Parlament Europejski
2019–2024

Komisja Przemysłu, Badań Naukowych i Energii

2023/0109(COD)

22.9.2023

POPRAWKI
46 - 216

Projekt sprawozdania
Lina Gálvez Muñoz
(PE752.795v01-00)

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

Wniosek dotyczący rozporządzenia
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Poprawka 46
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Tytuł 1

Tekst proponowany przez Komisję	*Poprawka*
Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY ustanawiające 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	Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY ustanawiające 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 ***(akt w sprawie cybersolidarności)***

Or. en

Poprawka 47
Ville Niinistö
w imieniu grupy Verts/ALE

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 ***i stanowią obszar podatny na zagrożenia*** 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.

Or. en

Uzasadnienie

Potrzeba wprowadzenia tej zmiany wynika z faktu, że podstawowe zależności wiążą się również z podatnością na zagrożenia.

Poprawka 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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	(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 ***w całej Unii*** 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 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.	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. ***W związku z tym w celu poprawy stanu cyberbezpieczeństwa Unii konieczna jest ścisła i skoordynowana współpraca między sektorem publicznym, sektorem prywatnym, państwami członkowskimi, instytucjami lub agencjami Unii oraz środowiskiem naukowym. Unia powinna reagować we współpracy z zaufanymi partnerami międzynarodowymi o podobnych poglądach i instytucjami międzynarodowymi oraz w sposób zgodny z ramami i umowami współpracy międzynarodowej.***
	Or. en

Poprawka 49
Ville Niinistö
w imieniu grupy Verts/ALE

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	(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 ***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.	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 ***oraz*** ze środowiskami przestępczymi, 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.

Or. en

Uzasadnienie

Ogólne uwzględnienie haktywizmu jako działań przestępczych nie odzwierciedla różnorodności takich działań, w tym zgodnych z prawem protestów i informowania o nieprawidłowościach. W tekście należy unikać nieścisłości i zapewnić ochronę działań zgodnych z prawem.

Poprawka 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

Wniosek dotyczący rozporządzenia
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(3) Konieczne jest wzmocnienie	(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.

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***, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (MŚP),*** i podmiotów obsługujących infrastrukturę krytyczną***, w tym organów lokalnych lub regionalnych,*** na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastruktury***,*** usługi ***i wysoko wykwalifikowany personel dysponujący niezbędnymi umiejętnościami***, 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***, również poprzez aktywne gromadzenie danych wywiadowczych***. Unia powinna również zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie gromadzenia i analizy danych dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie. ***[1] https://futureu.europa.eu/en/***

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

Or. en

Poprawka 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Coraz większe ryzyko w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń, w tym również wyraźne ryzyko szybkiego rozprzestrzeniania się incydentów w cyberbezpieczeństwie z jednego państwa członkowskiego na inne oraz z państwa trzeciego na Unię, wymagają większej solidarności na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie. W konkluzjach Rady o pozycji UE w kwestiach cyberprzestrzeni[21] państwa członkowskie wezwały również Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.	(5) Coraz większe ryzyko w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń, w tym również wyraźne ryzyko szybkiego rozprzestrzeniania się incydentów w cyberbezpieczeństwie z jednego państwa członkowskiego na inne oraz z państwa trzeciego na Unię, wymagają większej solidarności na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie***, a także skuteczniej usuwać ich skutki***. W konkluzjach Rady o pozycji UE w kwestiach cyberprzestrzeni[21] państwa członkowskie wezwały również Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.
[21] Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. (9364/22).	[21] Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. (9364/22).

Or. en

Poprawka 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 9 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(9a) W kontekście zmian geopolitycznych i rosnącego zagrożenia

cyberbezpieczeństwa duże znaczenie ma ciągłość i dalszy rozwój środków określonych w niniejszym rozporządzeniu, w szczególności europejskiej tarczy cybernetycznej i europejskiego mechanizmu cyberkryzysowego. W tym celu konieczne jest zapewnienie specjalnej linii budżetowej w wieloletnich ramach finansowych na lata 2028–2034. Państwa członkowskie powinny również zobowiązać się do wspierania wszelkich niezbędnych środków służących zwiększeniu solidarności w Unii oraz ograniczeniu cyberzagrożeń i cyberincydentów w całej Unii.

Or. en

Poprawka 53
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 12

Tekst proponowany przez Komisję	*Poprawka*
(12) Aby skuteczniej zapobiegać cyberzagrożeniom i cyberincydentom, oceniać je ***i*** reagować na nie, należy zdobyć bardziej kompleksową wiedzę na temat zagrożeń dla aktywów i infrastruktur krytycznych na terytorium Unii, w tym na temat ich rozmieszczenia geograficznego, wzajemnych połączeń i potencjalnych skutków w przypadku cyberataków mających wpływ na te infrastruktury. Należy wprowadzić wielkoskalową unijną infrastrukturę SOC („europejską tarczę cyberbezpieczeństwa”), składającą się z kilku interoperacyjnych platform transgranicznych, z których każda zrzesza kilka krajowych SOC. Infrastruktura ta powinna służyć krajowym i unijnym interesom i potrzebom w zakresie cyberbezpieczeństwa, wykorzystując najnowocześniejszą technologię	(12) Aby skuteczniej zapobiegać cyberzagrożeniom i cyberincydentom, oceniać je***,*** reagować na nie ***oraz usuwać ich skutki***, należy zdobyć bardziej kompleksową wiedzę na temat zagrożeń dla aktywów i infrastruktur krytycznych na terytorium Unii, w tym na temat ich rozmieszczenia geograficznego, wzajemnych połączeń i potencjalnych skutków w przypadku cyberataków mających wpływ na te infrastruktury***, również poprzez aktywne gromadzenie danych wywiadowczych***. Należy wprowadzić wielkoskalową unijną infrastrukturę SOC („europejską tarczę cyberbezpieczeństwa”), składającą się z kilku interoperacyjnych platform transgranicznych, z których każda zrzesza kilka krajowych SOC. ***Krajowe SOC to scentralizowane jednostki odpowiedzialne***

zaawansowanego gromadzenia danych i narzędzia analityki, zwiększając zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz zapewniając orientację sytuacyjną w czasie rzeczywistym. Infrastruktura ta powinna służyć lepszemu wykrywaniu zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie, a tym samym uzupełniać i wspierać unijne podmioty i sieci odpowiedzialne za zarządzanie kryzysowe w Unii, w szczególności europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe”), zdefiniowaną w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555[24].	***za stałe gromadzenie danych wywiadowczych na temat zagrożeń oraz poprawę stanu cyberbezpieczeństwa podmiotów podlegających krajowej jurysdykcji poprzez zapobieganie zagrożeniom cyberbezpieczeństwa oraz ich wykrywanie i analizowanie.*** Infrastruktura ta powinna służyć krajowym i unijnym interesom i potrzebom w zakresie cyberbezpieczeństwa, wykorzystując najnowocześniejszą technologię zaawansowanego gromadzenia danych i narzędzia analityki, zwiększając zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz zapewniając orientację sytuacyjną w czasie rzeczywistym. Infrastruktura ta powinna służyć lepszemu wykrywaniu zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie, a tym samym uzupełniać i wspierać unijne podmioty i sieci odpowiedzialne za zarządzanie kryzysowe w Unii, w szczególności europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe”), zdefiniowaną w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555[24].
[24] 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 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).	[24] 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 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

Or. en

Poprawka 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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.	(13) ***Aby uczestniczyć w europejskiej tarczy cyberbezpieczeństwa,*** każde państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń ***i wymiany informacji*** w tym państwie członkowskim. ***Zdecydowanie zachęca się państwa członkowskie do włączenia zdolności krajowych SOC do już istniejącej struktury cyberbezpieczeństwa i zarządzania cyberbezpieczeństwem, aby nie tworzyć dodatkowych warstw zarządzania i dostosować akt w sprawie cybersolidarności do już istniejącego prawodawstwa, w tym dyrektywy (UE) 2022/2555.*** Te krajowe SOC powinny pełnić funkcję punktu odniesienia i punktu dostępu na szczeblu krajowym do celów uczestnictwa ***podmiotów prywatnych i publicznych, w szczególności ich SOC,*** 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. ***Krajowe SOC powinny wzmacniać współpracę i wymianę informacji między podmiotami publicznymi i prywatnymi, aby przełamać sztywne struktury komunikacyjne. W ten sposób mogą wspierać tworzenie modeli wymiany danych oraz powinny ułatwiać i promować wymianę informacji w zaufanym i bezpiecznym środowisku. Ścisła i skoordynowana współpraca między podmiotami publicznymi i prywatnymi ma kluczowe znaczenie dla zwiększenia odporności Unii w obszarze cyberbezpieczeństwa.***

Or. en

Poprawka 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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***.	(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 im, wspieranie ***aktywnego*** 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. ***Transgraniczne SOC powinny ułatwiać i promować wymianę informacji w zaufanym i bezpiecznym środowisku. ENISA powinna wspierać transgraniczne SOC w kwestiach związanych ze współpracą operacyjną.*** Powinny one zapewnić nowe dodatkowe zdolności, ***a jednocześnie powinny zostać włączone do już istniejącej infrastruktury cyberbezpieczeństwa, w tym SOC i zespołów*** reagowania na incydenty komputerowe („CSIRT") ***oraz*** innych

odpowiednich ***podmiotów***.

Or. en

Poprawka 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 zdolności i suwerenności technologicznej Unii.	(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 ***włączona do istniejącej już infrastruktury cyberbezpieczeństwa, w szczególności*** sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych***, w szczególności ich SOC,*** 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 ***w celu zwiększenia odporności Unii***.

Or. en

Poprawka 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 zdolności ***suwerenności technologicznej*** Unii.	(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 ***znaczącego ekosystemu cyberbezpieczeństwa zapewniającego znaczne*** zdolności Unii ***oraz współpracy z partnerami o podobnych poglądach***.

Or. en

Poprawka 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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.

(„ISAC”), operatorów infrastruktury krytycznej)***, aby ułatwić przełamanie sztywnych struktur komunikacyjnych***. ***W ten sposób transgraniczne SOC mogłyby również wspierać tworzenie modeli wymiany danych w całej Unii.*** Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze o zagrożeniach, ***informacje zebrane w ramach aktywnego gromadzenia danych wywiadowczych,*** 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.

Or. en

Poprawka 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	(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 ***przeanalizowane*** dane z sieci***,*** czujników, ***logowania i telemetrii,*** dane wywiadowcze o zagrożeniach, oznaki naruszenia

na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.	integralności oraz informacje kontekstowe na temat ***taktyk, technik i procedur,*** incydentów, ***przypadków złośliwego oprogramowania,*** zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.

Or. en

Poprawka 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 17

Tekst proponowany przez Komisję	*Poprawka*
(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	(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 oraz potencjalnie poufny charakter wymienianych informacji.	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 ***zgodnie z obowiązującymi już przepisami dyrektywy (UE) 2022/2555***. 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 oraz potencjalnie poufny charakter wymienianych informacji.

Or. en

Poprawka 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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.	wysoce bezpieczne narzędzia, sprzęt i infrastruktury ***oraz zatrudniać wysoko wykwalifikowany personel***. 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.

Or. en

Poprawka 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 rozporządzeniem Rady (UE) 2021/1173[25].	(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 zwrócić jednak uwagę, że sztuczna inteligencja jest najbardziej skuteczna w połączeniu z analizą dokonywaną przez człowieka. W związku z tym wysoko wykwalifikowany personel ma zasadnicze znaczenie w kontekście zbierania wysokiej jakości danych i aktywnego gromadzenia danych wywiadowczych na temat zagrożeń.*** Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173[25].
[25] Rozporządzenie Rady (UE) 2021/1173	[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).

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).

Or. en

Poprawka 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 rozporządzeniem Rady (UE) 2021/1173[25].	(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna ***wzmocnić znaczący ekosystem cyberbezpieczeństwa*** 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 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).

Or. en

Poprawka 64
Ville Niinistö

w imieniu grupy Verts/ALE

Wniosek dotyczący rozporządzenia
Motyw 21

Tekst proponowany przez Komisję	*Poprawka*
(21) Chociaż europejska tarcza cyberbezpieczeństwa jest projektem cywilnym, społeczność zajmująca się cyberobroną mogłaby skorzystać na poprawie cywilnych zdolności w zakresie wykrywania i orientacji sytuacyjnej do celów ochrony infrastruktury krytycznej. Transgraniczne SOC, przy wsparciu Komisji i Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) oraz we współpracy z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa („wysoki przedstawiciel”), powinny stopniowo opracowywać specjalne protokoły i standardy, aby umożliwić współpracę ze społecznością zajmującą się cyberobroną, w tym warunki weryfikacji i bezpieczeństwa. Rozwojowi europejskiej tarczy cyberbezpieczeństwa powinna towarzyszyć refleksja umożliwiająca przyszłą współpracę z sieciami i platformami odpowiedzialnymi za wymianę informacji w społeczności zajmującej się cyberobroną, w ścisłej współpracy z wysokim przedstawicielem.	(21) Chociaż europejska tarcza cyberbezpieczeństwa jest projektem cywilnym, społeczność zajmująca się cyberobroną mogłaby skorzystać na poprawie cywilnych zdolności w zakresie wykrywania i orientacji sytuacyjnej do celów ochrony infrastruktury krytycznej. Transgraniczne SOC, przy wsparciu Komisji i Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) oraz we współpracy z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa („wysoki przedstawiciel”), powinny stopniowo opracowywać specjalne protokoły i standardy ***dotyczące warunków dostępu i zabezpieczeń***, aby umożliwić współpracę ze społecznością zajmującą się cyberobroną, w tym warunki weryfikacji i bezpieczeństwa***, z poszanowaniem cywilnego charakteru instytucji i przeznaczenia środków finansowych, a zatem z wykorzystaniem środków udostępnianych społeczności zajmującej się obroną***. Rozwojowi europejskiej tarczy cyberbezpieczeństwa powinna towarzyszyć refleksja umożliwiająca przyszłą współpracę z sieciami i platformami odpowiedzialnymi za wymianę informacji w społeczności zajmującej się cyberobroną, w ścisłej współpracy z wysokim przedstawicielem ***i przy pełnym poszanowaniu praw i wolności***.

Or. en

Uzasadnienie

Zgodnie z ideą unikania powielania działań i zapewnienia poszanowania praw i wolności współpraca między cywilnymi i obronnymi aspektami cyberbezpieczeństwa musi opierać się na zabezpieczeniach, dzięki czemu możliwe będzie uniknięcie zmiany przeznaczenia środków

udostępnianych na cele cywilne.

Poprawka 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 24

Tekst proponowany przez Komisję	*Poprawka*
(24) W związku z rosnącym ryzykiem i rosnącą liczbą cyberincydentów mających wpływ na państwa członkowskie konieczne jest ustanowienie instrumentu wsparcia kryzysowego, aby poprawić odporność Unii na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz uzupełnić działania państw członkowskich wsparciem finansowym w sytuacjach nadzwyczajnych na potrzeby gotowości, reagowania i natychmiastowego przywrócenia funkcjonowania usług kluczowych. Instrument ten powinien umożliwiać szybkie wdrażanie pomocy w określonych okolicznościach i na jasnych warunkach oraz uważne monitorowanie i wnikliwą ocenę sposobu wykorzystania zasobów. O ile podstawowa odpowiedzialność za zapobieganie incydentom i kryzysom w cyberbezpieczeństwie spoczywa na państwach członkowskich, mechanizm cyberkryzysowy propaguje solidarność między państwami członkowskimi zgodnie z art. 3 ust. 3 Traktatu o Unii Europejskiej („Traktat UE”).	(24) W związku z rosnącym ryzykiem i rosnącą liczbą cyberincydentów mających wpływ na państwa członkowskie konieczne jest ustanowienie instrumentu wsparcia kryzysowego, aby poprawić odporność Unii na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz uzupełnić działania państw członkowskich wsparciem finansowym w sytuacjach nadzwyczajnych na potrzeby gotowości, reagowania i natychmiastowego przywrócenia funkcjonowania usług kluczowych. Instrument ten powinien umożliwiać szybkie ***i skuteczne*** wdrażanie pomocy w określonych okolicznościach i na jasnych warunkach oraz uważne monitorowanie i wnikliwą ocenę sposobu wykorzystania zasobów. O ile podstawowa odpowiedzialność za zapobieganie incydentom i kryzysom w cyberbezpieczeństwie spoczywa na państwach członkowskich, mechanizm cyberkryzysowy propaguje solidarność między państwami członkowskimi zgodnie z art. 3 ust. 3 Traktatu o Unii Europejskiej („Traktat UE”).

Or. en

Poprawka 66
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 27

Tekst proponowany przez Komisję	*Poprawka*
(27) Wsparcie udzielane na podstawie niniejszego rozporządzenia powinno wspomagać i uzupełniać działania podejmowane przez państwa członkowskie na szczeblu krajowym. W tym celu należy zapewnić ścisłą współpracę i konsultacje między Komisją ***a*** zainteresowanym państwem członkowskim. Wnioskując o wsparcie w ramach mechanizmu cyberkryzysowego, państwo członkowskie powinno przedstawić odpowiednie informacje uzasadniające potrzebę wsparcia.	(27) Wsparcie udzielane na podstawie niniejszego rozporządzenia powinno wspomagać i uzupełniać działania podejmowane przez państwa członkowskie na szczeblu krajowym. W tym celu należy zapewnić ścisłą współpracę i konsultacje między Komisją***, ENISA i*** zainteresowanym państwem członkowskim. Wnioskując o wsparcie w ramach mechanizmu cyberkryzysowego, państwo członkowskie powinno przedstawić odpowiednie informacje uzasadniające potrzebę wsparcia.

Or. en

Poprawka 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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	(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***, a jednocześnie zwiększyć odporność i konkurencyjność Unii, w tym udział europejskich dostawców usług zarządzanych w zakresie bezpieczeństwa będących MŚP. Zaufani dostawcy, w tym***

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.	***MŚP, powinni móc współpracować ze sobą w celu spełnienia powyższych kryteriów***. 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. ***W miarę możliwości usługi te powinny opierać się na najnowocześniejszych technologiach, w tym chmurze i sztucznej inteligencji. W związku z tym rezerwa na cyberbezpieczeństwo powinna zapewniać zachęty do inwestowania w badania naukowe i innowacje pobudzające rozwój tych technologii. W stosownych przypadkach można przeprowadzić wspólne ćwiczenia z udziałem zaufanych dostawców i potencjalnych użytkowników rezerwy cyberbezpieczeństwa, aby w razie potrzeby zapewnić skuteczne funkcjonowanie rezerwy.*** 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.

Or. en

Poprawka 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 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.	(33) Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, ***której początkowe finansowanie na podstawie niniejszego rozporządzenia będzie wynosić 10 mln EUR do czasu przeprowadzenia oceny. Rezerwa składa*** 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. ***Komisja zapewnia, aby podobne inicjatywy nie były powielane w ramach NATO.***

Or. en

Uzasadnienie

Komisja przewiduje „stopniowe tworzenie” rezerwy, przy czym nie znajduje to odzwierciedlenia w pozostałej części proponowanego rozporządzenia. W związku z tym w niniejszej poprawce proponuje się zmniejszenie początkowego budżetu rezerwy z 36 mln do 10 mln EUR do czasu przeprowadzenia oceny przedmiotowego rozporządzenia. Spowoduje to zwrot 26 mln EUR do budżetu programu „Cyfrowa Europa” – cel specjalny nr 4 dotyczący zaawansowanych umiejętności cyfrowych (z 35 mln EUR pobranych z tego programu). Tworzenie unijnej rezerwy cyberbezpieczeństwa przy istniejącej rezerwie

cyberbezpieczeństwa NATO wiąże się z wysokim ryzykiem powielania działań i nie powinno odbywać się kosztem większych inwestycji w rozwój i przyciąganie talentów w dziedzinie cyberbezpieczeństwa w Europie.

Poprawka 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 35

Tekst proponowany przez Komisję	*Poprawka*
(35) Aby wesprzeć tworzenie unijnej rezerwy cyberbezpieczeństwa, Komisja ***mogłaby rozważyć zwrócenie*** się do ENISA o przygotowanie propozycji programu certyfikacji na podstawie rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa w obszarach objętych mechanizmem cyberkryzysowym.	(35) Aby wesprzeć tworzenie unijnej rezerwy cyberbezpieczeństwa, Komisja ***powinna zwrócić*** się do ENISA o przygotowanie propozycji programu certyfikacji na podstawie rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa w obszarach objętych mechanizmem cyberkryzysowym.

Or. en

Poprawka 70
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Wniosek dotyczący rozporządzenia
Motyw 35 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(35a) W związku z dodatkowymi zadaniami przewidzianymi w niniejszym rozporządzeniu, jak również we [wniosku dotyczącym rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi] należy zapewnić ENISA niezbędne zasoby ludzkie i finansowe w ramach budżetu Unii.

Or. en

Poprawka 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 37 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(37a) W celu zapewnienia określonych usług w ramach unijnej rezerwy cyberbezpieczeństwa mogą być potrzebni dostawcy usług reagowania na incydenty z państw trzecich, w tym państw trzecich stowarzyszonych z programem „Cyfrowa Europa" lub członków NATO lub innych państw będącymi partnerami międzynarodowymi o podobnych poglądach. W celu zwiększenia odporności i suwerenności Unii oraz zapewnienia ochrony jej strategicznych aktywów, interesów lub bezpieczeństwa konieczne może być ograniczenie lub wykluczenie udziału podmiotów prawnych mających siedzibę w państwach niestowarzyszonych lub przez nie kontrolowanych.

Or. en

Poprawka 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 38 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(38a) Wysoko wykwalifikowany personel, który jest w stanie niezawodnie świadczyć odpowiednie usługi w zakresie cyberbezpieczeństwa zgodnie z najwyższymi standardami, jest niezbędny do skutecznego wdrożenia europejskiej

tarczy cyberbezpieczeństwa i mechanizmu cyberkryzysowego. W związku z tym niepokojący jest fakt, że Unia stoi w obliczu niedoboru talentów, charakteryzującego się brakiem wykwalifikowanych specjalistów, a jednocześnie musi stawić czoła szybko zmieniającemu się krajobrazowi zagrożeń, co potwierdzono w komunikacie Komisji z dnia 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Należy wyeliminować ten niedobór talentów poprzez wzmocnienie współpracy i koordynacji między różnymi zainteresowanymi stronami, w tym sektorem prywatnym, środowiskiem akademickim, państwami członkowskimi, Komisją i ENISA, w celu zwiększenia skali i stworzenia synergii w zakresie inwestycji w kształcenie i szkolenie, rozwoju partnerstw publiczno-prywatnych, wspierania inicjatyw w zakresie badań naukowych i innowacji, rozwoju i wzajemnego uznawania wspólnych norm i procedur certyfikacji dotyczących umiejętności w dziedzinie cyberbezpieczeństwa, w tym za pośrednictwem europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa. Działania te powinny również ułatwić mobilność specjalistów w dziedzinie cyberbezpieczeństwa w Unii. Celem niniejszego rozporządzenia powinno być wspieranie większej różnorodności siły roboczej w sektorze cyberbezpieczeństwa.

Or. en

Poprawka 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 38 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(38b) Budowanie zdolności państw członkowskich ma zasadnicze znaczenie dla skoordynowanego ogólnounijnego podejścia do zwiększania odporności stanu cyberbezpieczeństwa Unii. Jak podkreślono w komunikacie Komisji z dnia 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa, nie można zagwarantować bezpieczeństwa Unii bez udziału najcenniejszego zasobu UE: jej obywateli. Europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa mogą przyczynić się do lepszego zrozumienia struktury siły roboczej w Unii, z uwzględnieniem obecnych i wymaganych kompetencji w uczestniczących podmiotach.

Or. en

Poprawka 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 39

Tekst proponowany przez Komisję	*Poprawka*
(39) Cel niniejszego rozporządzenia można lepiej osiągnąć na poziomie Unii niż państw członkowskich. W związku z tym Unia może podjąć działania zgodnie z zasadami pomocniczości i proporcjonalności określonymi w art. 5 Traktatu o Unii Europejskiej. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,	(39) Cel niniejszego rozporządzenia***, jakim jest przełamanie sztywnych struktur komunikacyjnych i wzmocnienie zdolności Unii w zakresie zapobiegania cyberzagrożeniom, ich wykrywania, reagowania na nie oraz usuwania ich skutków,*** można lepiej osiągnąć na poziomie Unii niż państw członkowskich. W związku z tym Unia może podjąć działania zgodnie z zasadami pomocniczości i proporcjonalności określonymi w art. 5 Traktatu o Unii Europejskiej. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

Or. en

Poprawka 75
Nicola Danti

Wniosek dotyczący rozporządzenia
Motyw 39 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(39a) W związku z dodatkowymi zadaniami przewidzianymi w niniejszym rozporządzeniu, jak również we [wniosku dotyczącym rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi] należy zapewnić ENISA niezbędne zasoby ludzkie i finansowe w ramach budżetu Unii.

Or. en

Poprawka 76
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. Niniejszym rozporządzeniem ustanawia się środki mające na celu zwiększenie zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty, w szczególności przez następujące działania:	1. Niniejszym rozporządzeniem ustanawia się środki mające na celu zwiększenie zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty, ***przy jednoczesnym poszanowaniu faktu, że odpowiedzialność za zapewnienie bezpieczeństwa narodowego, w tym w cyberprzestrzeni, spoczywa wyłącznie na poszczególnych państwach członkowskich, zgodnie z art. 4 ust. 2 TUE,*** w szczególności przez

następujące działania:

Or. en

Poprawka 77
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) wprowadzenie ***ogólnoeuropejskiej infrastruktury*** centrów monitorowania bezpieczeństwa (***europejskiej tarczy cyberbezpieczeństwa***) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej;	a) ***wzmocnienie zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), q których mowa w art. 10 dyrektywy (UE) 2022/2555, i sieci CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555, oraz*** wprowadzenie centrów monitorowania bezpieczeństwa (***SOC***) w celu zbudowania i wzmocnienia ***krajowych i*** wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej ***(„europejska tarcza cyberbezpieczeństwa”)***;

Or. en

Poprawka 78
Evžen Tošenovský

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.	***skreśla się***

Or. en

Poprawka 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, w tym MŚP,*** i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w suwerenność technologiczną Unii w dziedzinie cyberbezpieczeństwa;

Or. en

Poprawka 80
Johan Nissinen

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 ***dobrowolnego*** 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;

Or. en

Poprawka 81
Johan Nissinen

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 w ramach programu „Cyfrowa Europa”;	b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie ***dobrowolnej współpracy*** 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”;

Or. en

Poprawka 82
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) zwiększenie odporności Unii i przyczynianie się do skutecznej reakcji poprzez przegląd i ocenę poważnych incydentów lub incydentów na dużą skalę, w tym wyciąganie wniosków i w stosownych przypadkach wydawanie zaleceń.	***skreśla się***

Or. en

Poprawka 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia

Artykuł 1 – ustęp 2 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ca) rozwijanie i doskonalenie umiejętności i kompetencji siły roboczej w sektorze cyberbezpieczeństwa w sposób skoordynowany poprzez współpracę z Akademią Umiejętności Cybernetycznych w celu zapewnienia szkoleń i możliwości z myślą o wyeliminowaniu niedoboru talentów w sektorze cyberbezpieczeństwa.

Or. en

Poprawka 84
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla głównej odpowiedzialności państw członkowskich za bezpieczeństwo narodowe, bezpieczeństwo publiczne oraz za zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie.	3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla głównej odpowiedzialności państw członkowskich za bezpieczeństwo narodowe, bezpieczeństwo publiczne oraz za zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie***, a także zapobiega niepotrzebnemu powielaniu obecnych inicjatyw***.

Or. en

Poprawka 85
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Niniejsze rozporządzenie pozostaje	3. Niniejsze rozporządzenie pozostaje

bez uszczerbku dla ***głównej odpowiedzialności państw członkowskich za bezpieczeństwo narodowe, bezpieczeństwo publiczne*** oraz ***za zapobieganie*** przestępstwom, ***prowadzenie*** postępowań w ich sprawie, ich ***wykrywanie*** i ***ściganie***.	bez uszczerbku dla ***wyłącznej kompetencji*** państw członkowskich ***w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego*** oraz ***zapobiegania*** przestępstwom, ***prowadzenia*** postępowań w ich sprawie, ich ***wykrywania*** i ***ścigania***.

Or. en

Poprawka 86
Nicola Danti

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Każdego roku Komisja, przy okazji przedstawiania projektu budżetu na kolejny rok, przedkłada szczegółową ocenę zadań ENISA przewidzianych w niniejszym rozporządzeniu oraz [wniosku dotyczącym rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi] i innych przepisach Unii, a także szczegółowo określa zasoby finansowe i ludzkie niezbędne do realizacji tych zadań.

Or. en

Poprawka 87
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1

Tekst proponowany przez Komisję	*Poprawka*
1) „transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”) oznacza	***skreśla się***

wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma zapobiegać cyberzagrożeniom i cyberincydentom oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;

Or. en

Poprawka 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1

Tekst proponowany przez Komisję	*Poprawka*
1) „transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”) oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma zapobiegać ***cyberzagrożeniom i cyberincydentom*** oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;	1) „transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”) oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma ***wykrywać i analizować cyberzagrożenia i*** zapobiegać ***incydentom*** oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;

Or. en

Poprawka 89
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1

Tekst proponowany przez Komisję	*Poprawka*
1) „transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”) oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma zapobiegać cyberzagrożeniom i cyberincydentom oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;	1) „transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”) oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma zapobiegać cyberzagrożeniom i cyberincydentom oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze ***dobrowolnej*** wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;

Or. en

Poprawka 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a) „centrum monitorowania bezpieczeństwa” („SOC”) oznacza scentralizowaną jednostkę, która może być wewnętrzna lub zewnętrzna,

odpowiedzialną za ciągłe monitorowanie i poprawę stanu cyberbezpieczeństwa danego podmiotu w celu zapobiegania zagrożeniom cyberbezpieczeństwa, ich wykrywania i analizowania oraz reagowania na nie;

Or. en

Poprawka 91
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a) „centrum monitorowania bezpieczeństwa" („SOC") oznacza centrum utworzone przez podmioty prywatne i publiczne lub organy krajowe, zajmujące się nieustannym monitorowaniem i analizowaniem sieci komunikacyjnych i systemów komputerowych w celu wykrywania włamań i anomalii w czasie rzeczywistym;

Or. en

Poprawka 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 1 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1b) „krajowe centrum monitorowania bezpieczeństwa" („krajowe SOC") oznacza scentralizowaną jednostkę odpowiedzialną za stałe gromadzenie danych wywiadowczych na temat zagrożeń oraz poprawę stanu cyberbezpieczeństwa podmiotów

	podlegających krajowej jurysdykcji poprzez zapobieganie zagrożeniom cyberbezpieczeństwa oraz ich wykrywanie i analizowanie, aby móc lepiej reagować na zagrożenia cyberbezpieczeństwa. W stosownych przypadkach jednostka ta jest włączona do już istniejących struktur krajowych, takich jak CSIRT, ustanowionych na podstawie dyrektywy (UE) 2022/2555;

Or. en

Poprawka 93
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – ustęp 1 – punkt 2

Tekst proponowany przez Komisję	*Poprawka*
2) „podmiot ***publiczny***” oznacza podmiot ***prawa publicznego*** zdefiniowany w art. ***2 ust. 1*** pkt ***4*** dyrektywy ***Parlamentu Europejskiego i Rady 2014/24/UE***[30];	2) „podmiot ***administracji publicznej***” oznacza podmiot ***administracji publicznej*** zdefiniowany w art. ***6*** pkt ***35*** dyrektywy ***(UE) 2022/2555***;
[30] Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).	

Or. en

Poprawka 94
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 3

Tekst proponowany przez Komisję	*Poprawka*
3) „konsorcjum przyjmujące” oznacza konsorcjum składające się z	***skreśla się***

państw uczestniczących, reprezentowanych przez krajowe SOC, które zgodziły się utworzyć narzędzia i infrastrukturę na potrzeby transgranicznego SOC i jego funkcjonowania oraz wnieść wkład w nabycie tych narzędzi i infrastruktury;

Or. en

Poprawka 95
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a) „postępowanie w przypadku incydentu" oznacza postępowanie w przypadku incydentu zgodnie z definicją w art. 6 pkt 8 dyrektywy (UE) 2022/2555;

Or. en

Poprawka 96
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 5 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5b) „ryzyko" oznacza ryzyko zdefiniowane w art. 6 pkt 9 dyrektywy (UE) 2022/2555;

Or. en

Poprawka 97
Evžen Tošenovský

Wniosek dotyczący rozporządzenia

Artykuł 2 – akapit 1 – punkt 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	6a) „poważne cyberzagrożenie” oznacza cyberzagrożenie zdefiniowane w art. 6 pkt 11 dyrektywy (UE) 2022/2555;

Or. en

Poprawka 98
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 9

Tekst proponowany przez Komisję	*Poprawka*
9) „gotowość” oznacza stan przygotowania i zdolności do zapewnienia skutecznego szybkiego reagowania na poważny incydent w cyberbezpieczeństwie lub incydent w cyberbezpieczeństwie na dużą skalę, który to stan jest osiągnięty w wyniku podjętych uprzednio działań w zakresie oceny ryzyka i monitorowania;	***skreśla się***

Or. en

Poprawka 99
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 10

Tekst proponowany przez Komisję	*Poprawka*
10) „reakcja” oznacza działanie w przypadku poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w trakcie takiego incydentu lub po nim w celu zaradzenia jego natychmiastowym i krótkoterminowym negatywnym skutkom;	***skreśla się***

Or. en

Poprawka 100
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 2 – akapit 1 – punkt 11

Tekst proponowany przez Komisję	*Poprawka*
11) „zaufani dostawcy” oznaczają dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w art. 6 pkt 40 dyrektywy (UE) 2022/2555, wybranych zgodnie z art. 16 niniejszego rozporządzenia.	11) „zaufani dostawcy ***usług zarządzanych w zakresie bezpieczeństwa***” oznaczają dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w art. 6 pkt 40 dyrektywy (UE) 2022/2555, wybranych ***do włączenia do unijnej rezerwy cyberbezpieczeństwa*** zgodnie z art. 16 niniejszego rozporządzenia.

Or. en

Poprawka 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 1 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
W celu rozwijania zaawansowanych zdolności w Unii w zakresie wykrywania, analizowania i przetwarzania danych dotyczących cyberzagrożeń i ***cyberincydentów*** w Unii ustanawia się wzajemnie połączoną ogólnoeuropejską infrastrukturę centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa”). W jej skład wchodzą wszystkie krajowe centra monitorowania bezpieczeństwa („krajowe SOC”) oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC”).	W celu rozwijania zaawansowanych zdolności w Unii w zakresie wykrywania, analizowania i przetwarzania danych dotyczących cyberzagrożeń ***oraz zapobiegania incydentom*** w Unii ustanawia się wzajemnie połączoną ogólnoeuropejską infrastrukturę centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa”). W jej skład wchodzą wszystkie krajowe centra monitorowania bezpieczeństwa („krajowe SOC”) oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC”).

Or. en

Poprawka 102
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł ***za pośrednictwem*** transgranicznych SOC;	a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł ***poprzez dobrowolną wymianę informacji uzyskanych od*** transgranicznych SOC;

Or. en

Poprawka 103
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł za pośrednictwem transgranicznych SOC;	a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł za pośrednictwem transgranicznych SOC ***na poziomie zarówno krajowym, jak i unijnym***;

Or. en

Poprawka 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) przyczynia się do lepszej ochrony	c) przyczynia się do lepszej ochrony

przed cyberzagrożeniami i lepszego reagowania na nie;	przed cyberzagrożeniami i lepszego reagowania na nie***, w tym poprzez kierowanie konkretnych zaleceń do podmiotów***;

Or. en

Poprawka 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) przyczynia się do szybszego wykrywania cyberzagrożeń i zapewniania orientacji sytuacyjnej w całej Unii;	d) przyczynia się do szybszego wykrywania cyberzagrożeń i zapewniania orientacji sytuacyjnej w całej Unii***, w tym poprzez aktywne gromadzenie danych wywiadowczych***;

Or. en

Poprawka 106
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 1 – litera e

Tekst proponowany przez Komisję	*Poprawka*
e) udostępnia usługi i działania na rzecz społeczności zajmującej się cyberbezpieczeństwem w Unii, w tym przyczynia się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych.	*(Nie dotyczy polskiej wersji językowej)*

Or. en

Poprawka 107
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 4 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Krajowe centra monitorowania bezpieczeństwa	***Wzmocniona współpraca i wymiana informacji na poziomie krajowym***

Or. en

Poprawka 108
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 1 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
Aby ***uczestniczyć w europejskiej tarczy*** cyberbezpieczeństwa, każde państwo członkowskie wyznacza ***co najmniej jeden krajowy SOC. Krajowy SOC jest podmiotem publicznym***.	Aby ***wesprzeć europejską tarczę*** cyberbezpieczeństwa, każde państwo członkowskie wyznacza ***jeden ze swoich zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), o których mowa w art. 10 dyrektywy (UE) 2022/2555, do pełnienia funkcji ośrodka wymiany i analizy informacji (ISAC)***.

Or. en

Poprawka 109
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 1 – akapit 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Organizacje prywatne i publiczne lub organy krajowe, w szczególności podmioty działające w sektorach krytycznych lub wysoce krytycznych, zachęca się do ustanawiania i prowadzenia własnych niezależnych lub wspólnie zarządzanych SOC.

Or. en

Poprawka 110
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa 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. ***Krajowy SOC lub krajowy CSIRT może zwrócić się do zaufanych dostawców lub dostawców usług zarządzanych w zakresie bezpieczeństwa o dane telemetryczne, dane z czujników lub dane z rejestrów, które dotyczą sektorów kluczowych zdefiniowanych w dyrektywie (UE) 2022/2555. Dane te mogą być udostępniane wyłącznie w celu wspierania zadań i obowiązków krajowego SOC lub CSIRT w zakresie wykrywania incydentów w cyberbezpieczeństwie i zapobiegania im.***

Or. en

Poprawka 111
Evžen Tošenovský

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 ***przede wszystkim dla SOC ustanowionych przez podmioty prywatne i publiczne lub organy krajowe, innych CSIRT tego samego państwa członkowskiego, koordynatora zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę, a także*** dla innych organizacji publicznych i prywatnych na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz***, w stosownych przypadkach, udostępniania tych informacji innym członkom sieci CSIRT***. Jest on wyposażony w najnowocześniejsze technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

Or. en

Poprawka 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym***, w szczególności ich SOC,*** w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. Jest on wyposażony w najnowocześniejsze

analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.	technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

Or. en

Poprawka 113
Evžen Tošenovský

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.	***skreśla się***

Or. en

Poprawka 114
Ville Niinistö
w imieniu grupy Verts/ALE

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”) ***może wybrać*** 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.

Or. en

Uzasadnienie

Obowiązkowy charakter wyrażenia „wybiera” pozbawia treść koncepcji zaproszenia do wyrażenia zainteresowania i uczestniczenia w procesach wyboru. Oczywiście SOC mogą uczestniczyć i mogą zostać wybrane.

Poprawka 115
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Krajowy SOC wybrany na podstawie ust. 2 zobowiązuje się do złożenia wniosku o uczestnictwo w transgranicznym SOC w ciągu dwóch lat od dnia nabycia narzędzi i infrastruktur lub od dnia otrzymania finansowania w formie dotacji, w zależności od tego, która z tych dat przypada wcześniej. Jeżeli do tego czasu krajowy SOC nie zostanie	***skreśla się***

uczestnikiem transgranicznego SOC, nie kwalifikuje się do dodatkowego wsparcia Unii na mocy niniejszego rozporządzenia.

Or. en

Poprawka 116
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 5 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Transgraniczne centra monitorowania bezpieczeństwa	***Wspólne zamówienie na narzędzia i infrastruktury***

Or. en

Poprawka 117
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Konsorcjum przyjmujące, które składa się z co najmniej trzech państw członkowskich, reprezentowanych przez krajowe SOC, zobowiązujących się do współpracy w celu koordynowania swoich działań w zakresie wykrywania cyberataków i monitorowania zagrożeń, kwalifikuje się do uczestnictwa w działaniach mających na celu ustanowienie transgranicznego SOC.	***skreśla się***

Or. en

Poprawka 118
Evžen Tošenovský

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 ***może wybrać CSIRT-ISAC*** do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać ***CSIRT-ISAC*** 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 ***CSIRT-ISAC***. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i ***uczestniczące CSIRT-ISAC*** zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur***, w tym korzystanie z nich przez inne CSIRT i SOC w danym państwie członkowskim***.

Or. en

Poprawka 119
Ville Niinistö
w imieniu grupy Verts/ALE

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	2. W następstwie zaproszenia do wyrażenia zainteresowania ECCC ***może wybrać*** 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

% 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.	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.

Or. en

Uzasadnienie

Chociaż w rozporządzeniu nie zawarto wyraźnych kryteriów, inne obowiązujące przepisy mogą ograniczać pewność, że każdy wnioskodawca zostanie wybrany.

Poprawka 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Tekst proponowany przez Komisję	*Poprawka*
	2a. Należy zezwolić na udzielenie zamówienia podmiotowi prywatnemu mającemu siedzibę w państwie trzecim o podobnych poglądach oraz na udział takiego podmiotu, jeżeli nie narusza to interesów Unii i państw członkowskich w dziedzinie bezpieczeństwa i obrony, określonych w ramach wspólnej polityki zagranicznej i bezpieczeństwa zgodnie z tytułem V TUE, ani celów określonych w niniejszym rozporządzeniu. Takie podmioty prywatne nie powinny być kontrolowane przez niestowarzyszone państwo trzecie lub powinny podlegać monitorowaniu w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/452.

Or. en

Poprawka 121

Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Członkowie konsorcjum przyjmującego zawierają pisemną umowę konsorcjum określającą ich wewnętrzne ustalenia dotyczące wykonania umowy o przyjęciu i użytkowaniu.	***skreśla się***

Or. en

Poprawka 122
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Transgraniczny SOC jest reprezentowany do celów prawnych przez krajowy SOC pełniący funkcję koordynującego SOC lub przez konsorcjum przyjmujące, jeżeli ma ono osobowość prawną. Koordynujący SOC odpowiada za zgodność z wymogami umowy o przyjęciu i użytkowaniu oraz niniejszego rozporządzenia.	***skreśla się***

Or. en

Poprawka 123
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 6 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Współpraca i wymiana informacji ***w ramach transgranicznych SOC i między***	***Wzmocniona*** współpraca i wymiana informacji ***na poziomie UE***

nimi

Or. en

Poprawka 124
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. Członkowie konsorcjum przyjmującego ***wymieniają*** się istotnymi informacjami w ramach transgranicznego SOC, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:	1. Członkowie konsorcjum przyjmującego ***mogą wymieniać*** się istotnymi informacjami w ramach transgranicznego SOC, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:

Or. en

Poprawka 125
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. ***Członkowie konsorcjum przyjmującego*** wymieniają się istotnymi informacjami w ramach ***transgranicznego SOC***, w tym informacjami o cyberzagrożeniach, potencjalnych	1. ***CSIRT-ISAC i inne CSIRT*** wymieniają się istotnymi informacjami w ramach ***sieci CSIRT***, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa,

zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:	podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:

Or. en

Poprawka 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) ***ma na celu zapobieganie*** incydentom, ich ***wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach*** lub ***łagodzenie*** ich skutków;	a) ***usprawnia wymianę danych wywiadowczych na temat cyberzagrożeń między SOC i branżowymi ISAC w*** celu ***zapobiegania*** incydentom, ich ***wykrywania*** lub ***łagodzenia ich*** skutków;

Or. en

Poprawka 127
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 2 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
2. ***Pisemna*** umowa ***konsorcjum, o której mowa w art. 5 ust. 3,*** określa:	2. Umowa ***o wymianie danych wywiadowczych i informacji między CSIRT-ISAC lub, w stosownych przypadkach, innymi CSIRT*** określa:

Or. en

Poprawka 128
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 2 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) zobowiązanie do udostępniania ***znacznej ilości*** danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;	a) zobowiązanie do ***dobrowolnego*** udostępniania danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;

Or. en

Poprawka 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 2 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) zobowiązanie do udostępniania ***znacznej ilości*** danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;	a) zobowiązanie do udostępniania ***istotnych*** danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;

Or. en

Poprawka 130
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Aby wspierać wymianę informacji między transgranicznymi SOC, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. Aby ułatwić interoperacyjność między transgranicznymi SOC, Komisja może w	***skreśla się***

drodze aktów wykonawczych, po konsultacji z ECCC, określić warunki tej interoperacyjności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.

Or. en

Poprawka 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Aby wspierać wymianę informacji między transgranicznymi SOC, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. Aby ułatwić interoperacyjność między transgranicznymi SOC, ***Komisja może*** w drodze aktów ***wykonawczych, po konsultacji z ECCC, określić warunki*** tej interoperacyjności. Te akty ***wykonawcze*** przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.	3. Aby wspierać wymianę informacji między transgranicznymi SOC ***i z branżowymi ISAC***, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą ***oraz, w miarę możliwości, z branżowymi ISAC***. Aby ułatwić interoperacyjność między transgranicznymi SOC ***i z branżowymi ISAC***, ***należy dostosować standardy i protokoły wymiany informacji do międzynarodowych standardów i najlepszych praktyk branżowych. ECCC może również zwrócić się do Komisji*** w drodze aktów ***delegowanych o zaproponowanie warunków*** tej interoperacyjności ***w ścisłej koordynacji z regionalnymi SOC oraz w oparciu o międzynarodowe standardy i najlepsze praktyki branżowe***. Te akty ***delegowane*** przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.

Or. en

Poprawka 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Aby wspierać wymianę informacji między transgranicznymi SOC, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. ***Aby*** ułatwić interoperacyjność między transgranicznymi SOC, Komisja może w drodze aktów wykonawczych, po konsultacji z ECCC, określić warunki tej interoperacyjności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.	3. Aby wspierać wymianę informacji między transgranicznymi SOC, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. ***Wspólne zamówienia na infrastrukturę cybernetyczną, usługi i narzędzia mogą*** ułatwić interoperacyjność między transgranicznymi SOC***. Aby określić warunki interoperacyjności transgranicznych SOC***, Komisja może***,*** w drodze aktów wykonawczych, po konsultacji z ECCC ***i ENISA***, określić warunki tej interoperacyjności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.

Or. en

Poprawka 133
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Transgraniczne SOC zawierają między sobą umowy o współpracy określające zasady wymiany informacji między platformami transgranicznymi.	***skreśla się***

Or. en

Poprawka 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia

Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Transgraniczne SOC zawierają między sobą umowy o współpracy określające zasady wymiany informacji między platformami transgranicznymi.	4. Transgraniczne SOC zawierają między sobą umowy o współpracy określające zasady wymiany informacji między platformami transgranicznymi***, z uwzględnieniem istniejących już odpowiednich mechanizmów wymiany informacji na podstawie dyrektywy (UE) 2022/2555***. ***W kontekście potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę mechanizmy wymiany informacji muszą być zgodne z odpowiednimi przepisami dyrektywy (UE) 2022/2555.***

Or. en

Poprawka 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Transgraniczne SOC zawierają między sobą umowy o współpracy określające zasady wymiany informacji między platformami transgranicznymi.	4. Transgraniczne SOC zawierają między sobą ***i z branżowymi ISAC*** umowy o współpracy określające zasady wymiany informacji ***i interoperacyjności*** między platformami transgranicznymi.

Or. en

Poprawka 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 7 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Współpraca i wymiana informacji	Współpraca i wymiana informacji z ***siecią***

z ***podmiotami unijnymi*** ***CSIRT***

Or. en

Poprawka 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***na potrzeby wspólnej orientacji sytuacyjnej, koordynujące SOC*** bez zbędnej zwłoki przekazują istotne informacje ***swojemu CSIRT lub właściwemu organowi, które przekażą te informacje*** EU-CyCLONe, sieci CSIRT i Komisji, biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym ***i odpowiednie procedury*** zgodnie z dyrektywą (UE) 2022/2555.

Or. en

Uzasadnienie

Zaleca się stosowanie procedury określonej w dyrektywie NIS2 w przypadku incydentów na dużą skalę.

Poprawka 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	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.	cyberbezpieczeństwie na dużą skalę, bez zbędnej zwłoki przekazują istotne informacje EU-CyCLONe, sieci CSIRT i Komisji ***oraz ENISA, z uwzględnieniem*** ich ***odpowiednich ról*** w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555.

Or. en

Poprawka 139
Evžen Tošenovský

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 ***CSIRT-ISAC*** uzyskają informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, bez zbędnej zwłoki przekazują istotne informacje EU-CyCLONe ***i*** sieci CSIRT, biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555.

Or. en

Poprawka 140
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 7 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Komisja może w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w	***skreśla się***

art. 21 ust. 2 niniejszego rozporządzenia.

Or. en

Poprawka 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 7 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Komisja może w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.	2. Komisja może***, po konsultacji z platformami transgranicznymi i siecią CSIRT,*** w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia***, oraz zgodnie z dyrektywą (UE) 2022/2555***.

Or. en

Uzasadnienie

Zaleca stosowanie procedury określonej w dyrektywie NIS2 w przypadku incydentów na dużą skalę, a zatem najpierw skonsultowanie się z siecią CSIRT.

Poprawka 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 7 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Komisja może w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w	2. Komisja może***, po konsultacji z ENISA,*** w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której

art. 21 ust. 2 niniejszego rozporządzenia.	mowa w art. 21 ust. 2 niniejszego rozporządzenia.

Or. en

Poprawka 143
Johan Nissinen

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 ***poufności,*** 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.

Or. en

Poprawka 144
Evžen Tošenovský

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	***skreśla się***

rozporządzenia. Przyjmując te akty, Komisja, wspierana przez wysokiego przedstawiciela, uwzględnia odpowiednie normy bezpieczeństwa na poziomie obronnym, aby ułatwić współpracę z podmiotami wojskowymi.

Or. en

Poprawka 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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***, oraz dyrektywami (UE) 2022/2555 i 2022/2557***. Przyjmując te akty, Komisja, wspierana przez wysokiego przedstawiciela, uwzględnia odpowiednie normy bezpieczeństwa na poziomie obronnym, aby ułatwić współpracę z podmiotami wojskowymi.

Or. en

Poprawka 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Komisja może przyjąć akty	3. Komisja może***, po konsultacji z***

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.	***ENISA,*** 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.

Or. en

Poprawka 147
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na poważne zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm”).	1. ***Na wyraźny wniosek zainteresowanych państw członkowskich*** ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na poważne zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm”).

Or. en

Poprawka 148
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na poważne zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm”).	1. *(Nie dotyczy polskiej wersji językowej)*

Or. en

Poprawka 149
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) działania w zakresie reagowania wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków, realizowane przez zaufanych dostawców uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12;	b) działania w zakresie reagowania wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków, realizowane przez zaufanych dostawców uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12***, na wyraźny wniosek zainteresowanych państw członkowskich***;

Or. en

Poprawka 150
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) działania w zakresie reagowania	b) działania w zakresie reagowania

wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków, realizowane przez zaufanych dostawców uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12;	wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków, realizowane przez zaufanych dostawców ***usług zarządzanych w zakresie bezpieczeństwa*** uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12;

Or. en

Poprawka 151
Ville Niinistö
w imieniu grupy Verts/ALE

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a. Po uruchomieniu mechanizmu cyberkryzysowego Komisja co roku składa sprawozdanie z oceny zarówno pozytywnych, jak i negatywnych skutków działania mechanizmu, w tym kwestii, czy konieczne są dodatkowe wymogi w zakresie współpracy lub szkoleń.

Or. en

Poprawka 152
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 11 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 10 ust. 1 lit. a), Komisja, po konsultacji z grupą współpracy NIS i ENISA, określa odnośne sektory lub podsektory spośród sektorów	1. Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 10 ust. 1 lit. a), Komisja, po konsultacji z grupą współpracy NIS i ENISA, określa odnośne sektory lub podsektory spośród

kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, z których podmioty mogą podlegać skoordynowanemu testowaniu gotowości, z uwzględnieniem istniejących i planowanych skoordynowanych ocen ryzyka i testów odporności na szczeblu Unii.

sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, z których podmioty mogą podlegać ***dobrowolnemu*** skoordynowanemu testowaniu gotowości, z uwzględnieniem istniejących i planowanych skoordynowanych ocen ryzyka i testów odporności na szczeblu Unii.

Or. en

Poprawka 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 i wysokim przedstawicielem opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania ***gotowości. Pozwoli to na określenie sektorów lub podsektorów, w których podmioty mogą podlegać skoordynowanemu testowaniu gotowości zgodnie z ust. 1***.

Or. en

Poprawka 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	2. Grupa współpracy NIS we współpracy z Komisją, ENISA***,*** wysokim przedstawicielem ***i podmiotami, które mogą podlegać skoordynowanemu***

skoordynowanego testowania.	***testowaniu gotowości,*** opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania.

Or. en

Poprawka 155
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Ustanawia się unijną rezerwę cyberbezpieczeństwa, aby pomóc użytkownikom, o których mowa w ust. 3, w reagowaniu lub w udzielaniu wsparcia w reagowaniu na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz w natychmiastowym usuwaniu skutków takich incydentów.	1. Ustanawia się unijną rezerwę cyberbezpieczeństwa, aby pomóc użytkownikom, o których mowa w ust. 3, w reagowaniu lub w udzielaniu wsparcia w reagowaniu na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz w natychmiastowym usuwaniu skutków takich incydentów***, na wyraźny wniosek zainteresowanych państw członkowskich i bez uszczerbku dla szczególnego charakteru polityki bezpieczeństwa i obrony niektórych państw członkowskich***.

Or. en

Poprawka 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	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.	zadeklarowane usługi. Usługi te muszą być możliwe do wprowadzenia we wszystkich państwach członkowskich***, wzmacniać odporność i suwerenność Unii oraz zwiększać jej konkurencyjność***. ***Nazwy wybranych zaufanych dostawców i ich usług mają charakter poufny.***

Or. en

Poprawka 157
Johan Nissinen

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. ***Unijna rezerwa cyberbezpieczeństwa nie ogranicza konieczności zapewnienia państwom możliwości monitorowania i oceny własnych potrzeb.***

Or. en

Poprawka 158
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Unijna rezerwa cyberbezpieczeństwa składa się z usług reagowania na incydenty świadczonych	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.

przez zaufanych dostawców ***usług zarządzanych w zakresie bezpieczeństwa*** wybranych zgodnie z kryteriami określonymi w art. 16. Rezerwa obejmuje wcześniej zadeklarowane usługi. Usługi te ***mogą*** być***, na odpowiedni wniosek,*** możliwe do wprowadzenia we wszystkich państwach członkowskich.

Or. en

Poprawka 159
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 3 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ***instytucje, organy i jednostki organizacyjne Unii***.	b) ***państwa trzecie, o których mowa w art. 17 niniejszego rozporządzenia***.

Or. en

Poprawka 160
Evžen Tošenovský

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), ***mogą, na wniosek, korzystać*** 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.

Or. en

Poprawka 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***w porozumieniu z grupą koordynacyjną do spraw dyrektywy NIS2 oraz*** 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.

Or. en

Poprawka 162
Evžen Tošenovský

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,	5. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja ***we współpracy z ENISA*** 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

a także z innymi działaniami i programami unijnymi.	podstawie niniejszego rozporządzenia, a także z innymi działaniami i programami unijnymi.

Or. en

Poprawka 163
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Komisja może powierzyć ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu.	***skreśla się***

Or. en

Poprawka 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Komisja ***może powierzyć*** ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu.	6. Komisja ***powierza*** ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu.

Or. en

Poprawka 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 konsultuje się z wysokim przedstawicielem.	7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, ***w tym niezbędnych umiejętności i zdolności siły roboczej w sektorze cyberbezpieczeństwa,*** po konsultacji z państwami członkowskimi i Komisją. ENISA przygotowuje podobne zestawienie, po konsultacji z Komisją ***i we współpracy z sektorem prywatnym***, w celu określenia potrzeb państw trzecich kwalifikujących się do wsparcia z unijnej rezerwy cyberbezpieczeństwa zgodnie z art. 17. W stosownych przypadkach Komisja konsultuje się z wysokim przedstawicielem.

Or. en

Poprawka 166
Evžen Tošenovský

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 konsultuje się z wysokim przedstawicielem.	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 konsultuje się z wysokim przedstawicielem ***i informuje Radę o potrzebach państw***

trzecich.

Or. en

Poprawka 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 konsultuje się z wysokim przedstawicielem	7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, po konsultacji z państwami członkowskimi ***,*** Komisją***, dostawcami usług zarządzanych w zakresie bezpieczeństwa i przedstawicielami branży***. 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 konsultuje się z wysokim przedstawicielem

Or. en

Poprawka 168
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 8

Tekst proponowany przez Komisję	*Poprawka*
8. Komisja może ***w drodze aktów wykonawczych określić rodzaje*** i ***liczbę*** usług reagowania wymaganych na potrzeby unijnej rezerwy cyberbezpieczeństwa. Te akty	8. Komisja może ***przyjmować akty delegowane zgodnie z art. 20a niniejszego rozporządzenia w celu określenia rodzajów*** i ***liczby*** usług reagowania wymaganych na potrzeby unijnej rezerwy

wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.	cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.

Or. en

Poprawka 169
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 13 – ustęp 5 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) ***odpowiednie informacje na temat*** podmiotu, na który incydent ma wpływ, i potencjalnych skutków incydentu oraz planowanego wykorzystania wsparcia, którego dotyczy wniosek, w tym wskazanie szacowanych potrzeb;	a) ***rodzaj*** podmiotu, na który incydent ma wpływ, i potencjalnych skutków incydentu oraz planowanego wykorzystania wsparcia, którego dotyczy wniosek, w tym wskazanie szacowanych potrzeb;

Or. en

Poprawka 170
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 13 – ustęp 5 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) informacje o środkach zastosowanych w celu złagodzenia skutków incydentu będącego przedmiotem wniosku o wsparcie, o których to środkach mowa w ust. 2;	b) ***ogólne*** informacje o środkach zastosowanych w celu złagodzenia skutków incydentu będącego przedmiotem wniosku o wsparcie, o których to środkach mowa w ust. 2;

Or. en

Poprawka 171
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 13 – ustęp 5 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) informacje na temat innych form wsparcia dostępnych dla podmiotu, na który incydent ma wpływ***, w tym obowiązujących ustaleń umownych dotyczących usług w zakresie reagowania na incydenty i natychmiastowego usuwania skutków incydentów, a także umów ubezpieczenia potencjalnie obejmujących taki rodzaj incydentu***.	c) informacje na temat innych form wsparcia dostępnych dla podmiotu, na który incydent ma wpływ.

Or. en

Poprawka 172
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 13 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. Komisja może w drodze aktów wykonawczych doprecyzować szczegółowe ustalenia dotyczące przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.	***skreśla się***

Or. en

Poprawka 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 13 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*

7. Komisja może ***w drodze aktów wykonawczych doprecyzować szczegółowe ustalenia dotyczące*** przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.	7. Komisja może ***przyjmować akty delegowane zgodnie z art. 20a niniejszego rozporządzenia w celu doprecyzowania szczegółowych ustaleń dotyczących*** przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.

Or. en

Poprawka 174
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa są oceniane przez Komisję przy wsparciu ze strony ENISA ***lub zgodnie z ustaleniami zawartymi w umowach o przyznanie wkładu na podstawie art. 12 ust. 6***, a ***odpowiedź*** jest ***niezwłocznie*** przekazywana użytkownikom, o których mowa w art. 12 ust. 3.	1. Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa są oceniane przez Komisję przy wsparciu ze strony ENISA, a ***jej decyzja*** jest przekazywana użytkownikom, o których mowa w art. 12 ust. 3***, bez zbędnej zwłoki, a w każdym razie w terminie 24 godzin***.

Or. en

Poprawka 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 2 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) potencjalny transgraniczny charakter incydentu i ryzyko rozprzestrzenienia się incydentu na inne państwa członkowskie lub na innych użytkowników;	d) ***skalę i*** potencjalny transgraniczny charakter incydentu i ryzyko rozprzestrzenienia się incydentu na inne państwa członkowskie lub na innych użytkowników;

Or. en

Poprawka 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Usługi z unijnej rezerwy cyberbezpieczeństwa są świadczone zgodnie z konkretnymi umowami między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa. Umowy te zawierają warunki dotyczące odpowiedzialności.	3. Usługi z unijnej rezerwy cyberbezpieczeństwa są świadczone zgodnie z konkretnymi umowami między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa. Umowy te zawierają warunki dotyczące odpowiedzialności ***i wszelkie inne postanowienia, które strony umowy uznają za niezbędne w celu świadczenia odpowiedniej usługi***.

Or. en

Poprawka 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Usługi z unijnej rezerwy cyberbezpieczeństwa są świadczone zgodnie z konkretnymi umowami między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa. Umowy te zawierają warunki dotyczące odpowiedzialności.	3. Usługi z unijnej rezerwy cyberbezpieczeństwa są świadczone ***za zgodą użytkownika i*** zgodnie z konkretnymi umowami między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa. Umowy te zawierają warunki dotyczące odpowiedzialności.

Or. en

Poprawka 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Umowy, o których mowa w ust. 3, ***mogą opierać*** się na wzorach przygotowanych przez ENISA po konsultacji z państwami członkowskimi.	4. Umowy, o których mowa w ust. 3, ***opierają*** się na wzorach przygotowanych przez ENISA po konsultacji z państwami członkowskimi ***i innymi użytkownikami rezerwy***.

Or. en

Poprawka 179
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej rezerwy cyberbezpieczeństwa.	***skreśla się***

Or. en

Poprawka 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej	5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej

rezerwy cyberbezpieczeństwa.	rezerwy cyberbezpieczeństwa***, z wyjątkiem przypadków zaniedbania w odniesieniu do oceny wniosku dostawcy usługi lub przypadków, gdy Komisja lub ENISA są użytkownikami i uznaje się je za odpowiedzialne za szkody***.

Or. en

Poprawka 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej rezerwy cyberbezpieczeństwa.	5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej rezerwy cyberbezpieczeństwa***, z wyjątkiem przypadków, gdy Komisja lub ENISA są użytkownikami rezerwy zgodnie z art. 14 ust. 3***.

Or. en

Poprawka 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji i ENISA sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń. Jeżeli użytkownik pochodzi z państwa trzeciego, jak określono w art. 17, sprawozdanie to	6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji i ENISA sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń. Jeżeli użytkownik pochodzi z państwa trzeciego, jak określono w art. 17, sprawozdanie to

udostępnia się wysokiemu przedstawicielowi.

udostępnia się wysokiemu przedstawicielowi. ***Sprawozdanie sporządza się z poszanowaniem prawa unijnego lub krajowego dotyczącego ochrony informacji szczególnie chronionych lub niejawnych.***

Or. en

Poprawka 183
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji ***i*** ENISA sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń. Jeżeli użytkownik pochodzi z państwa trzeciego, jak określono w art. 17, sprawozdanie to udostępnia się wysokiemu przedstawicielowi.	6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji***,*** ENISA***, sieci CSIRT oraz – w stosownych przypadkach – EU-CyCLONe*** sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń. Jeżeli użytkownik pochodzi z państwa trzeciego, jak określono w art. 17, sprawozdanie to udostępnia się wysokiemu przedstawicielowi.

Or. en

Poprawka 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. Komisja regularnie składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia.	7. Komisja regularnie składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia. ***Informacje poufne chronione są w sprawozdaniu zgodnie z prawem***

unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych.

Or. en

Poprawka 185
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 14 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. Komisja ***regularnie*** składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia.	7. Komisja ***co najmniej dwa razy w roku*** składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia.

Or. en

Poprawka 186
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 15 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Koordynacja z mechanizmami zarządzania kryzysowego	Koordynacja ***mechanizmu cyberkryzysowego*** z mechanizmami zarządzania kryzysowego

Or. en

Poprawka 187
Evžen Tošenovský

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.

Or. en

Poprawka 188
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Zaufani dostawcy	Zaufani dostawcy ***usług zarządzanych w zakresie bezpieczeństwa***

Or. en

Poprawka 189
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. W postępowaniach o udzielenie zamówienia do celów utworzenia unijnej rezerwy cyberbezpieczeństwa instytucja zamawiająca działa zgodnie z zasadami określonymi w rozporządzeniu (UE, Euratom) 2018/1046 oraz zgodnie z następującymi zasadami:	1. W postępowaniach o udzielenie zamówienia do celów utworzenia unijnej rezerwy cyberbezpieczeństwa instytucja zamawiająca działa zgodnie z zasadami określonymi w rozporządzeniu (UE, Euratom) 2018/1046***, bez uszczerbku dla głównej odpowiedzialności państw***

członkowskich za bezpieczeństwo narodowe, oraz zgodnie z następującymi zasadami:

Or. en

Poprawka 190
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa obejmowała usługi, które mogą być wprowadzone we wszystkich państwach członkowskich, z uwzględnieniem w szczególności krajowych wymogów dotyczących świadczenia takich usług, w tym certyfikacji lub akredytacji;	a) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa obejmowała usługi, które mogą być wprowadzone we wszystkich państwach członkowskich ***i państwach trzecich zgodnie z art. 17 niniejszego rozporządzenia***, z uwzględnieniem w szczególności krajowych wymogów dotyczących świadczenia takich usług, w tym certyfikacji lub akredytacji;

Or. en

Poprawka 191
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa wnosiła unijną wartość dodaną przez wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w UE.	c) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa wnosiła unijną wartość dodaną przez wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w UE***, wzmacnianie odporności i suwerenności Unii oraz poprawę jej konkurencyjności***.

Or. en

Poprawka 192
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa wnosiła ***unijną wartość dodaną przez*** wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w UE.	c) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa wnosiła wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w UE.

Or. en

Poprawka 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***nowoczesne*** sprzęt i oprogramowanie techniczne niezbędne do obsługi żądanej usługi ***i musi spełniać wymogi określone w rozporządzeniu XX/XXXX (akt dotyczący cyberodporności), w stosownych przypadkach***;

Or. en

Poprawka 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Tekst proponowany przez Komisję	*Poprawka*
	fa) dostawca musi udowodnić, że jego struktury decyzyjne i zarządcze nie znajdują się pod niepotrzebnym wpływem rządów państw uznanych za rywali systemowych Unii;

Or. en

Poprawka 195
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera h

Tekst proponowany przez Komisję	*Poprawka*
h) dostawca musi być w stanie zapewnić usługę w krótkim terminie w państwach członkowskich, w których może świadczyć tę usługę;	h) dostawca musi być w stanie zapewnić usługę w krótkim terminie w państwach członkowskich ***lub państwach trzecich***, w których może świadczyć tę usługę;

Or. en

Poprawka 196
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera i

Tekst proponowany przez Komisję	*Poprawka*
i) dostawca musi być w stanie zapewnić usługę w języku lokalnym państw członkowskich, w których może świadczyć tę usługę;	i) dostawca musi być w stanie zapewnić usługę w języku lokalnym państw członkowskich ***lub państw trzecich***, w których może świadczyć tę usługę***, lub w jednym z języków roboczych instytucji Unii***;

Or. en

Poprawka 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera j

Tekst proponowany przez Komisję	*Poprawka*
j) po wprowadzeniu unijnego programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem.	j) po wprowadzeniu unijnego programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem ***w ciągu dwóch lat od przyjęcia programu***.

Or. en

Poprawka 198
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera j

Tekst proponowany przez Komisję	*Poprawka*
j) po wprowadzeniu ***unijnego*** programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem.	j) po wprowadzeniu ***europejskiego*** programu certyfikacji ***cyberbezpieczeństwa*** usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem.

Or. en

Poprawka 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera j

Tekst proponowany przez Komisję	*Poprawka*
j) po wprowadzeniu unijnego programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem.	j) po wprowadzeniu unijnego programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem ***w ciągu dwóch lat***.

Or. en

Uzasadnienie

Propozycja Komisji zakłada, że program certyfikacji zastąpi wymogi techniczne wymienione w tym rozporządzeniu. Ta poprawka daje przedsiębiorstwom, zwłaszcza MŚP, więcej czasu na przejście na ten program, a przy tym sprzyja zapewnieniu bardziej równych warunków działania w całej Unii. Do tego czasu przedsiębiorstwa będą musiały spełniać wymogi techniczne przedmiotowego rozporządzenia.

Poprawka 200
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Tekst proponowany przez Komisję	*Poprawka*
	ja) dostawca musi być w stanie oddzielić swoje usługi od szerszej umowy, tak aby użytkownik mógł zmienić dostawcę usług;

Or. en

Poprawka 201
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 17 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Komisja koordynuje z wysokim przedstawicielem działania dotyczące otrzymanych wniosków i wdrażania wsparcia przyznanego państwom trzecim	6. Komisja ***bez zbędnej zwłoki powiadamia Radę i*** koordynuje z wysokim przedstawicielem działania dotyczące otrzymanych wniosków i wdrażania

z unijnej rezerwy cyberbezpieczeństwa.	wsparcia przyznanego państwom trzecim z unijnej rezerwy cyberbezpieczeństwa.

Or. en

Poprawka 202
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 18

Tekst proponowany przez Komisję	*Poprawka*
Artykuł 18	***skreśla się***
Mechanizm przeglądu incydentów w cyberbezpieczeństwie	
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.	
2. W celu przygotowania sprawozdania z przeglądu incydentu, o którym to sprawozdaniu mowa w ust. 1, ENISA współpracuje ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym przedstawicielami państw członkowskich, Komisji, innych odpowiednich instytucji, organów i jednostek organizacyjnych UE, dostawców usług zarządzanych w zakresie bezpieczeństwa i użytkowników usług w zakresie cyberbezpieczeństwa. W stosownych przypadkach ENISA współpracuje również z podmiotami, na	

które poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę mają wpływ. Na potrzeby przeglądu ENISA może również konsultować się z innymi rodzajami zainteresowanych stron. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.

3. Sprawozdanie obejmuje przegląd i analizę konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w tym głównych przyczyn, podatności i zdobytych doświadczeń. Informacje poufne chronione są w sprawozdaniu zgodnie z prawem unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych.

4. W stosownych przypadkach sprawozdanie zawiera zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

5. W miarę możliwości wersję sprawozdania udostępnia się publicznie. Wersja ta zawiera wyłącznie informacje publiczne.

Or. en

Poprawka 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. W celu przygotowania sprawozdania z przeglądu incydentu, o którym to sprawozdaniu mowa w ust. 1, ENISA współpracuje ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym przedstawicielami państw	2. W celu przygotowania sprawozdania z przeglądu incydentu, o którym to sprawozdaniu mowa w ust. 1, ENISA współpracuje ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym przedstawicielami państw

członkowskich, Komisji, innych odpowiednich instytucji, organów i jednostek organizacyjnych UE, dostawców usług zarządzanych w zakresie bezpieczeństwa i użytkowników usług w zakresie cyberbezpieczeństwa. W stosownych przypadkach ENISA współpracuje również z podmiotami, na które poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę mają wpływ. Na potrzeby przeglądu ENISA może również konsultować się z innymi rodzajami zainteresowanych stron. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.	członkowskich, Komisji, innych odpowiednich instytucji, organów i jednostek organizacyjnych UE, dostawców usług zarządzanych w zakresie bezpieczeństwa i użytkowników usług w zakresie cyberbezpieczeństwa***, i gromadzi od nich informacje zwrotne***. W stosownych przypadkach ENISA współpracuje również z podmiotami, na które poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę mają wpływ. Na potrzeby przeglądu ENISA może również konsultować się z innymi rodzajami zainteresowanych stron. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.

Or. en

Poprawka 204
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Sprawozdanie obejmuje przegląd i analizę konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w tym głównych przyczyn, podatności i zdobytych doświadczeń. Informacje poufne chronione są w sprawozdaniu zgodnie z prawem unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych.	3. Sprawozdanie obejmuje przegląd i analizę konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w tym głównych przyczyn, podatności i zdobytych doświadczeń. Informacje poufne chronione są w sprawozdaniu zgodnie z prawem unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych. ***Sprawozdanie nie zawiera żadnych szczegółowych informacji na temat aktywnie wykorzystywanych podatności, które nie zostały jeszcze naprawione.***

Or. en

Poprawka 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. W stosownych przypadkach sprawozdanie zawiera zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.	4. W stosownych przypadkach sprawozdanie zawiera ***konkretne*** zalecenia***, w tym dla wszystkich zainteresowanych stron,*** mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

Or. en

Poprawka 206
Johan Nissinen

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. W stosownych przypadkach sprawozdanie zawiera zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.	4. W stosownych przypadkach sprawozdanie zawiera ***niewiążące prawnie, dobrowolne*** zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

Or. en

Poprawka 207
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 19 – akapit 1 – punkt 1 – litera a – podpunkt 1
Rozporządzenie (UE) 2021/694
Artykuł 1 – ustęp 1 – litera a a

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 ***CSIRT-ISAC oraz SOC***, które wnoszą wkład w orientację sytuacyjną w Unii oraz w zwiększanie unijnych zdolności wywiadowczych w zakresie cyberzagrożeń;

Or. en

Poprawka 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 19 – akapit 1 – punkt 3
Rozporządzenie (UE) 2021/694
Artykuł 14 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
Program może zapewniać finansowanie w dowolnej formie przewidzianej w rozporządzeniu finansowym, w tym w szczególności poprzez zamówienia stanowiące podstawową formę lub poprzez dotacje i nagrody.	Program może zapewniać finansowanie w dowolnej formie przewidzianej w rozporządzeniu finansowym, w tym w szczególności poprzez zamówienia stanowiące podstawową formę lub poprzez dotacje i nagrody. ***ENISA otrzymuje dodatkowe zasoby na realizację dodatkowych zadań określonych w rozporządzeniu XX/XXX (akt w sprawie cybersolidarności). To dodatkowe finansowanie nie może zagrażać osiągnięciu celów programu.***

Or. en

Poprawka 209
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 19 – akapit 1 – punkt 5
Rozporządzenie (UE) 2021/694
Artykuł 19 – akapit 2

Tekst proponowany przez Komisję	*Poprawka*
Wsparcie w formie dotacji może przyznawać bezpośrednio ECCC bez zaproszenia do składania wniosków ***krajowym SOC***, o których mowa w art. 4 rozporządzenia XXXX, ***oraz konsorcjum przyjmującemu,*** o którym mowa w art. 5 rozporządzenia XXXX, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.	Wsparcie w formie dotacji może przyznawać bezpośrednio ECCC bez zaproszenia do składania wniosków ***CSIRT-ISAC***, o których mowa w art. 4 rozporządzenia XXXX, o którym mowa w art. 5 rozporządzenia XXXX, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.

Or. en

Poprawka 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 20 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Ocena	Ocena ***i przegląd***

Or. en

Poprawka 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 [***dwa*** lata od daty rozpoczęcia stosowania niniejszego rozporządzenia] r.***, a następnie co dwa lata*** Komisja ***przeprowadza ocenę funkcjonowania środków określonych w niniejszym rozporządzeniu i*** przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie. ***Ocena obejmuje w szczególności:*** ***a) uczestnictwo państw członkowskich w***

europejskiej tarczy cyberbezpieczeństwa, w tym liczbę krajowych i transgranicznych SOC ustanowionych w ramach rozporządzenia oraz skuteczność wymiany informacji;

b) wkład niniejszego rozporządzenia we wzmacnianie odporności i suwerenności Unii, poprawę konkurencyjności odpowiednich sektorów przemysłu, w tym MŚP, oraz rozwój umiejętności w dziedzinie cyberbezpieczeństwa w UE;

c) wykorzystanie rezerwy cyberbezpieczeństwa, w tym ustalenie, czy zakres rezerwy należy rozszerzyć o usługi w zakresie gotowości na incydenty lub wspólne ćwiczenia z udziałem zaufanych dostawców i potencjalnych użytkowników rezerwy cyberbezpieczeństwa, aby w razie potrzeby zapewnić skuteczne funkcjonowanie rezerwy;

d) wkład niniejszego rozporządzenia w rozwój i doskonalenie umiejętności i kompetencji siły roboczej w sektorze cyberbezpieczeństwa, niezbędnych do wzmocnienia zdolności Unii do wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie, zapobiegania im, reagowania na nie i przywracania normalnego działania po ich wystąpieniu;

e) wkład niniejszego rozporządzenia we wdrażanie i rozwój najnowocześniejszych technologii w Unii.

Na podstawie tego sprawozdania Komisja w stosownych przypadkach przedkłada Parlamentowi i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.

Or. en

Poprawka 212
Evžen Tošenovský

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 [cztery lata od daty rozpoczęcia stosowania niniejszego rozporządzenia] r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia. ***Sprawozdaniu towarzyszy w razie potrzeby wniosek ustawodawczy.***

Or. en

Poprawka 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Wniosek dotyczący rozporządzenia
Artykuł 20 – akapit 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Każdego roku Komisja, przy okazji przedstawiania projektu budżetu na kolejny rok, przedkłada szczegółową ocenę zadań ENISA przewidzianych w niniejszym rozporządzeniu oraz [wniosku dotyczącym rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi] i innych przepisach Unii, a także szczegółowo określa zasoby finansowe i ludzkie niezbędne do realizacji tych zadań.

Or. en

Poprawka 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 20 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Artykuł 20a
	Wykonywanie przekazanych uprawnień
	1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.
	2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 12 ust. 8 i art. 13 ust. 7, powierza się Komisji na okres pięciu lat od ... [data wejścia w życie podstawowego aktu ustawodawczego lub inna data ustalona przez współprawodawców] r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem tego okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.
	3. Przekazanie uprawnień, o którym mowa w art. 12 ust. 8 i art. 13 ust. 7, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.
	4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 12 ust. 8 lub art. 13 ust. 7 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o [dwa miesiące] z inicjatywy Parlamentu Europejskiego lub Rady.

Or. en

Poprawka 215
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Załącznik I – akapit 1 – punkt 1
Rozporządzenie (UE) 2021/694
Załącznik I – rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie”

Tekst proponowany przez Komisję	*Poprawka*
1. Wspólne inwestycje z państwami członkowskimi w zaawansowane urządzenia, infrastrukturę i know-how w dziedzinie cyberbezpieczeństwa, które są niezbędne do ochrony infrastruktury krytycznej i całego jednolitego rynku cyfrowego. Takie wspólne inwestycje mogą obejmować inwestycje w infrastrukturę kwantową i zasoby danych na potrzeby cyberbezpieczeństwa, orientację sytuacyjną w cyberprzestrzeni, w tym krajowe ***SOC i transgraniczne*** SOC tworzące europejską tarczę cyberbezpieczeństwa, a także inne narzędzia, które zostaną udostępnione sektorowi publicznemu i prywatnemu	1. Wspólne inwestycje z państwami członkowskimi w zaawansowane urządzenia, infrastrukturę i know-how w dziedzinie cyberbezpieczeństwa, które są niezbędne do ochrony infrastruktury krytycznej i całego jednolitego rynku cyfrowego. Takie wspólne inwestycje mogą obejmować inwestycje w infrastrukturę kwantową i zasoby danych na potrzeby cyberbezpieczeństwa, orientację sytuacyjną w cyberprzestrzeni, w tym krajowe ***CSIRT oraz*** SOC tworzące europejską tarczę cyberbezpieczeństwa, a także inne narzędzia, które zostaną udostępnione sektorowi publicznemu i prywatnemu w całej Europie.

w całej Europie.

Or. en

Poprawka 216
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Załącznik I – akapit 1 – punkt 1
Rozporządzenie (UE) 2021/694
Załącznik I – rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie”

Tekst proponowany przez Komisję	*Poprawka*
5. Promowanie solidarności między państwami członkowskimi w zakresie przygotowania się i reagowania na poważne incydenty w cyberbezpieczeństwie poprzez transgraniczne wdrażanie usług w zakresie cyberbezpieczeństwa, w tym wspieranie udzielania wzajemnej pomocy między organami publicznymi i ustanowienie rezerwy zaufanych dostawców usług w zakresie ***cyberbezpieczeństwa*** na poziomie Unii.	5. Promowanie solidarności między państwami członkowskimi w zakresie przygotowania się i reagowania na poważne incydenty w cyberbezpieczeństwie poprzez transgraniczne wdrażanie usług w zakresie cyberbezpieczeństwa, w tym wspieranie udzielania wzajemnej pomocy między organami publicznymi i ustanowienie rezerwy zaufanych dostawców usług ***zarządzanych*** w zakresie ***bezpieczeństwa*** na poziomie Unii.

Or. en