Parlament Europejski
2019-2024

Komisja Transportu i Turystyki

2023/0109(COD)

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

PA_Legam

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].

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

[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).

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.

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.

[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