Rada
Unii Europejskiej

Bruksela, 6 czerwca 2025 r.
(OR. en)

9794/25

Międzyinstytucjonalny numer referencyjny:
2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	6 czerwca 2025 r.
Do:	Delegacje
Dotyczy:	Zalecenie Rady w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami – Zalecenie Rady zatwierdzone przez Radę na posiedzeniu 6 czerwca 2025 r.

Delegacje otrzymują w załączeniu zalecenie Rady w wersji zatwierdzonej przez Radę na posiedzeniu 6 czerwca 2025 r.

ZAŁĄCZNIK

ZALECENIE RADY

w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami

RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Technologia cyfrowa i globalna łączność są podstawą wzrostu gospodarczego, konkurencyjności i transformacji infrastruktury krytycznej Unii. Wzajemnie połączona i coraz bardziej cyfrowa gospodarka zwiększa jednak również ryzyko cyberincydentów i cyberataków. Ponadto rosnące napięcia geopolityczne, konflikty i strategiczna rywalizacja znajdują odzwierciedlenie we wpływie, skali i wyrafinowaniu szkodliwych działań w cyberprzestrzeni. Takie działania mogą stanowić część kampanii hybrydowych lub operacji wojskowych. Mogą również bezpośrednio wpływać na bezpieczeństwo, gospodarkę i społeczeństwo Unii. Ponadto mają one potencjał mnożnikowy, zwłaszcza gdy działania te są skierowane przeciwko krajom będącym międzynarodowymi partnerami strategicznymi, takim jak państwa kandydujące lub sąsiadujące.

(2) Cyberincydent na dużą skalę może powodować zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub wywierać znaczące skutki w co najmniej dwóch państwach członkowskich. W zależności od przyczyny i wpływu takie incydenty na dużą skalę mogą eskalować i przerodzić się w prawdziwe sytuacje kryzysowe utrudniające prawidłowe funkcjonowanie rynku wewnętrznego lub stanowiące poważne zagrożenie dla bezpieczeństwa publicznego i ryzyko dla bezpieczeństwa podmiotów lub obywateli w kilku państwach członkowskich lub w całej Unii. Skuteczne zarządzanie kryzysowe ma zasadnicze znaczenie dla utrzymania stabilności gospodarczej i ochrony europejskich rządów, infrastruktury krytycznej, przedsiębiorstw i obywateli, a także przyczynia się do międzynarodowego bezpieczeństwa i stabilności w cyberprzestrzeni. Zarządzanie cyberkryzysami stanowi zatem jedną z integralnych części nadrzędnych unijnych ram zarządzania kryzysowego.

(3) Biorąc pod uwagę współzależności i wzajemne powiązania między środowiskami ICT podmiotów unijnych i podmiotów państw członkowskich, incydent w podmiocie unijnym może stwarzać ryzyko w cyberprzestrzeni dla państw członkowskich i odwrotnie. Wymiana istotnych informacji i koordynacja zarówno w odniesieniu do cyberincydentów na dużą skalę, jak i poważnych incydentów, zdefiniowanych w art. 3 pkt 8 rozporządzenia (UE, Euratom) 2023/2841[1], ma kluczowe znaczenie w kontekście Planu działania UE na rzecz zarządzania cyberkryzysami („plan na rzecz cyberbezpieczeństwa”).

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii, Dz.U. L, 2023/2841, 18.12.2023, s. 1–27.

(4) W razie kryzysu, w przypadku którego uruchomiono zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) na podstawie decyzji wykonawczej Rady (UE) 2018/1993[2] („uzgodnienia IPCR"), plan na rzecz cyberbezpieczeństwa powinien być w pełni spójny z uzgodnieniami IPCR dotyczącymi koordynacji i reagowania. Koordynacja polityczna i strategiczna odbywałaby się w ramach IPCR. Uzgodnienia IPCR są narzędziem koordynacji horyzontalnej i reagowania na szczeblu politycznym Unii. Zgodnie z uzgodnieniami IPCR decyzję o aktywacji lub dezaktywacji IPCR podejmuje prezydencja Rady Unii Europejskiej. Sprawozdania ze zintegrowanej orientacji i analizy sytuacyjnej („sprawozdania ISAA") przygotowane przez służby Komisji i Europejską Służbę Działań Zewnętrznych (ESDZ) wspierają prace IPCR zarówno w trybie wymiany informacji, jak i w trybie pełnej aktywacji.

(5) Główną odpowiedzialność za zarządzanie cyberincydentami i cyberkryzysami ponoszą państwa członkowskie. Potencjalny transgraniczny i międzysektorowy charakter cyberincydentów wymaga jednak od państw członkowskich i odpowiednich podmiotów unijnych współpracy na poziomie technicznym, operacyjnym i politycznym w celu skutecznej koordynacji w całej Unii. Pełny cykl zarządzania cyberkryzysami obejmuje gotowość i wspólną orientację sytuacyjną w celu przewidywania cyberincydentów na dużą skalę, zdolności wykrywania niezbędne do identyfikacji narzędzi reagowania i przywracania sprawności operacyjnej potrzebnych w celu łagodzenia takich incydentów i ograniczania ich skutków, a także zdolności reagowania w celu powstrzymywania dalszych incydentów i zapobiegania im.

---

[2] 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. 28–34.

(6) W zaleceniu Komisji (UE) 2017/1584[3] w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę określono cele i sposoby współpracy między państwami członkowskimi a podmiotami Unii w zakresie reagowania na cyberincydenty i cyberkryzysy na dużą skalę. Określono w nim odpowiednie podmioty na poziomie technicznym, operacyjnym i politycznym oraz wyjaśniono, w jaki sposób zostały one włączone do istniejących unijnych mechanizmów zarządzania kryzysowego, takich jak uzgodnienia IPCR. Podstawowe zasady określone w zaleceniu (UE) 2017/1584, a mianowicie pomocniczość, komplementarność i poufność informacji, a także podejście trójpoziomowe (techniczne, operacyjne i polityczne) pozostają aktualne. Niniejsze zalecenie opiera się na tych podstawowych zasadach i ma zastąpić zalecenie (UE) 2017/1584, ustanawiając nowe unijne ramy zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa.

(7) Niektóre definicje stosowane w niniejszym zaleceniu opierają się na definicjach i terminach stosowanych w dyrektywie (UE) 2022/2555[4]. Zakres niniejszego zalecenia jest jednak inny niż zakres dyrektywy (UE) 2022/2555. W niniejszym zaleceniu określono unijne ramy zarządzania cyberkryzysami w kontekście ogólnej gotowości UE na cyberincydenty na dużą skalę i cyberkryzysy wynikające z takich incydentów – niezależnie od tego, jakiego sektora lub podmiotu dotykają. W miarę możliwości definicje opierają się na definicjach zawartych w dyrektywie (UE) 2022/2555.

---

[3] 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. 36–58.

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.U. L 333 z 27.12.2022, s. 80–152.

(8) Zaktualizowany plan na rzecz cyberbezpieczeństwa jest konieczny, aby zapewnić jasne i dostępne wskazówki wyjaśniające, czym jest cyberincydent na dużą skalę lub cyberkryzys na szczeblu Unii, w jaki sposób uruchamiane są ramy zarządzania kryzysowego oraz jakie są role odpowiednich sieci, podmiotów i mechanizmów na szczeblu Unii, a także jakie są interakcje między tymi podmiotami i mechanizmami na wszystkich etapach cyberkryzysu. Plan na rzecz cyberbezpieczeństwa ma na celu wspieranie szerszych ram stosunków cywilno-wojskowych UE w kontekście zarządzania cyberkryzysami, w tym w kontekście pogłębiania stosunków UE–-NATO, w miarę możliwości także poprzez inkluzywne, wzajemne i niedyskryminacyjne wzmocnione mechanizmy wymiany informacji w ramach zarządzania cyberkryzysami.

(9) Należy wzmocnić międzysektorowe zarządzanie kryzysowe na szczeblu Unii, aby umożliwić zintegrowane reagowanie kryzysowe, zwłaszcza w przypadkach, gdy cyberincydenty na dużą skalę i cyberkryzysy mają materialne konsekwencje. Niniejsze zalecenie uzupełnia uzgodnienia IPCR i inne unijne mechanizmy zarządzania kryzysowego, w tym wdrażany przez Komisję ogólny system szybkiego ostrzegania ARGUS, Unijny Mechanizm Ochrony Ludności (UMOL) wspierany przez Centrum Koordynacji Reagowania Kryzysowego (ERCC) ustanowione w ramach Unijnego Mechanizmu Ochrony Ludności decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności[5] („decyzja w sprawie Unijnego Mechanizmu Ochrony Ludności”), mechanizm reagowania kryzysowego ESDZ (CRM), a także inne procesy, takie jak procesy opisane w unijnym zestawie narzędzi dla dyplomacji cyfrowej[6], zestawie narzędzi do przeciwdziałania zagrożeniom hybrydowym[7] oraz w zmienionym protokole UE do celów przeciwdziałania zagrożeniom hybrydowym[8]. Niniejsze zalecenie stanowi również uzupełnienie zalecenia Rady (UE) 2024/4371 w sprawie w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne[9] („unijny plan dotyczący infrastruktury krytycznej”), które to zalecenie obejmuje odporność fizyczną niezwiązaną z cyberbezpieczeństwem i ma na celu poprawę koordynacji reagowania na szczeblu Unii w tym obszarze i z którym niniejsze zalecenie powinno być spójne.

---

5 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. 924–947.

6 Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne (9916/17).

7 Konkluzje Rady w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe, 22 czerwca 2022 r.

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

9 Dz.U. C, C/2024/4371, 5.7.2024.

(10) Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) to sieć służąca koordynacji zarządzania cyberincydentami na dużą skalę i cyberkryzysami na poziomie operacyjnym, również w przypadku międzysektorowych cyberincydentów na dużą skalę i cyberkryzysów. Aby nie komplikować jeszcze bardziej istniejących ram, należy unikać tworzenia struktur sektorowych, które powielałyby zadania EU-CyCLONe. EU-CyCLONe powinna otrzymywać operacyjne informacje związane z cyberbezpieczeństwem również z sektorów i wnosić wkład na szczeblu politycznym.

(11) Państwa członkowskie zachęca się do pełnego wykorzystywania zasobów finansowych przeznaczonych na zapewnienie cyberbezpieczeństwa w ramach odpowiednich programów unijnych. Należy zapewnić, aby programy te nakładały minimalne obciążenia administracyjne na wnioskodawców ubiegających się o finansowanie, a udział państw członkowskich w tych programach był ułatwiony poprzez zapewnienie odpowiednich wskazówek dotyczących realnych opcji wsparcia finansowego.

(12) Niniejsze zalecenie przyczynia się do szerszych działań w zakresie gotowości wymaganych od Unii w obliczu kryzysów międzysektorowych zgodnie z zasadami zawartymi w strategii UE na rzecz unii gotowości, a mianowicie ze zintegrowanym podejściem uwzględniającym wszystkie zagrożenia, obejmującym całą administrację rządową i ogół społeczeństwa, w szczególności w odniesieniu do szerzenia wiedzy na temat ryzyka i zagrożeń oraz międzysektorowego reagowania kryzysowego.

PRZYJMUJE NINIEJSZE ZALECENIE:

I: Cel, zakres i zasady przewodnie unijnych ram zarządzania cyberkryzysami

Cel i zakres

1) W niniejszym zaleceniu w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami („plan na rzecz cyberbezpieczeństwa") określono unijne ramy zarządzania cyberkryzysami w kontekście ogólnej gotowości UE na cyberincydenty na dużą skalę i cyberkryzysy. Ramy te odzwierciedlają rolę zarówno państw członkowskich, jak i instytucji, organów i jednostek organizacyjnych Unii („podmioty unijne") w ramach ich odpowiednich kompetencji, przy pełnym poszanowaniu przepisów krajowych i wewnętrznych zasad, w celu zapewnienia kompleksowego i skoordynowanego działania na szczeblu Unii.

2) Plan na rzecz cyberbezpieczeństwa należy stosować zgodnie z unijnym planem dotyczącym infrastruktury krytycznej, w szczególności w przypadku incydentów mających wpływ zarówno na odporność fizyczną, jak i cyberbezpieczeństwo infrastruktury krytycznej[10].

3) Plan na rzecz cyberbezpieczeństwa zawiera wskazówki dotyczące reagowania na cyberincydenty na dużą skalę lub cyberkryzysy i powinien być stosowany jako uzupełnienie wszelkich odpowiednich sektorowych mechanizmów reagowania, takich jak mechanizmy wymienione w załączniku II. Odpowiednie zainteresowane strony z sektora cyberbezpieczeństwa powinny pomagać w realizacji celów tych mechanizmów sektorowych oraz ją wspierać, zarówno na szczeblu krajowym, jak i unijnym.

4) W przypadku ogólnounijnego międzysektorowego kryzysu obejmującego aspekty dotyczące cyberbezpieczeństwa, w związku z którym aktywuje się IPCR, reagowanie na szczeblu politycznym Unii powinna koordynować Rada, korzystając z uzgodnień IPCR. Po aktywacji IPCR środki w ramach planu na rzecz cyberbezpieczeństwa powinny wspierać reakcję UE na szczeblu politycznym, zapewniając konkretne wsparcie w zakresie cyberbezpieczeństwa.

[10] Koordynację w takich przypadkach szczegółowo opisano w części I sekcja 4 załącznika do unijnego planu dotyczącego infrastruktury krytycznej.

Zasady przewodnie

5) Do zarządzania cyberkryzysami na szczeblu Unii zastosowanie mają następujące zasady przewodnie:

a) *Proporcjonalność*: większość cyberincydentów mających wpływ na państwa członkowskie znajduje się poniżej poziomu, który można uznać za krajowy lub unijny cyberincydent na dużą skalę lub cyberkryzys. W przypadku cyberincydentów i cyberzagrożeń państwa członkowskie dobrowolnie i regularnie wymieniają się informacjami w ramach sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego („sieć CSIRT") i EU-CyCLONe, zgodnie z obowiązującymi procedurami działania obu tych sieci.

b) *Pomocniczość*: na państwach członkowskich spoczywa główna odpowiedzialność za reagowanie i stosowanie środków zaradczych w przypadku uderzających w nie cyberincydentów, cyberincydentów na dużą skalę bądź cyberkryzysów. Z myślą o potencjalnych skutkach transgranicznych Rada, Komisja, Wysoki Przedstawiciel, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Służba ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii (CERT-UE), Europol i wszystkie inne odpowiednie podmioty unijne powinny współpracować na wszystkich etapach cyberkryzysu. Role te wynikają z przepisów prawa Unii i odzwierciedlają sposób, w jaki cyberincydenty na dużą skalę i cyberkryzysy mogą oddziaływać na jeden lub kilka sektorów działalności gospodarczej na jednolitym rynku, na bezpieczeństwo oraz stosunki międzynarodowe Unii, a także na same podmioty unijne.

c) *Komplementarność*: niniejsze zalecenie w pełni uwzględnia istniejące mechanizmy zarządzania kryzysowego na szczeblu Unii wymienione w załączniku II, w szczególności uzgodnienia IPCR, ARGUS oraz mechanizm reagowania kryzysowego ESDZ. W niniejszym zaleceniu uwzględniono mandaty sieci CSIRT i EU-CyCLONe, a także rozporządzenie (UE, Euratom) 2023/2841. W przypadku aktywacji IPCR prace odpowiednich sieci, podmiotów i aktywowanych mechanizmów sektorowych powinny być kontynuowane i powinny stanowić wkład w polityczną i strategiczną koordynację odbywającą się w ramach IPCR oraz wspierać tę koordynację.

d) *Poufność informacji*: wszystkie wymiany informacji w kontekście niniejszego zalecenia powinny być zgodne z obowiązującymi przepisami dotyczącymi bezpieczeństwa oraz ochrony danych osobowych. W stosownych przypadkach należy uwzględnić nieformalne porozumienia o zachowaniu poufności, takie jak kod poufności TLP na potrzeby oznaczania informacji szczególnie chronionych. Do celów wymiany informacji niejawnych, niezależnie od zastosowanego systemu klasyfikacji, obok dostępnych akredytowanych narzędzi należy stosować obowiązujące wiążące zasady i porozumienia dotyczące przetwarzania informacji niejawnych.

6) Zgodnie z wyżej wymienionymi zasadami przewodnimi państwa członkowskie i podmioty unijne powinny pogłębić współpracę w zakresie zarządzania cyberkryzysami, wzmacniając wzajemne zaufanie i opierając się na istniejących sieciach i mechanizmach. Współpracy tej, w ramach planu na rzecz cyberbezpieczeństwa, sprzyja wdrożenie art. 22 i 23 rozporządzenia (UE, Euratom) 2023/2841. W szczególności plan zarządzania kryzysami w cyberprzestrzeni ustanowiony na podstawie art. 23 rozporządzenia (UE, Euratom) 2023/2841 przyczynia się m.in. do regularnej wymiany istotnych informacji między podmiotami unijnymi i z państwami członkowskimi oraz określa ustalenia dotyczące koordynacji i przepływu informacji między podmiotami unijnymi.

II: Definicje

7) Do celów niniejszego planu na rzecz cyberbezpieczeństwa stosuje się następujące definicje:

a) „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

b) „znaczący incydent” oznacza incydent, który:

   a. spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu;

   b. wpłynął lub może wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe;

c) „cyberincydent na dużą skalę” oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej dwóch państwach członkowskich;

d) „cyberkryzys” oznacza cyberincydent na dużą skalę, który przerodził się w prawdziwy kryzys uniemożliwiający prawidłowe funkcjonowanie rynku wewnętrznego lub stanowiący poważne zagrożenie dla bezpieczeństwa publicznego i ryzyko dla bezpieczeństwa podmiotów lub obywateli w kilku państwach członkowskich lub w całej Unii.

III: Krajowe struktury i obowiązki w zakresie zarządzania cyberkryzysami

8) Na państwach członkowskich spoczywa główna odpowiedzialność za reagowanie w przypadku uderzających w nie cyberincydentów na dużą skalę bądź cyberkryzysów. Zgodnie z dyrektywą (UE) 2022/2555 każde państwo członkowskie posiada co najmniej jeden organ ds. zarządzania cyberkryzysami, a także co najmniej jedną sieć CSIRT.

9) Przyjmując dyrektywę (UE) 2022/2555 i inne instrumenty ustawodawcze i nieustawodawcze dotyczące cyberbezpieczeństwa, państwa członkowskie dostosowywały swoje ramy dotyczące cyberbezpieczeństwa poprzez: określenie minimalnych zasad funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim oraz zapewnienie skutecznych środków zaradczych i środków egzekwowania, które mają kluczowe znaczenie dla skutecznego egzekwowania tych obowiązków.

10) Zgodnie z art. 9 ust. 4 dyrektywy (UE) 2022/2555 państwa członkowskie powinny przyjąć krajowe plany reagowania na cyberincydenty na dużą skalę i cyberkryzysy. Plany te obejmują m.in. krajowe środki gotowości, procedury zarządzania cyberkryzysami oraz krajowe procedury i uzgodnienia między krajowymi organami i podmiotami w celu zapewnienia ich uczestnictwa w skoordynowanym zarządzaniu cyberincydentami na dużą skalę i cyberkryzysami na szczeblu Unii oraz w celu wsparcia tego zarządzania. Procedury zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa obejmują również przepisy dotyczące ich włączenia do ogólnych krajowych ram zarządzania kryzysowego oraz kanałów wymiany informacji.

11) Zgodnie z art. 9 ust. 1 dyrektywy (UE) 2022/2555 państwa członkowskie powinny zapewnić spójność z istniejącymi ogólnymi krajowymi ramami zarządzania kryzysowego. W przypadku aktywacji IPCR krajowe organy zarządzania kryzysowego powinny, do celów dostarczania informacji na potrzeby IPCR, gromadzić dane od organów ds. zarządzania cyberkryzysami i od krajowych sektorowych mechanizmów kryzysowych.

12) Zgodnie z art. 9 ust. 5 dyrektywy (UE) 2022/2555 sieć EU-CyCLONe powinna – na wniosek zainteresowanego państwa członkowskiego – udostępniać informacje na temat odpowiednich części krajowych planów reagowania na cyberincydenty na dużą skalę i cyberkryzysy, w szczególności na temat przepisów mających na celu zapewnienie skutecznego udziału w skoordynowanym zarządzaniu cyberincydentami na dużą skalę i cyberkryzysami na szczeblu Unii oraz wspieranie takiego zarządzania, w celu wymiany najlepszych praktyk i rozważenia, czy ogólne ramy funkcjonowałyby w praktyce.

13) Sieć EU-CyCLONe i Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB) zachęca się do wymiany informacji, w stosownych przypadkach, na temat spójności planu zarządzania kryzysami ustanowionego przez IICB zgodnie z art. 23 rozporządzenia (UE, Euratom) 2023/2841 z krajowymi planami reagowania na cyberincydenty na dużą skalę i cyberkryzysy.

14) Sieć EU-CyCLONe, przy wsparciu ENISA jako sekretariatu, powinna prowadzić regularnie uaktualniany wykaz krajowych organów ds. zarządzania cyberkryzysami, zawierający dane kontaktowe urzędników i kierownictwa sieci EU-CyCLONe, oraz udostępniać go jej członkom.

IV: Główne sieci i podmioty w unijnym ekosystemie zarządzania cyberkryzysami

15) Sieć CSIRT jest główną siecią techniczną służącą do wymiany istotnych informacji na temat incydentów, w szczególności w zakresie niniejszego zalecenia, zgodnie z odpowiednimi zadaniami opisanymi w art. 15 ust. 3 dyrektywy (UE) 2022/2555. Przyczynia się ona do wzrostu wzajemnego zaufania oraz promuje sprawną i skuteczną współpracę operacyjną między państwami członkowskimi. Przewodniczący sieci CSIRT może uczestniczyć w posiedzeniach IICB w charakterze obserwatora.

16) CERT-UE jest służbą ds. cyberbezpieczeństwa dla wszystkich podmiotów unijnych. CERT-UE działa jako punkt wymiany informacji na temat cyberbezpieczeństwa i koordynacji reagowania na incydenty dla podmiotów unijnych zgodnie z art. 13 rozporządzenia (UE) 2023/2841. CERT-UE jest członkiem sieci CSIRT i wspiera Komisję w EU-CyCLONe. CERT-UE działa na poziomie technicznym i odpowiada za koordynację zarządzania poważnymi incydentami mającymi wpływ na podmioty unijne.

17) EU-CyCLONe działa jako pośrednik między szczeblem technicznym a politycznym, w szczególności podczas cyberincydentów na dużą skalę i cyberkryzysów. Pomaga w skoordynowanym zarządzaniu na szczeblu operacyjnym cyberincydentami na dużą skalę i cyberkryzysami oraz zapewnia regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii zgodnie z art. 16 dyrektywy (UE) 2022/2555. Przewodniczący sieci EU-CyCLONe może uczestniczyć w posiedzeniach IICB w charakterze obserwatora.

18) ENISA jest agencją unijną wykonującą zadania powierzone na podstawie rozporządzenia (UE) 2019/881[11] w celu osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, w tym poprzez aktywne wspieranie państw członkowskich oraz instytucji, organów i agencji Unii. ENISA zapewnia między innymi sekretariat sieci CSIRT i EU-CyCLONe, usługi w zakresie orientacji sytuacyjnej oraz pomaga państwom członkowskim poprzez regularne organizowanie ćwiczeń w dziedzinie cyberbezpieczeństwa na szczeblu Unii. Zgodnie z dyrektywą (UE) 2022/2555 i rozporządzeniem (UE) 2024/2847[12] ENISA otrzymuje informacje na temat znaczących incydentów transgranicznych oraz aktywnie wykorzystywanych podatności i incydentów mających wpływ na produkty cyfrowe.

19) Rada Unii Europejskiej („Rada") jest instytucją, która zgodnie z art. 16 Traktatu o Unii Europejskiej (TUE) pełni funkcje określania polityki i koordynacji, i której powierzono IPCR obejmujący koordynację i reagowanie na szczeblu politycznym Unii. Rada działa za pośrednictwem składów Rady, Komitetu Stałych Przedstawicieli i odpowiednich organów przygotowawczych Rady, zwłaszcza Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni (HWPCI), a także, w stosownych przypadkach, uzgodnień IPCR.

---

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.6.2019, s. 15–69.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności), Dz.U. L, 2024/2847, 20.11.2024. s. 1–81.

20) Komisja, jako instytucja wspierająca ogólny interes Unii i podejmująca w tym celu odpowiednie inicjatywy, a także czuwająca nad stosowaniem Traktatów i środków przyjętych przez instytucje na mocy art. 17 TUE, jest odpowiedzialna za niektóre działania w zakresie ogólnej gotowości na szczeblu Unii i w zakresie orientacji sytuacyjnej, w tym za zarządzanie ERCC i wspólnym systemem łączności i informacji w sytuacjach nadzwyczajnych (CECIS), zgodnie z decyzją w sprawie Unijnego Mechanizmu Ochrony Ludności. Komisja dba o spójność i koordynację powiązanych działań w zakresie reagowania kryzysowego na szczeblu unijnym na poziomie operacyjnym. Jest konsultowana w sprawie decyzji o aktywacji lub dezaktywacji IPCR. Służby Komisji opracowują wraz z ESDZ sprawozdania ISAA. Komisja jest członkiem EU-CyCLONe w przypadkach, w których potencjalny lub trwający cyberincydent na dużą skalę ma lub może mieć znaczący wpływ na usługi i działania objęte zakresem stosowania dyrektywy (UE) 2022/2555, oraz obserwatorem w innych przypadkach. W ramach IICB jest punktem kontaktowym dla EU-CyCLONe. Jest obserwatorem w sieci CSIRT.

21) Wysoki Przedstawiciel do Spraw Zagranicznych i Polityki Bezpieczeństwa („Wysoki Przedstawiciel") przy wsparciu ESDZ prowadzi wspólną politykę zagraniczną i bezpieczeństwa Unii (WPZiB) i wnosi – poprzez proponowane wnioski – wkład w rozwój tej polityki, w tym wspólnej polityki bezpieczeństwa i obrony (WPBiO). Obejmuje to struktury i mechanizmy dyplomatyczne, wywiadowcze i wojskowe, w szczególności pojedynczą komórkę analiz wywiadowczych (SIAC) jako pojedynczy punkt kontaktowy dla wywiadów państw członkowskich, Sztab Wojskowy UE (EUMS) jako źródło wojskowej wiedzy fachowej, unijny zestaw narzędzi dla dyplomacji cyfrowej, a także sieć delegatur UE, które mogą wnosić wkład w zarządzanie kryzysowe w wymiarze zewnętrznym. ESDZ przygotowuje również wraz z Komisją sprawozdania ISAA.

22) W załączniku II opisano role i kompetencje odpowiednich podmiotów na szczeblu Unii, w tym głównych sieci i podmiotów, w odniesieniu do zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa.

V: Działania przygotowawcze na wypadek cyberincydentów na dużą skalę i cyberkryzysów

Krajobraz zagrożeń

23) Państwa członkowskie i odpowiednie podmioty unijne powinny wprowadzić niezbędne środki w celu zwiększenia orientacji sytuacyjnej, uznając, że krajobraz zagrożeń i orientacja sytuacyjna w odniesieniu do konkretnych incydentów wymagają odrębnych sposobów działania. Państwa członkowskie i odpowiednie podmioty unijne powinny współpracować na podstawie zweryfikowanych i wiarygodnych danych, w tym tendencji w zakresie incydentów, taktyk, technik i procedur oraz aktywnie wykorzystywanych podatności.

24) Udostępniając informacje na szczeblu UE, państwa członkowskie powinny w pełni wykorzystywać istniejące platformy współpracy technicznej i operacyjnej, takie jak platformy wykorzystywane przez sieć CSIRT i EU-CyCLONe.

25) Aby zwiększyć wspólną orientację sytuacyjną i ułatwić ocenę wpływu UE, EU-CyCLONe i sieć CSIRT przy wsparciu ENISA powinny korzystać z wewnętrznie uzgodnionego mechanizmu sprawozdawczości w celu sporządzenia unijnego przeglądu działań technicznych i operacyjnych w oparciu o informacje zgromadzone na szczeblu krajowym.

26) EU-CyCLONe i sieć CSIRT powinny:

a) współpracować w celu poprawy wymiany informacji między poziomem technicznym i operacyjnym oraz orientacji sytuacyjnej jako całości;

b) nadal budować atmosferę zaufania między swoimi członkami i między sieciami;

c) w pełni wykorzystywać dostępne narzędzia wymiany informacji, przy wsparciu ENISA, rozważyć sposoby ulepszenia tych narzędzi i zapewnienia interoperacyjności między sieciami.

27) EU-CyCLONe, sieć CSIRT i IICB powinny współpracować w celu zapewnienia skutecznej wymiany istotnych informacji.

28) ENISA – jako sekretariat sieci CSIRT i EU-CyCLONe – odgrywa centralną rolę we wspieraniu państw członkowskich oraz instytucji, organów i agencji Unii w dążeniu do osiągnięcia wspólnej unijnej orientacji sytuacyjnej na poziomie technicznym i operacyjnym w celu wsparcia działań przygotowawczych na wypadek cyberincydentów na dużą skalę i cyberkryzysów.

29) Zgodnie z dyrektywą (UE) 2022/2555 i rozporządzeniem (UE) 2019/881 państwa członkowskie i odpowiednie podmioty unijne powinny koordynować swoje działania z sektorem prywatnym, w tym ze środowiskami zajmującymi się otwartym oprogramowaniem i producentami takiego oprogramowania, aby usprawnić wymianę informacji. W tym zakresie ENISA powinna w szczególności wykorzystywać swój program partnerstwa. Ponadto państwa członkowskie i odpowiednie podmioty unijne mogłyby też korzystać z istniejących ośrodków wymiany i analizy informacji (ISAC) na szczeblu unijnym i krajowym, tak by zwiększyć zdolności w zakresie cyberbezpieczeństwa i reagowania na cyberincydenty, w tym poprzez wspólne posiedzenia sektora prywatnego z EU-CyCLONe lub siecią CSIRT.

30) Aby usprawnić wymianę informacji w ramach sieci i między nimi oraz wyjaśnić wzajemne oczekiwania co do takiej wymiany, EU-CyCLONe powinna – przy wsparciu ENISA jako sekretariatu i po konsultacji z siecią CSIRT i grupą współpracy NIS – w terminie 24 miesięcy od przyjęcia niniejszego zalecenia uzgodnić wspólną ujednoliconą taksonomię wagi incydentów. Ta taksonomia powinna umożliwić porównanie wagi incydentów we wszystkich państwach członkowskich poprzez uwzględnienie wpływu na świadczenie usług, liczby poszkodowanych podmiotów i ich odpowiedniego znaczenia, wpływu na inne usługi i infrastrukturę, a także wyrządzonych szkód pieniężnych, wizerunkowych i politycznych. Powinna ona opierać się na odpowiednich istniejących skalach lub taksonomii, takich jak Referencyjna taksonomia klasyfikacji incydentów.

Poziom techniczny

31) Sieć CSIRT jest platformą współpracy technicznej i wymiany informacji między wszystkimi państwami członkowskimi oraz za pośrednictwem CERT-UE z podmiotami unijnymi.

32) Zgodnie z dyrektywą (UE) 2022/2555 każdy zespół CSIRT ma za zadanie monitorować i analizować cyberzagrożenia, podatności i incydenty na szczeblu krajowym. Aby osiągnąć wspólną orientację sytuacyjną, zespoły CSIRT powinny wymieniać się, zarówno w ramach sieci CSIRT, jak i dwustronnie, istotnymi informacjami na temat incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa, cyberzagrożeń, ryzyka i podatności.

33) W celu zacieśnienia współpracy operacyjnej na szczeblu Unii sieć CSIRT powinna rozważyć zaproszenie do udziału w jej pracach organów i agencji Unii zaangażowanych w politykę cyberbezpieczeństwa, takich jak Europol.

34) Zgodnie z rozporządzeniem 2023/2841 służba CERT-UE powinna gromadzić, analizować i udostępniać instytucjom, organom i jednostkom organizacyjnym Unii informacje na temat cyberzagrożeń, podatności i incydentów w jawnej infrastrukturze ICT oraz zarządzać nimi, a także, w razie potrzeby, przedstawiać IICB konkretne wnioski dotyczące wytycznych i zaleceń dla instytucji, organów i jednostek organizacyjnych Unii. CERT-UE powinna współpracować i wymieniać informacje z odpowiednikami z państw członkowskich, w tym za pośrednictwem sieci CSIRT.

Poziom operacyjny

35) Zgodnie z dyrektywą (UE) 2022/2555 sieć EU-CyCLONe powinna służyć jako platforma współpracy między organami państw członkowskich ds. zarządzania cyberkryzysami oraz za pośrednictwem Komisji z odpowiednimi podmiotami unijnymi w celu zwiększenia poziomu gotowości w zakresie zarządzania cyberincydentami na dużą skalę i cyberkryzysami oraz rozwijania wspólnej orientacji sytuacyjnej w odniesieniu do cyberincydentów na dużą skalę i cyberkryzysów.

36) Zgodnie z dyrektywą (UE) 2022/2555 i rozporządzeniem (UE) 2024/2847 ENISA otrzymuje informacje na temat znaczących incydentów transgranicznych oraz aktywnie wykorzystywanych podatności i incydentów mających wpływ na produkty cyfrowe. ENISA działająca jako sekretariat powinna doradzać sieci CSIRT i EU-CyCLONe, tak by wspierać te sieci w określaniu, czy należy podjąć dalsze działania, oraz aby wnosić wkład we wspólną orientację sytuacyjną.

Poziom polityczny

37) Państwa członkowskie i odpowiednie podmioty unijne powinny monitorować rozwój sytuacji międzynarodowej, który ma wpływ na cyberbezpieczeństwo (w tym cyberzagrożenia, zagrożenia hybrydowe oraz zagraniczne manipulacje informacjami i ingerencje w informacje, w tym, w stosownych przypadkach, dezinformację). Należy wziąć pod uwagę inicjatywy takie jak wspólne raporty techniczne o stanie cyberbezpieczeństwa w UE (JCAR), analizy dostarczone przez SIAC i inne istotne produkty prezentujące opinie eksperckie.

38) Wysoki Przedstawiciel powinien w dalszym ciągu informować państwa członkowskie i angażować je w działania dyplomatyczne Unii związane z cyberzagrożeniami, zwłaszcza te, które dotyczą podmiotów państwowych, we współpracę z państwami trzecimi i organizacjami międzynarodowymi, w tym z NATO, oraz we wdrażanie środków dyplomatycznych, w tym środków ograniczających.

39) Prezydencja Rady Unii Europejskiej może uruchomić poświęconą monitoringowi stronę na platformie internetowej IPCR, na której państwa członkowskie oraz instytucje i organy UE mogłyby wymieniać informacje na temat ewentualnego rozwijającego się kryzysu.

Wspólne ćwiczenia

40) Komisja, we współpracy z Wysokim Przedstawicielem, przy wsparciu ENISA, po konsultacji z EU-CyCLONe i siecią CSIRT, powinna opracować skuteczny roczny kroczący program ćwiczeń w dziedzinie cyberbezpieczeństwa w celu przygotowania się na wypadek cyberkryzysów i zwiększenia efektywności organizacyjnej. Kroczący program ćwiczeń w dziedzinie cyberbezpieczeństwa powinien uwzględniać ćwiczenia w ramach UMOL i innych mechanizmów reagowania kryzysowego na szczeblu Unii, w tym ćwiczenia określone w unijnym planie dotyczącym infrastruktury krytycznej. Pierwszy program kroczący należy opracować w ciągu 12 miesięcy od przyjęcia planu na rzecz cyberbezpieczeństwa, a kolejne programy należy zakończyć do 31 marca każdego roku. Program kroczący należy przedłożyć Radzie do wiadomości.

41) Program kroczący powinien również obejmować ćwiczenia opracowane z wykorzystaniem unijnych scenariuszy skoordynowanej oceny ryzyka. Powinien on obejmować ćwiczenia z udziałem wszystkich odpowiednich podmiotów, w szczególności sektora prywatnego i NATO.

42) ENISA, pełniąc rolę sekretariatu sieci CSIRT i EU-CyCLONe, powinna zapewniać systematyczne gromadzenie doświadczeń i wniosków z ćwiczeń, a także określanie i proponowanie sposobów realizacji wynikających z nich działań, aby zagwarantować ich skuteczną realizację i pozytywny wpływ na wspólną odporność UE, w tym odpowiednie obowiązujące procedury działania.

43) Wszystkie podmioty i sieci powinny poprawić koordynację w przypadku cyberincydentu na dużą skalę lub cyberkryzysu na podstawie doświadczeń i wniosków z ćwiczeń.
Aby poprawić koordynację, w szczególności EU-CyCLONe i sieć CSIRT powinny zająć się wyzwaniami zidentyfikowanymi podczas ćwiczeń, zwłaszcza tymi dotyczącymi współpracy między sieciami oraz, w razie potrzeby, szybko dostosować obowiązujące procedury działania.

44) Grupa współpracy NIS powinna zwrócić się do sieci CSIRT, EU-CyCLONe i ENISA o przedstawienie doświadczeń i wniosków z ćwiczeń, a także określenie i zaproponowanie sposobów realizacji wynikających z nich działań.

45) Rada może zwrócić się do przewodniczących sieci CSIRT, EU-CyCLONe, grupy współpracy NIS i do ENISA o przedstawienie, w jaki sposób wdrożono doświadczenia i wnioski z tych ćwiczeń.

46) ENISA, we współpracy z Komisją i Wysokim Przedstawicielem, jest proszona o zorganizowanie ćwiczenia w celu przetestowania planu na rzecz cyberbezpieczeństwa podczas kolejnego ćwiczenia Cyber Europe. Ćwiczenie to powinno obejmować wszystkie odpowiednie podmioty, w tym poziom polityczny. ENISA proszona jest o koordynowanie z prezydencją Rady Unii Europejskiej zaangażowania poziomu politycznego. Ćwiczenie może również obejmować sektor prywatny i NATO.

VI: Wykrywanie incydentu, który mógłby przerodzić się w cyberincydent na dużą skalę lub cyberkryzys

47) Wszystkie podmioty – zgodnie ze swoimi właściwymi mandatami i w oparciu o podejście uwzględniające wszystkie zagrożenia – powinny przekazywać odpowiednim sieciom informacje wskazujące na potencjalny cyberincydent na dużą skalę lub cyberkryzys.

48) Zgodnie z rozporządzeniem (UE) 2025/38[13] w przypadku gdy transgraniczne centra cyberbezpieczeństwa otrzymują informacje na temat potencjalnego lub trwającego cyberincydentu na dużą skalę, powinny one zapewnić, do celów wspólnej orientacji sytuacyjnej, aby odpowiednie informacje przekazano bez zbędnej zwłoki organom państw członkowskich i Komisji za pośrednictwem EU-CyCLONe i sieci CSIRT.

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie zagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności), Dz.U. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) W przypadku zaobserwowania znaczącego incydentu, w szczególności powodującego natychmiastowe skutki, może on zostać zgłoszony CSIRT lub wykryty przez CSIRT, a także przez organy państw członkowskich ds. zarządzania cyberkryzysami lub inne organy sektorowe. Zachęca się państwa członkowskie do wymiany informacji związanych z takimi incydentami w ramach sieci, które powinny rozważyć podjęcie odpowiednich działań. Aktywowanie sieci CSIRT i EU-CyCLONe może być niezależne od siebie w zależności od charakteru incydentu i wymaganej reakcji. Zachęca się jednak obie sieci do kontynuowania wzajemnej współpracy na podstawie uzgodnionych ustaleń proceduralnych. Decyzja o aktywacji należy wyłącznie do danej sieci i jest podejmowana niezależnie.

50) Sieć CSIRT powinna doradzać EU-CyCLONe, czy zaobserwowany cyberincydent można uznać za potencjalny lub trwający cyberincydent na dużą skalę.

51) Jak wskazano w dyrektywie (UE) 2022/2555, sieć CSIRT i EU-CyCLONe powinny niezwłocznie uzgodnić ustalenia proceduralne na wypadek potencjalnego lub trwającego cyberincydentu na dużą skalę, aby zapewnić koordynację techniczno-operacyjną oraz terminowe i adekwatne przekazywanie informacji na poziom polityczny.

VII: Reagowanie na cyberincydenty na dużą skalę i cyberkryzysy na szczeblu Unii

Reagowanie na cyberincydent na dużą skalę lub cyberkryzys, w przypadku których nie aktywowano IPCR w pełnym trybie

52) Skuteczne reagowanie na cyberincydenty na dużą skalę lub cyberkryzysy na szczeblu UE zależy od skutecznej współpracy technicznej, operacyjnej i politycznej w ramach podejścia obejmującego całą administrację rządową, w tym, w miarę możliwości, organy ścigania.

53) Na każdym szczeblu zaangażowane podmioty powinny prowadzić konkretne działania w celu osiągnięcia wspólnej orientacji sytuacyjnej i skoordynowanej reakcji. Środki takie zapewniają uporządkowane i skuteczne rozpowszechnianie informacji.

54) Reagowanie powinno być odpowiednie do skutków cyberincydentu na dużą skalę lub cyberkryzysu. Zgodnie z dyrektywą (UE) 2022/2555 organy państw członkowskich ds. zarządzania cyberkryzysami powinny zapewnić krajową spójność i koordynację między sektorowymi reakcjami na cyberkryzys.

55) W przypadku cyberincydentu na dużą skalę lub cyberkryzysu wszystkie podmioty i sieci powinny reagować w ścisłej koordynacji w następujący sposób:

a) na poziomie technicznym:

i. Poszkodowane państwa członkowskie i ich CSIRT powinny współpracować z dotkniętymi podmiotami w celu reagowania na incydenty i, w stosownych przypadkach, udzielania pomocy;

ii. Zespoły CSIRT powinny współpracować za pośrednictwem sieci CSIRT w celu wymiany istotnych informacji technicznych na temat incydentu; zespoły CSIRT współpracują w ramach podejmowanych wysiłków na rzecz analizy dostępnych artefaktów technicznych i innych informacji technicznych związanych z incydentem w celu określenia przyczyny i możliwych technicznych środków łagodzących;

iii. W przypadku gdy zespół CSIRT lub organ państwa członkowskiego ds. zarządzania cyberkryzysami dowiadują się o znaczącym incydencie, zachęca się je do powiadomienia o tym sieci CSIRT lub EU-CyCLONe;

iv. Sieć CSIRT, przy wsparciu ENISA, powinna przygotować zestawienie sprawozdań krajowych dostarczanych przez CSIRT; zestawienie to powinno być przedstawiane EU-CyCLONe;

v. W przypadku gdy cyberincydent może potencjalnie przerodzić się w cyberincydent na dużą skalę lub cyberkryzys, sieć CSIRT powinna dzielić się odpowiednimi informacjami z EU-CyCLONe. EU-CyCLONe powinna wykorzystywać je do informowania Rady;

vi. Sieć CSIRT powinna pozostawać w ścisłym kontakcie z Europolem, aby zapewnić wymianę odpowiednich informacji technicznych. Sieć CSIRT i Europol powinny ustanowić punkty kontaktowe w celu usprawnienia wymiany informacji w przypadku cyberincydentu na dużą skalę, gdy jest to stosowne;

b) na poziomie operacyjnym:

i. Państwa członkowskie powinny złagodzić skutki incydentu na szczeblu krajowym za pomocą odpowiednich środków;

ii. Sieć CSIRT powinna zapewnić EU-CyCLONe oceny techniczne trwających incydentów, z których to ocen może korzystać EU-CyCLONe;

iii. EU-CyCLONe powinna ocenić konsekwencje i skutki odpowiednich cyberincydentów na dużą skalę i cyberkryzysów oraz proponować możliwe środki łagodzące, a także wspierać skoordynowane zarządzanie cyberincydentami na dużą skalę i cyberkryzysami oraz proces decyzyjny na szczeblu politycznym;

iv. Jeżeli cyberincydent na dużą skalę mający skutki międzysektorowe wymaga uruchomienia działań w zakresie reagowania na szczeblu Unii, w szczególności odpowiednich horyzontalnych i sektorowych mechanizmów zarządzania kryzysowego na szczeblu Unii wymienionych w załączniku II;

(a) odpowiednie podmioty mogą, w zależności od rodzaju sektorowych mechanizmów zarządzania kryzysowego na szczeblu Unii, zwrócić się o uruchomienie danego mechanizmu;

(b) w przypadku uruchomienia takiego mechanizmu sektorowego odpowiednie podmioty wspierają podmioty sektorowe w łagodzeniu skutków incydentu;

(c) Komisja powinna ułatwiać przepływ niezbędnych informacji między punktami kontaktowymi na potrzeby wymienionych w załączniku II odpowiednich horyzontalnych i sektorowych mechanizmów kryzysowych na szczeblu Unii a EU-CyCLONe oraz powinna przeprowadzić zintegrowaną analizę międzysektorową i zaproponować warianty odpowiedniego zintegrowanego planu reagowania;

(d) Komisja, za pośrednictwem EU-CyCLONe powinna, w stosownych przypadkach, we współpracy z Wysokim Przedstawicielem, zapewnić spójność i koordynację środków operacyjnych na szczeblu UE w dziedzinie cyberbezpieczeństwa z powiązanymi działaniami w zakresie reagowania na szczeblu Unii, w szczególności w odniesieniu do wniosków o pomoc za pośrednictwem UMOL;

(e) jeżeli uruchomiona została poświęcona monitoringowi strona na platformie internetowej IPCR, informacje o incydencie, jego skutkach i podjętych środkach powinny być również udostępniane państwom członkowskim i podmiotom unijnym za pośrednictwem platformy internetowej IPCR;

v. Państwa członkowskie mogą występować z wnioskami o usługi z rezerwy cyberbezpieczeństwa UE zgodnie z art. 15 rozporządzenia (UE) 2025/38. Bez uszczerbku dla przyszłych aktów wykonawczych na mocy tego rozporządzenia usługi z rezerwy cyberbezpieczeństwa UE powinny być świadczone w ciągu 24 godzin od złożenia wniosku;

c) na szczeblu politycznym:

i. Rada może zwrócić się o informacje do kluczowych zainteresowanych stron, w szczególności do Komisji, Wysokiego Przedstawiciela i EU-CyCLONe w celu przeprowadzenia odpowiedniej reakcji politycznej i strategicznej;

ii. Rada, wspierana przez Komisję i Wysokiego Przedstawiciela, może podjąć decyzję w sprawie odpowiednich środków reagowania na cyberincydent na dużą skalę, w tym w sprawie ewentualnych reakcji dyplomatycznych zgodnie z rozdziałem IX;

iii. W zależności od charakteru i skutków incydentu państwa członkowskie mogą uruchomić dodatkowe mechanizmy lub instrumenty zarządzania cyberkryzysami;

iv. Gdy IPCR aktywuje się w trybie wymiany informacji, uruchamia się zdolności wsparcia komórki ISAA, co zwiększa wymianę informacji za pośrednictwem platformy internetowej IPCR i zapewnia wspólną orientację sytuacyjną. Sprawozdania sytuacyjne EU-CyCLONe i sieci CSIRT powinny pozostać głównymi instrumentami przedstawiającymi wspólną orientację sytuacyjną odpowiednio na poziomie operacyjnym i technicznym. Sprawozdania te mogą stanowić podstawę sprawozdań ISAA;

v. W przypadku incydentu, który wymaga uruchomienia działań w zakresie reagowania na szczeblu Unii, w szczególności odpowiednich horyzontalnych i sektorowych mechanizmów zarządzania kryzysowego na szczeblu Unii wymienionych w załączniku II, Rada, we współpracy z Komisją i Wysokim Przedstawicielem, powinna zapewnić spójność i koordynację między reagowaniem na cyberkryzys a powiązanymi działaniami w zakresie reagowania na szczeblu Unii;

vi. W sytuacji gdy wnioskowano o uruchomienie odpowiednich mechanizmów, w szczególności usług z rezerwy cyberbezpieczeństwa, służby Komisji oraz, w stosownych przypadkach, ESDZ, a także odpowiednie organy Rady, w szczególności HWPCI i Horyzontalna Grupa Robocza ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym (HWP ERCHT), stosownie do przypadku, powinny koordynować opracowywanie i wdrażanie środków, a także odpowiedni proces decyzyjny z zastosowaniem dodatkowych środków, zgodnie z zestawem narzędzi do przeciwdziałania zagrożeniom hybrydowym[14] w przypadku szkodliwych działań w cyberprzestrzeni, które są częścią szerszej kampanii hybrydowej.

Reagowanie na cyberincydent na dużą skalę lub cyberkryzys, w przypadku których aktywowano IPCR w pełnym trybie

56) Należy wdrożyć kroki wymienione w sekcji „Reagowanie na cyberincydent na dużą skalę lub cyberkryzys, w przypadku których nie aktywowano IPCR w pełnym trybie" powyżej.

57) Gdy IPCR aktywuje się w pełnym trybie, sprawozdania ISAA służą zapewnieniu wspólnej orientacji sytuacyjnej na szczeblu politycznym. Sprawozdania sytuacyjne EU-CyCLONe i sieci CSIRT powinny pozostać głównymi instrumentami przedstawiającymi wspólną orientację sytuacyjną odpowiednio na poziomie operacyjnym i technicznym. Sprawozdania te mogą stanowić podstawę sprawozdań ISAA.

58) W przypadku cyberincydentu na dużą skalę lub cyberkryzysu, który skutkuje aktywacją IPCR w pełnym trybie, wszystkie podmioty powinny reagować w ścisłej koordynacji w ramach podejścia obejmującego całą administrację rządową w następujący sposób:

a) koordynację reakcji na poziomie politycznym Unii przeprowadza Rada z wykorzystaniem uzgodnień IPCR;

[14] Unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym stanowi ramy skoordynowanej reakcji na kampanie hybrydowe mające wpływ na UE i jej państwa członkowskie, które to narzędzia obejmują na przykład środki zapobiegawcze, środki oparte na współpracy, środki na rzecz stabilności, środki ograniczające i środki służące przywróceniu sprawności operacyjnej, wspierające solidarność i wzajemną pomoc.

b) EU-CyCLONe, we współpracy z siecią CSIRT, powinna przekazywać na poziom polityczny jasne informacje na temat skutków, możliwych konsekwencji oraz środków reagowania i środków zaradczych w odniesieniu do incydentu, w tym poprzez wkład w sprawozdania ISAA;

c) oprócz zdolności komórki ISAA prezydencja Rady Unii Europejskiej może zwołać posiedzenia okrągłego stołu IPCR, aby umożliwić polityczną i strategiczną koordynację reakcji UE, przy czym działania w ramach planu na rzecz cyberbezpieczeństwa oraz prace nad odpowiednimi mechanizmami sektorowymi byłyby uwzględniane w pracach IPCR. Podczas posiedzeń okrągłego stołu można ponadto zidentyfikować pewne konkretne luki w reakcji i zachęcić konkretne podmioty unijne do ich wyeliminowania i złożenia sprawozdania w tej sprawie podczas kolejnych tego typu posiedzeń, aby wesprzeć polityczną i strategiczną koordynację w ramach IPCR;

d) prezydencja Rady Unii Europejskiej powinna rozważyć zapraszanie UE-CyCLONe na odpowiednie posiedzenia, w tym na posiedzenia okrągłego stołu w ramach uzgodnień IPCR i inne odpowiednie posiedzenia Rady;

e) organy państw członkowskich ds. zarządzania kryzysowego powinny zapewniać spójność i koordynację między sektorowymi reakcjami na cyberkryzys wspieranymi przez organy ds. zarządzania cyberkryzysami;

f) ewentualne reakcje dyplomatyczne należy rozważyć i wdrożyć zgodnie z rozdziałem IX.

VIII: Działania w dziedzinie komunikacji ze społeczeństwem

59) Choć komunikacja z ludnością danego państwa członkowskiego na temat trwającego cyberincydentu na dużą skalę lub cyberkryzysu, w tym w ramach podnoszenia świadomości, należy do kompetencji krajowych, państwa członkowskie, Komisja i Wysoki Przedstawiciel powinni w miarę możliwości dążyć do koordynowania swojej komunikacji ze społeczeństwem. W stosownych przypadkach można zaangażować nieformalną sieć ds. komunikacji kryzysowej w ramach IPCR.

60) Na potrzeby działań przygotowawczych na wypadek cyberincydentów na dużą skalę i cyberkryzysów państwa członkowskie oraz, w stosownych przypadkach, Komisję i CERT-UE zachęca się do wymiany informacji na temat ich działań w dziedzinie komunikacji w ramach EU-CyCLONe i sieci CSIRT, w tym najlepszych praktyk, takich jak doradztwo lub kampanie uświadamiające. ENISA powinna zapewnić narzędzia wspierające taką wymianę i zapewniające łatwy dostęp.

61) W przypadku cyberincydentu na dużą skalę lub cyberkryzysu państwa członkowskie zachęca się do wymiany w ramach EU-CyCLONe informacji na temat ich działań w dziedzinie komunikacji ze społeczeństwem w celu budowania wspólnej orientacji i koordynowania działań. EU-CyCLONe może z własnej inicjatywy lub na wniosek Rady przekazać jej przegląd takich podejść.

IX: Reakcja dyplomatyczna i współpraca z partnerami strategicznymi

62) Wysoki Przedstawiciel, w ścisłej współpracy z Komisją i innymi odpowiednimi podmiotami Unii, powinien:

a) wspierać proces decyzyjny w Radzie, w tym poprzez analizy, sprawozdania i wnioski, dotyczące stosowania ewentualnych środków w ramach unijnego zestawu narzędzi dla dyplomacji cyfrowej. Umożliwi to wykorzystanie pełnego zakresu narzędzi Unii dostępnych na potrzeby zapobiegania szkodliwym działaniom w cyberprzestrzeni, powstrzymywania ich i reagowania na nie, a tym samym poprawi poziom cyberbezpieczeństwa oraz pozwoli propagować pokój, bezpieczeństwo i stabilność w skali międzynarodowej w cyberprzestrzeni;

b) w przypadku stwierdzenia odpowiedniego incydentu ułatwić przepływ niezbędnych informacji z partnerami strategicznymi, w tym w stosownych przypadkach, z NATO;

c) wzmocnić koordynację z partnerami strategicznymi, w tym w stosownych przypadkach z NATO, w zakresie reagowania na szkodliwe działania w cyberprzestrzeni prowadzone przez stałych agresorów, a w szczególności korzystać z unijnego zestawu narzędzi dla dyplomacji cyfrowej, zgodnie z wytycznymi wykonawczymi.

63) Państwa członkowskie, Wysoki Przedstawiciel, Komisja i inne odpowiednie podmioty unijne powinny współpracować z partnerami strategicznymi i organizacjami międzynarodowymi w celu propagowania dobrych praktyk i odpowiedzialnego zachowania państw w cyberprzestrzeni oraz zapewnienia szybkiej i skoordynowanej reakcji w przypadku potencjalnych cyberincydentów lub cyberincydentów na dużą skalę.

64) Współpraca Unii Europejskiej i NATO powinna przebiegać w myśl uzgodnionych zasad przewodnich dotyczących inkluzywności, wzajemności i przejrzystości oraz przy pełnym poszanowaniu autonomicznego procesu decyzyjnego Unii.

65) Uwzględniając istniejące umowy, takie jak umowa techniczna CERT-UE/NATO z 2016 r., Komisja i Wysoki Przedstawiciel powinni dążyć do ustanowienia punktów kontaktowych na potrzeby koordynacji z NATO w przypadku cyberkryzysu w celu wymiany niezbędnych informacji na temat sytuacji i wykorzystania mechanizmów reagowania kryzysowego, tak by zacieśnić współpracę w zakresie reagowania i zwiększyć jego skuteczność. W tym celu Unia powinna przeanalizować, jak poprawić wymianę informacji z NATO w sposób inkluzywny, wzajemny i niedyskryminacyjny, w szczególności poprzez zapewnienie narzędzi bezpiecznej komunikacji, przy jednoczesnym uwzględnieniu standardów wymiany informacji obowiązujących w poszczególnych państwach członkowskich.

66) W ramach wspomnianego powyżej w rozdziale V unijnego kroczącego programu ćwiczeń w dziedzinie cyberbezpieczeństwa służby Komisji i ESDZ powinny rozważyć zorganizowanie ćwiczenia z NATO na szczeblu personelu w celu przetestowania współpracy między podmiotami cywilnymi i wojskowymi na wypadek cyberincydentu na dużą skalę lub cyberkryzysu, w przypadku których państwa członkowskie lub sojusznicy NATO szukają rozwiązań w obliczu cyberataku mającego wpływ na ich bezpieczeństwo. Ćwiczenie to powinno być prowadzone w sposób inkluzywny i niedyskryminacyjny oraz z pełnym poszanowaniem uzgodnionych zasad dotyczących parametrów współpracy UE–NATO. Ćwiczenie to powinno zostać przeprowadzone w ramach unijnego ćwiczenia „Integrated Resolve" (równoległe i skoordynowane ćwiczenie – PACE). Należy podjąć wszelkie niezbędne środki w celu zapewnienia udziału wszystkich podmiotów, o których mowa w planie na rzecz cyberbezpieczeństwa.

67) W porozumieniu z Radą, Komisją i Wysokim Przedstawicielem należy również rozważyć wspólne ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu Unii z krajami Bałkanów Zachodnich, Republiką Mołdawii, Ukrainą, a także z innymi partnerami strategicznymi i państwami trzecimi o podobnych poglądach.

X. Koordynacja zarządzania cyberkryzysami z podmiotami wojskowymi na szczeblu UE

68) Państwa członkowskie powinny nadal zacieśniać współpracę między cywilnymi i wojskowymi podmiotami zajmującymi się cyberbezpieczeństwem na szczeblu krajowym.

69) EU-CyCLONe i sieć CSIRT powinny określić możliwe sposoby i procedury współpracy z odpowiednimi podmiotami wojskowymi UE, takimi jak unijna konferencja dowódców ds. obrony cyberprzestrzeni i operacyjna sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET), aby wykorzystać wspólną perspektywę wojskową i cywilną, w szczególności poprzez wspólne posiedzenia. EU-CyCLONe i sieć CSIRT powinny informować Radę o postępach poczynionych w odniesieniu do takiej współpracy.

70) W przypadku gdy w kontekście cyberincydentu na dużą skalę lub cyberkryzysu wykorzystywane są odpowiednie krajowe lub wielonarodowe wojskowe zdolności reagowania, poszkodowane państwo członkowskie zachęca się do powiadomienia o tym EU-CyCLONe, a także ESDZ, a powiadomienie takie powinno być wspólnie uzgodnione przez użytkownika i podmiot zapewniający taką zdolność reagowania.

71) W ramach wspomnianego powyżej w rozdziale V unijnego kroczącego programu ćwiczeń w dziedzinie cyberbezpieczeństwa Komisja i Wysoki Przedstawiciel powinni rozważyć zorganizowanie wspólnego ćwiczenia w celu przetestowania współpracy między cywilnymi i wojskowymi podmiotami zajmującymi się cyberbezpieczeństwem w przypadku cyberincydentu na dużą skalę lub cyberkryzysu, które mają wpływ na państwa członkowskie.

XI: Odzyskiwanie i wdrożone doświadczenia i wnioski z cyberkryzysu

72) Na etapie odzyskiwania po cyberkryzysie państwa członkowskie, odpowiednie podmioty unijne i sieci powinny współpracować, aby zapewnić szybkie przywrócenie podstawowych funkcji. W taką współpracę powinny być również zaangażowane, w stosownych przypadkach, organy ścigania. Na tym etapie kluczowe znaczenie ma współpraca z sektorem prywatnym, zwłaszcza w ułatwianiu odzyskiwania danych i przywracania systemów. W ramach skutecznej koordynacji między zainteresowanymi stronami priorytetowo należy traktować minimalizację zakłóceń i zapewnienie ciągłości działania.

73) Na etapie odzyskiwania państwa członkowskie, odpowiednie podmioty unijne i sieci powinny współpracować w oparciu o wdrożone doświadczenia i wnioski z cyberkryzysów lub cyberincydentów, którym stawiono czoła w przeszłości, a także w oparciu o zgłoszenia incydentów, w szczególności w kontekście europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie ustanowionego rozporządzeniem (UE) 2025/38.

74) EU-CyCLONe powinna przedstawić sieci CSIRT, grupie współpracy NIS oraz Radzie kompleksowy wykaz wdrożonych doświadczeń i wniosków z cyberkryzysów lub cyberincydentów, którym stawiono czoła w przeszłości, oraz najlepszych praktyków. ENISA powinna zapewnić odpowiednie odzwierciedlenie tych wdrożonych doświadczeń i wniosków w przyszłych działaniach w zakresie gotowości oraz podczas planowania przyszłych ćwiczeń.

XII: Bezpieczna łączność

75) Na podstawie mapy istniejących narzędzi bezpiecznej łączności[15] Komisja powinna do końca 2026 r. zaproponować interoperacyjny zestaw rozwiązań w zakresie bezpiecznej łączności. Rada, Komisja, Wysoki Przedstawiciel, EU-CyCLONe i sieć CSIRT powinni osiągnąć porozumienie w sprawie tego zestawu rozwiązań do końca 2027 r. Rozwiązania te powinny opierać się na działaniach w dziedzinie bezpiecznej łączności, które instytucje UE mogłyby podjąć w ramach strategii UE na rzecz unii gotowości, i powinny obejmować pełen zakres wymaganych trybów łączności (głos, dane, wideokonferencje, komunikaty, współpraca oraz wymiana dokumentów i konsultacje). Rozwiązania te powinny spełniać wspólnie określone wymogi w zakresie ochrony szczególnie chronionych informacji jawnych. Należy stosować rozwiązania oparte na otwartym protokole z wdrożeniami otwartego oprogramowania, odpowiednie do łączności w czasie rzeczywistym i zarządzane przez podmiot z siedzibą w UE.

76) Do celów wymiany informacji niejawnych opatrzonych klauzulą RESTREINT UE/EU RESTRICTED EU-CyCLONe i sieć CSIRT powinny w razie potrzeby móc korzystać z kanałów bezpiecznej łączności zapewnianych instytucjom, organom i agencjom UE na potrzeby wymiany informacji niejawnych między sobą oraz z państwami członkowskimi.

[15] Dok. WK 862/2023.

77) Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) ustanowione na mocy rozporządzenia (UE) 2021/887[16], bez uszczerbku dla przyszłych wieloletnich ram finansowych, powinno rozważyć finansowanie w ramach programu „Cyfrowa Europa", aby pomóc państwom członkowskim we wdrażaniu narzędzi bezpiecznej łączności. Należy unikać powielania inwestycji w interoperacyjne bezpieczne systemy.

78) W szczególności podmioty unijne i państwa członkowskie powinny opracować plany awaryjne na wypadek poważnych kryzysów, w których normalne kanały łączności oparte na sieciach internetowych lub telekomunikacyjnych są zakłócone lub niedostępne.

79) Z myślą o skutecznym reagowaniu kryzysowym należy ustanowić mechanizmy łączności i wymiany informacji między organami ścigania a sieciami ds. cyberbezpieczeństwa, zwłaszcza na poziomie technicznym. W ramach tych mechanizmów należy respektować rolę każdej ze stron i unikać ingerowania w bieżące działania, a także zagwarantować redundancję łączności. Opracowywany obecnie europejski system łączności krytycznej (EUCCS) może ułatwić wspólne reagowanie z odpowiednimi środowiskami zajmującymi się cyberbezpieczeństwem.

XIII: Postanowienia końcowe

80) EU-CyCLONe, we współpracy z siecią CSIRT i innymi głównymi podmiotami unijnego ekosystemu zarządzania cyberkryzysami, przy wsparciu ENISA, powinna opracować, w ciągu roku od publikacji niniejszego zalecenia, szczegółowe schematy przedstawiające przepływy informacji między odpowiednimi podmiotami, procesy decyzyjne i sprawozdania opracowane podczas zarządzania cyberincydentami na dużą skalę lub cyberkryzysami, jak opisano w niniejszym zaleceniu. Schematy przepływów powinny obejmować różne tryby i warstwy współpracy. Powinny być w razie konieczności aktualizowane.

---

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji, Dz.U. L 202 z 8.6.2021, s. 1–31.

81) Aby wesprzeć skuteczne stosowanie zmienionego planu na rzecz cyberbezpieczeństwa i opierając się na doświadczeniach zdobytych podczas wspólnych ćwiczeń w dziedzinie cyberbezpieczeństwa prowadzonych w jego ramach, Rada może w razie potrzeby opracować zestaw wytycznych wykonawczych. Wytyczne te mogłyby stanowić odpowiedź na praktyczne wyzwania zidentyfikowane w trakcie ćwiczeń oraz zlikwidować wykryte luki i brakujące ogniwa w zakresie koordynacji, komunikacji i interakcji operacyjnych.

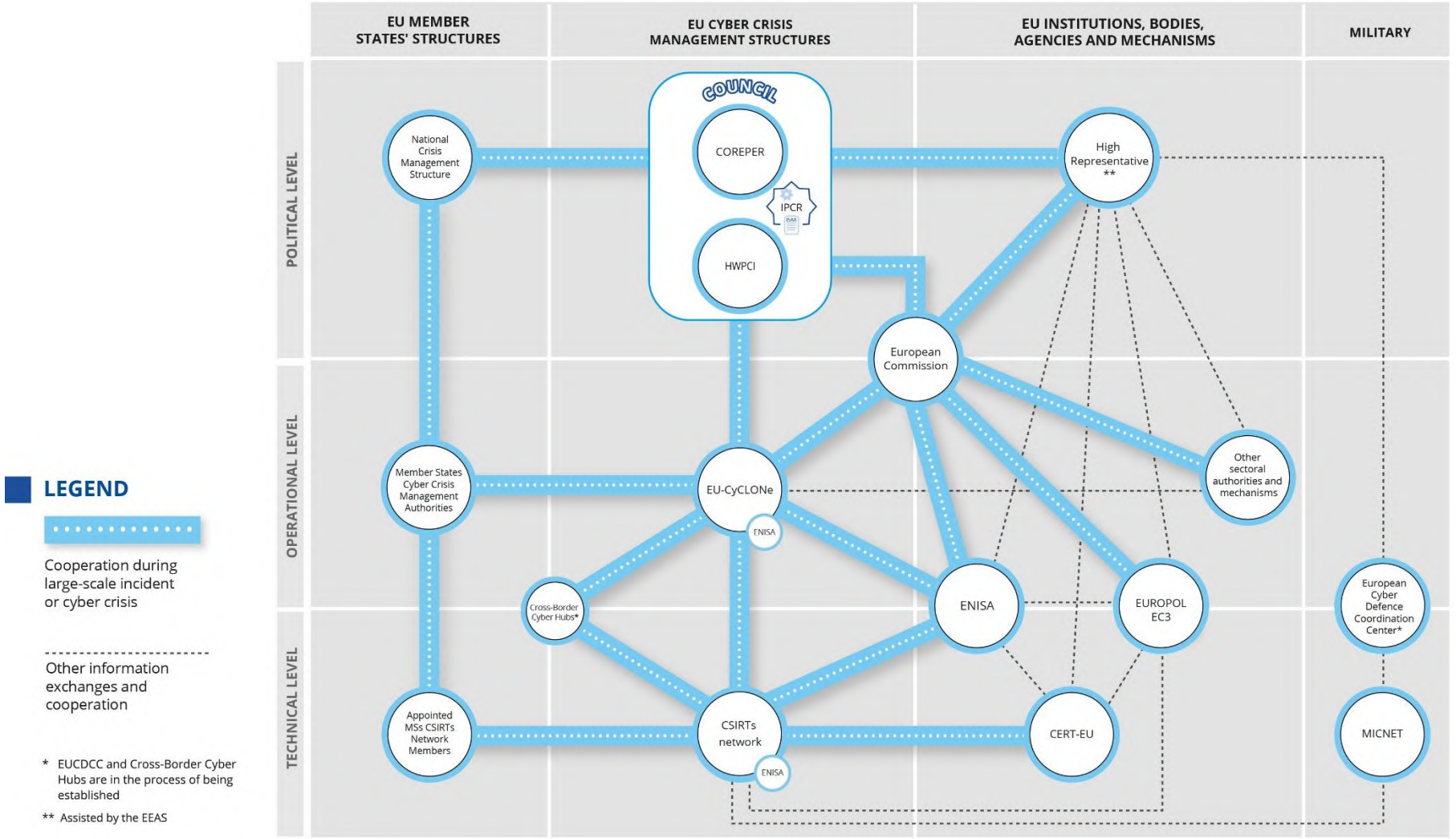
82) Komisja powinna dokonywać przeglądu niniejszego zalecenia we współpracy z państwami członkowskimi co najmniej raz na cztery lata po jego opublikowaniu. Po każdym przeglądzie Komisja powinna opublikować sprawozdanie i przedstawić je Radzie. Komisja i państwa członkowskie powinny uwzględnić w szczególności wpływ zmieniającego się krajobrazu zagrożeń, wyniki wspólnych ćwiczeń i zmiany legislacyjne, w szczególności wszelkie ewentualne zmiany wynikające ze zmiany rozporządzenia (UE) 2019/881.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady

Przewodniczący/Przewodnicząca

ZAŁĄCZNIK I – Unijny plan działania dotyczący reagowania na cyberkryzysy



ZAŁĄCZNIK II – ODPOWIEDNIE PODMIOTY (PODMIOTY I SIECI) ORAZ MECHANIZMY ZARZĄDZANIA KRYZYSOWEGO NA SZCZEBLU UNII

(1) Zaangażowanie głównych podmiotów w całym cyklu zarządzania cyberkryzysami (cyberincydenty na dużą skalę i cyberkryzysy)

	Gotowość	Wykrywanie	Reagowanie na cyberincydenty na dużą skalę i cyberkryzysy			Komunikacja ze społeczeństwem	Odzyskiwanie i wdrożone doświadczenia i wnioski
			na poziomie technicznym	na poziomie operacyjnym	na poziomie politycznym		
Państwa członkowskie	X	X	X	X	X	X	X
Komisja	X			X	X	X	
Wysoki Przedstawiciel wspierany przez ESDZ	X			X	X	X	
Rada	X				X	X	X
ENISA	X		X	X			
CERT-UE	X	X	X	X		X	X
Sieć CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Role i kompetencje odpowiednich podmiotów i mechanizmów na szczeblu Unii w odniesieniu do zarządzania cyberkryzysami (w porządku alfabetycznym)

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
CERT-UE	Techniczny/ operacyjny	Koordynuje reagowanie kryzysowe na poziomie technicznym oraz zarządzanie poważnymi incydentami mającymi wpływ na podmioty unijne. Prowadzi rejestr dostępnej fachowej wiedzy technicznej, która może być potrzebna, aby zareagować na incydenty w przypadku poważnych incydentów, oraz wspiera IICB w koordynowaniu planów zarządzania cyberkryzysami opracowywanych przez podmioty unijne na wypadek poważnych incydentów. Członek sieci CSIRT. Wspiera Komisję w ramach EU-CyCLONe w zakresie skoordynowanego zarządzania cyberincydentami na dużą skalę i cyberkryzysami. Działa jako centrum wymiany informacji na temat cyberbezpieczeństwa i koordynacji reagowania na incydenty, ułatwiając wymianę informacji na temat incydentów, cyberzagrożeń, podatności oraz potencjalnych zdarzeń dla	Rozporządzenie (UE, Euratom) 2023/2841 Rozporządzenie (UE) 2025/38

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		cyberbezpieczeństwa między podmiotami Unii a ich partnerami. Zwraca się w imieniu podmiotów unijnych o uruchomienie rezerwy cyberbezpieczeństwa UE. Współpracuje z Centrum ds. Cyberbezpieczeństwa NATO na podstawie umowy technicznej.	
Rada Unii Europejskiej	Polityczny	Funkcje związane z określaniem polityki i koordynacją. Powierzono jej IPCR, który dotyczy koordynacji i reagowania na szczeblu politycznym Unii.	Art. 16 Traktatu o Unii Europejskiej
Prezydencja Rady Unii Europejskiej	Polityczny	Podejmuje decyzję (z wyjątkiem przypadków powołania się na klauzulę solidarności na mocy art. 222 TFUE) o aktywacji lub dezaktywacji IPCR, w stosownych przypadkach po konsultacji z poszkodowanymi państwami członkowskimi, a także z Komisją i Wysokim Przedstawicielem.	Art. 16 Traktatu o Unii Europejskiej Decyzja wykonawcza Rady (UE) 2018/1993
Transgraniczne centra cyberbezpieczeństwa	Techniczny	Transgraniczne centrum cyberbezpieczeństwa to wielokrajowa platforma ustanowiona na podstawie pisemnej umowy konsorcjum, która	Rozporządzenie (UE) 2025/38

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		łączy w skoordynowanej strukturze sieciowej krajowe centra cyberbezpieczeństwa z co najmniej trzech państw członkowskich i która ma zwiększyć monitorowanie, wykrywanie i analizę cyberzagrożeń, aby zapobiegać incydentom oraz wspierać generowanie danych wywiadowczych na temat cyberzagrożeń, w szczególności poprzez wymianę odpowiednich danych i informacji, w stosownych przypadkach zanonimizowanych, a także poprzez udostępnianie najnowocześniejszych narzędzi oraz wspólne rozwijanie, w zaufanym środowisku, zdolności w zakresie wykrywania i analizy cyberataków, zapobiegania im i ochrony przed nimi; Ściśle współpracują z siecią CSIRT w celu wymiany informacji. Przekazują informacje dotyczące potencjalnego lub trwającego cyberincydentu na dużą skalę organom państw członkowskich i Komisji za pośrednictwem EU-CyCLONe i sieci CSIRT.	

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
Sieć CSIRT	Techniczny	Przyczynia się do wzrostu wzajemnego zaufania oraz promuje sprawną współpracę operacyjną między państwami członkowskimi. Jest główną siecią służącą wymianie stosownych informacji na temat incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa, cyberzagrożeń, ryzyka i podatności. Na wniosek członka, na którego może mieć wpływ incydent, sieć wymienia i omawia informacje dotyczące tego incydentu i związanych z nim cyberzagrożeń. Sieć może również ułatwić skoordynowaną reakcję na incydent zidentyfikowany w obrębie jurysdykcji członka składającego wniosek. Zapewnia państwom członkowskim pomoc w zarządzaniu incydentami transgranicznymi i bada dalsze formy współpracy, w tym wzajemną pomoc. Otrzymuje od państw członkowskich informacje dotyczące ich wniosków do rezerwy cyberbezpieczeństwa UE.	Dyrektywa (UE) 2022/2555 Rozporządzenie (UE) 2025/38

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
Konferencja dowódców ds. obrony cyberprzestrzeni		Forum dla dowódców ds. obrony cyberprzestrzeni na szczeblu krajowym w państwach członkowskich w celu współpracy i wymiany istotnych informacji na temat trwających operacji i strategii w cyberprzestrzeni na rzecz łagodzenia cyberincydentów na dużą skalę. Forum organizowane jest przez rotacyjną prezydencję Rady Unii Europejskiej przy wsparciu Europejskiej Agencji Obrony (EDA) i Europejskiej Służby Działań Zewnętrznych (ESDZ), w tym Sztabu Wojskowego Unii Europejskiej (EUMS).	Wspólny komunikat w sprawie polityki UE w zakresie cyberobrony (2022)
Komisja	Operacyjny/ polityczny	Organ wykonawczy Unii Europejskiej. Zapewnia sprawne funkcjonowanie rynku wewnętrznego. Dba o spójność i koordynację powiązanych działań w zakresie reagowania kryzysowego na szczeblu unijnym. Na podstawie decyzji w sprawie UMOL prowadzi pewne ogólne działania w zakresie gotowości na szczeblu Unii, w tym zarządza Centrum Koordynacji Reagowania Kryzysowego oraz	Art. 17 Traktatu o Unii Europejskiej Decyzja wykonawcza (UE) 2018/1993 Decyzja nr 1313/2013/UE Dyrektywa (UE) 2022/2555

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		wspólnym systemem łączności i informacji w sytuacjach nadzwyczajnych. Jest członkiem EU-CyCLONe w przypadkach, w których potencjalny lub trwający incydent na dużą skalę ma lub może mieć znaczący wpływ na usługi i działania objęte zakresem stosowania dyrektywy (UE) 2022/2555, oraz obserwatorem w innych przypadkach. Jest obserwatorem w sieci CSIRT. Ponosi ogólną odpowiedzialność za wdrożenie rezerwy cyberbezpieczeństwa UE. Działa jako punkt kontaktowy Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa do celów wymiany istotnych informacji dotyczących poważnych incydentów z EU-CyCLONe. Jest konsultowana przez prezydencję Rady w sprawie decyzji o aktywacji lub dezaktywacji IPCR (z wyjątkiem	Rozporządzenie (UE) 2025/38 Rozporządzenie (UE, Euratom) 2023/2841

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		przypadków powołania się na klauzulę solidarności na mocy art. 222 TFUE). Służby Komisji opracowują wraz z ESDZ sprawozdania ISAA.	
Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)	Techniczny/operacyjny	Wykonuje zadania w celu osiągnięcia wysokiego poziomu cyberbezpieczeństwa w całej Unii, w tym poprzez aktywne wspieranie państw członkowskich i instytucji Unii. Zapewnia sekretariat sieci CSIRT i EU-CyCLONe. Przygotowuje regularny raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i cyberzagrożeń (z EC3 i CERT-UE oraz w ścisłej współpracy z państwami członkowskimi). Pomaga w opracowaniu wspólnej reakcji na transgraniczne incydenty na dużą skalę lub kryzysy przede wszystkim poprzez: - agregowanie i analizę sprawozdań ze źródeł krajowych; - zapewnianie przepływu informacji między poziomem technicznym, operacyjnym i politycznym;	Dyrektywa (UE) 2022/2555 Rozporządzenie (UE) 2019/881 Rozporządzenie (UE) 2025/38 Rozporządzenie (UE) 2024/2847

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		- ułatwianie, na wniosek, postępowania w przypadku incydentów; - wspieranie podmiotów unijnych w komunikacji ze społeczeństwem; - wspieranie państw członkowskich, na ich wniosek, w zakresie komunikacji ze społeczeństwem; - testowanie zdolności reagowania na incydenty i regularne organizowanie ćwiczeń w zakresie cyberbezpieczeństwa. Pełni rolę instytucji zamawiającej, jeżeli powierzono jej pełne lub częściowe zarządzanie rezerwą cyberbezpieczeństwa UE. Co dwa lata organizuje kompleksowe ćwiczenia w zakresie cyberbezpieczeństwa na szczeblu Unii, obejmujące elementy techniczne, operacyjne lub strategiczne. We współpracy z zainteresowanym państwem członkowskim i innymi odpowiednimi zainteresowanymi stronami przygotowuje sprawozdanie z przeglądu incydentu w celu oceny przyczyn i skutków incydentu i środków łagodzących go (na wniosek Komisji lub EU-CyCLONe i za zgodą	

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		zainteresowanego państwa członkowskiego). Informuje EU-CyCLONe, jeżeli informacje przekazane na podstawie obowiązków sprawozdawczych określonych w akcie dotyczącym cyberodporności są istotne dla skoordynowanego zarządzania cyberincydentami na dużą skalę i cyberkryzysami na poziomie operacyjnym.	
Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe)	Operacyjny	Wspiera skoordynowane zarządzanie cyberincydentami na dużą skalę i cyberkryzysami na poziomie operacyjnym. Zapewnia regularną wymianę istotnych informacji między państwami członkowskimi oraz instytucjami, organami i jednostkami organizacyjnymi Unii. Koordynuje zarządzanie cyberincydentami na dużą skalę i cyberkryzysami oraz wspiera proces decyzyjny na szczeblu politycznym w odniesieniu do takich incydentów i kryzysów.	Dyrektywa (UE) 2022/2555 Rozporządzenie (UE) 2025/38

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		Ocenia konsekwencje i wpływ istotnych cyberincydentów na dużą skalę i cyberkryzysów oraz proponuje możliwe środki łagodzące. Omawia – na wniosek zainteresowanego państwa członkowskiego krajowe plany reagowania na cyberincydenty na dużą skalę i cyberkryzysy. Opracowuje, wraz z ENISA i Komisją, wzór ułatwiający składanie wniosków o wsparcie z rezerwy cyberbezpieczeństwa UE. Otrzymuje od państw członkowskich informacje dotyczące ich wniosków do rezerwy cyberbezpieczeństwa UE. Otrzymuje informacje dotyczące potencjalnego lub trwającego cyberincydentu na dużą skalę od transgranicznych centrów cyberbezpieczeństwa lub sieci CSIRT.	
Wysoki Przedstawiciel Unii do spraw Zagranicznych i Polityki Bezpieczeństwa	Polityczny	Kieruje wysiłkami Unii mającymi na celu przeciwdziałanie zewnętrznym zagrożeniom bezpieczeństwa w obszarach zagrożeń hybrydowych i cybernetycznych i koordynuje te wysiłki.	Decyzja Rady 2010/427/UE

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
wspierany przez Europejską Służbę Działań Zewnętrznych		Odpowiada za instrumenty unijnej dyplomacji cyfrowej i cyberobrony w celu powstrzymywania zagrożeń zewnętrznych i reagowania na nie, w tym za pomocą unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym i zestawu narzędzi dla dyplomacji cyfrowej. Współpracuje z partnerami zewnętrznymi, w tym również poprzez zaangażowanie w ramach WPBiO. Zapewnia gotowość Unii i państw członkowskich w zakresie orientacji sytuacyjnej i zdolności reagowania na zagrożenia hybrydowe i cyberzagrożenia, na przykład poprzez ćwiczenia praktyczne, szkolenia i sieci. Zajmuje się wpływem unijnych zasobów kosmicznych na bezpieczeństwo i obronę, zwłaszcza w ramach unijnej wspólnej polityki bezpieczeństwa i obrony (WPBiO). Wspiera konferencję unijnych dowódców ds. obrony cyberprzestrzeni. Wspiera unijną operacyjną sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET).	

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
		Jest konsultowany przez prezydencję Rady w sprawie decyzji o aktywacji lub dezaktywacji IPCR (z wyjątkiem przypadków powołania się na klauzulę solidarności na mocy art. 222 TFUE). ESDZ opracowuje wraz ze służbami Komisji sprawozdania ISAA.	
Centrum Koordynacji UE ds. Cyberobrony	Horyzontalny	Podstawowym celem jest przede wszystkim zwiększenie wspólnej orientacji sytuacyjnej Unii i jej państw członkowskich w zakresie szkodliwych działań w cyberprzestrzeni, w szczególności w odniesieniu do wojskowych misji i operacji w ramach WPBiO.	Wspólny komunikat w sprawie polityki UE w zakresie cyberobrony (2022)
Europol	Operacyjny	Zapewnia wsparcie operacyjne i techniczne właściwym organom państw członkowskich w zakresie zapobiegania cyberprzestępczości i przeciwdziałania jej. Udziela właściwym organom państw członkowskich, na ich wniosek, pomocy w podejmowaniu działań w odpowiedzi na podejrzenie popełnienia przestępstwa cyberataku.	Rozporządzenie (UE) 2016/794, ze wszystkimi zmianami

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa		Ustanawia plan zarządzania cyberkryzysami w celu wsparcia – na poziomie operacyjnym – skoordynowanego zarządzania poważnymi incydentami mającymi wpływ na podmioty unijne oraz w celu przyczynienia się do regularnej wymiany istotnych informacji. Koordynuje przyjmowanie planów zarządzania cyberkryzysami poszczególnych podmiotów unijnych. Przyjmuje, na podstawie wniosku CERT-UE, wytyczne lub zalecenia dotyczące współpracy w zakresie reagowania na incydenty w przypadku poważnych incydentów dotyczących podmiotów unijnych.	Rozporządzenie (UE, Euratom) 2023/2841
Operacyjna sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET)	Techniczny	Wspiera bardziej solidne i skoordynowane reagowanie na cyberzagrożenia mające wpływ na systemy obronne w Unii, w tym systemy wykorzystywane w misjach i operacjach wojskowych w ramach WPBiO; przy wsparciu Europejskiej Agencji Obrony.	Wspólny komunikat z 2022 roku w sprawie cyberobrony

Podmiot	Poziom	Rola i kompetencje	Podstawa prawna
Pojedyncza komórka analiz wywiadowczych (SIAC)		Składa się z (1) Centrum Analiz Wywiadowczych UE (Intcen) oraz (2) Dyrekcji ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT). Dostarcza strategicznych danych wywiadowczych na temat polityki zagranicznej, terroryzmu oraz cyberzagrożeń i zagrożeń hybrydowych. Zajmuje się wywiadem wojskowym na potrzeby misji WPBiO oraz wspiera unijne operacje obrony i zarządzania kryzysowego. Pod zwierzchnictwem Wysokiego Przedstawiciela.	Art. 38 i 42–46 Traktatu o Unii Europejskiej

(3) Istotne mechanizmy i platformy zarządzania kryzysowego na szczeblu Unii

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
ARGUS	Horyzontalny	Proces koordynacji i ogólny system ostrzegania stosowany przez Komisję w celu zapewnienia spójnej reakcji w przypadku poważnego kryzysu transgranicznego wymagającego działań na szczeblu UE. Skupia wszystkie właściwe służby i gabinety w celu podejmowania decyzji w sprawie środków i ich koordynowania. Umożliwia Komisji wymianę istotnych informacji na temat pojawiających się wielosektorowych sytuacji kryzysowych lub przewidywalnych lub bezpośrednich zagrożeń, które wymagają działań na szczeblu Unii.	Komunikat Komisji (2005)662
Centrum Reagowania Kryzysowego ESDZ (CRC)	Horyzontalny	Pojedynczy punkt kontaktowy w ESDZ dla wszystkich kwestii związanych z sytuacjami kryzysowymi oraz całodobowe stałe zdolności reagowania kryzysowego w sytuacjach nadzwyczajnych zagrażających bezpieczeństwu personelu w delegaturach UE lub	Strategiczny kompas na rzecz bezpieczeństwa i obrony – dla Unii Europejskiej, która chroni swoich obywateli, swoje wartości i interesy oraz przyczynia się do międzynarodowego pokoju

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
		w reakcji na sytuacje kryzysowe dotykające obywateli Unii za granicą. Skupia ekspertów ds. bezpieczeństwa, ekspertów konsularnych i ekspertów ds. orientacji sytuacyjnej, a jednocześnie polega na zaangażowanych specjalistach w terenie w delegaturach Unii.	i bezpieczeństwa, 21 marca 2022 r.
Plan dotyczący infrastruktury krytycznej	Horyzontalny	Koordynuje reakcję na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej o istotnym znaczeniu transgranicznym.	Zalecenie Rady C/2024/4371
System ostrzeżeń dotyczących cyberbezpieczeństwa	Związany z cyberbezpieczeństwem	Zapewnia zaawansowane zdolności Unii w zakresie zwiększania zdolności dotyczących wykrywania, analizy i przetwarzania danych w odniesieniu do cyberzagrożeń oraz zapobiegania incydentom w Unii.	Rozporządzenie (UE) 2025/38
Zestaw narzędzi dla dyplomacji cyfrowej (ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni)	Związany z cyberbezpieczeństwem	Umożliwia wspólną reakcję dyplomatyczną Unii na szkodliwe działania w cyberprzestrzeni, przyczyniając się do zapobiegania konfliktom, łagodzenia cyberzagrożeń i większej stabilności w stosunkach międzynarodowych.	Konkluzje Rady z dnia 19 czerwca 2017 r. Zmienione wytyczne wykonawcze, dok. 10289/23 z 8 czerwca 2023 r.

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
Rezerwa cyberbezpieczeństwa UE	Związany z cyberbezpieczeństwem	Mobilizuje ekspertów ds. cyberbezpieczeństwa i zasoby w sytuacjach kryzysowych w celu wsparcia reagowania w państwach członkowskich, instytucjach, organach i jednostkach organizacyjnych Unii.	Rozporządzenie (UE) 2025/38
Kodeks sieci dotyczący zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej	Sektorowy	Ustanawia cykliczny proces ocen ryzyka w cyberprzestrzeni w sektorze energii elektrycznej, na szczeblu Unii, państw członkowskich, regionów i podmiotów. Zawiera zasady dotyczące zarządzania kryzysowego oraz współpracy z siecią CSIRT i EU-CyCLONe w przypadkach, gdy cyberincydent na dużą skalę ma wpływ na inne sektory uzależnione od bezpieczeństwa dostaw energii elektrycznej.	Rozporządzenie delegowane Komisji (UE) 2024/1366
Unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym	Horyzontalny	Zawiera zestaw przepisów mających na celu zapewnienie przeglądu dostępnych na poziomie UE środków odpowiedzi na wszelkiego rodzaju zagrożenia hybrydowe oraz skoordynowane wykorzystanie tych środków, przy jednoczesnym zapewnieniu spójności działań UE w różnych	Konkluzje Rady w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe, 22 czerwca 2022 r. Wytyczne wykonawcze dotyczące ram skoordynowanej

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
		obszarach. Zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym pomaga zapewnić podejmowanie decyzji w oparciu o kompleksową orientację sytuacyjną i wdrożone doświadczenia i wnioski.	reakcji UE na kampanie hybrydowe, 14 grudnia 2022 r.
Zespoły szybkiego reagowania na zagrożenia hybrydowe (EU HRRT)	Horyzontalny	W ramach unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym zespoły szybkiego reagowania na zagrożenia hybrydowe korzystają z odpowiedniej krajowej i unijnej cywilnej i wojskowej wiedzy sektorowej, aby zapewnić dostosowaną i ukierunkowaną pomoc krótkoterminową państwom członkowskim, misjom i operacjom w ramach wspólnej polityki bezpieczeństwa i obrony oraz krajom partnerskim w przeciwdziałaniu zagrożeniom i kampaniom hybrydowym.	Ramy przewodnie na rzecz praktycznego utworzenia unijnych zespołów szybkiego reagowania na zagrożenia hybrydowe, 21 maja 2024 r. Wytyczne operacyjne dotyczące rozmieszczenia zespołów szybkiego reagowania na zagrożenia hybrydowe, zatwierdzone przez Coreper 4 grudnia 2024 r.
IPCR	Horyzontalny	Wspiera szybkie i skoordynowane podejmowanie decyzji na poziomie politycznym w Unii w przypadku poważnych	Decyzja wykonawcza Rady (UE) 2018/1993

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
		i złożonych sytuacji kryzysowych. Decyzję o aktywacji i dezaktywacji podejmuje prezydencja Rady, która konsultuje się (z wyjątkiem przypadków powołania się na klauzulę solidarności) z poszkodowanymi państwami członkowskimi, Komisją i Wysokim Przedstawicielem. Sekretariat Generalny Rady, służby Komisji i ESDZ mogą również uzgodnić, w porozumieniu z prezydencją, aktywizację IPCR w trybie wymiany informacji. Podstawą prac IPCR są sprawozdania ISAA opracowywane przez służby Komisji i ESDZ. Sprawozdania te opierają się na istotnych informacjach i analizach dostarczanych przez państwa członkowskie (np. z odpowiednich krajowych centrów kryzysowych) oraz przez właściwe agencje i organy Unii.	
Protokół działań UE w zakresie egzekwowania prawa	Horyzontalny	Narzędzie wspierające organy ścigania w Unii w zapewnianiu natychmiastowej reakcji na	Konkluzje Rady w sprawie skoordynowanego reagowania na

Mechanizm	Horyzontalny/ sektorowy/ związany z cyberbezpieczeństwem	Opis	Podstawa prawna
w sytuacjach kryzysowych		poważne transgraniczne cyberataki poprzez szybką ocenę, bezpieczną i terminową wymianę krytycznych informacji oraz skuteczną koordynację międzynarodowych aspektów prowadzonych przez nie postępowań przygotowawczych.	szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę, 26 czerwca 2018 r.
Zespoły szybkiego reagowania na cyberincydenty (CRRT) w ramach PESCO	Związany z cyberbezpieczeństwem	CRRT w ramach stałej współpracy strukturalnej (PESCO) to wspólnie rozwinięta cywilno-wojskowa zdolność cyberobrony państw członkowskich UE do szybkiego reagowania na cyberincydenty i cyberkryzysy, a także do prowadzenia działań zapobiegawczych, takich jak oceny podatności na zagrożenia i monitorowanie wyborów. Misją CRRT w ramach PESCO jest zapewniać, na wniosek, wsparcie w zakresie cyberbezpieczeństwa państwom członkowskim UE, instytucjom, organom i agencjom UE, misjom i operacjom wojskowym UE w dziedzinie WPBiO, a także krajom partnerskim.	Art. 42 ust. 6, art. 46 i protokół 10 Traktatu o Unii Europejskiej

Struktura reagowania na zagrożenia w przestrzeni kosmicznej (STRA)	Sektorowy (Zagrożenia w przestrzeni kosmicznej, w tym zagrożenia związane z cyberbezpieczeństwem)	Struktura reagowania na zagrożenia w przestrzeni kosmicznej (STRA) dotycząca obowiązków spoczywających na Radzie i Wysokim Przedstawicielu w celu oddalenia zagrożeń wynikających z wdrażania, udostępniania lub użytkowania systemów utworzonych lub usług świadczonych w ramach Unijnego programu kosmicznego.	Decyzja Rady (WPZiB) 2021/698
Ramy koordynacji w odniesieniu do cyberincydentów o charakterze systemowym (EU-SCICF)	Sektorowy	Opracowywane jeszcze ramy komunikacji i koordynacji na potrzeby zarządzania zdarzeniami związanymi z cyberbezpieczeństwem o potencjalnie systemowym charakterze w sektorze finansowym. Ramy te będą się opierać na jednej z przewidzianych w rozporządzeniu (UE) 2022/2554 ról Europejskich Urzędów Nadzoru, polegającej na stopniowym umożliwianiu skutecznej skoordynowanej reakcji na szczeblu Unii w przypadku poważnego transgranicznego incydentu związanego z technologiami informacyjno-komunikacyjnymi (ICT) lub związanego z nim zagrożenia mającego systemowy wpływ na cały sektor finansowy Unii.	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)
Unijny Mechanizm Ochrony Ludności (UMOL)	Horyzontalny	Zapewnia współpracę w zakresie ochrony ludności w celu lepszego zapobiegania klęskom żywiołowym, większej gotowości na ich wystąpienie i skuteczniejszego reagowania na nie.	Decyzja 1313/2013/UE
CISE – wspólny mechanizm	Specyfika morska	CISE to sieć łącząca systemy organów UE/EOG odpowiedzialnych	Strategiczny kompas na rzecz

wymiany informacji	obejmująca siedem sektorów	za nadzór morski. CISE umożliwia sprawną i zautomatyzowaną wymianę istotnych informacji w wymiarze transgranicznym i pomiędzy różnymi sektorami.	bezpieczeństwa i obrony – dla Unii Europejskiej, która chroni swoich obywateli, swoje wartości i interesy oraz przyczynia się do międzynarodowego pokoju i bezpieczeństwa, 21 marca 2022 r.

(4) Sektory kluczowe i inne sektory krytyczne na podstawie dyrektywy (UE) 2022/2555 oraz sektorowe mechanizmy kryzysowe na szczeblu Unii (w stosownych przypadkach)		
Sektory	**Podsektor**	**Obowiązujące sektorowe mechanizmy kryzysowe**
Energetyka	Energia elektryczna	Grupa Koordynacyjna ds. Energii Elektrycznej
	Systemy ciepłownicze i chłodnicze	Nie dotyczy
	Ropa naftowa	Grupa Koordynacyjna ds. Ropy Naftowej i Produktów Ropopochodnych Unijna grupa organów ds. wydobycia ropy naftowej i gazu ziemnego ze złóż podmorskich (EUOAG)
	Gaz	Grupa Koordynacyjna ds. Gazu
	Wodór	Nie dotyczy
Transport	Transport lotniczy	Europejska Komórka Koordynacji Kryzysowej ds. Lotnictwa (EACCC)
	Transport kolejowy	Nie dotyczy
	Transport wodny	Europejska Agencja Kontroli Rybołówstwa (EFCA) SafeSeaNet (SSN) Zintegrowane usługi morskie (IMS) System dalekiego zasięgu do identyfikacji i śledzenia statków (LRIT) Usługi wsparcia morskiego EMSA

	Transport drogowy	Nie dotyczy
	Horyzontalny	Sieć punktów kontaktowych ds. transportu, ustanowiona w ramach Planu awaryjnego dla transportu (COM(2022) 211)
Bankowość		EU-SCICF
Infrastruktura rynków finansowych		EU-SCICF Europejski mechanizm stabilizacji finansowej

Opieka zdrowotna		System wczesnego ostrzegania i reagowania (EWRS) Instrument operacyjny w nadzwyczajnych sytuacjach zdrowotnych (HEOF) system wczesnego ostrzegania dotyczący tkanek i komórek oraz składników krwi (RATC/RAB) Ramy na wypadek stanu zagrożenia zdrowia publicznego System wczesnego ostrzegania o incydentach chemicznych (RASCHEM) Europejski portal nadzoru nad chorobami zakaźnymi Urząd ds. Gotowości i Reagowania na Stany Zagrożenia Zdrowia (HERA) System informacji medycznej i na temat zdrowia (MediSys) Wykonawcza Grupa Sterująca ds. Wyrobów Medycznych (MDSSG) System wczesnego ostrzegania w zakresie nadzoru nad bezpieczeństwem farmakoterapii Grupa Zadaniowa UE ds. Zdrowia (EUHTF) Komitet ds. Bezpieczeństwa Zdrowia
Woda pitna		Nie dotyczy

Ścieki		Nie dotyczy
Infrastruktura cyfrowa		Nie dotyczy
Zarządzanie usługami ICT		Nie dotyczy
Administracja publiczna		Nie dotyczy
Przestrzeń kosmiczna		Struktura reagowania na zagrożenia w przestrzeni kosmicznej (STRA)
Usługi pocztowe i kurierskie		Nie dotyczy
Gospodarowanie odpadami		Nie dotyczy
Produkcja, wytwarzanie i dystrybucja chemikaliów		System wczesnego ostrzegania o incydentach chemicznych (RASCHEM)

Produkcja, przetwarzanie i dystrybucja żywności		Europejski system monitorowania upraw Globalne wykrywanie anomalii w produkcji rolnej (ASAP) Europejska sieć systemów informacji o zdrowiu roślin (EUROPHYT) Unijny weterynaryjny zespół kryzysowy (EUVET) System wczesnego ostrzegania o niebezpiecznej żywności i paszach (RASFF) Europejski mechanizm gotowości i reagowania na kryzysy związane z bezpieczeństwem żywnościowym (EFSCM) Akt o sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego (IMERA)
Produkcja	Wyroby medyczne	Nie dotyczy
	Komputery, wyroby elektroniczne i optyczne	Nie dotyczy
	Maszyny i urządzenia	Nie dotyczy
	Produkcja pojazdów samochodowych, przyczep i naczep	Nie dotyczy
	Produkcja pozostałego sprzętu transportowego	Nie dotyczy

Dostawcy usług cyfrowych		Nie dotyczy
Badania naukowe		Nie dotyczy

ZAŁĄCZNIK III – Unijne ramy zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa i powiązane instrumenty

Od 2017 r. Unia rozwinęła swoje ramy cyberbezpieczeństwa za pomocą szeregu instrumentów, które zawierają przepisy istotne dla zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa:

- rozporządzenie Parlamentu Europejskiego i Rady (EU) 2019/881[1],
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555[2],
- rozporządzenie wykonawcze Komisji (UE) 2024/2690[3], rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841[4],
- rozporządzenie Parlamentu Europejskiego i Rady (EU) 2021/887[5],
- rozporządzenie Parlamentu Europejskiego i Rady (EU) 2024/2847[6], oraz
- rozporządzenie Parlamentu Europejskiego i Rady (EU) 2025/38 (akt w sprawie cybersolidarności)[7].

Szczególne sektorowe środki dotyczące cyberkryzysów obejmują rozporządzenie delegowane Komisji (UE) 2024/1366[8] oraz przyszłe ramy koordynacji w odniesieniu do cyberincydentów o charakterze systemowym (EU-SCICF) w kontekście rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554[9].

Dyrektywa 2013/40/UE[10] stanowi odniesienie, jeśli chodzi o definiowanie działalności przestępczej związanej z cyberatakami, a unijne przepisy dotyczące transgranicznego dostępu do elektronicznego materiału dowodowego, w szczególności rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543[11], gdy tylko zostanie wdrożone, znacznie ułatwi działania organów ścigania w tej dziedzinie.

W polityce UE w zakresie cyberobrony[12] określono role unijnej operacyjnej sieci dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET) i unijnej konferencji dowódców ds. obrony cyberprzestrzeni oraz przewidziano utworzenie Centrum Koordynacji UE ds. Cyberobrony (EUCDCC).

W niektórych sektorach krytycznych wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 istnieją inne niezwiązane z cyberbezpieczeństwem mechanizmy orientacji sytuacyjnej i reagowania kryzysowego.

Zalecenie Rady w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne[13] przewiduje współpracę między odpowiednimi podmiotami w przypadku incydentu mającego wpływ zarówno na aspekty fizyczne, jak i na cyberbezpieczeństwo infrastruktury krytycznej.

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

[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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz.U. L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii (Dz.U. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

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

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności

w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie zagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności), Dz.U. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

[8] Rozporządzenie delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz.U. L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191 z 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022JC0049

[13] *Dz.U. C, C/2024/4371, 5.7.2024*. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:C_202404371