C/2024/4371

5.7.2024

ZALECENIE RADY

z dnia 25 czerwca 2024 r.

w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne

(Tekst mający znaczenie dla EOG)

(C/2024/4371)

RADA UNII EUROPEJSKIEJ,

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

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, działalności gospodarczej, zdrowia publicznego i bezpieczeństwa publicznego czy dla środowiska, jest podstawą sprawnego funkcjonowania rynku wewnętrznego i całego społeczeństwa.

(2) W zmieniającym się krajobrazie ryzyka i z uwagi na rosnące współzależności między infrastrukturą a sektorami oraz, w szerszym ujęciu, na wzajemne połączenia międzysektorowe i ponadgraniczne należy zająć się kwestią ochrony infrastruktury krytycznej oraz odporności podmiotów krytycznych będących operatorami tej infrastruktury, a także zwiększyć tę ochronę i tę odporność.

(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 podjąć środki pozwalające zaradzić w szczególności incydentom związanym z infrastrukturą krytyczną mającym istotne znaczenie transgraniczne, o których mowa w niniejszym zaleceniu.

(4) Skoordynowana reakcja na taki incydent mający istotne znaczenie transgraniczne może okazać się kluczowa, aby uniknąć poważnych zakłóceń na rynku wewnętrznym i zapewnić jak najszybsze przywrócenie świadczenia usług kluczowych, na które wpłynął incydent, ponieważ taki incydent może mieć poważne konsekwencje dla gospodarki i obywateli Unii. Szybka i skuteczna reakcja na taki incydent na szczeblu Unii wymaga sprawnej 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, dwustronnym, wielostronnym i, w stosownych przypadkach, 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, w przypadku zakłóceń mających istotne znaczenie transgraniczne celowe może okazać się zwiększenie koordynacji na szczeblu Unii. Szybka i skuteczna reakcja może zależeć 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 w tym zakresie.

(6) Za reagowanie na incydenty związane z infrastrukturą krytyczną, w tym na incydenty mające istotne znaczenie transgraniczne, odpowiadają przede wszystkim właściwe organy państw członkowskich. Niniejsze zalecenie nie wpływa na odpowiedzialność państw członkowskich za gwarantowanie bezpieczeństwa narodowego i obronności ani na ich uprawnienia w zakresie ochrony innych podstawowych funkcji państwa, w szczególności w zakresie bezpieczeństwa publicznego, integralności terytorialnej i utrzymywania porządku publicznego zgodnie z prawem Unii. Niniejsze zalecenie nie ma zatem zastosowania do infrastruktury krytycznej, która służy do prowadzenia działań w tych obszarach. Niniejsze zalecenie nie ma ponadto wpływu na procesy krajowe, takie jak komunikacja i kontakty podmiotów będących operatorami infrastruktury krytycznej z właściwymi organami krajowymi. Stosowanie niniejszego zalecenia nie wpływa na odnośne dwustronne lub wielostronne porozumienia zawarte przez państwa członkowskie i między nimi.

(7) 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 potrzeb w zakresie poprawy ochrony tej infrastruktury. Jest to główny filar europejskiego programu ochrony infrastruktury krytycznej (EPOIK) ustanowionego przez Komisję w swoim Komunikacie z dnia 12 grudnia w 2006 r. ([2]), w którym określono ramy ochrony infrastruktury krytycznej obejmujące wszystkie zagrożenia na szczeblu unijnym.

(8) Aby wyjść poza ochronę infrastruktury krytycznej i w szerszym ujęciu zapewnić odporność podmiotów krytycznych będących operatorami infrastruktury krytycznej i świadczących usługi kluczowe na rynku wewnętrznym, z dniem 18 października 2024 r. dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 ([3]) zastępuje dyrektywę 2008/114/WE. Dyrektywa (UE) 2022/2557 obejmuje 11 sektorów i reguluje 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.

(9) Po sabotażu gazociągów Nord Stream Rada na podstawie wniosku Komisji przyjęła zalecenie w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej ([4]) (zwane dalej „zaleceniem 2023/C 20/01"), którego celem jest zwiększenie gotowości oraz wzmocnienie reakcji oraz unijnej i międzynarodowej współpracy w tej dziedzinie. W zaleceniu zwrócono uwagę w szczególności na konieczność zapewnienia na szczeblu Unii skoordynowanej i skutecznej reakcji oraz gotowości operacyjnej do radzenia sobie z natychmiastowymi i pośrednimi skutkami zakłóceń mających istotne znaczenie transgraniczne, do których dochodzi w świadczeniu usług kluczowych przez infrastrukturę krytyczną.

(10) W związku z tym niniejsze zalecenie, niebędące aktem wiążącym, jest konieczne, aby wesprzeć i uzupełnić istniejące ramy prawne dodatkowym zaleceniem Rady ustanawiającym plan skoordynowanego reagowania na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne (zwany dalej „planem UE dotyczącym infrastruktury krytycznej"), a jednocześnie wykorzystać ustalenia już istniejące na szczeblu Unii.

(11) Niniejsze zalecenie zostało dostosowane do zalecenia 2023/C 20/01, aby zapewnić spójność i uniknąć powielania się obu aktów. W związku z tym niniejsze zalecenie nie obejmuje pozostałych elementów cyklu zarządzania sytuacjami kryzysowymi i nadzwyczajnymi, czyli zapobiegania, gotowości i odbudowy.

(12) 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. W niniejszym zaleceniu przyjmuje się podejście uwzględniające wszystkie zagrożenia i w miarę możliwości, przewiduje ono oparcie się na istniejących strukturach i mechanizmach, w tym na odpowiednich grupach roboczych w Radzie (czyli Grupie Roboczej ds. Ochrony Ludności – odporność podmiotów krytycznych „Grupa Robocza PROCIV CER"), a także na istniejących pojęciach, narzędziach i procesach przewidzianych we wspomnianej dyrektywie, takich jak Grupa ds. Odporności Podmiotów Krytycznych, działająca w granicach jej zadań określonych w tej dyrektywie, i punkty kontaktowe; niniejsze zalecenie przewiduje też wykorzystywanie tych struktur, mechanizmów, pojęć, narzędzi i procesów. Ponadto pojęcie „infrastruktury krytycznej" stosowane w niniejszym zaleceniu należy rozumieć w sposób określony w pkt 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 pojęcia zastosowane w tej dyrektywie. Na przykład koncepcję odporności, zdefiniowaną w art. 2 pkt 2 tej dyrektywy, należy również rozumieć jako dotyczącą 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 czy dla środowiska, a także dotyczącą zdolności tej infrastruktury do ochrony przed takimi zdarzeniami, reagowania na nie, przeciwstawiania się im, łagodzenia lub absorbowania ich skutków, przystosowywania się do nich lub przywracania po nich poprzedniego stanu.

(13) Zakres stosowania niniejszego zalecenia ograniczony jest do sektorów, podsektorów i rodzajów podmiotów, objętych zakresem dyrektywy (UE) 2022/2557. Wyłączenia przewidziane w tej dyrektywie dotyczą zakresu stosowania niniejszego zalecenia. Oprócz tego niniejsze zalecenie nie powinno powielać już istniejących ustaleń i struktur przewidzianych w odpowiednich sektorowych aktach prawnych Unii.

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

([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).

(14) 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 świadczenia tej usługi kluczowej.

(15) W trosce o efektywność i skuteczność plan UE dotyczący infrastruktury krytycznej powinien zapewnić pełne poszanowanie zintegrowanych uzgodnień Rady dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (zwanego dalej „IPCR") w zakresie koordynacji reagowania ([5]). Powinien również być w pełni skoordynowany, spójny i interoperacyjny ze wszystkimi pozostałymi sektorowymi instrumentami i procesami unijnymi, takimi jak procesy opisane w unijnym zestawie narzędzi do przeciwdziałania zagrożeniom hybrydowym ([6]) i w zmienionym unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym ([7]). Powinien on uwzględniać też i szanować mandaty europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (zwanej dalej „EU-CyCLONe") i zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „CSIRT") określone w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 ([8]). Należy w stosownych przypadkach uwzględniać także plan działania na rzecz skoordynowanego reagowania na transgraniczne incydenty i kryzysy cybernetyczne na dużą skalę ustanowiony zaleceniem Komisji (UE) 2017/1584 ([9]) (zwany dalej „planem na rzecz cyberbezpieczeństwa") oraz ogólnoeuropejskie ramy koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (zwanych dalej „EU-SCICF") zalecane przez Europejską Radę ds. Ryzyka Systemowego (ERRS). W miarę możliwości należy unikać powielania struktur i działań.

(16) Niniejsze zalecenie opiera się na istniejących ustaleniach dwustronnych lub wielostronnych i na ugruntowanych unijnych mechanizmach zarządzania w sytuacjach kryzysowych i nadzwyczajnych i jest, w szerszym ujęciu, z nimi spójne oraz stanowi ich uzupełnienie – do tych mechanizmów i ustaleń należą w szczególności uzgodnienia IPCR Rady, wewnętrzny proces koordynacji kryzysowej Komisji ARGUS ([10]) i Unijny Mechanizm Ochrony Ludności ([11]) (zwany dalej „UMOL"), wspierany przez Centrum Koordynacji Reagowania Kryzysowego (zwane dalej „ERCC") ([12]), mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych (ESDZ), a także rozporządzenie ustanawiające ramy środków dotyczących sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego – które to mechanizmy i ustalenia mogą odgrywać rolę w reagowaniu na poważne zakłócenia funkcjonowania infrastruktury krytycznej.

(17) Wyżej wspomniane narzędzia i mechanizmy na szczeblu Unii można stosować w odpowiedzi na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, zgodnie z zasadami i procedurami mającymi zastosowanie do tych narzędzi i mechanizmów, a niniejsze zalecenie powinno te zasady i procedury uzupełniać, lecz nie powinno na nie wpływać. Na przykład uzgodnienia IPCR Rady pozostają głównym narzędziem koordynowania między państwami członkowskimi reakcji 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, można wykorzystać mechanizm reagowania kryzysowego ESDZ. Na mocy decyzji nr 1313/2013/UE UMOL można aktywować w odpowiedzi na wystąpienie lub groźby wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka w Unii i poza nią (w tym klęsk i katastrof wynikających z incydentów mających wpływ na infrastrukturę krytyczną) przy operacyjnym wsparciu ze strony ERCC. ERCC ściśle współpracuje z krajowymi organami odpowiedzialnymi za ochronę ludności i z odpowiednimi organami unijnymi, aby propagować międzysektorowe podejście do zarządzania klęskami i katastrofami.

([5]) 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).

([6]) Zob. konkluzje Rady z dnia 21 czerwca 2022 r. w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe oraz wytyczne wykonawcze przyjęte przez Radę w dniu 13 grudnia 2022 r. dotyczące ram skoordynowanej reakcji UE na kampanie hybrydowe.

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

([8]) 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).

([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]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 23 grudnia 2005 r. - Ustalenia Komisji w sprawie bezpiecznego ogólnego systemu szybkiego ostrzegania „ARGUS" (COM (2005) 662 final).

([11]) 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).

([12]) Decyzja nr 1313/2013/UE tworzy ramy uwzględniające wszystkie zagrożenia i 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 Unii i poza nią.

(18) Procesy określone w niniejszym zaleceniu należy w stosownych przypadkach uwzględniać w związku z innymi narzędziami lub mechanizmami, jak tylko zostaną one zastosowane, jednak w niniejszym zaleceniu opisuje się również działania, które można podjąć na szczeblu Unii w odniesieniu do wspólnej orientacji sytuacyjnej, skoordynowanej komunikacji ze społeczeństwem i skutecznej reakcji poza ramami wspomnianych unijnych mechanizmów koordynacji kryzysowej w przypadkach, w których nie są one wykorzystywane.

(19) Aby lepiej koordynować, w stosownych przypadkach, reakcję na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne, należy zacieśnić współpracę między państwami członkowskimi a instytucjami Unii, odpowiednimi organami, urzędami i agencjami Unii działającymi na podstawie obowiązujących ustaleń, zgodnie z ramami planu UE dotyczącego infrastruktury krytycznej. Plan UE dotyczący infrastruktury krytycznej powinien mieć zatem zastosowanie wtedy, gdy występuje istotne zakłócenie świadczenia usług kluczowych, które to zakłócenie stwierdza i o którym informuje co najmniej sześć państw członkowskich, a także wtedy, gdy zakłócenie dotyczy podmiotu krytycznego o szczególnym znaczeniu europejskim w rozumieniu dyrektywy (UE) 2022/2557, które to zakłócenie stwierdzają i o którym informują państwa członkowskie, których dotyczy zakłócenie. Plan ten powinien mieć zastosowanie także wtedy, gdy incydenty mają istotny skutek zakłócający świadczenie usług kluczowych w co najmniej dwóch państwach członkowskich lub na ich rzecz, a prezydencja Rady stwierdzi, w porozumieniu z państwami członkowskimi, których dotyczy incydent, i w konsultacji z Komisją, że konieczna jest terminowa koordynacja reakcji na szczeblu Unii.

(20) Chociaż ramy współpracy na szczeblu Unii w zakresie skoordynowanej reakcji na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne 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 – i nie powinny zwiększać ich odpowiedzialności.

(21) Należy jasno określić odpowiednie podmioty zaangażowane we wdrażanie planu UE dotyczącego infrastruktury krytycznej, aby uzyskać jasny i kompleksowy obraz instytucji, organów, urzędów, agencji i władz, które mogłyby reagować na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne.

(22) Wyznaczenie lub ustanowienie punktów kontaktowych przez odpowiednie podmioty ma zasadnicze znaczenie dla skutecznej i terminowej współpracy w ramach planu UE dotyczącego infrastruktury krytycznej. Aby zapewnić spójność, państwa członkowskie powinny rozważyć możliwość wyznaczenia lub ustanowienia w tych ramach pojedynczych punktów kontaktowych, które będą punktami kontaktowymi wyznaczonymi lub ustanowionymi na mocy dyrektywy (UE) 2022/2557.

(23) Aby zapewnić skuteczność, kluczowym elementem utrzymania wysokiego poziomu gotowości na wypadek incydentów związanych z infrastrukturą krytyczną mających istotne znaczenie transgraniczne oraz zapewnienia zdolności do szybkiego i dobrze skoordynowanego reagowania przy udziale odpowiednich podmiotów powinno być testowanie i sprawdzanie planu UE dotyczącego infrastruktury krytycznej, a także składanie sprawozdań i omawianie wniosków wyciągniętych z jego stosowania.

(24) Ze względu na strukturę mechanizmu Rady dotyczącego koordynacji kryzysowej IPCR oraz mając na uwadze, w szerszym ujęciu, potencjalne uruchomienie mechanizmów koordynacji kryzysowej, które już istnieją na szczeblu Unii, w planie UE dotyczącym infrastruktury krytycznej należy przewidzieć dwa tryby współpracy podczas reagowania na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne. Pierwszy z trybów powinien polegać na wymianie stosownych informacji między wszystkimi odpowiednimi podmiotami, na koordynacji komunikacji ze społeczeństwem oraz, w stosownych przypadkach, na 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 całodobowego punktu kontaktowego IPCR i ARGUS, oraz mechanizmu reagowania kryzysowego ESDZ. Drugi tryb powinien obejmować dalsze działania w zakresie reagowania zależnie od tego, jaka jest skala incydentu i jak istotne jest skoordynowanie reakcji. Współpraca ta powinna wiązać się z zaangażowaniem na poziomach operacyjnym oraz strategicznym/politycznym, odzwierciedlając poziomy określone w zaleceniu (UE) 2017/1584 i w unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym, aby umożliwić skuteczną i sprawną koordynację działań i reakcję na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne. W oparciu o zasady proporcjonalności, pomocniczości, poufności informacji i komplementarności oraz w celu zapewnienia skutecznej współpracy, w planie UE dotyczącym infrastruktury krytycznej należy opisać, jak wygląda wspólna orientacja sytuacyjna odpowiednich podmiotów, a także skoordynowana komunikacja ze społeczeństwem i skuteczne reagowanie.

(25) Niniejsze zalecenie powinno pozostawać bez uszczerbku dla art. 346 Traktatu o funkcjonowaniu Unii Europejskiej. Informacje, które są poufne na podstawie przepisów unijnych lub krajowych, takich jak przepisy dotyczące tajemnicy przedsiębiorstwa, powinny podlegać wymianie z Komisją i innymi odpowiednimi organami zgodnie z zasadą wiedzy koniecznej i tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszego zalecenia. Od żadnego państwa członkowskiego nie należy oczekiwać, na podstawie niniejszego zalecenia, że udzieli informacji, których ujawnienie naraziłoby na szwank podstawowe interesy tego państwa, jego bezpieczeństwo narodowe, bezpieczeństwo publiczne lub obronność lub naraziłoby na szwank interesy gospodarcze 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 i tylko w takim zakresie, w jakim jest to istotne i proporcjonalne, zgodnie z mającymi zastosowanie przepisami i przy zwróceniu szczególnej uwagi na wykorzystywane kanały transmisji i zdolności przechowywania,

NINIEJSZYM ZALECA:

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 UE dotyczącego infrastruktury krytycznej, zawartego w niniejszym zaleceniu, aby osiągnąć cele określone w części I sekcja 1 załącznika, oraz powinny, z uwzględnieniem zasad określonych w części I sekcja 2 załącznika, zapewniać skoordynowaną reakcję na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne.

2) Państwa członkowskie, Rada, Komisja oraz, w stosownych przypadkach, ESDZ, a także odpowiednie organy, urzędy i agencje Unii powinny bez zbędnej zwłoki zastosować plan UE dotyczący infrastruktury krytycznej w każdym przypadku wystąpienia incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, o ile wyrazi na to zgodę państwo członkowskie, w którym znajduje się infrastruktura krytyczna, której dotyczy incydent. W kontekście tego planu UE dotyczącego infrastruktury krytycznej incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne zachodzi wówczas, gdy incydent dotyczący infrastruktury krytycznej ma jeden z następujących skutków:

   a) istotny skutek zakłócający świadczenie usług kluczowych, który stwierdziło co najmniej sześć państw członkowskich odczuwających ten skutek i o którym została poinformowana prezydencja Rady i Komisja;

   b) istotny skutek zakłócający świadczenie usług kluczowych przez podmiot krytyczny o szczególnym znaczeniu europejskim w rozumieniu art. 17 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 ([13]), który stwierdziło co najmniej jedno państwo członkowskie odczuwające ten skutek i o którym została poinformowana prezydencja Rady i Komisja; lub

   c) istotny skutek zakłócający świadczenie usług kluczowych w co najmniej dwóch państwach członkowskich lub na ich rzecz, w przypadku gdy prezydencja Rady stwierdzi, w porozumieniu z państwami członkowskimi odczuwającymi ten skutek i w konsultacji z Komisją, że konieczna jest terminowa koordynacja reakcji na szczeblu Unii ze względu na, przykładowo, szeroko zakrojony i znaczący wpływ incydentu mający techniczne lub polityczne znaczenie.

3) Odpowiednie podmioty planu UE dotyczącego infrastruktury krytycznej, określone na poziomach operacyjnym oraz 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 odpowiednich informacji, w tym koordynację komunikacji ze społeczeństwem oraz skoordynowaną reakcję, o których mowa w części II załącznika.

4) Plan UE dotyczący infrastruktury krytycznej należy 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 koordynację i synergię z przepisami dotyczącymi skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na dużą skalę zawartymi w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 ([14]).

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, niezależnie od tego, czy incydenty te mają istotne znaczenie transgraniczne czy też nie.

([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).

([14]) 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).

6) Państwa członkowskie, Rada, ESDZ, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (zwana dalej „Europolem") i inne właściwe agencje Unii oraz Komisja powinny wyznaczyć lub ustanowić punkty kontaktowe do spraw związanych z planem UE dotyczącym infrastruktury krytycznej. Z informacjami należy postępować zgodnie z ustanowionymi procedurami i regulacjami, w tym w zakresie postępowania z informacjami niejawnymi. Punkty kontaktowe powinny wspierać stosowanie planu UE dotyczącego infrastruktury krytycznej poprzez udzielanie niezbędnych informacji i ułatwianie działań koordynacyjnych w odpowiedzi na znaczące incydenty związane z infrastrukturą krytyczną. W przypadku państw członkowskich w miarę możliwości funkcję tych punktów kontaktowych powinny pełnić pojedyncze punkty kontaktowe wyznaczone lub ustanowione na podstawie art. 9 ust. 2 dyrektywy (UE) 2022/2557.

7) Państwo członkowskie sprawujące prezydencję w Radzie powinno, w porozumieniu z państwami członkowskimi, których dotyczy incydent, poinformować wszystkie odpowiednie podmioty zaangażowane w reakcję na incydent, za pośrednictwem punktów kontaktowych, o których mowa w pkt 6, o incydencie związanym z infrastrukturą krytyczną mającym istotne znaczenie transgraniczne oraz o zastosowaniu planu UE dotyczącego infrastruktury krytycznej. Wymiana informacji na temat incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne powinna odbywać się tylko w takim zakresie, w jakim jest to istotne i proporcjonalne do celów tej wymiany, i powinna odbywać się za pośrednictwem odpowiednich kanałów komunikacji, w tym, gdy jest to stosowne i celowe, za pośrednictwem platformy zintegrowanych uzgodnień dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych ([15]) (zwanych dalej „IPCR") oraz ERCC.

8) W razie potrzeby kanały transmisji powinny obejmować kanały zabezpieczone, aby nie narażać na szwank bezpieczeństwa narodowego ani bezpieczeństwa i interesów gospodarczych podmiotów krytycznych. Wymiana informacji odbywająca się zgodnie z załącznikiem nie powinna obejmować informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności państw członkowskich lub narażałoby na szwank bezpieczeństwo i interesy gospodarcze podmiotów krytycznych; wymiana ta powinna się odbywać zgodnie z prawem Unii. W szczególności dostęp do informacji szczególnie chronionych, ich wymiana i postępowanie z nimi powinny odbywać się z zachowaniem ostrożności. Przy postępowaniu z informacjami niejawnymi i przy ich wymianie należy korzystać z dostępnych akredytowanych narzędzi oraz stosować odpowiednie środki bezpieczeństwa.

9) Odpowiednie podmioty powinny sprawdzać i testować funkcjonowanie planu UE dotyczącego infrastruktury krytycznej oraz skoordynowaną reakcję na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne, na szczeblu krajowym, regionalnym i unijnym, na przykład w kontekście ćwiczeń. W sprawdzaniu i testach mogą uczestniczyć podmioty sektora prywatnego, za zgodą wszystkich stron, a w szczególności zainteresowanych państw członkowskich. Wszelkie kontakty z podmiotami krytycznymi powinny odbywać się za pośrednictwem zainteresowanego państwa członkowskiego. Komisja, w ścisłej współpracy z państwami członkowskimi – w tym za pośrednictwem Grupy Roboczej PROCIV CER, EU-CyCLONe, sieci CSIRT oraz przy wsparciu ENISA – powinna zorganizować ćwiczenie na szczeblu Unii, w którym uwzględnione zostaną aspekty bezpieczeństwa fizycznego i cybernetycznego. Cele ćwiczenia należy wcześniej uzgodnić z państwami członkowskimi. Ćwiczenie powinno odbyć się do dnia 26 grudnia 2026 r. Na podstawie wniosków z tego ćwiczenia wymienionych przez państwa członkowskie należy rozważyć potrzebę przeprowadzenia dalszych ćwiczeń oraz stosowne scenariusze.

10) Po zastosowaniu planu UE dotyczącego infrastruktury krytycznej w odniesieniu do incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne Grupa Robocza PROCIV CER powinna omówić wyciągnięte wnioski, z których może wyniknąć, że istnieją niedociągnięcia i konieczne są usprawnienia w pewnych obszarach. W ten proces omawiania wyciągniętych wniosków mogą być włączone, w stosownych przypadkach, inne odpowiednie grupy robocze. Zachęca się państwa członkowskie, aby w stosownych przypadkach zebrały wnioski wyciągnięte przez wszystkie odpowiednie podmioty bezpośrednio zaangażowane w reakcję na dany incydent. Na podstawie tych dyskusji prezydencja Rady, przy wsparciu Sekretariatu Generalnego Rady w konsultacji z Komisją i z państwami członkowskimi, których dotyczył incydent, powinna sporządzić sprawozdanie zawierające wyciągnięte wnioski. W razie konieczności sprawozdanie powinno zostać objęte klauzulą niejawności na odpowiednim poziomie.

Sporządzono w Luksemburgu dnia 25 czerwca 2024 r.

W imieniu Rady

Przewodnicząca

H. LAHBIB

([15]) 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).

ZAŁĄCZNIK

W niniejszym załączniku opisano cele, zasady, główne odpowiednie podmioty, wzajemne oddziaływanie z innymi odpowiednimi mechanizmami zarządzania w sytuacjach kryzysowych i nadzwyczajnych funkcjonowanie planu, który służy skoordynowanemu reagowaniu na incydenty związane z infrastrukturą krytyczną mające istotne znaczenie transgraniczne (zwanego dalej „planem UE dotyczącym infrastruktury krytycznej"), a także, w stosownych przypadkach, poprawie współpracy między państwami członkowskimi a odpowiednimi instytucjami, organami, urzędami i agencjami Unii w odniesieniu do takich incydentów, zgodnie z mającymi zastosowanie przepisami i procedurami. Niniejszy plan UE dotyczący infrastruktury krytycznej w żaden sposób nie wpływa na rolę i funkcjonowanie innych ustaleń.

Część I: Cele, zasady, podmioty i inne instrumenty

1. **Cele**

Plan UE dotyczący infrastruktury krytycznej służy promowaniu poniższych trzech głównych celów, które należy w stosownych przypadkach realizować podczas reakcji na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne:

a) wspólna orientacja sytuacyjna – ponieważ dobre zrozumienie w państwach członkowskich incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, jego przyczyn i potencjalnych konsekwencji dla wszystkich zainteresowanych stron na poziomach operacyjnym oraz strategicznym/politycznym jest podstawą odpowiedniej skoordynowanej reakcji;

b) skoordynowana komunikacja ze społeczeństwem – ponieważ pomaga ona łagodzić negatywne skutki incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne i minimalizować rozbieżności w komunikatach kierowanych do społeczeństw w poszczególnych państwach członkowskich, przy pełnym poszanowaniu krajowych kompetencji w zakresie komunikacji kryzysowej. Gdy jasna komunikacja ze społeczeństwem leży w interesie społeczeństwa i nie utrudnia operacji zarządzania w sytuacjach kryzysowych i nadzwyczajnych, jest również ważna w łagodzeniu skutków dezinformacji;

c) skoordynowana i skuteczna reakcja – ponieważ poprawa reakcji państw członkowskich i zacieśnienie współpracy państw członkowskich między sobą oraz z odpowiednimi instytucjami, organami, urzędami i agencjami Unii może przyczynić się do łagodzenia skutków incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne i do umożliwienia szybkiego przywrócenia usług kluczowych w sposób minimalizujący podatność tej infrastruktury na dalsze znaczące incydenty.

2. **Zasady**

Proporcjonalność

Incydenty zakłócające funkcjonowanie infrastruktury krytycznej lub świadczenie usług kluczowych często nie przekraczają progu pozwalającego uznać je za incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, określony w pkt 2 niniejszego zalecenia. W związku z tym, co do zasady, można się nimi skutecznie zająć na szczeblu krajowym. Dlatego stosowanie planu UE dotyczącego infrastruktury krytycznej powinno ograniczać się do incydentów związanych z infrastrukturą krytyczną mających istotne znaczenie transgraniczne.

Pomocniczość

Zgodnie z prawem Unii główna odpowiedzialność za reagowanie na zakłócenia funkcjonowania infrastruktury krytycznej lub świadczenia usług kluczowych przez podmioty krytyczne spoczywa na państwach członkowskich. Odpowiednie instytucje, organy, urzędy i agencje Unii, w szczególności Europejska Służba Działań Zewnętrznych (ESDZ) mogą jednak odgrywać ważną rolę uzupełniającą w przypadku incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, ponieważ taki incydent może mieć wpływ na niektóre lub nawet wszystkie obszary działalności gospodarczej w obrębie jednolitego rynku, na życie mieszkańców Unii, na bezpieczeństwo Unii oraz na jej stosunki międzynarodowe z partnerami – bez uszczerbku dla odpowiedzialności państw członkowskich za gwarantowanie bezpieczeństwa narodowego i obronności.

Komplementarność

Plan UE dotyczący infrastruktury krytycznej powinien uwzględniać i odzwierciedlać funkcjonowanie istniejących mechanizmów zarządzania w sytuacjach kryzysowych i nadzwyczajnych na szczeblu Unii, czyli zintegrowanych uzgodnień Rady dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR"), wewnętrznego procesu koordynacji kryzysowej Komisji ARGUS, Unijnego Mechanizmu Ochrony Ludności („UMOL"), wspieranego przez Centrum Koordynacji Reagowania Kryzysowego („ERCC"), ustanowionego w ramach UMOL decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE ([1]) oraz mechanizmu reagowania kryzysowego ESDZ. Powinien także opierać się na ustaleniach sektorowych, w tym na przepisach dotyczących skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na

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

dużą skalę, które to przepisy zawarte są w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 ([2]), na ramach „EU-SCICF" zalecanych przez Europejską Radę ds. Ryzyka Systemowego ([3]) (ERRS), na sieci punktów kontaktowych ds. transportu ([4]), na Europejskiej Komórce Koordynacji Kryzysowej ds. Lotnictwa ([5]) oraz na grupach koordynacyjnych ds. energii elektrycznej ([6]), gazu ([7]) i ropy naftowej ([8]).

Ponadto plan UE dotyczący infrastruktury krytycznej powinien przewidywać oparcie się na istniejących strukturach i mechanizmach na szczeblu Unii, w tym na odpowiednich grupach roboczych w Radzie (czyli Grupie Roboczej PROCIV CER) oraz strukturach i mechanizmach ustanowionych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557 ([9]), a także powinien przewidywać ich wykorzystywanie, w szczególności w kontekście współpracy właściwych organów państw członkowskich między sobą, z Komisją oraz w ramach Grupy ds. Odporności Podmiotów Krytycznych („CERG"), ustanowionej dyrektywą (UE) 2022/2557. Ponadto w planie powinno się uwzględniać obowiązki odpowiednich instytucji, organów, urzędów i agencji Unii zgodnie z mającymi do nich zastosowanie ramami prawnymi. Działania w zakresie reagowania kryzysowego dotyczące infrastruktury krytycznej stanowią uzupełnienie innych mechanizmów zarządzania w sytuacjach kryzysowych i nadzwyczajnych na szczeblu unijnym, krajowym i sektorowym, które to mechanizmy wspierają koordynację międzysektorową.

Poufność informacji

W planie UE dotyczącym infrastruktury krytycznej powinno się uwzględniać znaczenie ochrony poufności informacji niejawnych i szczególnie chronionych informacji jawnych związanych z infrastrukturą krytyczną i podmiotami krytycznymi.

Od żadnego państwa członkowskiego nie oczekuje się, że udzieli ono informacji, których ujawnienie naraziłoby na szwank podstawowe interesy jego bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi lub krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, powinny podlegać wymianie z Komisją i innymi odpowiednimi organami tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszego zalecenia. Wymiana informacji powinna odbywać się tylko w takim zakresie, w jakim jest to istotne i proporcjonalne do celów takiej wymiany. Przy wymianie informacji należy chronić poufność tych informacji oraz bezpieczeństwo i interesy gospodarcze podmiotów krytycznych, przy jednoczesnym poszanowaniu bezpieczeństwa państw członkowskich.

3. **Odpowiednie podmioty**

Każde państwo członkowskie oraz odpowiednie instytucje, organy, urzędy i agencje Unii, o których mowa w lit. a)–g) poniżej, powinny w stosownych przypadkach, zgodnie z mającymi do nich zastosowanie zasadami i procedurami, wskazać – w odniesieniu do każdego incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne – odpowiednie podmioty, w zależności od rodzaju incydentu i od tego, których sektorów on dotyczy.

a) Państwa członkowskie

— Właściwe organy (np. organy odpowiedzialne za infrastrukturę krytyczną, odpowiednie organy sektorowe, pojedyncze punkty kontaktowe wyznaczone lub ustanowione na podstawie art. 9 ust. 2 dyrektywy (UE) 2022/2557, organy wyznaczone lub ustanowione na podstawie art. 9 ust. 1 dyrektywy (UE) 2022/2557).

— Inne zainteresowane strony, w tym podmioty lub osoby z sektora prywatnego pełniące szczególne funkcje, takie jak operatorzy infrastruktury krytycznej, w tym operatorzy zidentyfikowani jako podmioty krytyczne.

— Ministrowie odpowiedzialni za odporność infrastruktury krytycznej lub ministrowie odpowiedzialni za sektor lub sektory, na które najbardziej wpłynął incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne.

b) Rada

— Prezydencja Rady.

— Coreper, Komitet Polityczny i Bezpieczeństwa, uzgodnienia IPCR.

([2]) 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).

([3]) Zalecenie Europejskiej Rady ds. Ryzyka Systemowego z dnia 2 grudnia 2021 r. w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17) (Dz.U. C 134 z 25.3.2022, s. 1).

([4]) Komunikat Komisji z dnia 23 maja 2022 r. pt. „Plan awaryjny dla transportu" (COM (2022) 211 final).

([5]) Ustanowionej na mocy art. 19 rozporządzenia wykonawczego Komisji (UE) 2019/123 z dnia 24 stycznia 2019 r. ustanawiającego szczegółowe przepisy wykonawcze dotyczące funkcji sieciowych zarządzania ruchem lotniczym (ATM) oraz uchylające rozporządzenie Komisji (UE) nr 677/2011 (Dz.U. L 28 z 31.1.2019, s. 1).

([6]) Decyzja Komisji 2012/C 353/02 z dnia 15 listopada 2012 r. ustanawiająca Grupę Koordynacyjną ds. Energii Elektrycznej (Dz. U. C 353 z 17.11.2012, s. 2).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010 (Dz.U. L 280 z 28.10.2017, s. 1).

([8]) Dyrektywa Rady 2009/119/WE z dnia 14 września 2009 r. nakładająca na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów ropopochodnych (Dz.U. L 265 z 9.10.2009, s. 9).

([9]) 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).

— Odpowiednie grupy robocze, takie jak Grupa Robocza ds. Ochrony Ludności – odporność podmiotów krytycznych („Grupa Robocza PROCIV CER"), oraz przewodniczący innych odpowiednich grup roboczych.

— Sekretariat Generalny Rady.

c) Rada Europejska

— Przewodniczący Rady Europejskiej.

d) Komisja

— Wyznaczone właściwe służby i Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych jako służba odpowiedzialną w danym obszarze, a w przypadku incydentu międzysektorowego – Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych oraz inne odpowiednie służby Komisji.

— Dyrekcja Generalna ds. Komunikacji i służba rzecznika.

— Dyrekcja Generalna HERA, europejski Urząd ds. Gotowości i Reagowania na Stany Zagrożenia Zdrowia.

— CERG, której przewodniczy przedstawiciel Komisji (Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych), oraz inne odpowiednie grupy ekspertów i komitety.

— ERCC ustanowione w ramach UMOL (całodobowe operacyjne centrum zarządzania kryzysowego w ramach UMOL w Dyrekcji Generalnej ds. Prowadzonych przez UE Operacji Ochrony Ludności i Pomocy Humanitarnej).

— Komitet ds. Bezpieczeństwa Zdrowia ustanowiony w art. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 ([10]).

— Sekretariat Generalny Komisji (sekretariat ARGUS) i (zastępca) sekretarza generalnego (proces ARGUS), Dyrekcja Generalna ds. Zasobów Ludzkich (Dyrekcja ds. Bezpieczeństwa).

— Inne odpowiednie grupy ekspertów Komisji wspierające Komisję w koordynowaniu środków w sytuacji nadzwyczajnej lub kryzysowej.

— Inne sieci zarządzania w sytuacjach kryzysowych i nadzwyczajnych, w tym sieci sektorowe (np. sieć punktów kontaktowych ds. transportu zarządzana przez Dyrekcję Generalną ds. Mobilności i Transportu, międzyinstytucjonalna grupa zadaniowa ds. cyberkryzysów ([11]), Europejska Komórka Koordynacji Kryzysowej ds. Lotnictwa).

— Przewodniczący lub odpowiedzialny wiceprzewodniczący/komisarz.

— Inne służby Komisji, które mogą mieć kompetencje w konkretnych obszarach wiedzy fachowej.

e) ESDZ

— Pojedyncza komórka analiz wywiadowczych („SIAC") złożona z Centrum Analiz Wywiadowczych („IntCen") i Dyrekcji ds. Wywiadu w Sztabie Wojskowym UE („EUMS Int").

— Centrum Reagowania Kryzysowego („CRC").

— Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa / wiceprzewodniczący Komisji (zwany dalej „Wysokim Przedstawicielem").

f) Odpowiednie organy, urzędy oraz agencje unijne, takie jak Europol lub ENISA, w zależności od tego, których sektorów dotyczy incydent ([12])

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz.U. L 314 z 6.12.2022, s. 26).

([11]) Nieformalna grupa obejmująca odpowiednie służby Komisji, ESDZ, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), CERT-UE i Europol, której współprzewodniczą Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii oraz ESDZ.

([12]) Np. sektor transportu: Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA), Europejska Agencja Bezpieczeństwa Morskiego (EMSA), Agencja Kolejowa Unii Europejskiej (ERA); sektor zdrowia: Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) i Europejska Agencja Leków (EMA); sektor energii: Agencja ds. Współpracy Organów Regulacji Energetyki (ACER); sektor kosmiczny: Agencja Unii Europejskiej ds. Programu Kosmicznego (EUSPA); sektor spożywczy: Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA); sektor morski: Europejska Agencja Kontroli Rybołówstwa (EFCA); w przypadku cyberincydentów: zespoły reagowania na incydenty bezpieczeństwa komputerowego („CSIRT"), Służba ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii („CERT-EU"), EBC, ERRS, Europejskie Urzędy Nadzoru („ESA").

g) Inne odpowiednie struktury

— Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe") ustanowiona w art. 16 dyrektywy (UE) 2022/2555.

— Sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego („CSIRT"), ustanowiona w art. 15 dyrektywy (UE) 2022/2555.

— Ogólnoeuropejskie ramy koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym („EU-SCICF"), o których mowa w zaleceniu ERRS ERRS/2021/17.

4. **Wzajemne oddziaływanie planu z innymi odpowiednimi mechanizmami i instrumentami zarządzania w sytuacjach kryzysowych i nadzwyczajnych**

Plan UE dotyczący infrastruktury krytycznej powinien być elastycznym narzędziem określającym różne działania, które można podjąć częściowo lub całkowicie z wykorzystaniem różnych istniejących ustaleń, w zależności od charakteru i powagi incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne oraz od potrzeby koordynacji operacyjnej lub strategicznej/politycznej.

a) Zintegrowane uzgodnienia dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR)

Zgodnie z decyzją wykonawczą Rady (UE) 2018/1993 ([13]), w przypadku kryzysu, w związku z którym uzgodnienia IPCR zostały aktywowane, środki przewidziane w planie UE dotyczącym infrastruktury krytycznej mogłyby stanowić część reakcji UE na szczeblu politycznym. W takiej sytuacji zastosowanie będzie miał proces decyzyjny IPCR, a plan UE dotyczący infrastruktury krytycznej można wykorzystać jako narzędzie uzupełniające zapewniające konkretne wsparcie IPCR pod kątem infrastruktury krytycznej w celu zapewnienia dobrze skoordynowanej reakcji. Uzgodnienia IPCR mają umożliwiać terminową koordynację polityki i reagowanie na szczeblu politycznym Unii (Coreper/Rada) w przypadku poważnych sytuacji nadzwyczajnych lub kryzysowych. IPCR wykorzystuje się również do koordynowania – na szczeblu strategicznym/politycznym – reakcji na powołanie się na klauzulę solidarności (art. 222 TFUE), aby zapewnić spójność i komplementarność działań Unii i państw członkowskich. Ustalenia dotyczące stosowania przez Unię klauzuli solidarności są zdefiniowane w decyzji Rady 2014/415/UE ([14]).

b) Unijny Mechanizm Ochrony Ludności („UMOL")

Na mocy decyzji nr 1313/2013/UE UMOL można aktywować w odpowiedzi na wystąpienie lub groźby wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka w Unii i poza nią (w tym klęsk i katastrof wynikających z incydentów mających wpływ na infrastrukturę krytyczną) przy operacyjnym wsparciu ze strony ERCC. ERCC ściśle współpracuje z krajowymi organami odpowiedzialnymi za ochronę ludności i z odpowiednimi organami unijnymi, aby propagować międzysektorowe podejście do zarządzania klęskami i katastrofami.

c) Unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym i unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym

W unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym ([15]) (zwany dalej „unijnym protokołem do celów przeciwdziałania zagrożeniom hybrydowym") określono procesy i narzędzia mające zastosowanie w przypadku zagrożeń lub kampanii hybrydowych w całym cyklu zarządzania w sytuacjach kryzysowych i nadzwyczajnych.

W przypadku znaczącego incydentu o wymiarze hybrydowym związanego z infrastrukturą krytyczną procesy i narzędzia określone w unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym stosuje się, w stosownych przypadkach, jako uzupełnienie planu UE dotyczącego infrastruktury krytycznej, np. w odniesieniu do konkretnych informacji, analiz lub komunikacji na temat hybrydowych aspektów incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne oraz w odniesieniu do współpracy z partnerami zewnętrznymi. W szczególności unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym ([16]) zapewnia ramy skoordynowanej reakcji UE na kampanie hybrydowe. Ponieważ główna odpowiedzialność za przeciwdziałanie zagrożeniom hybrydowym spoczywa na państwach członkowskich, zastosowanie ma proces decyzyjny opisany w wytycznych wykonawczych dotyczących ram skoordynowanej reakcji Unii na kampanie hybrydowe.

d) Przepisy dotyczące skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na dużą skalę zawarte w dyrektywie (UE) 2022/2555

Dyrektywa (UE) 2022/2555 zawiera przepisy dotyczące skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na dużą skalę za pośrednictwem istniejących sieci współpracy, w szczególności EU-CyCLONe i sieci CSIRT. EU-CyCLONe i sieć CSIRT współpracują w oparciu o uzgodnienia proceduralne, które określają szczegóły tej współpracy, i unikają powielania zadań.

([13]) 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).

([14]) Decyzja Rady 2014/415/UE z dnia 24 czerwca 2014 r. w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności (Dz.U. L 192 z 1.7.2014, s. 53).

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

([16]) Konkluzje Rady z dnia 21 czerwca 2022 r. w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe; wytyczne wykonawcze dotyczące ram skoordynowanej reakcji UE na kampanie hybrydowe (15880/22).

EU-CyCLONe pośredniczy między szczeblem technicznym a szczeblem politycznym podczas incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę, zacieśnia współpracę na szczeblu operacyjnym i wspiera proces decyzyjny na szczeblu politycznym. EU-CyCLONe opiera się na ustaleniach sieci CSIRT i wykorzystuje własne zdolności do sporządzania analizy skutków incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę. W przypadku incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, który zbiega się z cyberincydentem na dużą skalę lub wydaje się z nim powiązany, odpowiednie grupy robocze Rady powinny ustalić stosowną koordynację na szczeblu operacyjnym, w tym we współpracy z EU-CyCLONe. Celem koordynacji powinno być określenie, które podmioty, narzędzia lub mechanizmy mogłyby najskuteczniej przyczynić się do reakcji na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, przy jednoczesnym unikaniu powielania działań i równoległych kierunków prac. Taka koordynacja powinna być spójna z istniejącymi odpowiednimi ustaleniami podjętymi w chwili incydentu.

e) Inne mechanizmy i instrumenty sektorowe lub międzysektorowe

W planie UE dotyczącym infrastruktury krytycznej nie powinno się powielać innych sektorowych lub międzysektorowych narzędzi zarządzania w sytuacjach kryzysowych i nadzwyczajnych ani mechanizmów koordynacji. Jeżeli takie narzędzia lub mechanizmy już istnieją, plan UE dotyczący infrastruktury krytycznej, zgodnie z jego zakresem stosowania, należy wykorzystać jako narzędzie uzupełniające narzędzia lub mechanizmy sektorowe lub międzysektorowe, ale nie należy ich zastępować tym planem. Należy zapewnić niezbędną koordynację działań poszczególnych podmiotów, aby uniknąć takiego powielenia. W przypadku aktywacji IPCR koordynacja polityczna i strategiczna będzie odbywać się w ramach IPCR. W Komisji wewnętrzną koordynację kryzysową umożliwia komisyjny wewnętrzny proces koordynacji kryzysowej ARGUS, wspierany przez ERCC.

Część II: Wymiana informacji i skoordynowana reakcja

Opisane poniżej działania polegają na różnych trybach współpracy, czyli wymianie informacji, skoordynowanej komunikacji i reagowaniu. Struktura ta odpowiada trybom funkcjonowania mechanizmu koordynacji kryzysowej Rady IPCR i w szerszym ujęciu uwzględnia potencjalne wykorzystanie mechanizmów koordynacji kryzysowej, które już istnieją na szczeblu Unii. Struktura ta pokazuje, jak zintegrować te sposoby współpracy ze wspomnianymi mechanizmami w przypadku ich zastosowania. Większość tych działań można jednak również podjąć autonomicznie, gdyż nie zależą one od zastosowania tych mechanizmów, lecz je uzupełniają. Działania przedstawiono w porządku chronologicznym; należy jednak pamiętać, że w przypadku kryzysu na dużą skalę, który stanowi incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, niektóre działania można podjąć jednocześnie i w sposób ciągły.

1. **Wymiana informacji**

a) Na szczeblu operacyjnym

Państwa członkowskie, których dotyczy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, stosują własne środki awaryjne i zapewniają koordynację z odpowiednimi krajowymi mechanizmami zarządzania w sytuacjach kryzysowych i nadzwyczajnych oraz, w stosownych przypadkach, zaangażowanie wszystkich odpowiednich podmiotów krajowych, regionalnych i lokalnych.

Jeżeli ma to znaczenie dla pomocy w zakresie ochrony ludności i dla UMOL, koordynację między państwami członkowskimi i z Komisją zapewnia się za pośrednictwem ERCC i punktów kontaktowych państw członkowskich zgodnie z przepisami prawnymi dotyczącymi UMOL.

(i) Wymiana informacji i dokonywanie zgłoszeń przez właściwe organy krajowe

Oprócz obowiązków w zakresie zgłaszania i informowania określonych w art. 15 dyrektywy (UE) 2022/2557 i zgodnie z odpowiednimi krajowymi ramami prawnymi właściwe organy krajowe odpowiedzialne za infrastrukturę krytyczną w państwach członkowskich, których dotyczy incydent związany z tą infrastrukturą mający istotne znaczenie transgraniczne, powinny przekazywać prezydencji Rady i Komisji – za pośrednictwem swoich pojedynczych punktów kontaktowych i bez zbędnej zwłoki, chyba że jest to niemożliwe z operacyjnego punktu widzenia – odpowiednie informacje, które mogą obejmować informacje otrzymane od podmiotów krytycznych lub operatorów infrastruktury krytycznej lub z innych źródeł dotyczące uruchomionych mechanizmów zarządzania w sytuacjach kryzysowych i nadzwyczajnych.

Wymiana informacji na temat incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne powinna odbywać się tylko w takim zakresie, w jakim jest to istotne i proporcjonalne do celów tej wymiany, i powinna odbywać się za pośrednictwem odpowiednich kanałów komunikacji z właściwymi służbami Komisji. Gdy jest to stosowne i celowe, można wykorzystać IPCR i ERCC. Z informacjami należy postępować zgodnie z ustanowionymi procedurami i zasadami, w tym w zakresie postępowania z informacjami niejawnymi. Potencjalne wykorzystanie ERCC nie powinno wpłynąć na zasoby UMOL ani dostępność ERCC w zakresie stałego, pełnego obsługiwania UMOL.

Taka wymiana informacji może dotyczyć, w stosownych przypadkach, charakteru i przyczyny incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, zaobserwowanego lub szacowanego wpływu zakłócenia na infrastrukturę krytyczną i na świadczenie usług kluczowych, konsekwencji incydentu w różnych sektorach i ponad granicami oraz środków łagodzących – już wprowadzonych albo planowanych – na szczeblu krajowym lub we współpracy z odpowiednimi innymi państwami członkowskimi i Komisją w ramach istniejących uzgodnień, np. ustaleń dotyczących wymiany informacji na podstawie art. 9 i 15 dyrektywy (UE) 2022/2557. Taka wymiana informacji nie powinna skutkować przekierowaniem zasobów infrastruktury krytycznej lub, w niektórych przypadkach, zasobów podmiotu krytycznego lub państw członkowskich z działań podejmowanych w reakcji na incydent, które to działania należy traktować priorytetowo.

Aby zapewnić podjęcie działań następczych, powiadomione służby Komisji, w tym służby odpowiedzialne za sektor, w którym wystąpił incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, powinny informować punkt kontaktowy Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych i Sekretariat Generalny Komisji.

Jeżeli dane informacje mogą mieć znaczenie dla działań dotyczących wymiaru cyberbezpieczeństwa incydentu lub mogą być związane z cyberincydentem, Komisja i prezydencja Rady powinny przekazać istotne informacje EU-CyCLONe. Właściwe organy, o których mowa w dyrektywie (UE) 2022/2557 i w dyrektywie (UE) 2022/2555, powinny również bez zbędnej zwłoki podjąć ze sobą współpracę i wymianę informacji w odniesieniu do takich incydentów.

W przypadku sektora morskiego właściwe organy krajowe powinny rozważyć możliwość wykorzystania wspólnego mechanizmu wymiany informacji („CISE") do udostępniania informacji bez zbędnej zwłoki.

(ii) Wymiana informacji na szczeblu Unii

Komisja jak najszybciej zwołuje CERG, aby ułatwić właściwym organom krajowym odpowiedzialnym za infrastrukturę krytyczną i odpowiednim instytucjom, organom, urzędom i agencjom Unii wymianę istotnych informacji na temat incydentu (jego charakteru, przyczyny, wpływu i konsekwencji w różnych sektorach i ponad granicami), i informuje o tym prezydencję Rady. Ponieważ to posiedzenie CERG będzie dotyczyło odnośnego incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne oraz jego skutków, przypomina się państwom członkowskim, że mogą one zwrócić się do Komisji o zaproszenie na to posiedzenie krajowych ekspertów z tej dziedziny, aby zapewnić jak najodpowiedniejszą reprezentację państw członkowskich. W zależności od tego, którego sektora incydent najbardziej dotyczy, odpowiednie służby Komisji mogą być silnie zaangażowane w posiedzenie CERG w celu wymiany informacji zgromadzonych za pośrednictwem istniejących instrumentów sektorowych.

W przypadku incydentów łączących aspekty cyberbezpieczeństwa i aspekty bezpieczeństwa fizycznego niezwiązane z cyberbezpieczeństwem sieć CSIRT i EU-CyCLONe będą współpracować na podstawie ustaleń proceduralnych określonych w art. 15 ust. 6 dyrektywy (UE) 2022/2555. Prezydencja powinna zapewnić koordynację działań z odpowiednimi grupami roboczymi, odpowiednimi służbami Komisji, ESDZ, CERT-EU, ENISA i Europolem. W stosownych przypadkach CERT-EU udostępnia istotne informacje sieci CSIRT, a Komisja przekazuje informacje EU-CyCLONe. W porozumieniu z przewodniczącymi odnośnych grup i sieci Komisja (Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych oraz Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii) może, w stosownych przypadkach, zaproponować wspólne posiedzenie CERG, EU-CyCLONe i sieci CSIRT i informuje o tym prezydencję Rady.

W razie incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne, który to incydent dotyczy różnych sektorów i ma szeroko zakrojony wpływ lub znaczenie polityczne na szczeblu Unii, prezydencja Rady – z własnej inicjatywy i po konsultacji z państwami członkowskimi, których dotyczy incydent, z Komisją i Wysokim Przedstawicielem, lub na wniosek co najmniej jednego państwa członkowskiego – może przeanalizować możliwości koordynowania międzysektorowego za pośrednictwem IPCR. W przypadku aktywacji IPCR np. w trybie wymiany informacji koordynacja polityczna i strategiczna odbywałaby się w ramach IPCR, przy czym plan UE dotyczący infrastruktury krytycznej zapewniłby niezbędny wkład dotyczący tej infrastruktury w ramach wsparcia prac IPCR.

Jeżeli incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne dotyczy także państwa trzeciego, prezydencja Rady – po konsultacji z państwami członkowskimi, których dotyczy incydent i z Komisją – powinna przeanalizować stosowność i sposoby współpracy z tym państwem trzecim.

(iii) Wsparcie ze strony Komisji i agencji unijnych

W stosownych przypadkach Europol, zgodnie ze swoim mandatem, przedstawia na szczeblu Unii raport sytuacyjny na temat incydentu. Inne agencje unijne, w stosownych przypadkach, zgodnie ze swoimi odpowiednimi mandatami, przekazują istotne informacje, które są przydatne do opracowania orientacji sytuacyjnej lub skoordynowanej reakcji na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, odpowiednim „macierzystym" dyrekcjom generalnym, które z kolei przekazują te informacje Komisji (Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych), która przewodniczy CERG. Komisja stale przekazuje prezydencji Rady odpowiednie informacje.

W stosownych przypadkach i zgodnie z mającymi zastosowanie unijnymi i krajowymi ramami prawnymi Komisja może zapewnić informacje na potrzeby orientacji sytuacyjnej z wykorzystaniem zasobów unijnego programu kosmicznego ([17]), takich jak Copernicus, Galileo lub EGNOS.

b) Na szczeblu strategicznym

(i) Sporządzanie sprawozdań na podstawie wkładów państw członkowskich

Komisja przygotowuje sprawozdanie w dziedzinie odporności infrastruktury krytycznej na podstawie informacji (na temat incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne i istniejących najlepszych praktyk w zakresie postępowania wobec takiego incydentu) przekazanych przez właściwe organy krajowe na posiedzeniu CERG lub na wspólnych posiedzeniach z odpowiednimi służbami, grupami ekspertów czy sieciami, a także na podstawie innych dostępnych informacji. Sprawozdanie to zostanie udostępnione członkom CERG, członkom Grupy Roboczej PROCIV CER, a po konsultacji z prezydencją Rady – innym zainteresowanym stronom. W razie konieczności sprawozdanie zostanie objęte klauzulą niejawności na odpowiednim poziomie, a w każdym przypadku zostanie przekazane odpowiednim odbiorcom w państwach członkowskich, zgodnie zasadami i procedurami dotyczącymi bezpieczeństwa informacji określonymi w mających zastosowanie ramach prawnych.

W stosownych przypadkach w sprawozdaniu tym uwzględni się wyniki odpowiednich ocen, oszacowań i scenariuszy ryzyka na szczeblu Unii opracowanych pod kątem cyberbezpieczeństwa, m.in. przez Komisję, Wysokiego Przedstawiciela oraz Grupę Współpracy.

W przypadku aktywacji IPCR sprawozdanie to może stanowić wkład w zintegrowaną orientację i analizę sytuacyjną („ISAA") przygotowywaną przez służby Komisji i ESDZ.

W stosownych przypadkach SIAC przedstawia aktualną ocenę incydentu opartą na danych wywiadowczych.

(ii) Uruchomienie unijnych mechanizmów koordynacji kryzysowej i wykorzystanie unijnych narzędzi

Zgodnie z przepisami prawnymi dotyczącymi UMOL, ERCC może rozpocząć udzielanie wsparcia w zakresie orientacji sytuacyjnej w związku z incydentem, jeżeli zdarzenie powoduje uruchomienie UMOL ([18]). Ponadto – za pośrednictwem usługi systemu Copernicus w zakresie zarządzania kryzysowego – państwa członkowskie, których dotyczy incydent, mogą zwrócić się o obrazy satelitarne swojego terytorium.

W przypadku gdy uzna się za stosowne przekazanie informacji przez Komisję do ESDZ i odpowiednich agencji unijnych, główna dyrekcja generalna lub Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych w koordynacji z Sekretariatem Generalnym uruchamia wewnętrzny proces koordynacji kryzysowej Komisji ARGUS – Faza I przez otwarcie zdarzenia w narzędziu informatycznym ARGUS. Komisja dopilnowuje, aby odpowiednie informacje zostały przekazane państwom członkowskim podczas rozmów przy okrągłym stole IPCR lub za pośrednictwem platformy IPCR.

Prezydencja Rady może aktywować uzgodnienia IPCR w trybie wymiany informacji, co wiąże się z opracowywaniem sprawozdań ISAA przez Komisję i ESDZ w oparciu o informacje uzyskane od właściwych organów krajowych i, w stosownych przypadkach, z innych źródeł. Nawet, gdy IPCR nie zostaną aktywowane, prezydencja Rady może uruchomić stronę służącą monitorowaniu na platformie internetowej IPCR. Sekretariat Generalny Rady w porozumieniu z prezydencją może utworzyć stronę służącą monitorowaniu na wniosek państwa członkowskiego, którego dotyczy incydent, służb Komisji czy ESDZ.

W stosownych przypadkach można uruchomić inne (sektorowe) unijne mechanizmy i narzędzia zarządzania w sytuacjach kryzysowych i nadzwyczajnych zgodnie z odpowiednimi procedurami. Komisja zapewni koordynację między tymi mechanizmami i narzędziami.

Jeżeli incydent fizyczny zbiega się z cyberincydentem na dużą skalę zdefiniowanym w art. 6 pkt 7 dyrektywy (UE) 2022/2555 lub wydaje się z nim powiązany, prezydencja Rady może również zastosować przepisy dotyczące skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na dużą skalę określone w dyrektywie (UE) 2022/2555 do ustalenia odpowiedniej koordynacji angażującej m.in. Horyzontalną Grupę Roboczą ds. Cyberprzestrzeni, Grupę Roboczą PROCIV CER, CERG, EU CyCLONe i sieć CSIRT, zgodnie z ich własnymi zasadami i procedurami.

([17]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/696 z dnia 28 kwietnia 2021 r. ustanawiające Unijny program kosmiczny i Agencję Unii Europejskiej ds. Programu Kosmicznego oraz uchylające rozporządzenia (UE) nr 912/2010, (UE) nr 1285/2013 i (UE) nr 377/2014 oraz decyzję nr 541/2014/UE (Dz.U. L 170 z 12.5.2021, s. 69).

([18]) Mowa tu np. o publikacji produktów monitorowania mediów, komunikatów dotyczących ochrony ludności, briefingów analitycznych, map dziennych ECHO, codziennych aktualizacji ECHO oraz innych produktów dostosowanych do indywidualnych potrzeb.

(iii) Koordynacja komunikacji ze społeczeństwem

Państwa członkowskie, których dotyczy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, powinny koordynować w miarę możliwości swoją komunikację ze społeczeństwem na temat kryzysu przy jednoczesnym poszanowaniu krajowych kompetencji i ram administracyjnych w tym zakresie. W stosownych przypadkach można zaangażować sieć ds. komunikacji kryzysowej IPCR.

W oparciu o wspólną orientację sytuacyjną Grupa Robocza PROCIV CER, we współpracy z państwami członkowskimi, których dotyczy incydent, i po konsultacji z Komisją, może zorganizować wymianę poglądów na temat podejść do komunikacji ze społeczeństwem stosowanych przez państwa członkowskie i Komisję. Gdy okaże się to konieczne, Grupa Robocza PROCIV CER powinna starać się określić wspólne metody działania, aby ułatwić koordynację między państwami członkowskimi.

Należy przy tym uważać, aby działania komunikacyjne nie utrudniały krajowych operacji w zakresie zarządzania w sytuacjach kryzysowych i nadzwyczajnych.

Europol i inne odpowiednie agencje unijne koordynują swoje publiczne działania komunikacyjne ze służbą rzecznika Komisji w oparciu o wspólną orientację sytuacyjną i po konsultacji z państwami członkowskimi, których dotyczy incydent. Zgodnie z planem ERCC nie będzie odgrywać żadnej roli w komunikacji kryzysowej ze społeczeństwem.

Jeżeli incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne obejmuje wymiar zewnętrzny lub hybrydowy, komunikację ze społeczeństwem koordynuje się z ESDZ i służbą rzecznika Komisji, jak opisano w unijnym protokole do celów przeciwdziałania zagrożeniom hybrydowym.

2. **Reagowanie (obejmujące stałe działania opisane w częściach dotyczących wymiany informacji oraz dodatkowe działania na szczeblu strategicznym/politycznym)**

a) Na szczeblu strategicznym

(i) Stałe sporządzanie raportów sytuacyjnych

Grupa Robocza PROCIV CER powinna być informowana o sporządzaniu raportów (np. sprawozdań ISAA w przypadku aktywacji IPCR lub sprawozdania w dziedzinie odporności infrastruktury krytycznej przygotowywanego przez Komisję na podstawie wkładów państw członkowskich) i powinna przygotować posiedzenie Coreperu, jeżeli nie zostało ono jeszcze zwołane, lub, w stosownych przypadkach, posiedzenie Komitetu Politycznego i Bezpieczeństwa.

SIAC intensyfikuje działania informacyjne skierowane do służb wywiadowczych państw członkowskich, agreguje informacje ze wszystkich źródeł oraz przygotowuje analizę i ocenę incydentu, a także, w razie konieczności, regularnie je aktualizuje.

(ii) Organizacja posiedzeń koordynacyjnych

W oparciu o wspólną orientację sytuacyjną prezydencja Rady powinna jak najszybciej zwoływać posiedzenia Grupy Roboczej PROCIV CER w celu omówienia niedociągnięć, w dziedzinie odporności infrastruktury krytycznej, w reakcji Unii na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, a także zbadać możliwości koordynacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii. Jeżeli zostają aktywowane IPCR, wnioski z tych posiedzeń mogą być przedstawiane przez prezydencję podczas kryzysowych okrągłych stołów IPCR. Podczas kryzysowych okrągłych stołów IPCR można również wskazywać pewne konkretne niedociągnięcia w reakcji Unii na incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne i nakazać m.in. Grupie Roboczej PROCIV CER ich eliminowanie, a następnie informowanie o wynikach podczas kolejnych kryzysowych okrągłych stołów IPCR, tak by wspierać wysiłki IPCR w zakresie koordynacji politycznej i strategicznej.

(iii) Pełne uruchomienie unijnych mechanizmów koordynacji kryzysowej i wykorzystanie unijnych instrumentów

W przypadku aktywacji przez prezydencję Rady IPCR w trybie pełnym:

Koordynację reakcji na szczeblu politycznym Unii powinna przeprowadzić Rada z wykorzystaniem uzgodnień IPCR.

Prezydencja Rady zwołuje w stosownym terminie nieformalne rozmowy przy okrągłym stole, w których uczestniczą odpowiednie podmioty krajowe, unijne i międzynarodowe; podczas rozmów państwa członkowskie, których dotyczy incydent, mogą przekazać informacje na jego temat, prezydencja może przedstawić wnioski odpowiednich grup Roboczych w Radzie, a służby Komisji mogą poinformować o uprzednio zwołanych posiedzeniach grup, w stosownych przypadkach przy udziale ESDZ.

Można zwrócić się do SIAC i odpowiednich agencji unijnych o przedstawienie na tym posiedzeniu aktualnej sytuacji w zakresie incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne.

Służba właściwa ds. ISAA (Komisji lub ESDZ) przygotowuje sprawozdanie ISAA z wykorzystaniem materiałów dostarczonych przez odpowiednie służby Komisji, odpowiednie urzędy, organy i agencje Unii oraz właściwe organy krajowe. O wkład zostają także poproszone państwa członkowskie za pośrednictwem platformy internetowej IPCR.

Jeżeli przewodniczący Komisji uruchomi Fazę II wewnętrznego procesu koordynacji kryzysowej Komisji ARGUS, w krótkim czasie zwołuje się posiedzenia Komitetu Koordynacji Kryzysowej z udziałem odpowiednich służb Komisji, agencji i, w stosownych przypadkach, ESDZ na potrzeby koordynacji działań w odniesieniu do wszystkich aspektów incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne.

W przypadku gdy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne jest przedmiotem wspólnego zainteresowania Unii i NATO, służby Komisji i ESDZ mogą zwołać posiedzenie w ramach zorganizowanego dialogu UE–NATO na temat odporności, aby wnieść wkład we wspólną orientację sytuacyjną i wymienić się informacjami na temat środków zastosowanych odpowiednio przez Unię i przez NATO, przy pełnym poszanowaniu kompetencji Unii i państw członkowskich przewidzianych w Traktatach oraz głównych zasad regulujących współpracę UE–NATO uzgodnionych przez Radę Europejską, w szczególności zasad wzajemności, inkluzywności i autonomii decyzyjnej i przy zachowaniu pełnej przejrzystości względem wszystkich państw członkowskich. Z uwagi na znaczenie niezakłóconej wymiany informacji między Unią a NATO, informacje o incydentach uznanych za szczególnie chronione przez państwo członkowskie, którego dany incydent dotyczy, mogą być udostępnione NATO za wyraźną zgodą tego państwa. Państwa członkowskie zostaną poinformowane o wynikach zorganizowanego dialogu w odniesieniu do stosowania planu UE dotyczącego infrastruktury krytycznej.

(iv) Komunikacja ze społeczeństwem

W stosownych przypadkach Rada powinna organizować wymiany poglądów na temat podejść do komunikacji ze społeczeństwem i w razie konieczności powinna starać się określić wspólne metody działania, aby ułatwić koordynację między państwami członkowskimi i Komisją. Nieformalna sieć ds. komunikacji kryzysowej, ustanowiona w ramach IPCR, może wspierać te prace. W stosownych przypadkach również służby Komisji przygotowują komunikaty dla społeczeństwa, po konsultacji z państwem członkowskim, którego dotyczy incydent.

Jeżeli incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne obejmuje wymiar zewnętrzny lub hybrydowy, komunikację ze społeczeństwem należy koordynować z ESDZ i służbą rzecznika Komisji. Zgodnie z planem ERCC nie będzie odgrywać żadnej roli w komunikacji kryzysowej ze społeczeństwem.

(v) Wsparcie dla państw członkowskich i skuteczne reagowanie

Prezydencja Rady może zwołać kolejne posiedzenia Grupy Roboczej PROCIV CER i innych odpowiednich grup roboczych w celu wsparcia działań prowadzonych w ramach IPCR, jeżeli IPCR zostały aktywowane.

Państwa członkowskie, których dotyczy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, mogą zwrócić się – za pośrednictwem prezydencji Rady lub Grupy Roboczej PROCIV CER – do innych państw członkowskich o udzielenie, dwustronnie, wsparcia technicznego, np. o udostępnienie konkretnej wiedzy fachowej w celu złagodzenia szkodliwego wpływu incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne.

Państwa członkowskie, których dotyczy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, mogą zwrócić się również o wsparcie techniczne lub finansowe do Komisji lub odpowiednich agencji unijnych. Po otrzymaniu takiego wniosku Komisja, we współpracy z odpowiednimi agencjami unijnymi, ocenia, jakiego wsparcia może udzielić, i – w stosownych przypadkach oraz za zgodą państw członkowskich, których dotyczy incydent – uruchamia techniczne środki łagodzące na szczeblu Unii zgodnie z odpowiednimi procedurami Komisji lub agencji oraz koordynuje zdolności techniczne niezbędne do powstrzymania lub ograniczenia wpływu incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne. Komisja i prezydencja powinny przekazywać sobie odpowiednie informacje o takich wnioskach w celu zapewnienia skutecznej koordynacji.

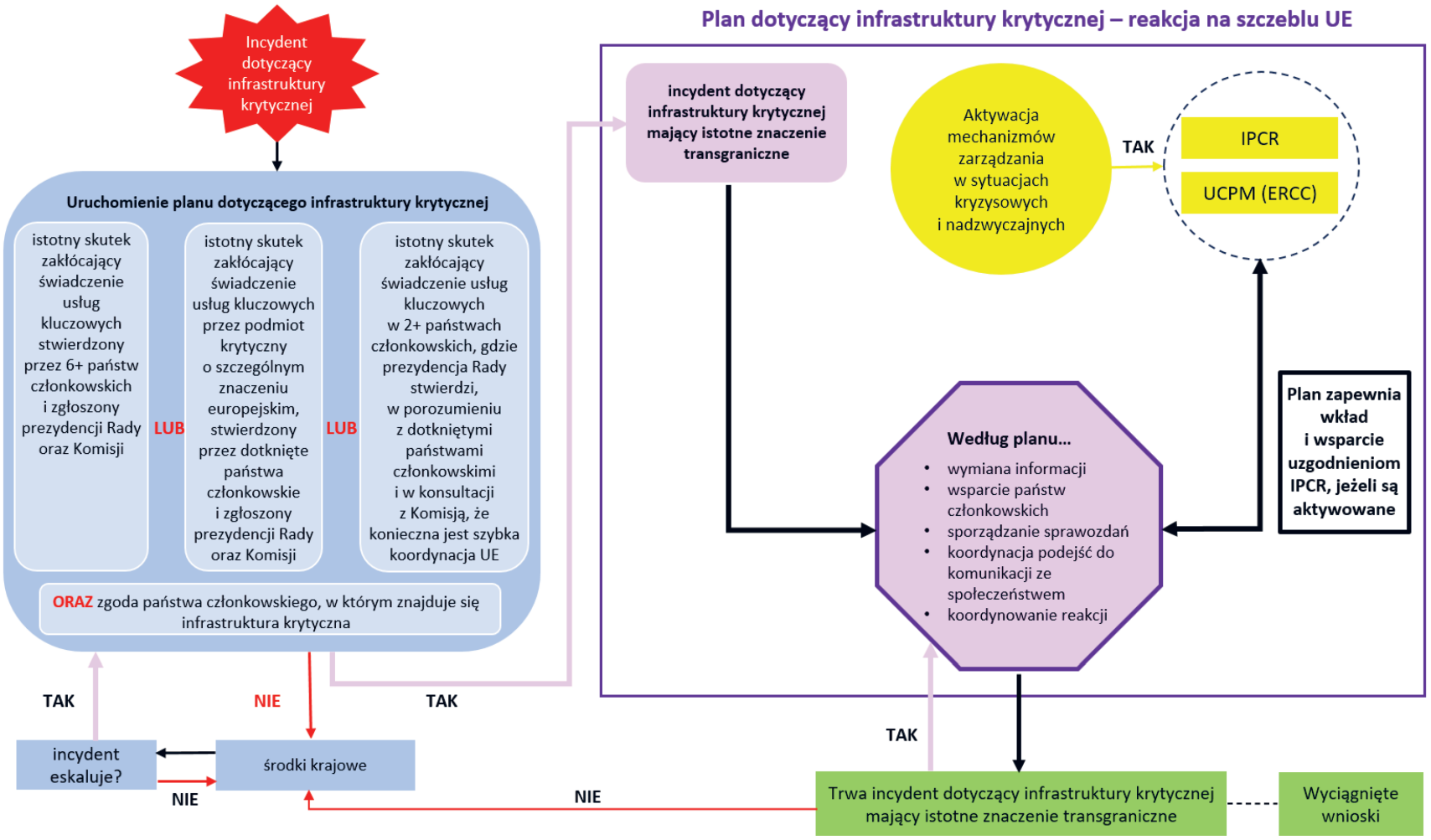
Państwa, których dotyczy incydent, mogą uruchomić UMOL, aby zwrócić się o wsparcie, a następnie ERCC podejmie prace z punktami kontaktowymi państw członkowskich zgodnie z przepisami prawnymi dotyczącymi UMOL w celu koordynowania udzielania wsparcia.

W ramach swoich odpowiednich mandatów i na stosowny wniosek Europol i inne odpowiednie agencje unijne mogą pomagać państwom członkowskim, których dotyczy incydent związany z infrastrukturą krytyczną mający istotne znaczenie transgraniczne, w prowadzeniu dochodzenia w sprawie incydentu.

b) Na szczeblu politycznym

Prezydencja Rady może rozważyć konieczność zwołania rozmów przy okrągłym stole IPCR, posiedzeń grup roboczych Rady, Coreperu, Rady w celu wymiany informacji na temat możliwego źródła i spodziewanych konsekwencji incydentu związanego z infrastrukturą krytyczną mającego istotne znaczenie transgraniczne dla państw członkowskich i Unii, w celu uzgodnienia wspólnych wytycznych oraz przyjęcia niezbędnych środków na potrzeby wsparcia państw członkowskich, których dotyczy dany incydent, i złagodzenia jego skutków. Sprawą może się też zająć Rada Europejska.

Schemat planu UE dotyczącego infrastruktury krytycznej



ELI: http://data.europa.eu/eli/C/2024/4371/oj