KOMISJA
EUROPEJSKA

Bruksela, dnia 24.2.2025 r.
COM(2025) 66 final

2025/0036 (NLE)

Wniosek

ZALECENIE RADY

w sprawie planu działania UE na rzecz zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Rada w swoich konkluzjach w sprawie przyszłości cyberbezpieczeństwa z 22 maja 2024 r.

> „[wezwała] Komisję do szybkiej oceny obecnego planu działania na rzecz cyberbezpieczeństwa i do zaproponowania na tej podstawie zmienionego planu działania na rzecz cyberbezpieczeństwa w formie zalecenia Rady, który uwzględni obecne wyzwania i złożony krajobraz zagrożeń cyberbezpieczeństwa, wzmocni istniejące sieci, zwiększy współpracę i zniesie bariery między organizacjami z wykorzystaniem przede wszystkim istniejących struktur. Ponadto zmieniony plan działania powinien opierać się na sprawdzonych w praktyce zasadach przewodnich współpracy (proporcjonalność, pomocniczość, komplementarność i poufność informacji) i rozszerzyć je na pełny cykl zarządzania kryzysowego, a także powinien przyczynić się do ujednolicenia i poprawy bezpiecznej komunikacji w dziedzinie cyberbezpieczeństwa. Zmieniony plan działania powinien zapewnić zgodność z istniejącymi ramami, takimi jak IPCR, unijny zestaw narzędzi dla dyplomacji cyfrowej, unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym, protokół działań UE w zakresie egzekwowania prawa w sytuacjach kryzysowych (LERP), powstającymi ramami, takimi jak plan dotyczący infrastruktury krytycznej, procedurami sektorowymi oraz ogólnymi strukturami zarządzania kryzysowego w ramach podmiotów Unii, w tym również z udziałem Wysokiego Przedstawiciela i Europolu. W tym zmienionym planie rola Komisji, Wysokiego Przedstawiciela i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), zgodnie z ich kompetencjami, powinna koncentrować się w szczególności na wspieraniu koordynacji horyzontalnej”.

Celem niniejszego projektu zalecenia Rady w sprawie unijnego planu działania na rzecz zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa (plan na rzecz cyberbezpieczeństwa) jest przedstawienie, w jasny, prosty i przystępny sposób, unijnych ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa Plan na rzecz cyberbezpieczeństwa powinien umożliwiać odpowiednim podmiotom Unii (tj. poszczególnym podmiotom i sieciom podmiotów na szczeblu Unii) zrozumienie, w jaki sposób współdziałać i jak najlepiej wykorzystywać dostępne mechanizmy w całym cyklu zarządzania kryzysowego. Jego celem jest wyjaśnienie, czym jest kryzys cyberbezpieczeństwa i co uruchamia mechanizm zarządzania kryzysami cyberbezpieczeństwa na szczeblu Unii. Wyjaśniono w nim wykorzystanie dostępnych mechanizmów, takich jak mechanizm cyberkryzysowy, w tym rezerwa cyberbezpieczeństwa UE, w przygotowywaniu sposobów zarządzania kryzysem wynikającym z incydentu w cyberbezpieczeństwie na dużą skalę, reagowania na niego i przezwyciężania jego skutków. Ponadto plan ma na celu wspieranie bardziej zorganizowanej współpracy między podmiotami cywilnymi i wojskowymi, w tym współpracy z Organizacją Traktatu Północnoatlantyckiego (NATO), biorąc pod uwagę, że incydent w cyberbezpieczeństwie na dużą skalę mający wpływ na unijną infrastrukturę cywilną, na której może polegać wojsko, może również uruchomić mechanizmy reagowania NATO.

Plan na rzecz cyberbezpieczeństwa jest niewiążącym instrumentem, w którym określono konkretne działania odpowiednich podmiotów w sytuacji kryzysu cyberbezpieczeństwa i który może zwiększyć ogólną skuteczność ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa. Zaktualizowano w nim plan działania określony w zaleceniu Komisji (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę oraz wykorzystano wyniki i wnioski wyciągnięte z ćwiczeń na

szczeblu unijnym od czasu przyjęcia tego zalecenia. Jest to część szerszych priorytetów politycznych w dziedzinie gotowości i bezpieczeństwa.

Zgodnie z definicją zawartą w dyrektywie (UE) 2022/2555 (dyrektywa NIS 2), incydent w cyberbezpieczeństwie 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. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwe sytuacje kryzysowe uniemożliwiające 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.

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

Projekt jest spójny z odpowiednimi instrumentami Unii w dziedzinie cyberbezpieczeństwa, w szczególności z dyrektywą NIS 2 oraz rozporządzeniem (UE) 2023/2841 w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii. Jest on również spójny z ramami Unijnego Mechanizmu Ochrony Ludności (UMOL), ustanowionego decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE, z decyzją wykonawczą (UE) 2018/1993 w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) oraz z sektorowymi instrumentami orientacji sytuacyjnej i zarządzania kryzysowego, w tym w sektorze energii elektrycznej.

- **Spójność z innymi politykami Unii**

Plan na rzecz cyberbezpieczeństwa uzupełnia niedawno przyjęte zalecenie Rady w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mającej istotne znaczenie transgraniczne i jest z nim spójny, ponieważ zalecenie to obejmuje zakłócenia związane z odpornością fizyczną niezwiązane z cyberbezpieczeństwem. Plan pozostaje też w ścisłym związku z mechanizmami i narzędziami zarządzania kryzysowego w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB) oraz Wspólnej Polityki Bezpieczeństwa i Obrony (WPBiO), jak określono w opracowanym przez Radę Strategicznym kompasie na rzecz bezpieczeństwa i obrony. Ponadto cele niniejszego zalecenia mogą wspierać unijne inicjatywy na rzecz zwalczania cyberprzestępczości.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawą wniosku jest art. 292 TFUE, w którym określono odpowiednie przepisy dotyczące przyjmowania zaleceń.

Wniosek stanowiłby uzupełnienie całych ram prawnych dotyczących cyberbezpieczeństwa ustanowionych na szczeblu Unii. Wniosek nie dotyczy zarządzania poważnymi incydentami mającymi wpływ na podmioty Unii w rozumieniu rozporządzenia 2023/2841 przyjętego na podstawie art. 298 TFUE. Dotyczy on jednak wymiany informacji między podmiotami Unii a państwami członkowskimi, w tym przepisów rozporządzenia (UE) 2023/2841 dotyczących przedstawiciela Komisji w Międzyinstytucjonalnej Radzie ds. Cyberbezpieczeństwa (IICB), który ma być punktem kontaktowym ułatwiającym IICB wymianę istotnych informacji dotyczących poważnych incydentów z europejską siecią organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa EU-CyCLONe i wnosić tym samym wkład we wspólną orientację sytuacyjną.

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

Podczas gdy za reagowanie na zakłócenia w funkcjonowaniu infrastruktury krytycznej lub usług świadczonych przez kluczowe i ważne podmioty odpowiadają przede wszystkim państwa członkowskie, niektóre szkodliwe działania w cyberprzestrzeni o charakterze transgranicznym mogą zakłócać i niszczyć krytyczną infrastrukturę informacyjną, od której zależy sprawne funkcjonowanie rynku wewnętrznego. W związku z tym Unia odgrywa ważną rolę w przypadku poważnego incydentu lub poważnej sytuacji kryzysowej. Takie zakłócenie może mieć wpływ na szereg obszarów działalności gospodarczej w obrębie jednolitego rynku lub nawet na wszystkie te obszary, jak również na bezpieczeństwo i stosunki międzynarodowe Unii. W celu zapewnienia funkcjonowania rynku wewnętrznego koordynacja na szczeblu Unii w przypadku zakłóceń infrastruktury krytycznej o znaczących skutkach transgranicznych jest nie tylko odpowiednia, ale również konieczna. Skoordynowane reakcje na poziomie Unii będą wspierać reagowanie państw członkowskich na zakłócenia poprzez wspólną orientację sytuacyjną, skoordynowaną komunikację publiczną i łagodzenie skutków zakłóceń na rynku wewnętrznym.

- **Proporcjonalność**

Niniejszy wniosek jest zgodny z zasadą proporcjonalności, o której mowa w art. 5 ust. 4 Traktatu o Unii Europejskiej. Ani treść, ani forma zalecenia Rady, którego dotyczy niniejszy wniosek, nie wykraczają poza to, co jest konieczne do osiągnięcia jego celów. Proponowane działania są proporcjonalne do zamierzonych celów, które koncentrują się na zapewnieniu skoordynowanego unijnego zarządzania kryzysami cyberbezpieczeństwa.

- **Wybór instrumentu**

Aby osiągnąć cele, o których mowa powyżej, TFUE przewiduje, zwłaszcza w art. 292, przyjęcie przez Radę zaleceń na podstawie wniosku Komisji. Zgodnie z art. 288 TFUE zalecenia nie mają mocy wiążącej. Zalecenie Rady jest w tym przypadku odpowiednim instrumentem, ponieważ sygnalizuje zobowiązanie państw członkowskich na rzecz zawartych w nim środków i stanowi solidną podstawę współpracy w zakresie koordynacji zarządzania incydentami w cyberbezpieczeństwie i kryzysami cyberbezpieczeństwa na dużą skalę. W ten sposób proponowane zalecenie stanowiłoby uzupełnienie wiążących ram prawnych (w szczególności dyrektywy NIS 2).

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

- **Konsultacje z zainteresowanymi stronami**

Opracowując niniejszy wniosek, Komisja skonsultowała się w sprawie przeglądu planu na rzecz cyberbezpieczeństwa i zwróciła się do państw członkowskich i odpowiednich podmiotów Unii o przekazanie informacji. Komisja uwzględniła opinie ekspertów z państw członkowskich oraz ENISA wyrażone podczas warsztatów zorganizowanych 5 września 2024 r. w Karpaczu przez Komisję i Polskę.

Komisja skonsultowała się z przedstawicielami państw członkowskich w sieci CSIRT, EU-CyCLONe i grupie współpracy NIS na posiedzeniach we wrześniu 2024 r. i zwróciła się o przedstawienie pisemnych uwag.

Komisja przedstawiła i zgromadziła informacje zwrotne od Rady podczas dwóch specjalnych dyskusji na forum Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni, które odbyły się w październiku i listopadzie 2024 r.

Podczas warsztatów zorganizowanych przez polskie Stałe Przedstawicielstwo przy UE w listopadzie 2024 r. w Brukseli Komisja skonsultowała się z przedstawicielami sektora prywatnego, a także z państwami członkowskimi, Europejską Służbą Działań Zewnętrznych (ESDZ) i ENISA.

Komisja skonsultowała się z odpowiednimi podmiotami Unii, a mianowicie z ESDZ, ENISA, Europolem i CERT-UE, w tym poprzez dyskusje na wysokim szczeblu na posiedzeniach grupy zadaniowej ds. cyberkryzysów[1], które to posiedzenia odbyły się w lipcu i listopadzie 2024 r.

Osiągnięto konsensus co do potrzeby opracowania aktualnego, jasnego, prostego i operacyjnego dokumentu, który umożliwi odpowiednim podmiotom zrozumienie ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa i skuteczne wykorzystanie dostępnych mechanizmów. Uzgodniono również, że należy unikać powielania instrumentów oraz efektywnie wykorzystywać istniejące unijne mechanizmy w zakresie koordynacji, wymiany informacji i reagowania, nie tworząc przy tym nowych struktur ani nie ingerując w wewnętrzne standardowe procedury operacyjne istniejących sieci i sektorowych mechanizmów.

[1] Nieformalna grupa złożona ze służb Komisji i innych służb UE.

2025/0036 (NLE)

Wniosek

ZALECENIE RADY

w sprawie planu działania UE na rzecz zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 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 incydentów w cyberbezpieczeństwie 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 wielowymiarowych zagrożeń 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) Incydent w cyberbezpieczeństwie na dużą skalę może powodować poziom zakłócenia przekraczający zdolność danego państwa członkowskiego do reagowania na nie lub wywierać znaczące skutki w co najmniej dwóch państwach członkowskich. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwe sytuacje kryzysowe uniemożliwiające 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, obywateli i przedsiębiorstw, a także przyczynia się do międzynarodowego bezpieczeństwa i stabilności w cyberprzestrzeni. Zarządzanie kryzysami cyberbezpieczeństwa stanowi zatem integralną część nadrzędnych unijnych ram zarządzania kryzysowego.

(3) Zgodnie z procedurami określonymi w decyzji wykonawczej Rady (UE) 2018/1993[2] decyzję o aktywacji i dezaktywacji zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) podejmuje

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

prezydencja Rady, która konsultuje się (z wyjątkiem przypadków, w których powołano się na klauzulę solidarności) z dotkniętymi państwami członkowskimi, Komisją i Wysokim Przedstawicielem (WP). Ponadto zgodnie z procedurami IPCR Sekretariat Generalny Rady, służby Komisji i ESDZ mogą również uzgodnić, w porozumieniu z prezydencją, aktywację IPCR w trybie wymiany informacji. Podstawą dyskusji w ramach IPCR są sprawozdania ze zintegrowanej orientacji i analizy sytuacyjnej opracowane przez służby Komisji i Europejską Służbę Działań Zewnętrznych („ESDZ").

(4) Chociaż państwa członkowskie ponoszą główną odpowiedzialność za zarządzanie krajowymi kryzysami cyberbezpieczeństwa, potencjalny transgraniczny i międzysektorowy charakter incydentów w cyberbezpieczeństwie wymaga od państw członkowskich i odpowiednich podmiotów Unii współpracy na poziomie technicznym, operacyjnym i politycznym w celu skutecznej koordynacji w całej Unii. Jednocześnie reagowanie kryzysowe i przywracanie sprawności operacyjnej są kosztowne dla dotkniętych podmiotów i sektorów. W związku z tym pełny cykl zarządzania kryzysowego w obejmuje gotowość i wspólną orientację sytuacyjną w celu przewidywania incydentów w cyberbezpieczeństwie, zdolności wykrywania niezbędne do identyfikacji oraz narzędzia reagowania i przywracania sprawności operacyjnej w celu łagodzenia, powstrzymywania i ograniczania tych incydentów.

(5) 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 incydenty w cyberbezpieczeństwie i kryzysy cyberbezpieczeństwa na dużą skalę. Określono w nim odpowiednie podmioty na poziomie technicznym, operacyjnym i politycznym oraz wyjaśniono, w jaki sposób zostały one włączone do szerszego unijnego zarządzania kryzysowego, takiego 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.

(6) Od 2017 r. Unia rozwinęła swoje ramy cyberbezpieczeństwa za pomocą szeregu instrumentów, które zawierają przepisy istotne dla zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa: rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[4], dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[5], rozporządzenia wykonawczego Komisji 2024/2690[6], rozporządzenia Parlamentu

---

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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 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).

5 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).

6 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

Europejskiego i Rady (UE, Euratom) 2023/2841[7], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887[8], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847[9] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/38 („akt w sprawie cybersolidarności")[10]. Szczególne sektorowe środki dotyczące kryzysu cyberbezpieczeństwa obejmują rozporządzenie delegowane Komisji (UE) 2024/1366[11] oraz przyszłe ramy koordynacji w odniesieniu do cyberincydentów o charakterze systemowym (EU-SCICF) w kontekście rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554[12]. Dyrektywa 2013/40/UE[13] zawiera odniesienie do definicji 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[14], gdy tylko zostaną wdrożone, znacznie

---

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).

7 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).

8 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).

9 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).

10 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 cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (Dz.U. L, 2025/28, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

11 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).

12 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).

13 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).

14 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).

ułatwią działania organów ścigania w tej dziedzinie. W polityce UE w zakresie cyberobrony[15] określono rolę 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[16] przewiduje współpracę między odpowiednimi podmiotami w przypadku incydentu mającego wpływ zarówno na aspekty fizyczne, jak i na cyberbezpieczeństwo infrastruktury krytycznej.

(7) Na szczeblu Unii odpowiednie podmioty, które mają obowiązki w zakresie zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, obejmują Komisję, ESDZ, w tym pojedynczą komórkę analiz wywiadowczych (SIAC), Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Służbę ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii (CERT-UE), Europol za pośrednictwem Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3), europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), Centrum Satelitarne Unii Europejskiej (SATCEN), centrum monitorowania bezpieczeństwa systemu Galileo oraz unijną sieć delegatur. Te podmioty Unii powinny wspólnie określać obszary współpracy i przyczyniać się do wdrażania unijnych ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, zgodnie z ich kompetencjami wynikającymi z mającego zastosowanie prawa.

(8) Zaktualizowane zalecenie określające plan działania na rzecz cyberbezpieczeństwa („plan na rzecz cyberbezpieczeństwa”) jest konieczne, aby zapewnić jasne i dostępne wytyczne wyjaśniające, czym jest kryzys cyberbezpieczeństwa na szczeblu Unii, w jaki sposób uruchamiane są ramy zarządzania kryzysowego oraz jakie są role odpowiednich podmiotów i mechanizmów na szczeblu Unii, a także jakie są interakcje między tymi podmiotami i mechanizmami w całym cyklu kryzysu cyberbezpieczeństwa. Plan na rzecz cyberbezpieczeństwa należy postrzegać w szerszym kontekście stosunków cywilno-wojskowych oraz stosunków UE–NATO.

(9) Niniejsze zalecenie uzupełnia ustalenia dotyczące zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i szerszych unijnych mechanizmów kryzysowych, w tym ogólnego systemu wczesnego ostrzegania Komisji ARGUS, Unijnego Mechanizmu Ochrony Ludności (UMOL) wspieranego przez Centrum Koordynacji Reagowania Kryzysowego (ERCC), mechanizmu reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych (CRM), a także innych procesów, takich jak procesy opisane w unijnym zestawie narzędzi do przeciwdziałania zagrożeniom hybrydowym[17] i w zmienionym unijnym protokole w sprawie przeciwdziałania zagrożeniom hybrydowym. Niniejsze zalecenie stanowi również uzupełnienie zalecenia Rady w sprawie w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu

15 JOIN(2022) 49 final.

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

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

infrastruktury krytycznej mające istotne znaczenie transgraniczne („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.

(10) Należy wspierać kompleksowe i zintegrowane podejście do zarządzania kryzysowego we wszystkich sektorach i na wszystkich szczeblach sprawowania rządów. Należy wzmocnić międzysektorowe zarządzanie kryzysowe na szczeblu Unii, aby umożliwić zintegrowane reagowanie kryzysowe, zwłaszcza w przypadkach, gdy incydenty w cyberbezpieczeństwie mają rzeczywiste konsekwencje. Gdy incydenty w cyberbezpieczeństwie są częścią szerszej kampanii hybrydowej lub hybrydowej sytuacji kryzysowej, odpowiednie podmioty powinny wspierać wysiłki na rzecz opracowania jednolitego obrazu sytuacji w szeregu sektorów i dziedzin. Zalecenie przyczynia się do szerszych działań w zakresie gotowości wymaganych dla Unii w obliczu wielowymiarowych zagrożeń hybrydowych (zgodnie z zasadami zawartymi w strategii na rzecz unii gotowości).

(11) Bezpieczeństwo krytycznej infrastruktury cyfrowej ma zasadnicze znaczenie dla odporności gospodarki, społeczeństwa i obronności Unii. Podmioty objęte zakresem dyrektywy (UE) 2022/2555, w tym podmioty zapewniające podmorskie kable komunikacyjne, muszą wprowadzić środki w celu ochrony bezpieczeństwa fizycznego i środowiskowego sieci i systemów informatycznych w oparciu o podejście uwzględniające wszystkie zagrożenia, takie jak awarie systemu, błąd ludzki, działania złośliwe lub zjawiska naturalne. Ponadto podmioty te powinny zgłaszać incydenty, w tym incydenty dotyczące podmorskich kabli komunikacyjnych, do CSIRT lub, w stosownych przypadkach, właściwego organu. Chociaż podstawowe zasady leżące u podstaw planu na rzecz cyberbezpieczeństwa są istotne dla bezpieczeństwa kabli podmorskich, mechanizmy w nim określone nie są wystarczająco kompleksowe, aby objąć cały cykl odporności na sytuacje kryzysowe. Szczególny charakter tego cyklu wymaga skoordynowanych i dostosowanych do potrzeb wysiłków w celu zaspokojenia potrzeb w zakresie zintegrowanego nadzoru zagrożeń i orientacji sytuacyjnej w basenach morskich wokół UE, strategicznych inwestycji w celu stworzenia redundancji, a także wspólnego europejskiego podejścia do zwiększenia zdolności w zakresie naprawy i przywracania sprawności operacyjnej. Strategia UE w zakresie bezpieczeństwa morskiego obejmuje działania mające na celu zwiększenie cyberbezpieczeństwa w obszarze morskim oraz wzmocnienie nadzoru i ochrony krytycznej infrastruktury morskiej, w tym kabli podmorskich. W odniesieniu do zarządzania kryzysowego na szczeblu Unii jedną z możliwości do rozważenia byłaby specjalna sieć krajowych punktów kontaktowych i bliskich interakcji cywilno-wojskowych, w tym z NATO.

(12) Gotowość na wypadek kryzysu wymaga kompleksowej oceny ryzyka uwzględniającej wszystkie zagrożenia i wszystkie rodzaje ryzyka, biorąc pod uwagę zbieżność interesów gospodarczych i interesów bezpieczeństwa Unii Europejskiej. Wspólna unijna orientacja sytuacyjna wśród państw członkowskich i podmiotów Unii, ułatwiona dzięki uzgodnieniu wspólnej taksonomii i bezpiecznych kanałów komunikacji, powinna umożliwić skoordynowaną i świadomą reakcję na potencjalne incydenty w cyberbezpieczeństwie na dużą skalę, a także odstraszanie stałych agresorów. W oparciu o zasadę ograniczonego dostępu i biorąc pod uwagę znaczenie zaufania do wymiany informacji, grupy państw członkowskich w różnych konfiguracjach oraz, w stosownych przypadkach, odpowiednie podmioty Unii mogą chcieć współpracować i wymieniać się informacjami istotnymi dla zarządzania

incydentami w cyberbezpieczeństwie. Państwa członkowskie i podmioty Unii dzielące się informacjami dotyczącymi zagrożeń, ryzyka i luk w poziomie dojrzałości powinny umożliwić określenie właściwych priorytetów w zakresie należytych inwestycji i konkretnych działań, które doprowadziłyby do poprawy cyberodporności.

(13) Zgodnie z art. 7 ust. 6 rozporządzenia (UE) 2019/881 ENISA, w ścisłej współpracy z państwami członkowskimi, przygotowuje regularny pogłębiony raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i cyberzagrożeń. Raport ten, znany jako unijne wspólne sprawozdanie z oceny cyberbezpieczeństwa (EU-JCAR), jest przygotowywany wraz z Europolem/EC3 i CERT-UE w celu zwiększenia gotowości Unii, ponieważ zapewnia orientację sytuacyjną w oparciu o analizę incydentów i cyberzagrożeń.

(14) Kluczowa infrastruktura krytyczna, taka jak infrastruktura energetyczna, transportowa, cyfrowa, w zakresie opieki zdrowotnej lub usług finansowych, a także rozwiązania w zakresie bezpieczeństwa wdrożone w celu jej ochrony są zazwyczaj obsługiwane przez przedsiębiorstwa prywatne. Ochrona tej infrastruktury przed incydentami w cyberbezpieczeństwie na dużą skalę wymaga ścisłej współpracy między podmiotami publicznymi i prywatnymi, w tym producentami i podmiotami opracowującymi otwarte oprogramowanie, która to współpraca musi być oparta na zaufaniu oraz jasnych i specjalnych procedurach wymiany informacji, rozpowszechniania i koordynacji reagowania.

(15) Ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu Unii są wysoce skutecznym narzędziem testowania procedur i mechanizmów współpracy, a tym samym zwiększają gotowość. Ponieważ ćwiczenia są zasobochłonne, program ćwiczeń musi być jak najbardziej usprawniony i skonsolidowany oraz musi uwzględniać scenariusze opracowane w ramach unijnych skoordynowanych ocen ryzyka i innych odpowiednich inicjatyw.

(16) Europejska infrastruktura cyfrowa ma wiele głęboko zakorzenionych zależności technicznych. Należy zająć się tymi zależnościami w celu zapewnienia ciągłości działania operacji w sytuacji kryzysowej. Dotyczy to na przykład systemu nazw domen (DNS), który jest kluczowym elementem leżącym u podstaw funkcjonowania internetu. Resolwery DNS mają zasadnicze znaczenie dla dostępu do internetu, w tym w czasie poważnego kryzysu cyberbezpieczeństwa, ponieważ przekładają nazwy domen internetowych na adresy IP. W dyrektywie (UE) 2022/2555 zachęca się odpowiednie zainteresowane strony do przyjęcia strategii dywersyfikacji rozwiązywania nazw DNS. Zachęca się w niej również państwa członkowskie do wspierania rozwoju i korzystania z publicznej i bezpiecznej europejskiej usługi resolwera DNS jako kluczowego środka zapewniającego gotowość i odporność na sytuacje kryzysowe.

(17) Ponadto, aby zwiększyć odporność innych kluczowych komponentów, takich jak system routingu, oraz zapewnić ich funkcjonalność podczas poważnych kryzysów cyberbezpieczeństwa, konieczne jest terminowe wdrożenie odpowiednich najlepszych praktyk i najnowszych dostępnych norm. W związku z tym w rozporządzeniu wykonawczym (UE) 2024/2690 nakłada się obowiązek utworzenia wielostronnego forum w celu określenia najlepszych dostępnych norm i technik wdrażania istotnych elementów cyberbezpieczeństwa oraz zachęca się do udziału odpowiednie podmioty.

(18) Aby skutecznie wykrywać szkodliwe działania w coraz bardziej złożonych globalnych łańcuchach dostaw, które to działania mogą mieć wpływ na całą Unię, konieczne jest skoordynowane podejście. Jest to szczególnie istotne w przypadku obszarów, w

których Unia opiera się na technologii dostawców wysokiego ryzyka podlegających jurysdykcji państwa trzeciego wymagającego zgłaszania do władz informacji o podatnościach w oprogramowaniu lub sprzęcie, zanim podatności te staną się publicznie znane jako aktywnie wykorzystywane. Podmioty wspierane przez państwa mogą również zawczasu ulokować się w infrastrukturze krytycznej z zamiarem spowodowania zakłóceń w późniejszym czasie, na przykład podczas konfliktu. Trudno jest to wykryć za pomocą tradycyjnych metod, ponieważ agresorzy ukrywają swoją działalność, łącząc ją z legalnym ruchem w sieci i stosując techniki LotL (ang. *living off the land*), czyli wykorzystują „naturalne zasoby" systemu operacyjnego, które opierają się na legalnych narzędziach i procesach, w celu ukrycia szkodliwych działań. To samo dotyczy państw trzecich, w których – zgodnie z publicznymi oświadczeniami Unii lub jej państw członkowskich – agresorzy działający z terytorium tych państw prowadzili szkodliwe działania w cyberprzestrzeni przeciwko Unii. Łańcuchy dostaw powinny stać się bardziej odporne i zróżnicowane, przy jednoczesnym utrzymaniu wspólnego poziomu gotowości.

(19) Na poziomie technicznym zasadniczą rolę w wykrywaniu incydentów, cyberzagrożeń i podatności, wspieraniu alokacji technicznej i przywracaniu sprawności operacyjnej po cyberatakach odgrywają CSIRT, organy ścigania, a także krajowe i transgraniczne centra cyberbezpieczeństwa (centra cyberbezpieczeństwa), które mają zostać ustanowione na podstawie rozporządzenia (UE) 2025/38. Niezbędne są skuteczne ustalenia proceduralne dotyczące współpracy między siecią CSIRT a EU-CyCLONe, zgodnie z wymogami dyrektywy (UE) 2022/2555. Europejski system ostrzeżeń dotyczących cyberbezpieczeństwa ma na celu wspieranie rozwoju zaawansowanych zdolności Unii w zakresie wykrywania, analizy i przetwarzania danych w odniesieniu do cyberzagrożeń oraz zapobiegania incydentom w Unii.

(20) Jeżeli chodzi o natychmiastową reakcję, mechanizmy dostępne państwom członkowskim obejmują rezerwę cyberbezpieczeństwa UE oraz działania w zakresie wspierania wzajemnej pomocy ustanowione na mocy rozporządzenia (UE) 2025/38, zespoły szybkiego reagowania na zagrożenia hybrydowe i stałą współpracę strukturalną (PESCO), zespoły szybkiego reagowania na cyberincydenty (CRRT), a także mechanizmy przewidziane dla sojuszników NATO. Ponadto protokół działań UE w zakresie egzekwowania prawa w sytuacjach kryzysowych (LE ERP) wspiera unijne organy ścigania w zapewnianiu natychmiastowej reakcji na poważne transgraniczne cyberataki poprzez szybką ocenę, bezpieczną i terminową wymianę krytycznych informacji oraz skuteczną koordynację międzynarodowych aspektów prowadzonych przez nie dochodzeń, w tym dekonfliktowanie na etapie ścigania oraz koordynację z partnerami niebędącymi organami ścigania. Uzyskanie jasnego obrazu, które warianty reagowania są dostępne w przypadku incydentów w cyberbezpieczeństwie i działań hybrydowych oraz w jaki sposób są one wykorzystywane, może zapewnić skuteczną alokację zasobów i pomóc uniknąć ich powielania. W związku z tym zgodnie z rozporządzeniem (UE) 2025/38 państwa członkowskie są zobowiązane do informowania sieci CSIRT i EU-CyCLONe przy zwracaniu się o usługi z rezerwy cyberbezpieczeństwa UE.

(21) Zasadnicze znaczenie dla cyberbezpieczeństwa ma skuteczne zwalczanie cyberprzestępczości. Prewencji nie można realizować wyłącznie poprzez odporność, konieczne są również identyfikacja i ściganie sprawców oraz odpowiednie reagowanie. Współpraca za pośrednictwem dostosowanych systemów i platform technicznych oraz wymiana istotnych informacji między podmiotami zajmującymi się cyberbezpieczeństwem, podmiotami dyplomacji cyfrowej i organami ścigania mają

zatem zasadnicze znaczenie dla zapewnienia kompleksowego zrozumienia krajobrazu zagrożeń i zdolności reagowania w sposób spójny i skoordynowany.

(22) Kryzysy powodują niepewność, którą przeciwnicy mogą łatwo wykorzystać do rozpowszechniania dezinformacji i wzbudzania nieufności. Aby temu przeciwdziałać, niezbędne jest jasne i spójne informowanie społeczeństwa o sytuacji i działaniach podejmowanych w celu zaradzenia tej sytuacji. Skoordynowana komunikacja strategiczna może również wspierać działania dyplomatyczne przeciwko stałym agresorom, jak również przyczyniać się do opracowania narracji na temat zagrożeń dla Unii i jej działań prewencyjnych oraz potrzeby promowania odpowiedzialnego zachowania państwa w cyberprzestrzeni.

(23) W celu skutecznego zarządzania kryzysowego konieczne jest określenie wspólnych bezpiecznych rozwiązań komunikacyjnych w dziedzinie cyberbezpieczeństwa i wdrożenie ich w całej Unii, w tym, w razie potrzeby, do celów wymiany informacji niejawnych UE. Na wniosek Rady Komisja i inne odpowiednie podmioty Unii dokonały określenia istniejących bezpiecznych narzędzi komunikacji oraz przedstawiły wyniki tego procesu w grudniu 2022 r. Podmioty Unii podejmują szereg odrębnych wysiłków na rzecz budowania bezpiecznych zdolności komunikacyjnych w sytuacji kryzysowej, które wymagają lepszej koordynacji i efektu mnożnikowego. Obejmuje to ustanowienie unijnego systemu łączności krytycznej (EUCCS) w celu zwiększenia odporności publicznej infrastruktury łączności na szkodliwe zakłócenia oraz poprawy codziennej współpracy operacyjnej, w tym transgranicznej.

(24) Środowisko bezpieczeństwa Unii wymaga podejścia uwzględniającego wszystkie zagrożenia, obejmującego całą administrację rządową i całe społeczeństwo, w odniesieniu do przygotowania i gotowości zarówno cywilnej, jak i wojskowej. Organy wojskowe polegają na cywilnej infrastrukturze krytycznej, takiej jak infrastruktura łączności, energetyczna, w zakresie opieki zdrowotnej, transportowa i logistyczna. W związku z tym, jak podkreślono w polityce UE w zakresie cyberobrony[18], cyberbezpieczeństwo UE wymaga ściślejszej współpracy i synergii między zdolnościami sieci cywilnych i wojskowych w zakresie gotowości i reagowania, w tym w przypadku ataku zbrojnego. Podmioty zajmujące się cyberbezpieczeństwem powinny współpracować ponad granicami schematów instytucjonalnych i operacyjnych w celu przewidywania i przeciwdziałania zagrożeniu wielosektorowymi, wielowymiarowymi zakłóceniami, zgodnie z zasadami, które należy włączyć do strategii na rzecz unii gotowości. Ponadto szkodliwe działania w cyberprzestrzeni odgrywają coraz większą rolę w szerszych kampaniach hybrydowych skierowanych przeciwko Unii, jej państwom członkowskim i partnerom strategicznym. Konieczna jest zatem ściślejsza współpraca między Unią a NATO.

(25) W społeczności wojskowej przyszłe Centrum Koordynacji UE ds. Cyberobrony i pojedyncza komórka analiz wywiadowczych (SIAC) w ramach Europejskiej Służby Działań Zewnętrznych, operacyjna sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET) i unijna konferencja dowódców ds. obrony cyberprzestrzeni wspierana przez Europejską Agencję Obrony (EDA), a także odpowiednie projekty w ramach stałej współpracy strukturalnej (PESCO) reprezentują ważne podmioty i inicjatywy na rzecz koordynacji i współpracy w zakresie gotowości do wykrywania cyberzagrożeń mających wpływ na Unię i państwa członkowskie, prewencji i obrony przed takimi zagrożeniami oraz przywracania sprawności

[18] Polityka UE w zakresie cyberobrony, JOIN(2022) 49 final.

operacyjnej po wystąpieniu takich zagrożeń. W związku z tym należy zachęcać do współpracy między podmiotami cywilnymi i wojskowymi, np. do współpracy między EU-CyCLONe a konferencją unijnych dowódców ds. obrony cyberprzestrzeni, a także do potencjalnej współpracy między MICNET a siecią CSIRT.

(26) Współpraca z krajami i organizacjami spoza Unii będącymi międzynarodowymi partnerami strategicznymi zwiększa zdolności Unii w zakresie cyberbezpieczeństwa. Wspierając współpracę międzynarodową, Unia i jej partnerzy mogą zapewnić wspólną orientację sytuacyjną i spójność w zarządzaniu kryzysami cyberbezpieczeństwa oraz solidną pozycję w cyberprzestrzeni, przyczyniając się do stworzenia globalnej, otwartej, stabilnej, bezpiecznej i odpornej cyberprzestrzeni. Współpraca ta powinna opierać się na zaufaniu i wspólnym celu, jakim jest ochrona infrastruktury krytycznej i podstawowych usług przed cyberzagrożeniami, w tym poprzez promowanie odpowiedzialnego zachowania państw w cyberprzestrzeni, osadzonego w ramach Organizacji Narodów Zjednoczonych (ONZ) oraz pociąganie agresorów do odpowiedzialności za ich niewłaściwe i nielegalne zachowanie w cyberprzestrzeni. Środki dyplomacji cyfrowej przyczyniają się do prewencji i reagowania na szkodliwe działania w cyberprzestrzeni oraz zapewniają koordynację i współpracę ze krajami będącymi strategicznymi partnerami międzynarodowymi,

PRZYJMUJE NINIEJSZE ZALECENIE:

I. Cel, zakres i zasady unijnych ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa

1) W niniejszym zaleceniu określono unijne ramy zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa w kontekście ogólnej gotowości UE na wielowymiarowe zagrożenia hybrydowe. Sposób, w jaki incydent może przekształcić się w incydent na dużą skalę, a tym samym w sytuację kryzysową na szczeblu UE, przedstawiono i streszczono w załączniku 1, z uwzględnieniem przypadku, gdy taki incydent zbiega się z innymi zagrożeniami hybrydowymi wymagającymi interakcji między niezbędnymi reakcjami. Ramy zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa powinny umożliwiać odpowiednim stronom na szczeblu Unii, w tym podmiotom i sieciom, zrozumienie sposobu interakcji i jak najlepszego wykorzystania istniejących mechanizmów wymienionych w załączniku II w całym cyklu zarządzania kryzysowego. Ponadto uwzględniono zalecenia dla stron na szczeblu Unii określające, w jaki sposób można poprawić skuteczność istniejących mechanizmów.

2) Unia i jej państwa członkowskie powinny stosować się do planu na rzecz cyberbezpieczeństwa w zarządzaniu sytuacją kryzysową wynikającą z incydentu w cyberbezpieczeństwie na dużą skalę, zdefiniowanego w art. 6 pkt 7 dyrektywy (UE) 2022/2555, która to sytuacja wpływa na prawidłowe funkcjonowanie rynku wewnętrznego lub stwarza poważne ryzyko dla bezpieczeństwa publicznego i bezpieczeństwa podmiotów lub obywateli w kilku państwach członkowskich lub w całej Unii („kryzys cyberbezpieczeństwa”).

3) W przypadku gdy incydent w cyberbezpieczeństwie, wykryty na poziomie technicznym przez CSIRT lub centrum cyberbezpieczeństwa, skutkuje eskalacją w ramach wewnętrznych procedur sieci CSIRT, odpowiednie informacje należy udostępniać EU-CyCLONe zgodnie z odpowiednimi ustaleniami proceduralnymi, a EU-CyCLONe powinna z kolei rozważyć, czy incydent ten stanowi potencjalny czy trwający incydent na dużą skalę zdefiniowany w art. 6 pkt 7 dyrektywy (UE) 2022/2555. Ustalenie, czy w wyniku tego incydentu na dużą skalę istnieje lub

przestał istnieć kryzys cyberbezpieczeństwa, należy przeprowadzić zgodnie z decyzją wykonawczą (UE) 2018/1993, w szczególności z jej art. 4 i 5.

4) Zgodnie z zasadami proporcjonalności, pomocniczości, komplementarności i poufności informacji określonymi w załączniku III państwa członkowskie i podmioty Unii powinny pogłębić współpracę w zakresie zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, wspierając wzajemne zaufanie i opierając się na istniejących sieciach i mechanizmach. Chociaż plan na rzecz cyberbezpieczeństwa nie koliduje ze sposobem, w jaki podmioty określają swoje procedury wewnętrzne, każdy podmiot powinien jasno określić interfejsy wykorzystywane do współpracy z innymi podmiotami. Interfejsy te powinny być uzgodnione wspólnie pomiędzy zainteresowanymi podmiotami i odpowiednio udokumentowane.

5) Plan na rzecz cyberbezpieczeństwa należy stosować zgodnie z planem dotyczącym infrastruktury krytycznej, w szczególności w przypadku incydentów mających wpływ zarówno na odporność fizyczną, jak i cyberbezpieczeństwo infrastruktury krytycznej[19]. W przypadku gdy istnieją sektorowe środki zarządzania kryzysowego obejmujące incydenty w cyberbezpieczeństwie, środki te należy wdrażać w sposób spójny z niniejszym zaleceniem.

II. Działania przygotowawcze w związku z kryzysem cyberbezpieczeństwa na szczeblu Unii

a) Orientacja sytuacyjna i wymiana informacji

6) Podstawę wspólnej orientacji sytuacyjnej wśród państw członkowskich i podmiotów Unii na temat krajobrazu cyberzagrożeń powinny stanowić zweryfikowane, wiarygodne dane, w tym tendencje w zakresie incydentów, taktyk, technik i procedur, oraz aktywnie wykorzystywane podatności. Państwa członkowskie i podmioty Unii powinny wykorzystywać tę wspólną wiedzę do przewidywania cyberataków, przygotowywania się na nie oraz wykrywania ich, zgodnie z odpowiednimi zakresami kompetencji tych państw i podmiotów. Wspólna orientacja sytuacyjna powinna:

   a) dotyczyć wszystkich sektorów krytycznych wymienionych w dyrektywie (UE) 2022/2555, w szczególności łączności, infrastruktury cyfrowej, energii, transportu, finansów, przestrzeni kosmicznej i zdrowia, i mieć również zastosowanie, za pośrednictwem CERT-UE, do sieci i systemów podmiotów Unii zgodnie z rozporządzeniem (UE, Euratom) 2023/2841;

   b) opierać się na wysokiej jakości zróżnicowanych i zintegrowanych zbiorach danych, które są gromadzone, przetwarzane i udostępniane w czasie rzeczywistym;

   c) być uwzględniona we wspólnym sprawozdaniu z oceny cyberbezpieczeństwa (JCAR) i innych odpowiednich dokumentach;

   d) uwzględniać powiązane zagrożenia hybrydowe, w tym zagraniczne manipulacje informacjami i ingerencje w informacje oraz dezinformację;

   e) wspierać krótkoterminowe działania i środki reagowania, a także mieć wkład w długoterminowe planowanie polityki w kontekście gotowości i prewencji;

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

f) [zapewniać powiązanie z innymi ocenami ryzyka i zagrożeń sporządzanymi regularnie i wzmacnianymi w ramach strategii na rzecz unii gotowości w celu zapewnienia synergii i uproszczenia obowiązków sprawozdawczych państw członkowskich.]

7) EU-CyCLONe i sieć CSIRT powinny:

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

b) kontynuować budowanie atmosfery zaufania między członkami;

c) w pełni wykorzystywać dostępne narzędzia wymiany informacji.

8) Państwa członkowskie i odpowiednie podmioty Unii powinny udoskonalać sposoby koordynacji i partnerstwa z sektorem prywatnym, w tym społecznościami zajmujących się otwartym oprogramowaniem i producentami otwartego oprogramowania, w celu poprawy wymiany informacji, w oparciu o istniejące centra wymiany i analizy informacji na szczeblu unijnym i krajowym, w celu zwiększenia zdolności w zakresie cyberbezpieczeństwa i reagowania na incydenty w cyberbezpieczeństwie, w tym poprzez dyskusje z udziałem EU-CyCLONe i sieci CSIRT.

9) Państwa członkowskie i odpowiednie podmioty Unii mogłyby zdecydować, w celu zacieśnienia współpracy i wzmocnienia zaufania oraz w oparciu o ustalenia dotyczące wymiany informacji na temat cyberbezpieczeństwa zawarte w dyrektywie (UE) 2022/2555 i w przepisach rozporządzenia (UE) 2025/38 dotyczących centrów cyberbezpieczeństwa, o utworzeniu dobrowolnych klastrów współpracy na zasadzie ograniczonego dostępu, gdy istnieją wspólne interesy związane z zapobieganiem konkretnemu rodzajowi zagrożenia, wykrywaniem konkretnego zagrożenia lub reagowaniem na takie zagrożenie, któremu te państwa i podmioty muszą sprostać. Wszelkie takie klastry powinny być zgodne z mandatem odpowiednich podmiotów, a także z już ustanowionymi strukturami. Takie klastry współpracy mogłyby zwracać się do podmiotów Unii o ułatwienie ich współdziałania, w tym poprzez odpowiednią infrastrukturę.

10) Państwa członkowskie, za pośrednictwem grupy współpracy NIS ustanowionej dyrektywą (UE) 2022/2555, powinny w terminie 12 miesięcy od przyjęcia planu na rzecz cyberbezpieczeństwa opracować wspólną taksonomię w odniesieniu do zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa oraz przedstawić przewodnik dotyczący bezpiecznego postępowania z informacjami dotyczącymi incydentów w cyberbezpieczeństwie i kryzysów cyberbezpieczeństwa oraz wymiany tych informacji, zawierający sekcję poświęconą określeniu poziomu poufności tych informacji (kategoryzacja).

11) Przy określaniu poziomu poufności dostępnych informacji państwa członkowskie i odpowiednie podmioty Unii powinny wziąć pod uwagę potencjalny wpływ, jaki zawyżenie klauzuli tajności może mieć na dobrowolną wymianę informacji i osiągnięcie wspólnej orientacji sytuacyjnej. Udostępniając informacje jawne, państwa członkowskie powinny w pełni wykorzystywać istniejące platformy współpracy technicznej i operacyjnej, takie jak platformy wykorzystywane przez sieć CSIRT i EU-CyCLONe.

b) Wspólne ćwiczenia

12) Państwa członkowskie i odpowiednie podmioty Unii powinny opracować skuteczny cykl ćwiczeń w cyberprzestrzeni, aby przygotować się na kryzysy cyberbezpieczeństwa i zwiększyć efektywność organizacyjną. Ćwiczenia te powinny opierać się na scenariuszach opracowanych na podstawie unijnych skoordynowanych ocen ryzyka, w tym na scenariuszach dotyczących wielosektorowej sytuacji kryzysowej. Cykl ćwiczeń w cyberprzestrzeni powinien uwzględniać UMOL i inne mechanizmy reagowania kryzysowego na szczeblu Unii. Powinien on zapewniać skuteczne wdrażanie wniosków wyciągniętych z ćwiczeń.

13) Odpowiednie podmioty Unii mogłyby przeprowadzać ćwiczenia na mniejszą skalę w celu przetestowania swoich interakcji i interfejsów w przypadku eskalacji incydentów w cyberbezpieczeństwie.

14) Służby Komisji, ESDZ i ENISA proszone są o zorganizowanie ćwiczenia w celu przetestowania planu na rzecz cyberbezpieczeństwa w ciągu 18 miesięcy od daty jego przyjęcia, z udziałem wszystkich odpowiednich podmiotów, w tym sektora prywatnego.

c) Zdolności w zakresie rozwiązywania nazw DNS

15) Państwa członkowskie, odpowiednie podmioty Unii, a także podmioty prywatne, takie jak operatorzy infrastruktury krytycznej, powinny udoskonalić swoją strategię dywersyfikacji rozwiązywania nazw DNS (systemów nazw domen), w tym wykorzystanie co najmniej jednej unijnej infrastruktury DNS, takiej jak DNS4EU, w celu zapewnienia niezawodnego rozwiązywania nazw DNS podczas poważnej sytuacji kryzysowej. ENISA i EU-CyCLONe powinny opracować i udostępnić wytyczne dotyczące automatycznego przełączania w sytuacjach kryzysowych, określające kroki niezbędne do przejścia na unijną infrastrukturę DNS w przypadku awarii innych usług DNS, zapewniającego ciągłość działania usług krytycznych podczas sytuacji kryzysowej.

16) Ponadto krajowe i transgraniczne centra cyberbezpieczeństwa powinny dzielić się z takimi unijnymi infrastrukturami DNS odpowiednimi informacjami na temat zagrożeń, aby wspierać te infrastruktury w zapewnianiu wysokiego poziomu ochrony przed zagrożeniami specyficznymi dla Unii, a tym samym w dalszym zwiększaniu zdolności w zakresie wykrywania i ograniczania zagrożeń specyficznych dla Unii.

17) Aby ogólnie zwiększyć bezpieczeństwo i dostępność krytycznej infrastruktury internetowej, również w sytuacjach kryzysowych, państwa członkowskie powinny aktywnie promować udział wszystkich odpowiednich zainteresowanych stron – w tym tych, których nie uwzględniono bezpośrednio w akcie wykonawczym do dyrektywy NIS2 – w upoważnionym wielostronnym forum, którego zadaniem jest wskazanie najlepszych dostępnych norm i technik wdrażania kluczowych środków bezpieczeństwa sieci. Ponadto państwa członkowskie powinny rozważyć zaangażowanie się w forum i same przyjąć zalecane wytyczne.

d) Zasoby

18) Państwa członkowskie powinny w pełni wykorzystywać zasoby finansowe przeznaczone na zapewnienie cyberbezpieczeństwa w ramach odpowiednich programów unijnych.

III. Wykrywanie incydentu, który mógłby przerodzić się w kryzys cyberbezpieczeństwa

19) Aby zaradzić rosnącej złożoności incydentów w cyberbezpieczeństwie i rosnącym wyzwaniom związanym z ich wykrywaniem, zarówno podmioty publiczne, jak i

prywatne powinny wdrożyć w swoich infrastrukturach cyfrowych strategie wykrywania oparte na analizie zagrożeń w celu identyfikacji potencjalnego ulokowania się z wyprzedzeniem w systemach, które może zostać później wykorzystane do przeprowadzenia ataku zakłócającego. W przypadku zidentyfikowania operacji prowadzonych w sposób utajony podmioty powinny aktywnie dzielić się istotnymi informacjami ze swoimi partnerami, zanim sytuacje przerodzą się w kryzysy cyberbezpieczeństwa.

20) Wszystkie podmioty powinny przekazywać odpowiednim sieciom, zgodnie ze swoimi właściwymi mandatami i w oparciu o podejście uwzględniające wszystkie zagrożenia, informacje wskazujące na potencjalny kryzys cyberbezpieczeństwa.

21) Sieci CSIRT i EU-CyCLONe powinny dokonać uzgodnień proceduralnych na wypadek potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, aby zapewnić koordynację techniczno-operacyjną oraz terminowe i adekwatne przekazywanie informacji na poziom polityczny.

22) Sieć CSIRT powinna doradzać EU-CyCLONe, czy zaobserwowany incydent w cyberbezpieczeństwie można uznać za potencjalny lub trwający incydent na dużą skalę.

23) Transgraniczne centra cyberbezpieczeństwa, które zostały już ustanowione lub mają zostać ustanowione na podstawie rozporządzenia (UE) 2025/38, powinny przekazywać odpowiednie informacje do mechanizmów na szczeblu Unii w przypadku potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę w oparciu o podejście uwzględniające wszystkie zagrożenia, w tym szkody fizyczne w infrastrukturze krytycznej, które zagrażają dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych lub udostępnianych za pośrednictwem sieci i systemów informatycznych.

24) W przypadku wykrycia potencjalnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę o wielosektorowym wpływie:

   a) Komisja powinna ułatwiać przepływ niezbędnych informacji między punktami kontaktowymi dla odpowiednich horyzontalnych i sektorowych mechanizmów kryzysowych na poziomie Unii wymienionych w załączniku II a EU-CyCLONe;

   b) odpowiednie podmioty Unii powinny wspierać EU-CyCLONe w ocenie skutków sektorowych i skutków dla ludności.

IV. Reagowanie na kryzys cyberbezpieczeństwa na szczeblu Unii

25) W przypadku kryzysu cyberbezpieczeństwa ustalonego w ramach IPCR wszystkie podmioty powinny reagować w ścisłej koordynacji z innymi podmiotami w odpowiedzi na szersze zagrożenia hybrydowe w ramach podejścia obejmującego całą administrację rządową w następujący sposób:

   a) poszkodowane państwa członkowskie i sieć CSIRT powinny współpracować w celu szybkiego przywrócenia dotkniętych systemów, zapewniając minimalne zakłócenia operacyjne;

   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 sprawozdanie ze zintegrowanej orientacji i analizy sytuacyjnej (ISAA) w ramach uzgodnień IPCR;

c) Komisja, w stosownych przypadkach we współpracy z Wysokim Przedstawicielem, powinna zapewnić spójność i koordynację działań podejmowanych w odpowiedzi na sytuację kryzysową i powiązanych działań w zakresie reagowania na szczeblu Unii, w szczególności odpowiednich sektorowych mechanizmów zarządzania kryzysowego na szczeblu Unii wymienionych w załączniku II, oraz w odniesieniu do zwracania się o pomoc za pośrednictwem UMOL;

d) prezydencja Rady powinna rozważyć zaproszenie przewodniczącego UE-CyCLONe na nieformalne posiedzenia okrągłego stołu i inne odpowiednie posiedzenia Rady w ramach uzgodnień IPCR;

e) Rada, wspierana przez EU-CyCLONe i odpowiednie podmioty Unii, powinna koordynować publiczne działania komunikacyjne, w tym w celu zapewnienia, aby sytuacja kryzysowa nie była wykorzystywana do rozpowszechniania niedokładnych informacji;

f) Wysoki Przedstawiciel, w ścisłej współpracy z Komisją i innymi odpowiednimi podmiotami Unii, powinien wspierać, w tym poprzez analizy i sprawozdania, proces podejmowania przez Radę decyzji dotyczących stosowania ewentualnych środków w ramach 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.

g) Komisja, Wysoki Przedstawiciel i państwa członkowskie powinny również skuteczniej wykorzystywać narzędzia ekonomiczne, takie jak zakazy handlu, aby lepiej zapobiegać utrzymującym się szkodliwym działaniom w cyberprzestrzeni prowadzonym przez podmioty państwowe, powstrzymywać takie działania i reagować na nie.

26) W przypadku gdy użytkownik usług świadczonych przez rezerwę cyberbezpieczeństwa UE[20] zwraca się o usługi z tej rezerwy zgodnie z art. 15 rozporządzenia (UE) 2025/38 i bez uszczerbku dla wszelkich przyszłych aktów wykonawczych na mocy tego rozporządzenia:

a) świadczenie usług powinno rozpocząć się w ciągu 24 godzin od złożenia wniosku;

b) Komisja i Wysoki Przedstawiciel powinni zapewnić koordynację z dodatkowymi środkami, zgodnie z unijnym zestawem narzędzi do

[20] Rezerwa cyberbezpieczeństwa UE to mechanizm oparty na usługach oferowanych przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa, mający na celu wspieranie – na wniosek – reagowania i wstępnego usuwania skutków w przypadku poważnych incydentów w cyberbezpieczeństwie, incydentów w cyberbezpieczeństwie na dużą skalę lub incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę mających wpływ na państwa członkowskie, instytucje, organy i jednostki organizacyjne Unii lub państwa trzecie stowarzyszone z programem „Cyfrowa Europa”.

przeciwdziałania zagrożeniom hybrydowym[21], w przypadku szkodliwych działań w cyberprzestrzeni, które są częścią szerszej kampanii hybrydowej;

c) w przypadku szkodliwego działania w cyberprzestrzeni mającego wymiar wojskowy wnioskujące państwo członkowskie powinno poinformować unijną konferencję dowódców ds. obrony cyberprzestrzeni o złożeniu wniosku.

27) W przypadku incydentu w cyberbezpieczeństwie na dużą skalę, który wpływa na właściwe funkcjonowanie usług kosmicznych mających kluczowe znaczenie dla bezpieczeństwa Unii lub jej państw członkowskich, EU-CyCLONe powinna poinformować o tym Wysokiego Przedstawiciela w celu skoordynowania ewentualnej reakcji w ramach struktury reagowania na zagrożenia związane z przestrzenią kosmiczną ustanowionej zgodnie z decyzją Rady (WPZiB) 2021/698.

V. Przywracanie sprawności operacyjnej po kryzysie cyberbezpieczeństwa

28) Państwa członkowskie, odpowiednie podmioty i sieci Unii powinny współpracować na etapie przywracania sprawności operacyjnej, opierając się na wnioskach wyciągniętych z przeprowadzonych ćwiczeń, a także na zgłoszeniach incydentów, w szczególności w kontekście europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie ustanowionego rozporządzeniem (UE) 2025/38.

VI. Bezpieczna komunikacja

29) Na podstawie mapy istniejących bezpiecznych narzędzi komunikacji[22] Komisja, Wysoki Przedstawiciel, EU-CyCLONe, sieć CSIRT i odpowiednie podmioty Unii powinny do końca 2026 r. uzgodnić interoperacyjny zestaw bezpiecznych rozwiązań komunikacyjnych dla odpowiednich podmiotów Unii. Rozwiązania te powinny obejmować pełen zakres wymaganych sposobów komunikacji (połączenia głosowe, przesyłanie danych, wideokonferencje, komunikaty, współpracę oraz wymianę dokumentów i konsultacje). Rozwiązania te powinny odzwierciedlać kluczowe zasady, takie jak interesy Unii w zakresie bezpieczeństwa, suwerenność technologiczna i poufność, a także takie cechy jak użyteczność, uwzględnianie bezpieczeństwa na etapie projektowania, certyfikacja przez europejskie organy ds. bezpieczeństwa informacji, pełne szyfrowanie transmisji, uwierzytelnianie, dostępność i kryptografia postkwantowa. Rozwiązania te powinny spełniać wspólnie określone wymogi dotyczące ochrony szczególnie chronionych informacji jawnych i obejmować narzędzia wymiany informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED.

30) Na tej podstawie podmioty na szczeblu Unii powinny wykorzystywać rozwiązania oparte na protokole Matrix do komunikacji w czasie rzeczywistym. Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) ustanowione na mocy rozporządzenia (UE) 2021/887, bez uszczerbku dla przyszłych wieloletnich ram finansowych, powinno rozważyć finansowanie w ramach programu „Cyfrowa Europa”, aby pomóc państwom członkowskim we wdrażaniu tych narzędzi.

---

[21] 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.

[22] Horyzontalna Grupa Robocza ds. Cyberprzestrzeni, WK 862/23.

31) W szczególności podmioty Unii i państwa członkowskie powinny opracować plany awaryjne na wypadek poważnych sytuacji kryzysowych, w których normalne kanały komunikacji oparte na sieciach internetowych lub telekomunikacyjnych są zakłócone lub niedostępne.

32) W perspektywie średniookresowej należy ustanowić mechanizmy komunikacji i wymiany informacji między organami ścigania a sieciami ds. cyberbezpieczeństwa, zwłaszcza na poziomie technicznym, w celu skutecznego reagowania kryzysowego. W ramach tych mechanizmów należy respektować rolę każdej ze stron i unikać ingerowania w bieżące działania. Komisja współpracuje z państwami członkowskimi nad ustanowieniem europejskiego systemu łączności krytycznej (EUCCS), który do 2030 r. powinien połączyć sieci komunikacyjne organów ścigania i ochrony ludności w całej strefie Schengen, tak aby krytyczne urządzenia komunikacyjne mogły być wykorzystywane na terytorium innych państw członkowskich. EUCCS może zatem również przynieść korzyści w zakresie wspólnego reagowania wraz z odpowiednimi społecznościami zajmującymi się cyberbezpieczeństwem. System ten powinien obejmować łączność rezerwową, np. poprzez łączność satelitarną.

VII. Koordynacja z podmiotami wojskowymi w odniesieniu do kryzysów cyberbezpieczeństwa

33) EU-CyCLONe i konferencja unijnych dowódców ds. obrony cyberprzestrzeni, MICNET i sieć CSIRT, a także przyszłe Centrum Koordynacji UE ds. Cyberobrony oraz jego kontrahenci cywilni powinni współpracować w celu rozwijania wspólnej orientacji sytuacyjnej między podmiotami cywilnymi i wojskowymi.

34) Uwzględniając istniejące umowy, takie jak umowa techniczna CERT-UE/NATO z 2016 r., Unia powinna dążyć do ustanowienia punktów kontaktowych na potrzeby koordynacji z NATO w przypadku kryzysu cyberbezpieczeństwa w celu wymiany niezbędnych informacji na temat sytuacji i wykorzystania mechanizmów reagowania kryzysowego. Aby to osiągnąć, Unia powinna zbadać sposoby poprawy zdolności w zakresie wymiany informacji z NATO, w tym poprzez ewentualne wzajemne połączenia między ich odpowiednimi systemami komunikacyjnymi i informacyjnymi.

35) W przypadku gdy państwo członkowskie w kontekście incydentu w cyberbezpieczeństwie korzysta z odpowiednich inicjatyw obronnych, takich jak CRRT PESCO lub inne odpowiednie inicjatywy, takie jak unijne zespoły szybkiego reagowania na zagrożenia hybrydowe (HRRT), powinno poinformować o tym EU-CyCLONe, a także konferencję unijnych dowódców ds. obrony cyberprzestrzeni.

VIII. Współpraca z partnerami strategicznymi

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

a) w przypadku stwierdzenia odpowiedniego incydentu ułatwić przepływ niezbędnych informacji z partnerami strategicznymi;

b) wzmocnić koordynację z partnerami strategicznymi w zakresie reagowania na utrzymujące się szkodliwe działania w cyberprzestrzeni prowadzone przez stałych agresorów, a w szczególności korzystać z zestawu narzędzi dla dyplomacji cyfrowej, zgodnie z wytycznymi dotyczącymi wdrażania tego zestawu narzędzi.

37) Państwa członkowskie, Wysoki Przedstawiciel, Komisja i inne odpowiednie podmioty Unii 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 incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę.

38) W ramach cyklu ćwiczeń, o którym mowa w sekcji II powyżej, służby Komisji i ESDZ powinny rozważyć zorganizowanie wspólnego ćwiczenia kadrowego w celu przetestowania współpracy między komponentami cywilnymi i wojskowymi w przypadku incydentu w cyberbezpieczeństwie na dużą skalę mającego wpływ na państwa członkowskie Unii i sojuszników NATO, w tym w przypadku uruchomienia lub prawdopodobnego uruchomienia art. 4 lub 5 Traktatu Północnoatlantyckiego.

39) Biorąc pod uwagę narażenie krajów kandydujących i potencjał incydentów w cyberbezpieczeństwie mających miejsce w sąsiedztwie Unii, należy rozważyć wspólne ćwiczenia z udziałem krajów kandydujących.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady

Przewodniczący