Parlament Europejski
2019-2024

Komisja Spraw Zagranicznych

2023/0109(COD)

27.10.2023

OPINIA

Komisji Spraw Zagranicznych

dla Komisji Przemysłu, Badań Naukowych i Energii

w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Sprawozdawca komisji opiniodawczej: Dragoş Tudorache

PA_Legam

Poprawka 1

Wniosek dotyczący rozporządzenia
Motyw 1

Tekst proponowany przez Komisję	*Poprawka*
(1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu we wszystkich sektorach działalności gospodarczej, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.	(1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu we wszystkich sektorach działalności gospodarczej, ***a także wojskowej,*** gdyż administracje publiczne, przedsiębiorstwa i obywatele ***oraz podmioty wojskowe i zajmujące się obronnością*** są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) Rosną skala, częstotliwość i wpływ incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw, które to ataki mają na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. Stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Z uwagi na szybko zmieniający się krajobraz zagrożeń zagrożenie możliwymi incydentami na dużą skalę powodującymi poważne zakłócenie lub uszkodzenie infrastruktur krytycznych wymaga podwyższonej gotowości na wszystkich szczeblach unijnych ram cyberbezpieczeństwa. ***To zagrożenie wykracza*** poza rosyjską napaść na Ukrainę i prawdopodobnie ***będzie*** się utrzymywać, biorąc pod uwagę wielość podmiotów powiązanych z organami państwowymi, ze środowiskami przestępczymi	(2) Rosną skala, częstotliwość i wpływ incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw, które to ataki mają na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. Stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Z uwagi na szybko zmieniający się krajobraz zagrożeń zagrożenie możliwymi incydentami na dużą skalę powodującymi poważne zakłócenie lub uszkodzenie infrastruktur krytycznych wymaga podwyższonej gotowości na wszystkich szczeblach unijnych ram cyberbezpieczeństwa. ***Zagrożenia te jeszcze się zwiększyły wraz z powrotem wojny do Europy. Te zagrożenia wykraczają*** poza rosyjską napaść na Ukrainę i prawdopodobnie ***będą*** się utrzymywać, biorąc pod uwagę wielość

i haktywistycznymi, które mają swój udział w generowaniu obecnych napięć geopolitycznych. Takie incydenty mogą utrudniać świadczenie usług publicznych i prowadzenie działalności gospodarczej, w tym w sektorach krytycznych lub wysoce krytycznych, powodować znaczne straty finansowe, podważać zaufanie użytkowników, powodować poważne szkody dla gospodarki Unii, a nawet mieć konsekwencje zagrażające zdrowiu lub życiu. Ponadto incydenty w cyberbezpieczeństwie są nieprzewidywalne, ponieważ często pojawiają się i ewoluują w bardzo krótkim czasie, nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach.	podmiotów powiązanych z organami państwowymi, ze środowiskami przestępczymi i haktywistycznymi, które mają swój udział w generowaniu obecnych napięć geopolitycznych. Takie incydenty mogą utrudniać świadczenie usług publicznych i prowadzenie działalności gospodarczej, w tym w sektorach krytycznych lub wysoce krytycznych, powodować znaczne straty finansowe, podważać zaufanie użytkowników, powodować poważne szkody dla gospodarki Unii, ***i bezpieczeństwa w Unii,*** a nawet mieć konsekwencje zagrażające zdrowiu lub życiu***, jeżeli na szwank zostanie narażona lokalna lub krajowa infrastruktura związana z bezpieczeństwem***. Ponadto incydenty w cyberbezpieczeństwie są nieprzewidywalne, ponieważ często pojawiają się i ewoluują w bardzo krótkim czasie, nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach. ***Cyberbezpieczeństwo jest ważne dla ochrony naszych europejskich wartości i zapewnienia funkcjonowania naszych demokracji poprzez ochronę naszej infrastruktury wyborczej i procedur demokratycznych przed wszelką zagraniczną ingerencją.***

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2a) Ochrona cyberbezpieczeństwa jest niezbędna, jeśli chcemy zapewnić bezpieczeństwo Unii i nie pozwolić, by działające w złej wierze podmioty – państwowe i nie tylko – zagrażały naszej demokracji, gospodarce i bezpieczeństwu. Bezwzględnie należy zapobiegać rozdrobnieniu, ponieważ nie byłoby to

odpowiednie podejście, w szczególności w obliczu wyzwania związanego z ewentualnymi przyszłymi cyberatakami na dużą skalę wymierzonymi w kilka państw członkowskich w tym samym czasie lub w transnarodową infrastrukturę krytyczną. A zatem potrzebny jest organ Unii, który działałby jako platforma koordynacji wszystkich istniejących i przyszłych instrumentów, funduszy i mechanizmów cyberbezpieczeństwa.

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(3) Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy[16], konieczne jest zwiększenie odporności obywateli, przedsiębiorstw i podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastruktury i usługi, które będą wspierać szybsze wykrywanie zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz reagowanie na nie, a państwa członkowskie potrzebują pomocy w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i w reagowaniu na nie. Unia powinna również zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie gromadzenia i analizy danych dotyczących	(3) Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy[16], konieczne jest zwiększenie odporności obywateli, przedsiębiorstw i podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastruktury i usługi, które będą wspierać szybsze wykrywanie zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz reagowanie na nie, a państwa członkowskie potrzebują pomocy w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i w reagowaniu na nie. Unia powinna również zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie gromadzenia i analizy danych dotyczących

zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie***, a także w zakresie proaktywnego działania i stanowczego reagowania na zagrożenia i incydenty w zakresie cyberbezpieczeństwa***.

---

[16] https://futureu.europa.eu/pl/

[16] https://futureu.europa.eu/pl/

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 4

Tekst proponowany przez Komisję

(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[20]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

Poprawka

(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[20]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, ***proaktywnej,*** solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym. ***Ponadto w marcu 2022 r. Unia zatwierdziła i uruchomiła swój Strategiczny kompas na rzecz bezpieczeństwa i obrony, który koncentruje się między innymi na***

wzmocnieniu cyberbezpieczeństwa i zacieśnianiu współpracy międzynarodowej z sojusznikam i partnerami demokratycznymi i o podobnym podejściu, zwłaszcza w tej kwestii. Ponadto cyberbezpieczeństwo było centralnym punktem niedawnej trzeciej wspólnej deklaracji w sprawie współpracy UE–NATO ze stycznia 2023 r. W szczególności w swoim sprawozdaniu końcowym z oceny grupa zadaniowa UE-NATO zaleciła pełne wykorzystanie synergii między UE a NATO[1], w tym wymiany między podmiotami cywilnymi i wojskowymi najlepszych praktyk w zakresie wdrażania odpowiednich strategii i przepisów dotyczących cyberprzestrzeni.

[1]

https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022).

[18] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

[19] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds.

---

[17] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022).

[18] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

[19] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds.

Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 6

Tekst proponowany przez Komisję	*Poprawka*
(6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”[22], przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka.	(6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”[22], przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka. ***Ponadto szybko zmieniający się krajobraz cyberzagrożeń i równie szybkie tempo rozwoju technologicznego wskazują także na potrzebę sprawniejszej koordynacji i współpracy cywilno-wojskowej, na co zwróciła uwagę Rada w swoich konkluzjach w sprawie polityki UE w zakresie cyberobrony[1].*** ***[1] Konkluzje Rady w sprawie polityki UE w zakresie cyberobrony zatwierdzone przez Radę na posiedzeniu w dniu 22 maja 2023 r. (9618/23).***

[22] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

[22] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

Poprawka 7

Wniosek dotyczący rozporządzenia
Motyw 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(6a) Ze względu na zacieranie się granic między kwestiami cywilnymi a wojskowymi, a także możliwość podwójnego zastosowania cybernarzędzi i cybertechnologii konieczne jest kompleksowe i całościowe podejście do dziedziny cyfrowej. W przypadku incydentów i sytuacji kryzysowych na dużą skalę w cyberbezpieczeństwie, które dotyczą więcej niż jednego państwa członkowskiego, należy przewidzieć odpowiednie zarządzanie kryzysowe. Tego rodzaju struktury powinny umożliwić zorganizowanie wymiany informacji, koordynacji i współpracy z unijnymi strukturami odpowiedzialnymi za bezpieczeństwo zewnętrzne i wojskowe zarządzanie kryzysowe oraz organami państw członkowskich odpowiedzialnymi za bezpieczeństwo i obronę (społecznością zajmującą się cyberobroną). Dotyczy to również operacji i misji w ramach wspólnej polityki bezpieczeństwa i obrony prowadzonych przez Unię w celu zapewnienia pokoju i stabilności w jej sąsiedztwie i poza nim.

Poprawka 8

Wniosek dotyczący rozporządzenia
Motyw 7

Tekst proponowany przez Komisję	*Poprawka*
(7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę. Dlatego należy wprowadzić ogólnoeuropejską infrastrukturę SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków; należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).	(7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę. Dlatego należy wprowadzić ogólnoeuropejską infrastrukturę SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w ***tym incydenty dotyczące dwóch lub większej liczby państw członkowskich, w*** reagowaniu na nie i w natychmiastowym usuwaniu ich skutków***. Jeśli jest to konieczne i wykonalne, mechanizm cyberkryzysowy powinien organizować wymianę informacji i współpracę z organami obrony państw członkowskich i być wspierany przez instytucje, organy i agencje UE (unijną społeczność zajmująca się cyberobroną)***; należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę***. Takie nowe struktury powinny również udzielać wsparcia operacjom i misjom UE w dziedzinie WPBiO***. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

Poprawka 9

Wniosek dotyczący rozporządzenia
Motyw 11

Tekst proponowany przez Komisję	*Poprawka*
(11) Do celów należytego zarządzania finansami należy ustanowić przepisy szczegółowe dotyczące przenoszenia niewykorzystanych środków na zobowiązania i środków na płatności. Z poszanowaniem zasady, że budżet Unii jest ustalany corocznie, w niniejszym rozporządzeniu należy – ze względu na nieprzewidywalny, wyjątkowy i specyficzny charakter krajobrazu cyberbezpieczeństwa – przewidzieć – obok możliwości określonych w rozporządzeniu finansowym – możliwość przenoszenia niewykorzystanych środków, a tym samym maksymalnie zwiększyć zdolność mechanizmu cyberkryzysowego do wspierania państw członkowskich w skutecznym zwalczaniu cyberzagrożeń.	(11) Do celów należytego zarządzania finansami należy ustanowić przepisy szczegółowe dotyczące przenoszenia niewykorzystanych środków na zobowiązania i środków na płatności. Z poszanowaniem zasady, że budżet Unii jest ustalany corocznie, w niniejszym rozporządzeniu należy – ze względu na nieprzewidywalny, wyjątkowy i specyficzny charakter krajobrazu cyberbezpieczeństwa – przewidzieć – obok możliwości określonych w rozporządzeniu finansowym – możliwość przenoszenia niewykorzystanych środków, a tym samym maksymalnie zwiększyć zdolność mechanizmu cyberkryzysowego do wspierania państw członkowskich w skutecznym zwalczaniu cyberzagrożeń. ***Te przepisy szczegółowe pozwoliłyby również na długoterminowe wsparcie finansowe na rzecz wspólnych zamówień na ultrabezpieczne narzędzia i infrastrukturę nowej generacji i zwiększenie tym samym zdolności zbiorowego wykrywania incydentów dzięki wykorzystaniu najnowszych możliwości w dziedzinie sztucznej inteligencji (AI) i analizy danych.***

Poprawka 10

Wniosek dotyczący rozporządzenia
Motyw 13

Tekst proponowany przez Komisję	*Poprawka*
(13) Każde państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym	(13) Każde państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym

państwie członkowskim. Te krajowe SOC powinny pełnić funkcję punktu odniesienia i punktu dostępu na szczeblu krajowym do celów uczestnictwa w europejskiej tarczy cyberbezpieczeństwa oraz powinny zapewniać, aby informacje o cyberzagrożeniach uzyskiwane od podmiotów publicznych i prywatnych skutecznie i sprawnie wymieniano i gromadzono na szczeblu krajowym.

państwie członkowskim. Te krajowe SOC powinny pełnić funkcję punktu odniesienia i punktu dostępu na szczeblu krajowym do celów uczestnictwa w europejskiej tarczy cyberbezpieczeństwa oraz powinny zapewniać, aby informacje o cyberzagrożeniach uzyskiwane od podmiotów publicznych i prywatnych skutecznie i sprawnie wymieniano i gromadzono na szczeblu krajowym. ***W razie potrzeby i jeśli jest to wykonalne SOC powinny umożliwiać również udział podmiotów działających w dziedzinie obrony dzięki ustanowieniu „filaru obronnego" w zakresie zarządzania i rodzaju udostępnianych informacji, zgodnie z propozycją zawartą we wspólnym komunikacie w sprawie polityki UE w zakresie cyberobrony[1] i popartą przez wysokiego przedstawiciela.***

[1] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

Poprawka 11

Wniosek dotyczący rozporządzenia
Motyw 14

Tekst proponowany przez Komisję	*Poprawka*
(14) W ramach europejskiej tarczy cyberbezpieczeństwa należy ustanowić szereg transgranicznych centrów monitorowania bezpieczeństwa („transgraniczne SOC"). Powinny one zrzeszać krajowe SOC z co najmniej trzech państw członkowskich, tak aby można było w pełni osiągnąć korzyści płynące z transgranicznego wykrywania zagrożeń, wymiany informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych SOC powinno być zwiększanie zdolności w zakresie analizy i wykrywania zagrożeń cyberbezpieczeństwa oraz zapobiegania	(14) W ramach europejskiej tarczy cyberbezpieczeństwa należy ustanowić szereg transgranicznych centrów monitorowania bezpieczeństwa („transgraniczne SOC"). Powinny one zrzeszać krajowe SOC z co najmniej trzech państw członkowskich, ***w tym „filar obrony",*** tak aby można było w pełni osiągnąć korzyści płynące z transgranicznego wykrywania zagrożeń, wymiany informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych SOC powinno być zwiększanie zdolności w zakresie analizy i wykrywania zagrożeń

im, wspieranie generowania wysokiej jakości danych wywiadowczych dotyczących zagrożeń cyberbezpieczeństwa, w szczególności w drodze wymiany danych z różnych źródeł publicznych lub prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami i ich wspólne używanie oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń oraz zapobiegania im w zaufanym otoczeniu. Powinny one zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, zespołach reagowania na incydenty bezpieczeństwa komputerowego („CSIRT") i innych odpowiednich podmiotach oraz uzupełniając je.	cyberbezpieczeństwa oraz zapobiegania im, wspieranie generowania wysokiej jakości danych wywiadowczych dotyczących zagrożeń cyberbezpieczeństwa, w szczególności w drodze wymiany danych z różnych źródeł publicznych lub prywatnych, a ***w razie konieczności i jeśli jest to wykonalne wojskowych, przy zapewnieniu wystarczających wytycznych dotyczących wymiany informacji, a*** także przez dzielenie się najnowocześniejszymi narzędziami i ich wspólne używanie oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń oraz zapobiegania im w zaufanym otoczeniu. Powinny one zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, zespołach reagowania na incydenty bezpieczeństwa komputerowego („CSIRT") i innych odpowiednich podmiotach oraz uzupełniając je.

Poprawka 12

Wniosek dotyczący rozporządzenia
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Na szczeblu krajowym monitorowanie, wykrywanie i analizę cyberzagrożeń zazwyczaj zapewniają SOC funkcjonujące w podmiotach publicznych i prywatnych w połączeniu z CSIRT. Ponadto CSIRT wymieniają informacje w kontekście sieci CSIRT zgodnie z dyrektywą (UE) 2022/2555. Transgraniczne SOC powinny stanowić nową zdolność, która jest uzupełnieniem sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych oraz wymienianie takich danych, zwiększanie wartości takich danych dzięki analizie eksperckiej oraz wspólnie nabytym infrastrukturom i najnowocześniejszym narzędziom oraz poprzez wkład w rozwój	(15) Na szczeblu krajowym monitorowanie, wykrywanie i analizę cyberzagrożeń zazwyczaj zapewniają SOC funkcjonujące w podmiotach publicznych i prywatnych w połączeniu z CSIRT. Ponadto CSIRT wymieniają informacje w kontekście sieci CSIRT zgodnie z dyrektywą (UE) 2022/2555. Transgraniczne SOC powinny stanowić nową zdolność, która jest uzupełnieniem sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych oraz wymienianie takich danych, zwiększanie wartości takich danych dzięki analizie eksperckiej oraz wspólnie nabytym infrastrukturom i najnowocześniejszym narzędziom oraz poprzez wkład w rozwój

zdolności i ***suwerenności technologicznej*** Unii.

zdolności i ***odporności*** Unii.

Poprawka 13

Wniosek dotyczący rozporządzenia
Motyw 16

Tekst proponowany przez Komisję	*Poprawka*
(16) Transgraniczne SOC powinny działać jako centralny punkt, który umożliwia szerokie gromadzenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwala na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy podmiotów (np. zespołów reagowania na incydenty komputerowe („CERT”), CSIRT, ośrodków wymiany i analizy informacji („ISAC”), operatorów infrastruktury krytycznej). Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze o zagrożeniach, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.	(16) Transgraniczne SOC powinny działać jako centralny punkt, który umożliwia szerokie gromadzenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwala na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy podmiotów (np. zespołów reagowania na incydenty komputerowe („CERT”), CSIRT, ośrodków wymiany i analizy informacji („ISAC”), operatorów infrastruktury krytycznej ***oraz społeczności zajmującej się cyberobroną***). Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze o zagrożeniach, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC***, a po jej ustanowieniu także z operacyjną siecią dla milCERT (MICNET)***.

Poprawka 14

Wniosek dotyczący rozporządzenia
Motyw 17

Tekst proponowany przez Komisję	*Poprawka*
(17) Wspólna orientacja sytuacyjna wśród właściwych organów jest niezbędnym warunkiem gotowości	(17) Wspólna orientacja sytuacyjna wśród właściwych organów jest niezbędnym warunkiem gotowości

i koordynacji w całej Unii w odniesieniu do poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę. Dyrektywą (UE) 2022/2555 ustanowiono EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. W zaleceniu (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę uwzględniono rolę wszystkich odpowiednich podmiotów. W dyrektywie (UE) 2022/2555 przypomniano również o odpowiedzialności Komisji w ramach Unijnego Mechanizmu Ochrony Ludności („UMOL”) ustanowionego decyzją Parlamentu Europejskiego i Rady 1313/2013/UE oraz o spoczywającej na niej odpowiedzialności za przedstawianie sprawozdań analitycznych dotyczących uzgodnień na potrzeby mechanizmu reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR”) na podstawie decyzji wykonawczej (UE) 2018/1993. W związku z tym w sytuacjach, w których transgraniczne SOC uzyskają informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, powinny przekazywać istotne informacje EU-CyCLONe, sieci CSIRT i Komisji. W szczególności, w zależności od sytuacji, przekazywane informacje mogą obejmować informacje techniczne, informacje na temat charakteru i motywów sprawcy lub potencjalnego sprawcy ataku oraz informacje nietechniczne wyższego szczebla na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę. W tym kontekście należy zwrócić należytą uwagę na zasadę ograniczonego dostępu

i koordynacji w całej Unii w odniesieniu do poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę. Dyrektywą (UE) 2022/2555 ustanowiono EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. W zaleceniu (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę uwzględniono rolę wszystkich odpowiednich podmiotów. W dyrektywie (UE) 2022/2555 przypomniano również o odpowiedzialności Komisji w ramach Unijnego Mechanizmu Ochrony Ludności („UMOL”) ustanowionego decyzją Parlamentu Europejskiego i Rady 1313/2013/UE oraz o spoczywającej na niej odpowiedzialności za przedstawianie sprawozdań analitycznych dotyczących uzgodnień na potrzeby mechanizmu reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR”) na podstawie decyzji wykonawczej (UE) 2018/1993. W związku z tym w sytuacjach, w których transgraniczne SOC uzyskają informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, powinny przekazywać istotne informacje EU-CyCLONe, sieci CSIRT***, społeczności zajmującej się cyberobroną*** i Komisji. W szczególności, w zależności od sytuacji, przekazywane informacje mogą obejmować informacje techniczne, informacje na temat charakteru i motywów sprawcy lub potencjalnego sprawcy ataku oraz informacje nietechniczne wyższego szczebla na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę. W tym kontekście należy zwrócić należytą

oraz potencjalnie poufny charakter wymienianych informacji.	uwagę na zasadę ograniczonego dostępu oraz potencjalnie poufny charakter wymienianych informacji.

Poprawka 15

Wniosek dotyczący rozporządzenia
Motyw 19

Tekst proponowany przez Komisję	*Poprawka*
(19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów i terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych.	(19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury***, z wyjątkiem dostawców wysokiego ryzyka dostarczających krytyczne produkty z elementami cyfrowymi***. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów i terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych. ***Przy korzystaniu ze sztucznej inteligencji należy zadbać o sprawowanie nadzoru przez człowieka oraz zapewnić wystarczający poziom umiejętności w zakresie sztucznej inteligencji, niezbędne wsparcie i uprawnienia do wykonywania tej funkcji.***

Poprawka 16

Wniosek dotyczący rozporządzenia
Motyw 19 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(19a) Zgodnie z rozporządzeniem [XX/XXXX (akt dotyczący

	cyberodporności)] podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny również spełniać wymogi tego rozporządzenia w odniesieniu do wszystkich produktów z elementami cyfrowymi. Ze względu na coraz większe ryzyko, jakie stanowią zależności gospodarcze, należy zminimalizować ekspozycję na dostawców wysokiego ryzyka dostarczających produkty krytyczne dzięki wspólnym ramom strategicznym bezpieczeństwa gospodarczego UE. Zależność od dostawców wysokiego ryzyka dostarczających krytyczne produkty z elementami cyfrowymi wiąże się z ryzykiem strategicznym, któremu należy zapobiegać na szczeblu Unii, w szczególności gdy któreś państwo ucieka się do szpiegostwa przemysłowego czy wymuszenia ekonomicznego, a jego przepisy wymagają arbitralnego dostępu do wszelkiego rodzaju operacji czy danych przedsiębiorstwa, zwłaszcza gdy z produktów krytycznych mają korzystać podmioty kluczowe zdefiniowane w dyrektywie (UE) 2022/2555.

Poprawka 17

Wniosek dotyczący rozporządzenia
Motyw 20

Tekst proponowany przez Komisję	*Poprawka*
(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną Unii. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną	(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną***, autonomię strategiczną, konkurencyjność i odporność*** Unii. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa

rozporządzeniem Rady (UE) 2021/1173[25].

z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173[25].

[25] Rozporządzenie Rady (UE) 2021/1173 z dnia 13 lipca 2021 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali i uchylające rozporządzenie (UE) 2018/1488 (Dz.U. L 256 z 19.7.2021, s. 3).

[25] Rozporządzenie Rady (UE) 2021/1173 z dnia 13 lipca 2021 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali i uchylające rozporządzenie (UE) 2018/1488 (Dz.U. L 256 z 19.7.2021, s. 3).

Poprawka 18

Wniosek dotyczący rozporządzenia
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach PESCO***26*** i zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii	(25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach ***PESCO[1], nowy projekt*** PESCO ***o nazwie Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (CIDCC)*** i ***jego proponowany następca w postaci Centrum Koordynacji UE ds. Cyberobrony (EUCDCC) oraz*** zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy

i w państwach trzecich.	uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii i w państwach trzecich***, zwłaszcza w państwach kandydujących do UE, które przestrzegają zasad wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony UE, wspierając te kraje w budowaniu zdolności w zakresie cyberbezpieczeństwa i zacieśnianiu współpracy transgranicznej i regionalnej w dziedzinie cyberbezpieczeństwa między tymi krajami***. ***[1] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.***
[26] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.	[26] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.

Poprawka 19

Wniosek dotyczący rozporządzenia
Motyw 26

Tekst proponowany przez Komisję	*Poprawka*
(26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL[27], IPCR[28], i dyrektywy (UE) 2022/2555. Może on wnosić wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również	(26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL[27], IPCR[28], i dyrektywy (UE) 2022/2555. Może on wnosić wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również

skoordynowane***, w stosownych przypadkach,*** z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej.	skoordynowane z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej***, zacieśniając strategiczną, operacyjną i techniczną współpracę między społecznością zajmującą się cyberobroną a innymi społecznościami działającymi w cyberprzestrzeni, w szczególności w celu wzmocnienia zdolności w zakresie przeciwdziałania zagrożeniom dla cyberbezpieczeństwa spoza Unii, w tym środków ograniczających, które można wykorzystać do zapobiegania szkodliwym działaniom w cyberprzestrzeni i reagowania na nie***.
[27] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).	[27] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).
[28] Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.	[28] Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

Poprawka 20

Wniosek dotyczący rozporządzenia
Motyw 28

Tekst proponowany przez Komisję	*Poprawka*
(28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również	(28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również

państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych.	państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych ***przy odpowiednim wykorzystaniu całego szeregu opcji obronnych dostępnych dla społeczności cywilnych i wojskowych*** .

Poprawka 21

Wniosek dotyczący rozporządzenia
Motyw 29

Tekst proponowany przez Komisję	*Poprawka*
(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. ***Sektory*** lub ***podsektory*** należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe"). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane	(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. ***W stosownych przypadkach w dokonywanie aktualnych ocen i pomoc w identyfikacji sektorów*** lub ***podsektorów, które*** należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe")***, powinna być również zaangażowana Europejska Służba Działań Zewnętrznych (ESDZ), w szczególności za pośrednictwem Centrum Analiz Wywiadowczych UE (INTCEN) i jego Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych, przy wsparciu Dyrekcji Wywiadu Sztabu Wojskowego Unii Europejskiej (EUMS) działającej w ramach pojedynczej komórki analiz wywiadowczych (SIAC)***. Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach***. Powinno ono również odgrywać ważną rolę w usprawnianiu współpracy między podmiotami cywilnymi i wojskowymi. Organizując ćwiczenia, Komisja, ESDZ i ENISA powinny zatem systematycznie rozważyć włączenie uczestników z innych społeczności działających w cyberprzestrzeni, takich jak Europejska Agencja Obrony (EDA) i inne odpowiednie podmioty.*** Przy wyborze sektorów i opracowywaniu scenariuszy

oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/***255429***. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/***2554[1]***. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

---

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora

finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

Poprawka 22

Wniosek dotyczący rozporządzenia
Motyw 32

Tekst proponowany przez Komisję	*Poprawka*
(32) Mechanizm cyberkryzysowy powinien wspierać pomoc udzielaną przez państwa członkowskie państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555. Udzielające pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.	(32) Mechanizm cyberkryzysowy powinien wspierać pomoc udzielaną przez państwa członkowskie państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555. Udzielające pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy***, by zapewnić skuteczną koordynację odpowiednich programów i instrumentów UE, w tym Europejskiego Instrumentu na rzecz Pokoju (EPF), WPZiB i ISWMR, przy udzielaniu pomocy państwom trzecim, w szczególności Ukrainie i Mołdawii***. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.

Poprawka 23

Wniosek dotyczący rozporządzenia
Motyw 33

Tekst proponowany przez Komisję	*Poprawka*
(33) Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług	(33) Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług

zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i natychmiastowe usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę. Unijna rezerwa cyberbezpieczeństwa powinna zapewniać dostępność i gotowość usług. Usługi z unijnej rezerwy cyberbezpieczeństwa powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom działającym w sektorach krytycznych lub wysoce krytycznych jako uzupełnienie działań tych organów na szczeblu krajowym. Wnioskując o wsparcie z unijnej rezerwy cyberbezpieczeństwa, państwa członkowskie powinny wskazać wsparcie udzielone na szczeblu krajowym podmiotowi dotkniętemu incydentem, które należy uwzględnić przy ocenie wniosku państwa członkowskiego. Usługi z unijnej rezerwy cyberbezpieczeństwa mogą również służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii na podobnych warunkach.	zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i natychmiastowe usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę. Unijna rezerwa cyberbezpieczeństwa powinna zapewniać dostępność i gotowość usług. Usługi z unijnej rezerwy cyberbezpieczeństwa powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom działającym w sektorach krytycznych lub wysoce krytycznych jako uzupełnienie działań tych organów na szczeblu krajowym. Wnioskując o wsparcie z unijnej rezerwy cyberbezpieczeństwa, państwa członkowskie powinny wskazać wsparcie udzielone na szczeblu krajowym podmiotowi dotkniętemu incydentem, które należy uwzględnić przy ocenie wniosku państwa członkowskiego. Usługi z unijnej rezerwy cyberbezpieczeństwa mogą również służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii ***, w tym misjom WPBiO,*** na podobnych warunkach.

Poprawka 24

Wniosek dotyczący rozporządzenia
Motyw 34

Tekst proponowany przez Komisję	*Poprawka*
(34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach	(34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach krytycznych lub wysoce krytycznych**,**

krytycznych lub wysoce krytycznych.	***biorąc również pod uwagę ryzyko związane z udziałem dostawców ze strategicznych państw konkurencyjnych ze względu na potencjalne zagrożenie bezpieczeństwa gospodarczego oraz konsekwencje dla bezpieczeństwa strategicznego Unii***.

Poprawka 25

Wniosek dotyczący rozporządzenia
Motyw 36

Tekst proponowany przez Komisję	*Poprawka*
(36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, państwami członkowskimi, Komisją i innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi UE. Jeżeli chodzi o sektor prywatny, ENISA opracowuje kanały wymiany informacji z wyspecjalizowanymi dostawcami, w tym z dostawcami i sprzedawcami rozwiązań zarządzanych w zakresie bezpieczeństwa, aby realizować misję ENISA polegającą na osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii.	(36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. ***Z uwagi na opracowywanie bezpiecznego systemu łączności, korzystającego z doświadczeń europejskiej kwantowej infrastruktury komunikacyjnej (EuroQCI) oraz rządowej łączności satelitarnej w Unii Europejskiej (GOVSATCOM), w szczególności wdrożenia systemu GALILEO/GNSS dla użytkowników z dziedziny obronności, wszelkie ewentualne rozwiązania w przyszłości powinny uwzględniać pojawienie się „hiperwojny" łączącej szybkość i wyrafinowanie kwantowych technologii obliczeniowych z wysoce autonomicznymi systemami wojskowymi.*** Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we

Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji i powinno ono stanowić wkład w ich prace. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja udostępni sprawozdanie również wysokiemu przedstawicielowi.	współpracy z odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, państwami członkowskimi, Komisją i innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi UE. Jeżeli chodzi o sektor prywatny, ENISA opracowuje kanały wymiany informacji z wyspecjalizowanymi dostawcami, w tym z dostawcami i sprzedawcami rozwiązań zarządzanych w zakresie bezpieczeństwa, aby realizować misję ENISA polegającą na osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji i powinno ono stanowić wkład w ich prace. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja udostępni sprawozdanie również wysokiemu przedstawicielowi***, ESDZ i każdej misji WPBiO w państwie dotkniętym incydentem za pośrednictwem ich siedziby głównej***.

Poprawka 26

Wniosek dotyczący rozporządzenia
Motyw 37

Tekst proponowany przez Komisję	*Poprawka*
(37) Biorąc pod uwagę	(37) Biorąc pod uwagę

nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa” ***mogą*** otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, ***jeżeli*** jest ***to przewidziane w odpowiednim układzie o stowarzyszeniu z*** tym ***programem***. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”.	nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących***, zwłaszcza Ukrainy i Mołdawii,*** i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa” ***powinny*** otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa***. Wsparcie powinny uzyskać też państwa trzecie***, ***w których prowadzona*** jest ***misja WPBiO mająca za zadanie wzmocnienie odporności na zagrożenia hybrydowe, w*** tym ***cyberzagrożenia, lub w których zastosowano środek pomocy EPFw celu wzmocnienia cyberodporności państwa***. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”.

Poprawka 27

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny poważnych incydentów lub incydentów na dużą skalę.	c) ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny poważnych incydentów lub ***zagrożeń bądź*** incydentów ***lub zagrożeń*** na dużą skalę.

Poprawka 28

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) wzmocnienie wspólnego unijnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, co umożliwi wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w ***suwerenność*** technologiczną Unii w dziedzinie cyberbezpieczeństwa;	a) wzmocnienie wspólnego unijnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, co umożliwi wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w ***odporność*** technologiczną Unii w dziedzinie cyberbezpieczeństwa;

Poprawka 29

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym	b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa” ***lub***

w ramach programu „Cyfrowa Europa”;	***państwom trzecim, które kandydują do członkostwa i nie naruszają interesów Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określonych w WPZiB zgodnie z tytułem V TUE; Państwa członkowskie powinny uznać aktywny program cyberobrony za element ich krajowej strategii w dziedzinie cyberbezpieczeństwa, która obejmuje regularne wspólne ćwiczenia państw członkowskich i organizacji międzynarodowych. Program taki powinien zapewniać zsynchronizowaną zdolność wykrywania, analizowania i łagodzenia zagrożeń w czasie rzeczywistym***;

Poprawka 30

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a. ograniczenie systemowego ryzyka w cyberprzestrzeni wynikającego z uzależnienia od krytycznego sprzętu z państw, które naruszałyby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE;

Poprawka 31

Wniosek dotyczący rozporządzenia
Artykuł 2 – punkt 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	„społeczność zajmująca się cyberobroną” oznacza organy państw członkowskich odpowiedzialne za obronę wspierane przez instytucje, organy i agencje UE, jak określono we wspólnym komunikacie w sprawie polityki UE w zakresie cyberobrony[1];

[1] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

Poprawka 32

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera b a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ba) pomaga modernizować całe systemy cyberobrony, podnosząc jakość zdolności w dziedzinie cyberobrony dzięki wprowadzeniu systemów AI, oraz przyspiesza wymianę informacji między krajowymi SOC a transgranicznymi SOC;

Poprawka 33

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera d a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	da) dokonuje przeglądu i oceny krytycznych technologii i urządzeń z zakresu cyberbezpieczeństwa wykorzystywanych przez SOC w odpowiedzi na incydenty w cyberbezpieczeństwie związane z ryzykiem systemowym wynikającym z kontrolowania dostawców wysokiego ryzyka przez kraje, które naruszałyby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE.

Poprawka 34

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 1 – akapit 2

Tekst proponowany przez Komisję	*Poprawka*
Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. Jest on wyposażony w najnowocześniejsze technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.	Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych***, a w razie potrzeby wojskowych*** na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. Jest on wyposażony w najnowocześniejsze technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

Poprawka 35

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. W następstwie zaproszenia do wyrażenia zainteresowania Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) wybiera krajowe SOC do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać wybranym krajowym SOC dotacje na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 50 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa państwo członkowskie. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i krajowy SOC zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.	2. W następstwie zaproszenia do wyrażenia zainteresowania Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) wybiera krajowe SOC do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać wybranym krajowym SOC dotacje na finansowanie funkcjonowania tych narzędzi i infrastruktur***, pod bezwzględnym warunkiem że zostaną one dostarczone przez zaufanych dostawców, o których mowa w art. 16***. Wkład finansowy Unii pokrywa do 50 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa państwo członkowskie. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i krajowy SOC zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych

narzędzi i infrastruktur.

Poprawka 36

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa konsorcjum przyjmujące. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.	2. W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi i infrastruktur***, pod bezwzględnym warunkiem że zostaną one dostarczone przez zaufanych dostawców, o których mowa w art. 16***. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa konsorcjum przyjmujące. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.

Poprawka 37

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a. Należy automatycznie wykluczyć infrastrukturę lub dostawcę z państwa trzeciego wysokiego ryzyka.

Poprawka 38

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 1 – litera b a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ba) bezpośrednio wspiera wzmacnianie zdolności wojskowych i obronnych uczestniczących w niej członków lub zapobiega nadciągającemu bezpośredniemu zagrożeniu ich bezpieczeństwa. Jako że wykorzystywanie podatności w sektorze obronności może spowodować znaczne zakłócenia i szkody, cyberbezpieczeństwo przemysłu obronnego wymaga specjalnych środków w celu zapewnienia bezpieczeństwa łańcuchów dostaw, w szczególności w przypadku podmiotów znajdujących się na niższym poziomie w łańcuchu dostaw, które nie potrzebują dostępu do informacji niejawnych, ale mogą stanowić poważne zagrożenie dla całego sektora. Szczególną uwagę należy zwrócić na skutki, jakie może wywrzeć każde naruszenie, oraz na zagrożenie ewentualną manipulacją danymi sieciowymi, która mogłaby sprawić, że krytyczne zasoby obronne staną się bezużyteczne, a nawet przestawieniem systemów operacyjnych na sterowanie ręczne, co uczyniłoby je podatnymi na przechwycenie.

Poprawka 39

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 1 – litera b a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	bb) wspiera wzmacnianie zdolności obronnych uczestniczących w niej członków lub zapobiega zbliżającemu się bezpośredniemu zagrożeniu ich bezpieczeństwa, zapewniając bezpieczeństwo łańcuchów dostaw, w szczególności w przypadku podmiotów znajdujących się na niższym poziomie w łańcuchu dostaw, które nie potrzebują dostępu do informacji niejawnych, ale mogą stanowić poważne zagrożenie dla

całego sektora.

Poprawka 40

Wniosek dotyczący rozporządzenia
Artykuł 7 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. W przypadku gdy transgraniczne SOC uzyskają informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, bez zbędnej zwłoki przekazują istotne informacje EU-CyCLONe, sieci CSIRT i Komisji, biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555.	1. W przypadku gdy transgraniczne SOC uzyskają informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, bez zbędnej zwłoki przekazują istotne informacje EU-CyCLONe, sieci CSIRT i Komisji ***– w tym wysokiemu przedstawicielowi i ESDZ**, **jeśli incydent ten dotyczy państw trzecich –*** biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555.

Poprawka 41

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają wysoki poziom bezpieczeństwa danych i bezpieczeństwa fizycznego infrastruktury europejskiej tarczy cyberbezpieczeństwa oraz zapewniają, aby infrastruktura ta była odpowiednio zarządzana i kontrolowana w taki sposób, aby chronić ją przed zagrożeniami oraz zapewnić bezpieczeństwo jej i systemów, w ***tym bezpieczeństwo*** danych wymienianych za pośrednictwem tej infrastruktury.	1. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają wysoki poziom bezpieczeństwa danych i bezpieczeństwa fizycznego infrastruktury europejskiej tarczy cyberbezpieczeństwa oraz zapewniają, aby infrastruktura ta była odpowiednio zarządzana i kontrolowana w taki sposób, aby chronić ją przed zagrożeniami oraz zapewnić bezpieczeństwo jej i systemów, ***zmniejszając ryzyko i wspierając przewagę technologiczną UE*** w ***sektorach krytycznych, również dzięki działaniom zmierzającym do ograniczenia lub wykluczenia dostawców wysokiego ryzyka oraz ochrony bezpieczeństwa*** danych wymienianych za pośrednictwem tej

infrastruktury.

Poprawka 42

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają, aby wymiana informacji w ramach europejskiej tarczy cyberbezpieczeństwa z podmiotami, które nie są podmiotami publicznymi państw członkowskich, nie wpływała negatywnie na interesy Unii w zakresie bezpieczeństwa.	2. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają, aby wymiana informacji w ramach europejskiej tarczy cyberbezpieczeństwa z podmiotami, które nie są podmiotami publicznymi państw członkowskich, nie wpływała negatywnie na interesy Unii w zakresie bezpieczeństwa ***i aby wymiana informacji z dostawcami wysokiego ryzyka odbywała się w ograniczonym zakresie i nie zagrażała bezpieczeństwu i strategicznym interesom Unii***.

Poprawka 43

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Komisja może przyjąć akty wykonawcze określające wymogi techniczne dla państw członkowskich w celu wypełnienia ich obowiązku wynikającego z ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia. Przyjmując te akty, Komisja, wspierana przez wysokiego przedstawiciela, uwzględnia odpowiednie normy bezpieczeństwa na poziomie obronnym, aby ułatwić współpracę z podmiotami wojskowymi.	3. Komisja może przyjąć akty wykonawcze określające wymogi techniczne dla państw członkowskich w celu wypełnienia ich obowiązku wynikającego z ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia. Przyjmując te akty, Komisja, wspierana przez wysokiego przedstawiciela, uwzględnia odpowiednie normy bezpieczeństwa na poziomie obronnym, aby ułatwić współpracę z podmiotami wojskowymi***, korzystając przy tym odpowiednio z całego szeregu opcji obronnych dostępnych dla społeczności cywilnych i wojskowych działających na***

	rzecz wzmocnienia bezpieczeństwa i obrony UE, oraz informuje Parlament Europejski.

Poprawka 44

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Działania służące wdrażaniu mechanizmu cyberkryzysowego wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3**.**	2. Działania służące wdrażaniu mechanizmu cyberkryzysowego wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3***, oraz ze środków Europejskiego Instrumentu na rzecz Pokoju (EPF) w przypadku środków pomocy stosowanych wobec państw trzecich, w szczególności Ukrainy i Mołdawii;***

Poprawka 45

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych w całej Unii;	a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych***, takich jak infrastruktura publiczna, infrastruktura wyborcza, transport, opieka zdrowotna, finanse, telekomunikacja, zaopatrzenie*** w ***żywność i bezpieczeństwo w*** całej Unii;

Poprawka 46

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) działania w zakresie wzajemnej pomocy polegające na udzielaniu pomocy przez organy krajowe jednego państwa członkowskiego innemu państwu członkowskiemu, w szczególności zgodnie z art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555.	c) działania w zakresie wzajemnej pomocy polegające na udzielaniu pomocy przez organy krajowe jednego państwa członkowskiego innemu państwu członkowskiemu, w szczególności zgodnie z art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555 ***i w kontekście art. 42 ust. 7 TUE i art. 222 TFUE;***

Poprawka 47

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ca) wymiana i stopniowe wycofywanie krytycznego sprzętu od dostawców wysokiego ryzyka, którzy naruszaliby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE.

Poprawka 48

Wniosek dotyczący rozporządzenia
Artykuł 11 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Grupa współpracy NIS we współpracy z Komisją, ENISA ***i*** wysokim przedstawicielem opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania.	2. Grupa współpracy NIS we współpracy z Komisją, ENISA**,** wysokim przedstawicielem***, ESDZ i, w stosownych przypadkach, EDA*** opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania.

Poprawka 49

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Unijna rezerwa cyberbezpieczeństwa składa się z usług reagowania na incydenty świadczonych przez zaufanych dostawców wybranych zgodnie z kryteriami określonymi w art. 16. Rezerwa obejmuje wcześniej zadeklarowane usługi. Usługi te muszą być możliwe do wprowadzenia we wszystkich państwach członkowskich.	2. Unijna rezerwa cyberbezpieczeństwa składa się z usług reagowania na incydenty świadczonych przez zaufanych dostawców wybranych zgodnie z kryteriami określonymi w art. 16. Rezerwa obejmuje wcześniej zadeklarowane usługi. Usługi te muszą być możliwe do wprowadzenia we wszystkich państwach członkowskich ***i państwach trzecich spełniających stosowne wymogi niniejszego rozporządzenia***.

Poprawka 50

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 3 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) instytucje, organy i jednostki organizacyjne Unii.	b) instytucje, organy i jednostki organizacyjne Unii***, w tym misje WPBiO***.

Poprawka 51

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Użytkownicy, o których mowa w ust. 3 lit. a), korzystają z usług z unijnej rezerwy cyberbezpieczeństwa, aby reagować lub wspierać reagowanie na poważne incydenty lub incydenty na dużą skalę mające wpływ na podmioty działające w sektorach krytycznych lub wysoce krytycznych oraz aby natychmiast usuwać skutki takich incydentów.	4. Użytkownicy, o których mowa w ust. 3 lit. a), korzystają z usług z unijnej rezerwy cyberbezpieczeństwa, aby reagować lub wspierać reagowanie na poważne incydenty lub incydenty na dużą skalę mające wpływ na podmioty działające w sektorach krytycznych lub wysoce krytycznych***, takich jak infrastruktura publiczna, infrastruktura wyborcza, transport, opieka zdrowotna, finanse, telekomunikacja, zaopatrzenie w żywność i bezpieczeństwo,*** oraz aby natychmiast usuwać skutki takich incydentów.

Poprawka 52

Wniosek dotyczący rozporządzenia
Artykuł 12 − ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja decyduje o priorytetach i rozwoju unijnej rezerwy cyberbezpieczeństwa zgodnie z wymogami użytkowników, o których mowa w ust. 3, i nadzoruje jej wdrażanie oraz zapewnia komplementarność, spójność, synergię i powiązania z innymi działaniami wspierającymi prowadzonymi na podstawie niniejszego rozporządzenia, a także z innymi działaniami i ***programami*** unijnymi.	5. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja decyduje o priorytetach i rozwoju unijnej rezerwy cyberbezpieczeństwa zgodnie z wymogami użytkowników, o których mowa w ust. 3, i nadzoruje jej wdrażanie oraz zapewnia komplementarność, spójność, synergię i powiązania z innymi działaniami wspierającymi prowadzonymi na podstawie niniejszego rozporządzenia, a także z innymi działaniami***, programami*** i ***celami*** unijnymi***, zwłaszcza strategicznym celem w postaci zmniejszenia uzależnienia od dostawców wysokiego ryzyka, którzy naruszaliby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE***.

Poprawka 53

Wniosek dotyczący rozporządzenia
Artykuł 12 − ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, po konsultacji z państwami członkowskimi i Komisją. ENISA przygotowuje podobne zestawienie, po konsultacji z Komisją, w celu określenia potrzeb państw trzecich kwalifikujących się do wsparcia z unijnej rezerwy cyberbezpieczeństwa zgodnie z art. 17. W stosownych przypadkach Komisja	7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, po konsultacji z państwami członkowskimi i Komisją. ENISA przygotowuje podobne zestawienie, po konsultacji z Komisją ***i przy wsparciu ESDZ***, w celu określenia potrzeb państw trzecich kwalifikujących się do wsparcia z unijnej rezerwy cyberbezpieczeństwa zgodnie z art. 17. W stosownych

konsultuje się z wysokim przedstawicielem.	przypadkach Komisja konsultuje się z wysokim przedstawicielem.

Poprawka 54

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 2 – litera a a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	aa) wpływ incydentu na bezpieczeństwo i obronę Unii;

Poprawka 55

Wniosek dotyczący rozporządzenia
Artykuł 15 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. W porozumieniu z wysokim przedstawicielem wsparcie w ramach mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty. Może ono również uzupełniać pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub wnosić wkład w taką pomoc w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej.	3. W porozumieniu z wysokim przedstawicielem wsparcie w ramach mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty***(CRRTs), by w ten sposób lepiej wspierać państwa członkowskie UE, misje i operacje WPBiO oraz państwa trzecie, które w swoich działaniach na rzecz budowania zdolności w zakresie cyberobrony przestrzegają zasad wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony UE, w szczególności Ukrainę i Mołdawię***. Może ono również uzupełniać pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub wnosić wkład w taką pomoc w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej.

Poprawka 56

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera b a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	aa) dostawca musi wykazać, że jego struktury decyzyjne i zarządcze są wolne od wszelkich bezprawnych wpływów ze strony rządów państw, które to wpływy naruszałyby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE;

Poprawka 57

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) dostawca musi być wyposażony w sprzęt i oprogramowanie techniczne niezbędne do obsługi żądanej usługi;	f) dostawca musi być wyposażony w sprzęt i oprogramowanie techniczne niezbędne do obsługi żądanej usługi ***oraz spełniać wymogi określone w art. X rozporządzenia XX/XXXX (akt dotyczący cyberodporności)***;

Poprawka 58

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera j a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ja) nie należy dopuszczać żadnego dostawcy pochodzącego z państwa trzeciego wysokiego ryzyka.

Poprawka 59

Wniosek dotyczący rozporządzenia
Artykuł 2 – ustęp 2 – litera j b (nowa)

Tekst proponowany przez Komisję	*Poprawka*

	jb) dostawca musi w miarę możliwości ściśle współpracować z odpowiednimi MŚP;

Poprawka 60

Wniosek dotyczący rozporządzenia
Artykuł 17 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa trzecie mogą wystąpić z wnioskiem o wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli ***przewidują to układy o stowarzyszeniu zawarte w związku z uczestnictwem tych państw w programie „Cyfrowa Europa”.***	1. Państwa trzecie mogą wystąpić z wnioskiem o wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli***:***
	a) przewidują to układy o stowarzyszeniu zawarte w związku z uczestnictwem tych państw w programie „Cyfrowa Europa”;
	b) w tych państwach trzecich prowadzona jest misja WPBiO mająca za zadanie wzmocnienie odporności na zagrożenia hybrydowe, w tym cyberzagrożenia, lub zastosowano w nich środek pomocy EPF w celu wzmocnienia cyberodporności państwa.

Poprawka 61

Wniosek dotyczący rozporządzenia
Artykuł 17 − ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Wsparcie z unijnej rezerwy cyberbezpieczeństwa musi być zgodne z niniejszym rozporządzeniem i z wszelkimi szczegółowymi warunkami określonymi w układach o stowarzyszeniu, o których mowa w ust. 1.	2. Wsparcie z unijnej rezerwy cyberbezpieczeństwa musi być zgodne z niniejszym rozporządzeniem i z wszelkimi szczegółowymi warunkami określonymi w układach o stowarzyszeniu, o których mowa w ust. 1***, z wyjątkiem państw trzecich objętych przepisami ust. 1 lit. b)***.

Poprawka 62

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA dokonuje przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA przekazuje sieci CSIRT, EU-CyCLONe i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań, w szczególności w świetle zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. ***W stosownych*** przypadkach Komisja udostępnia sprawozdanie to wysokiemu przedstawicielowi.	1. Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA dokonuje przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA przekazuje sieci CSIRT, EU-CyCLONe i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań, w szczególności w świetle zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. ***W stosownych*** przypadkach***, a zwłaszcza gdy incydent dotyczy państwa trzeciego,*** Komisja udostępnia sprawozdanie to wysokiemu przedstawicielowi ***i ESDZ***.

Poprawka 63

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Sprawozdanie jest udostępniane Parlamentowi Europejskiemu zgodnie z prawem unijnym lub krajowym dotyczącym ochrony szczególnie chronionych informacji niejawnych.

Poprawka 64

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 1 – litera a – punkt 1
Rozporządzenie (UE) 2021/694
Artykuł 6 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
aa) wspieraniu rozwoju europejskiej tarczy cyberbezpieczeństwa, w tym rozwijaniu, wprowadzaniu i eksploatacji platform krajowych i transgranicznych SOC, które wnoszą wkład w orientację sytuacyjną w Unii oraz w zwiększanie unijnych zdolności wywiadowczych w zakresie cyberzagrożeń;	aa) wspieraniu rozwoju europejskiej tarczy cyberbezpieczeństwa, w tym rozwijaniu, wprowadzaniu i eksploatacji platform krajowych i transgranicznych SOC, które wnoszą wkład w orientację sytuacyjną w Unii oraz w zwiększanie unijnych zdolności wywiadowczych w zakresie cyberzagrożeń ***i zmniejszanie uzależnienia Unii od dostawców wysokiego ryzyka dostarczających krytyczne urządzenia i komponenty z zakresu cyberbepieczeństwa, które naruszałyby interesy Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE***;

Poprawka 65

Wniosek dotyczący rozporządzenia
Artykuł 20 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
Do dnia ***[cztery*** lata od daty rozpoczęcia stosowania niniejszego ***rozporządzenia]*** r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia.	Do dnia ***[trzy*** lata od daty rozpoczęcia stosowania niniejszego ***rozporządzenia, a następnie co dwa lata]*** r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia.

PROCEDURA W KOMISJI OPINIODAWCZEJ

Tytuł	Ustanowienie środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty
Odsyłacze	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 1.6.2023
Opinia wydana przez Data ogłoszenia na posiedzeniu	AFET 1.6.2023
Sprawozdawca(czyni) komisji opiniodawczej Data powołania	Dragoş Tudorache 16.6.2023
Rozpatrzenie w komisji	18.9.2023
Data przyjęcia	24.10.2023
Wynik głosowania końcowego	+: 39 –: 4 0: 0
Posłowie obecni podczas głosowania końcowego	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Zastępcy obecni podczas głosowania końcowego	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się