośrednio realizację usług kluczowych, w sytuacji kiedy jest konieczne wykorzystanie przetwarzania i przechowywania w chmurze za celowe uznajemy ograniczenie ich wyłącznie do świadczonych przez narodowego operatora takiego np. jak NASK czy Exatel | **Uwaga nieuwzględniona**  Materia poza zakresem Strategii. |  |
|  | IBiS | Uwaga o cel szczegółowy 1.1 (p 5.1) | Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnych w cyberprzestrzeni. | IBiS: Istotnym w naszej ocenie wydaje się nadanie priorytetu pracom regulującym wytwarzanie, posiadanie, pozyskiwanie oraz wykorzystanie specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnym w cyberprzestrzeni, **jak też takich które służą tylko i wyłącznie do tego celu.** | **Uwaga nieuwzględniona**  Wszystkie wskazane w Strategii kierunki interwencji są priorytetowe. |  |
|  | IBiS | Uwaga o cel szczegółowy 1.2 (p 5.2) | Standaryzacja i wymagania cyberbezpieczeństwa, opracowane i wykorzystywane przez administrację publiczną w ramach Narodowych Standardów Cyberbezpieczeństwa, powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli. | IBiS: Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowania dobrych praktyk i zaleceń w naszej ocenie, celem przyspieszenia procesu ich powstania i implementacji wymaga zapisu o celowość wykorzystania już istniejących w krajach NATO i UE. | **Uwaga nieuwzględniona**  NSC będą ustalane odrębnie. |  |
|  | IBiS | Uwaga o cel szczegółowy 5.1 (p 9.1) | W obliczu wszechobecnych procesów globalizacyjnych i związanych z nimi współzależności państw, międzynarodowa współpraca jest kluczowa dla osiągnięcia bezpieczeństwa globalnej cyberprzestrzeni. | IBiS: Za słuszne należy uznać podkreślenie wagi współpracy międzynarodowej i wymienienie odpowiednich organizacji międzynarodowych i form współpracy regionalnej. Konieczne jednak jest precyzyjne określenie roli jaką Polska powinna odgrywać w takich międzynarodowych formatach oraz w regionalnych forach współpracy, takich jak inicjatywa Trójmorza czy Grupa Wyszehradzka. Aktywna obecność i współpraca międzynarodowa musi służyć konkretnym celom, tak aby nie stała się sztuka dla sztuki, albo celem samym w sobie. | **Uwaga nieuwzględniona**  Rola RP została opisana. |  |
|  | IBiS | Uwaga o cel szczegółowy 5.1 (p 9.1) | Silna pozycja międzynarodowa Polski w obszarze cyberbezpieczeństwa nie będzie możliwa bez odpowiedniego zaplecza merytorycznego. Zasób kadrowy wsparty odpowiednim finansowaniem będzie podstawą do zbudowania wizerunku Polski jako kompetentnego gracza na arenie międzynarodowej. | IBiS: Strategia mówi również o konieczności posiadania zaplecza merytorycznego, czyli ludzi łączących wiedzę o cyberbezpieczeństwie z wiedza o polityce międzynarodowej i bezpieczeństwie. Nie przedstawiono konkretnych pomysłów jak takie osoby pozyskać lub/i wyszkolić. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań*.* |  |
|  | IBiS | Uwaga ogólna |  | IBiS: Brakuje również jasnego określenia zasobów, które Polska posiada do realizacji tej strategii oraz przedstawienia zagrożeń w wymiarze strategicznym dla kraju. Autorzy nie przedstawiają jasno, jakie mogą być skutki zaniedbań. | **Uwaga nieuwzględniona**  Strategia nie jest dokumentem analitycznym. |  |
|  | IBiS | Uwaga ogólna |  | IBiS: Niektóre postulaty jak np. zacieśnianie współpracy prywatno-publicznej są w naszej opinii zbyt ogólne, Oczywiście celem strategii jest wskazanie najważniejszych kierunków rozwoju państwa w cyberprzestrzeni, ale warto byłoby uwzględnić konkretne pomysły i inicjatywy. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | IBiS | Uwaga o cel szczegółowy 4.2 (p 8.2) |  | IBiS: Strategia przewiduje poważne zmiany w systemie edukacji na różnych szczeblach. Konieczne jest uwzględnienie by propozycje te były konsultowane z ministerstwem edukacji i wkomponowane w szerszą reformę edukacji. | **Uwaga uwzględniona**  Zmiany w tym obszarze mogą zostać poczynione jedynie w drodze współpracy z MEN. |  |
|  | FBC | Uwaga o Wstęp | Współpraca ta odgrywa istotną rolę w reagowaniu na zwiększającą się liczbę incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, powodujących rosnące rokrocznie straty materialne i wizerunkowe. W działaniach **tych** uczestniczą pojedyncze osoby, zorganizowane grupy przestępcze | FBC: W opinii Fundacji zastosowanie zaimka "**tych**", biorąc pod uwagę zdanie poprzedzające, sugerowałoby działania odnoszące się do współpracy.  FBC proponuje zamianę na zwrot: „**przestępczych**” | **Uwaga uwzględniona** |  |
|  | FBC | Uwaga o treść Kontekstu strategicznego | Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim **odporności systemów informacyjnych**, | FBC: W opinii Fundacji należy doprecyzować na co mają być odporne systemy informacyjne. W pkt 4.2 zostało to wskazane. Wydaje się, że zapisy te należy powtórzyć również w tym miejscu. | **Uwaga uwzględniona** |  |
|  | FBC | Uwaga o cel główny (p 4.2) | Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, | FBC: Prosimy o informację w jaki sposób może to być zapewnione, skoro systemy przetwarzające informacje w wojsku są utrzymywane i zarządzane przez MON? Czy podział odpowiedzialności nie jest tu już sprecyzowany? | **Uwaga nieuwzględniona**  Podnoszenie poziomu odporności będzie się odbywało w ramach konkretnych systemach. Odpowiedzialność leży po stronie zarządzających systemami. |  |
|  | FBC | Uwaga o treść celów szczegółowych (p 4.3) | **Cel szczegółowy 2.** Stymulowanie podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom. | FBC: Cel szczegółowy w rozdziale 6 (str. 15) ma inną nazwę. Która z nazw jest właściwa? | **Uwaga uwzględniona** |  |
|  | FBC | Uwaga o cel szczegółowy 1 (p 5) | Cel szczegółowy 1 – **rozwój** Krajowego Systemu Cyberbezpieczeństwa | FBC: Użycie określenia "rozwój" sugerowałoby sytuację, w której system jest wdrożony i może w związku z tym podlegać przeglądowi i modyfikacjom w celu poprawy jego efektywności. Treść rozdziału takiego stan rzeczy nie opisuje, stąd użycie określenia "rozwój", w opinii Fundacji, wydaje się nieuzasadnione. FBC: sugeruje zmianę na zwrot: „**kontynuacja wdrażania**” | **Uwaga nieuwzględniona**  W opinii MC system jest obecnie rozwijany. |  |
|  | FBC | Uwaga o cel szczegółowy 1.1 (p 5.1) | W ramach realizacji Strategii uregulowane zostaną kwestie współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny. | FBC: Wydaje się, że treść powinna zostać przeniesiona do rozdziału 5.2, który opisuje współpracę operacyjną pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny | **Uwaga nieuwzględniona**  W opinii MC jest to odpowiednia lokalizacja. |  |
|  | FBC | Uwaga o cel szczegółowy 1.1 (p 5.1) | Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. | FBC: Proponujemy usunąć. Nie ma uzasadnienia umieszczania w Strategii działań Kolegium, które opisane są bezpośrednio w art. 65 ustawy o krajowym systemie cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Nie jest to dublowanie zapisów, tylko wskazywanie roli Kolegium w działaniach określonych w Strategii. |  |
|  | FBC | Uwaga o cel szczegółowy 1.2 (p 5.2) | Niezbędne jest wdrożenie systemowych rozwiązań pozwalających na wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do zagrożeń i incydentów. | FBC: To jest ewidentnie kwestia do uregulowania w ustawie o KSC. W opinii Fundacji powinno to być wskazane obligatoryjnie jako zadanie do Planu działania na rzecz wdrożenia Strategii | **Uwaga uwzględniona**  Kwestia ta może być przedmiotem dyskusji w trakcie nowelizacji ustawy o ksc. |  |
|  | FBC | Uwaga o cel szczegółowy 1.2 (p 5.2) | Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa ma również podnieść wprowadzenie standaryzacji rozwiązań zabezpieczających, w tym wprowadzenie minimalnych wymagań bezpieczeństwa dla sieci i systemów teleinformatycznych używanych przez administrację publiczną. | FBC: Wydaje się, że takie wymagania zostały nałożone rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Czy zatem uzasadnione jest opracowywanie nowych Narodowych Standardów Cyberbezpieczeństwa i czy te standardy zastąpią wymagania w zakresie bezpieczeństwa wskazane w rozporządzeniu o KRI? | **Uwaga nieuwzględniona**  Ustawa o informatyzacji ma bardzo szeroki zakres podmiotowy i przedmiotowy. Uzasadnione jest utworzenie specjalnych wymogów, które do tego będą działały na zasadzie dobrowolności, a nie obowiązku jak w KRI. |  |
|  | FBC | Uwaga o cel szczegółowy 1.2 (p 5.2) | Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych, inicjowanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa | FBC: Efektywność w przypadku ćwiczeń może być testowana. Temat ćwiczeń powinien zostać rozszerzony, brakuje informacji dot.:  - budżetowania (modelu);  - ćwiczeń międzysektorowych;  - poziomu ponad krajowego;  (takie relacje zakłada UoKSC).  Co w praktyce oznacza inicjowanie ćwiczeń? W jak sposób zamierzają Państwo zapewnić przejście z "inicjacji" ćwiczeń do ich "realizacji"? | **Uwaga nieuwzględniona**  Szczegółowe zasady prowadzenia ćwiczeń są poza zakresem Strategii. |  |
|  | FBC | Uwaga o cel szczegółowy 1.2 (p 5.2) | W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni. | FBC: Ten punkt stoi w sprzeczności do poprzedniego zdania. Proszę zwrócić uwagę, że w kontekście efektywności Systemu mówi się o weryfikacji (testowaniu?) efektywności, a w kontekście SZRP, mówi się o podnoszeniu zdolności. W opinii Fundacji, podnoszenie zdolności defensywnych oraz testowanie efektywności KSC wymaga innego rodzaju przedsięwzięć, na różnym poziomie zaawansowania.  Proponujemy rozszerzyć zapisy o ćwiczeniach, które sugerowałyby różne typy ćwiczeń (proceduralne, techniczne, symulacje, gry decyzyjne itd.)  Może potrzebny jest osobny punkt? | **Uwaga nieuwzględniona**  Szczegółowe zasady prowadzenia ćwiczeń są poza zakresem Strategii. |  |
|  | FBC | Uwaga o cel szczegółowy 1.3 (p 5.3) | W celu usprawnienia zarządzania bezpieczeństwem, prowadzone będą działania mające na celu wymianę informacji i uzgadnianie reakcji, tak na poziomie strategicznym jak i poziomie operacyjnym, w szczególności pomiędzy sferą cywilną i sferą wojskową. Niezbędna jest budowa odpornego na cyberzagrożenia systemu wymiany informacji dla potrzeb administracji publicznej wykorzystującego najnowocześniejsze technologie wymiany informacji, uwzględniające konieczność wysokiej mobilności. System ten będzie wykorzystywany w różnych stanach nadzwyczajnych oraz stanach gotowości obronnej państwa. | FBC: W opinii Fundacji opis tego punktu należy uzupełnić o wskazanie jakichkolwiek zadań na rzecz osiągnięcia tego podcelu. Obecnie treść stanowi jedynie zestaw oczekiwań w stosunku do systemu wymiany informacji, uniemożliwiające stworzenie szczegółowych zadań w Planie działania. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | 5.4. **Zwiększenie** cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej | FBC proponuje zamienić zwrot: **Zapewnienie spójności działań w zakresie** cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej | **Uwaga nieuwzględniona**  Preferowany jest pierwotny zapis. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | Technologie informatyczne (IT)[[7]](#footnote-7) wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom | FBC: Jest to zdanie ogólne i idące za daleko w kontekście UoKSC. Nie wszystkie technologie informatyczne (IT) są kluczowe dla krytycznych procesów w przedsiębiorstwach, co w oczywisty sposób oznacza, że nie wszystkie też wpływają na ciągłość działania państwa i bezpieczeństwo obywateli. | **Uwaga nieuwzględniona**  Nie jest wskazane, że chodzi o wszystkie technologie informatyczne. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa. | FBC proponuje wykreślić całość.  Zdania te nie mają związku z opisem punktu. Ponadto zdania o charakterze przypuszczającym ("zakłada się") nie powinno znaleźć się w strategii. Proponujemy zmianę w kierunku prostego stwierdzenia o konieczności zmian prawnych lub zaniechanie tego typu deklaracji. | **Uwaga nieuwzględniona**  Obszar ten podlega obecnie analizom – stąd tryb przypuszczający. Pominięcie kwestii 5G, kiedy została przyjęta tzw. megaustawa, a Polska dokonała analizy ryzyka w obszarze cyberbezpieczeństwa sieci 5G jest niezasadne. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | Oprócz tego, mając na uwadze, że odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie podmiotów je świadczących, rząd podejmie działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. | FBC proponuje wykreślić całość.  Fragment nie ma związku z opisywanym rozdziałem. | **Uwaga nieuwzględniona**  W opinii MC jest to powiązane ze zwiększeniem cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | Ponadto, rząd będzie wspierał te podmioty w reagowaniu na incydenty poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych. | FBC proponuje wykreślić całość.  Skąd przekonanie, że incydenty poważne (a także krytyczne, jeśli tak ocenią właściwe CSIRT-y, warto uwzględnić) o charakterze ponadsektorowym mogą mieć wyższy priorytet dla wsparcia rządowego? Odnosimy wrażenie, że takie same potrzeby mogą mieć OUK w zakresie incydentów dot. pojedynczych sektorów. Tutaj być może jest i trudniej, ponieważ w analizę i powstrzymanie zagrożenia jest zaangażowane mniej stron. | **Uwaga częściowo uwzględniona**  Dodany zostanie zapis o incydentach krytycznych. |  |
|  | FBC | Uwaga o cel szczegółowy 1.4 (p 5.4) | przede wszystkim w ramach Grupy Współpracy Dyrektywy NIS, a także w ramach współpracy **transatlantyckiej z brytyjskimi i amerykańskimi, jak i wszelkimi innymi instytucjami** stymulującymipodnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych. | FBC proponuje zamienić zwrot na: „**współpracy z instytucjami**".  W opinii FBC nie ma potrzeby wskazywania konkretnych aktorów państwowych | **Uwaga nieuwzględniona**  Nie są one wskazanie konkretnie, tylko kierunkowo. |  |
|  | FBC | Uwaga o cel szczegółowy 1.6 (p 5.6) | 5.6. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym | FBC: Treść rozdziału należy zmienić. Zwalczanie przestępczości jest związane przede wszystkim ze zwiększeniem zdolności podmiotów uprawnionych do tego. Brak tego typu zapisów spowoduje, że w planie działania nie znajdzie się żadne zadnia zwiększające zdolności np. Policji. Współpraca z operatorami i wymiana informacji, jakkolwiek cenne, są zadaniami w ramach operacyjnej współpracy. | **Uwaga nieuwzględniona**  Przyznając rację tej tezie, należy zauważyć, że wciąż należy nadać odpowiednią rangę wymianie informacji. |  |
|  | FBC | Uwaga o cel szczegółowy 1.6 (p 5.6) | Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe. | FBC: W opinii FBC warto również rozważyć umieszczenie na tej liście mediów (zarówno publicznych, jak i prywatnych). Wydaje się, że wówczas lepszym określeniem byłoby "media ogólnopolskie". Uwaga dotyczy zapowiadanych "programów informacyjnych". | **Uwaga nieuwzględniona**  W opinii MC media będą miały w tym zadaniu rolę wtórną. Nie chodzi o „programy informacyjne” w sensie wiadomości. |  |
|  | FBC | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa | FBC: Jakie jest uzasadnienie konieczności opracowania narodowych Standardów Cyberbezpieczeństwa? Wydaje się, że egzekwowanie istniejących przepisów (np. rozporządzenia KRI) byłoby wystarczającym bodźcem do "stymulowania" podniesienia poziomu odporności systemów informacyjnych administracji publicznej. | **Uwaga nieuwzględniona**  Ustawa o informatyzacji ma bardzo szeroki zakres podmiotowy i przedmiotowy. Uzasadnione jest utworzenie specjalnych wymogów, które do tego będą działały na zasadzie dobrowolności, a nie obowiązku jak w KRI. | **.** |
|  | FBC | Uwaga o cel szczegółowy 2.2 (p 6.2) | Zapewnienie cyberbezpieczeństwa wymaga**,** stosowania zabezpieczeń | FBC proponuje usunąć przecinek po słowie „wymaga”. | **Uwaga uwzględniona** |  |
|  | FBC | Uwaga o cel szczegółowy 2.3 (p 6.3) | Jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń, są okresowe audyty. Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz specyfikę poszczególnych sektorów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów. | FBC: Uważamy, że niniejszy akapit jest niejasny. Czego mają dotyczyć audyty? Gdzie mają być przeprowadzane? Czy chodzi o audyty zgodności z UoKSC, czy chodzi o audyty systemów informacyjnych/rozwiązań pod kątem cyberbezpieczeństwa? Kto ma wykonywać audyty? Czy poprzez wskazanie wymogów dla metodyk (uwzględnienie norm, dobrych praktyk itd.), należy rozumieć, że jest intencja powstania dedykowanych metodyk? | **Uwaga nieuwzględniona**  To jest ogólny zapis o audycie, a nie pełnoprawny obowiązek. W uwadze jest mowa o pełnej regulacji ustawowej. |  |
|  | FBC | Uwaga o cel szczegółowy 2.3 (p 6.3) | propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty[[8]](#footnote-8)* | FBC: Uwaga tak jak wyżej w kontekście audytów. Dodatkowo, czy Autorzy mają na myśli rządowe programy bug-bounty? Może warto to podkreślić. | **Uwaga nieuwzględniona**  Nie chodzi o rządowe programy bug-bounty, choć ich nie wyklucza. |  |
|  | FBC | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i *start-upów*, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. | FBC: W opinii Fundacji absolutnie niezbędne jest doprecyzowanie wskazanego zapisu, pozwalającego na ukierunkowanie działań w Planie działania na rzecz wdrożenia Strategii. Obecna forma umożliwia wskazanie jakiegokolwiek działania, które niekoniecznie może mieć wpływ na Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | FBC | Uwaga o cel szczegółowy 3.2 (p 7.2) | 7.2 Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym | FBC: Niezbędne jest uszczegółowienie zapisów rozdziału. Obecnie nie jest wiadomo jakie działania mają przyczynić się do osiągnięcia tego celu, tym samym niemożliwe będzie opracowanie działań w Planie działania. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | FBC | Uwaga o cel szczegółowy 3.3 (p 7.3) | w szczególności w związku z **perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6,** a także | FBC: Obecnie nie jest to już perspektywa, a realne procesy. FBC proponuje zamienić na zwrot: „**przejściem na protokół komunikacyjny IPv6**” | **Uwaga uwzględniona** |  |
|  | FBC | Uwaga o cel szczegółowy 3.3 (p 7.3) | W związku z rozwojem idei **Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0,** jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy megadanych (*Big Data)* zachodzi konieczność | FBC proponuje napisać wszystkie nazwy z małej litery: w związku z rozwojem **idei internetu rzeczy, inteligentnych miast, przemysłu 4.0**, jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy megadanych (*Big Data)* zachodzi | **Uwaga nieuwzględniona**  W dokumentach z których korzystamy, dominuje używanie tych pojęć pisanych wielką literą. |  |
|  | FBC | Uwaga o cel szczegółowy 3.3 (p 7.3) | W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze, mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami. | FBC: Zasadnym wydaje się, aby wprost wskazać, że jednym z zadań w Planie działań na rzecz wdrożenia Strategii będzie dokonanie przeglądu programów badawczych. Programy, które zyskały finansowanie NCBiR i tak będą musiały być kontynuowane, zgodnie z umowami. | **Uwaga nieuwzględniona**  Strategia nie ma możliwości kontroli NCBR ani przeglądu programów. |  |
|  | FBC | Uwaga o cel szczegółowy 3.3 (p 7.3) | Ponadto we współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu:   * ocenę skuteczności zabezpieczeń i odporności na cyberzagrożenia, * ocenę skuteczności reagowania na incydenty, * **metody wykrywania i analizy nowych typów cyberprzestępstw, cyberterroryzmu i cyberszpiegostwa,** | FBC: Jeżeli mowa w tym punkcie o funkcjach cyber threat intelligence, to może warto to napisać bardziej wprost. Jeżeli Autorzy mają na myśli innego typu metody, to proponujemy dopisanie punktu o CTI.  W opinii Fundacji punkt ten mógłby brzmieć:  "**metody budowania infrastruktury, procesów i usług umożliwiających rozpoznanie, identyfikację i zrozumienie zagrożeń w cyberprzestrzeni**" | **Uwaga częściowo uwzględniona**  Wymieniony katalog nie jest zamknięty. |  |
|  | FBC | Uwaga o cel szczegółowy 4.1 (p 8.1) | dla wszystkich pracowników **podmiotów istotnych dla cyberbezpieczeństwa** oraz dla przedstawicieli | FBC: Prosimy o doprecyzowanie o jakie podmioty chodzi i w jaki sposób będzie to zidentyfikowane. | **Uwaga nieuwzględniona**  Pojęcie celowo nieostre. |  |
|  | FBC | Uwaga o cel szczegółowy 4.1 (p 8.1) | Równocześnie rząd RP przygotuje i wdroży systemowe rozwiązanie w celu zapewnienia merytorycznego wsparcia dla podniesienia kompetencji pracowników jednostek administracji samorządowej w zakresie cyberbezpieczeństwa. | FBC: Należy doprecyzować jakie rozwiązania wdroży Rząd lub podać przykłady oczekiwań, tak by móc sformułować jakiekolwiek zadanie do Planu działania. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | FBC | Uwaga o cel szczegółowy 4.1 (p 8.1) | Kierownictwo jednostek administracji rządowej będzie dynamicznie określało odpowiedzialność i uprawnienia dla osób pełniących istotną rolę w zakresie zarządzania cyberbezpieczeństwem i odpowiednio komunikowało te ustalenia wszystkim interesariuszom. | FBC: W opinii Fundacji ten akapit wymaga doprecyzowania. W jaki sposób należy rozumieć "dynamiczne określanie odpowiedzialności"? Ad hoc? O jaką odpowiedzialność i uprawnienia chodzi? Co to za osoby? Wyznaczone w ramach jednostek administracji rządowej do zarządzania cyberbezpieczeństwem w tychże jednostkach? | **Uwaga nieuwzględniona**  W opinii MC użyte pojęcia są zrozumiałe. Chodzi o rozdzielanie zadań w sposób reakcyjny, zależny od zagrożeń |  |
|  | FBC | Uwaga o cel szczegółowy 4.3 (p 8.3) | 8.3 Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni | FBC: W opinii Fundacji, istotne jest też zapewnienie działań mających na celu wykrywanie i obsługę kampanii dezinformacyjnych posługującymi się modus operandi "klasycznych" cyberprzestępców. Chodzi tutaj o warstwę techniczną; realizowanie kampanii wpływu informacyjnego poprzez narzędzia hakerskie (np. przejmowanie kont w mediach społecznościowych, ataki webowe umożliwiające modyfikację zawartości) | **Uwaga nieuwzględniona**  Prośba o propozycje zapisów w sposób odnoszący się do reszty rozdziału. |  |
|  | FBC | Uwaga o Zarządzanie Strategią (p 10) | Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. | FBC: Biorąc pod uwagę ogólnikowe zapisy samej Strategii wydaje się, że przeglądowi powinien podlegać przede wszystkim Plan działania na rzecz wdrożenia Strategii Cyberbezpieczeństwa. W opinii Fundacji do każdego z celów należy wskazać główne działania służące jego realizacji. | **Uwaga częściowo uwzględniona**  W *Planie działania* będą wskazane ramy czasowe, w tym także terminy jego aktualizacji. |  |
|  | FBC | Uwaga o Finansowanie (p 11) | Szczegółowa wielkość i struktura kosztów poszczególnych przedsięwzięć będzie określona w procesie inicjowania konkretnych projektów. Oszacowanie kosztów finansowania wdrażania Strategii Cyberbezpieczeństwa nastąpi w ramach *Planu działań*. | FBC: Koszty poszczególnych przedsięwzięć muszą być ujęte w Planie działania inaczej, biorąc pod uwagę kolejny akapit, nie znajdą one źródeł finansowania, które muszą być ujęte w planach budżetowych na kolejne lata. W najlepszym przypadku oznacza to roczne opóźnienia (od czasu ustalenia wielkości i struktury kosztów do czasu ujęcia w budżecie danej jednostki i jego akceptacji) | **Uwaga nieuwzględniona**  Uchwała Rady Ministrów nie może nakładać zobowiązań finansowych, gdyż może to nastąpić jedynie w drodze ustawy.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. |  |
|  | FBC | Uwaga o Finansowanie (p 11) | Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Strategii Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej, w miarę zaistnienia takich możliwości. | FBC: Taki zapis znacząco podnosi ryzyko, że zadania nie znajdą finansowania lub ujęte zostaną zadania niskokosztowe, które w niewielkim stopniu przyczynią się do osiągnięcia celów strategii. Najważniejsze zadania powinny znaleźć się bezpośrednio w Strategii. | **Uwaga nieuwzględniona**  Uchwała Rady Ministrów nie może nakładać zobowiązań finansowych, gdyż może to nastąpić jedynie w drodze ustawy.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. |  |
|  | IGG | Uwaga o cel szczegółowy 1.4 (p 5.4) | Ponadto, rząd będzie wspierał te podmioty w reagowaniu na incydenty poważne, **szczególnie w przypadku wystąpienia incydentów ponadsektorowych.** | IGG proponuje zamienić na zwrot: „**istotne, krytyczne**”.  W ustawie o KSC przewidziane zostały definicje incydentów poważnych, istotnych, krytycznych. Posłużenie się tymi definicjami wraz z postanowieniami aktów wykonawczych ustawy dają możliwość w miarę obiektywnej oceny skutków incydentu. Tym samym rekomendujemy aby w dokumentach o charakterze strategicznym posługiwać się pojęciami ustawowymi, a nie wprowadzać kolejną kategoryzację incydentów – incydenty ponadsektorowe. W takim przypadku powstanie potrzeba wyjaśnienia i wprowadzenia progów do ustalenia czym i kiedy incydent ma charakter ponadsektorowy. | **Uwaga uwzględniona** |  |
|  | IGG | Uwaga o cel szczegółowy 4.1 (p 8.1) |  | IGG: Rekomendujemy nadać priorytet działaniom opisanym w akapicie 2 rozdziału 8.1, w szczególności organizacji szkoleń dla organów ścigania i wymiaru sprawiedliwości | **Uwaga nieuwzględniona**  Wszystkie opisane kierunki interwencji rządu są priorytetowe. |  |
|  | IGG | Uwaga o cel szczegółowy 2.1 (p 6.1) |  | IGG: Rekomendujemy w rozdziale 6.1 uwzględnić zalecenia, dobre praktyki dla urządzeń IoT | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty. |  |
|  | KIGEiT | Uwaga o treść Wstępu (p 1) |  | KIGEiT: Proponujemy wprowadzenie odnośnika do infrastruktury krytycznej już we wprowadzeniu. | **Uwaga nieuwzględniona**  Jest to strategia cyberbezpieczeństwa, w której wielokrotnie pojawia się kwestia infrastruktury krytycznej, w tym kierunki działań związane z zapewnieniem interoperacyjności obu systemów. |  |
|  | KIGEiT | Uwaga o przypis we Wstępie (p 1) | Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne **i elektroniczne**, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.2), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – art. 1 ust. 1b Ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222 z 2011 r., poz. 1323). | KIGEiT proponuje dodać zwrot: „**i elektroniczne**” | **Uwaga nieuwzględniona**  Jest to definicja prawna. |  |
|  | KIGEiT | Uwaga o Kontekst Strategiczny (p 2) | Podejmując działania mające na celu wdrożenie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, rząd będzie w pełni **respektować** prawo do prywatności | KIGEiT proponuje zamienić na zwrot: „gwarantował”.  Zwracamy uwagę, że Państwo powinno nie tylko respektować, ale powinno gwarantować prawo do prywatności. | **Uwaga uwzględniona** |  |
|  | KIGEiT | Uwaga o treść Wizji (p 4.1) | Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych, prowadzenie badań naukowych, tak aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze **wsparcia/utrzymania sieci,** oprogramowania, urządzeń i usług **cyfrowych**. | KIGEiT proponuje dodanie zwrotu: „**wsparcia/utrzymania sieci**”  Oraz usunięcie zwrotu: „**cyfrowych**”  Wizja powinna uwzględniać również fakt, że zagrożenia wynikające z działalności kryminalnej mają zasadniczo różny charakter, skalę i poziom zaawansowania technologicznego od zagrożeń wynikających z ataków dywersyjnych i militarnych przeprowadzanych przez jednostki organizacyjne korzystające ze wsparcia technologicznego, finansowego i ochrony prawnej państwa. To oznacza, że te typy zagrożeń powinny być uwzględnione odrębnie zarówno w Krajowym Systemie Cyberbezpieczeństwa jak i w ramach zmian, jakich wymaga dyrektywa NIS. | **Uwaga nieuwzględniona**  Uzasadnienie nie odnosi się do propozycji zmiany zapisu. |  |
|  | KIGEiT | Uwaga o Cele szczegółowe (p 4.3) | **Cel szczegółowy 2.** Stymulowanie podniesienia poziomu odporności **sieci i systemów teleinformatycznych** administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zwalczania skutków incydentów. | KIGEiT proponuje zamienić zwrot: „**sieci i systemów informacyjnych**” na „**cyberprzestrzeni**” | **Uwaga nieuwzględniona**  Używamy terminologii ustawowej. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.1 (p 5.1) | Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi publicznych chmur obliczeniowych | KIGEiT proponuje dodanie zwrotu: „**publicznych**” | **Uwaga nieuwzględniona**  Nie ograniczamy się do chmur tylko publicznych. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.1 (p 5.1) | narzędzi podwójnego zastosowania do prowadzenia działań **defensywno-ofensywnych** w cyberprzestrzeni. | KIGEiT proponuje zamienić zwrot: „**defensywno-ofensywnych**” na „**defensywnych i ofensywnych**”  Sugerujemy, że legislacja w dziedzinie narzędzi podwójnego zastosowania powinna odbyć się na poziomie ogólnoeuropejskim (tak jak na poziomie europejskim regulowany jest eksport dóbr podwójnego zastosowania). Legislacja zagrożeń o charakterze militarnym i dywersyjnym powinna być spójna w ramach systemu cyberobrony NATO. | **Uwaga nieuwzględniona**  Obszar cyberbezpieczeństwa militarnego jest do decyzji MON. | **.** |
|  | KIGEiT | Uwaga o cel szczegółowy 1.1 (p 5.1) | Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie **okresowe** monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. | KIGEiT proponuje zamienić zwrot: „**okresowe**” na „**ciągłe**” | **Uwaga uwzględniona** |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.1 (p 5.1) | Organy właściwe, odpowiedzialne za sprawowanie nadzoru **w zakresie systemów teleinformatycznych** w sektorach w których świadczone są usługi kluczowe i usługi cyfrowe, będą prowadziły działania mające wspierać operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług. Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne, a także udostępniać narzędzia i wiedzę dotyczącą najlepszych praktyk sektorowych i ponadsektorowych podnoszących cyberbezpieczeństwo. | KIGEiT proponuje zamienić zwrot: „**w zakresie systemów teleinformatycznych**” na „**nad bezpieczeństwem cyberprzestrzeni**” | **Uwaga nieuwzględniona**  Z definicji: „Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne” |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.2 (p 5.2) | Organy właściwe, odpowiedzialne za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach w których świadczone są usługi kluczowe i usługi cyfrowe, będą prowadziły działania mające wspierać operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług. Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne, a także udostępniać narzędzia i wiedzę dotyczącą najlepszych praktyk sektorowych i ponadsektorowych podnoszących cyberbezpieczeństwo. | KIGEiT: Do tego akapitu nasuwa się pytanie o procedurę w jakiej organy te będą wyznaczone? Ponadto sugerujemy wypracowanie definicji/katalogu usług kluczowych. | **Uwaga nieuwzględniona**  Wszystko to już jest określone w ustawie o ksc. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.2 (p 5.2) | przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji **wykorzystujących technologie mikroelektroniczne** oraz korzystania z bezpiecznych systemów mobilnych. | KIGEiT proponuje dodać zwrot: „**wykorzystujących technologie mikroelektroniczne**” | **Uwaga nieuwzględniona**  W tym punkcie nie chodzi o technologie mikroelektroniczne. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.2 (p 5.2) | Standaryzacja i wymagania cyberbezpieczeństwa, opracowane i wykorzystywane przez administrację publiczną w ramach Narodowych Standardów Cyberbezpieczeństwa, powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli. | KIGEiT: W tym miejscu pojawia się pytanie, czy sektor prywatny automatycznie przyjmie/zaakceptuje standardy wprowadzone przez administrację publiczną? Opracowane standardy mogą stać się obligatoryjne tylko wtedy, gdy zostaną wprowadzone jako specyfikacje techniczne poprzez odpowiednie rozporządzenia. To wymaga również postawienia pytania o delegację ustawową do takich rozporządzeń i ich spójność w ramach systemu prawnego UE. | **Uwaga nieuwzględniona**  Sektor prywatny będzie zachęcany do stosowania NSC. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.3 (p 5.3) | W celu usprawnienia zarządzania bezpieczeństwem, prowadzone będą działania mające na celu wymianę informacji i uzgadnianie reakcji, tak na poziomie strategicznym jak i poziomie operacyjnym, w szczególności pomiędzy **sferą cywilną i sferą wojskową**. | KIGEiT proponuje zamienić zwrot: „**sferą cywilną i sferą wojskową**” na „**podmiotami sfery cywilnej, policją i służbami przeciwdziałającymi przestępczości oraz służbami odpowiadającymi za bezpieczeństwo wewnętrzne i obronność**” | **Uwaga nieuwzględniona**  Użyto terminologii z ustawy o działach administracji rządowej. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.3 (p 5.3) | technologie wymiany informacji, **technologie mikroelektroniczne,** uwzględniające konieczność wysokiej mobilności. | KIGEiT proponuje dodanie zwrotu: „**technologie mikroelektroniczne,**” | **Uwaga nieuwzględniona**  W tym punkcie nie chodzi o technologie mikroelektroniczne. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.3 (p 5.3) | System ten będzie wykorzystywany w różnych stanach nadzwyczajnych oraz stanach **podwyższonej** gotowości obronnej państwa. | KIGEiT proponuje dodanie zwrotu: „**podwyższonej**” | **Uwaga nieuwzględniona**  Do decyzji MON. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.4 (p 5.4) | Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, **w tym rozwiązań systemowych mających na celu podnoszenie bezpieczeństwa sprzętowych mikroelektronicznych komponentów systemów teleinformatycznych** będzie traktowane przez Radę Ministrów | KIGEiT proponuje dodać: „**w tym rozwiązań systemowych mających na celu podnoszenie bezpieczeństwa sprzętowych mikroelektronicznych komponentów systemów teleinformatycznych**” | **Uwaga nieuwzględniona**  W tym punkcie nie chodzi o technologie mikroelektroniczne. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 1.5 (p 5.5) | p. 5.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym | KIGEiT: W opinii KIGEiT jest to bardzo ważny punkt, dlatego w miarę możliwości postulujemy o jak najszybsze (jeszcze przed 2020) wypracowanie takiej metodyki i narzędzi. | **Wyjaśnienie:**  Opracowanie takiej metodyki jest obecnie realizowane zgodnie z zapisanym harmonogramem. | **.** |
|  | KIGEiT | Uwaga o cel szczegółowy 1.6 (p 5.6) | a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych **wykorzystujących bezpieczne krajowe rozwiązania mikroelektroniczne, oraz zapewnienie „łańcucha zaufania”** | KIGEiT sugeruje dodanie: **wykorzystujących bezpieczne krajowe rozwiązania mikroelektroniczne, oraz zapewnienie „łańcucha zaufania”** | **Uwaga nieuwzględniona**.  Zbyt wyszczególnione. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.1 (p 6.1) | Wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, **instytutach Sieci Badawczej Łukasiewicz** | KIGEiT proponuje dodać: „**instytutach Sieci Badawczej Łukasiewicz**” | **Uwaga nieuwzględniona**  Instytuty Sieci Badawczej Łukasiewicz też są instytutami badawczymi. Wyróżnienie niepotrzebne. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.1 (p 6.1) | opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm **i** standardów | KIGEiT proponuje zamienić zwrot: „**i**” na „**do**” | **Uwaga nieuwzględniona**  Nie chodzi o przekładanie norm do standardów, tylko ich tłumaczenie i przyjmowanie do systemu polskich norm. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.1 (p 6.1) | Wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, a także w zainteresowanych podmiotach publicznych i prywatnych, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm i standardów **na konkretne rekomendacje w zakresie** ich wdrażania. | KIGEiT proponuje zamienić: „**na konkretne rekomendacje w zakresie**” na „**definiujących zakres**” | **Uwaga nieuwzględniona**  Zmiana niezgodna z intencją pierwotnego zapisu. Proszę o uzasadnienie zmiany. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.1 (p 6.1) |  | KIGEiT: Ponadto dla systemów/produktów dla których istnieją odpowiednie normy międzynarodowe powinny być one bezpośrednio przyjęte poprzez ich umieszczenie w odpowiednich standardach (specyfikacjach technicznych). Sugerujemy zatem odpowiednią zmianę zapisu wskazującą, że:  PKN we współpracy z ośrodkami akademickimi (…) powinien skatalogować istniejące normy międzynarodowe dla poszczególnych kategorii oraz przyjąć konkretne rekomendacje w zakresie ich wdrażania. | **Uwaga nieuwzględniona**  PKN na bieżąco nad tym pracuje w ramach zwykłej działalności. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.1 (p 6.1) | dotyczących w szczególności bezpieczeństwa:   1. aplikacji, 2. urządzeń mobilnych, 3. stacji roboczych, 4. serwerów i sieci, 5. modeli chmur obliczeniowych. 6. **wsparcia i utrzymania sieci/systemów teleinformatycznych** | KIGEiT proponuje dodać pkt 6 do listy:  **6) wsparcia i utrzymania sieci/systemów teleinformatycznych** | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.2 (p 6.2) |  | KIGEiT: Proponujemy dodać paragraf o konieczności weryfikowania poziomu zaufania sprzętu przeznaczonego do infrastruktury, uwzględniając jego podatność na cyberataki. | **Uwaga nieuwzględniona**  Jest to już zawarte w punkcie.  „Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług).” |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.2 (p 6.2) | Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów **i systemów** (w szczególności oprogramowania, urządzeń i usług). | KIGEiT proponuje dodać zwrot: „**i systemów**” | **Uwaga nieuwzględniona**  Systemy zawierają się w poszczególnych komponentach. Systemy zarządzania nie są objęte tym zapisem. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 2.2 (p 6.2) | Efektem tych działań będzie uzyskanie na poziomie krajowym zdolności do wspierania **polskich** producentów, którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE. | KIGEiT proponuje usunąć zwrot: „**polskich**” | **Uwaga nieuwzględniona**  Zdanie bez tego słowa nie ma sensu. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju **działających w Polsce** przedsiębiorstw, ośrodków naukowo-badawczych | KIGEiT proponuje dodać: „**działających w Polsce**” | **Uwaga nieuwzględniona**  Niepotrzebnie dodane słowo. |  |
|  | KIGEiT | Uwaga o cel szczegółowy 3.1 (p 7.1) | Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, **projektowania i wytwarzania mikroelektronicznych przyrządów półprzewodnikowych w tym bezpiecznych układów scalonych,** urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność. | KIGEiT proponuje dodać: „**projektowania i wytwarzania mikroelektronicznych przyrządów półprzewodnikowych w tym bezpiecznych układów scalonych,**” | **Uwaga nieuwzględniona**  W tym punkcie nie chodzi o technologie mikroelektroniczne. |  |
|  | KIGEiT | Uwaga o dodanie punktu 7.5 |  | KIGEiT proponuje rozważenie włączenia nowego elementu strategii jako punkt 7.5. skupionego na poprawie cyberbezpieczeństwa sektora Public Safety (bezpieczeństwa publicznego). | **Uwaga nieuwzględniona**  Uwaga wymaga dodatkowych wyjaśnień lub propozycji zapisów. Do wyjaśnienia na konferencji uzgodnieniowej. |  |
|  | SKOK | Uwaga ogólna | W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym ( w tym działań o charakterze hybrydowym), ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych. Zwiększenie efektywności czynności procesowych i operacyjnych wymaga podjęcia i poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego i ubezpieczeniowego. Niezbędne jest także zapewnienie, ciągłej wymiany informacji o zagrożeniach i podatnościach zarówno na poziomie krajowym, jak i międzynarodowym | SKOK: Wyrażając poparcie dla tak sformułowanych celów pragnę zgłosić gotowość Kasy Krajowej do udziału  zarówno w planowanej konferencji uzgodnieniowej, jak i w dalszych pracach, w tym legislacyjnych, zapowiedzianych konsultowanym dokumentem.   Pragnę jednocześnie wskazać, że zarówno spółdzielcze kasy oszczędnościowo-kredytowe, jak i zrzeszająca te podmioty Kasa Krajowa – mają ustawowy obowiązek przeciwdziałania wykorzystaniu swojej działalności dla celów mających związek z przestępstwem, o którym mowa w art. 165a lub art. 299 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2018 r. poz. 1600 i 2077, jak również, że Załącznik do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa obejmuje sektor spółdzielczych kas oszczędnościowo-kredytowych. | **Uwaga częściowo uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga ogólna |  | Instytut: Uważamy, że Strategia powinna być bardziej precyzyjna i przekonywująca w zakresie strategicznych celów długofalowych, które mają być wynikiem jej wdrożenia. Projekt w aktualnym kształcie w dużej części (nie w całości) stanowi zbiór obszarów, które z reguły wskazuje się w tego typu dokumentach. W dynamicznie zmieniającym się krajobrazie cyfrowego świata, wynikającym zarówno ze zmian geopolitycznych jak i wykładniczego postępu technologicznego, jej treść powinna być wynikiem diagnozy aktualnego stanu cyberbezpieczeństwa i pogłębionej analizy *stricte* dotyczącej zarówno uwarunkowań wewnętrznych i zewnętrznych Polski, jak i przewidywanych w tejże domenie trendów. Cyberbezpieczeństwo nie jest celem samym w sobie. Powinno być osiągane dla realizacji innych celów narodowych | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga ogólna |  | Instytut: Dokument jest miejscami niespójny i chaotyczny, na przykład nie tłumaczy relacji pomiędzy postulowanymi działaniami, mimo, że te same wątki pojawiają się w różnych odsłonach w różnych częściach tekstu. | **Uwaga nieuwzględniona**  Prosimy o wskazanie niespójnych fragmentów. |  |
|  | Instytut Kościuszki | Uwaga ogólna |  | Instytut: Daje się również zauważyć niespójność definicyjną i pojęciową np. „systemy informacyjne” vs „środki komunikacji elektronicznej” vs. „systemy teleinformatyczne”. Sugeruje się, aby Strategia posługiwała się przede wszystkim pojęciami zawartymi w ustawie o krajowym systemie cyberbezpieczeństwa, a jednocześnie zawierała postulat podjęcia niezbędnych działań legislacyjnych w celu ujednolicenia kluczowych pojęć i definicji zawartych w takich aktach prawnych, jak ustawa o krajowym systemie cyberbezpieczeństwa, ustawa o stanie wojennym i kompetencjach Naczelnego Dowódcy Sił Zbrojnych, ustawa o Policji, ustawa o działaniach antyterrorystycznych | **Uwaga nieuwzględniona**  Pojęcie „systemy informacyjne” wynika z ustawy o krajowym systemie cyberbezpieczeństwa.  Termin system informacyjny jest ponadto pojęciem szerszym niż systemy teleinformatyczne.  Używamy w zależności od kontekstu. |  |
|  | Instytut Kościuszki | Uwaga ogólna | Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na celu podniesienie poziomu cyberbezpieczeństwa w RP. Poprzednie działania obejmowały wejście w życie ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa oraz przyjęcie przez rząd:  •w roku 2013 Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej  •w roku 2017 Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017 –2022.” | Instytut: Ponieważ dokument opisywany jest jako kontynuacja Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, przyjętych uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r., to należałoby w finalnej jego wersji zachować kontynuacje (lub wyjaśnić jej brak) wielu projektów i zadań, które w poprzednim dokumencie strategicznym, wskazywane były jako ważne i priorytetowe jak np. Cyber Park Enigma czy Złota Setka. Brak nawiązania do tych koncepcji oraz przedstawienia rezultatów dotychczasowych strategii i polityk oraz działań regulacyjnych sprawia bowiem wrażenie, że po stronie rządu brakuje zdeterminowanej ciągłości realizowania zadań przyjętych uprzednio jako strategiczne. Co z kolei może zostać odebrane jako brak długofalowego myślenia o cyberbezpieczeństwie i w konsekwencji negatywnie wpłynąć na percepcję przez interesariuszy woli realizacji celów i działań prezentowanych w projekcie nowej Strategii. | **Uwaga nieuwzględniona**  Strategia wpisuje się w kontynuacje poprzednich działań rządu RP, jednakże konkretne zapisy są efektem ich ewaluacji. |  |
|  | Instytut Kościuszki | Uwaga o Wstęp (p 1) | Rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Dynamiczny rozwój systemów informacyjnych, a także zwiększanie wydajności centrów przetwarzania danych, służą rozwojowi gospodarki narodowej, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych. Z wykorzystaniem technologii cyfrowych tworzących cyberprzestrzeń tworzone są i kształtowane relacje społeczne, a usługi w sieci Internet stały się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej. | Instytut: Dokument rozpoczyna się od wskazania, że to dostęp do informacji jest krytyczny dla wielu obszarów funkcjonowania państwa. Sprawia to wrażenie, że tak rozumiane jest sedno cyberbezpieczeństwa – zapewnianie dostępu do informacji i jej wykorzystania. Jednak wykorzystanie systemów teleinformatycznych jest dalece szersze i tym samym cyberbezpieczeństwo jest zadaniem znacznie bardziej wielowymiarowym. Tak też powinno być ujmowane w strategii. Należy wyjaśnić także jak rozumiane są systemy informacyjne. | **Uwaga nieuwzględniona**  Definicja systemów informacyjnych wynika z ustawy o KSC. Prosimy o wskazanie wielowymiarowości cyberbezpieczeństwa celem poprawy definicji. |  |
|  | Instytut Kościuszki | Uwaga o Wstęp (p 1) |  | Instytut: We wstępie do projektu Strategii nie nawiązano również do wymiaru obronnego, który szeroko obejmuje dokument w dalszej swojej części. Zatem dla zapewnienia spójności konieczne jest rozszerzenie opisu części Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo o te związane z uwarunkowaniami nowoczesnego pola walki, zarówno w zakresie świadomości sytuacyjnej (informacja), jak i zdolności obronnych i defensywnych (zależnych od sprawnie funkcjonujących sieci i systemów teleinformatycznych), a także odziaływaniem cyberprzestrzeni w sferze geopolitycznej. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. |  |
|  | Instytut Kościuszki | Uwaga o Wstęp (p 1) | Dynamiczny rozwój sieci i systemów informatycznych, służy rozwojowi gospodarki narodowej | Instytut: Uzasadnienia wymaga także uwzględnienie w początkowej, kluczowej dla strategii, części kwestii zwiększenia wydajności centrów przetwarzania danych – jest wiele innych elementów, które np. wpływają na rozwój gospodarki, a które można byłoby wskazać. | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty, tylko przykładowe wskazanie. |  |
|  | Instytut Kościuszki | Uwaga o Wstęp (p 1) | Ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, organów władzy publicznej, organów odpowiedzialnych za bezpieczeństwo narodowe, a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej | Instytut: W części tej należy wyjaśnić i doprecyzować czy krajowy system cyberbezpieczeństwa jest rzeczywiście rozumiany tak jak w tekście strategii czy jak w Ustawie o Krajowym Systemie Cyberbezpieczeństwa. Definicja ustawowa jest inna i nie pokrywa się z tymże zapisem, co wpływa na to czyim wyzwaniem jest ochrona systemów informacyjnych i przetwarzanych w nich informacji. | **Uwaga nieuwzględniona**  W opinii MC nie wymaga to doprecyzowania. |  |
|  | Instytut Kościuszki | Uwaga o Wstęp (p 1) | Współpraca ta odgrywa istotną rolę w reagowaniu na zwiększającą się liczbę incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, powodujących rosnące rokrocznie straty materialne i wizerunkowe. | Instytut: Pominięte zostały incydenty nie związane z działaniami nielegalnymi, np. zupełnie nieintencjonalne, które również bardzo mocno wpływają na cyberbezpieczeństwo. | **Uwaga nieuwzględniona**  Incydenty nieintencjonalne typu błędna konfiguracja czy błąd ludzki nie wymagają w takim samym stopniu współpracy. |  |
|  | Instytut Kościuszki | Uwaga o Kontekst strategiczny (p 2) | Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni, a także zwiększyć poziom ochrony informacji w systemach informacyjnych poprzez standaryzację zabezpieczeń | Instytut: Po pierwsze, należałoby założyć, że Strategia nie powinna mieć zamierzeń tylko jasno wskazywać cele. Po drugie, Strategia narodowa powinna dążyć do systemowego zapewnienia cyberbezpieczeństwa, gdzie podmioty, realizujące krytyczne funkcje, powinny być priorytetem, ale nie wyłączną grupą objętą działaniami. | **Uwaga częściowo uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga o Kontekst strategiczny (p 2) | Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni | Instytut: Realizacja Strategii, powinna również wpłynąć na zapewnienie suwerenności cyfrowej, powinno zostać to ujęte w definicji celu głównego. Na kwestię strategicznej autonomii zwracają uwagę także dokumenty strategiczne Unii Europejskiej. Strategia powinna wziąć pod uwagę, że dalsze pogłębianie zależności, od zewnętrznych dostawców technologii zwłaszcza z krajów nie należących do grona tzw. like-minded countries, oddala Polskę (i szerzej także Unię Europejską) od realizacji celu jakim jest jej suwerenność cyfrowa. Zatem strategicznym celem winno być także aktywizowanie rodzimych zasobów i „organiczny” oraz efektywny rozwój cyfrowej suwerenności.  Uważamy, że zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości jest środkiem do osiągnięcia celu – przeciwdziałania, zapobiegania, karania przestępczości - nie odwrotnie. | **Uwaga nieuwzględniona**  Konieczne jest doprecyzowanie intencji składającego uwagi oraz zaproponowanie konkretnych zapisów. |  |
|  | Instytut Kościuszki | Uwaga o Kontekst strategiczny (p 2) | Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 jest spójna z prowadzonymi działaniami dotyczącymi systemów teleinformatycznych operatorów infrastruktury krytycznej oraz działaniami mającymi na celu zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia cybernetycznych działań w przypadku zagrożenia bezpieczeństwa sieci i systemów teleinformatycznych. | Instytut: Konieczność doprecyzowania. Czy chodzi o spójność z NPOIK? W jakim zakresie jest spójna?  Dodatkowo, wzmacnianie zdolności SZRP postulujemy aby zostało ujęte jako immanentny cel strategii, a nie tylko je uwzględniało. Zresztą dalsza część dokumentu odnosi się bezpośrednio do sektora militarnego – choć naszym zdaniem powinna szerzej. Jednocześnie podkreślenia wymaga fakt, że potrzeba „zapewnienia Siłom Zbrojnym RP zdolności do prowadzenia działań militarnych w układzie krajowym sojuszniczym i koalicyjnym” nie powinna ograniczać się wyłącznie do przypadków „[...]zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych”. Posiadanie przez Siły Zbrojne niezakłóconego dostępu do niezawodnych systemów informacyjnych i łączności, w tym łączności utajonej, jest istotne zarówno w czasie pokoju, jak i kryzysu czy wojny. Wynika to choćby z potrzeby gromadzenia, przetwarzania i analizowania danych wywiadowczych (również w czasie pokoju) czy posiadania niezawodnych środków łączności podczas użycia Sił Zbrojnych również w innych celach niż prowadzenie działań obronnych (reagowanie kryzysowe, zwalczanie skutków klęsk żywiołowych, wsparcie działań służb ochrony porządku publicznego np. w trybie art. 18 ustawy o Policji czy udział w działaniach kontrterrorystycznych). | **Uwaga nieuwzględniona**  Obie ustawy: o ZK i o ksc są ze sobą spójne. Ponadto istotna jest rola RCB w obu systemach. |  |
|  | Instytut Kościuszki | Uwaga o Kontekst strategiczny (p 2) | Podejmując działania mające na celu wdrożenie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, rząd będzie w pełni respektował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa | Instytut: Fragment ten wymaga kategorycznego przeformułowania, tak aby nie pozostawiał miejsca na interpretację, iż rząd mógłby nie respektować tego prawa. | **Uwaga uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga o Zakres strategii (p 3) | Strategia uwzględnia, w szczególności[[9]](#footnote-9):   1. cele i priorytety państwa w zakresie cyberbezpieczeństwa, 2. podmioty zaangażowane we wdrażanie i realizację Strategii, 3. środki służące realizacji celów Strategii, 4. określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym 5. podejście do oceny ryzyka, 6. działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, 7. działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa,   Ponadto Strategia uwzględnia międzynarodową współpracę w zakresie cyberbezpieczeństwa. | Instytut: We fragmencie „określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym” konieczne jest określenie środków gotowości (…) wobec czego?  W punkcie 1 mówi się o celach i priorytetach Strategii, następnie w punkcie 6 wskazuje się działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, a w punkcie 7 działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa, oraz odrębnie wskazuje się, że „Ponadto Strategia uwzględnia międzynarodową współpracę w zakresie cyberbezpieczeństwa”. Czy oznacza to że punkt 6, 7 i dotyczący współpracy międzynarodowej nie mieści się w celach i priorytetach? | **Uwaga nieuwzględniona**  W opinii MC nie jest konieczne doprecyzowanie. |  |
|  | Instytut Kościuszki | Uwaga o Wizję (p 4.1) | Pomyślny rozwój Polski, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym i aktywność społeczna oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa są związane ze sprawnym i bezpiecznym działaniem systemów informacyjnych i środków komunikacji elektronicznej | Instytut: Konieczne jest wyjaśnienie jak rozumiany jest „pomyślny rozwój”.  Jak rozumiane są środki informacyjne, na jakiej zasadzie są one odrębne od komunikacji elektronicznej? Odpowiedź na te pytania jest konieczna do określenia, czy we fragmencie, a w konsekwencji całościowo w podejściu, nie występuje niekorzystne niezrozumienie. | **Uwag nieuwzględniona**  Nie ma konieczności definiowania pojęcia „pomyślny rozwój”.  We fragmencie nie ma zwrotu „środki informacyjne” tylko „systemy informacyjne” do którego terminu jest definicja w polskim ustawodawstwie |  |
|  | Instytut Kościuszki | Uwaga o Wizję (p 4.1) | Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych, prowadzenie badań naukowych, tak aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń i usług cyfrowych | Instytut: Wszystkie owe działania powinny być podejmowane po to aby zapewnić poziom cyberbezpieczeństwa adekwatny do ryzyk, a tym samym umożliwić realizację określonych celów państwa. Wskazanie wyłącznie trzech obszarów – aby zapewnić cyberbezpieczeństwo, wydaje się tu jednak niewystraczające, należy mieć na uwadze wiele innych działań. W takim kontekście należałoby także sprecyzować – o jakie, czyje oprogramowanie, urządzenia i usługi chodzi. | **Uwaga nieuwzględniona**  W opinii MC nie ma potrzeby doprecyzowania. |  |
|  | Instytut Kościuszki | Uwaga o Wizję (p 4.1) | Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz poprzez budowę zaufania pomiędzy poszczególnymi sektorami rynkowymi a administracją publiczną | Instytut: Zaufanie to podstawa, ale dokument musi mówić także o realnej współpracy. | **Uwaga nieuwzględniona**  Cel szczegółowy 3.2 |  |
|  | Instytut Kościuszki | Uwaga o Cel główny (p 4.2) | Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji | Instytut: Należałoby przemyśleć zredefiniowanie celu głównego, który naszym zdaniem został sformułowany zawężająco. Cyberbezpieczeństwo to nie tylko ochrona informacji, a budowanie odporności na cyberzagrożenia, owszem zawiera jej ochronę, ale także wiele innych elementów, których tutaj nie zdecydowano się wymienić (słowo „oraz” wskazuje, że ochrona informacji jest czymś obok cyberbezpieczeństwa). W ramach określania celu głównego należy uwzględnić zarówno ochronę informacji, ochronę infrastruktury umożliwiającej przetwarzanie informacji cyfrowych, jak i sam proces przetwarzania informacji cyfrowych obejmujący szereg podmiotów. Nie do przecenienia jest – podkreślana choćby w ustawie o działaniach antyterrorystycznych – kwestia ochrony infrastruktury krytycznej przed cyberzagrożeniami.  Podniesienie odporności jest kluczowe, ale nie można zapominać np. o przeciwdziałaniu incydentom. Po raz kolejny, zastosowanie detalicznego wyliczenia jest niepotrzebne przy określaniu celu głównego. Np. w wyliczeniu zdecydowano się na włączenie dobrych praktyk a nie np. rozwój badań naukowych. Można dać wiele innych przykładów. Ponadto np. samo promowanie wiedzy może być uznane za budowanie odporności.  W ramach wskazanego celu głównego wymieniono „promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.” – działanie takie stanowi środek do osiągnięcia celu, nie sam cel, jakim jest ochrona informacji oraz procesów opartych o narzędzia cyfrowe wykonywanych przez obywateli.    W związku z powyższym proponujemy poniższe brzmienie celu głównego „**Podniesienie poziomu odporności na cyberzagrożenia oraz zdolności reakcji na zmaterializowane zagrożenia w cyberprzestrzenie. Zwiększenie poziomu ochrony informacji, obiektów infrastruktury krytycznej, infrastruktury cyfrowej oraz procesów opartych na niej w sektorze publicznym, prywatnym oraz wśród samych obywateli.**” | **Uwaga nieuwzględniona**  Proponowany zapis jest niezgodny z intencją i zakresem Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cele szczegółowe (p 4.3) | **Cel szczegółowy 1.** Rozwój Krajowego Systemu Cyberbezpieczeństwa.  **Cel szczegółowy 2.** Stymulowanie podniesienia poziomu odporności sieci i systemów telein-formatycznych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zwalczania skutków incydentów.  **Cel szczegółowy 3.** Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyber-przestrzeni.  **Cel szczegółowy 4.** Budowanie świadomości i kompetencji społecznych w zakresie cyberbez-pieczeństwa  **Cel szczegółowy 5.** Aktywna rola RP na arenie międzynarodowej w obszarze cyberbezpie-czeństwa. | Instytut: W naszej ocenie cele szczegółowe są skonstruowane niespójnie. Np. Czy budowanie świadomości i kompetencji oraz aktywna rola RP na arenie międzynarodowej nie są traktowane jako takie, które zwiększają narodowy potencjał cyberbezpieczeństwa? Jeśli nawet nie, to czy budowanie potencjału nie powinno dotyczyć także dwóch elementów? Są one wyodrębnione od pkt. 3. | **Uwaga nieuwzględniona**  Cele szczegółowe są wydzielone także ze względów na różnicę w dobieraniu środków. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.1 (p 5.1) | Podstawą rozwoju Krajowego Systemu Cyberbezpieczeństwa jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system, w powiązaniu z innymi przepisami, w szczególności z ustawą o zarządzaniu kryzysowym, ustawą o ochronie informacji niejawnych, strategią bezpieczeństwa narodowego. Rezultatem dokonanej oceny może być konieczność przygotowania niezbędnych zmian przepisów usuwających bariery dla skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty. | Instytut: Ponownie chcielibyśmy zwrócić uwagę na nie w pełni adekwatne zawężenie – zmiany przepisów powinny dotyczyć eliminacji wszystkich brakujących, niewystarczająco, źle funkcjonujących elementów – nie tylko tych które dotyczą wymiany informacji czy reagowania na incydenty.  W ramach opisu celu szczegółowego 1, postulujemy, że celem ewaluacji przepisów dot. KSC oraz ich implementacji powinna być holistyczna ocena funkcjonowania systemu uwzględniająca możliwe zmiany przepisów mające na celu poprawę kluczowych aspektów jego działania, a więc nie tylko „skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty”. Należy znacznie rozszerzyć możliwy katalog zmian, lub wręcz otworzyć go bez zawężania do określonego wycinka KSC. | **Uwaga nieuwzględniona**  Strategia nie zamyka możliwości zmian prawnych w innych obszarach, a jedynie wskazuje priorytetowe obszary. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.1 (p 5.1) | Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej w sprawie zmiany przepisów samej Dyrektywy NIS, tak aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych | Instytut: W innych miejscach nie jest tak szczegółowo określane jak poszczególne działania będą realizowane. Autorzy dokumentu powinni utrzymać spójność w sprawie decyzji o charakterze dokumentu: ogólnym lub bardziej szczegółowym. | **Uwaga nieuwzględniona**  Punkt ten nazywa się „wdrożenie i ocena funkcjonowania przepisów o KSC”, uwagi te odnoszą się do wyzwań jakie stoją przed polską w tej kwestii. Wymienione usługi chmur obliczeniowych sa tylko przykładem takich wyzwań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.1 (p 5.1) | W ramach prac legislacyjnych minister właściwy do spraw informatyzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych i szczególnych, które dotyczą omawianej problematyki oraz regulacji prawnych, które mogą mieć oddziaływanie na inne obszary, na przykład na ochronę danych osobowych, czy infrastrukturę krytyczną w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej | Instytut: Akapit wcześniej autorzy wskazywali, że za zmiany prawne odpowiadają poszczególni ministrowie. Tu natomiast wskazuje się, że prace sektorowe wykonuje min. ds. cyfryzacji. Wymaga to doprecyzowania. | **Uwaga nieuwzględniona**  Zaznaczone jest, że „we współpracy z innymi resortami”.  Minister właściwy ds. informatyzacji jest koordynatorem wdrażania Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.1 (p 5.1) | Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk **tam** zachodzących i inicjowanie ewentualnych zmian w przepisach prawa | Instytut: Wyjaśnienia wymaga słowo „**tam**” | **Uwaga uwzględniona**  Usunąć zwrot „tam zachodzących” – zbędne powtórzenie. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.1 (p 5.1) | Propozycje kierunków zmian i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa | Instytut: Należy doprecyzować zmian czego. Dodatkowo postuluje się otwarcie możliwości konsultacji dla innych interesariuszy. Ponadto, zapis ten stanowi częściowe powtórzenie Art. 64 i 65 ustawy o krajowym systemie cyberbezpieczeństwa. Czy postulowane są zmiany w składzie albo zadaniach Kolegium? | **Uwaga nieuwzględniona**  Zapis ma na celu wskazanie roli Kolegium w realizacji Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.2 (p 5.2) | Niezbędne jest wdrożenie systemowych rozwiązań pozwalających na wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do zagrożeń i incydentów | Instytut: Uważamy, że systemowe rozwiązania związane ze wsparciem powinny dotykać także innych obszarów, stąd takie zawężenie jest nieuzasadnione | **Uwaga nieuwzględniona**  Nie jest to zawężenie, a wskazanie priorytetów. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.2 (p 5.2) | Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych | Instytut: Odpowiedz na pytania, o które postulujemy rozszerzyć cytowany fragment dotyczą tego w jakim zakresie będą przygotowane rekomendacje, kto będzie je realizował, czy przewidywane jest wsparcie czy wyłącznie rekomendacje? | **Uwaga nieuwzględniona**  Konkretne działania wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.4 (p 5.4) | Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa | Instytut: Z punktu widzenia bezpieczeństwa IT/OT w kontekście procesów przemysłowych, funkcjonowania infrastruktury krytycznej, rzeczywiście bezpieczeństwo 5G jest kluczowe. Nie jest to jednak jedyne działanie które powinno być podejmowane. Jest jeszcze wiele niewymienionych działań, które winny być podjęte, a nie zostały szczegółowo opisane, co niniejszym postulujemy. | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.4 (p 5.4) | W pierwszej kolejności zostanie zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten przebiegał będzie we współpracy ze wszystkimi sektorami. Wykorzystując mechanizmy przewidziane prawem rekomendowane będą minimalne wymagania w zakresie cyberbezpieczeństwa ze szczególnym uwzględnianiem zarządzania ciągłością działania | Instytut: W tym fragmencie sugerujemy doprecyzować i wyjaśnić następujące kwestie. Np. czego dotyczyć mają wymagania? Kogo mają dotyczyć? Jak wiąże się to z istniejącymi już obowiązkami wynikającymi z innych dokumentów np. Ustawy o KSC, jak wiąże się to z zapowiadanymi Narodowymi Standardami etc. Ponadto, wdrażanie minimalnych wymagań będzie wymagało stosownych mechanizmów prawnych. O ile dla podmiotów sektora administracji publicznej czy państwowych jednostek organizacyjnych nie będzie to stanowiło problemu, o tyle „narzucanie” standardów podmiotom sektora prywatnego może zostać uznane za niedozwoloną ingerencję w swobodę prowadzenia działalności. Rozważyć zatem należy stosowny mechanizm implementacji standardów, np. poprzez wprowadzenie wymogu udokumentowania spełnienia standardów dla podmiotów ubiegających się o udzielenie zamówień publicznych w zakresie usług kluczowych i cyfrowych świadczonych na rzecz podmiotów sektora publicznego. | **Uwaga nieuwzględniona**  Minimalne wymagania w zakresie cyberbezpieczeństwa będą procedowane odrębnie.  W zależności od podstawy prawnej będą one obowiązkowe (por. KRI) lub dobrowolne (Narodowe Standardy Cyberbezpieczeństwa). |  |
|  |  | Uwaga o cel szczegółowy 1.5 (p 5.5) | Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka | Instytut: W kontekście metodyki szacowania ryzyka na poziomie krajowym należy wskazać kto będzie odpowiedzialny za wdrożenie jej oraz w jakich celach, poza raportami o zagrożeniach bezpieczeństwa narodowego, będzie ona wykorzystywana. Postulujemy wykorzystanie szacowania ryzyka na poziomie krajowym jako podstawy do konkretnej alokacji środków publicznych na określone działania związane z cyberbezpieczeństwem. W praktyce może oznaczać to włączenie takiej analizy jako jednego z kroków w ramach fazy koncepcyjnej tworzenia Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Metodyka jest opracowywana w ramach projektu NPC. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.6 (p 5.6) | W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym ( w tym działań o charakterze hybrydowym), ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych | Instytut: Wyrażenie „zdarzeń o charakterze terrorystycznym (w tym działań o charakterze hybrydowym) zdaje się sugerować, że działania hybrydowe stanowią wycinek działań terrorystycznych, podczas gdy to właśnie działania hybrydowe stanowią znacznie szerszą kategorię zagrożeń, wśród których jedną z metod oddziaływania mogą być ataki terrorystyczne. Nie należy jednakże zapominać, że podstawowym narzędziem oddziaływania w działaniach hybrydowych są środki komunikacji elektronicznej, w tym media społecznościowe. Zatem zwiększanie cyberbezpieczeństwa powinno również odbywać się poprzez budowanie zdolności do przeciwdziałania propagandzie i dezinformacji rozpowszechnianych przy użyciu środków komunikacji elektronicznej, przy czym nie należy zapominać, że rozpowszechnianie propagandy czy dezinformacji nie zawsze będzie wiązało się z popełnieniem czynu karalnego. Działania o charakterze hybrydowym, nie dotyczą wyłącznie działań terrorystycznych. Wskazana grupa podmiotów, choć kluczowa i priorytetowa w zakresie otrzymywania wsparcia, nie jest grupą, na której owe działania powinny być zakończone. Jeśli celem jest skuteczna walka z cyberprzestępczością (jak mówi tytuł) działania te powinny być określone znacznie szerzej.  Współpraca i koordynacja jest ważna. Ale równie istotne np. zapewnianie dostępu do potrzebnych technologii. To podstawa bez które nie uda się zrealizować współpracy.  Niezrozumiałym jest wtrącenie „którymi kierują się sprawcy przestępstw”.  Nieuzasadnionym zawężeniem jest również uznanie za kluczowe zabezpieczenia dowodów cyfrowych, jest to oczywiście bardzo ważną kwestią, ale informatyka śledcza niesie wiele innych działań, które są równie istotne i powinny być podejmowane. Dodatkowo działania nie będą skuteczne np. jeśli nie zadba się o implementację mechanizmów, które pozwolą uzyskać dostęp do dowodów cyfrowych. Z tego względu proponujemy przeformułowanie tego zapisu projektu Strategii. Podobnie, jak w przypadku zwalczania internetowej propagandy i dezinformacji, dla pozyskania dowodów cyfrowych niezbędne będzie ustanowienie stosownych mechanizmów współpracy i wymiany informacji z operatorami usług cyfrowych | **Uwaga częściowo uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.6 (p 5.6) | Biorąc pod uwagę dużą dynamikę przestępstwa w cyberprzestrzeni (…) | Instytut: Sformułowanie wydaje się, że zostało omyłkowo zapisane niepoprawnie. | **Uwaga uwzględniona**  Zmiana zapisu |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 1.6 (p 5.6) | Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych | Instytut: Postulujemy uzupełnienie tego fragmentu o element wspierania działalności, kompetencji np. wymiaru sprawiedliwości - równie kluczowego dla przeciwdziałania cyberprzestępczości. | **Uwaga nieuwzględniona**  Konkretne działania wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej, która już w bliskiej przyszłości rozpocznie korzystanie z nowych form przetwarzania i przechowywania informacji m.in. poprzez wykorzystywanie usług chmury obliczeniowej, niezbędne będzie przygotowanie zaleceń i promowanie dobrych praktyk podnoszących odporność na potencjalne cyberzagrożenia | Instytut: Konieczne jest zaprezentowanie definicji „infrastruktury przetwarzania systemów IT | **Uwaga nieuwzględniona**  Chodzi o przetwarzanie danych. Dalsze definiowanie wydaje się niezasadne i zawężające. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 2.2 (p 6.2) | Zapewnienie cyberbezpieczeństwa wymaga, stosowania zabezpieczeń organizacyjnych i technicznych na wszystkich etapach cyklu życia systemów teleinformatycznych. Działania te składają się na tak zwany bezpieczny łańcuch dostaw budowy, który obejmuje projektowanie, budowę, wdrażanie, eksploatację oraz wycofywanie z użycia. Pod pojęciem łańcucha dostaw należy rozumieć system, na który składają się podsystemy produkcji, dystrybucji, transportu, magazynowania oraz recyklingu komponentów systemów teleinformatycznych, jak również ich instalacja, uruchomienie, bieżące utrzymanie, serwisowanie oraz naprawy. | Instytut: Zapewnienie cyberbezpieczeństwa może wymagać także innych działań np. regulacyjnych.    Strategia czasem odnosi się do systemów teleinformatycznych, czasem do informacyjnych – należy to wyjaśnić i możliwie ujednolicić.  Niezrozumiałe sformułowanie „łańcuch dostaw budowy” – wydaje się, że słowo „budowy” zostało w tekście umieszczone omyłkowo.  Zdanie wyjaśnia czym jest łańcuch dostaw, a kolejne zdanie prezentuje inne wyjaśnienie – należy to ujednolicić. | **Uwaga częściowo uwzględniona**  Pojęcie „systemy informacyjne” wynika z ustawy o krajowym systemie cyberbezpieczeństwa.  Termin system informacyjny jest ponadto pojęciem szerszym niż systemy teleinformatyczne.  Używamy w zależności od kontekstu.  Słowo „budowy” należy usunąć. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 2.2 (p 6.2) | Ważnym elementem zapewnienia jakości i bezpieczeństwa w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług) | Instytut: Pojawia się pytanie, czy autorzy rozumieją usługi jako podkategorię produktów? | **Uwaga nieuwzględniona**  Jest to podejście zgodne z tym wyrażonym w rozporządzeniu UE 2019/881 (Cyber Security Act). |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 2.2 (p 6.2) | Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa, co umożliwi Polsce uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa | Instytut: Należy zwrócić uwagę, że sama certyfikacja, choć ważna, nie jest działaniem wystarczającym do uzyskania owego statusu. | **Wyjaśnienie**  MC zdaje sobie z tego sprawę. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 2.3 (p 6.3) |  | Instytut: W kwestii testów i audytów bezpieczeństwa – postulat doprecyzowania przepisów art. 269b Kodeksu karnego w taki sposób, aby doprowadzić do jego pełnej zgodności z Art. 6 konwencji Rady Europy o cyberprzestępczości (narzędzia przystosowane przede wszystkim do popełniania przestępstw komputerowych, zamiar przestępczy), a także penalizować nie tylko posiadanie i obrót, ale i użycie narzędzi hakerskich w celu przestępczym, przy wyłączeniu odpowiedzialności za wytwarzanie, obrót, udostępnianie etc. takich narzędzi na potrzeby służb ochrony porządku publicznego, a także ich użycie wyłącznie w celu sprawdzenia zabezpieczeń systemu teleinformatycznego. | **Wyjaśnienie**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel (…) stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa | Instytut: Biorąc pod uwagę charakterystykę rynku cyberbezpieczeństwa w Europie (w tym w Polsce), a także fakt, że start-upy stanowią określoną kategorię przedsiębiorstw, proponujemy następujące przeformułowanie zapisu:  „Rząd Polski stawia sobie za cel (…) **stwarzanie warunków dla rozwoju przedsiębiorstw, w tym szczególnie MŚP oraz start-upów, a także ośrodków naukowo-badawczych, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa**”. | **Uwaga uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i *start-upów*, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność | Instytut: Należy wyjaśnić relację między tym zapisem, a kwestiami cyberbezpieczeństwa. Czy cyberbezpieczeństwo jest rozumiane jako warunek budowania wszystkich rozwiązań i na tej zasadzie przyczynia się do konkurencyjności, czy sama branża cyberbezpieczeństwa ma przyczynić się do wzrostu konkurencyjności? | **Wyjaśnienie**  Zasada security by design to koncepcja, która powinna być stosowana szeroko, także poza tzw. branżą security. Jednocześnie bezpieczeństwo rozwiązań pozytywnie wpływa na konkurecyjność. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.1 (p 7.1) | Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w kształceniu w zakresie szeroko rozumianego cyberbezpieczeństwa . Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych | Instytut: Naszym zdaniem nie jasne jak rozumie się realizację tego zapisu, czy postuluje się ażeby ośrodki naukowe same powinny być bezpieczne, czy chodzi o postulat nabywania umiejętności do kształcenia w tym zakresie. Zdanie następne sugeruje drugie rozumienie, ale sugerujemy sprecyzowanie tego zapisu.  Dodatkowo proponujemy aby postulat ten znajdował się w części strategii dotyczącej rozbudowy potencjału ludzkiego. | **Uwaga nieuwzględniona**  Chodzi o kształcenie. Warto jednak wskazać, że uczelnie są też zobowiązane do stosowania ustawy o KSC. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.1 (p 7.1) | W celu wyrównania szans polskich przedsiębiorców na globalnym rynku rząd będzie wspierać rozwój polskiego biznesu w uzyskiwaniu zdolności cyfrowych oraz zapewniał pomoc w ubieganiu się o środki na rozwój innowacyjnych rozwiązań, a także doradztwo w dostępie do nowych rynków jak i pomoc w nawiązaniu współpracy z innymi przedsiębiorcami | Instytut: Należy doprecyzować czy wsparcie dotyczy obszaru cyberbezpieczeństwa czy transformacji cyfrowej w szerokim rozumieniu? | **Uwaga nieuwzględniona**  Poza zakresem Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.2 (p 7.2) | Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga wspólnego wysiłku sektora prywatnego, publicznego oraz obywateli. Rząd będzie kontynuował budowanie efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za cyberbezpieczeństwo. Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie inicjowania i prowadzenia projektów w dziedzinie cyberbezpieczeństwa | Instytut: Doskonalenie potencjału powinno także obejmować realizację projektów. | **Uwaga nieuwzględniona**  Zapis niepotrzebny. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.2 (p 7.2) | Realizując nową wizję rozwoju kraju i wspierając innowacyjność polskiej gospodarki, istotna będzie budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, prowadzonych we współpracy świata nauki oraz przedsiębiorstw komercyjnych | Instytut: Konieczne jest wyjaśnienie na czym polega nowa wizja rozwoju kraju lub zapisów jakiego innego strategicznego dokumentu dotyczy. | **Uwaga nieuwzględniona**  Chodzi o strategie rozwoju kraju np. SOR. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.3 (p 7.3) | W związku z dynamicznie rozwijającym się rynkiem informatycznym, w szczególności w związku z perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6, a także w związku z rozwojem idei Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0, jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy megadanych (*Big Data)* | Instytut: Bardziej zasadne w tym kontekście jest pisanie o obszarze teleinformatycznym. We tym kontekście pominięte zostały technologie, które niewątpliwie zmienią krajobraz cyberbezpieczeństwa, są nimi informatyka kwantowa oraz sztucznej inteligencji i dlatego w tym punkcie nie powinny one zostać pominięte. | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.3 (p 7.3) | Ważne zadania w systemie zapewnienia cyberbezpieczeństwa mają organizacje pozarządowe, które są bardzo sprawnymi organizatorami działań edukacyjnych w społeczeństwie, a także jako dostawcy analiz i opinii dla administracji publicznej. Możliwe jest także pozyskiwanie specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa. | Instytut: Nie zrozumiały cel owego zapisu. Czy jest to postulat jakiegoś konkretnego działania, czy wskazówka dla organizacji eksperckich dotycząca możliwości pozyskania specjalistów? | **Uwaga nieuwzględniona**  Jest to wskazanie roli NGO w działaniach rządu w obszarze cyberbezpieczeństwa. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.3 (p 7.3) |  | Instytut: W ramach programów badawczych, które zostaną opracowane we współpracy ze środowiskiem naukowo-akademickim postulujemy uzupełnienie o temat „Odpowiedzialne wdrażanie technologii cyfrowych z uwzględnieniem średnio i długookresowych skutków społecznych oraz ekonomicznych dla państwa oraz obywateli (ang. Digital Sustainable Growth). W tym z uwzględnieniem zasady „privacy by design” oraz modeli implementacji rozwiązań technologicznych zapewniających zarówno bezpieczeństwo danych jak i realną wartość dodaną dla polskiej gospodarki.” | **Wyjaśnienie**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3.4 (p 7.4) | Siły Zbrojne RP, jako podstawowy element systemu obronnego państwa, powinny angażować się w działania w cyberprzestrzeni na tym samym poziomie co w powietrzu, na lądzie i na morzu. Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych oraz zwalczanie źródeł zagrożeń. | Instytut: Siły Zbrojne maja obowiązek angażować się w działania w domenie cyberprzestrzeni. Dodatkowo rozpoznawanie zagrożeń, obrona i ochrona, zwalczanie zagrożeń powinno być uzupełnione o minimalizację skutków.  Ponadto, dla skutecznego prowadzenia działań w cyberprzestrzeni niezbędne jest posiadanie stosownych narzędzi, w tym bezpiecznych i niezawodnych systemów łączności. Powinny one (zarówno narzędzia, jak i systemy łączności) w możliwie największym stopniu opierać się na rozwiązaniach krajowych, wytwarzanych wyłącznie bądź przede wszystkim na potrzeby Sił Zbrojnych RP, w celu uniezależnienia się od dostawców zagranicznych pozostających pod kontrolą obcych rządów, których interesy nie zawsze będą zgodne z interesami państwa polskiego. Tendencja do uzależniania się w sektorze wysokich technologii obronnych od jednego państwa budzi uzasadnione wątpliwości w zakresie nie tylko pozyskiwania rozwiązań optymalnych i tworzonych „na miarę” zapotrzebowania sił zbrojnych, ale również kompatybilności i interoperacyjności, nie wspominając o bezpieczeństwie informacyjnym. Nie można też wykluczyć, że producent celowo pozostawi w oprogramowaniu przekazanym użytkownikom luki i furtki mające na celu potajemne pobieranie danych od użytkowania. | **Uwaga nieuwzględniona**  Uwaga niejasna wobec zapisu w celu szczegółowym. Konieczne doprecyzowanie, jaki jest sens uwagi. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 3 |  | Instytut: W ramach celu szczegółowego 3 nie uwzględniono wykorzystywanego aktualnie na całym świecie m.in. w ramach działań UE, podejścia opartego na wsparciu całego ekosystemu tworzenia innowacji dla cyberbezpieczeństwa (Zob. R. Siudak, Z. Jóźwik, Regional innovation centres and their role in dealing with cyber disruption, The Kosciuszko Institute Policy Brief, November 2017, ISSN 1689-9873, Kraków; Por. R. Siudak, Anat Karmona, David Crozier, Dan Craigen, Darin Andersen, Richard Franken, Selected regional Innovation Centres for Cybersecurity, “European Cybersecurity Market” Vol. 1, No. 4, 2017, pp. 5-12). Podejście to obecne m.in. w ramach unijnych inicjatyw na rzecz Digital Innovation Hubs oraz tworzenia dedykowanych centrów kompetencji, zakłada promocję oraz wsparcie nie tylko w zakresie rozwoju określonych rozwiązań technologicznych (projekty B+R) ale całego łańcucha niezbędnego do wytworzenia konkurencyjnego globalnie sektora cyberbezpieczeństwa: Kompetencje pracowników (edukacja) – technologie (projekty B+R) – produkty/usługi dostępne na rynku (komercjalizacja/podaż) – wykorzystanie narzędzi cyfrowych w gospodarce (wdrożenia/popyt). Analizując aktualną sytuację rynku cyberbezpieczeństwa w Polsce segmentami w ramach których brakuje wystarczających działań celowych, są komercjalizacja oraz wdrożenia. Szczególnie ważne wydaje się w tym kontekście wsparcie dla sektor MŚP w fazie komercjalizacji technologii (firmy oferujące rozwiązania z branży cyberbezpieczeństwa) a także w fazie wdrażania (przedsiębiorstwa przechodzące przez transformację cyfrową). | **Uwaga częściowo uwzględniona** |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 4.1 (p 8.1) | Podnoszenie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP będzie realizowane poprzez stworzenie i wdrożenie takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników | Instytut: Konieczne jest wyjaśnienie jakie kadry są istotne dla cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  W zależności od potrzeb instytucji i rodzaju projektów. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 4.1 (p 8.1) | Kierownictwo jednostek administracji rządowej będzie dynamicznie określało odpowiedzialność i uprawnienia dla osób pełniących istotną rolę w zakresie zarządzania cyberbezpieczeństwem i odpowiednio komunikowało te ustalenia wszystkim interesariuszom | Instytut: Fragment wymaga rozwinięcia i wyjaśnienia – np. w jaki sposób działanie wiąże się z już istniejącymi wymaganiami regulacyjnymi, standardami. Kim są osoby pełniące istotną rolę itd. | **Uwaga nieuwzględniona**  W opinii MC użyte pojęcia są zrozumiałe. Chodzi o rozdzielanie zadań w sposób reakcyjny, zależny od zagrożeń |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 4.2 (p 8.2) | Uczelnie wyższe będą zachęcane do tego, aby rozwijane były specjalizacje interdyscyplinarne, obejmujące między innymi zarządzanie bezpieczeństwem informacji, ocenę i weryfikację zabezpieczeń systemów teleinformatycznych, ochronę danych osobowych, ochronę własności intelektualnej w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, które są tego pochodnymi | Instytut: Zwracamy uwagę na zawężające wyliczenie – jest wiele innych obszarów zasługujących na wskazanie.  Ponadto, warto zastanowić się czy fragmentu tego nie należałoby przenieść do 8.1. | **Uwaga nieuwzględniona**  Nie jest to katalog zamknięty |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 4.3 (p 8.3) | W obliczu coraz liczniejszych zagrożeń nakierowanych na wywarcie określonego wpływu na społeczeństwo, a także mając na uwadze konsekwencje celowego wykorzystywania narzędzi z obszaru inżynierii społecznej, do działań o charakterze manipulacyjnym, w postaci m.in. kampanii dezinformacyjnych, lub działań inspiracyjnych bądź dezintegracyjnych, potrzebne jest podjęcie systemowych działań pozwalających na rozwijanie świadomości obywateli w kontekście weryfikacji autentyczności informacji oraz reagowania na próby jej zakłócenia | Instytut: Przeciwdziałanie tym zagrożeniom nie powinno ograniczać się do działań zwiększających świadomość. To niekorzystne ograniczenie (patrz uwagi do zapisów ze str. 13 w kontekście zagrożeń hybrydowych). | **Uwaga nieuwzględniona**  Punkt ten jest nazwany „Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni” |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | W obliczu wszechobecnych procesów globalizacyjnych i związanych z nimi współzależności państw, międzynarodowa współpraca jest kluczowa dla osiągnięcia bezpieczeństwa globalnej cyberprzestrzeni | Instytut: Rodzi się pytanie jak definiowane jest bezpieczeństwo globalnej cyberprzestrzeni i jak rozumiana jest ta współpraca? | **Uwaga nieuwzględniona**  W opinii MC to pojęcie nie wymaga definicji. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | Realizując te zadania na poziomie europejskim, Polska zintensyfikuje działania na rzecz zapewnienia bezpieczeństwa Jednolitego Rynku Cyfrowego jako motoru wzrostu gospodarczego i innowacyjności | Instytut: W tym aspekcie nie zostały określone zadania. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | Członkostwo w Organizacji Traktatu Północnoatlantyckiego jest istotnym filarem bezpieczeństwa Polski jak i bezpieczeństwa euroatlantyckiego. Nasilające się ataki o charakterze hybrydowym czynią nieodzownym inwestowanie w zdolności odstraszania i obronne, w tym doskonalenie swojej odporności i zdolności do szybkiego i skutecznego reagowania na cyberataki | Instytut: Wzrastają także zagrożenie o charakterze nie hybrydowym, które należy brać pod uwagę i wobec których także należy podejmować działania. Dodatkowo, wzmacnianie własnego potencjału zostało omówione we wcześniejszych częściach dokumentu. Tu warto wskazać elementy związane z członkostwem w NATO i innymi działaniami związanymi z aktywnością na arenie międzynarodowej. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | Współpracując w ramach systemu Organizacji Narodów Zjednoczonych Polska będzie dążyła do kontynuacji debaty dotyczącej sprawnie funkcjonującego systemu międzynarodowego zarządzania siecią globalną oraz zagadnień związanych z prawną oceną cyberataków, w celu wypracowania spójnych rozwiązań, gwarantujących pewność międzynarodowej wymiany informacji w Internecie. Polska będzie angażować się we wzmacnianie środków budowy zaufania i bezpieczeństwa w ramach istniejących forów międzynarodowych, w tym OBWE. Rząd będzie włączał się również w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym | Instytut: Pragniemy zwrócić uwagę, że katalog zagadnień i tematów podejmowanych przez ONZ i inne organizacje jest znacznie szerszy, a wymienione są zaledwie fragmentami. Dodatkowo Polska nie powinna wyłącznie reaktywnie brać w nich udział, a proaktywnie inspirować działania, aby to zrealizować proponujemy aby w Strategii określone zostały cele jakie Polska chce w tym wymiarze osiągnąć. Równocześnie zwracamy uwagę, że opis zawiera wiele niezrozumiałych sformułowań np. dot. „rozwiązań gwarantujących pewność wymian informacji w Internecie”. Poza trudnym do zrozumienia sformułowaniem, należy wspomnieć, że nie jest to kluczowy cel procesów które mają miejsce na wyżej wymienionych forach, a na pewno nie jedyny zasługujący na wymienienie. Polska powinna wykorzystać czas członkostwa w Radzie Bezpieczeństwa ONZ do tego, aby aktywnie promować rozwój norm odpowiedzialnego zachowania państw w cyberprzestrzeni w duchu Raportu Konsensusu UN GGE z 2015 r. i wspierać osiągnięcie konsensusu podczas prac kolejnej edycji Grupy. | **Uwaga nieuwzględniona**  Udział Polski w RB ONZ jest poza zakresem Strategii. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | Wzmocnienie polskiej pozycji międzynarodowej będzie możliwe tylko na drodze wewnętrznej ścisłej kooperacji pomiędzy instytucjami i agencjami odpowiadającymi w Polsce za zapewnienie cyberbezpieczeństwa, w tym szczególnie pomiędzy ministrem właściwym ds. informatyzacji oraz z ministrem spraw zagranicznych odpowiadającym za całokształt polskiej polityki zagranicznej | Instytut: Zapis pomija wielu interesariuszy którzy powinni być wskazani, w tym m.in. ministra obrony narodowej. Także wobec zapisów Ustawy o krajowym systemie. | **Uwaga nieuwzględniona**  Katalog jest otwarty. |  |
|  | Instytut Kościuszki | Uwaga o cel szczegółowy 5.1 (p 9.1) | W obszarze współpracy międzynarodowej Polska będzie aktywnie włączać się w ćwiczenia prowadzone zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe | Instytut: To działanie było omawiane już wcześniej.  Rozdział pomija wiele istotnych elementów. Poza wspomnianymi wyżej celami, np. brak zapisów np. o współpracy z sektorem pozarządowym w zakresie kreowania, wdrażania polityki międzynarodowej w omawianym obszarze. | **Uwaga nieuwzględniona**  NGOsy mieszczą się w kategorii innych podmiotów międzynarodowych.  Proszę o wskazanie brakujących elementów celem oceny ich przydatności. |  |
|  | Instytut Kościuszki | Uwaga o Zarządzanie Strategią (p 10) |  | Instytut: W ramach oczekiwanych działań projektowych należy wyznaczyć nie tylko harmonogram, organy, efekty i budżet ale także kluczowe wskaźniki efektywności (ang. Key Performance Indicators, KPI). Monitorowane w trakcie realizacji projektu przez organ realizujący/nadzorujący pozwolą na realną ocenę postępów oraz ewentualną potrzebę podjęcia dodatkowych działań lub zmianę przyjętych działań w celu osiągnięcia założonego efektu. | **Uwaga nieuwzględniona**  Konkretne działa wraz z harmonogramem ich realizacji będą ustalone w Planie działań. |  |
|  | Instytut Kościuszki | Uwaga o Finansowanie (p 11) |  | Instytut: Naszym zdaniem ze względu na strategiczny wymiar wyzwań związanych z bezpieczeństwem cyfrowym niezbędne jest stworzenie bezpośredniego, zapisanego ustawowo mechanizmu zapewniania odpowiedniego finansowania dla projektów znajdujących się w Planie działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa. Mechanizm ten stanowić powinien uzupełnienie dla wydatków ponoszonych przez poszczególne jednostki zaangażowane we wdrażanie Strategii Cyberbezpieczeństwa. Finansowanie projektów znajdujących się w Planie działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa powinno odbywać się w formule 50%/50%, gdzie połowę kosztów ponosi poszczególna jednostka zaangażowane we wdrażanie Strategii Cyberbezpieczeństwa, połowę stanowią środki z rezerwy celowej budżetu centralnego. W związku z powyższym proponujemy zapisanie w ramach odpowiedniej ustawy przeznaczania rocznie określonego procentu PKB na projekty związane z wdrożeniem Strategii Cyberbezpieczeństwa oraz podnoszeniem poziomu cyberbezpieczeństwa w Polsce. Procent ten powinien zostać określony na etapie tworzenia pierwszego Planu działań na rzecz Strategii Cyberbezpieczeństwa, gdy wiadome będą szacunkowe koszty planowanych w nim projektów. Dodatkowo w tym celu w ramach rezerwy celowej budżetu centralnego należy odpowiednio zaplanować i zabezpieczyć środki w wysokości połowy określonej procentowo części PKB przeznaczonej na wyżej opisane działania. | **Uwaga nieuwzględniona**  Uchwała Rady Ministrów nie może nakładać zobowiązań finansowych, gdyż może to nastąpić jedynie w drodze ustawy.  Natomiast kwestia ta może to być przedmiotem dyskusji w trakcie prac nad zmianą ustawy o ksc. |  |
|  | Osoba fizyczna 2 | Uwaga o cel szczegółowy 4.2 (p 8.2) | byłaby prowadzona przed wejściem **w** świat cyfrowy | Osoba fizyczna 2 proponuje dodać zwrot: **„w”** | **Uwaga uwzględniona** |  |
|  | Osoba fizyczna 2 | Uwaga o cel szczegółowy 4.3 (p 8.3) | Społeczeństwo na zagrożenia płynące z **w** cyberprzestrzeni | Osoba fizyczna 2 proponuje wykreślić zwrot: **„w”** | **Uwaga uwzględniona** |  |
|  | Osoba fizyczna 2 | Uwaga o cel szczegółowy 2.2 (p 6.2) | wyznaczenie krajowego **orangu** ds. certyfikacji cyberbezpieczeństwa | Osoba fizyczna 2 proponuje zamienić zwrot na: **„organu”** | **Uwaga uwzględniona** |  |

1. Art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa. [↑](#footnote-ref-1)
2. Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną. [↑](#footnote-ref-2)
3. IT – ang. Information technologies [↑](#footnote-ref-3)
4. OT – ang. operational technologies [↑](#footnote-ref-4)
5. Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną. [↑](#footnote-ref-5)
6. Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną. [↑](#footnote-ref-6)
7. IT – ang. Information technologies [↑](#footnote-ref-7)
8. Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną. [↑](#footnote-ref-8)
9. Art. 69 ust. 2 ustawy KSC [↑](#footnote-ref-9)