Rada
Unii Europejskiej

Bruksela, 7 września 2023 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2023/0318(NLE)

12485/23
ADD 1

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	6 września 2023 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2023) 526 final
Dotyczy:	Wniosek dotyczący ZALECENIA RADY w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym

Delegacje otrzymują w załączeniu dokument COM(2023) 526 final.

Zał.: COM(2023) 526 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 6.9.2023 r.
COM(2023) 526 final

2023/0318 (NLE)

Wniosek

ZALECENIE RADY

w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym

(Tekst mający znaczenie dla EOG)

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W obecnej sytuacji geopolitycznej, charakteryzującej się rosnącą niestabilnością, zwłaszcza z powodu rosyjskiej wojny napastniczej przeciwko Ukrainie i coraz większej złożoności zagrożeń bezpieczeństwa, a także skutkami zmiany klimatu, takimi jak wzrost liczby nietypowych zjawisk klimatycznych lub niedobór wody, Unia musi zachować czujność i stale się dostosowywać. Obywatele, przedsiębiorstwa i organy w Unii polegają na infrastrukturze krytycznej[1] ze względu na usługi kluczowe świadczone przez podmioty będące operatorami takiej infrastruktury. Usługi te mają decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska i muszą być świadczone na rynku wewnętrznym w sposób niezakłócony. W związku z tym, ze względu na znaczenie tych usług kluczowych dla rynku wewnętrznego, a co za tym idzie, potrzebę zwiększenia odporności infrastruktury krytycznej oraz, w szerszym ujęciu, zapewnienia odporności podmiotów krytycznych świadczących te usługi, Unia musi wprowadzić środki zwiększające taką odporność i łagodzące wszelkie zakłócenia w świadczeniu takich usług kluczowych. W przeciwnym razie takie zakłócenia mogą mieć poważne konsekwencje dla obywateli Unii, naszych gospodarek i zaufania do naszych systemów demokratycznych oraz mogą negatywnie wpływać na sprawne funkcjonowanie rynku wewnętrznego, w szczególności w kontekście rosnących współzależności sektorów i krajów.

Unia wprowadziła już szereg środków poprawy ochrony infrastruktury krytycznej, w szczególności w odniesieniu do infrastruktury transgranicznej, oraz zwiększenia odporności podmiotów krytycznych, aby uniknąć zakłóceń w świadczeniu przez nie usług kluczowych na rynku wewnętrznym lub złagodzić te zakłócenia.

Dyrektywa 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej[2] („dyrektywa w sprawie europejskiej infrastruktury krytycznej”) była pierwszym instrumentem prawnym służącym ustanowieniu ogólnounijnej procedury rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz ustanowieniu wspólnego unijnego podejścia do oceny potrzeby poprawy ochrony takiej infrastruktury przed zagrożeniami spowodowanymi przez człowieka – zarówno umyślnymi, jak i przypadkowymi – a także klęskami żywiołowymi. Skoncentrowano się w niej jednak wyłącznie na sektorach energii i transportu oraz na ochronie infrastruktury krytycznej i nie przewidziano szerszych środków mających na celu zwiększenie odporności podmiotów będących operatorami takiej infrastruktury.

Ze względu na coraz ściślejsze powiązania między operacjami na rynku wewnętrznym i na ich transgraniczny charakter, zaistniała potrzeba uwzględnienia więcej niż dwóch sektorów i wykroczenia poza środki ochrony pojedynczych składników infrastruktury. Dlatego też w 2022 r. przyjęto dyrektywę (UE) 2022/2557 w sprawie odporności podmiotów

[1] Infrastruktura krytyczna oznacza składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu, niezbędne do świadczenia usługi kluczowej (art. 2 pkt 4 dyrektywy (UE) 2022/2557 w sprawie odporności podmiotów krytycznych).

[2] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. L 345 z 23.12.2008, s. 75).

krytycznych[3] („dyrektywa CER”) wraz z dyrektywą (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii[4] („dyrektywa NIS 2”). Ich celem jest zapewnienie kompleksowego poziomu fizycznej i cyfrowej odporności podmiotów krytycznych. Dyrektywa CER weszła w życie dnia 16 stycznia 2023 r. i ma na celu pomoc państwom członkowskim w zwiększaniu ogólnej odporności podmiotów krytycznych oraz wzmocnienie koordynacji na szczeblu Unii. 18 października 2024 r. zastąpi ona dyrektywę w sprawie europejskiej infrastruktury krytycznej. Do tego dnia państwa członkowskie muszą wprowadzić niezbędne środki w celu zapewnienia zgodności z dyrektywą CER. Dyrektywa CER ma zastosowanie do 11 sektorów[5]. Przeniesiono w niej punkt ciężkości z ochrony infrastruktury krytycznej na szerszą koncepcję odporności podmiotów krytycznych będących operatorami takiej infrastruktury krytycznej, obejmującą okres przed incydentem, w jego trakcie i po nim. Dyrektywa NIS 2 weszła w życie 16 stycznia 2023 r. i modernizuje istniejące ramy prawne, aby je dostosować do powszechniejszej cyfryzacji i zmieniającego się krajobrazu zagrożeń cyberbezpieczeństwa. W dyrektywie NIS 2 rozszerzono również zakres przepisów dotyczących cyberbezpieczeństwa na nowe sektory i podmioty, a także poprawiono odporność podmiotów publicznych i prywatnych, właściwych organów i całej Unii oraz ich zdolności do reagowania na incydenty.

Dyrektywa CER zawiera przepisy dotyczące zgłaszania incydentów przez podmiot krytyczny właściwemu organowi krajowemu, powiadamiania przez właściwy organ krajowy państw członkowskich, których dotyczy (lub może dotyczyć) incydent, oraz powiadamiania Komisji, jeżeli incydent dotyczy co najmniej sześciu państw członkowskich. W dyrektywie CER określono pewne obowiązki w zakresie zgłaszania incydentów, które mają lub mogą mieć istotny wpływ na podmioty krytyczne oraz na ciągłość świadczenia usług kluczowych na rzecz co najmniej jednego innego państwa członkowskiego lub w co najmniej jednym innym państwie członkowskim[6].

Jak pokazał sabotaż gazociągów Nord Stream we wrześniu 2022 r., kontekst bezpieczeństwa, w którym funkcjonuje infrastruktura krytyczna, znacznie się zmienił i potrzebne są dodatkowe pilne działania na szczeblu Unii w celu zwiększenia odporności infrastruktury krytycznej nie tylko w odniesieniu do gotowości, lecz także w odniesieniu do skoordynowanej reakcji.

W tym kontekście, 8 grudnia 2022 r., na wniosek Komisji przyjęto zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej[7] („zalecenie w sprawie odporności infrastruktury krytycznej”). W zaleceniu tym podkreśla się między innymi potrzebę zapewnienia na szczeblu Unii skoordynowanej i skutecznej odpowiedzi na obecne i przyszłe zagrożenia dla świadczenia usług kluczowych. Rada zwróciła się do Komisji o opracowanie „planu działania dotyczącego skoordynowanej reakcji na zakłócenia infrastruktury krytycznej o istotnym znaczeniu

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164).

[4] 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, s. 80).

[5] Energia, transport, bankowość, infrastruktura rynku finansowego, infrastruktura cyfrowa, administracja publiczna, przestrzeń kosmiczna, zdrowie, woda pitna, ścieki, produkcja, przetwarzanie i dystrybucja żywności.

[6] Zgodnie z art. 15 ust. 1 i 3 dyrektywy CER.

[7] Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej 2023/C 20/01 (Dz.U. C 20 z 20.1.2023, s. 1).

transgranicznym". W zaleceniu wspomniano, że ten plan powinien być spójny z unijnym protokołem do celów przeciwdziałania zagrożeniom hybrydowym[8], powinien uwzględniać zalecenie Komisji 2017/1584 w sprawie skoordynowanego reagowania na wypadek wystąpienia incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych[9] („plan na rzecz cyberbezpieczeństwa") i powinien być zgodny ze zintegrowanymi uzgodnieniami dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych[10] („IPCR").

W tym kontekście niniejszy wniosek dotyczący dodatkowego zalecenia Rady zawiera taki plan działania. Wniosek ten ma na celu uzupełnienie obecnych ram prawnych o opis skoordynowanej reakcji na szczeblu Unii na zakłócenia funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym przy jednoczesnym wykorzystaniu uzgodnień istniejących na szczeblu Unii. Konkretnie wniosek zawiera opis zakresu i celów planu działania, a także opis podmiotów, procesów i istniejących narzędzi, które można wykorzystać do reagowania – w skoordynowany sposób na szczeblu Unii – na incydenty zakłócające funkcjonowanie infrastruktury krytycznej, mające istotne skutki transgraniczne. Wniosek zawiera także opis sposobów współpracy między państwami członkowskimi, instytucjami, organami, urzędami i agencjami Unii w takich sytuacjach.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Niniejszy wniosek dotyczący zalecenia Rady jest zgodny z obecnymi ramami prawnymi dotyczącymi ochrony infrastruktury krytycznej i odporności podmiotów krytycznych – odpowiednio z dyrektywą w sprawie europejskiej infrastruktury krytycznej i dyrektywą CER, a także z zaleceniem w sprawie odporności infrastruktury krytycznej – i uzupełnia te ramy, ponieważ ma na celu zapewnienie, w sposób komplementarny, koordynacji między państwami członkowskimi oraz między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii w zakresie reagowania na incydenty powodujące zakłócenia funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym oraz świadczenia usług kluczowych. We wniosku wykorzystuje się struktury i mechanizmy istniejące na szczeblu Unii, w tym struktury i mechanizmy ustanowione na mocy dyrektywy CER, mianowicie współpracę właściwych organów i Grupę ds. Odporności Podmiotów Krytycznych, ustanowioną na mocy dyrektywy CER w celu wspierania Komisji oraz ułatwiania współpracy państw członkowskich i wymiany informacji na temat kwestii związanych z dyrektywą CER.

Niniejszy wniosek dotyczący zalecenia Rady jest również zgodny z unijnymi ramami dotyczącymi cyberbezpieczeństwa ustanowionymi w dyrektywie NIS 2 i je uzupełnia.

Niniejszy wniosek ma na celu przedstawienie – w obszarze odporności podmiotów krytycznych i ochrony infrastruktury krytycznej – planu dotyczącego infrastruktury krytycznej podobnego do planu na rzecz cyberbezpieczeństwa.

W części I pkt 4 lit. b) załącznika wyjaśniono również wzajemne powiązania z planem na rzecz cyberbezpieczeństwa, który ma zastosowanie w przypadku wystąpienia cyberincydentów na dużą skalę, które powodują zakłócenia na skalę zbyt szeroką, aby dotknięte nimi państwo członkowskie zdołało się z nimi samodzielnie uporać, lub które

[8] Wspólny dokument roboczy służb „Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym", SWD(2023) 116 final.

[9] 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).

[10] 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).

dotykają co najmniej dwóch państw członkowskich bądź instytucji unijnych i mają tak szeroko zakrojony i znaczący wpływ o charakterze technicznym bądź politycznym, że wymagają terminowej koordynacji działań i reakcji na unijnym poziomie politycznym. Incydent zdefiniowano w dyrektywie NIS 2 jako „zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem" („cyberincydent").

Organy właściwe na mocy dyrektywy CER i dyrektywy NIS 2 mają obowiązek współpracy i wymiany informacji na temat cyberincydentów i incydentów wpływających na podmioty krytyczne, w tym w odniesieniu do odpowiednich zastosowanych środków. W przypadku gdy znaczący incydent związany z infrastrukturą krytyczną i incydent w cyberbezpieczeństwie na dużą skalę mają wpływ na ten sam podmiot, odpowiednie podmioty powinny skoordynować swoje reakcje.

Wniosek jest spójny z unijnym protokołem do celów przeciwdziałania zagrożeniom hybrydowym, który ma zastosowanie w przypadku incydentów hybrydowych. W części I pkt 4 lit. a) załącznika wyjaśniono wzajemne powiązania z tym protokołem oraz wskazano, który instrument ma zastosowanie w przypadku, gdy znaczący incydent o wymiarze hybrydowym związany jest z infrastrukturą krytyczną.

Wniosek jest również spójny z innymi istniejącymi mechanizmami zarządzania kryzysowego na szczeblu Unii, takimi jak uzgodnienia IPCR Rady, wewnętrzny proces koordynacji kryzysowej Komisji „ARGUS"[11] i Unijny Mechanizm Ochrony Ludności[12] („UMOL") wspierany przez Centrum Koordynacji Reagowania Kryzysowego („ERCC") oraz mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych.

Wniosek jest również spójny z innymi odpowiednimi przepisami sektorowymi, w szczególności z określonymi w nich środkami, które regulują niektóre aspekty reagowania na zakłócenia przez podmioty działające w odnośnych sektorach.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawą wniosku jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE"), który dotyczy zbliżenia przepisów w celu usprawnienia rynku wewnętrznego, wraz z art. 292 TFUE, w którym ustanowiono odpowiednie przepisy dotyczące przyjmowania zaleceń.

Wybór art. 114 TFUE jako materialnej podstawy prawnej jest uzasadniony faktem, że proponowane zalecenie Rady ma na celu zapewnienie skoordynowanej reakcji w przypadku zakłóceń funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym. Takie zakłócenia wpływają na kilka państw członkowskich i mogą mieć wpływ na funkcjonowanie rynku wewnętrznego ze względu na rosnące współzależności między infrastrukturą a sektorami w coraz bardziej współzależnej gospodarce Unii. Z kolei lepsza reakcja na takie zakłócenia pozwoli uniknąć zakłóceń w funkcjonowaniu rynku wewnętrznego, ponieważ ta infrastruktura krytyczna i świadczone przez nią usługi kluczowe

[11] Komunikat Komisji do Parlamentu europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Ustalenia Komisji w sprawie bezpiecznego ogólnego systemu szybkiego ostrzegania „ARGUS", COM(2005) 662 final.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/836 z dnia 20 maja 2021 r. zmieniające decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 185 z 26.5.2021, s. 1).

mają decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska.

Wniosek ma stanowić uzupełnienie dyrektywy w sprawie europejskiej infrastruktury krytycznej i dyrektywy CER, które również opierają się na art. 114 TFUE. Także zalecenie w sprawie odporności infrastruktury krytycznej, podobnie jak obecnie proponowane zalecenie, opiera się na art. 114 i 292 TFUE.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Podczas gdy reagowanie na zakłócenia w funkcjonowaniu infrastruktury krytycznej lub w usługach świadczonych przez podmioty krytyczne będące operatorami tej infrastruktury krytycznej jest przede wszystkim obowiązkiem państw członkowskich, Unia odgrywa ważną rolę w przypadku zakłócenia funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym, ponieważ takie zakłócenie może mieć wpływ na szereg obszarów działalności w obrębie jednolitego rynku, bezpieczeństwa i stosunków międzynarodowych Unii lub nawet na wszystkie te obszary. W celu zapewnienia funkcjonowania rynku wewnętrznego koordynacja na szczeblu Unii w przypadku zakłóceń funkcjonowania infrastruktury krytycznej o istotnym skutku transgranicznym jest nie tylko właściwa, lecz także konieczna, ponieważ taka skoordynowana reakcja na szczeblu Unii będzie wspierać reakcję państw członkowskich na zakłócenie polegającą na wspólnej orientacji sytuacyjnej, skoordynowanej komunikacji publicznej i łagodzeniu skutków zakłócenia na rynku wewnętrznym.

- **Proporcjonalność**

Niniejszy wniosek jest zgodny z zasadą proporcjonalności, o której mowa w art. 5 ust. 4 Traktatu o Unii Europejskiej.

Ani treść, ani forma zalecenia Rady, którego dotyczy niniejszy wniosek, nie wykraczają poza to, co jest konieczne do osiągnięcia jego celów. Proponowane działania są proporcjonalne do zamierzonych celów, polegających głównie na zapewnieniu skoordynowanej reakcji na szczeblu Unii w przypadku zakłóceń funkcjonowania infrastruktury krytycznej lub zakłóceń świadczenia usług przez podmioty krytyczne będące operatorami tej infrastruktury krytycznej i które mają istotne znaczenie transgraniczne. Proponowana skoordynowana reakcja jest proporcjonalna do prerogatyw i obowiązków państw członkowskich wynikających z prawa krajowego. Incydenty zakłócające funkcjonowanie infrastruktury krytycznej lub świadczenie usług kluczowych przez podmioty krytyczne często nie przekraczają progu pozwalającego uznać je za znaczący incydent związany z infrastrukturą krytyczną, wobec czego można skutecznie zajmować się nimi na szczeblu krajowym. W związku z tym korzystanie z mechanizmu przewidzianego w niniejszym wniosku ogranicza się do poważnych zakłóceń o istotnym znaczeniu transgranicznym, które mają wpływ na kilka państw członkowskich.

- **Wybór instrumentu**

Aby osiągnąć cele, o których mowa powyżej, TFUE przewiduje, zwłaszcza w art. 292, przyjęcie przez Radę zaleceń na podstawie wniosku Komisji. Zgodnie z art. 288 TFUE zalecenia nie mają mocy wiążącej. Zalecenie Rady jest odpowiednim instrumentem w tym przypadku, ponieważ sygnalizuje zaangażowanie państw członkowskich w stosowanie zawartych w nim środków i stanowi solidną podstawę współpracy w dziedzinie skoordynowanej reakcji w przypadku znaczących zakłóceń funkcjonowania infrastruktury krytycznej. W ten sposób proponowane zalecenie może uzupełnić wiążące ramy prawne (w szczególności dyrektywę CER), a także wcześniej przyjęte zalecenie w sprawie odporności infrastruktury krytycznej, w którym apeluje się o wprowadzenie takich środków

uzupełniających, przy pełnym poszanowaniu obowiązków państw członkowskich w przedmiotowej dziedzinie.

3. WYNIKI OCEN EX POST, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

• Konsultacje z zainteresowanymi stronami

Przy opracowywaniu niniejszego wniosku przeprowadzono konsultacje z państwami członkowskimi oraz instytucjami i agencjami Unii. Uwzględniono ponadto opinie ekspertów z państw członkowskich wyrażone zarówno podczas warsztatów w dniu 24 kwietnia 2023 r., jak i przesłane później na piśmie.

Panował ogólny konsensus co do przydatności zwiększenia koordynacji reagowania na szczeblu Unii na zakłócenia funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym w obecnym kontekście zagrożeń, przy jednoczesnym poszanowaniu kompetencji państw członkowskich w tej dziedzinie i poufności informacji szczególnie chronionych. Panował również konsensus co do potrzeby niepowielania instrumentów i właściwego wykorzystania mechanizmów koordynacji, wymiany informacji i reagowania, które istnieją już na szczeblu Unii.

Podczas gdy niektóre państwa członkowskie pozytywnie oceniły szerszy zakres planu dotyczącego infrastruktury krytycznej, inne uznały, że próg wynoszący co najmniej sześć państw członkowskich przewidziany w dyrektywie CER w odniesieniu do identyfikacji podmiotów krytycznych o szczególnym znaczeniu europejskim jest wystarczający i nie jest konieczne włączenie w ten zakres drugiego rodzaju incydentu. Kilka państw członkowskich zwróciło uwagę na to, jak ważne będzie angażowanie, w stosownych przypadkach, operatorów infrastruktury krytycznej świadczących usługi kluczowe ze względu na ich wiedzę fachową oraz, jak istotne jest wzięcie pod uwagę wymiaru dotyczącego cyberbezpieczeństwa.

• Szczegółowe objaśnienia poszczególnych przepisów wniosku

Wniosek dotyczący zalecenia Rady składa się z części głównej i załącznika.

Część główna składa się z 11 punktów.

W pkt 1 przedstawiono potrzebę wzmocnienia współpracy w zakresie reagowania – zgodnie z planem dotyczącym infrastruktury krytycznej zawartym w niniejszym zaleceniu, w tym ze stosownymi częściami załącznika do tego zalecenia – na znaczące incydenty związane z infrastrukturą krytyczną.

W pkt 2 wyjaśniono zakres planu dotyczącego infrastruktury krytycznej, odnoszącego się do następujących dwóch rodzajów incydentów zakłócających, które spowodowałyby jego zastosowanie: incydent mający istotny skutek zakłócający świadczenie usług kluczowych na rzecz co najmniej sześciu państw członkowskich albo w co najmniej sześciu państwach członkowskich lub incydent mający istotny skutek zakłócający w co najmniej dwóch państwach członkowskich, przy czym odpowiednie podmioty wymienione w planie działania zgadzają się co do potrzeby koordynacji na szczeblu unijnym ze względu na istotny wpływ incydentu.

W pkt 3 mowa jest o identyfikacji odpowiednich podmiotów, które mają być zaangażowane w realizację planu dotyczącego infrastruktury krytycznej, oraz poziomów, na których plan ten będzie realizowany (operacyjny, strategiczny/polityczny). Jest to bardziej szczegółowo wyjaśnione w załączniku do zalecenia.

W pkt 4 zaleca się stosowanie planu dotyczącego infrastruktury krytycznej zgodnie z innymi odpowiednimi instrumentami opisanymi w załączniku.

W pkt 5 zaleca się państwom członkowskim skuteczne reagowanie na szczeblu krajowym na znaczące zakłócenia funkcjonowania infrastruktury krytycznej.

W pkt 6 zaleca się ustanowienie lub wyznaczenie punktów kontaktowych przez odpowiednie podmioty, które to punkty powinny wspomagać stosowanie planu dotyczącego infrastruktury krytycznej. W miarę możliwości funkcję tę powinny pełnić pojedyncze punkty kontaktowe ustanowione na podstawie dyrektywy CER.

W pkt 7 mowa jest o przepływie informacji w przypadku znaczącego incydentu związanego z infrastrukturą krytyczną.

W pkt 8 wyjaśnia się, w jaki sposób powinna odbywać się wymiana informacji.

W pkt 9 zaleca się przeprowadzanie ćwiczeń, aby testować funkcjonowanie planu dotyczącego infrastruktury krytycznej.

W pkt 10 zaleca się omówienie wyciągniętych wniosków na forum Grupy ds. Odporności Podmiotów Krytycznych, która powinna przygotować sprawozdanie zawierające zalecenia. Sprawozdanie powinno zostać przyjęte przez Komisję.

W pkt 11 zaleca się państwom członkowskim omówienie sprawozdania na forum Rady.

W załączniku opisano cele, zasady, główne podmioty planu dotyczącego infrastruktury krytycznej, jego funkcjonowanie oraz jego wzajemne oddziaływanie z istniejącymi mechanizmami reagowania kryzysowego. Uwzględniono w nim dwa tryby współpracy: wymianę informacji i reagowanie.

2023/0318 (NLE)

Wniosek

ZALECENIE RADY

w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym

(Tekst mający znaczenie dla EOG)

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114 i 292,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Możliwość polegania na odpornej infrastrukturze krytycznej i odpornych podmiotach krytycznych świadczących usługi, które mają decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, ma zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego i całego społeczeństwa.

(2) Zważywszy na zmieniający się krajobraz ryzyka i rosnące współzależności między infrastrukturą a sektorami oraz, w szerszym ujęciu, wzajemne połączenia między sektorami a granicami, trzeba zająć się – w sposób kompleksowy i skoordynowany – ochroną i poprawą ochrony infrastruktury krytycznej oraz odporności operujących nią podmiotów krytycznych.

(3) Incydent, który zakłóca funkcjonowanie infrastruktury krytycznej, a tym samym uniemożliwia lub poważnie utrudnia świadczenie usług kluczowych, może mieć istotne skutki transgraniczne i negatywnie wpływać na rynek wewnętrzny. Aby zapewnić ukierunkowane, proporcjonalne i skuteczne podejście, należy wprowadzić środki w celu zaradzenia w szczególności znaczącym incydentom związanym z infrastrukturą krytyczną, jak określono w niniejszym zaleceniu, obejmujące na przykład sytuacje, w których zakłócenie spowodowane incydentem trwa długo lub może mieć znaczące skutki kaskadowe w tych samych lub innych sektorach lub państwach członkowskich.

(4) Skoordynowana reakcja na znaczące incydenty związane z infrastrukturą krytyczną jest kluczowa, aby uniknąć poważnych zakłóceń na rynku wewnętrznym i zapewnić jak najszybsze przywrócenie świadczenia tych usług kluczowych, ponieważ takie incydenty mogą mieć poważne konsekwencje dla gospodarki i obywateli Unii. Szybka i skuteczna reakcja na takie incydenty na szczeblu Unii wymaga szybkiej i skutecznej współpracy wszystkich odpowiednich podmiotów oraz skoordynowanego działania wspieranego na szczeblu Unii. Taka reakcja zależy zatem od istnienia wcześniej ustanowionych i, w miarę możliwości, dobrze przećwiczonych procedur

i mechanizmów współpracy, w których kluczowe podmioty na szczeblu krajowym i unijnym mają określone role i obowiązki.

(5) Chociaż odpowiedzialność za zapewnienie reakcji na znaczące incydenty związane z infrastrukturą krytyczną spoczywa głównie na państwach członkowskich i podmiotach będących operatorami infrastruktury krytycznej i świadczących usługi kluczowe, zwiększona koordynacja na szczeblu Unii jest właściwa w przypadku zakłóceń o istotnym znaczeniu transgranicznym. Szybka i skuteczna reakcja zależy nie tylko od wdrożenia przez państwa członkowskie mechanizmów krajowych, lecz także od skoordynowanych działań wspieranych na szczeblu Unii, w tym od szybkiej i skutecznej współpracy.

(6) Ochronę europejskiej infrastruktury krytycznej reguluje obecnie dyrektywa Rady 2008/114/WE[1], która obejmuje tylko dwa sektory – transportu i energii. Dyrektywa ta ustanawia procedurę rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz wspólne podejście do oceny potrzeby wzmocnienia jej ochrony. Jest to główny filar europejskiego programu ochrony infrastruktury krytycznej[2] („EPOIK") przyjętego przez Komisję w 2006 r., w którym określono ramy ochrony infrastruktury krytycznej obejmujące wszystkie zagrożenia na szczeblu europejskim.

(7) Aby wyjść poza ochronę infrastruktury krytycznej i w szerszym ujęciu zapewnić odporność podmiotów krytycznych będących operatorami takiej infrastruktury, które świadczą usługi kluczowe na rynku wewnętrznym, z dniem 18 października 2024 r. dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557[3] zastąpi dyrektywę 2008/114/WE. Dyrektywa (UE) 2022/2557 obejmuje 11 sektorów i określa obowiązki państw członkowskich i podmiotów krytycznych w zakresie zwiększania odporności, kwestię współpracy państw członkowskich między sobą i z Komisją, a także wsparcie ze strony Komisji dla organów krajowych i podmiotów krytycznych oraz wsparcie ze strony państw członkowskich dla podmiotów krytycznych.

(8) Po sabotażu gazociągów Nord Stream konieczne jest przyjęcie na szczeblu Unii większej liczby środków zwiększających odporność infrastruktury krytycznej. W związku z tym – na podstawie wniosku Komisji – Rada przyjęła zalecenie w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej („zalecenie 2023/C 20/01")[4], którego celem jest zwiększenie gotowości, reakcji i współpracy międzynarodowej w tej dziedzinie. W zaleceniu tym podkreślono między innymi potrzebę zapewnienia na szczeblu Unii skoordynowanej i skutecznej odpowiedzi na zagrożenia dla świadczenia usług kluczowych.

(9) Wobec tego konieczne jest uzupełnienie istniejących ram prawnych dodatkowym zaleceniem Rady ustanawiającym plan skoordynowanego reagowania na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym („plan dotyczący

---

[1] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. L 345 z 23.12.2008, s. 75).

[2] COM(2006) 786 final z dnia 12 grudnia 2006 r. – Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej.

[3] 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).

[4] Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej 2023/C 20/01 (Dz.U. C 20 z 20.1.2023, s. 1).

infrastruktury krytycznej”), a jednocześnie wykorzystanie ustaleń istniejących już na szczeblu unijnym.

(10) Niniejsze zalecenie należy dostosować do zalecenia 2023/C 20/01, aby zapewnić spójność i uniknąć powielania działań. W związku z tym niniejsze zalecenie nie powinno obejmować pozostałych elementów cyklu zarządzania kryzysowego, czyli zapobiegania, gotowości i odbudowy.

(11) Niniejsze zalecenie powinno uzupełniać dyrektywę (UE) 2022/2557, w szczególności pod względem skoordynowanej reakcji, i należy je wdrażać przy zapewnieniu spójności z tą dyrektywą i wszelkimi innymi mającymi zastosowanie przepisami prawa Unii. Niniejsze zalecenie powinno więc opierać się również na pojęciach, narzędziach i procesach zawartych w tej dyrektywie, takich jak Grupa ds. Odporności Podmiotów Krytycznych, działająca w granicach jej zadań określonych w tej dyrektywie, i punkty kontaktowe, oraz wykorzystywać te pojęcia, narzędzia i procesy. Pojęcie „infrastruktury krytycznej” stosowane w niniejszym zaleceniu należy ponadto rozumieć w taki sam sposób, jak określono w motywie 7 zalecenia 2023/C 20/01, tj. jako obejmujące odpowiednią infrastrukturę krytyczną wskazaną przez państwo członkowskie na szczeblu krajowym lub wyznaczoną jako europejska infrastruktura krytyczna na mocy dyrektywy 2008/114/WE, oraz podmioty krytyczne, które należy wskazać na mocy dyrektywy (UE) 2022/2557. Aby zapewnić spójność z dyrektywą (UE) 2022/2557, pojęcia użyte w niniejszym zaleceniu należy zatem interpretować jako mające takie samo znaczenie jak w tej dyrektywie. Na przykład pojęcie odporności, zdefiniowane w art. 2 pkt 2 tej dyrektywy, należy rozumieć jako odnoszące się także do zdolności infrastruktury krytycznej do zapobiegania zdarzeniom, które w istotny sposób zakłócają lub mogą w istotny sposób zakłócić świadczenie usług kluczowych na rynku wewnętrznym, tj. usług, które mają kluczowe znaczenie dla utrzymania niezbędnych funkcji społecznych i gospodarczych, bezpieczeństwa publicznego, zdrowia ludności lub środowiska, a także do zdolności tej infrastruktury do ochrony przed takimi zdarzeniami, reagowania na nie, przeciwstawiania się im, łagodzenia lub amortyzowania ich skutków, przystosowywania się do nich lub przywracania po nich poprzedniego stanu.

(12) Ponadto pojęcie „istotnego skutku zakłócającego” należy rozumieć w świetle kryteriów przewidzianych w art. 7 ust. 1 dyrektywy (UE) 2022/2557, obejmujących: i) liczbę użytkowników zależnych od usługi kluczowej świadczonej przez odnośny podmiot; ii) stopień, w jakim inne sektory i podsektory określone w załączniku do tej dyrektywy zależą od danej usługi kluczowej; iii) wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publiczne lub na zdrowie ludności; iv) udział podmiotu w rynku odnośnej usługi kluczowej lub odnośnych usług kluczowych; v) obszar geograficzny, którego mógłby dotyczyć incydent, z uwzględnieniem wszelkiego wpływu transgranicznego oraz podatności na zagrożenia związanej ze stopniem odizolowania niektórych rodzajów obszarów geograficznych, takich jak regiony wyspiarskie, regiony oddalone lub obszary górskie; vi) znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia.

(13) W trosce o efektywność i skuteczność plan dotyczący infrastruktury krytycznej powinien być w pełni spójny i interoperacyjny ze zmienionym unijnym protokołem

operacyjnym do celów przeciwdziałania zagrożeniom hybrydowym[5] oraz uwzględniać istniejący plan skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych określony w zaleceniu Komisji (UE) 2017/1584[6] („plan na rzecz cyberbezpieczeństwa") oraz mandat europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe") określony w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555[7], a także powinien unikać powielania struktur i działań. Należy w nim również zapewnić pełne poszanowanie zintegrowanych uzgodnień Rady dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych[8] („IPCR") w zakresie koordynacji reagowania.

(14) Niniejsze zalecenie opiera się na ustanowionych unijnych mechanizmach zarządzania kryzysowego i, w szerszym ujęciu, jest z nimi spójne i stanowi ich uzupełnienie – do mechanizmów tych należą w szczególności uzgodnienia IPCR Rady, wewnętrzny proces koordynacji kryzysowej Komisji „ARGUS"[9] i Unijny Mechanizm Ochrony Ludności („UMOL")[10], wspierany przez Centrum Koordynacji Reagowania Kryzysowego („ERCC")[11], mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych („ESDZ"), a także nadzwyczajny instrument jednolitego rynku[12] – które to mechanizmy mogą odgrywać rolę w reagowaniu na poważne zakłócenia funkcjonowania infrastruktury krytycznej.

(15) Wyżej wspomniane narzędzia lub mechanizmy na szczeblu Unii można stosować w odpowiedzi na znaczący incydent związany z infrastrukturą krytyczną, zgodnie z mającymi do nich zastosowanie zasadami i procedurami, a niniejsze zalecenie powinno te zasady i procedury uzupełniać, lecz na nie nie wpływać. Na przykład uzgodnienia IPCR Rady pozostają głównym narzędziem koordynacji reakcji państw członkowskich na szczeblu politycznym Unii. Koordynacja wewnętrzna w Komisji odbywa się zgodnie z międzysektorowym procesem koordynacji w sytuacjach kryzysowych w ramach ARGUS. Jeżeli kryzys ma wymiar zewnętrzny lub wymiar wspólnej polityki bezpieczeństwa i obrony („WPBiO"), można wykorzystać mechanizm reagowania kryzysowego ESDZ. Zgodnie z decyzją nr 1313/2013/UE

---

[5] Wspólny dokument roboczy służb „Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym", SWD(2023) 116 final.

[6] 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).

[7] 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, s. 80).

[8] 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).

[9] Komunikat Komisji do Parlamentu europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Ustalenia Komisji w sprawie bezpiecznego ogólnego systemu szybkiego ostrzegania „ARGUS", COM(2005) 662 final.

[10] 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).

[11] Decyzja nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności tworzy ramy uwzględniające wszystkie zagrożenia, określające na szczeblu unijnym uzgodnienia dotyczące zapobiegania, gotowości i reagowania w celu zarządzania wszelkiego rodzaju klęskami żywiołowymi i katastrofami spowodowanymi przez człowieka lub zagrażającymi klęskami i katastrofami w UE i poza nią.

[12] Rozporządzenie Parlamentu Europejskiego i Rady …/… w sprawie ustanowienia nadzwyczajnego instrumentu jednolitego rynku i uchylenia rozporządzenia Rady (WE) nr 2679/98, COM(2022) 459 final.

w sprawie Unijnego Mechanizmu Ochrony Ludności („UMOL”) reakcje operacyjne w ramach UMOL w przypadku wystąpienia lub groźby wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka w Unii i poza nią (w tym katastrof mających wpływ na infrastrukturę krytyczną) organizuje ERCC, które jest pojedynczym całodobowym centrum operacyjnym Komisji odpowiedzialnym za zarządzanie reagowaniem kryzysowym. W takich przypadkach ERCC może zapewniać wczesne ostrzeganie, powiadamianie, analizę i wspomaganie wymiany informacji, a w przypadku uruchomienia UMOL przez państwo członkowskie – wysyłać do dotkniętych obszarów pomoc operacyjną i ekspertów. ERCC może ponadto ułatwiać koordynację sektorową i międzysektorową zarówno na szczeblu UE, jak i między UE a odpowiednimi organami krajowymi, w tym organami odpowiedzialnymi za ochronę ludności i odporność infrastruktury krytycznej.

(16) Chociaż procesy określone w niniejszym zaleceniu należy w stosownych przypadkach uwzględnić przy korzystaniu z tych innych narzędzi lub mechanizmów, w niniejszym zaleceniu należy również opisać działania, które można podjąć na szczeblu Unii w odniesieniu do wspólnej orientacji sytuacyjnej, skoordynowanej komunikacji publicznej i skutecznej reakcji poza ramami tych unijnych mechanizmów koordynacji kryzysowej, w przypadkach, w których nie są one wykorzystywane.

(17) Aby lepiej koordynować reakcję na znaczące incydenty związane z infrastrukturą krytyczną, należy wzmocnić współpracę między państwami członkowskimi a instytucjami Unii, odpowiednimi agencjami, organami i urzędami Unii działającymi na podstawie istniejących ustaleń, zgodnie z ramami planu dotyczącego infrastruktury krytycznej. Plan dotyczący infrastruktury krytycznej powinien zatem mieć zastosowanie, jeżeli osiągnięty zostanie próg co najmniej sześciu państw członkowskich przewidziany w dyrektywie (UE) 2022/2557 w odniesieniu do identyfikacji podmiotów krytycznych o szczególnym znaczeniu europejskim, jak również w przypadku, gdy zachodzą incydenty mające wpływ na mniejszą liczbę państw członkowskich, ponieważ incydenty takie mogą wywierać szeroki wpływ ze względu na transgraniczne skutki kaskadowe, a zatem korzystna byłaby koordynacja reagowania na szczeblu unijnym.

(18) Chociaż ramy współpracy na szczeblu Unii w zakresie skoordynowanej reakcji na znaczące incydenty związane z infrastrukturą krytyczną uznaje się za konieczne, nie powinny one skutkować przekierowaniem zasobów podmiotów krytycznych i właściwych organów z działań podejmowanych w reakcji na incydent, które to działania powinny pozostać priorytetem.

(19) Należy jasno określić odpowiednie podmioty zaangażowane we wdrażanie planu dotyczącego infrastruktury krytycznej, aby istniał jasny i kompleksowy przegląd instytucji, organów, urzędów, agencji i władz, które mogłyby reagować na znaczące incydenty związane z infrastrukturą krytyczną.

(20) Za reagowanie na incydenty związane z infrastrukturą krytyczną, w tym na incydenty znaczące, odpowiadają przede wszystkim właściwe organy państw członkowskich. Niniejsze zalecenie nie powinno wpływać na odpowiedzialność państw członkowskich za ochronę bezpieczeństwa narodowego i obronności ani innych podstawowych funkcji państwa, w szczególności w zakresie bezpieczeństwa publicznego, integralności terytorialnej i utrzymywania porządku publicznego zgodnie z prawem Unii. Niniejsze zalecenie nie powinno ponadto mieć wpływu na procesy krajowe, takie jak komunikacja i kontakty operatorów infrastruktury krytycznej z właściwymi organami krajowymi. Niniejsze zalecenie powinno mieć zastosowanie bez wpływu na

odpowiednie dwustronne lub wielostronne porozumienia zawarte między państwami członkowskimi.

(21) Wyznaczenie lub ustanowienie punktów kontaktowych przez odpowiednie podmioty ma zasadnicze znaczenie dla skutecznej i terminowej współpracy w ramach planu działania infrastruktury krytycznej. Aby zapewnić spójność, państwa członkowskie powinny rozważyć wyznaczenie lub ustanowienie – jako punkty kontaktowe, o których tutaj mowa – pojedynczych punktów kontaktowych wyznaczonych lub ustanowionych na mocy dyrektywy (UE) 2022/2557.

(22) Aby zapewnić skuteczność, kluczowym elementem utrzymania wysokiego poziomu gotowości w przypadku znaczących incydentów związanych z infrastrukturą krytyczną oraz zapewnienia zdolności do szybkiego i dobrze skoordynowanego reagowania przy udziale odpowiednich podmiotów powinno być testowanie i wdrażanie planu dotyczącego infrastruktury krytycznej, a także składanie sprawozdań i omawianie wniosków wyciągniętych z jego stosowania.

(23) Ze względu na strukturę mechanizmu koordynacji kryzysowej Rady w postaci IPCR oraz, w szerszym ujęciu, potencjalne uruchomienie mechanizmów koordynacji kryzysowej, które już istnieją na szczeblu Unii, plan dotyczący infrastruktury krytycznej powinien obejmować dwa tryby współpracy przy reagowaniu na znaczący incydent związany z infrastrukturą krytyczną. Pierwszy z nich powinien polegać na wymianie informacji między wszystkimi odpowiednimi podmiotami, koordynacji komunikacji publicznej oraz, w stosownych przypadkach, koordynacji za pośrednictwem już istniejących mechanizmów, takich jak uzgodnienia IPCR Rady lub koordynacja w ramach Komisji z wykorzystaniem ARGUS, przy wsparciu ze strony ERCC jako operacyjnego całodobowego punktu kontaktowego, oraz mechanizmu reagowania kryzysowego ESDZ. Drugi tryb powinien obejmować dalsze działania w zakresie reagowania w zależności od skali incydentu. Współpraca ta powinna obejmować zaangażowanie na poziomach operacyjnym oraz strategicznym/politycznym, co odzwierciedla poziomy określone w zaleceniu 2017/1584 i w unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym, aby umożliwić skuteczną i efektywną koordynację działań i reakcję na znaczący incydent związany z infrastrukturą krytyczną. Na podstawie zasad proporcjonalności, pomocniczości, poufności informacji i komplementarności oraz w celu zapewnienia skutecznej współpracy, w planie dotyczącym infrastruktury krytycznej należy opisać, w jaki sposób odbywa się wspólna orientacja sytuacyjna odpowiednich podmiotów, a także skoordynowana komunikacja publiczna i skuteczne reagowanie.

(24) Wymiana informacji na podstawie niniejszego zalecenia powinna odbywać się bez narażania bezpieczeństwa narodowego lub bezpieczeństwa i interesów handlowych podmiotów będących operatorami infrastruktury krytycznej. W związku z tym dostęp do informacji szczególnie chronionych, ich wymiana i postępowanie z nimi powinny odbywać się z zachowaniem ostrożności, zgodnie z obowiązującymi przepisami i ze zwróceniem szczególnej uwagi na wykorzystywane kanały transmisji i zdolności przechowywania,

PRZYJMUJE NINIEJSZE ZALECENIE:

1) Państwa członkowskie, Rada, Komisja oraz, w stosownych przypadkach, Europejska Służba Działań Zewnętrznych („ESDZ”), a także odpowiednie organy, urzędy

i agencje Unii powinny współpracować w ramach planu dotyczącego infrastruktury krytycznej, zawartego w niniejszym zaleceniu, aby osiągnąć cele określone w części I sekcja 1 załącznika, oraz zapewniać skoordynowaną reakcję na znaczące incydenty związane z infrastrukturą krytyczną, przy uwzględnieniu zasad określonych w części I sekcja 2 załącznika.

2) Państwa członkowskie, Rada, Komisja oraz, w stosownych przypadkach, ESDZ, a także odpowiednie organy, urzędy i agencje Unii powinny bez zbędnej zwłoki stosować plan dotyczący infrastruktury krytycznej w każdym przypadku wystąpienia znaczącego incydentu związanego z infrastrukturą krytyczną, tj. incydentu dotyczącego infrastruktury krytycznej mającego jeden z następujących skutków:

   a) istotny skutek zakłócający świadczenie usług kluczowych na rzecz co najmniej sześciu państw członkowskich lub w co najmniej sześciu państwach członkowskich, w tym w przypadku wpływu na podmiot krytyczny o szczególnym znaczeniu europejskim w rozumieniu art. 17 dyrektywy (UE) 2022/2557 w sprawie odporności podmiotów krytycznych[13] lub

   b) istotny skutek zakłócający świadczenie usług kluczowych w co najmniej dwóch państwach członkowskich, w przypadku gdy państwo członkowskie sprawujące rotacyjną prezydencję w Radzie, w porozumieniu ze wspomnianymi państwami członkowskimi i z Komisją, uzna, że konieczna jest terminowa koordynacja w zakresie reagowania na szczeblu Unii ze względu na szeroko zakrojony i znaczący wpływ incydentu, mający techniczne lub polityczne znaczenie.

3) Odpowiednie podmioty planu dotyczącego infrastruktury krytycznej, określone na poziomach operacyjnym lub strategicznym/politycznym, zgodnie z częścią I sekcja 3 załącznika, powinny dążyć do współdziałania i współpracy, aby zapewnić komplementarność. Powinny one zapewniać odpowiednią i terminową wymianę informacji, w tym koordynację komunikacji publicznej, oraz skoordynowaną reakcję, określone w części II załącznika.

4) Plan dotyczący infrastruktury krytycznej powinno się stosować z uwzględnieniem innych odpowiednich instrumentów i spójnie z nimi, zgodnie z częścią I sekcja 4 załącznika. W przypadku gdy incydent ma wpływ zarówno na aspekty fizyczne, jak i na cyberbezpieczeństwo infrastruktury krytycznej, należy zapewnić synergię z odpowiednimi procesami określonymi w planie na rzecz cyberbezpieczeństwa.

5) Państwa członkowskie powinny zapewniać skuteczne reagowanie na szczeblu krajowym, zgodnie z prawem Unii, na zakłócenia funkcjonowania infrastruktury krytycznej w następstwie znaczących incydentów związanych z tą infrastrukturą.

6) Państwa członkowskie, Rada, ESDZ, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania („Europol”) i inne właściwe agencje Unii oraz Komisja powinny wyznaczyć lub ustanowić punkty kontaktowe do spraw związanych z planem dotyczącym infrastruktury krytycznej. Punkty kontaktowe powinny wspierać stosowanie planu dotyczącego infrastruktury krytycznej przez udzielanie niezbędnych informacji i ułatwianie działań koordynacyjnych w odpowiedzi na

[13] 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).

znaczące incydenty związane z infrastrukturą krytyczną. W przypadku państw członkowskich w miarę funkcję tę powinny pełnić pojedyncze punkty kontaktowe wyznaczone lub ustanowione na podstawie art. 9 ust. 2 dyrektywy (UE) 2022/2557. W przypadku Komisji ERCC zapewnia całodobowy kontakt i zdolności operacyjne oraz koordynuje, monitoruje i wspiera w czasie rzeczywistym reagowanie na sytuacje nadzwyczajne na szczeblu Unii, a jednocześnie służy państwom członkowskim i Komisji za operacyjne centrum reagowania kryzysowego, propagujące międzysektorowe podejście do zarządzania katastrofami.

7) Państwo członkowskie sprawujące rotacyjną prezydencję w Radzie, w porozumieniu z państwami członkowskimi, których dotyczy incydent, powinno poinformować wszystkie odpowiednie podmioty, za pośrednictwem punktów kontaktowych, o których mowa w pkt 6, o znaczącym incydencie związanym z infrastrukturą krytyczną oraz o stosowaniu planu dotyczącego infrastruktury krytycznej. Wymiana informacji o znaczącym incydencie związanym z infrastrukturą krytyczną powinna odbywać się za pośrednictwem odpowiednich kanałów komunikacji, w tym, w stosownych przypadkach, platformy zintegrowanych uzgodnień dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych[14] („IPCR") oraz ERCC za pośrednictwem wspólnego systemu łączności i informacji w sytuacjach nadzwyczajnych („CECIS") – internetowej aplikacji do ostrzegania i powiadamiania, która umożliwia wymianę informacji w czasie rzeczywistym.

8) W razie potrzeby kanały transmisji powinny obejmować kanały zabezpieczone, aby nie narażać bezpieczeństwa narodowego ani bezpieczeństwa i interesów handlowych zainteresowanych podmiotów. Także wymiana informacji opisana w części II sekcja 1 załącznika do niniejszego zalecenia powinna odbywać się bez narażania bezpieczeństwa narodowego lub bezpieczeństwa i interesów handlowych podmiotów krytycznych oraz zgodnie z prawem Unii, w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) .../... [15]. W szczególności dostęp do informacji szczególnie chronionych, ich wymiana i postępowanie z nimi powinny odbywać się z zachowaniem ostrożności. Przy przetwarzaniu i wymianie informacji niejawnych należy korzystać z dostępnych, akredytowanych narzędzi oraz stosować odpowiednie środki bezpieczeństwa.

9) Odpowiednie podmioty powinny regularnie testować funkcjonowanie planu dotyczącego infrastruktury krytycznej oraz trenować skoordynowaną reakcję na znaczące incydenty związane z infrastrukturą krytyczną na szczeblu krajowym, regionalnym i unijnym, na przykład w kontekście ćwiczeń. Takie ćwiczenia i testy mogą w stosownych przypadkach obejmować podmioty sektora prywatnego. Ćwiczenia na szczeblu Unii, w których uwzględnione zostaną aspekty bezpieczeństwa fizycznego i cybernetycznego, powinny odbyć się do dnia [*data przyjęcia niniejszego zalecenia + 12 miesięcy*].

10) Po zastosowaniu planu dotyczącego infrastruktury krytycznej w odniesieniu do znaczącego incydentu związanego z infrastrukturą krytyczną Grupa ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19 dyrektywy (UE) 2022/2557, powinna w odpowiednim czasie omówić z odpowiednimi podmiotami wyciągnięte

[14] 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, ST/13422/2018/INIT (Dz.U. L 320 z 17.12.2018, s. 28).

[15] Rozporządzenie (UE) …/… w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii, COM(2022) 119 final.

wnioski, które mogą wskazywać na luki i obszary wymagające poprawy, a następnie przygotować sprawozdanie zawierające zalecenia umożliwiające osiągnięcie takiej poprawy. Przygotowanie tego sprawozdania powinny wspomagać odpowiednie podmioty zaangażowane w stosowanie planu działania infrastruktury krytycznej. Sprawozdanie powinno zostać przyjęte przez Komisję.

11) Państwa członkowskie powinny omówić sprawozdanie, o którym mowa w pkt 10, na forum odpowiednich organów przygotowawczych Rady lub na forum Rady.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący