Parlament Europejski
2019-2024

Dokument z posiedzenia

A9-0426/2023

8.12.2023

***I
SPRAWOZDANIE

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

Komisja Przemysłu, Badań Naukowych i Energii

Sprawozdawczyni: Lina Gálvez Muñoz

Objaśnienie używanych znaków

*	Procedura konsultacji
***	Procedura zgody
***I	Zwykła procedura ustawodawcza (pierwsze czytanie)
***II	Zwykła procedura ustawodawcza (drugie czytanie)
***III	Zwykła procedura ustawodawcza (trzecie czytanie)

(Wskazana procedura opiera się na podstawie prawnej zaproponowanej w projekcie aktu)

Poprawki do projektu aktu

Poprawki Parlamentu w postaci dwóch kolumn

Skreślenia zaznacza się ***wytłuszczonym drukiem i kursywą*** w lewej kolumnie. Zmianę brzmienia zaznacza się ***wytłuszczonym drukiem i kursywą*** w obu kolumnach. Nowy tekst zaznacza się ***wytłuszczonym drukiem i kursywą*** w prawej kolumnie.

Pierwszy i drugi wiersz nagłówka każdej poprawki wskazuje element rozpatrywanego projektu aktu, którego dotyczy poprawka. Jeżeli poprawka odnosi się do obowiązującego aktu, do którego zmiany zmierza projekt aktu, nagłówek zawiera dodatkowo trzeci wiersz wskazujący obowiązujący akt i czwarty wiersz wskazujący przepis tego aktu, którego dotyczy poprawka.

Poprawki Parlamentu w postaci tekstu skonsolidowanego

Nowe fragmenty tekstu zaznacza się ***wytłuszczonym drukiem i kursywą***. Fragmenty tekstu, które zostały skreślone, zaznacza się za pomocą symbolu ▌ lub przekreśla. Zmianę brzmienia zaznacza się przez wyróżnienie nowego tekstu ***wytłuszczonym drukiem i kursywą*** i usunięcie lub przekreślenie zastąpionego tekstu.
Tytułem wyjątku nie zaznacza się zmian o charakterze ściśle technicznym wprowadzonych przez służby w celu opracowania końcowej wersji tekstu.

SPIS TREŚCI

Strona

PROJEKT REZOLUCJI USTAWODAWCZEJ PARLAMENTU EUROPEJSKIEGO

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

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Parlament Europejski,

– uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2023)0209),

– uwzględniając art. 294 ust. 2 oraz art. 173 ust. 3 i art. 322 ust. 1 lit. a) Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C9-0136/2023),

– uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 13 lipca 2023 r.[1],

– uwzględniając art. 59 Regulaminu,

– uwzględniając opinie przedstawione przez Komisję Spraw Zagranicznych oraz Komisję Transportu i Turystyki,

– uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii (A9-0426/2023),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zatwierdza swoje oświadczenie załączone do niniejszej rezolucji;

3. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

4. zobowiązuje swoją przewodniczącą do przekazania stanowiska Parlamentu Radzie i Komisji, a także parlamentom narodowym.

[1] Dz.U. C 349 z 29.9.2023, s. 167.

Poprawka 1

POPRAWKI PARLAMENTU EUROPEJSKIEGO*

do wniosku Komisji

2023/0109 (COD)

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 *oraz zmieniające rozporządzenie (UE) 2021/694*

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 173 ust. 3 i art. 322 ust. 1 lit. a),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Trybunału Obrachunkowego[2],

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[3],

uwzględniając opinię Komitetu Regionów[4],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu***, ale równocześnie stały się źródłem potencjalnych podatności*** we wszystkich sektorach działalności gospodarczej ***i demokracji***, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.

---

* Poprawki: tekst nowy lub zmieniony został zaznaczony wytłuszczonym drukiem i kursywą; symbol ▌ sygnalizuje skreślenia.

2 Dz.U. C […] z […], s. […].

3 Dz.U. C […] z […], s. […].

4 Dz.U. C […] z […], s. […].

(2) ***W całej Unii i na całym świecie rosną – pod względem metod i skutków –*** 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 ***oraz szkody dla gospodarek i demokracji 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 ***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. ***Potrzebna jest zatem ścisła i skoordynowana współpraca między sektorem publicznym, sektorem prywatnym, środowiskiem akademickim, społeczeństwem obywatelskim i mediami. Ponadto Unia musi skoordynować swoją reakcję z instytucjami międzynarodowymi, a także z zaufanymi partnerami międzynarodowymi o podobnych poglądach. Zaufani partnerzy międzynarodowi o podobnych poglądach to kraje, które podzielają unijne wartości demokracji, zaangażowanie na rzecz praw człowieka, faktyczny multilateralizm i porządek oparty na zasadach, zgodnie z ramami i umowami o współpracy międzynarodowej. Aby zapewnić współpracę z zaufanymi partnerami międzynarodowymi o podobnych poglądach oraz ochronę przed rywalami systemowymi, podmioty mające siedzibę w państwach trzecich, które nie są stronami GPA, nie powinny mieć możliwości udziału w zamówieniach publicznych na podstawie niniejszego rozporządzenia.***

(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[5], konieczne jest zwiększenie odporności obywateli, przedsiębiorstw***, w szczególności mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (MŚP), w tym przedsiębiorstw typu start-up,*** i podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, ***w tym organów lokalnych lub regionalnych,*** które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastruktury i usługi ***oraz budowanie zdolności z myślą o rozwoju umiejętności w dziedzinie cyberbezpieczeństwa***, 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

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

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.

(3a) Cyberataki są często wymierzone w lokalne, regionalne lub krajowe usługi publiczne i infrastrukturę. Władze lokalne należą do najbardziej podatnych celów cyberataków ze względu na brak zasobów finansowych i ludzkich. Dlatego szczególnie ważne jest, aby uświadomić decydentom na szczeblu lokalnym potrzebę zwiększenia odporności cyfrowej i zdolności do ograniczania skutków cyberataków oraz wykorzystania możliwości przewidzianych w niniejszym rozporządzeniu.

(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[6], zalecenie Komisji (UE) 2017/1584[7], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[8] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[9]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

(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 ***do nich*** **,** reagować na nie ***i usuwać ich skutki***. W konkluzjach Rady o pozycji UE w kwestiach cyberprzestrzeni państwa członkowskie wezwały również Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego[10].

---

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

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

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

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

[10] Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. (9364/22).

(6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”[11], przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej ***sieci*** centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka.

(7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do ***zapobiegania poważnym incydentom*** w cyberbezpieczeństwie i ***incydentom*** w cyberbezpieczeństwie na dużą skalę ***oraz reagowania na nie***. Dlatego należy wprowadzić ogólnoeuropejską ***sieć*** SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej ***oraz zwiększenia zdolności Unii do wykrywania zagrożeń i wymiany informacji;*** należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków; należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

(8) Aby osiągnąć te cele, należy również w niektórych obszarach zmienić rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694[12]. W szczególności niniejszym rozporządzeniem należy zmienić rozporządzenie (UE) 2021/694 przez dodanie nowych celów operacyjnych związanych z europejską tarczą cyberbezpieczeństwa i mechanizmem cyberkryzysowym w ramach celu szczegółowego nr 3 programu „Cyfrowa Europa”, który to cel obejmuje zagwarantowanie odporności, integralności i wiarygodności jednolitego rynku cyfrowego, zwiększenie zdolności w zakresie monitorowania cyberataków i cyberzagrożeń oraz reagowania na nie, a także wzmocnienie współpracy transgranicznej w dziedzinie cyberbezpieczeństwa. Jako uzupełnienie tych zmian należy ustanowić szczegółowe warunki, na jakich można przyznawać wsparcie finansowe na te działania, i określić mechanizmy zarządzania i koordynacji niezbędne do osiągnięcia zamierzonych celów. Inne zmiany rozporządzenia (UE) 2021/694 powinny obejmować opisy proponowanych działań w ramach nowych celów operacyjnych, jak również mierzalne wskaźniki umożliwiające monitorowanie realizacji tych nowych celów operacyjnych.

(9) Finansowanie działań na podstawie niniejszego rozporządzenia należy przewidzieć w rozporządzeniu (UE) 2021/694, które powinno pozostać właściwym aktem podstawowym dla tych działań objętych celem szczegółowym nr 3 programu „Cyfrowa

---

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

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa” oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

Europa”. Szczegółowe warunki uczestnictwa dotyczące każdego działania zostaną określone w odpowiednich programach prac zgodnie z mającym zastosowanie przepisem rozporządzenia (UE) 2021/694.

(9a) W świetle zmian geopolitycznych i rosnącego zagrożenia cyberbezpieczeństwa oraz w celu zapewnienia ciągłości i dalszego opracowywania środków określonych w niniejszym rozporządzeniu na okres po 2027 r., w szczególności europejskiej tarczy cyberbezpieczeństwa i mechanizmu cyberkryzysowego, konieczne jest zapewnienie specjalnej linii budżetowej w wieloletnich ramach finansowych na lata 2028–2034. Państwa członkowskie powinny również dążyć do tego, by zobowiązać się do wspierania wszelkich niezbędnych środków służących ograniczeniu cyberzagrożeń i cyberincydentów w całej Unii oraz do zwiększenia solidarności.

(10) Do niniejszego rozporządzenia zastosowanie mają horyzontalne zasady finansowe przyjęte przez Parlament Europejski i Radę na podstawie art. 322 TFUE. Zasady te są ustanowione w rozporządzeniu ***Parlamentu Europejskiego i Rady (UE) 2018/1046***[13]. i określają w szczególności procedurę uchwalania i wykonywania budżetu Unii oraz przewidują kontrole odpowiedzialności podmiotów upoważnionych do działań finansowych. Zasady przyjęte na podstawie art. 322 TFUE obejmują również ogólny system warunkowości służący ochronie budżetu Unii ustanowiony w rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092[14].

(11) Do celów należytego zarządzania finansami należy ustanowić przepisy szczegółowe dotyczące przenoszenia niewykorzystanych środków na zobowiązania i środków na płatności. Z poszanowaniem zasady, że budżet Unii jest ustalany corocznie, w niniejszym rozporządzeniu należy – ze względu na nieprzewidywalny, wyjątkowy i specyficzny charakter krajobrazu cyberbezpieczeństwa – przewidzieć – obok możliwości określonych w rozporządzeniu ***(UE, Euratom) 2018/1046*** – możliwość przenoszenia niewykorzystanych środków, a tym samym maksymalnie zwiększyć zdolność mechanizmu cyberkryzysowego do wspierania państw członkowskich w skutecznym zwalczaniu cyberzagrożeń.

(11a) Mechanizm cyberkryzysowy i unijna rezerwa cyberbezpieczeństwa ustanowione w niniejszym rozporządzeniu są nowymi inicjatywami, których nie przewidziano przy ustanawianiu wieloletnich ram finansowych na lata 2021–2027, a finansowanie tych inicjatyw ma zminimalizować zmniejszenie finansowania innych priorytetów programu „Cyfrowa Europa”. Należy zatem zmniejszyć kwotę zasobów finansowych przeznaczonych na unijną rezerwę bezpieczeństwa cybernetycznego i pozyskać ją przede wszystkim z nieprzydzielonych marginesów w ramach pułapów wieloletnich ram finansowych lub uruchomić za pośrednictwem nietematycznych instrumentów szczególnych wieloletnich ram finansowych. Wszelkie przeznaczanie lub realokację środków z istniejących programów należy ograniczyć do absolutnego minimum, aby

---

13 ***Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

14 ***Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092 z dnia 16 grudnia 2020 r. w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii (Dz.U. L 433I z 22.12.2020, s. 1)ELI: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32020R2092).***

chronić istniejące programy, w szczególności Erasmus+, przed negatywnymi skutkami i zapewnić, aby programy te mogły osiągnąć wyznaczone cele.

(12) Aby skuteczniej zapobiegać cyberzagrożeniom i cyberincydentom, oceniać je i 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. ***Proaktywne podejście do identyfikowania i łagodzenia potencjalnych cyberzagrożeń oraz zapobiegania im obejmuje zwiększenie zaawansowanych zdolności wykrywania cyberataków, niezbędnych do powstrzymania zaawansowanych, trwałych zagrożeń. Dane wywiadowcze dotyczące zagrożeń to informacje gromadzone, analizowane i interpretowane w celu zrozumienia potencjalnych zagrożeń i ryzyka. Analizując i korelując ogromne ilości danych, wskazują one wzorce, tendencje i oznaki naruszenia integralności systemu, które mogą ujawnić szkodliwe działania lub podatności.*** Należy wprowadzić unijną ***sieć*** 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 zaawansowanego gromadzenia danych i narzędzia analityki, zwiększając zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz zapewniając orientację sytuacyjną w czasie rzeczywistym. ***Krajowa SOC to scentralizowana jednostka odpowiedzialna 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 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[15].

(13) ***Aby uczestniczyć w tarczy cyberbezpieczeństwa, każde*** państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym państwie członkowskim. ***Zachęca się państwa członkowskie do włączenia zdolności krajowych SOC do istniejącej struktury cyberbezpieczeństwa i zarządzania cyberbezpieczeństwem, aby uniknąć tworzenia dodatkowych warstw zarządzania i dostosować niniejsze rozporządzenie do istniejących aktów ustawodawczych, 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 krajowych SOC***, w europejskiej tarczy cyberbezpieczeństwa oraz powinny zapewniać, aby informacje o cyberzagrożeniach uzyskiwane od podmiotów publicznych i prywatnych skutecznie i sprawnie

[15] 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).

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.***

(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 tym gromadzenia i wymiany danych i informacji na temat ewentualnego hakowania, nowo opracowanych złośliwych zagrożeń i exploitów, które nie zostały jeszcze wykorzystane w cyberincydentach, oraz wysiłków analitycznych,*** 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 ***i bezpiecznym*** otoczeniu ***przy wsparciu ze strony ENISA, w kwestiach związanych ze współpracą operacyjną między państwami członkowskimi***. ***Transgraniczne SOC powinny ułatwiać i promować wymianę informacji w zaufanym i bezpiecznym środowisku oraz*** zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, zespołach reagowania na incydenty bezpieczeństwa komputerowego („CSIRT") i innych odpowiednich podmiotach oraz uzupełniając je.

(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 infrastruktury cyberbezpieczeństwa, w szczególności stanowi uzupełnienie*** sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych***, zwłaszcza ich SOC***, oraz wymienianie takich danych, zwiększanie wartości takich danych dzięki analizie eksperckiej oraz wspólnie nabytym infrastrukturom i najnowocześniejszym narzędziom oraz poprzez wkład w ***suwerenność technologiczną*** Unii***, jej otwartą strategiczną autonomię, konkurencyjność i odporność oraz w rozwój znaczącego ekosystemu cyberbezpieczeństwa, w tym we współpracy z zaufanymi partnerami międzynarodowymi o podobnych poglądach***. .

(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)***, 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, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności, w ***tym gromadzenie i udostępnianie danych i informacji na temat ewentualnego hakowania, nowo opracowanych złośliwych zagrożeń i exploitów, które nie zostały jeszcze wykorzystane w cyberincydentach, oraz działań analitycznych***. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.

(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[16] 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 ***Rady*** (UE) 2018/1993[17]. 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 dyrektywą (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.

(18) Podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny zapewnić wysoki poziom interoperacyjności między sobą, w tym w stosownych przypadkach w odniesieniu do formatów danych, taksonomii, narzędzi przetwarzania i analizy danych oraz bezpiecznych kanałów komunikacji, minimalnego poziomu bezpieczeństwa warstwy aplikacji, tablicy wskaźników orientacji sytuacyjnej oraz samych wskaźników. Przy przyjmowaniu wspólnej taksonomii i opracowywaniu wzoru sprawozdań sytuacyjnych na potrzeby opisywania technicznej przyczyny i skutków

---

16 ***Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Tekst mający znaczenie dla EOG) (***Dz.U. L 347 z 20.12.2013, s. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

17 ***Decyzja wykonawcza Rady (UE) 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (***Dz.U. L 320 z 17.12.2018, s. 28, ***ELI: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32018D1993).***

incydentów w cyberbezpieczeństwie należy uwzględnić trwające prace nad zgłaszaniem incydentów w kontekście wdrażania dyrektywy (UE) 2022/2555.

(19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym ***i bezpiecznym*** środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury ***oraz 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.

(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną, ***autonomię strategiczną, konkurencyjność i odporność oraz sprzyjać znaczącemu ekosystemowi cyberbezpieczeństwa Unii***. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. ***Sztuczna inteligencja jest najskuteczniejsza w połączeniu z analizą dokonywaną przez człowieka. W związku z tym do gromadzenia wysokiej jakości danych niezbędna pozostaje wykwalifikowana siła robocza.*** Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173[18].

(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***.

(22) Wymiana informacji między uczestnikami europejskiej tarczy cyberbezpieczeństwa powinna być zgodna z obowiązującymi wymogami prawnymi, w szczególności z unijnymi i krajowymi przepisami o ochronie danych, a także z unijnymi regułami konkurencji regulującymi wymianę informacji. Odbiorca informacji powinien wdrożyć – o ile konieczne jest przetwarzanie danych osobowych – środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą, oraz zniszczyć

[18] 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). ***ELI: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021R1173***).

dane, gdy tylko przestaną one być niezbędne do określonego celu, i poinformować organ udostępniający dane o ich zniszczeniu.

(23) Bez uszczerbku dla art. 346 TFUE wymiana informacji, które zgodnie z przepisami unijnymi lub krajowymi mają status informacji poufnych, powinna być ograniczona do tego, co jest istotne i proporcjonalne do celów tej wymiany. Podczas wymiany takich informacji należy zachować poufność informacji oraz chronić bezpieczeństwo i interesy handlowe danych podmiotów, z pełnym poszanowaniem tajemnic handlowych i tajemnic przedsiębiorstwa.

(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”).

(25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach PESCO[19] i zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii i w państwach trzecich.

(26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL[20], IPCR[21], i dyrektywy (UE) 2022/2555. Może on wnosić wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również skoordynowane,

---

[19] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.

[20] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

[21] Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

w stosownych przypadkach, z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej.

(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*** a zainteresowanym państwem członkowskim. Wnioskując o wsparcie w ramach mechanizmu cyberkryzysowego, państwo członkowskie powinno przedstawić odpowiednie informacje uzasadniające potrzebę wsparcia.

(28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych.

(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe”). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi

sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554[22]. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

(30) Ponadto w ramach mechanizmu cyberkryzysowego należy oferować wsparcie innych działań w zakresie gotowości i wsparcie gotowości w innych sektorach, nieobjętych skoordynowanym testowaniem podmiotów działających w sektorach wysoce krytycznych. Działania te mogą obejmować różnego rodzaju krajowe działania związane z gotowością.

(31) Mechanizm cyberkryzysowy powinien również zapewniać wsparcie działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych. W stosownych przypadkach powinien on uzupełniać UMOL, aby zapewnić kompleksowe podejście do reagowania na skutki incydentów w cyberbezpieczeństwie dla obywateli.

(32) Mechanizm cyberkryzysowy powinien wspierać pomoc udzielaną przez państwa członkowskie państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555. Udzielające pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.

(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, ***przy jednoczesnym wzmocnieniu odporności Unii, w tym udziału europejskich dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy są MŚP, oraz stworzeniu ekosystemu cyberbezpieczeństwa, w szczególności mikroprzedsiębiorstw, MŚP, w tym przedsiębiorstw typu start-up, z inwestycjami w badania naukowe i innowacje służące opracowaniu najnowocześniejszych technologii, takich jak technologie związane z chmurą i sztuczną inteligencją***. ***Zaufani dostawcy, w tym MŚP, powinni móc współpracować ze sobą w celu spełnienia powyższych kryteriów.*** Usługi z unijnej rezerwy

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

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 związku z tym rezerwa cyberbezpieczeństwa 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. ***Komisja powinna zapewnić zaangażowanie państw członkowskich i szeroko zakrojoną wymianę informacji z nimi, aby uniknąć powielania podobnych inicjatyw, w tym w ramach Organizacji Traktatu Północnoatlantyckiego (NATO).***

(34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach krytycznych lub wysoce krytycznych. ***Należy zachęcać do udziału mniejszych dostawców działających na szczeblu regionalnym i lokalnym.***

(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. ***Aby realizować dodatkowe zadania wynikające z tego przepisu, ENISA powinna otrzymać odpowiednie, dodatkowe finansowanie.***

(36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, państwami członkowskimi, Komisją i innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi UE. Jeżeli chodzi o sektor prywatny, ENISA opracowuje kanały wymiany informacji z wyspecjalizowanymi dostawcami, w tym z dostawcami i sprzedawcami rozwiązań zarządzanych w zakresie bezpieczeństwa, aby realizować misję ENISA polegającą na osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu

oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji i powinno ono stanowić wkład w ich prace. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja udostępni sprawozdanie również wysokiemu przedstawicielowi.

(37) Biorąc pod uwagę nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa" mogą otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli jest to przewidziane w odpowiednim układzie o stowarzyszeniu z tym programem. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa".

(37a) Państwa trzecie mogłyby uzyskać dostęp do zasobów i wsparcia zgodnie z niniejszym rozporządzeniem, korzystając ze wsparcia w zakresie reagowania na incydenty z unijnej rezerwy cyberbezpieczeństwa. Ponadto w celu świadczenia określonych usług w ramach unijnej rezerwy cyberbezpieczeństwa mogą być potrzebni dostawcy z państw trzecich, w tym z państw trzecich stowarzyszonych z programem „Cyfrowa Europa" lub innych państw będącymi partnerami międzynarodowymi oraz państw należących do NATO świadczący usługi reagowania na incydenty. Na zasadzie odstępstwa od rozporządzenia (UE, Euratom) 2018/1046, w celu wzmocnienia suwerenności technologicznej Unii, jej otwartej strategicznej autonomii, konkurencyjności i odporności oraz w celu ochrony jej strategicznych aktywów, interesów lub bezpieczeństwa nie należy zezwalać na udział podmiotów mających siedzibę w państwach trzecich, które nie przystąpiły do GPA i które nie zostały poddane monitorowaniu w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/452[23] i w razie potrzeby objęte środkami ograniczania ryzyka z uwzględnieniem celów określonych w niniejszym rozporządzeniu. Wymiar zewnętrzny niniejszego rozporządzenia powinien być zgodny z postanowieniami układu o stowarzyszeniu w programie „Cyfrowa Europa". Udział państw trzecich powinien podlegać kontroli publicznej z udziałem władzy ustawodawczej, aby zapewnić obywatelom możliwość udziału w tym procesie.

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/452 z dnia 19 marca 2019 r. ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii (Dz.U. L 79I z 21.3.2019, s. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

(38) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze do określenia warunków interoperacyjności między transgranicznymi SOC; określenia ustaleń proceduralnych dotyczących wymiany informacji między transgranicznymi SOC a podmiotami unijnymi na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę; ustanowienia wymogów technicznych zapewniających bezpieczeństwo europejskiej tarczy cyberbezpieczeństwa; określenia rodzaju i liczby usług reagowania wymaganych do celów unijnej rezerwy cyberbezpieczeństwa; oraz doprecyzowania szczegółowych ustaleń dotyczących przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011*.

---

* ***Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13, ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj).***

(38a) 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, na wszystkich terytoriach, 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. Wszystkie środki służące zwiększeniu umiejętności w dziedzinie cyberbezpieczeństwa wymagają zabezpieczeń, aby uniknąć drenażu mózgów i ryzyka dla mobilności pracowników.

(38b) Trzeba podnosić specjalistyczne, interdyscyplinarne i ogólne umiejętności i kompetencje w całej Unii, ze szczególnym uwzględnieniem kobiet, ponieważ w dziedzinie cyberbezpieczeństwa utrzymują się dysproporcje między płciami, a średnia światowa reprezentacja kobiet wynosi 20 %. Kobiety muszą być obecne i uczestniczyć w projektowaniu cyfrowej przyszłości i zarządzaniu nią.

(38c) Wzmocnienie badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa ma zwiększyć odporność i otwartą strategiczną autonomię Unii. Podobnie ważne jest

stworzenie synergii z programami w zakresie badań naukowych i innowacji oraz z istniejącymi instrumentami i instytucjami, a także wzmocnienie współpracy i koordynacji między różnymi zainteresowanymi stronami, w tym sektorem prywatnym, społeczeństwem obywatelskim, środowiskiem akademickim, państwami członkowskimi, Komisją i ENISA.

(38d) Niniejsze rozporządzenie powinno przyczynić się do realizacji zobowiązania zapisanego w Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie do ochrony interesów naszych demokracji, obywateli, przedsiębiorstw i instytucji publicznych przed ryzykiem w cyberprzestrzeni i cyberprzestępczością, w tym przed naruszaniem ochrony danych oraz kradzieżą tożsamości lub manipulowaniem tożsamością. Stosowanie niniejszego rozporządzenia powinno również przyczynić się do poprawy wdrażania innych przepisów, na przykład dotyczących sztucznej inteligencji, prywatności danych i regulacji danych pod względem cyberbezpieczeństwa i cyberodporności.

(38e) Kluczowe znaczenie dla skutecznego wdrożenia niniejszego rozporządzenia będzie miał rozwój kultury cyberbezpieczeństwa, w której bezpieczeństwo, w tym bezpieczeństwo środowiska cyfrowego, uznaje się za dobro publiczne. Dlatego kolejnym środkiem gwarantującym ochronę naszych demokracji i podstawowych wartości powinno być opracowanie metod włączania i zwiększania świadomości obywateli.

(38f) W celu uzupełnienia niektórych innych niż istotne elementów niniejszego rozporządzenia należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE, określających warunki interoperacyjności między transgranicznymi SOC, ustalenia proceduralne dotyczące wymiany informacji między transgranicznymi SOC a EU-CyCLONe, siecią CSIRT i Komisją, rodzaje i liczbę usług reagowania wymaganych do celów unijnej rezerwy cyberbezpieczeństwa oraz doprecyzujących szczegółowe ustalenia dotyczące przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa*. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

**** Dz.U. L 123 z 12.5.2016, s. 1, ELI: https://eur-lex.europa.eu/eli/agree_interinstit/2016/512/oj.***

(39) ***Ponieważ cel*****e** niniejszego rozporządzenia***, a mianowicie wzmocnienie unijnych zdolności w zakresie zapobiegania cyberzagrożeniom, ich wykrywania, reagowania na nie oraz usuwania ich skutków oraz ustanowienie ogólnych ram przełamujących sztywne struktury komunikacyjne, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie,*** 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. ***Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze*** rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Rozdział I

CELE OGÓLNE, PRZEDMIOT I DEFINICJE

Artykuł 1

Przedmiot i cele

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:

a) wprowadzenie ogólnoeuropejskiej ***sieci*** centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa”) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej;

b) stworzenie mechanizmu cyberkryzysowego, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków;

c) ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny poważnych incydentów lub incydentów na dużą skalę.

2. Celem niniejszego rozporządzenia jest zwiększenie solidarności na szczeblu unijnym przez następujące cele szczegółowe:

a) wzmocnienie wspólnego unijnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, co umożliwi ***zwiększenie potencjału przemysłowego Unii i jej państw członkowskich w sektorze cyberbezpieczeństwa oraz*** wzmocnienie konkurencyjnej pozycji sektorów przemysłu***, zwłaszcza mikroprzedsiębiorstw, MŚP***, ***w tym przedsiębiorstw typu start-up,*** i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w suwerenność technologiczną Unii w dziedzinie cyberbezpieczeństwa***, jej otwartą strategiczną autonomię, konkurencyjność i odporność w tym sektorze, wzmacniając ekosystem cyberbezpieczeństwa w celu zapewnienia znacznych zdolności Unii, w tym we współpracy z partnerami międzynarodowymi***;

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”;

c) zwiększenie odporności Unii i przyczynianie się do skutecznej reakcji dzięki przeglądowi i ocenie poważnych incydentów lub incydentów na dużą skalę, w tym wyciągnięciu wniosków i w stosownych przypadkach wydaniu zaleceń.

ca) skoordynowane rozwijanie umiejętności, know-how i kompetencji siły roboczej w celu zapewnienia cyberbezpieczeństwa i stworzenia synergii z Akademią Umiejętności w dziedzinie Cyberbezpieczeństwa.

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.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

-1a) „krajowe centrum monitorowania bezpieczeństwa” („krajowe SOC”) oznacza scentralizowaną jednostkę, która stale gromadzi i analizuje informacje wywiadowcze o cyberzagrożeniach oraz poprawia stan cyberbezpieczeństwa zgodnie z art. 4;

1) **„transgraniczne centrum monitorowania bezpieczeństwa”** ***lub*** **„transgraniczne SOC”** oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC ***zgodnie z art. 5***;

2) **„podmiot publiczny”** oznacza ***podmioty prawa publicznego zdefiniowane*** w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE[24];

3) **„konsorcjum przyjmujące”** oznacza konsorcjum składające się z państw uczestniczących, reprezentowanych przez krajowe SOC, ***zgodnie z art. 5***;

4) **„podmiot”** oznacza podmiot zdefiniowany w art. 6 pkt 38 dyrektywy (UE) 2022/2555;

4a) „podmiot krytyczny” oznacza podmiot krytyczny zdefiniowany w art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557[25];

5) „podmioty działające w sektorach krytycznych lub wysoce krytycznych” oznaczają podmioty ***w sektorach wymienionych*** w ***załącznikach*** I i ▌ II do dyrektywy (UE) 2022/2555;

---

[24] 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).

[25] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164, ELI: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022L2557).

5a) „obsługa incydentu" oznacza obsługę incydentu zdefiniowaną w art. 6 pkt 8 dyrektywy (UE) 2022/2555;

5b) „ryzyko" oznacza ryzyko zdefiniowane w art. 6 pkt 9 dyrektywy (UE) 2022/2555;

6) „**cyberzagrożenie**" oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

6a) „poważne cyberzagrożenie" oznacza znaczące cyberzagrożenie zdefiniowane w art. 6 pkt 11 dyrektywy (UE) 2022/2555;

7) „**poważny incydent w cyberbezpieczeństwie**" oznacza incydent w cyberbezpieczeństwie spełniający kryteria określone w art. 23 ust. 3 dyrektywy (UE) 2022/2555;

8) „**incydent w cyberbezpieczeństwie na dużą skalę**" oznacza incydent zdefiniowany w art. 6 pkt 7 dyrektywy (UE) 2022/2555;

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;

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;

10a) „dostawca usług zarządzanych w zakresie bezpieczeństwa" oznacza dostawcę usług zarządzanych zdefiniowanego w art. 6 pkt 40 dyrektywy (UE) 2022/2555;

11) „**zaufani dostawcy *usług zarządzanych w zakresie bezpieczeństwa***" oznaczają dostawców usług zarządzanych w zakresie bezpieczeństwa wybranych ***do włączenia do unijnej rezerwy cyberbezpieczeństwa*** zgodnie z art. 16 niniejszego rozporządzenia.

Rozdział II

EUROPEJSKA TARCZA CYBERBEZPIECZEŃSTWA

Artykuł 3

Ustanowienie europejskiej tarczy cyberbezpieczeństwa

1. W celu rozwijania zaawansowanych zdolności w Unii w zakresie wykrywania, analizowania i przetwarzania danych dotyczących cyberzagrożeń ***oraz zapobiegania cyberincydentom*** w Unii ustanawia się ***sieć*** centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa"). W jej skład wchodzą wszystkie krajowe centra monitorowania bezpieczeństwa („krajowe SOC") oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC").

Działania służące wdrażaniu europejskiej tarczy cyberbezpieczeństwa wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

2. Europejska tarcza cyberbezpieczeństwa:

a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł za pośrednictwem transgranicznych SOC***, a w stosownych przypadkach wymienia informacje z siecią CSIRT***;

b) generuje wysokiej jakości i użyteczne operacyjnie informacje i dane wywiadowcze dotyczące cyberzagrożeń, wykorzystując najnowocześniejsze narzędzia, w szczególności sztuczną inteligencję i technologie analityki danych;

c) przyczynia się do lepszej ochrony przed cyberzagrożeniami i lepszego reagowania na nie***, także dzięki wydawaniu podmiotom konkretnych zaleceń***;

d) przyczynia się do szybszego wykrywania cyberzagrożeń i zapewniania orientacji sytuacyjnej w całej Unii;

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.

Jest ona rozwijana we współpracy z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną na podstawie rozporządzenia (UE) 2021/1173.

Artykuł 4

Krajowe centra monitorowania bezpieczeństwa

1. Aby ***móc*** uczestniczyć w europejskiej tarczy cyberbezpieczeństwa, każde państwo członkowskie wyznacza co najmniej jeden krajowy SOC. Krajowy SOC jest ***scentralizowaną jednostką w podmiocie*** publicznym. ***W miarę możliwości krajowy SOC włącza się do CSIRT lub innych istniejących infrastruktur cyberbezpieczeństwa i struktur zarządzania cyberbezpieczeństwem.***

Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym***, zwłaszcza ich krajowych SOC,*** w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie***, w stosownych przypadkach wymiany tych informacji z członkami sieci CSIRT danego państwa członkowskiego, a także*** wnoszenia wkładu w transgraniczny SOC. Jest on wyposażony w najnowocześniejsze technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie ***oraz zapobiegania im***.

Krajowy SOC lub CSIRT może wystąpić o dane telemetryczne, dane z czujników lub dane z rejestrów ich krajowych podmiotów krytycznych do dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy świadczą usługę na rzecz podmiotu krytycznego. Dane te są udostępniane zgodnie z unijnymi przepisami o ochronie danych i wyłącznie jako wsparcie dla krajowego SOC lub CSIRT w wykrywaniu zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz zapobieganiu im.

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.

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

Artykuł 5

Transgraniczne centra monitorowania bezpieczeństwa

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. ***Transgraniczny SOC ma na celu wykrywanie i analizę cyberzagrożeń, zapobieganie incydentom i wspieranie generowania wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami i wspólne rozwijanie zdolności w zakresie wykrywania i analizy cyberataków, zapobiegania im i ochrony przed nimi w zaufanym i bezpiecznym środowisku.***

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 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.

2a. Na zasadzie odstępstwa od art. 176 rozporządzenia (UE, Euratom) 2018/1046 podmioty, które mają siedzibę w państwach trzecich i nie są stronami GPA, nie biorą udziału we wspólnych zamówieniach na narzędzia i infrastruktury.

3. Członkowie konsorcjum przyjmującego zawierają pisemną umowę konsorcjum określającą ich wewnętrzne ustalenia dotyczące wykonania umowy o przyjęciu i użytkowaniu.

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.

Artykuł 6

Współpraca i wymiana informacji w ramach transgranicznych SOC i między nimi

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:

a) ***usprawnia wymianę danych wywiadowczych na temat cyberzagrożeń między krajowymi i transgranicznymi SOC oraz branżowymi ISAC w celu zapobiegania zagrożeniom, ich wykrywania lub łagodzenia ich skutków;***

b) zwiększa poziom cyberbezpieczeństwa, zwłaszcza przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub wspieranie badań nad zagrożeniami prowadzonych w ramach współpracy między podmiotami publicznymi i prywatnymi.

2. Pisemna umowa konsorcjum, o której mowa w art. 5 ust. 3, określa:

a) zobowiązanie do udostępniania ***istotnych*** danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;

b) ramy zarządzania zachęcające wszystkich uczestników do wymiany informacji;

c) cele dotyczące wkładu w rozwój zaawansowanych narzędzi sztucznej inteligencji i analityki danych.

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, można zharmonizować standardy i protokoły wymiany informacji z międzynarodowymi standardami i najlepszymi praktykami branżowymi. Zachęca się również do wspólnych zamówień na infrastrukturę, usługi i narzędzia w zakresie cyberbezpieczeństwa. Ponadto*** po konsultacji z ECCC ***i ENISA do dnia... [sześć miesięcy od dnia wejścia w życie niniejszego rozporządzenia] Komisja może zgodnie z art. 20a przyjąć akty delegowane w celu uzupełnienia niniejszego rozporządzenia poprzez określenie warunków*** tej interoperacyjności ***w ścisłym porozumieniu z transgranicznymi SOC i w oparciu o standardy międzynarodowe i najlepsze praktyki branżowe***.

4. Transgraniczne SOC zawierają między sobą ***i, w stosownych przypadkach, z branżowymi ISAC*** umowy o współpracy określające zasady wymiany informacji ***i interoperacyjności*** między platformami transgranicznymi ***z uwzględnieniem istniejących już odpowiednich mechanizmów wymiany informacji przewidzianych w dyrektywie (UE) 2022/2555***. ***W stosownych przypadkach transgraniczne SOC zawierają umowy o współpracy z branżowymi ISAC. W kontekście potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę mechanizmy wymiany informacji muszą być zgodne z odpowiednimi przepisami dyrektywy (UE) 2022/2555.***

Artykuł 7

Współpraca i wymiana informacji z *siecią CSIRT*

1. W przypadku gdy transgraniczne SOC uzyskają informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę ***na potrzeby wspólnej orientacji sytuacyjnej***, ***koordynujący SOC*** bez zbędnej zwłoki ***przekazuje*** istotne informacje ***swojemu CSIRT lub właściwemu organowi, które przekażą te informacje*** EU-CyCLONe, sieci CSIRT***,*** Komisji ***i ENISA zależnie od ich odpowiednich ról*** w zarządzaniu kryzysowym ***i związanych z tym procedur*** zgodnie z dyrektywą (UE) 2022/2555. ***Niniejszy ustęp nie nakłada na podmioty publiczne ani prywatne żadnych dodatkowych obowiązków w zakresie informowania o potencjalnym lub trwającym incydencie w cyberbezpieczeństwie na dużą skalę na potrzeby wypełnienia obowiązków określonych w dyrektywie (UE) 2022/2555.***

2. Komisja ***jest uprawniona do przyjmowania zgodnie z art. 20a i po konsultacji z siecią CSIRT aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia przez określenie ustaleń proceduralnych dotyczących*** wymiany informacji przewidzianej w ust. 1 ***niniejszego artykułu i zgodnie z dyrektywą (UE) 2022/2555***.

Artykuł 8

Bezpieczeństwo

1. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają wysoki poziom ***poufności i*** 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.

2. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają, aby wymiana informacji w ramach europejskiej tarczy cyberbezpieczeństwa z podmiotami, które nie są podmiotami publicznymi państw członkowskich, nie wpływała negatywnie na interesy Unii w zakresie bezpieczeństwa.

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

Rozdział III

MECHANIZM CYBERKRYZYSOWY

Artykuł 9

Ustanowienie mechanizmu cyberkryzysowego

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”).

2. Działania służące wdrażaniu mechanizmu ▌ wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

Artykuł 10

Rodzaje działań

1. W ramach mechanizmu wspiera się następujące rodzaje działań:

a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych w całej Unii;

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 ***usług zarządzanych w zakresie bezpieczeństwa*** uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12;

c) działania w zakresie wzajemnej pomocy polegające na udzielaniu pomocy przez organy krajowe jednego państwa członkowskiego innemu państwu członkowskiemu, w szczególności zgodnie z art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555.

1a. Po uruchomieniu mechanizmu Komisja co roku ocenia zarówno pozytywne, jak i negatywne aspekty działania mechanizmu, rozstrzygając również, czy potrzebne są dodatkowe wymogi w zakresie współpracy lub szkoleń, i publikuje sprawozdanie na ten temat.

Artykuł 11

Skoordynowane testowanie gotowości podmiotów

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 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 ***zgodnie z ustaleniami określonymi w odniesieniu do podmiotów w sektorach kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555***.

2. Grupa współpracy NIS we współpracy z Komisją, ENISA***,*** wysokim przedstawicielem ***i podmiotami podlegającymi skoordynowanemu testowaniu gotowości na podstawie ust. 1*** opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania ***gotowości, których efektem końcowym jest wspólny plan prac***. ***Podmioty podlegające skoordynowanemu testowaniu gotowości opracowują i wdrażają plan działań naprawczych, w ramach którego realizują zalecenia wynikające z testów gotowości.***

Grupa współpracy NIS może pomóc w ustaleniu sektorów lub podsektorów, które w pierwszej kolejności powinny podlegać skoordynowanemu testowaniu gotowości.

Artykuł 12

Ustanowienie unijnej rezerwy cyberbezpieczeństwa

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.

Jeżeli okaże się, że zamówionych usług nie można w pełni wykorzystać jako wsparcia w reagowaniu na poważne incydenty lub incydenty na dużą skalę, usługi te można w drodze

wyjątku przekształcić w ćwiczenia lub szkolenia, które instytucja zamawiająca organizuje na życzenie użytkowników, by pomóc im w radzeniu sobie z incydentami.

2. Unijna rezerwa cyberbezpieczeństwa składa się z usług reagowania na incydenty świadczonych przez zaufanych dostawców ***usług zarządzanych w zakresie bezpieczeństwa*** wybranych zgodnie z kryteriami określonymi w art. 16. ***Unijna*** rezerwa ***cyberbezpieczeństwa*** obejmuje wcześniej zadeklarowane usługi. Usługi te muszą być możliwe do wprowadzenia we wszystkich państwach członkowskich ***oraz muszą zwiększać suwerenność technologiczną Unii, jej otwartą strategiczną autonomię, konkurencyjność i odporność w sektorze cyberbezpieczeństwa, także dzięki pobudzaniu innowacji na jednolitym rynku cyfrowym w całej Unii***.

3. Użytkownikami usług z unijnej rezerwy cyberbezpieczeństwa są:

a) organy państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie i CSIRT, o których mowa odpowiednio w art. 9 ust. 1 i 2 oraz w art. 10 dyrektywy (UE) 2022/2555;

b) instytucje, organy i jednostki organizacyjne Unii***, o których mowa w art. 3 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) .../2023[26], oraz CERT-UE***.

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.

5. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja decyduje o priorytetach i rozwoju unijnej rezerwy cyberbezpieczeństwa ***w porozumieniu z grupą współpracy 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.

6. Komisja ***powierza*** ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu.

7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, ***w tym niezbędnych umiejętności i zdolności pracowników sektora cyberbezpieczeństwa,*** po konsultacji z państwami członkowskimi i Komisją***, a w stosownych przypadkach dostawcami usług zarządzanych w zakresie bezpieczeństwa i innymi przedstawicielami branży cyberbezpieczeństwa***. ENISA przygotowuje podobne zestawienie, po konsultacji z Komisją***, dostawcami usług zarządzanych w zakresie bezpieczeństwa, a w stosownych przypadkach innymi przedstawicielami branży cyberbezpieczeństwa***, 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***.

---

[26] ***Rozporządzenie (UE) .../2023 ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii (Dz.U. C z , s. , ELI: ...).***

8. Komisja ***jest uprawniona do przyjmowania zgodnie z art. 20a aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia przez szczegółowe określenie rodzajów i liczby*** usług reagowania wymaganych na potrzeby unijnej rezerwy cyberbezpieczeństwa. ▌

Artykuł 13

Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa

1. Użytkownicy, o których mowa w art. 12 ust. 3, mogą składać wnioski o usługi z unijnej rezerwy cyberbezpieczeństwa w celu wsparcia reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów.

2. Aby otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, użytkownicy, o których mowa w art. 12 ust. 3, stosują środki łagodzące skutki incydentu będącego przedmiotem wniosku o wsparcie, które to środki obejmują zapewnienie bezpośredniej pomocy technicznej i innych zasobów, aby wspomóc reagowanie na incydent, oraz działania służące natychmiastowemu usunięciu skutków incydentu.

3. Wnioski o wsparcie składane przez użytkowników, o których mowa w art. 12 ust. 3 lit. a) niniejszego rozporządzenia, przekazuje się Komisji i ENISA za pośrednictwem pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego przez państwo członkowskie zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555.

4. Państwa członkowskie informują sieć CSIRT i w stosownych przypadkach EU-CyCLONe o swoich wnioskach o wsparcie w reagowaniu na incydenty i w natychmiastowym usuwaniu skutków incydentów na podstawie niniejszego artykułu.

5. Wnioski o wsparcie w reagowaniu na incydenty i w natychmiastowym usuwaniu skutków incydentów zawierają:

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;

b) informacje o środkach zastosowanych w celu złagodzenia skutków incydentu będącego przedmiotem wniosku o wsparcie, o których to środkach mowa w ust. 2;

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.

6. ENISA, we współpracy z Komisją i grupą współpracy NIS, opracowuje wzór ułatwiający składanie wniosków o wsparcie z unijnej rezerwy cyberbezpieczeństwa.

7. Komisja ***jest uprawniona do przyjmowania zgodnie z art. 20a*** aktów ***delegowanych w celu uzupełnienia niniejszego rozporządzenia przez doprecyzowanie szczegółowych ustaleń dotyczących*** przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. ▌

Artykuł 14

Wdrożenie wsparcia z unijnej rezerwy cyberbezpieczeństwa

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 ▌ przekazywana użytkownikom, o których mowa w art. 12 ust. 3***, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin***.

2. Aby ustalić hierarchię ważności wniosków w przypadku istnienia równocześnie wielu wniosków, w stosownych przypadkach uwzględnia się następujące kryteria:

a) dotkliwość incydentu w cyberbezpieczeństwie;

b) rodzaj podmiotu, na który incydent ma wpływ, przy czym jako ważniejsze traktuje się incydenty mające wpływ na podmioty kluczowe zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2022/2555;

c) potencjalne skutki dla państw członkowskich lub użytkowników, na których incydent ma wpływ;

d) ***skalę oraz*** potencjalny transgraniczny charakter incydentu i ryzyko rozprzestrzenienia się incydentu na inne państwa członkowskie lub na innych użytkowników;

e) środki zastosowane przez użytkownika w celu wsparcia reagowania oraz działania służące natychmiastowemu usunięciu skutków incydentu, o których to środkach i działaniach mowa w art. 13 ust. 2 i art. 13 ust. 5 lit. b).

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 potrzebne do świadczenia odnośnej usługi***.

4. Umowy, o których mowa w ust. 3, ***opierają*** się na wzorach przygotowanych przez ENISA po konsultacji z państwami członkowskimi ***i, w stosownych przypadkach, innymi użytkownikami 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 rażącego niedbalstwa, jakiego dopuszczono się w ocenie wniosku dostawcy usługi, lub przypadków, w których Komisja lub ENISA są użytkownikami unijnej rezerwy cyberbezpieczeństwa zgodnie z art. 14 ust. 3***.

6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji***,*** ENISA***, sieci CSIRT i – 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.
Sprawozdanie sporządza się z poszanowaniem prawa unijnego i krajowego dotyczącego ochrony informacji szczególnie chronionych lub niejawnych.

7. Komisja regularnie***, co najmniej dwa razy w roku*** składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia. ***Informacje poufne chronione są***

w sprawozdaniu zgodnie z prawem unijnym i krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych.

Artykuł 15

Koordynacja z mechanizmami zarządzania kryzysowego

1. W przypadkach gdy poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę wynikają z klęsk lub katastrof zdefiniowanych w decyzji nr 1313/2013/UE[27] lub skutkują takimi klęskami lub katastrofami, wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na takie incydenty uzupełnia działania podejmowane na podstawie decyzji nr 1313/2013/UE i pozostaje bez uszczerbku dla tej decyzji.

2. W przypadku wystąpienia transgranicznego incydentu w cyberbezpieczeństwie na dużą skalę, w którym uruchamiane są zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na taki incydent odbywa się zgodnie z odpowiednimi protokołami i procedurami w ramach IPCR.

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 ***TUE***.

4. Wsparcie w ramach mechanizmu cyberkryzysowego może stanowić część wspólnej reakcji Unii i państw członkowskich w sytuacjach, o których mowa w art. 222 ***TFUE***.

Artykuł 16

Zaufani dostawcy

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:

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;

b) zapewnienie ochrony podstawowych interesów Unii i jej państw członkowskich w zakresie bezpieczeństwa;

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***, jak również w zapewnienie równowagi płci w sektorze oraz wzmacnianie***

[27] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

suwerenności technologicznej, otwartej strategicznej autonomii, konkurencyjności i odporności Unii.

2. Przy zamawianiu usług na potrzeby unijnej rezerwy cyberbezpieczeństwa instytucja zamawiająca uwzględnia w dokumentach zamówienia następujące kryteria kwalifikacji:

a) dostawca musi wykazać, że jego personel charakteryzuje się najwyższym stopniem uczciwości zawodowej, niezależności, odpowiedzialności i kompetencji technicznych niezbędnych do wykonywania działań w danej dziedzinie oraz zapewnia trwałość/ciągłość wiedzy fachowej, a także wymagane zasoby techniczne;

b) dostawca, jego jednostki zależne i podwykonawcy muszą dysponować ramami chroniącymi informacje szczególnie chronione dotyczące usług, a w szczególności dowody, ustalenia i sprawozdania, oraz zgodnymi z unijnymi przepisami bezpieczeństwa dotyczącymi ochrony informacji niejawnych UE;

c) dostawca musi dostarczyć wystarczające dowody na to, że jego struktura zarządzania jest przejrzysta, nie zagraża jego bezstronności i jakości świadczonych przez niego usług ani nie powoduje konfliktów interesów;

d) dostawca musi posiadać odpowiednie poświadczenie bezpieczeństwa, przynajmniej w odniesieniu do personelu mającego wprowadzać usługi;

e) dostawca musi dysponować odpowiednim poziomem bezpieczeństwa swoich systemów informatycznych;

f) dostawca musi być wyposażony w ***nowoczesny*** sprzęt i oprogramowanie techniczne niezbędne do obsługi żądanej usługi***, a w stosownych przypadkach musi przestrzegać przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) .../...[28] (2022/0272(COD))***;

g) dostawca musi być w stanie wykazać, że ma doświadczenie w świadczeniu podobnych usług odpowiednim organom krajowym lub podmiotom działającym w sektorach krytycznych lub wysoce krytycznych;

h) dostawca musi być w stanie zapewnić usługę w krótkim terminie w państwach członkowskich, w których może świadczyć tę usługę;

i) dostawca musi być w stanie zapewnić usługę w języku lokalnym państw członkowskich, w których może świadczyć tę usługę***, lub w jednym z języków roboczych instytucji unijnych***;

j) po wprowadzeniu ***europejskiego*** programu certyfikacji ***cyberbezpieczeństwa*** usług zarządzanych w zakresie bezpieczeństwa ***na mocy rozporządzenia*** (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem ***w ciągu dwóch lat od jego przyjęcia;***

ja) dostawca musi być w stanie świadczyć usługę niezależnie, a nie w ramach pakietu, tak by użytkownik miał możliwość zmiany dostawcy usług;

jb) do celów art. 12 ust. 1 dostawca musi uwzględnić w ofercie przetargowej możliwość przekształcenia niewykorzystanych usług reagowania na incydenty w ćwiczenia lub szkolenia;

---

[28] ***Rozporządzenie Parlamentu Europejskiego i Rady (UE) .../... z dnia ... w sprawie ... (Dz.U. L z ., …, ELI: …).***

jc) dostawca musi mieć siedzibę i zarządcze struktury wykonawcze w Unii, państwie stowarzyszonym lub państwie trzecim, które przystąpiło do Porozumienia w sprawie zamówień rządowych Światowej Organizacji Handlu (GPA);

jd) dostawca nie może podlegać kontroli ze strony niestowarzyszonego państwa trzeciego lub podmiotu z niestowarzyszonego państwa trzeciego, które nie przystąpiło do GPA, lub alternatywnie podmiot ten musi zostać uprzednio poddany monitorowaniu w rozumieniu rozporządzenia (UE) 2019/452 i w razie potrzeby objęty środkami ograniczania ryzyka z uwzględnieniem celów określonych w niniejszym rozporządzeniu.

Artykuł 17

Wsparcie dla państw trzecich

1. Państwa trzecie mogą wystąpić z wnioskiem o wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli przewidują to układy o stowarzyszeniu zawarte w związku z uczestnictwem tych państw w programie „Cyfrowa Europa”.

2. Wsparcie z unijnej rezerwy cyberbezpieczeństwa musi być zgodne z niniejszym rozporządzeniem i z wszelkimi szczegółowymi warunkami określonymi w układach o stowarzyszeniu, o których mowa w ust. 1.

3. Do użytkowników ze stowarzyszonych państw trzecich kwalifikujących się do otrzymania usług z unijnej rezerwy cyberbezpieczeństwa należą właściwe organy, takie jak CSIRT i organy ds. zarządzania kryzysowego w cyberbezpieczeństwie.

4. Każde państwo trzecie kwalifikujące się do wsparcia z unijnej rezerwy cyberbezpieczeństwa wyznacza organ, który będzie pełnił funkcję pojedynczego punktu kontaktowego do celów niniejszego rozporządzenia.

5. Przed otrzymaniem jakiegokolwiek wsparcia z unijnej rezerwy cyberbezpieczeństwa państwa trzecie przekazują Komisji i wysokiemu przedstawicielowi informacje na temat swoich zdolności w zakresie cyberodporności i zarządzania ryzykiem, w tym co najmniej informacje na temat środków krajowych wprowadzonych w celu przygotowania się na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, a także informacje na temat odpowiedzialnych podmiotów krajowych, w tym CSIRT lub równoważnych podmiotów, ich zdolności i przydzielonych im zasobów. W przypadku gdy w przepisach art. 13 i 14 niniejszego rozporządzenia mowa jest o państwach członkowskich, przepisy te mają zastosowanie do państw trzecich określonych w ust. 1.

6. Komisja ***bez zbędnej zwłoki powiadamia Radę i*** koordynuje z wysokim przedstawicielem działania dotyczące otrzymanych wniosków i wdrażania wsparcia przyznanego państwom trzecim z unijnej rezerwy cyberbezpieczeństwa.

Rozdział IV

MECHANIZM PRZEGLĄDU INCYDENTÓW W CYBERBEZPIECZEŃSTWIE

Artykuł 18

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***, urzędów*** i jednostek organizacyjnych UE, dostawców usług zarządzanych w zakresie bezpieczeństwa w ***krajowych i transgranicznych*** SOC i użytkowników usług w zakresie cyberbezpieczeństwa***, uzyskując od nich informacje zwrotne i uzupełniając je gwarancjami i monitorowaniem, które pozwalają upewnić się, że wyciągnięte wnioski i wskazane najlepsze praktyki spotykają się z poparciem podmiotów z branży 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. ***Sprawozdanie nie ujawnia szczegółów na temat aktywnie wykorzystywanych podatności, którym nie udało się jeszcze zaradzić.***

3a. Sprawozdanie, o którym mowa w ust. 1 niniejszego artykułu, zawiera wnioski wyciągnięte z ocen wzajemnych przeprowadzonych zgodnie z art. 19 dyrektywy (UE) 2022/2555.

4. W stosownych przypadkach sprawozdanie zawiera zalecenia **–** ***także dla wszystkich zainteresowanych stron*** **–** mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

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

Rozdział V

PRZEPISY KOŃCOWE

Artykuł 19

Zmiany w rozporządzeniu (UE) 2021/694

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

1) w art. 6 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

(***i***) dodaje się lit. aa) w brzmieniu:

„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;”;

(***ii***) dodaje się lit. g) w brzmieniu:

„g) utworzeniu i obsłudze mechanizmu cyberkryzysowego w celu wspierania państw członkowskich w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i reagowaniu na nie, stanowiącego uzupełnienie krajowych zasobów i zdolności oraz innych form wsparcia dostępnych na szczeblu Unii, w tym utworzeniu unijnej rezerwy cyberbezpieczeństwa.”;

b) ust. 2 otrzymuje brzmienie:

„2. Działania w ramach celu szczegółowego nr 3 będą realizowane przede wszystkim za pośrednictwem Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieci krajowych ośrodków koordynacji zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887*, z wyjątkiem działań służących wdrażaniu unijnej rezerwy cyberbezpieczeństwa, które będą realizowane przez Komisję i ENISA. ▌

---

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (Dz.U. L 202 z 8.6.2021, s. 1**,** ***ELI: http://data.europa.eu/eli/reg/2021/887/oj***).***”;***

2) w art. 9 wprowadza się następujące zmiany:

a) ust. 2 lit. b), c) i d) otrzymują brzmienie:

„b) 1 776 956 000 EUR na cel szczegółowy nr 2 – »Sztuczna inteligencja«;

c) ***1 620 566 000*** EUR na cel szczegółowy nr 3 – »Cyberbezpieczeństwo i zaufanie«;

d) ***500 347 000*** EUR na cel szczegółowy nr 4 – »Zaawansowane umiejętności cyfrowe«;”;

aa) dodaje się nowy ust. 2a w brzmieniu:

„2a) Kwotę, o której mowa w ust. 2 lit. c), wykorzystuje się przede wszystkim do realizacji celów operacyjnych określonych w art. 6 ust. 1 lit. a)–f) Programu.”;

ab) dodaje się nowy ust. 2b w brzmieniu:

„2b) Kwota przeznaczona na utworzenie i wdrażanie unijnej rezerwy cyberbezpieczeństwa nie może przekroczyć 27 mln EUR w planowanym okresie obowiązywania rozporządzenia 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.”;

b) dodaje się ust. 8 w brzmieniu:

„8. Na zasadzie odstępstwa od art. 12 ust. 4 rozporządzenia (UE, Euratom) 2018/1046 niewykorzystane środki na zobowiązania i środki na płatności przeznaczone na działania ***dotyczące wdrażania unijnej rezerwy cyberbezpieczeństwa i*** służące osiągnięciu celów określonych w art. 6 ust. 1 lit. g) niniejszego rozporządzenia są automatycznie przenoszone i mogą być przeznaczane na zobowiązania i płatności realizowane do dnia 31 grudnia następnego roku budżetowego.

Komisja informuje Parlament Europejski i Radę o środkach przeniesionych zgodnie z art. 12 ust. 6 rozporządzenia (UE, Euratom) 2018/1046.”;

3) art. 14 ust. 2 otrzymuje brzmienie:

„2. Program może zapewniać finansowanie w dowolnej formie przewidzianej w rozporządzeniu ***(UE, Euratom) 2018/1046***, w tym w szczególności poprzez zamówienia stanowiące podstawową formę lub poprzez dotacje i nagrody.

W przypadku gdy osiągnięcie celu działania wymaga zamówienia innowacyjnych towarów i usług, dotacje można przyznać tylko beneficjentom będącym instytucjami zamawiającymi lub podmiotami zamawiającymi zdefiniowanymi w dyrektywach Parlamentu Europejskiego i Rady 2014/24/UE[27] i 2014/25/UE[28].

W przypadku gdy do osiągnięcia celów działania niezbędne jest dostarczenie innowacyjnych towarów lub usług, które nie są jeszcze powszechnie dostępne na rynku, instytucja zamawiająca lub podmiot zamawiający mogą zezwolić na udzielenie więcej

niż jednego zamówienia w ramach tego samego postępowania o udzielenie zamówienia.

Z powodów należycie uzasadnionych względami bezpieczeństwa publicznego instytucja zamawiająca lub podmiot zamawiający mogą wymagać, aby miejsce wykonania zamówienia znajdowało się na terytorium Unii.

Realizując postępowania o udzielenie zamówienia na potrzeby unijnej rezerwy cyberbezpieczeństwa ustanowionej na mocy art. 12 rozporządzenia (UE) 2023/**...**, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz państw trzecich stowarzyszonych z Programem zgodnie z art. 10. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedając lub przekazując jako darowiznę towary i usługi, w tym przedmioty najmu, tym państwom trzecim. Na zasadzie odstępstwa od art. 169 ust. 3 rozporządzenia (UE) **.../...** wniosek jednego państwa trzeciego wystarcza, aby upoważnić Komisję lub ENISA do działania.

Realizując postępowania o udzielenie zamówienia na potrzeby unijnej rezerwy cyberbezpieczeństwa ustanowionej na mocy art. 12 rozporządzenia (UE) 2023/**...**, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz instytucji, organów i jednostek organizacyjnych Unii. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedając lub przekazując jako darowiznę towary i usługi, w tym przedmioty najmu, instytucjom, organom i jednostkom organizacyjnym Unii. Na zasadzie odstępstwa od art. 169 ust. 3 rozporządzenia (UE) **.../...** wniosek jednej instytucji, jednego organu lub jednej jednostki organizacyjnej Unii wystarcza, aby upoważnić Komisję lub ENISA do działania.

Program może również zapewniać finansowanie w formie instrumentów finansowych w operacjach łączonych.”;

4) dodaje się art. 16a w brzmieniu:

„***Artykuł 16a***

W przypadku działań służących wdrażaniu europejskiej tarczy cyberbezpieczeństwa ustanowionej na mocy art. 3 rozporządzenia (UE) 2023/XX przepisami mającymi zastosowanie są przepisy określone w art. 4 i 5 rozporządzenia (UE) 2023/**...**. W przypadku konfliktu między przepisami niniejszego rozporządzenia a przepisami art. 4 i 5 rozporządzenia (UE) 2023/**...** te ostatnie mają pierwszeństwo i mają zastosowanie do tych konkretnych działań.”;

5) art. 19 otrzymuje brzmienie:

„Dotacje w ramach Programu przyznaje się i zarządza się nimi zgodnie z tytułem VIII rozporządzenia ***(UE, Euratom) 2018/1046*** i mogą one pokrywać do 100 % kosztów kwalifikowalnych, bez uszczerbku dla zasady współfinansowania ustanowionej w art. 190 rozporządzenia ***(UE, Euratom) 2018/1046***. Takie dotacje przyznaje się i zarządza się nimi w sposób określony dla poszczególnych celów.

Wsparcie w formie dotacji może przyznawać bezpośrednio ECCC bez zaproszenia do składania wniosków krajowym SOC, o których mowa w art. 4 rozporządzenia ***(UE) .../...***, oraz konsorcjum przyjmującemu, o którym mowa w art. 5 rozporządzenia ***(UE) .../...***, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia ***(UE, Euratom) 2018/1046***.

Wsparcie w formie dotacji do celów mechanizmu cyberkryzysowego określonego w art. 10 rozporządzenia ***(UE) .../...*** może przyznawać bezpośrednio ECCC państwom członkowskim bez zaproszenia do składania wniosków, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia ***(UE, Euratom) 2018/1046***.

W przypadku działań określonych w art. 10 ust. 1 lit. c) rozporządzenia ***(UE) .../...*** ECCC informuje Komisję i ENISA o wnioskach państw członkowskich o udzielenie dotacji bezpośrednich bez zaproszenia do składania wniosków.

Do celów wsparcia wzajemnej pomocy w reagowaniu na poważny incydent w cyberbezpieczeństwie lub incydent w cyberbezpieczeństwie na dużą skalę, o której to wzajemnej pomocy mowa w art. 10 lit. c) rozporządzenia ***(UE) .../...***, oraz zgodnie z art. 193 ust. 2 akapit drugi lit. a) rozporządzenia ***(UE, Euratom) 2018/1046*** w należycie uzasadnionych przypadkach koszty można uznać za kwalifikowalne, nawet jeżeli zostały poniesione przed przedłożeniem wniosku o udzielenie dotacji.”;

6) w załącznikach I i II wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

Artykuł 19a
Dodatkowe zasoby dla ENISA

ENISA otrzymuje dodatkowe zasoby na realizację dodatkowych zadań powierzonych jej na mocy niniejszego rozporządzenia. To dodatkowe wsparcie, obejmujące również środki finansowe, nie może zagrażać realizacji celów innych programów unijnych, w szczególności programu „Cyfrowa Europa”.

Artykuł 20

Ocena *i przegląd*

1. 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 ▌.

2. Ocena ta dotyczy w szczególności:

a) wykorzystania i wartości dodanej transgranicznych SOC oraz stopnia, w jakim przyczyniają się one do szybszego wykrywania cyberzagrożeń i reagowania na nie oraz poprawy orientacji sytuacyjnej; aktywnego udziału krajowych SOC w europejskiej tarczy cyberbezpieczeństwa, w tym liczby ustanowionych krajowych i transgranicznych SOC oraz stopnia, w jakim przyczyniły się one do powstawania i wymiany wysokiej jakości użytecznych informacji operacyjnych i danych wywiadowczych dotyczących cyberzagrożeń; liczby i kosztów infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa, lub jednych i drugich nabytych w drodze wspólnych zamówień; liczby umów o współpracy zawartych między transgranicznymi SOC i z branżowymi ISAC; liczby incydentów zgłoszonych do sieci CSIRT i jej wpływu na działanie sieci CSIRT;

b) pozytywnych, jak i negatywnych aspektów działania mechanizmu cyberkryzysowego, w tym ewentualnej potrzeby wprowadzenia dodatkowych wymogów w zakresie współpracy lub szkoleń;

c) wkładu niniejszego rozporządzenia we wzmacnianie odporności i otwartej strategicznej autonomii Unii, poprawę konkurencyjności odpowiednich sektorów przemysłu, mikroprzedsiębiorstw i MŚP, w tym start-upów, oraz rozwój umiejętności w dziedzinie cyberbezpieczeństwa w Unii;

d) wykorzystania i wartości dodanej unijnej rezerwy cyberbezpieczeństwa, w tym liczby zaufanych dostawców usług bezpieczeństwa będących częścią tej rezerwy; liczby, rodzaju, kosztów i wpływu działań podjętych, by wesprzeć reagowanie na incydenty w cyberbezpieczeństwie, a także odnośnych użytkowników i dostawców; średniego czas odnotowania incydentu przez Komisję, zastosowania unijnej rezerwy cyberbezpieczeństwa i reakcji z jej strony oraz usunięcia skutków incydentu przez użytkownika; ewentualnej potrzeby rozszerzenia zakresu unijnej rezerwy cyberbezpieczeństwa o usługi w zakresie gotowości na incydenty lub wspólne ćwiczenia z udziałem zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa i potencjalnych użytkowników unijnej rezerwy cyberbezpieczeństwa, aby w razie konieczności zapewnić skuteczne jej funkcjonowanie;

e) wkładu niniejszego rozporządzenia w rozwój i doskonalenie umiejętności i kompetencji pracowników sektora cyberbezpieczeństwa niezbędnych do wzmocnienia

zdolności Unii do wykrywania cyberzagrożeń i incydentów w cyberbezpieczeństwie, zapobiegania im, reagowania na nie i usuwania ich skutków;

f) wkładu niniejszego rozporządzenia we wdrażanie i rozwój nowoczesnych technologii w Unii.

3. Na podstawie sprawozdań, o których mowa w ust. 1, Komisja w stosownych przypadkach przedkłada Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.

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. 6 ust. 3, art. 7 ust. 2, art. 12 ust. 8 i art. 13 ust. 7, powierza się Komisji na okres ... lat od ... [data wejścia w życie podstawowego aktu ustawodawczego lub inna data ustalona przez współprawodawców]. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu ... 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. 6 ust. 3, art. 7 ust. 2, 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 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. 6 ust. 3, art. 7 ust. 2, 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.

Artykuł 21

Procedura komitetowa

1. Komisję wspomaga Komitet Koordynacyjny ds. Programu „Cyfrowa Europa" ustanowiony rozporządzeniem (UE) 2021/694. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 22

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Strasburgu dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*

ZAŁĄCZNIK

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

(1) w załączniku I sekcja/rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie” otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

Program ma stymulować wzmocnienie, budowę i nabywanie podstawowych zdolności w celu zabezpieczenia unijnej gospodarki cyfrowej, społeczeństwa i demokracji poprzez wzmocnienie unijnego potencjału przemysłowego i konkurencyjności w dziedzinie cyberbezpieczeństwa, a także zwiększenie zdolności sektora prywatnego i publicznego do ochrony obywateli i przedsiębiorstw przed cyberzagrożeniami, w tym poprzez wspieranie wdrażania dyrektywy (UE) 2016/1148.

Początkowe, a w stosownych przypadkach późniejsze działania w ramach niniejszego celu obejmują:

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 w całej Europie.

2. Zwiększanie istniejących zdolności technologicznych i łączenie w sieć ośrodków kompetencji w państwach członkowskich oraz zapewnienie, aby zdolności te odpowiadały potrzebom sektora publicznego i przemysłu, w tym w odniesieniu do produktów i usług, które wzmacniają cyberbezpieczeństwo i zaufanie w ramach jednolitego rynku cyfrowego.

3. Zapewnienie szerokiego wdrożenia skutecznych, najnowocześniejszych rozwiązań z zakresu cyberbezpieczeństwa i zaufania w państwach członkowskich. Takie wdrożenie obejmuje zwiększenie bezpieczeństwa i ochrony produktów od momentu ich zaprojektowania do komercjalizacji.

4. Zapewnienie wsparcia w celu wyeliminowania luki w umiejętnościach w zakresie cyberbezpieczeństwa***, ze szczególnym uwzględnieniem osiągnięcia równowagi płci w branży,*** poprzez na przykład ujednolicenie programów dotyczących umiejętności w zakresie cyberbezpieczeństwa, dostosowanie ich do konkretnych potrzeb sektorowych ***z zastosowaniem podejścia interdyscyplinarnego i ogólnego*** oraz ułatwienie dostępu do

ukierunkowanych specjalistycznych szkoleń ***w trosce o umożliwienie bezwzględnie wszystkim osobom i terytoriom korzystania z możliwości przewidzianych w niniejszym rozporządzeniu***.

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 cyberbezpieczeństwa na poziomie Unii.";

(2) w załączniku II sekcja/rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie" otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

3.1. Liczba infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień ***w ramach tarczy cyberbezpieczeństwa***

3.2. Liczba użytkowników i społeczności użytkowników uzyskujących dostęp do europejskiej infrastruktury z zakresu cyberbezpieczeństwa

3.3. Liczba***, rodzaj, koszty i wpływ*** działań ***podjętych, by wesprzeć*** gotowość i reagowanie na incydenty w cyberbezpieczeństwie w ramach mechanizmu cyberkryzysowego ***Stopień przestrzegania i wypełnienia przez użytkowników zaleceń wynikających z testów gotowości, jak również średni czas odnotowania incydentu przez Komisję, zastosowania unijnej rezerwy cyberbezpieczeństwa i reakcji z jej strony oraz usunięcia skutków incydentu przez użytkownika".***

UZASADNIENIE

KONTEKST

Cyberbezpieczeństwo jest i powinno być podstawą naszych demokracji. Zagrożenia dla cyberbezpieczeństwa wiążą się z coraz większą niepewnością wśród obywateli i firm, a także ze wzrostem dezinformacji, co stanowi wyzwanie dla demokratycznych zasad chroniących poszanowanie praw człowieka. Aby temu zapobiec, nasze demokracje bezwzględnie potrzebują bezpiecznego środowiska cyfrowego podlegającego kontroli publicznej.

Cyberataki w UE nasilają się pod względem metod i skutków. Ponadto według sprawozdania ENISA opisującego krajobraz zagrożeń w 2022 r.[1] rosyjska napaść na Ukrainę spowodowała głębokie zmiany jeszcze przed inwazją i zapoczątkowała nową erę **oprogramowania cybernetycznego**. Priorytety określone w związku z tym konfliktem w cyberprzestrzeni to potrzeba **budowania zdolności** w **wielostronnych programach** i projektach oraz potrzeba szybkiego **doskonalenia umiejętności**. Aby zwiększyć odporność, pilnie potrzebujemy wspólnej europejskiej reakcji opartej na ściślejszej współpracy na poziomie europejskim i wykraczającej poza poziom krajowy.

Kluczowe znaczenie dla skutecznego wdrożenia omawianego rozporządzenia będzie miał rozwój kultury cyberbezpieczeństwa, w której bezpieczeństwo, w tym bezpieczeństwo środowiska cyfrowego, uznaje się za dobro publiczne.

Ponadto cyberataki są często wymierzone w **lokalne, regionalne lub krajowe usługi publiczne** i infrastrukturę (np. sektor opieki zdrowotnej, który pozostaje głównym celem cyberataków[2]). Z danych wynika również, że **władze lokalne** należą do najbardziej podatnych celów ze względu na brak zasobów finansowych i ludzkich, dlatego szczególnie istotne dla zwiększenia odporności cyfrowej jest zwiększenie świadomości wśród przywódców na szczeblu lokalnym[3]. Ataki wpływają przede wszystkim i bezpośrednio na obywateli, a tym samym zagrażają naszym demokracjom, także poprzez kampanie dezinformacyjne. Poczucie niepewności, jakie mogą wywołać w społeczeństwie takie sytuacje, może rodzić preferencje polityczne w postaci radykalnego zaangażowania na rzecz bezpieczeństwa ze szkodą dla poszanowania praw podstawowych. Powinno być jednak odwrotnie: bezpieczeństwo jest bowiem istotną częścią naszych demokracji, zgodną ze wszystkimi innymi prawami i niezbędną do ich realizacji.

Ponadto **firmy i MŚP** w UE również doświadczają cyberprzestępczości, a wraz z rosnącym wykorzystaniem sfery cyfrowej do prowadzenia działalności gospodarczej wzrasta obawa o cyberbezpieczeństwo. MŚP są gorzej przygotowane, dysponują mniejszymi zasobami potrzebnymi do ochrony, a nawet są mniej świadome, że mogą stać się celem takich ataków.

---

[1] ENISA, Threat Landscape 2022, październik 2022 r. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[2] ENISA, Threat Landscape: Health Sector, lipiec 2023 r. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[3] Europejski Komitet Regionów, Digital Resilience, 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

Przewiduje się, że w przyszłości ataki te nadal będą mieć miejsce, a wręcz się nasilą. Będzie do nich dochodzić zwłaszcza w niestabilnej sytuacji politycznej, a w szczególności w czasie wojny. Jako że transformacja cyfrowa postępuje każdego dnia, odporność cyfrowa staje się coraz ważniejsza dla naszego codziennego życia i dla **otwartej strategicznej autonomii UE**.

PROPOZYCJA SPRAWOZDAWCZYNI

Sprawozdawczyni uważa, że UE musi być lepiej przygotowana na przyszłość, i z zadowoleniem przyjmuje ten pilnie potrzebny akt prawny, który służy połączeniu zasobów, informacji i wiedzy w celu zapewnienia solidarności między państwami członkowskimi, zwiększenia potencjału przemysłowego w UE, **skoordynowanego rozwijania umiejętności i zdolności** na potrzeby cyberbezpieczeństwa, większej odporności na przyszłe ataki oraz ochrony naszych demokracji przed wykorzystywaniem we własnym interesie zapotrzebowania w zakresie bezpieczeństwa. Istotne jest też, by chronić integralność naszych procesów wyborczych. Ten akt prawny stanowi niezwykle ważne zobowiązanie na rzecz osiągnięcia celu **otwartej strategicznej autonomii**.

Z tych powodów UE potrzebuje silnego i **skoordynowanego zarządzania** oraz zorganizowanej współpracy z sektorem prywatnym, aby wspierać rozwój europejskiej branży cyberbezpieczeństwa. Konieczna jest również współpraca z międzynarodowymi partnerami o podobnym światopoglądzie, ale także z innymi krajami, które nie mają takich samych możliwości i mogą potrzebować pomocy w razie cyberataku. Unijny akt w sprawie cybersolidarności powinien dokładnie określić sposób zarządzania i nie powinien pokrywać się z już istniejącymi inicjatywami i przepisami, takimi jak dyrektywa NIS 2.

Wniosek opiera się w znacznym stopniu na dobrowolnej wymianie informacji między państwami członkowskimi. Z tego powodu sprawozdawczyni proponuje wzmocnienie gwarancji z myślą o budowaniu zaufania między państwami członkowskimi i zwiększenia ich udziału i współpracy, na przykład w odniesieniu do wspólnego nabywania infrastruktury czy zaangażowania władzy ustawodawczej, tak aby zapewnić zaufanie obywateli i **gwarancje demokratyczne**.

Po drugie sprawozdawczyni proponuje **zapewnienie budżetu** z przyszłych WRF na tę inicjatywę, również przy zaangażowaniu państw członkowskich, aby w ten sposób zagwarantować ciągłość działań proponowanych w unijnym akcie w sprawie cybersolidarności w okresie po 2027 r.

Po trzecie sprawozdawczyni proponuje, aby poprawić **strukturę zarządzania**, stworzyć jasną definicję zarządzania i powiązać ją z istniejącym prawodawstwem.

Proponuje ona również lepszą **koordynację** działań podejmowanych przez różne podmioty odpowiedzialne za cyberbezpieczeństwo w państwach członkowskich z myślą o zaoferowaniu wspólnej tarczy cyberbezpieczeństwa. Proponuje też, aby zwiększyć wkład ENISA w koordynację i interakcję między poszczególnymi podmiotami społeczności krajowych.

Jeśli chodzi o **nową rezerwę cyberbezpieczeństwa**, sprawozdawczyni uważa, że może ona rozwijać potencjał przemysłowy UE, w tym MŚP, przez inwestycje w badania naukowe i innowacje służące opracowywaniu nowoczesnych technologii, takich jak technologie

związane z chmurą i sztuczną inteligencją. Ponadto sprawozdawczyni proponuje utrzymanie udziału branży, wzmocnienie kryteriów i zaufania do jej udziału (tj. powiązanie tego udziału z przedsiębiorstwem krajowym lub lokalnym) przez wyjaśnienie **kryteriów** i definicji **suwerenności technologicznej**, a także zagwarantowanie równowagi między podmiotami spoza UE i z UE. Sprawozdawczyni proponuje też, aby w ramach **mechanizmu cyberkryzysowego** zastosować **system certyfikacji**, z którego mogliby skorzystać prywatni dostawcy, aby stworzyć długotrwałe i oparte na zaufaniu partnerstwo.

W odniesieniu do **mechanizmu przeglądu incydentów** sprawozdawczyni proponuje wzmocnienie roli ENISA i sektora prywatnego w SOC oraz zastosowanie odpowiednich gwarancji i monitorowania, aby sprawdzić, czy wyciągnięte wnioski spotykają się z poparciem podmiotów z branży. Poza tym sprawozdawczyni proponuje, aby uwzględnić wnioski wyciągnięte z ocen wzajemnych, jak określono w dyrektywie NIS 2, oraz zwiększyć finansowanie ENISA w celu zapewnienia skutecznego stosowania przepisów i odpowiedniej ochrony przed zagrożeniami cyberbezpieczeństwa.

Omawiany wniosek ma ponadto z definicji bardzo istotny **wymiar zewnętrzny**, ponieważ państwa trzecie mogą uzyskać dostęp do zasobów i wsparcia na podstawie unijnego aktu w sprawie cybersolidarności, korzystając ze wsparcia w zakresie reagowania na incydenty w ramach unijnej rezerwy cyberbezpieczeństwa, a rezerwa cybernetycznej nadal potrzebuje podmiotów z sektora prywatnego spoza UE. Wymiar zewnętrzny musi również podlegać kontroli publicznej z udziałem władzy ustawodawczej, aby zagwarantować obywatelom możliwość uczestniczenia w tym procesie. Cyberbezpieczeństwo należy uznać za dobro publiczne.

Jednym z głównych filarów niniejszego wniosku jest też rozwój umiejętności i kompetencji, który powinien wykraczać poza zwykłe inwestowanie w rozwój wiedzy i wspierać inwestowanie w dostęp wszystkich obywateli do szkolenia tych umiejętności. Sprawozdawczyni proponuje, aby zacieśnić relacje z **unijną Akademią Umiejętności w dziedzinie Cyberbezpieczeństwa**, która ma zaradzić niedoborowi talentów w dziedzinie cyberbezpieczeństwa przez połączenie inicjatyw prywatnych i publicznych oraz zapewnienie obywatelom szkoleń i certyfikacji. Będzie to wymagało zabezpieczeń, które pozwolą uniknąć drenażu mózgów i nie zaszkodzić mobilności pracowników.

Ponadto sprawozdawczyni proponuje, by inwestować i włączać aktywne działania na rzecz rozwoju umiejętności w tym sektorze, biorąc pod uwagę, że rok 2023 jest Europejskim Rokiem Umiejętności, a także by zwiększyć świadomość obywateli w tym obszarze. Działania te zostaną przygotowane w taki sposób, aby inwestycje nie zakłócały równowagi między państwami członkowskimi, ponieważ wysoki popyt i wysokie płace występujące obecnie w tym sektorze mogą prowadzić do pewnego rodzaju drenażu mózgów na rzecz lepiej płatnych stanowisk.

Z tych powodów sprawozdawczyni proponuje wzmocnienie specjalistycznych, interdyscyplinarnych i ogólnych umiejętności i kompetencji w całej UE ze szczególnym uwzględnieniem kobiet, gdyż w obszarze cyberbezpieczeństwa utrzymują się dysproporcje

między płciami, a średnia światowa reprezentacja kobiet wynosi 20 %[4]. Kobiety muszą być obecne i uczestniczyć w planowaniu cyfrowej przyszłości i zarządzaniu nią.

Sprawozdawczyni proponuje również, aby zacieśnić relacje między krajowymi centrami kompetencji, Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) i ENISA w zakresie rozwijania umiejętności i kompetencji. Ponadto trzeba wzmocnić rolę **branży** w **rozwijaniu umiejętności** i tworzeniu partnerstw ze **środowiskiem akademickim** i podmiotami społeczeństwa obywatelskiego, biorąc pod uwagę regionalne doświadczenie, wiedzę i specjalizację oraz sojusze państw trzecich i współpracując z partnerami o podobnym światopoglądzie, by zwiększać wymianę i zapewniać globalne podejście do wspierania obywateli, przedsiębiorstw i instytucji.

Sprawozdawczyni proponuje też współpracę w zakresie poszukiwania talentów i szacowania szkód ponoszonych przez ludzi w związku z cyberatakami (np. wpływ ataku typu ransomware na sektor zdrowia).

Sprawozdawczyni proponuje środki mające na celu włączenie i zwiększenie świadomości obywateli bez wzbudzania niepokoju jako kolejny sposób na zapewnienie ochrony naszych demokracji i podstawowych wartości. Proponuje rozwój **kultury cyberbezpieczeństwa**, w której bezpieczeństwo, w tym bezpieczeństwo środowiska cyfrowego, uznaje się za dobro publiczne. Dzięki temu będziemy w stanie zagwarantować model demokracji cyfrowej, który w przeciwieństwie do modelu cyfrowego autorytaryzmu opiera się na przejrzystości, demokracji i pewności, jaką może przynieść rozwój przepisów *ex ante*.

Sprawozdawczyni uważa poza tym, że nacisk na **badania i innowacje** w dziedzinie cyberbezpieczeństwa zwiększy odporność i otwartą strategiczną autonomię UE. Należy też zapewnić synergię z programami w zakresie badań i innowacji oraz z istniejącymi instrumentami i instytucjami, a także wzmocnić trójkąt wiedzy, aby zaradzić niedoborowi kwalifikacji w całej UE.

Przedmiotowe przepisy zwiększą także odporność UE i jej państw członkowskich, nie tylko bezpośrednio dzięki aktom prawnym dotyczącym cyberbezpieczeństwa i cyberodporności, lecz również dzięki możliwemu wpływowi na gwałtowny rozwój sztucznej inteligencji oraz wpływowi regulacji danych i prywatności danych na cyberbezpieczeństwo.

Ponadto przepisy te pomogą zrealizować zawarte w **Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie** zobowiązanie do ochrony interesów obywateli, przedsiębiorstw i instytucji publicznych przed zagrożeniami w cyberprzestrzeni i cyberprzestępczością, w tym przed naruszaniem ochrony danych oraz kradzieżą tożsamości lub manipulowaniem tożsamością.

W tym świetle sprawozdawczyni uważa, że należy jak najszybciej wdrożyć omawiany wniosek, w tym europejską tarczę cyberbezpieczeństwa i mechanizm cyberkryzysowy, aby stworzyć ogólne ramy i uniknąć efektu silosu, gdyż cyberprzestrzeń nie ma granic.

[4] Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie wspierania równouprawnienia płci w kształceniu i pracy zawodowej w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki (STEM) (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_PL.html#def_1_22

ZAŁĄCZNIK PODMIOTY LUB OSOBY, OD KTÓRYCH SPRAWOZDAWCZYNI OTRZYMAŁA INFORMACJE

Zgodnie z art. 8 załącznika I do Regulaminu sprawozdawczyni oświadcza, że przy sporządzaniu sprawozdania, do czasu przyjęcia go w komisji, otrzymała informacje od następujących podmiotów lub osób:

Podmiot lub osoba
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Powyższy wykaz został sporządzony na wyłączną odpowiedzialność sprawozdawczyni.

27.10.2023

OPINIA KOMISJI SPRAW ZAGRANICZNYCH

dla Komisji Przemysłu, Badań Naukowych i Energii

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

Sprawozdawca komisji opiniodawczej: Dragoş Tudorache

Poprawka 1

Wniosek dotyczący rozporządzenia
Motyw 1

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

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) Rosną skala, częstotliwość i wpływ	(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.

incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw, które to ataki mają na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. Stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Z uwagi na szybko zmieniający się krajobraz zagrożeń zagrożenie możliwymi incydentami na dużą skalę powodującymi poważne zakłócenie lub uszkodzenie infrastruktur krytycznych wymaga podwyższonej gotowości na wszystkich szczeblach unijnych ram cyberbezpieczeństwa. ***Zagrożenia te jeszcze się zwiększyły wraz z powrotem wojny do Europy. Te zagrożenia wykraczają*** poza rosyjską napaść na Ukrainę i prawdopodobnie ***będą*** się utrzymywać, biorąc pod uwagę wielość podmiotów powiązanych z organami państwowymi, ze środowiskami przestępczymi i haktywistycznymi, które mają swój udział w generowaniu obecnych napięć geopolitycznych. Takie incydenty mogą utrudniać świadczenie usług publicznych i prowadzenie działalności gospodarczej, w tym w sektorach krytycznych lub wysoce krytycznych, powodować znaczne straty finansowe, podważać zaufanie użytkowników, powodować poważne szkody dla gospodarki Unii, ***i bezpieczeństwa w Unii,*** a nawet mieć konsekwencje zagrażające zdrowiu lub życiu***, jeżeli na szwank zostanie narażona lokalna lub krajowa infrastruktura związana z bezpieczeństwem***. Ponadto incydenty w cyberbezpieczeństwie są nieprzewidywalne, ponieważ często pojawiają się i ewoluują w bardzo krótkim czasie, nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach. ***Cyberbezpieczeństwo jest ważne dla ochrony naszych europejskich wartości i zapewnienia funkcjonowania naszych demokracji poprzez ochronę***

	naszej infrastruktury wyborczej i procedur demokratycznych przed wszelką zagraniczną ingerencją.

Poprawka 3

Wniosek dotyczący rozporządzenia
Motyw 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2a) Ochrona cyberbezpieczeństwa jest niezbędna, jeśli chcemy zapewnić bezpieczeństwo Unii i nie pozwolić, by działające w złej wierze podmioty – państwowe i nie tylko – zagrażały naszej demokracji, gospodarce i bezpieczeństwu. Bezwzględnie należy zapobiegać rozdrobnieniu, ponieważ nie byłoby to odpowiednie podejście, w szczególności w obliczu wyzwania związanego z ewentualnymi przyszłymi cyberatakami na dużą skalę wymierzonymi w kilka państw członkowskich w tym samym czasie lub w transnarodową infrastrukturę krytyczną. A zatem potrzebny jest organ Unii, który działałby jako platforma koordynacji wszystkich istniejących i przyszłych instrumentów, funduszy i mechanizmów cyberbezpieczeństwa.

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(3) Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości	(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.

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

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

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

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE)	(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE)

2019/881[20]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

2019/881[20]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, ***proaktywnej,*** solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym. ***Ponadto w marcu 2022 r. Unia zatwierdziła i uruchomiła swój Strategiczny kompas na rzecz bezpieczeństwa i obrony, który koncentruje się między innymi na wzmocnieniu cyberbezpieczeństwa i zacieśnianiu współpracy międzynarodowej z sojusznikami i partnerami demokratycznymi i o podobnym podejściu, zwłaszcza w tej kwestii. Ponadto cyberbezpieczeństwo było centralnym punktem niedawnej trzeciej wspólnej deklaracji w sprawie współpracy UE–NATO ze stycznia 2023 r. W szczególności w swoim sprawozdaniu końcowym z oceny grupa zadaniowa UE-NATO zaleciła pełne wykorzystanie synergii między UE a NATO[1], w tym wymiany między podmiotami cywilnymi i wojskowymi najlepszych praktyk w zakresie wdrażania odpowiednich strategii i przepisów dotyczących cyberprzestrzeni.***

[1]

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

[17] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii,

[17] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii,

zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022).

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

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

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022).

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

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

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 6

Tekst proponowany przez Komisję	*Poprawka*
(6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”[22], przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE	(6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”[22], przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE

rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka.	rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka. ***Ponadto szybko zmieniający się krajobraz cyberzagrożeń i równie szybkie tempo rozwoju technologicznego wskazują także na potrzebę sprawniejszej koordynacji i współpracy cywilno-wojskowej, na co zwróciła uwagę Rada w swoich konkluzjach w sprawie polityki UE w zakresie cyberobrony[1].***
	[1] Konkluzje Rady w sprawie polityki UE w zakresie cyberobrony zatwierdzone przez Radę na posiedzeniu w dniu 22 maja 2023 r. (9618/23).
[22] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.	[22] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

Poprawka 7

Wniosek dotyczący rozporządzenia
Motyw 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(6a) Ze względu na zacieranie się granic między kwestiami cywilnymi a wojskowymi, a także możliwość podwójnego zastosowania cybernarzędzi i cybertechnologii konieczne jest kompleksowe i całościowe podejście do dziedziny cyfrowej. W przypadku incydentów i sytuacji kryzysowych na dużą skalę w cyberbezpieczeństwie, które dotyczą więcej niż jednego państwa członkowskiego, należy przewidzieć odpowiednie zarządzanie kryzysowe. Tego rodzaju struktury powinny umożliwić zorganizowanie wymiany informacji,

koordynacji i współpracy z unijnymi strukturami odpowiedzialnymi za bezpieczeństwo zewnętrzne i wojskowe zarządzanie kryzysowe oraz organami państw członkowskich odpowiedzialnymi za bezpieczeństwo i obronę (społecznością zajmującą się cyberobroną). Dotyczy to również operacji i misji w ramach wspólnej polityki bezpieczeństwa i obrony prowadzonych przez Unię w celu zapewnienia pokoju i stabilności w jej sąsiedztwie i poza nim.

Poprawka 8

Wniosek dotyczący rozporządzenia
Motyw 7

Tekst proponowany przez Komisję	*Poprawka*
(7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę. Dlatego należy wprowadzić ogólnoeuropejską infrastrukturę SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków; należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę.	(7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę. Dlatego należy wprowadzić ogólnoeuropejską infrastrukturę SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w ***tym incydenty dotyczące dwóch lub większej liczby państw członkowskich, w*** reagowaniu na nie i w natychmiastowym usuwaniu ich skutków***. Jeśli jest to konieczne i wykonalne, mechanizm cyberkryzysowy powinien organizować wymianę***

Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

informacji i współpracę z organami obrony państw członkowskich i być wspierany przez instytucje, organy i agencje UE (unijną społeczność zajmująca się cyberobroną); należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę***. Takie nowe struktury powinny również udzielać wsparcia operacjom i misjom UE w dziedzinie WPBiO***. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

Poprawka 9

Wniosek dotyczący rozporządzenia
Motyw 11

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

	wykorzystaniu najnowszych możliwości w dziedzinie sztucznej inteligencji (AI) i analizy danych.

Poprawka 10

Wniosek dotyczący rozporządzenia
Motyw 13

Tekst proponowany przez Komisję	*Poprawka*
(13) Każde państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym 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) 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. ***W razie potrzeby i jeśli jest to wykonalne SOC powinny umożliwiać również udział podmiotów działających w dziedzinie obrony dzięki ustanowieniu „filaru obronnego” w zakresie zarządzania i rodzaju udostępnianych informacji, zgodnie z propozycją zawartą we wspólnym komunikacie w sprawie polityki UE w zakresie cyberobrony[1] i popartą przez wysokiego przedstawiciela.*** ***[1] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.***

Poprawka 11

Wniosek dotyczący rozporządzenia
Motyw 14

Tekst proponowany przez Komisję	*Poprawka*
(14) W ramach europejskiej tarczy cyberbezpieczeństwa należy ustanowić szereg transgranicznych centrów monitorowania bezpieczeństwa („transgraniczne SOC"). Powinny one zrzeszać krajowe SOC z co najmniej trzech państw członkowskich, tak aby można było w pełni osiągnąć korzyści płynące z transgranicznego wykrywania zagrożeń, wymiany informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych SOC powinno być zwiększanie zdolności w zakresie analizy i wykrywania zagrożeń cyberbezpieczeństwa oraz zapobiegania 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, ***w tym „filar obrony",*** tak aby można było w pełni osiągnąć korzyści płynące z transgranicznego wykrywania zagrożeń, wymiany informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych SOC powinno być zwiększanie zdolności w zakresie analizy i wykrywania zagrożeń cyberbezpieczeństwa oraz zapobiegania im, wspieranie generowania wysokiej jakości danych wywiadowczych dotyczących zagrożeń cyberbezpieczeństwa, w szczególności w drodze wymiany danych z różnych źródeł publicznych lub prywatnych, a ***w razie konieczności i jeśli jest to wykonalne wojskowych, przy zapewnieniu wystarczających wytycznych dotyczących wymiany informacji, a*** także przez dzielenie się najnowocześniejszymi narzędziami i ich wspólne używanie oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń oraz zapobiegania im w zaufanym otoczeniu. Powinny one zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, zespołach reagowania na incydenty bezpieczeństwa komputerowego („CSIRT") i innych odpowiednich podmiotach oraz uzupełniając je.

Poprawka 12

Wniosek dotyczący rozporządzenia
Motyw 15

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

Poprawka 13

Wniosek dotyczący rozporządzenia
Motyw 16

Tekst proponowany przez Komisję	*Poprawka*
(16) Transgraniczne SOC powinny działać jako centralny punkt, który umożliwia szerokie gromadzenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwala na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy podmiotów (np. zespołów reagowania na incydenty komputerowe („CERT”), CSIRT, ośrodków wymiany i analizy informacji („ISAC”), operatorów infrastruktury krytycznej). Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze o zagrożeniach, oznaki naruszenia	(16) Transgraniczne SOC powinny działać jako centralny punkt, który umożliwia szerokie gromadzenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwala na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy podmiotów (np. zespołów reagowania na incydenty komputerowe („CERT”), CSIRT, ośrodków wymiany i analizy informacji („ISAC”), operatorów infrastruktury krytycznej ***oraz społeczności zajmującej się cyberobroną***). Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze

integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.	o zagrożeniach, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC***, a po jej ustanowieniu także z operacyjną siecią dla milCERT (MICNET)***.

Poprawka 14

Wniosek dotyczący rozporządzenia
Motyw 17

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

reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR”) na podstawie decyzji wykonawczej (UE) 2018/1993. W związku z tym w sytuacjach, w których transgraniczne SOC uzyskają informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, powinny przekazywać istotne informacje EU-CyCLONe, sieci CSIRT***, społeczności zajmującej się cyberobroną*** i Komisji. W szczególności, w zależności od sytuacji, przekazywane informacje mogą obejmować informacje techniczne, informacje na temat charakteru i motywów sprawcy lub potencjalnego sprawcy ataku oraz informacje nietechniczne wyższego szczebla na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę. W tym kontekście należy zwrócić należytą uwagę na zasadę ograniczonego dostępu oraz potencjalnie poufny charakter wymienianych informacji.

Poprawka 15

Wniosek dotyczący rozporządzenia
Motyw 19

Tekst proponowany przez Komisję	*Poprawka*
(19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów i terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii	(19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury***, z wyjątkiem dostawców wysokiego ryzyka dostarczających krytyczne produkty z elementami cyfrowymi***. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów i terminowe ostrzeganie organów i odpowiednich

sztucznej inteligencji i analityki danych.	podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych. ***Przy korzystaniu ze sztucznej inteligencji należy zadbać o sprawowanie nadzoru przez człowieka oraz zapewnić wystarczający poziom umiejętności w zakresie sztucznej inteligencji, niezbędne wsparcie i uprawnienia do wykonywania tej funkcji.***

Poprawka 16

Wniosek dotyczący rozporządzenia
Motyw 19 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(19a) Zgodnie z rozporządzeniem [XX/XXXX (akt dotyczący cyberodporności)] podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny również spełniać wymogi tego rozporządzenia w odniesieniu do wszystkich produktów z elementami cyfrowymi. Ze względu na coraz większe ryzyko, jakie stanowią zależności gospodarcze, należy zminimalizować ekspozycję na dostawców wysokiego ryzyka dostarczających produkty krytyczne dzięki wspólnym ramom strategicznym bezpieczeństwa gospodarczego UE. Zależność od dostawców wysokiego ryzyka dostarczających krytyczne produkty z elementami cyfrowymi wiąże się z ryzykiem strategicznym, któremu należy zapobiegać na szczeblu Unii, w szczególności gdy któreś państwo ucieka się do szpiegostwa przemysłowego czy wymuszenia ekonomicznego, a jego przepisy wymagają arbitralnego dostępu do wszelkiego rodzaju operacji czy danych przedsiębiorstwa, zwłaszcza gdy z produktów krytycznych mają korzystać podmioty kluczowe zdefiniowane w dyrektywie (UE) 2022/2555.

Poprawka 17

Wniosek dotyczący rozporządzenia
Motyw 20

Tekst proponowany przez Komisję	*Poprawka*
(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną Unii. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173[25].	(20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną***, autonomię strategiczną, konkurencyjność i odporność*** Unii. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173[25].
[25] Rozporządzenie Rady (UE) 2021/1173 z dnia 13 lipca 2021 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali i uchylające rozporządzenie (UE) 2018/1488 (Dz.U. L 256 z 19.7.2021, s. 3).	[25] Rozporządzenie Rady (UE) 2021/1173 z dnia 13 lipca 2021 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali i uchylające rozporządzenie (UE) 2018/1488 (Dz.U. L 256 z 19.7.2021, s. 3).

Poprawka 18

Wniosek dotyczący rozporządzenia
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w	(25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w

cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach PESCO***26*** i zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii i w państwach trzecich.

cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach ***PESCO[1], nowy projekt*** PESCO ***o nazwie Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (CIDCC)*** i ***jego proponowany następca w postaci Centrum Koordynacji UE ds. Cyberobrony (EUCDCC) oraz*** zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii i w państwach trzecich***, zwłaszcza w państwach kandydujących do UE, które przestrzegają zasad wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony UE, wspierając te kraje w budowaniu zdolności w zakresie cyberbezpieczeństwa i zacieśnianiu współpracy transgranicznej i regionalnej w dziedzinie cyberbezpieczeństwa między tymi krajami***.

[1] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.

---

[26] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy

[26] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy

uczestniczących w niej państw członkowskich.

uczestniczących w niej państw członkowskich.

Poprawka 19

Wniosek dotyczący rozporządzenia
Motyw 26

Tekst proponowany przez Komisję	*Poprawka*
(26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL[27], IPCR[28], i dyrektywy (UE) 2022/2555. Może on wnosić wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również skoordynowane***, w stosownych przypadkach,*** z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej.	(26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL[27], IPCR[28], i dyrektywy (UE) 2022/2555. Może on wnosić wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również skoordynowane z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej***, zacieśniając strategiczną, operacyjną i techniczną współpracę między społecznością zajmującą się cyberobroną a innymi społecznościami działającymi w cyberprzestrzeni, w szczególności w celu wzmocnienia zdolności w zakresie przeciwdziałania zagrożeniom dla cyberbezpieczeństwa spoza Unii, w tym środków ograniczających, które można wykorzystać do zapobiegania szkodliwym działaniom w cyberprzestrzeni i reagowania na nie***.
[27] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).	[27] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).
[28] Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE)	[28] Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE)

2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

Poprawka 20

Wniosek dotyczący rozporządzenia
Motyw 28

Tekst proponowany przez Komisję	*Poprawka*
(28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać	(28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać

pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych.	pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych ***przy odpowiednim wykorzystaniu całego szeregu opcji obronnych dostępnych dla społeczności cywilnych i wojskowych*** .

Poprawka 21

Wniosek dotyczący rozporządzenia
Motyw 29

Tekst proponowany przez Komisję	*Poprawka*
(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. ***Sektory*** lub ***podsektory*** należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe"). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania	(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. ***W stosownych przypadkach w dokonywanie aktualnych ocen i pomoc w identyfikacji sektorów*** lub ***podsektorów, które*** należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe")***, powinna być również zaangażowana Europejska Służba Działań Zewnętrznych (ESDZ), w szczególności za pośrednictwem Centrum Analiz Wywiadowczych UE (INTCEN) i jego Komórki UE ds. Syntezy Informacji o***

powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/***255429***. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

Zagrożeniach Hybrydowych, przy wsparciu Dyrekcji Wywiadu Sztabu Wojskowego Unii Europejskiej (EUMS) działającej w ramach pojedynczej komórki analiz wywiadowczych (SIAC). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach***. Powinno ono również odgrywać ważną rolę w usprawnianiu współpracy między podmiotami cywilnymi i wojskowymi. Organizując ćwiczenia, Komisja, ESDZ i ENISA powinny zatem systematycznie rozważyć włączenie uczestników z innych społeczności działających w cyberprzestrzeni, takich jak Europejska Agencja Obrony (EDA) i inne odpowiednie podmioty.*** Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/***2554[1]***. Przy wyborze sektorów należy również uwzględnić zalecenie Rady

w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

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

---

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

---

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

Poprawka 22

Wniosek dotyczący rozporządzenia
Motyw 32

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

WPZiB i ISWMR, przy udzielaniu pomocy państwom trzecim, w szczególności Ukrainie i Mołdawii. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.

Poprawka 23

Wniosek dotyczący rozporządzenia
Motyw 33

Tekst proponowany przez Komisję	*Poprawka*
(33) Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług 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, 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***, w tym misjom WPBiO,*** na podobnych warunkach.

Poprawka 24

Wniosek dotyczący rozporządzenia
Motyw 34

Tekst proponowany przez Komisję	*Poprawka*
(34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach krytycznych lub wysoce krytycznych.	(34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach krytycznych lub wysoce krytycznych***, biorąc również pod uwagę ryzyko związane z udziałem dostawców ze strategicznych państw konkurencyjnych ze względu na potencjalne zagrożenie bezpieczeństwa gospodarczego oraz konsekwencje dla bezpieczeństwa strategicznego Unii***.

Poprawka 25

Wniosek dotyczący rozporządzenia
Motyw 36

Tekst proponowany przez Komisję	*Poprawka*
(36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub	(36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub

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

incydentu w cyberbezpieczeństwie na dużą skalę. ***Z uwagi na opracowywanie bezpiecznego systemu łączności, korzystającego z doświadczeń europejskiej kwantowej infrastruktury komunikacyjnej (EuroQCI) oraz rządowej łączności satelitarnej w Unii Europejskiej (GOVSATCOM), w szczególności wdrożenia systemu GALILEO/GNSS dla użytkowników z dziedziny obronności, wszelkie ewentualne rozwiązania w przyszłości powinny uwzględniać pojawienie się „hiperwojny" łączącej szybkość i wyrafinowanie kwantowych technologii obliczeniowych z wysoce autonomicznymi systemami wojskowymi.*** Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, państwami członkowskimi, Komisją i innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi UE. Jeżeli chodzi o sektor prywatny, ENISA opracowuje kanały wymiany informacji z wyspecjalizowanymi dostawcami, w tym z dostawcami i sprzedawcami rozwiązań zarządzanych w zakresie bezpieczeństwa, aby realizować misję ENISA polegającą na osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy

dostarczyć EU-CyCLONe, sieci CSIRT i Komisji i powinno ono stanowić wkład w ich prace. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja udostępni sprawozdanie również wysokiemu przedstawicielowi***, ESDZ i każdej misji WPBiO w państwie dotkniętym incydentem za pośrednictwem ich siedziby głównej***.

Poprawka 26

Wniosek dotyczący rozporządzenia
Motyw 37

Tekst proponowany przez Komisję	*Poprawka*
(37) Biorąc pod uwagę nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa” ***mogą*** otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, ***jeżeli*** jest ***to przewidziane w odpowiednim układzie o stowarzyszeniu z*** tym ***programem***. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy	(37) Biorąc pod uwagę nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących***, zwłaszcza Ukrainy i Mołdawii,*** i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa” ***powinny*** otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa***. Wsparcie powinny uzyskać też państwa trzecie***, ***w których prowadzona*** jest ***misja WPBiO mająca za zadanie wzmocnienie odporności na zagrożenia hybrydowe, w*** tym ***cyberzagrożenia, lub w których zastosowano środek pomocy EPFw celu wzmocnienia cyberodporności państwa***. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty

cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”.	w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”.

Poprawka 27

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 1 – litera c

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

Poprawka 28

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera a

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

Poprawka 29

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;	b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa” ***lub państwom trzecim, które kandydują do członkostwa i nie naruszają interesów Unii i jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określonych w WPZiB zgodnie z tytułem V TUE; Państwa członkowskie powinny uznać aktywny program cyberobrony za element ich krajowej strategii w dziedzinie cyberbezpieczeństwa, która obejmuje regularne wspólne ćwiczenia państw członkowskich i organizacji międzynarodowych. Program taki powinien zapewniać zsynchronizowaną zdolność wykrywania, analizowania i łagodzenia zagrożeń w czasie rzeczywistym***;

Poprawka 30

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

Tekst proponowany przez Komisję	*Poprawka*
	2a. ograniczenie systemowego ryzyka w cyberprzestrzeni wynikającego z uzależnienia od krytycznego sprzętu z państw, które naruszałyby interesy Unii i

	jej państw członkowskich w dziedzinie bezpieczeństwa i obrony określone w WPZiB zgodnie z tytułem V TUE;

Poprawka 31

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

Tekst proponowany przez Komisję	*Poprawka*
	„społeczność zajmująca się cyberobroną” oznacza organy państw członkowskich odpowiedzialne za obronę wspierane przez instytucje, organy i agencje UE, jak określono we wspólnym komunikacie w sprawie polityki UE w zakresie cyberobrony[1];
	[1] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

Poprawka 32

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

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

Poprawka 33

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

Tekst proponowany przez Komisję	*Poprawka*
	da) dokonuje przeglądu i oceny

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

Poprawka 34

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 1 – akapit 2

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

Poprawka 35

Wniosek dotyczący rozporządzenia
Artykuł 4 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. W następstwie zaproszenia do wyrażenia zainteresowania Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) wybiera	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.

krajowe SOC do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać wybranym krajowym SOC dotacje na finansowanie funkcjonowania tych narzędzi i infrastruktur***, pod bezwzględnym warunkiem że zostaną one dostarczone przez zaufanych dostawców, o których mowa w art. 16***. Wkład finansowy Unii pokrywa do 50 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa państwo członkowskie. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i krajowy SOC zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.

Poprawka 36

Wniosek dotyczący rozporządzenia
Artykuł 5 – ustęp 2

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

Poprawka 37

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

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

Poprawka 38

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

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

Poprawka 39

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

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

Poprawka 40

Wniosek dotyczący rozporządzenia
Artykuł 7 – ustęp 1

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

Poprawka 41

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 1

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

Poprawka 42

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 2

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

Poprawka 43

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 3

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

Poprawka 44

Wniosek dotyczący rozporządzenia
Artykuł 9 – ustęp 2

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

Poprawka 45

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*

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

Poprawka 46

Wniosek dotyczący rozporządzenia
Artykuł 10 – ustęp 1 – litera c

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

Poprawka 47

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

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

Poprawka 48

Wniosek dotyczący rozporządzenia
Artykuł 11 – ustęp 2

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

Poprawka 49

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 2

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

Poprawka 50

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 3 – litera b

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

Poprawka 51

Wniosek dotyczący rozporządzenia
Artykuł 12 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*

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

Poprawka 52

Wniosek dotyczący rozporządzenia
Artykuł 12 − ustęp 5

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

Poprawka 53

Wniosek dotyczący rozporządzenia
Artykuł 12 − ustęp 7

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

Poprawka 54

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

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

Poprawka 55

Wniosek dotyczący rozporządzenia
Artykuł 15 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. W porozumieniu z wysokim przedstawicielem wsparcie w ramach mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty. Może ono również uzupełniać pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub wnosić	3. W porozumieniu z wysokim przedstawicielem wsparcie w ramach mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty***(CRRTs), by w ten sposób lepiej wspierać państwa członkowskie UE, misje i operacje WPBiO oraz państwa trzecie, które w swoich***

wkład w taką pomoc w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej.	***działaniach na rzecz budowania zdolności w zakresie cyberobrony przestrzegają zasad wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony UE, w szczególności Ukrainę i Mołdawię***. Może ono również uzupełniać pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub wnosić wkład w taką pomoc w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej.

Poprawka 56

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

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

Poprawka 57

Wniosek dotyczący rozporządzenia
Artykuł 16 – ustęp 2 – litera f

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

Poprawka 58

Wniosek dotyczący rozporządzenia

Artykuł 16 – ustęp 2 – litera j a (nowa)

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

Poprawka 59

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

Tekst proponowany przez Komisję	*Poprawka*
	jb) dostawca musi w miarę możliwości ściśle współpracować z odpowiednimi MŚP;

Poprawka 60

Wniosek dotyczący rozporządzenia
Artykuł 17 – ustęp 1

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

Poprawka 61

Wniosek dotyczący rozporządzenia
Artykuł 17 − ustęp 2

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

Poprawka 62

Wniosek dotyczący rozporządzenia
Artykuł 18 – ustęp 1

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

Poprawka 63

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

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

Poprawka 64

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

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

Poprawka 65

Wniosek dotyczący rozporządzenia
Artykuł 20 – akapit 1

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

rozporządzenia.	niniejszego rozporządzenia.

PROCEDURA W KOMISJI OPINIODAWCZEJ

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

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

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

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

0	0

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

25.10.2023

OPINIA KOMISJI TRANSPORTU I TURYSTYKI

dla Komisji Przemysłu, Badań Naukowych i Energii

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

Sprawozdawca komisji opiniodawczej: Gheorghe Falcă

ZWIĘZŁE UZASADNIENIE

Organizacje dotknięte cyberatakami, m.in. w sektorze transportu, zwłaszcza przedsiębiorstwa sektora prywatnego, rzadko je zgłaszają, ponieważ zazwyczaj postrzegają je jako złą reklamę. Większość organizacji woli zajmować się nimi wewnętrznie i często to atakujący je upubliczniają. W UE dobrą wiadomością jest to, że wejście w życie dyrektywy 2022/2555 w sprawie bezpieczeństwa sieci (zwanej „dyrektywą NIS 2”), którą państwa członkowskie muszą transponować do października 2024 r., harmonizuje obowiązki w zakresie zgłaszania incydentów we wszystkich państwach członkowskich. Dlatego też w nadchodzących latach prawdopodobnie uda się lepiej zrozumieć charakter i skalę problemu.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opublikowała niedawno sprawozdanie[1] zawierające informacje o zagrożeniach dla cyberbezpieczeństwa w sektorze transportu, w którym podkreśliła, że cyberprzestępcy byli odpowiedzialni za ponad połowę (55 %) incydentów zaobserwowanych w okresie sprawozdawczym (2022), a główną motywacją tych ataków było uzyskanie korzyści finansowych. Zauważa również, że większość cyberataków w sektorze transportu jest wymierzona w systemy informatyczne, co powoduje zakłócenia operacyjne.

Jeżeli chodzi o gotowość i reagowanie na incydenty w cyberbezpieczeństwie, obecnie wsparcie na szczeblu unijnym i solidarność między państwami członkowskimi są ograniczone. W konkluzjach z maja 2022 r. Rada podkreśliła, że należy wyeliminować te niedostatki, i wezwała Komisję, aby przedstawiła wniosek dotyczący nowego **Funduszu Reagowania Cyberkryzysowego**[2].

[1] „Zrozumieć cyberzagrożenia w transporcie”, ENISA, opublikowane 21 marca 2023 r.
[2] Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni z 23 maja 2022 r. (9364/22).

Omawiane tu rozporządzenie wdraża również przyjętą w grudniu 2020 r. **unijną strategię cyberbezpieczeństwa**, w której zapowiedziano utworzenie **europejskiej tarczy cyberbezpieczeństwa**, wzmacniającej zdolności do wykrywania cyberzagrożeń i wymiany informacji w Unii Europejskiej za pośrednictwem federacji krajowych i transgranicznych (SOC). Działania na mocy rozporządzenia będą wspierane ze **środków przeznaczonych na cel strategiczny „Cyberbezpieczeństwo" programu „Cyfrowa Europa".**

Całkowity budżet obejmuje zwiększenie środków o 100 mln EUR, które w rozporządzeniu proponuje się przesunąć z innych celów strategicznych programu „Cyfrowa Europa". Dzięki temu nowa całkowita kwota dostępna na działania w ramach celu „Cyberbezpieczeństwo" programu „Cyfrowa Europa" wyniesie 842,8 mln EUR.

Część z dodatkowych 100 mln EUR posłuży zwiększeniu budżetu, którym zarządza ECCC, przeznaczonego na realizację działań dotyczących SOC i gotowości w ramach ich programów prac. Ponadto dodatkowe środki finansowe posłużą wsparciu ustanowienia unijnej rezerwy cyberbezpieczeństwa. Stanowią one uzupełnienie budżetu przewidzianego już na podobne działania w programie prac dotyczącym głównego programu „Cyfrowa Europa" i celu „Cyberbezpieczeństwo" na lata 2023–2027, co mogłoby zwiększyć łączną kwotę na lata 2023–2027 do 551 mln EUR, podczas gdy 115 mln EUR rozdysponowano już w formie projektów pilotażowych na lata 2021–2022. Z uwzględnieniem wkładów państw członkowskich budżet całkowity może wynieść maksymalnie 1,109 mld EUR.

Stanowisko sprawozdawcy

Sprawozdawca z zadowoleniem przyjmuje nowy wniosek i uważa, że przyniesie znaczne korzyści różnym zainteresowanym stronom. Sprawozdawca podkreśla, że trzeba lepiej zrozumieć potrzeby i wymogi w zakresie cyberbezpieczeństwa w transporcie, a także zapewnić transportowym podmiotom krytycznym dostęp do odpowiedniego finansowania gotowości, reagowania i rozwiązywania incydentów.

Sprawozdawca popiera zestaw narzędzi w zakresie cyberbezpieczeństwa w transporcie, który ma przyczynić się do zwiększenia poziomu świadomości w dziedzinie cyberbezpieczeństwa i higieny cyberbezpieczeńswa, ze szczególnym uwzględnieniem sektora transportu. Dotyczy on organizacji transportowych, niezależnie od ich wielkości i zakresu działalności, a także uwzględnia krytyczną infrastrukturę transportową i mobilność wojskową – zwłaszcza w odniesieniu do wojny w Ukrainie – w szczególności, choć nie tylko:

- przewoźników lotniczych, organy zarządzające portami lotniczymi, główne porty lotnicze, ośrodki zarządzania ruchem lotniczym i kontroli ruchu lotniczego, Europejską Agencję Bezpieczeństwa Lotniczego i organizację Eurocontrol;
- zarządców infrastruktury, przedsiębiorstwa kolejowe oraz europejski system zarządzania ruchem kolejowym (ERTMS);
- armatorów śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów, podmioty zarządzające portami, w tym ich obiekty portowe, podmioty wykonujące prace i operujące sprzętem znajdującym się w portach, operatorów

systemów ruchu statków;
- organy administracji drogowej odpowiedzialne za kontrolę zarządzania ruchem, operatorów inteligentnych systemów transportowych;
- usługi pocztowe i kurierskie.

Sprawozdawca uważa, że wielkość budżetu przeznaczonego na funkcjonowanie **Funduszu Reagowania Cyberkryzysowego** będzie miał wpływ na jego powodzenie. W związku z tym powinien być wystarczający, aby wesprzeć państwa członkowskie **w przygotowaniu się** na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, **w reagowaniu na nie i w usuwaniu ich skutków**. Wsparcie w reagowaniu na incydenty zapewnia się także instytucjom, organom, urzędom i agencjom unijnym.

Ustanowienie europejskiej tarczy cyberbezpieczeństwa poprawi zdolności państw członkowskich do wykrywania cyberzagrożeń. Mechanizm cyberkryzysowy uzupełni działania państw członkowskich w sytuacjach nadzwyczajnych dzięki wsparciu w zakresie gotowości, reagowania, natychmiastowego usuwania skutków lub przywrócenia funkcjonowania kluczowych usług.

POPRAWKA

Komisja Transportu i Turystyki zwraca się do Komisji Przemysłu, Badań Naukowych i Energii, jako komisji przedmiotowo właściwej, o wzięcie pod uwagę następujących poprawek:

Poprawka 1

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 cyberbezpieczeństwie są nieprzewidywalne, ponieważ często	(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, jak również dla krytycznej infrastruktury informatycznej i fizycznej. 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, oferowanie transportu publicznego i prywatnego 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 oraz dla mobilności wewnątrz Unii, a nawet mieć

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.	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.

Poprawka 2

Wniosek dotyczący rozporządzenia
Motyw 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2a) Coraz poważniejszym zagrożeniem cyberbezpieczeństwa w sektorze transportu są podmioty sponsorowane przez państwo, cyberprzestępcy i haktywiści atakujący organy, przewoźników, producentów, dostawców i usługodawców w transporcie lotniczym, morskim, kolejowym i drogowym. W 2022 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) odnotowała wzrost o 25 % średniej miesięcznej liczby zgłaszanych incydentów mających wpływ na sektor transportowy w porównaniu z poziomami z 2021 r. Większość ataków na sektor transportowy jest wymierzona w systemy informatyczne, co może prowadzić do zakłóceń operacyjnych[14a].
	[14a] ENISA (2023), „ENISA threat landscape: Transport sector" [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor transportowy], s. 7 i 17.

Poprawka 3

Wniosek dotyczący rozporządzenia

Motyw 2 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2b) Niczym niesprowokowana inwazja Rosji na Ukrainę spowodowała znaczny wzrost liczby incydentów w cyberbezpieczeństwie, w tym rozproszonych cyberataków typu „odmowa usługi" (DDoS), wymierzonych w sektor transportowy w UE i na obszarach położonych blisko UE, głównie w porty lotnicze, koleje i organy ds. transportu[14b]. Wzrost liczby ataków prawdopodobnie będzie się utrzymywał.
	[14b] ENISA (2023), „ENISA threat landscape: Transport sector" [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor transportowy], s. 9.

Poprawka 4

Wniosek dotyczący rozporządzenia
Motyw 2 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2c) Cyberataki są wymierzane w organy i jednostki we wszystkich podsektorach transportu, a ich ofiarą padają przedsiębiorstwa kolejowe i zarządcy infrastruktury, a także operatorzy portów. Jeśli chodzi o sektor drogowy, celami ataków byli producenci oryginalnego sprzętu (OEM), dostawcy i usługodawcy, a także przewoźnicy w transporcie publicznym. W sektorze lotniczym ataki wymierzano głównie w linie lotnicze i operatorów portów lotniczych, a następnie dostawców usług, przewoźników w transporcie powierzchniowym oraz łańcuch dostaw[14c].
	[14c] ENISA (2023), „ENISA threat

	landscape: Transport sector" [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor transportowy], s. 17.

Poprawka 5

Wniosek dotyczący rozporządzenia
Motyw 3

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

zakresu wykrywania i reagowania.

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

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

Poprawka 6

Wniosek dotyczący rozporządzenia
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[20]. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.	(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555[17], zalecenie Komisji (UE) 2017/1584[18], dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE[19] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[20]***, jak również wniosek dotyczący rozporządzenia w sprawie wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej oraz wniosek dotyczący rozporządzenia w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt o cyberodporności)***. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

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

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

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

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

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

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

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

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

Poprawka 7

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Choć z zadowoleniem przyjmuje się opracowany przez Komisję Europejską zestaw narzędzi w zakresie cyberbezpieczeństwa w transporcie[2a] zawierający podstawowe informacje o zagrożeniach, które mogą mieć wpływ na

organizacje transportowe (rozpowszechnianie złośliwego oprogramowania, odmowa usługi, nieuprawniony dostęp i kradzież oraz manipulacja oprogramowaniem komputerowym), oraz wykaz dobrych praktyk łagodzących, przewoźnikom należy zapewnić odpowiednie szkolenia z zakresu cyberbezpieczeństwa i odpowiednie narzędzia do zapobiegania zagrożeniom cyberbezpieczeństwa. Z budżetu Unii należy także pokryć wsparcie, takie jak szkolenia, udzielane przez ENISA w celu umożliwienia przewoźnikom skutecznego wdrożenia najlepszych praktyk łagodzących przewidzianych w zestawie narzędzi.

[1a] „ENISA threat landscape: transport sector" [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor transportowy], ENISA, marzec 2023.

[2a] Komisja Europejska (2021). Zestaw narzędzi w zakresie cyberbezpieczeństwa w transporcie, dostępny pod adresem https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_pl.

Poprawka 8

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Ogólnounijne skoordynowane podejście do kwestii wzmocnienia gotowości i odporności infrastruktury krytycznej, takiej jak infrastruktura transportowa, opiera się na budowaniu zdolności państw członkowskich. Jak stwierdzono w opublikowanym niedawno komunikacie Komisji do Parlamentu Europejskiego i Rady w sprawie wyeliminowania niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu

zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE[19a], nie można zagwarantować bezpieczeństwa Unii bez udziału najcenniejszego zasobu UE: jej obywateli.

[19a] Komunikat Komisji do Parlamentu Europejskiego i Rady pt. „Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE (»Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa«)", COM(2023) 207 final.

Poprawka 9

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 zaawansowanego gromadzenia danych i narzędzia analityki, zwiększając zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz	(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. Te aktywa i infrastruktury krytyczne obejmują inteligentne systemy transportowe, które, choć niezbędne dla zautomatyzowanej i multimodalnej mobilności, działają w oparciu o kluczową wymianę danych wrażliwych. 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

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].

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).

Poprawka 10

Wniosek dotyczący rozporządzenia
Motyw 14 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(14a) Sektor transportowy w coraz większym stopniu staje się jednym z najbardziej lukratywnych rodzajów działalności gospodarczej dla cyberprzestępców, ponieważ dane klientów uważa się za bardzo cenny towar, a łańcuch dostaw w transporcie coraz częściej pada celem ataków. Z tego powodu infrastrukturę transportową o

transgranicznym charakterze lub charakteryzującą się wymianą danych za pośrednictwem technologii bezprzewodowych należy uznać za kluczowy przedmiot analizy i monitorowania zarówno dla krajowych, jak i – w szczególności – transgranicznych SOC. Na przykład przedstawiony niedawno wniosek dotyczący zmiany rozporządzenia w sprawie TEN-T zawiera wymóg większej solidarności i współpracy w zakresie wymiany informacji na temat transgranicznych zagrożeń cyberbezpieczeństwa, z którymi może się mierzyć ta transnarodowa sieć. Podobnie inteligentne systemy transportowe (ITS) mają kluczowe znaczenie dla zwiększenia bezpieczeństwa, wydajności i zrównoważoności transportu, ale sprawiają, że systemy transportowe są bardziej podatne na cyberataki, które mogą powodować wypadki, zatory komunikacyjne lub przynosić straty ekonomiczne zarówno prywatnym, jak i publicznym przewoźnikom. W celu zapewnienia bezpieczeństwa pasażerów, ochrony danych użytkowników i dostawców oraz uniknięcia szkód finansowych konieczne jest, aby program wdrażania zmienionej dyrektywy w sprawie inteligentnych systemów transportowych obejmował przepisy i narzędzia wzmacniające współpracę między państwami członkowskimi w celu wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty.

Poprawka 11

Wniosek dotyczący rozporządzenia
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Na szczeblu krajowym	(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.	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. ***W tym względzie w celu wzmocnienia autonomii Unii w dziedzinie cyberbezpieczeństwa oraz w odniesieniu do art. 47 ust. 4 wniosku dotyczącego rozporządzenia w sprawie wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej (COM(2021)0812) konieczne jest również zapobieganie dostępowi do danych prowadzącemu do zagrożeń cyberbezpieczeństwa przez egzekwowanie solidnych ram regulacyjnych, które regulują kwestię udziału podmiotów zagranicznych i inwestycje w infrastrukturę krytyczną taką jak transport.***

Poprawka 12

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.	(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.	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. ***Powinna ona również umożliwiać synergię z planem działania na rzecz mobilności wojskowej 2.0. Dobrze funkcjonująca sieć mobilności wojskowej musi być odporna, w tym w kontekście zagrożeń cyberbezpieczeństwa i innych zagrożeń hybrydowych, które mogą mieć wpływ na krytyczne węzły systemu transportowego o podwójnym zastosowaniu. Na przykład cyberatak na systemy wykorzystywane w portach lotniczych, portach morskich lub na drogach kolejowych czy cyberatak na zasoby wojskowe może mieć poważne konsekwencje. W związku z tym cyfryzacja procesów i procedur, w tym na potrzeby niezbędnej współpracy cywilnej i wojskowej, będzie wymagała wzmocnienia komputerowych systemów informatycznych przed zagrożeniami cyberbezpieczeństwa.***

Poprawka 13

Wniosek dotyczący rozporządzenia
Motyw 21 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*

	(21a) W przypadku kryzysu cyberbezpieczeństwa kluczowe znaczenie dla zapewnienia orientacji sytuacyjnej w wojskowym i cywilnym sektorze transportowym ma skuteczna wymiana informacji. Taka wymiana informacji powinna również pobudzać współpracę między odpowiednimi organami sektorowymi odpowiedzialnymi za transport, właściwymi organami ds. cyberbezpieczeństwa, SOC i CSIRT.

Poprawka 14

Wniosek dotyczący rozporządzenia
Motyw 29

Tekst proponowany przez Komisję	*Poprawka*
(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe”). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które	(29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe”). Szczególną uwagę należy zwrócić na sektor transportowy i jego podsektory (lotniczy, kolejowy, wodny, drogowy), ponieważ obejmują one infrastrukturę krytyczną, w której incydenty w cyberbezpieczeństwie i cyberataki mogą poważnie zagrozić bezpieczeństwu pasażerów i przewoźników. Skoordynowane testowanie powinno opierać się na wspólnych

zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554[29]. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

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

scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554[29]. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

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

Poprawka 15

Wniosek dotyczący rozporządzenia
Motyw 30 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(30a) Ze względu na kluczowe znaczenie tego sektora oraz konsekwencje zagrożeń cyberbezpieczeństwa dla mobilności, a w konsekwencji dla życia pasażerów i pieszych, sektor transportowy powinien być traktowany priorytetowo w odniesieniu do skoordynowanego testowania gotowości podmiotów.

Poprawka 16

Wniosek dotyczący rozporządzenia
Motyw 35 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(35a) Ze względu na poszerzony zakres zadań i obowiązków powierzonych ENISA w niniejszym wniosku, a także we wniosku dotyczącym aktu dotyczącego odporności cybernetycznej konieczne jest przyjęcie budżetu korygującego ENISA 1/2022 na pilotażowe wdrożenie działania wspierającego w zakresie cyberbezpieczeństwa. Ponadto z uwagi na interesy Unii należy przydzielić ENISA dodatkowe zasoby finansowe i ludzkie.

Poprawka 17

Wniosek dotyczący rozporządzenia
Motyw 38 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(38a) Rozwój umiejętności i kompetencji powinien zatem zajmować centralne miejsce we wszystkich sektorach, nie tylko w tych, które są podatne na zagrożenia cyberbezpieczeństwa, takich jak

	pracownicy w sektorze komunikacji zbiorowej lub infrastruktury krytycznej, w tym zajmujący się systemami sterowania pociągiem i cyfrowymi narzędziami planowania transportu w odniesieniu do wszystkich rodzajów transportu. Wprowadzenie i dalszy rozwój kultury cyberbezpieczeństwa ma zatem zasadnicze znaczenie dla powodzenia wdrożenia niniejszego rozporządzenia zarówno pod względem świadomości obywateli, jak i wiedzy specjalistów we wszystkich sektorach infrastruktury krytycznej.

Poprawka 18

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 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, infrastruktury transportowej i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w suwerenność technologiczną Unii w dziedzinie cyberbezpieczeństwa;

Poprawka 19

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,	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, ze

między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;	szczególnym uwzględnieniem krytycznej infrastruktury informatycznej i fizycznej, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;

Poprawka 20

Wniosek dotyczący rozporządzenia
Artykuł 1 – ustęp 2 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ca) zwiększenie gotowości, współpracy i skuteczności Unii w zakresie ochrony infrastruktury transportowej i usług transportowych w państwach członkowskich przed incydentami w cyberbezpieczeństwie w celu zapewnienia ciągłości funkcjonowania sektora transportowego, integralności łańcuchów dostaw i mobilności w całej Unii.

Poprawka 21

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

Tekst proponowany przez Komisję	*Poprawka*
c) przyczynia się do lepszej ochrony przed cyberzagrożeniami i lepszego reagowania na nie;	c) przyczynia się do lepszej ochrony przed cyberzagrożeniami i lepszego reagowania na nie, w tym w odniesieniu do infrastruktury transportowej o transgranicznym charakterze, takiej jak sieć TEN-T, lub charakteryzującej się wymianą danych za pośrednictwem technologii bezprzewodowych takich jak inteligentne systemy transportowe;

Poprawka 22

Wniosek dotyczący rozporządzenia
Artykuł 3 – ustęp 2 – akapit 2

Tekst proponowany przez Komisję	*Poprawka*
Jest ona rozwijana we współpracy z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną na podstawie rozporządzenia (UE) 2021/1173.	Jest ona rozwijana we współpracy z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną na podstawie rozporządzenia (UE) 2021/1173. ***Umożliwia ona opartą na specjalnych protokołach i normach współpracę ze społecznością zajmującą się cyberobroną w celu zapewnienia rozwoju lepszych cywilnych zdolności w zakresie wykrywania i orientacji sytuacyjnej do celów ochrony infrastruktury krytycznej. W związku z tym należy rozwijać synergie również z planem działania na rzecz mobilności wojskowej 2.0 oraz zadbać o skuteczną wymianę informacji w celu zapewnienia orientacji sytuacyjnej w wojskowym i cywilnym sektorze transportowym.***

Poprawka 23

Wniosek dotyczący rozporządzenia
Artykuł 8 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a. Komisja angażuje europejską tarczę cybernetyczną, w szczególności transgraniczne SOC, w proces sporządzania opinii dla państw członkowskich w ramach wniosku dotyczącego rozporządzenia w sprawie transeuropejskiej sieci transportowej (COM(2021)0812) w każdym przypadku, gdy udział lub jakikolwiek wkład osoby fizycznej z państwa trzeciego lub przedsiębiorstwa z państwa trzeciego może mieć wpływ na cyberbezpieczeństwo transgranicznej infrastruktury krytycznej takiej jak TEN-T.

Poprawka 24

Wniosek dotyczący rozporządzenia

Artykuł 10 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych w całej Unii;	a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych w całej Unii, ze szczególnym uwzględnieniem infrastruktury transportowej i jej podsektorów wymienionych w załączniku I do dyrektywy (UE) 2022/2555;

Poprawka 25

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 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.	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, w tym z przewoźnikami. Na potrzeby przeglądu ENISA może również konsultować się z innymi rodzajami zainteresowanych stron. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.

Poprawka 26

Wniosek dotyczący rozporządzenia
Artykuł 19 – akapit 1 – punkt 1 – litera b
Rozporządzenie (UE) 2021/694
Artykuł 6 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a. Ze względu na interesy Unii, w związku z jej zobowiązaniami dotyczącymi przygotowania propozycji programów certyfikacji zgodnie z rozporządzeniem (UE) 2019/881, jej zobowiązaniami dotyczącymi przeglądu i oceny zagrożeń, podatności i działań łagodzących, przygotowania sprawozdania z przeglądu incydentu na potrzeby mechanizmu przeglądu incydentów w cyberbezpieczeństwie, a także zapewnienia operatorom infrastruktury krytycznej szkolenia w zakresu przeciwdziałania cyberatakom i incydentom w cyberbezpieczeństwie, jak również w świetle nowo powierzonych jej obowiązków w ramach wniosku dotyczącego aktu dotyczącego cyberodporności ENISA otrzymuje niezbędne zasoby w ramach budżetu Unii zgodnie z obowiązującymi przepisami.

Poprawka 27

Wniosek dotyczący rozporządzenia
Artykuł 19 – akapit 1 – punkt 1 a (nowy)
Rozporządzenie (UE) 2021/694
Artykuł 7 – ustęp 1 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	1a) w art. 7 wprowadza się następujące zmiany:
	a) w ust. 1 wprowadza się następujące zmiany:
	1) dodaje się lit. ca) w brzmieniu:
	ca) wspieraniu wysokiej jakości szkoleń dla przewoźników oraz kadry zarządzającej i pracowników w krytycznej infrastrukturze transportowej, również w

celu skutecznej wymiany i skutecznego wdrażania praktyk ograniczających ryzyko cyberataków lub incydentów w cyberbezpieczeństwie dotyczących infrastruktury krytycznej, takich jak te zawarte w zestawie narzędzi w zakresie cyberbezpieczeństwa w transporcie.

PROCEDURA W KOMISJI OPINIODAWCZEJ

Tytuł	Ustanowienie środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty
Odsyłacze	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 1.6.2023
Opinia wydana przez Data ogłoszenia na posiedzeniu	TRAN 1.6.2023
Sprawozdawca(czyni) komisji opiniodawczej Data powołania	Gheorghe Falcă 7.7.2023
Data przyjęcia	25.10.2023
Wynik głosowania końcowego	+: 38 –: 0 0: 0
Posłowie obecni podczas głosowania końcowego	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Zastępcy obecni podczas głosowania końcowego	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

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

PROCEDURA W KOMISJI PRZEDMIOTOWO WŁAŚCIWEJ

Tytuł	Ustanowienie środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty			
Odsyłacze	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Data przedstawienia Parlamentowi	19.4.2023			
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 1.6.2023			
Komisje opiniodawcze Data ogłoszenia na posiedzeniu	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Rezygnacja z wydania opinii Data decyzji	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Sprawozdawcy Data powołania	Lina Gálvez Muñoz 2.5.2023			
Rozpatrzenie w komisji	19.9.2023			
Data przyjęcia	7.12.2023			
Wynik głosowania końcowego	+: –: 0:	43 10 1		
Posłowie obecni podczas głosowania końcowego	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Zastępcy obecni podczas głosowania końcowego	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Zastępcy (art. 209 ust. 7) obecni podczas głosowania końcowego	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Data złożenia	8.12.2023			

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI PRZEDMIOTOWO WŁAŚCIWEJ

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

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