Rada
Unii Europejskiej

Bruksela, 9 grudnia 2022 r.
(OR. en)

15623/22

Międzyinstytucjonalny numer referencyjny:
2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	13713/22, 15454/22
Dotyczy:	ZALECENIE RADY w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej

Delegacje otrzymują w załączeniu zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej, w wersji przyjętej przez Radę na jej 3920. posiedzeniu, które odbyło się 8 grudnia 2022 r.

ZAŁĄCZNIK

ZALECENIE RADY (UE) 2022/...

z dnia...

w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej

(Tekst mający znaczenie dla EOG)

RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Aby możliwe było zapewnienie funkcjonowania rynku wewnętrznego, w interesie wszystkich państw członkowskich i Unii jako całości leży jasne wskazanie i ochrona odpowiedniej infrastruktury krytycznej zapewniającej w ramach tego rynku usługi kluczowe, zwłaszcza w kluczowych sektorach, takich jak energetyka, infrastruktura cyfrowa, transport i przestrzeń kosmiczna, a także wskazanie i ochrona infrastruktury krytycznej o istotnym znaczeniu transgranicznym[1], której zakłócenie mogłoby mieć znaczący wpływ na inne państwa członkowskie.

[1] Państwa członkowskie powinny ocenić to znaczenie transgraniczne zgodnie ze swoimi praktykami krajowymi i mogą to uczynić m.in. w oparciu o ocenę ryzyka oraz wpływ zdarzenia i jego charakter.

(2) Niniejsze zalecenie, które jest aktem niewiążącym, świadczy o politycznej woli państw członkowskich do wspólnego działania oraz o ich zaangażowaniu na rzecz zalecanych środków, uwypuklonych w pięciopunktowym planie przedstawionym przez przewodniczącą Komisji Europejskiej, przy pełnym poszanowaniu kompetencji państw członkowskich. Niniejsze zalecenie nie wpływa na ochronę podstawowych interesów bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności państw członkowskich i nie należy oczekiwać, że państwa członkowskie będą udzielać informacji ze szkodą dla tych interesów.

(3) Chociaż odpowiedzialność za zapewnienie bezpieczeństwa i świadczenie usług kluczowych przez infrastrukturę krytyczną spoczywa przede wszystkim na państwach członkowskich i ich operatorach infrastruktury krytycznej, zwiększona koordynacja na szczeblu Unii jest właściwa, zwłaszcza w świetle zmieniających się zagrożeń, takich jak rosyjska wojna napastnicza przeciwko Ukrainie i kampanie hybrydowe przeciwko państwom członkowskim, które to zagrożenia mogą mieć wpływ na kilka państw członkowskich jednocześnie lub wpływać na odporność i dobre funkcjonowanie unijnej gospodarki, rynku wewnętrznego i całego społeczeństwa. Szczególną uwagę należy zwrócić na infrastrukturę krytyczną poza terytorium państw członkowskich, taką jak podmorska infrastruktura krytyczna lub infrastruktura energii morskiej.

(4) W konkluzjach z 20 i 21 października 2022 r. Rada Europejska zdecydowanie potępiła akty sabotażu wymierzone w infrastrukturę krytyczną, jak np. te, których celem były gazociągi Nord Stream, wskazując na wolę Unii, by każde zamierzone zakłócanie funkcjonowania infrastruktury krytycznej lub inne działania hybrydowe spotkały się ze wspólną i zdecydowaną reakcją.

(5) W związku z szybko zmieniającym się krajobrazem zagrożeń należy priorytetowo przyjąć środki zwiększające odporność w kluczowych sektorach, takich jak energetyka, infrastruktura cyfrowa, transport i przestrzeń kosmiczna, i w innych odpowiednich sektorach wskazanych przez państwa członkowskie. Środki takie powinny koncentrować się na zwiększaniu odporności infrastruktury krytycznej, z uwzględnieniem odpowiednich rodzajów ryzyka, w szczególności efektów kaskadowych, zakłóceń w łańcuchu dostaw, zależności, skutków zmiany klimatu, niewiarygodnych sprzedawców i partnerów oraz zagrożeń i kampanii hybrydowych, w tym zagranicznych manipulacji informacjami i ingerencji w informacje. W przypadku krajowej infrastruktury krytycznej, z uwagi na możliwe konsekwencje, priorytetowo należy potraktować infrastrukturę krytyczną o istotnym znaczeniu transgranicznym. Zachęca się państwa członkowskie do zapewnienia takich środków zwiększających odporność – w stosownych przypadkach w trybie pilnym – przy jednoczesnym utrzymaniu podejścia określonego w zmieniających się ramach prawnych.

(6) Ochrona europejskiej infrastruktury krytycznej w sektorze energetycznym i transportowym jest obecnie regulowana dyrektywą Rady 2008/114/WE[2], a bezpieczeństwo sieci i systemów informatycznych w całej Unii z naciskiem na zagrożenia dla cyberbezpieczeństwa zapewnia dyrektywa Parlamentu Europejskiego i Rady 2016/1148[3]. W celu zapewnienia wyższego wspólnego poziomu odporności i ochrony infrastruktury krytycznej, cyberbezpieczeństwa i rynku finansowego obowiązujące ramy prawne są zmieniane i uzupełniane przez przyjęcie nowych przepisów mających zastosowanie do podmiotów krytycznych (dyrektywa CER), wzmocnionych przepisów dotyczących wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS 2) oraz nowych przepisów mających zastosowanie do operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA).

(7) Państwa członkowskie powinny, zgodnie z prawem unijnym i krajowym, wykorzystywać wszystkie dostępne narzędzia, aby poczynić postępy i przyczynić się do wzmocnienia odporności fizycznej i cyberodporności. W tym względzie infrastrukturę krytyczną należy rozumieć jako obejmującą odpowiednią infrastrukturę krytyczną wskazaną przez państwo członkowskie na szczeblu krajowym lub wyznaczoną jako europejska infrastruktura krytyczna na mocy dyrektywy 2008/114/WE, jak i podmioty krytyczne, które należy wskazać na mocy dyrektywy CER, lub, w stosownych przypadkach, podmioty objęte dyrektywą NIS 2. Pojęcie odporności należy rozumieć jako odnoszące się 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 poprzedniego stanu.

---

[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).

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

(8) Należy zgromadzić ekspertów krajowych w celu skoordynowania prac służących osiągnięciu wyższego wspólnego poziomu odporności i ochrony infrastruktury krytycznej, który ma zostać wprowadzony nowymi przepisami mającymi zastosowanie do podmiotów krytycznych. Takie skoordynowane prace umożliwiłyby współpracę między państwami członkowskimi i wymianę informacji dotyczących działań takich jak opracowywanie metod wskazywania usług kluczowych świadczonych przez infrastrukturę krytyczną. Komisja rozpoczęła już powoływanie tych ekspertów i ułatwianie ich prac, i zamierza kontynuować te działania. Po wejściu w życie dyrektywy CER i utworzeniu na podstawie tej dyrektywy Grupy ds. Odporności Podmiotów Krytycznych grupa ta powinna kontynuować wspomniane działania wstępne, zgodnie z powierzonymi jej zadaniami.

(9) Biorąc pod uwagę zmianę krajobrazu zagrożeń, należy dalej rozwijać możliwości przeprowadzania na szczeblu krajowym testów warunków skrajnych dotyczących infrastruktury krytycznej, ponieważ testy takie mogłyby być przydatne do zwiększenia odporności infrastruktury krytycznej. W odniesieniu do szczególnego znaczenia sektora energetycznego i ogólnounijnych skutków jego ewentualnych zakłóceń, najbardziej korzystne dla tego sektora byłoby przeprowadzenie testów warunków skrajnych w oparciu o wspólnie uzgodnione zasady. Takie testy wchodzą w zakres kompetencji państw członkowskich, które powinny zachęcać operatorów infrastruktury krytycznej do przeprowadzania takich testów, jeżeli zostaną one uznane za korzystne i zgodne z ich krajowymi ramami prawnymi, oraz wspierać operatorów w tym zakresie.

(10) Aby zapewnić skoordynowaną i skuteczną odpowiedź na obecne i przewidywane zagrożenia, zachęca się Komisję do udzielenia dodatkowego wsparcia państwom członkowskim, w szczególności poprzez dostarczanie odpowiednich informacji w formie briefingów, niewiążących podręczników i wytycznych. Europejska Służba Działań Zewnętrznych (ESDZ), w szczególności za pośrednictwem Centrum Analiz Wywiadowczych UE i jego Komórki ds. Syntezy Informacji o Zagrożeniach Hybrydowych, przy wsparciu Dyrekcji Wywiadu Sztabu Wojskowego UE w ramach pojedynczej komórki analiz wywiadowczych (SIAC), powinna zapewniać oceny zagrożeń. Wzywa się również Komisję, by we współpracy z państwami członkowskimi promowała wykorzystywanie projektów badawczych i innowacyjnych finansowanych przez Unię.

(11) Ze względu na rosnącą współzależność infrastruktury fizycznej i cyfrowej, szkodliwe działania w cyberprzestrzeni ukierunkowane na obszary krytyczne mogą powodować zakłócenia lub szkody w infrastrukturze fizycznej, a sabotaż infrastruktury fizycznej może sprawić, że niedostępne staną się usługi cyfrowe. Wzywa się państwa członkowskie do przyspieszenia prac przygotowawczych nad transpozycją i stosowaniem nowych ram prawnych mających zastosowanie do podmiotów krytycznych oraz wzmocnionych ram prawnych w dziedzinie cyberbezpieczeństwa, z wykorzystaniem przy tym – na jak najwcześniejszym etapie – doświadczeń zdobytych w ramach grupy współpracy ustanowionej dyrektywą (UE) 2016/1148 („grupa współpracy ds. bezpieczeństwa sieci i informacji”), z jednoczesnym uwzględnieniem terminów transpozycji, oraz tego, że takie prace przygotowawcze powinny przebiegać równolegle i w sposób spójny.

(12) Oprócz zwiększenia gotowości ważne jest też wzmocnienie zdolności do szybkiego i skutecznego reagowania na zakłócenia w świadczeniu usług kluczowych przez infrastrukturę krytyczną. W związku z tym w niniejszym zaleceniu przewidziano środki zarówno na szczeblu unijnym, jak i krajowym, w tym akcentując wspierającą rolę i wartość dodaną, jakie można uzyskać dzięki wprowadzeniu wzmocnionej współpracy i wymiany informacji w kontekście Unijnego Mechanizmu Ochrony Ludności (UMOL) ustanowionego decyzją Parlamentu Europejskiego i Rady nr 1313/2013/EU[4] oraz wykorzystaniu odpowiednich zasobów unijnego programu kosmicznego ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/696[5].

(13) Komisja, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa („wysoki przedstawiciel") oraz grupa współpracy ds. bezpieczeństwa sieci i informacji mają – we współpracy z odpowiednimi cywilnymi i wojskowymi organami i agencjami oraz istniejącymi sieciami, w tym europejską siecią organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) – przeprowadzić ocenę ryzyka i opracować scenariusze ryzyka. Ponadto w następstwie wspólnego ministerialnego wezwania z Nevers grupa współpracy ds. bezpieczeństwa sieci i informacji, przy wsparciu Komisji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), przeprowadza obecnie ocenę ryzyka. Te dwa działania będą spójne i skoordynowane z prowadzonymi obecnie przez Komisję i państwa członkowskie pracami na rzecz opracowania scenariuszy w ramach UMOL obejmujących zdarzenia związane z cyberbezpieczeństwem i ich rzeczywiste skutki. Aby zapewnić efektywność, skuteczność i spójność, a także należyte stosowanie niniejszego zalecenia, wyniki tych działań mają zostać odzwierciedlone na szczeblu krajowym.

---

4 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).

5 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).

(14) Aby w trybie natychmiastowym zwiększyć gotowość i zdolność do reagowania na cyberincydenty na dużą skalę, Komisja ustanowiła krótkoterminowy program wspierania państw członkowskich, przyznając ENISA dodatkowe środki finansowe. Oferowane usługi obejmują między innymi działania w zakresie gotowości, np. test penetracyjny podmiotów pozwalający zidentyfikować słabe punkty. Dzięki programowi mogą również wzrosnąć możliwości udzielania pomocy państwom członkowskim w przypadku wystąpienia cyberincydentu na dużą skalę mającego wpływ na podmioty krytyczne. Jest to pierwszy krok zgodny z konkluzjami Rady z dnia 23 maja 2022 r. w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni („konkluzje Rady w sprawie pozycji UE w kwestiach cyberprzestrzeni"), w których Rada zwróciła się do Komisji o przedstawienie wniosku w sprawie nowego funduszu reagowania kryzysowego w zakresie cyberbezpieczeństwa. Państwa członkowskie powinny w pełni wykorzystywać te możliwości, zgodnie z mającymi zastosowanie wymogami; zachęca się je też do kontynuowania prac w obszarze unijnego zarządzania kryzysami cyberbezpieczeństwa, w szczególności poprzez regularne monitorowanie i podsumowywanie postępów poczynionych we wdrażaniu planu działania w zakresie zarządzania kryzysami cyberbezpieczeństwa opracowanego niedawno przez Radę. Ten plan działania jest żyjącym dokumentem i w razie potrzeby powinien zostać ponownie przeanalizowany i zaktualizowany.

(15) Zasadnicze znaczenie dla globalnej i wewnątrzunijnej łączności mają globalne podmorskie kable telekomunikacyjne. Ze względu na znaczną długość takich kabli i ich położenie na dnie morskim niezwykle trudne jest wizualne monitorowanie większości podwodnych odcinków kabla. Wspólna jurysdykcja i inne kwestie dotyczące jurysdykcji w odniesieniu do takich kabli stanowią szczególny przypadek dla europejskiej i międzynarodowej współpracy w zakresie ochrony i odbudowy infrastruktury. Należy zatem uzupełnić bieżące i planowane oceny ryzyka dotyczące infrastruktur cyfrowych i fizycznych, od których zależą usługi cyfrowe, o szczególne oceny ryzyka i warianty środków ograniczających ryzyko dotyczących podmorskich kabli telekomunikacyjnych. Państwa członkowskie wzywają Komisję do przeprowadzenia badań w tym kierunku i przekazania państwom członkowskim swoich ustaleń.

(16) Na sektor energetyczny i transportowy mogą mieć również wpływ zagrożenia związane z infrastrukturą cyfrową, na przykład w odniesieniu do technologii energetycznych wykorzystujących elementy cyfrowe. Bezpieczeństwo powiązanych łańcuchów dostaw jest ważne dla ciągłości świadczenia usług kluczowych oraz dla strategicznej kontroli infrastruktury krytycznej w sektorze energetycznym. Okoliczności te należy uwzględnić przy podejmowaniu działań służących zwiększeniu odporności infrastruktury krytycznej zgodnie z niniejszym zaleceniem.

(17) Rosnące znaczenie infrastruktury kosmicznej, związanych z przestrzenią kosmiczną aktywów naziemnych, w tym obiektów produkcyjnych, i usług wykorzystujących instalacje w przestrzeni kosmicznej w kontekście działań związanych z bezpieczeństwem sprawia, że konieczne jest zapewnienie odporności i ochrony unijnych zasobów kosmicznych i powiązanych aktywów naziemnych oraz usług sektora kosmicznego w UE. Z tych samych powodów istotne jest również, w ramach niniejszego zalecenia, by w bardziej uporządkowany sposób wykorzystywać dane satelitarne i usługi oparte na tych danych dostarczanych przez systemy i programy kosmiczne do celów nadzoru, śledzenia i ochrony infrastruktury krytycznej w innych sektorach. Przy wdrażaniu niniejszego zalecenia należy wziąć pod uwagę odpowiednie działania w tym zakresie, które zostaną zaproponowane w przyszłej strategii kosmicznej UE na rzecz bezpieczeństwa i obrony.

(18) Konieczna jest także współpraca na szczeblu międzynarodowym, aby móc skutecznie przeciwdziałać zagrożeniom dla infrastruktury krytycznej, między innymi na wodach międzynarodowych. W związku z tym wzywa się państwa członkowskie do współpracy z Komisją i wysokim przedstawicielem w celu podjęcia określonych kroków służących osiągnięciu takiej współpracy, z uwzględnieniem faktu, że wszelkie takie kroki mogą być podejmowane wyłącznie w zgodzie z ich odnośnymi zadaniami i obowiązkami wynikającymi z prawa Unii, w szczególności z postanowieniami Traktatów dotyczącymi stosunków zewnętrznych.

(19) Jak określono w komunikacie z dnia 15 lutego 2022 r. pt. „Wkład Komisji w europejską obronność” w ramach wsparcia „Strategicznego kompasu na rzecz bezpieczeństwa i obrony – dla Unii Europejskiej, która chroni swoich obywateli, swoje wartości i interesy oraz przyczynia się do międzynarodowego pokoju i bezpieczeństwa”, Komisja – we współpracy z wysokim przedstawicielem i państwami członkowskimi – oceni wyjściowe poziomy odporności sektorowej na zagrożenia hybrydowe, wskazując luki i potrzeby oraz działania służące zaradzeniu im do 2023 r. Inicjatywa ta powinna pomóc w realizacji prac prowadzonych w ramach niniejszego zalecenia, przyczyniając się do usprawnienia wymiany informacji i koordynacji działań w zakresie dalszego wzmacniania odporności, w tym odporności infrastruktury krytycznej.

(20) W strategii UE w zakresie bezpieczeństwa morskiego z 2014 r. i związanym z nią zmienionym planie działania wezwano do zwiększenia ochrony krytycznej infrastruktury morskiej, w tym podwodnej, a w szczególności morskiej infrastruktury transportowej, energetycznej i telekomunikacyjnej, między innymi poprzez poprawę orientacji w obszarze morskim dzięki wzmocnionej interoperacyjności i usprawnionej wymianie informacji (obowiązkowej i dobrowolnej). Ta strategia i ten plan działania są obecnie aktualizowane i będą obejmować wzmożone działania mające na celu ochronę krytycznej infrastruktury morskiej. Działania te powinny uzupełniać niniejsze zalecenie.

(21) Wzmocnienie odporności infrastruktury krytycznej przyczynia się do szerzej zakrojonych wysiłków na rzecz przeciwdziałania hybrydowym zagrożeniom i kampaniom przeciwko Unii i jej państwom członkowskim. Niniejsze zalecenie opiera się na wspólnym komunikacie Parlamentu Europejskiego i Rady pt. „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej”. Działanie 1 określone w tych wspólnych ramach, a mianowicie badanie zagrożeń hybrydowych, odgrywa kluczową rolę w identyfikowaniu słabych punktów, które mogą mieć wpływ na krajowe i ogólnoeuropejskie struktury i sieci. Ponadto wdrożenie konkluzji Rady z 21 czerwca 2022 r. w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe zapewni bardziej zdecydowane skoordynowane działania dzięki zastosowaniu unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym we wszystkich odnośnych dziedzinach.

PRZYJMUJE NINIEJSZE ZALECENIE:

ROZDZIAŁ I: CEL, ZAKRES STOSOWANIA I USTALANIE PRIORYTETÓW

1) W niniejszym zaleceniu określono szereg ukierunkowanych działań na szczeblu unijnym i krajowym mających na celu wspieranie i zwiększanie odporności infrastruktury krytycznej, na zasadzie dobrowolności, ze szczególnym uwzględnieniem infrastruktury krytycznej o istotnym znaczeniu transgranicznym i we wskazanych kluczowych sektorach, takich jak energetyka, infrastruktura cyfrowa, transport i przestrzeń kosmiczna. Takie ukierunkowane działania obejmują zwiększoną gotowość, wzmocnioną reakcję i współpracę międzynarodową.

2) Udostępnione, by osiągnąć cele niniejszego zalecenia, informacje, które mają charakter poufny zgodnie z przepisami unijnymi i krajowymi, a także przepisami dotyczącymi tajemnicy przedsiębiorstwa, powinny podlegać wymianie z Komisją i innymi stosownymi organami tylko wtedy, gdy wymiana ta jest niezbędna do należytego stosowania niniejszego zalecenia. Niniejsze zalecenie nie wpływa na ochronę podstawowych interesów bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności państw członkowskich i nie należy oczekiwać, że państwa członkowskie będą udzielać informacji ze szkodą dla tych interesów.

ROZDZIAŁ II: WZMOCNIONA GOTOWOŚĆ

Działania na szczeblu państw członkowskich

3) Przy aktualizowaniu swoich ocen ryzyka lub istniejących równoważnych analiz państwa członkowskie powinny rozważyć podejście uwzględniające wszystkie zagrożenia, zgodnie ze zmieniającym się charakterem obecnych zagrożeń dla ich infrastruktury krytycznej, zwłaszcza we wskazanych kluczowych sektorach oraz, w miarę możliwości, we wszystkich sektorach objętych przyszłymi nowymi ramami prawnymi mającymi zastosowanie do podmiotów krytycznych.

4) Wzywa się państwa członkowskie do przyspieszenia prac przygotowawczych i przyjęcia, w miarę możliwości, środków zwiększających odporność, zgodnie z przyszłymi ramami prawnymi mającymi zastosowanie do podmiotów krytycznych, ze szczególnym uwzględnieniem współpracy i wymiany odpowiednich informacji między państwami członkowskimi i z Komisją, wskazywania podmiotów krytycznych o istotnym znaczeniu transgranicznym oraz zwiększania wsparcia dla zidentyfikowanych podmiotów krytycznych w celu poprawy ich odporności.

5) Państwa członkowskie powinny wspierać szkolenia ekspertów, ćwiczenia oraz wymianę najlepszych praktyk i doświadczeń między nimi. Państwa członkowskie powinny zachęcać ekspertów do uczestnictwa w istniejących platformach szkoleniowych, zarówno krajowych, jak i międzynarodowych, na przykład w ramach UMOL.

6) Państwa członkowskie powinny zachęcać i wspierać operatorów infrastruktury krytycznej przynajmniej w sektorze energetycznym, aby przeprowadzali testy warunków skrajnych zgodnie z zasadami uzgodnionymi wspólnie na szczeblu Unii, jeżeli jest to korzystne. Testy warunków skrajnych powinny oceniać odporność infrastruktury krytycznej na zagrożenia typu antagonistycznego spowodowane przez człowieka. W związku z tym państwa członkowskie powinny dążyć do jak najszybszego – nie później niż do końca pierwszego kwartału 2023 r. – wskazania odpowiedniej infrastruktury krytycznej, która ma zostać poddana takim testom, i do przeprowadzenia konsultacji z jej operatorami. Ponadto państwa członkowskie powinny wspierać operatorów tej infrastruktury krytycznej, aby przeprowadzili wspomniane testy jak najszybciej, mając na celu ich ukończenie do końca 2023 r., zgodnie z prawem krajowym. Rada zamierza ocenić sytuację w zakresie testów warunków skrajnych do końca kwietnia 2023 r.

7) Ze względu na szybko zmieniające się zagrożenia dla infrastruktury krytycznej utrzymanie wysokiego poziomu jej ochrony ma kluczowe znaczenie. Zachęca się państwa członkowskie do przeznaczenia wystarczających zasobów finansowych na wzmocnienie zdolności swoich odpowiednich organów krajowych i do wspierania ich, aby możliwe było zwiększenie odporności infrastruktury krytycznej. Zachęca się również państwa członkowskie do przeznaczenia wystarczających zasobów finansowych dla organów odpowiedzialnych za zarządzanie cyberincydentami na dużą skalę, wspierania tych organów oraz zapewnienia, aby ich zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) i właściwe organy były w pełni wykorzystywane w ramach, odpowiednio, sieci CSIRT i EU-CyCLONe.

8) Wzywa się państwa członkowskie, by zgodnie z mającymi zastosowanie wymogami wykorzystywały potencjalne możliwości finansowania na szczeblu unijnym i krajowym w celu zwiększenia odporności infrastruktury krytycznej w Unii na własne potrzeby, a także by zachęcały operatorów infrastruktury krytycznej do korzystania z takich możliwości finansowania, w tym na przykład z sieci transeuropejskich, w odniesieniu do pełnego zakresu poważnych zagrożeń, zwłaszcza w ramach programów finansowanych z Funduszu Bezpieczeństwa Wewnętrznego ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/1149[6], Europejskiego Funduszu Rozwoju Regionalnego ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1301/2013[7], UMOL i planu Komisji REPowerEU. Państwa członkowskie zachęca się również do jak najlepszego wykorzystania wyników odpowiednich projektów w ramach programów badawczych, takich jak „Horyzont Europa” ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/695[8].

---

6 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1149 z dnia 7 lipca 2021 r. ustanawiające Fundusz Bezpieczeństwa Wewnętrznego (Dz.U. L 251 z 15.7.2021, s. 94).

7 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1301/2013 z dnia 17 grudnia 2013 r. w sprawie Europejskiego Funduszu Rozwoju Regionalnego i przepisów szczególnych dotyczących celu „Inwestycje na rzecz wzrostu i zatrudnienia” oraz w sprawie uchylenia rozporządzenia (WE) nr 1080/2006 (Dz.U. L 347 z 20.12.2013, s. 289).

8 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/695 z dnia 28 kwietnia 2021 r. ustanawiające program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa” oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie oraz uchylające rozporządzenia (UE) nr 1290/2013 i (UE) nr 1291/2013 (Dz.U. L 170 z 12.5.2021, s. 1).

9) Jeżeli chodzi o infrastrukturę łączności i sieci w Unii, wzywa się grupę współpracy ds. bezpieczeństwa sieci i informacji – działającą zgodnie z art. 11 dyrektywy (UE) 2016/1148 – do przyspieszenia bieżących, opartych na wspólnym ministerialnym wezwaniu z Nevers, prac nad ukierunkowaną oceną ryzyka i jak najszybszego przedstawienia pierwszych zaleceń. Ta ocena ryzyka powinna być źródłem informacji na potrzeby trwającej międzysektorowej oceny ryzyka i scenariuszy ryzyka w cyberprzestrzeni, o które Rada zwróciła się w konkluzjach w sprawie rozwijania pozycji UE w kwestiach cyberprzestrzeni. Ponadto prace te należy prowadzić w taki sposób, by zapewnić spójność i komplementarność z pracami prowadzonymi przez grupę współpracy ds. bezpieczeństwa sieci i informacji w obszarze działań dotyczącym bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych, a także przez inne odpowiednie grupy.

10) Grupa współpracy ds. bezpieczeństwa sieci i informacji jest również proszona, by przy wsparciu Komisji i ENISA kontynuowała prace nad bezpieczeństwem infrastruktury cyfrowej, w tym w odniesieniu do infrastruktury podmorskiej, a mianowicie podmorskich kabli telekomunikacyjnych. Zachęca się ją również do rozpoczęcia prac dotyczących sektora kosmicznego, w tym, w razie potrzeby, poprzez przygotowanie wytycznych politycznych i metod zarządzania ryzykiem w cyberprzestrzeni w oparciu o podejście uwzględniające wszystkie zagrożenia i podejście oparte na analizie ryzyka dla operatorów w sektorze kosmicznym, mające na celu zwiększenie odporności infrastruktury naziemnej wspierającej świadczenie usług w przestrzeni kosmicznej.

11) Państwa członkowskie powinny również w pełni korzystać z usług w zakresie gotowości do reagowania w obszarze cyberbezpieczeństwa oferowanych w ramach realizowanego przez Komisję krótkoterminowego programu wsparcia wdrażanego wraz z ENISA, na przykład z testowania penetracyjnego, które pozwala identyfikować słabe punkty; w tym kontekście zachęca się państwa członkowskie, by priorytetowo traktowały podmioty obsługujące infrastrukturę krytyczną w sektorach energetycznym i transportowym oraz w sektorze infrastruktury cyfrowej.

12) Państwa członkowskie powinny w pełni wykorzystywać Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC). Państwa członkowskie powinny zachęcać swoje krajowe ośrodki koordynacji do proaktywnej współpracy z członkami społeczności zajmującej się cyberbezpieczeństwem w celu budowania zdolności na szczeblu unijnym i krajowym, by lepiej wspierać operatorów usług kluczowych.

13) Ważne jest, aby państwa członkowskie w pełni wdrożyły środki zalecane we wspólnym unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, a w szczególności aby wprowadziły ograniczenia wobec dostawców wysokiego ryzyka, zważywszy, że strata czasu może zwiększyć podatność unijnych sieci na zagrożenia; państwa członkowskie powinny również wzmocnić fizyczną i niefizyczną ochronę krytycznych i wrażliwych części sieci 5G, w tym poprzez rygorystyczne kontrole dostępu. Państwa członkowskie powinny ponadto we współpracy z Komisją ocenić konieczność podjęcia działań uzupełniających, aby zapewnić spójny poziom bezpieczeństwa i odporności sieci 5G.

14) Państwa członkowskie wraz z Komisją i ENISA powinny skupić się na wdrażaniu konkluzji Rady z dnia 17 października 2022 r. w sprawie bezpieczeństwa łańcucha dostaw ICT.

15) Państwa członkowskie powinny uwzględnić przyszły kodeks sieci dotyczący aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej [...], opierając się przy tym na doświadczeniach zdobytych przy wdrażaniu dyrektywy (UE) 2016/1148 oraz na odpowiednich wytycznych opracowanych przez grupę współpracy ds. bezpieczeństwa sieci i informacji, w szczególności na przygotowanym przez nią dokumencie referencyjnym w sprawie środków bezpieczeństwa dla operatorów usług kluczowych.

16) Państwa członkowskie powinny rozwijać wykorzystanie programu Copernicus oraz systemu Galileo i europejskiego systemu wspomagania satelitarnego (EGNOS) do celów nadzoru, by dzielić się odpowiednimi informacjami z ekspertami zgromadzonymi zgodnie z pkt 15. Należy efektywnie wykorzystać możliwości oferowane przez unijną rządową łączność satelitarną (Govsatcom) w ramach unijnego programu kosmicznego w celu monitorowania infrastruktury krytycznej i wspierania przewidywania kryzysów i reagowania na nie.

Działania na szczeblu Unii

17) Należy wzmocnić dialog i współpracę między wyznaczonymi ekspertami państw członkowskich oraz z Komisją, aby zwiększyć fizyczną odporność infrastruktury krytycznej, w szczególności poprzez:

a) wkład w przygotowanie, opracowanie i promowanie wspólnych dobrowolnych narzędzi – w tym metod i scenariuszy ryzyka – mających pomóc państwom członkowskim w zwiększeniu takiej odporności;

b) wspieranie państw członkowskich we wdrażaniu nowych ram prawnych mających zastosowanie do podmiotów krytycznych, w tym poprzez zachęcanie Komisji do terminowego przyjęcia aktu delegowanego;

c) wspieranie przeprowadzania testów warunków skrajnych, o których mowa w pkt 6, w oparciu o wspólne zasady, począwszy od takich testów, które koncentrują się na zagrożeniach o charakterze antagonistycznym spowodowanych przez człowieka w sektorze energetycznym, a następnie w innych kluczowych sektorach, a także wspieranie przeprowadzania takich testów warunków skrajnych i doradzanie w tym zakresie, na wniosek państwa członkowskiego;

d) wykorzystanie wszelkich bezpiecznych platform – po ustanowieniu przez Komisję – w celu gromadzenia, podsumowywania i wymiany, na zasadzie dobrowolności, najlepszych praktyk, wniosków wyciągniętych z doświadczeń krajowych i innych informacji dotyczących takiej odporności.

W pracach wyznaczonych ekspertów należy zwracać szczególną uwagę na zależności międzysektorowe i infrastrukturę krytyczną o istotnym znaczeniu transgranicznym; w stosownych przypadkach Rada i Komisja powinny kontynuować te prace.

18) Państwa członkowskie zachęca się do korzystania z wszelkiego wsparcia, jakie oferuje Komisja, poprzez na przykład opracowywanie podręczników i wytycznych, takich jak podręcznik dotyczący ochrony infrastruktury krytycznej i przestrzeni publicznej przed systemami bezzałogowych statków powietrznych, a także do korzystania z narzędzi oceny ryzyka. Wzywa się ESDZ, by – w szczególności poprzez swoje Centrum Analiz Wywiadowczych UE i Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych, przy wsparciu ze strony Dyrekcji Wywiadu Sztabu Wojskowego UE w ramach SIAC – prowadziła briefingi na temat zagrożeń dla infrastruktury krytycznej w Unii w celu poprawy orientacji sytuacyjnej.

19) Państwa członkowskie powinny wspierać działania podejmowane przez Komisję w celu wykorzystania wyników projektów dotyczących odporności infrastruktury krytycznej, które są finansowane z unijnych programów w zakresie badań naukowych i innowacji. Rada przyjmuje do wiadomości, że Komisja zamierza zwiększyć finansowanie odporności takiej infrastruktury, wykorzystując budżet przydzielony na program „Horyzont Europa” w wieloletnich ramach finansowych na lata 2021–2027, bez szkody dla finansowania pozostałych projektów w dziedzinie badań naukowych i innowacji związanych z bezpieczeństwem cywilnym w ramach programu „Horyzont Europa”.

20) Ze względu na zadania określone w konkluzjach Rady w sprawie rozwijania pozycji UE w kwestiach cyberbezpieczeństwa wzywa się Komisję, wysokiego przedstawiciela oraz grupę współpracy ds. bezpieczeństwa sieci i informacji, aby – zgodnie z ich odpowiednimi zadaniami i obowiązkami wynikającymi z prawa Unii – intensywniej współpracowali z odpowiednimi sieciami oraz organami i agencjami cywilnymi i wojskowymi nad przeprowadzaniem ocen ryzyka i tworzeniem scenariuszy ryzyka w cyberprzestrzeni, uwzględniając w szczególności znaczenie infrastruktury energetycznej, cyfrowej, transportowej i kosmicznej oraz współzależności między sektorami i państwami członkowskimi. W działaniu tym należy wziąć po uwagę powiązane ryzyko dla infrastruktury, od której sektory te zależą. O ile jest to korzystne, oceny ryzyka i scenariusze ryzyka można przeprowadzać regularnie; powinny one uzupełniać istniejące lub planowane oceny ryzyka w tych sektorach, opierać się na nich, lecz unikać ich powielania; należy je ponadto wykorzystywać jako wkład w dyskusje na temat sposobów wzmacniania ogólnej odporności podmiotów obsługujących infrastrukturę krytyczną i eliminowania słabych punktów.

21) Wzywa się Komisję do przyspieszenia – zgodnie z jej odpowiednimi zadaniami w ramach zarządzania kryzysami cyberbezpieczeństwa– realizacji działań dotyczących wspierania państw członkowskich w osiąganiu gotowości i w reagowaniu na cyberincydenty na dużą skalę, a w szczególności do:

a) przeprowadzenia, w uzupełnieniu odpowiednich ocen ryzyka w kontekście bezpieczeństwa sieci i informacji, kompleksowego badania[9] oceniającego infrastrukturę podmorską, a mianowicie podmorskie kable telekomunikacyjne, które łączą państwa członkowskie oraz Europę z resztą świata, i przekazania ustaleń z tego badania państwom członkowskim;

b) wspierania państw członkowskich oraz instytucji, organów i agencji Unii w osiąganiu gotowości na wypadek wystąpienia cyberincydentów na dużą skalę lub poważnych incydentów oraz w reagowaniu na nie, zgodnie ze wzmocnionymi ramami prawnymi dotyczącymi cyberbezpieczeństwa i innymi odpowiednimi mającymi zastosowanie przepisami[10];

c) przyspieszenia prac nad główną koncepcją funduszu reagowania kryzysowego w zakresie cyberbezpieczeństwa poprzez odpowiednią dyskusję z państwami członkowskimi.

22) Zachęca się Komisję do: intensywniejszych prac nad ukierunkowanymi na przyszłość działaniami przygotowawczymi, w tym we współpracy z państwami członkowskimi na podstawie art. 6 i 10 decyzji 1313/2013/UE, oraz w formie planowania ewentualnościowego celem wsparcia Centrum Koordynacji Reagowania Kryzysowego (ERCC) w osiągnięciu gotowości operacyjnej i w reagowaniu na zakłócenia infrastruktury krytycznej; do zwiększenia inwestycji w podejścia zapobiegawcze i gotowość ludności oraz zwiększenia wsparcia związanego z budowaniem zdolności w ramach unijnej sieci wiedzy w zakresie ochrony ludności.

---

9 Badanie to powinno obejmować mapowanie jej zdolności i redundancji, podatności na zagrożenia, zagrożeń i ryzyka dla dostępności usług, wpływu awarii (transatlantyckich) kabli podmorskich na państwa członkowskie i Unię jako całość oraz na ograniczanie ryzyka, przy jednoczesnym uwzględnieniu wrażliwości takich informacji i potrzeby ich ochrony.

10 Szczególną uwagę należy również zwrócić na wszystkie działania przygotowujące do skutecznej skoordynowanej reakcji na szczeblu Unii w przypadku poważnego transgranicznego cyberincydentu lub powiązanego zagrożenia, które mogłyby mieć systemowy wpływ na sektor finansowy Unii, zgodnie z nowymi ramami prawnymi dotyczącymi operacyjnej odporności cyfrowej.

23) Komisja powinna promować wykorzystanie unijnych zasobów nadzoru (Copernicus, Galileo i EGNOS) do wspierania państw członkowskich w monitorowaniu infrastruktury krytycznej i, w stosownych przypadkach, jej bezpośredniego sąsiedztwa, a także do wspierania innych opcji nadzoru przewidzianych w programie kosmicznym Unii, takich jak ramy dotyczące świadomości sytuacyjnej w przestrzeni kosmicznej oraz unijne ramy obserwacji i śledzenia obiektów kosmicznych.

24) Wzywa się agencje i inne właściwe organy Unii – stosownie do przypadku i zgodnie z ich odpowiednimi mandatami – do udzielania wsparcia w kwestiach związanych z odpornością infrastruktury krytycznej, w szczególności w następujący sposób:

a) Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) – wsparcie w gromadzeniu informacji, analizie kryminalnej i wsparciu dochodzeniowym na rzecz transgranicznych działań organów ścigania; oraz, w razie potrzeby i w stosownych przypadkach, dzieleniu się wynikami z państwami członkowskimi;

b) Europejska Agencja Bezpieczeństwa Morskiego (EMSA) – wsparcie w obszarze ochrony i bezpieczeństwa sektora morskiego w Unii, w tym usług nadzoru morskiego odnoszących się do kwestii związanych z ochroną na morzu i bezpieczeństwem morskim;

c) Agencja Unii Europejskiej ds. Programu Kosmicznego (EUSPA) i Centrum Satelitarne UE (SatCen) – możliwość wsparcia poprzez operacje w ramach unijnego programu kosmicznego;

d) ECCC – wsparcie w odniesieniu do działań związanych z cyberbezpieczeństwem, również we współpracy z ENISA, możliwość wspierania innowacji i polityki przemysłowej w dziedzinie cyberbezpieczeństwa.

ROZDZIAŁ III: WZMOCNIONA REAKCJA

Działania na szczeblu państw członkowskich

25) Wzywa się państwa członkowskie, by:

a) nadal wzajemnie koordynowały swoją reakcję, w stosownych przypadkach, i miały ogólny obraz międzysektorowych reakcji na znaczące zakłócenia w świadczeniu usług kluczowych przez infrastrukturę krytyczną. Można by to przewidzieć w ramach: przyszłego planu działania dotyczącego skoordynowanej reakcji na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym; istniejących uzgodnień dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) na potrzeby koordynacji reagowania na szczeblu politycznym w odniesieniu do infrastruktury krytycznej o znaczeniu transgranicznym; planu działania w sprawie cyberincydentów i kryzysów cyberbezpieczeństwa na dużą skalę na podstawie zalecenia Komisji (UE) 2017/1584[11]; EU-CyCLONe; w ramach skoordynowanej reakcji UE na kampanie hybrydowe oraz unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym w przypadku takich zagrożeń i kampanii hybrydowych; oraz w ramach systemu wczesnego ostrzegania w przypadku dezinformacji;

b) zintensyfikowały wymianę informacji z ERCC na szczeblu operacyjnym w ramach UMOL, aby usprawnić wczesne ostrzeganie i skoordynować reakcję w ramach UMOL w przypadku zakłóceń funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym, zapewniając tym samym w razie potrzeby szybszą reakcję wspomaganą przez Unię;

c) zwiększały swoją gotowość do reagowania – w stosownych przypadkach, za pomocą istniejących narzędzi lub narzędzi, które mają zostać opracowane – na takie poważne zakłócenia, o których mowa w lit. a);

[11] 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).

d) angażowały się w dalszy rozwój odpowiednich zdolności reagowania w ramach europejskiej puli ochrony ludności (ECPP) i rescEU;

e) zachęcały operatorów infrastruktury krytycznej i odpowiednie organy krajowe do zwiększania ich zdolności do szybkiego przywracania podstawowego funkcjonowania usług kluczowych świadczonych przez tych operatorów infrastruktury krytycznej;

f) zachęcały operatorów infrastruktury krytycznej, by przy odbudowie ich infrastruktury krytycznej dążyli do tego, by była jak najbardziej odporna – z uwzględnieniem proporcjonalności środków w odniesieniu do oceny ryzyka i kosztów – na pełen zakres poważnych zagrożeń, które mogą się do niej odnosić, w tym w przypadku niekorzystnych scenariuszy klimatycznych.

26) Wzywa się państwa członkowskie do przyspieszenia – w miarę możliwości – prac przygotowawczych, zgodnie ze wzmocnionymi ramami prawnymi dotyczącymi cyberbezpieczeństwa, poprzez zwiększenie zdolności krajowych CSIRT w związku z nowymi zadaniami tych zespołów oraz większą liczbą podmiotów reprezentujących nowe sektory, terminowy przegląd i terminową aktualizację ich strategii cyberbezpieczeństwa oraz jak najszybsze przyjęcie krajowych planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, o ile plany takie jeszcze nie istnieją.

27) Wzywa się państwa członkowskie do rozważenia, na szczeblu krajowym, najodpowiedniejszych środków zapewniających, aby odpowiednie zainteresowane strony były świadome potrzeby zwiększenia odporności infrastruktury krytycznej poprzez współpracę z zaufanymi sprzedawcami i partnerami. Ważne jest inwestowanie w dodatkową przepustowość, zwłaszcza w sektorach, w których obecna infrastruktura znajduje się na końcu okresu eksploatacji, jak ma to miejsce np. w przypadku podmorskiej infrastruktury kabli telekomunikacyjnych, aby móc zapewnić ciągłość świadczenia usług kluczowych w przypadku zakłóceń oraz zmniejszyć niepożądane zależności.

28) Zachęca się państwa członkowskie do zwracania uwagi na proaktywną komunikację strategiczną na szczeblu krajowym w kontekście przeciwdziałania zagrożeniom i kampaniom hybrydowym oraz z uwagi na potencjał, jaki przeciwnicy mogą starać się angażować w zagraniczne manipulacje informacjami i ingerencję w informacje poprzez kształtowanie narracji wokół incydentów wymierzonych w infrastrukturę krytyczną.

Działania na szczeblu Unii

29) Wzywa się Komisję do ścisłej współpracy z państwami członkowskimi nad dalszym rozwojem odpowiednich organów, instrumentów i zdolności reagowania z myślą o zwiększeniu gotowości operacyjnej do radzenia sobie z natychmiastowymi i pośrednimi skutkami znaczących zakłóceń w świadczeniu usług kluczowych przez infrastrukturę krytyczną, w szczególności chodzi o ekspertów i zasoby dostępne poprzez ECPP i rescEU w ramach UMOL lub przyszłych zespołów szybkiego reagowania na zagrożenia hybrydowe.

30) Zważywszy na zmieniający się krajobraz zagrożeń, Komisję – we współpracy z państwami członkowskimi – wzywa się w kontekście UMOL do:

a) stałej analizy i testowania adekwatności i gotowości operacyjnej istniejących zdolności reagowania;

b) regularnego monitorowania i wskazywania potencjalnie znaczących luk w zdolnościach reagowania w ramach zdolności ECPP i rescEU;

c) dalszego pogłębiania współpracy międzysektorowej, aby zadbać o odpowiednią reakcję na szczeblu Unii, oraz organizowania regularnych szkoleń lub ćwiczeń w celu testowania takiej współpracy przy udziale co najmniej jednego z państw członkowskich;

d) dalszego rozwijania ERCC jako międzysektorowego centrum reagowania na sytuacje nadzwyczajne na szczeblu Unii służącego koordynacji wsparcia dla państw członkowskich dotkniętych sytuacją nadzwyczajną.

31) Rada jest zdecydowana rozpocząć prace zmierzające do zatwierdzenia planu działania dotyczącego skoordynowanej reakcji na zakłócenia funkcjonowania infrastruktury krytycznej o istotnym znaczeniu transgranicznym, w którym opisane i określone zostaną cele i sposoby współpracy między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii w zakresie reagowania na incydenty wymierzone w taką infrastrukturę krytyczną. Rada oczekuje przedstawienia przez Komisję projektu takiego planu działania na podstawie wsparcia i uwag odpowiednich agencji unijnych. Ten plan działania powinien być w pełni spójny i interoperacyjny ze zmienionym unijnym protokołem operacyjnym do celów przeciwdziałania zagrożeniom hybrydowym („unijny podręcznik taktyczny") oraz uwzględniać istniejący plan skoordynowanego reagowania na wypadek wystąpienia transgranicznych cyberincydentów na dużą skalę i cyberkryzysów[12] i mandat EU CyCLONe określony w dyrektywie NIS 2, a także powinien unikać powielania struktur i działań. W celu koordynowania reakcji plan działania powinien w pełni uwzględniać istniejące uzgodnienia IPCR.

[12] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

32) Wzywa się Komisję do prowadzenia z odpowiednimi zainteresowanymi stronami i ekspertami konsultacji na temat właściwych środków dotyczących ewentualnych znaczących incydentów związanych z infrastrukturą podmorską, które to środki mają być przedstawione wraz z badaniem podsumowującym, o którym mowa w pkt 20 lit. a), a także do dalszego opracowywania planów ewentualnościowych, scenariuszy ryzyka oraz unijnych celów w zakresie odporności na klęski i katastrofy przewidzianych w decyzji nr 1313/2013/UE.

ROZDZIAŁ IV: WSPÓŁPRACA MIĘDZYNARODOWA

Działania na szczeblu państw członkowskich

33) Państwa członkowskie powinny współpracować, w stosownych przypadkach i zgodnie z prawem Unii, z odpowiednimi państwami trzecimi w zakresie odporności infrastruktury krytycznej o istotnym znaczeniu transgranicznym.

34) Zachęca się państwa członkowskie do współpracy z Komisją i wysokim przedstawicielem w celu skutecznego przeciwdziałania zagrożeniom dla infrastruktury krytycznej na wodach międzynarodowych.

35) Wzywa się państwa członkowskie, by – we współpracy z Komisją i wysokim przedstawicielem – przyczyniły się do szybszego opracowania i wdrożenia unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym i wytycznych wykonawczych, o których mowa w konkluzjach Rady z dnia 21 czerwca 2022 r. w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe, a następnie korzystały z takich narzędzi i wytycznych, by zapewnić pełną skuteczność ram skoordynowanej reakcji UE na kampanie hybrydowe, w szczególności na etapie rozważania i przygotowywania kompleksowych i skoordynowanych reakcji Unii na kampanie hybrydowe i zagrożenia hybrydowe, w tym te wymierzone przeciwko operatorom infrastruktury krytycznej.

Działania na szczeblu Unii

36) Wzywa się Komisję i wysokiego przedstawiciela do wspierania – w stosownych przypadkach i zgodnie ze swoimi odpowiednimi zadaniami i obowiązkami wynikającymi z prawa Unii – odpowiednich państw trzecich w zwiększaniu odporności infrastruktury krytycznej na ich terytorium, a w szczególności infrastruktury krytycznej, która jest fizycznie połączona z ich terytorium oraz z terytorium jednego z państw członkowskich.

37) Komisja i wysoki przedstawiciel wzmocnią – zgodnie ze swoimi odpowiednimi zadaniami i obowiązkami wynikającymi z prawa Unii – koordynację z NATO w zakresie odporności infrastruktury krytycznej będącej przedmiotem wspólnego zainteresowania poprzez zorganizowany dialog UE–NATO na temat odporności, przy pełnym poszanowaniu kompetencji Unii i państw członkowskich zgodnie z Traktatami i kluczowych zasad regulujących współpracę UE–NATO uzgodnionych przez Radę Europejską, w szczególności w zakresie wzajemności, inkluzywności i autonomii decyzyjnej. W tym kontekście współpraca ta będzie kontynuowana w ramach zorganizowanego dialogu UE–NATO na temat odporności, wbudowanego w istniejący mechanizm kontaktów między pracownikami obu organizacji służący wdrażaniu wspólnych deklaracji, przy jednoczesnym zapewnieniu pełnej przejrzystości i zaangażowania wszystkich państw członkowskich.

38) Wzywa się Komisję do rozważenia – w razie potrzeby i w stosownych przypadkach – udziału przedstawicieli odpowiednich państw trzecich w ramach współpracy i wymiany informacji między państwami członkowskimi w dziedzinie odporności infrastruktury krytycznej, która jest fizycznie połączona z terytorium jednego z państw członkowskich i terytorium państwa trzeciego.

Sporządzono w … dnia …

W imieniu Rady

Przewodniczący / Przewodnicząca