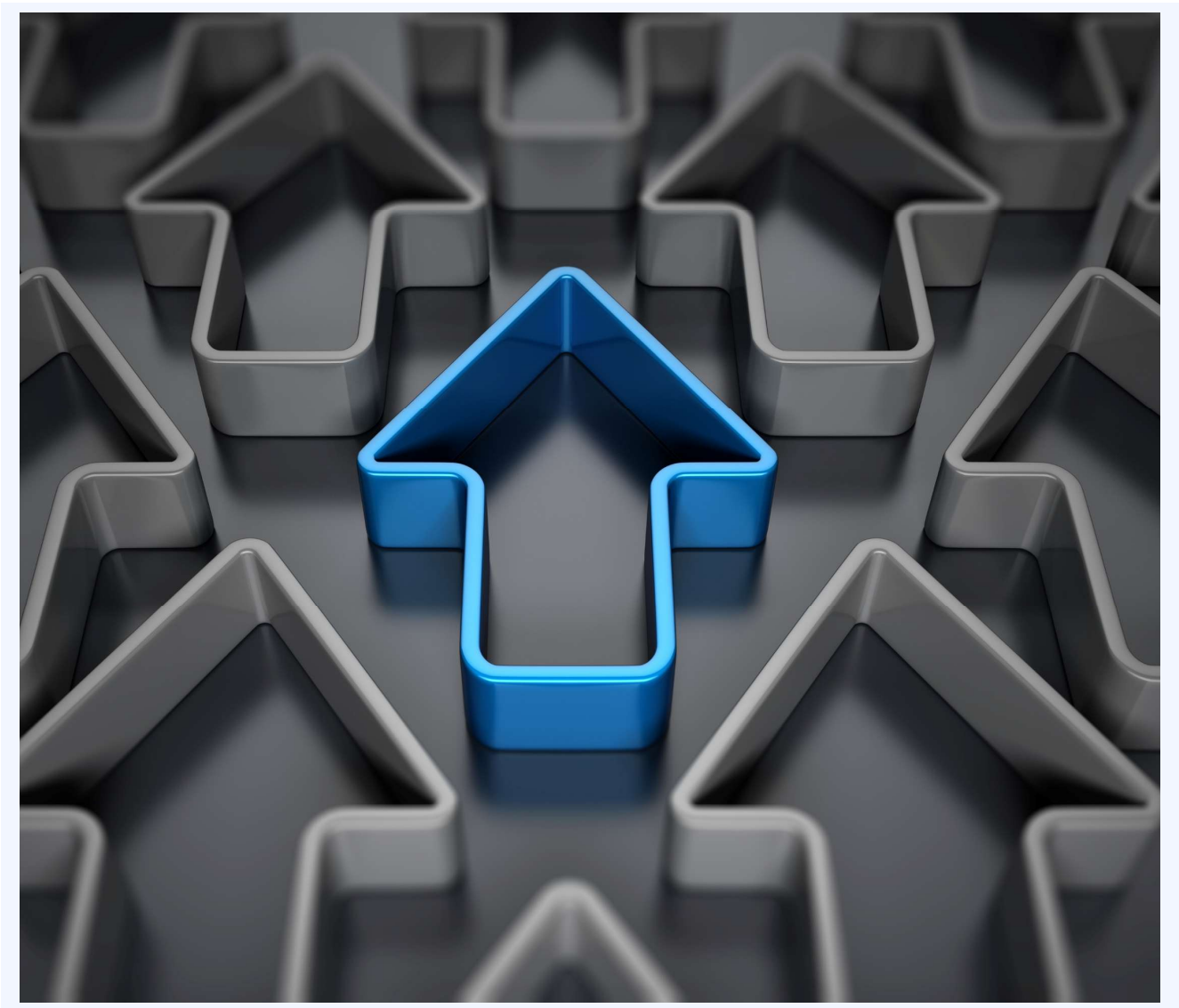
NASK



# Zalecenie Rady w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami (Cyber Blueprint)

**Piotr Słowiński, Emilia Zalewska-Czajczyńska**

**NASK-PIB**
ul. Kolska 12
01–045 Warszawa

**NIP:** 521 04 17 157
**Regon:** 010464542
**KRS:** 0000012938

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

nask.pl

NASK

## Spis treści

# Wstęp

**W dniu 6 czerwca 2025 r. Rada Unii Europejskiej przyjęła zalecenie w sprawie Planu działań UE na rzecz zarządzania cyberkryzysami (EU Cyber Blueprint). Jest to dokument o strategicznym znaczeniu dla kształtowania unijnych ram reagowania na kryzysy i incydenty o dużej skali w obszarze cyberbezpieczeństwa. Ma on zapewnić spójne, zintegrowane i efektywne podejście do zarządzania tymi wyzwaniami, które mogą mieć dalekosiężne konsekwencje dla państw członkowskich i całej Unii.**

Nowe zalecenie Rady zastąpiło poprzednią wersję, przyjętą w 2017r[1]. Jej rewizja i aktualizacja była konieczna ze względu na stale postępującą ewolucję i rosnącą złożoność krajobrazu cyberzagrożeń. Incydenty na dużą skalę występują coraz częściej i stają się coraz bardziej wyrafinowane, stanowiąc zagrożenie dla kluczowych sektorów gospodarki, infrastruktury krytycznej oraz stabilności społecznej i politycznej Unii i jej państw członkowskich.

W obliczu tych wyzwań, Rada w Cyber Blueprint kładzie nacisk na dostarczenie jasnych i dostępnych wskazówek w zakresie identyfikowania zagrożeń, sposobu uruchamiania ram zarządzania kryzysowego oraz ról i interakcji różnych sieci, podmiotów i mechanizmów na wszystkich etapach cyberkryzysu. Istotną rolę odgrywają również krajowe plany na rzecz cyberbezpieczeństwa oraz różnego rodzaju działania przygotowawcze, co wskazuje na ewolucję strategicznego myślenia w Unii o cyberbezpieczeństwie nie tylko w kategoriach reakcji na bieżące zagrożenia, ale także świadomego dążenia do zbudowania proaktywnej i odpornej postawy.

# 1. Zakres i zasady przewodnie zalecenia

Zalecenie Rady określa unijne ramy zapewniania gotowości i reagowania na cyberincydenty na dużą skalę oraz cyberkryzysy w Unii Europejskiej, nazwane w dokumencie ,,planem na rzecz cyberbezpieczeństwa". Uwzględniono w nich rolę i kompetencje państw członkowskich oraz instytucji, organów i jednostek organizacyjnych Unii, a także przewidziano koordynację polityczną Rady UE w przypadku ogólnounijnych, międzysektorowych kryzysów.

W Cyber Blueprint przedstawiono cztery zasady przewodnie, które mają zastosowanie do planu na rzecz cyberbezpieczeństwa. Pierwszą z nich jest **proporcjonalność** – w tym kontekście oznacza, że działania wskazane w zaleceniu mają zastosowanie do incydentów o zasięgu oddziaływania pozwalającym na zakwalifikowanie ich jako cyberincydenty na dużą skalę lub cyberkryzysy. Zdarzenia poniżej tego poziomu powinny podlegać dobrowolnej wymianie informacji w ramach sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieci CSIRT) i EU-CyCLONe.

Druga zasada to **pomocniczość** – główną odpowiedzialność za reagowanie na cyberincydenty, cyberincydenty na dużą skalę bądź cyberkryzysy ponoszą państwa członkowskie. Ze względu jednak na możliwe skutki transgraniczne takich zdarzeń, wszystkie wyznaczone zgodnie z przepisami prawa UE podmioty powinny współpracować z państwami i wspierać ich działania na każdym etapie zwalczania kryzysu lub incydentu.

Trzecią zasadą jest **komplementarność** – plan ma bowiem za zadanie przede wszystkim uzupełniać odpowiednie, sektorowe mechanizmy reagowania i mechanizmy zarządzania kryzysowego w Unii oraz być z nimi spójny. Do takich mechanizmów należą IPCR (zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych), ogólny system szybkiego ostrzegania ARGUS, Unijny Mechanizm

[1] 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.

Ochrony Ludności (UMOL) wspierany przez Centrum Koordynacji Reagowania Kryzysowego (ERCC), mechanizm reagowania kryzysowego ESDZ (CRM), a także inne procesy, takie jak procesy opisane w unijnym zestawie narzędzi dla dyplomacji cyfrowej[2], zestawie narzędzi do przeciwdziałania zagrożeniom hybrydowym[3] oraz w zmienionym protokole UE do celów przeciwdziałania zagrożeniom hybrydowym[4].

Czwartą, ostatnią zasadą jest zachowanie **poufności informacji** – oznacza to, że jakakolwiek wymiana informacji w ramach planu powinna odbywać się zgodnie z przepisami o bezpieczeństwie i ochronie danych osobowych, z uwzględnieniem również nieformalnych porozumień o zachowaniu poufności, np. kodu poufności TLP oraz obowiązujących zasad przetwarzania informacji niejawnych.

# 2. Zalecenie a dyrektywa NIS 2

Dyrektywa (UE) 2022/2555 (dyrektywa NIS 2)[5] ustanawia wspólny wysoki poziom cyberbezpieczeństwa w Unii Europejskiej i wprowadza obowiązki dla różnych grup podmiotów w zakresie zgłaszania incydentów. Celem zalecenia Rady jest z kolei stworzenie ram operacyjnych dla zarządzania kryzysami wynikającymi z tych incydentów na poziomie UE. W ten sposób stanowi ono pomost pomiędzy przepisami NIS 2 a praktycznym, skoordynowanym reagowaniem na cyberkryzysy i pozwala na efektywne wykorzystanie mechanizmów ustanowionych przez dyrektywę w szerszym systemie zarządzania kryzysowego Unii, zapobiegając fragmentacji działań i wzmacniając ogólną zdolność reagowania.

Jednocześnie, Cyber Blueprint odwołuje się do dyrektywy NIS 2 w zakresie dużej części definicji wykorzystywanych pojęć. Dokument dodaje do tego nową definicję ,,cyberkryzysu" jako cyberincydentu 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.

# 3. Zakres podmiotowy zalecenia

Przedstawiony w zaleceniu plan na rzecz cyberbezpieczeństwa obejmuje szeroki zakres podmiotowy, zarówno na poziomie państw członkowskich, jak i instytucji UE. Poniżej pokrótce opisane zostały wybrane podmioty, wskazane w dokumencie jako główni aktorzy europejskiego ekosystemu zarządzania cyberkryzysami.

## 3.1. Państwa członkowskie

W Cyber Blueprint wskazano, że główna odpowiedzialność za reagowanie na cyberincydenty na dużą skalę i cyberkryzysy spoczywa na państwach członkowskich. Wynika to bezpośrednio z dyrektywy NIS 2, która nakłada na nie obowiązek posiadania co najmniej jednego organu ds. zarządzania cyberkryzysami oraz sieci CSIRT, a także przyjęcia krajowych planów reagowania na cyberincydenty na dużą skalę i cyberkryzysy, obejmujących stosowne środki gotowości oraz procedury zapewniające uczestnictwo krajowych organów i podmiotów w skoordynowanym zarządzaniu na szczeblu Unii. W sytuacji kryzysu, który spowoduje uruchomienie IPCR,

[2] Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne (9916/17).
[3] Konkluzje Rady w sprawie ram skoordynowanej reakcji UE na kampanie hybrydowe, 22 czerwca 2022 r.
[4] Wspólny dokument roboczy służb „Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym" (SWD (2023) 116 final).
[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. 80–152.

krajowe organy kryzysowe powinny gromadzić informacje od organów ds. zarządzania cyberkryzysami i od krajowych sektorowych mechanizmów kryzysowych.

## 3.2. Sieć CSIRT

Sieć CSIRT jest główną siecią techniczną służącą do wymiany istotnych informacji na temat incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa, cyberzagrożeń, ryzyka i podatności, w tym w zakresie objętym zaleceniem. Udziela ona państwom członkowskim pomocy m. in. w zarządzaniu incydentami transgranicznymi.

## 3.3. CERT-UE

CERT-UE jest służbą ds. cyberbezpieczeństwa dla wszystkich podmiotów unijnych. Koordynuje reagowanie kryzysowe na poziomie technicznym oraz zarządzanie poważnymi incydentami mającymi wpływ na podmioty unijne. Działa także jako punkt wymiany informacji na temat cyberbezpieczeństwa i incydentów. CERT-UE jest członkiem sieci CSIRT i wspiera Komisję w ramach EU-CyCLONe w zakresie skoordynowanego zarządzania cyberincydentami na dużą skalę i cyberkryzysami.

## 3.4. EU-CyCLONe

EU-CyCLONe działa jako pośrednik między szczeblem technicznym a politycznym podczas zarządzania cyberincydentami na dużą skalę i cyberkryzysami. Pomaga w skoordynowanym zarządzaniu na szczeblu operacyjnym oraz zapewnia regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii, chociażby w zakresie krajowych planów reagowania oraz najlepszych praktyk. EU-CyCLONe ocenia również konsekwencje i wpływ cyberincydentów na dużą skalę i cyberkryzysów oraz proponuje możliwe środki łagodzące.

## 3.5. ENISA

ENISA zapewnia sekretariat sieci CSIRT i EU-CyCLONe. Ponadto, pomaga w opracowaniu wspólnej reakcji na transgraniczne incydenty na dużą skalę lub kryzysy poprzez m. in. agregowanie i analizę sprawozdań ze źródeł krajowych, zapewnianie przepływu informacji między poziomem technicznym, operacyjnym i politycznym oraz wspieranie podmiotów unijnych i państw członkowskich w zakresie komunikacji ze społeczeństwem.

## 3.6. Rada Unii Europejskiej

Zadaniem Rady UE jest określanie polityk w zakresie zarządzania cyberincydentami na dużą skalę oraz cyberkryzysami, czego wyrazem jest omawiane zalecenie. Ponadto, powierzono jej IPCR, obejmujące koordynację i reagowanie na kryzysy na szczeblu politycznym Unii. Decyzję w zakresie ich aktywacji lub dezaktywacji podejmuje Prezydencja Rady UE, po konsultacji z poszkodowanymi państwami członkowskimi, Komisją Europejską i Wysokim Przedstawicielem.

## 3.7. Komisja Europejska

Komisja ma za zadanie dbać o spójność i koordynację powiązanych działań w zakresie reagowania kryzysowego na szczeblu unijnym. Jest odpowiedzialna za niektóre działania w zakresie ogólnej gotowości i orientacji sytuacyjnej, w tym za zarządzanie przez Centrum Koordynacji Reagowania Kryzysowego (ERCC) i wspólnym systemem łączności i informacji w sytuacjach nadzwyczajnych (CECIS). Ponadto, 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 NIS 2 oraz obserwatorem w innych przypadkach. Jest również obserwatorem w sieci CSIRT. Komisja działa także jako punkt kontaktowy

Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa do celów wymiany istotnych informacji dotyczących poważnych incydentów z EU-CyCLONe.

### 3.8. Wysoki Przedstawiciel do Spraw Zagranicznych i Polityki Bezpieczeństwa

Wysoki Przedstawiciel prowadzi wspólną politykę zagraniczną i bezpieczeństwa Unii, w tym odpowiada za instrumenty unijnej dyplomacji cyfrowej i cyberobrony w celu powstrzymywania zagrożeń zewnętrznych i reagowania na nie. Obejmuje to wsparcie gotowości Unii i państw członkowskich w zakresie orientacji sytuacyjnej i zdolności reagowania na zagrożenia hybrydowe i cyberzagrożenia. Wysoki Przedstawiciel wspiera również unijną operacyjną sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET).

Kompletna lista podmiotów odgrywających rolę w wykonaniu planu na rzecz cyberbezpieczeństwa wraz z opisem ich kompetencji stanowi załącznik II do zalecenia.

## 4. Działania przygotowawcze na wypadek wystąpienia cyberincydentów na dużą skalę i cyberkryzysów

Skuteczne zarządzanie cyberkryzysami wymaga solidnych i odpowiednich działań przygotowawczych, które obejmują: ciągłe monitorowanie krajobrazu zagrożeń, rozwijanie wspólnej świadomości sytuacyjnej, prowadzenie regularnych ćwiczeń oraz ustanawianie jasnych procedur współpracy na wszystkich poziomach: technicznym, operacyjnym i politycznym/strategicznym.

### 4.1. Krajobraz zagrożeń i świadomość sytuacyjna

Państwa członkowskie i odpowiednie podmioty unijne powinny wprowadzić niezbędne środki w celu zwiększenia świadomości sytuacyjnej, z uwagi na to, że konkretne incydenty wymagają odpowiednich sposobów działania. Współpraca pomiędzy wspomnianymi podmiotami powinna opierać się na zweryfikowanych i wiarygodnych danych, w tym w zakresie incydentów, taktyk, technik i procedur oraz aktywnie wykorzystywanych podatności. Przy udostępnianiu informacji na szczeblu unijnym państwa członkowskie powinny w jak najszerszym zakresie wykorzystywać już istniejące platformy współpracy technicznej i operacyjnej, takie jak te w ramach sieci CSIRT i EU-CyCLONe. Ponadto sieć CSIRT, EU-CyCLONe wraz z Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB) powinny współpracować w celu zapewnienia skutecznej wymiany istotnych informacji.

ENISA odgrywa centralną rolę we wspieraniu państw członkowskich oraz instytucji, organów i agencji UE w dążeniu do osiągnięcia wspólnej unijnej świadomości sytuacyjnej na poziomie technicznym i operacyjnym. W założeniach zalecenia same państwa członkowskie i odpowiednie podmioty unijne powinny koordynować swoje działania z sektorem prywatnym, w tym ze środowiskami zajmującymi się otwartym oprogramowaniem i producentami, aby usprawnić wymianę informacji, wykorzystując program partnerstwa ENISA. Mogą również korzystać z istniejących ośrodków wymiany i analizy informacji (ISAC) na szczeblu unijnym i krajowym, aby zwiększyć zdolności w zakresie cyberbezpieczeństwa i reagowania. Realizacją założenia usprawnienia wymiany informacji jest możliwość uzgodnienia przez EU-CyCLONe, przy wsparciu ENISA oraz po konsultacji z siecią CSIRT i grupą współpracy NIS, w ciągu 24 miesięcy od przyjęcia Cyber Blueprint wspólnej ujednoliconej taksonomii wagi incydentów. Powinna się opierać na istniejących skalach i uwzględniać wpływ na usługi, liczbę potencjalnie poszkodowanych podmiotów, szkody finansowe, wizerunkowe i polityczne.

### 4.1.1. Poziom techniczny

Sieć CSIRT jest platformą współpracy technicznej i wymiany informacji między wszystkimi państwami członkowskimi oraz za pośrednictwem CERT-UE z podmiotami unijnymi. W celu zacieśnienia współpracy operacyjnej na szczeblu Unii, sieć CSIRT powinna rozważyć zaproszenie do udziału w jej pracach organów i agencji UE zaangażowanych w politykę cyberbezpieczeństwa, takich jak Europol. CERT-UE powinien gromadzić, analizować i udostępniać instytucjom, organom i jednostkom organizacyjnym Unii informacje na temat cyberzagrożeń, podatności i incydentów w jawnej infrastrukturze ICT oraz zarządzać nimi. CERT-UE powinna również współpracować i wymieniać informacje ze swoimi odpowiednikami z państw członkowskich, w tym za pośrednictwem sieci CSIRT.[6]

### 4.1.2. Poziom operacyjny

Zgodnie z dyrektywą NIS 2, sieć EU-CyCLONe powinna służyć jako platforma współpracy między organami państw członkowskich ds. zarządzania cyberkryzysami oraz z odpowiednimi podmiotami unijnymi w celu zwiększenia poziomu gotowości w zakresie zarządzania cyberincydentami na dużą skalę i cyberkryzysami oraz rozwijania wspólnej świadomości sytuacyjnej. ENISA z kolei, na podstawie przepisów dyrektywy, ma otrzymywać informacje na temat znaczących incydentów transgranicznych oraz aktywnie wykorzystywanych podatności i incydentów mających wpływ na produkty cyfrowe. Ma ona również obowiązek doradzać sieci CSIRT i EU-CyCLONe w zakresie konieczności podejmowania dalszych działań.

### 4.1.3. Poziom polityczny/strategiczny

Państwa członkowskie i odpowiednie podmioty unijne powinny monitorować rozwój sytuacji międzynarodowej, który ma wpływ na cyberbezpieczeństwo, w tym występujące lub potencjalne cyberzagrożenia, zagrożenia hybrydowe oraz zagraniczne manipulacje informacjami i ingerencje w informacje lub dezinformację. Powinny wziąć pod uwagę inicjatywy takie jak wspólne raporty techniczne o stanie cyberbezpieczeństwa w UE (JCAR), analizy dostarczone przez pojedyncze komórki analiz wywiadowczych (SIAC) i inne, istotne produkty prezentujące opinie eksperckie. Wysoki Przedstawiciel powinien informować państwa członkowskie i angażować je w działania dyplomatyczne Unii związane z cyberzagrożeniami, we współpracę z państwami trzecimi i organizacjami międzynarodowymi, w tym z NATO, oraz we wdrażanie środków dyplomatycznych, w tym środków ograniczających. 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 kryzysu.

## 4.2. Wspólne ćwiczenia

Obowiązek opracowania skutecznego, rocznego, kroczącego programu ćwiczeń, w tym na wypadek cyberkryzysów, leży w gestii Komisji, we współpracy z Wysokim Przedstawicielem i przy wsparciu ENISA, a także po konsultacji z EU-CyCLONe i siecią CSIRT. Program powinien uwzględniać także ćwiczenia w ramach innych mechanizmów reagowania kryzysowego na szczeblu Unii, takich jak UMOL i ćwiczenia określone w unijnym planie dotyczącym infrastruktury krytycznej. Ponadto, powinien on obejmować ćwiczenia opracowane z wykorzystaniem unijnych scenariuszy skoordynowanej oceny ryzyka.

Program kroczący powinien zakładać udział w ćwiczeniach wszystkich odpowiednich podmiotów, w szczególności z sektora prywatnego i NATO. ENISA, pełniąc rolę sekretariatu sieci CSIRT i EU-CyCLONe, powinna zapewniać systematyczne gromadzenie doświadczeń i wniosków z ćwiczeń, a także określać i

[6] Zgodnie z rozporządzeniem w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii - 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.

proponować sposoby ich wdrożenia. Grupa współpracy NIS powinna zwrócić się do sieci CSIRT, EU-CyCLONe i ENISA o przedstawienie takich doświadczeń i wniosków, a Rada może z kolei poprosić te podmioty o wskazanie, jakie działania podjęto na ich podstawie. Wszystkie podmioty i sieci powinny dążyć do poprawy koordynacji reagowania w przypadku cyberincydentu na dużą skalę lub cyberkryzysu na podstawie doświadczeń i wniosków z ćwiczeń. 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, obejmującego wszystkie odpowiednie podmioty, w tym poziom polityczny, sektor prywatny i NATO.

Pierwszy, kroczący program ćwiczeń należy opracować w ciągu 2 miesięcy od przyjęcia planu na rzecz cyberbezpieczeństwa, a kolejne programy należy zakończyć do 31 marca każdego roku i przedłożyć Radzie do wiadomości.

# 5. Wykrywanie incydentu, który mógłby przerodzić się w cyberincydent na dużą skalę lub cyberkryzys

Wczesne wykrywanie i odpowiednia klasyfikacja incydentów są kluczowe dla skutecznego zarządzania cyberkryzysami. Każda instytucja, zgodnie ze swoimi zadaniami, uprawnieniami oraz zakresem odpowiedzialności, która zauważy sygnały wskazujące na potencjalny cyberincydent na dużą skalę lub cyberkryzys, ma obowiązek niezwłocznie poinformować o tym odpowiednie sieci współpracy.

Zgodnie z aktem w sprawie cybersolidarności[7], jeśli transgraniczne centra cyberbezpieczeństwa dowiedzą się o dużym incydencie, muszą natychmiast przekazać te informacje państwom członkowskim i Komisji. Celem tego działania jest zapewnienie, aby wszyscy mieli taki sam, jak najbardziej aktualny obraz sytuacji. Centra przekazują informacje za pośrednictwem sieci CSIRT oraz EU-CyCLONe.

W przypadku zaobserwowania znaczącego incydentu, w szczególności takiego, który wywołuje natychmiastowe skutki, może on zostać zgłoszony do lub wykryty przez CSIRT, a także przez organy państw członkowskich ds. zarządzania cyberkryzysami lub inne organy sektorowe. Państwa UE powinny na bieżąco wymieniać się informacjami na ten temat w ramach istniejących kanałów komunikacji i sieci współpracy.

Co ważne, sieć CSIRT i EU-CyCLONe mogą zacząć działać niezależnie od siebie, w zależności od charakteru zagrożenia. Obie sieci powinny jednak ze sobą ściśle współpracować. Eksperci z sieci CSIRT doradzają sieci EU-CyCLONe, czy dany atak jest na tyle poważny, by uznać go za incydent na dużą skalę. Decyzja o aktywacji danej sieci należy wyłącznie do niej i jest podejmowana niezależnie.

Zgodnie z dyrektywą NIS 2, 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.

[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.

# 6. Reagowanie na cyberincydenty na dużą skalę i cyberkryzysy na szczeblu Unii

Skuteczne reagowanie na cyberincydenty na dużą skalę i cyberkryzysy na szczeblu Unii wymaga skoordynowanej współpracy przez wszystkich zaangażowanych - w ramach podejścia obejmującego całą administrację rządową, w tym, w miarę możliwości, organy ścigania - na każdym z poziomów: technicznym, operacyjnym i politycznym. Dotyczy to zarówno sytuacji, gdy mechanizm zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) nie został aktywowany w pełnym trybie, jak i gdy jest w pełni uruchomiony.

Na każdym szczeblu zaangażowane podmioty powinny prowadzić konkretne działania w celu osiągnięcia wspólnej świadomości sytuacyjnej oraz skoordynowanej reakcji, co zapewni uporządkowaną i skuteczną wymianę informacji. Reakcja powinna być adekwatna do skutków cyberincydentu lub cyberkryzysu, a organy państw członkowskich ds. zarządzania cyberkryzysami powinny zapewnić krajową spójność i koordynację pomiędzy poszczególnymi sektorowymi reakcjami lub działaniami.

## 6.1. Reagowanie w przypadku IPCR nieaktywnego w pełnym trybie

W przypadku cyberincydentu na dużą skalę lub cyberkryzysu, wszystkie podmioty i sieci powinny reagować w ścisłej koordynacji w sposób określony w Cyber Blueprint, przy uwzględnieniu trzech poziomów: technicznego, operacyjnego i politycznego.

**Tabela 1. Reagowanie w przypadku IPCR nieaktywnego w pełnym trybie**

| Poziom działania | Kto działa? (Główny podmiot) | Co robi? (Kluczowe zadania i działania) |
|---|---|---|
| **TECHNICZNY** | Zespół CSIRT na poziomie krajowym | • *Bezpośrednio współpracuje z zaatakowanymi firmami i instytucjami, udzielając im pomocy technicznej.*<br>• *Za pośrednictwem sieci CSIRT państwa wymieniają istotne informacje techniczne na temat incydentu, analizy dostępnych artefaktów technicznych oraz inne informacje w celu określenia przyczyny i możliwych technicznych środków łagodzących.* |
| | Sieć CSIRT | • *Łączy ekspertów z całej UE, by wymieniać dane, analizować artefakty techniczne i szukać technicznych środków łagodzących.*<br>• *Dzieli się informacjami z EU-CyCLONe w sytuacji, gdy cyberincydent może potencjalnie przerodzić się w cyberincydent na dużą skalę lub cyberkryzys.*<br>• *Utrzymuje stały kontakt z Europolem w celu wymiany informacji kluczowych dla potencjalnego śledztwa.* |

| | | |
|---|---|---|
| | Sieć CSIRT przy wsparciu ENISA | *Zbiera krajowe raporty i tworzy z nich zbiorcze podsumowanie dla poziomu operacyjnego (EU-CyCLONe).* |
| | Państwa członkowskie | *Powinny współpracować wspólnie z CSIRT z dotkniętymi incydentem podmiotami w celu reagowania i, w stosownych przypadkach, udzielania pomocy.* |
| | Zespół CSIRT lub organ państwa członkowskiego ds. zarządzania cyberkryzysami | *W przypadku powzięcia informacji o znaczącym incydencie, zachęca się je do powiadomienia o tym sieci CSIRT lub EU-CyCLONe.* |
| **OPERACYJNY** | Państwa członkowskie | • *Ograniczają skutki ataku, łagodzą jego konsekwencje i zarządzają kryzysem na własnym terytorium.*<br>• *Mogą zawnioskować o pomoc z Unijnego Mechanizmu Ochrony Ludności (UMOL) lub z rezerwy cyberbezpieczeństwa UE.*<br>  • *Państwa członkowskie mogą występować z wnioskami o usługi z rezerwy cyberbezpieczeństwa UE zgodnie z aktem o cybersolidarności, a usługi te powinny być świadczone w ciągu 24 godzin od złożenia wniosku.* |
| | EU-CyCLONe | *Ocenia skutki i konsekwencje ataku dla całej Unii, proponuje działania zaradcze i wspiera poziom polityczny w podejmowaniu decyzji.* |
| | Sieć CSIRT | *Zapewnia EU-CyCLONe oceny techniczne trwających incydentów.* |
| | Komisja Europejska | • *Koordynuje działania, gdy atak ma skutki międzysektorowe i ułatwia przepływ informacji między punktami kontaktowymi mechanizmów kryzysowych.*<br>• *Za pośrednictwem EU-CyCLONe, a w stosownych przypadkach we współpracy z Wysokim Przedstawicielem, zapewnia spójność i koordynację środków operacyjnych na szczeblu UE w dziedzinie cyberbezpieczeństwa z powiązanymi działaniami reagowania na szczeblu Unii, w szczególności w odniesieniu do wniosków o pomoc za pośrednictwem UMOL.* |

| | | |
|---|---|---|
| **POLITYCZNY** | Rada UE | *Może zażądać pełnych informacji w szczególności od Komisji, Wysokiego Przedstawiciela i EU-CyCLONe, by mieć podstawy do podjęcia odpowiedniej reakcji politycznej i strategicznej.* |
| | Rada UE (wspierana przez Komisję i Wysokiego Przedstawiciela) | • *Może podjąć decyzje strategiczne w sprawie środków reagowania, w tym o ewentualnych reakcjach dyplomatycznych (np. sankcjach).*<br>• *W przypadku konieczności uruchomienia działań w zakresie reagowania na szczeblu UE we współpracy z Komisją i Wysokim Przedstawicielem zapewnia spójność i koordynację między reagowaniem na cyberkryzys a powiązanymi działaniami reagowania na poziomie unijnym.* |
| | Służby KE (w stosownych przypadkach Europejska Służba Działań Zewnętrznych oraz odpowiednie organy Rady) | *Koordynują opracowywanie i wdrażanie środków, a także odpowiedni proces decyzyjny, zgodnie z zestawem narzędzi do przeciwdziałania zagrożeniom hybrydowym w przypadku szkodliwych działań w cyberprzestrzeni, będących częścią szerszej kampanii hybrydowej w sytuacji, gdy złożono wniosek o uruchomienie odpowiednich mechanizmów.* |
| | Państwa członkowskie | *Mogą uruchomić dodatkowe mechanizmy lub instrumenty działania w zależności od charakteru i skutków incydentu.* |
| | Różne podmioty (w ramach IPCR) | *Uruchamiają IPCR w trybie wymiany informacji, używając zdolności w zakresie zintegrowanej orientacji i analizy sytuacyjnej (ISAA) do budowania wspólnej świadomości sytuacyjnej.* |

W kontekście działań operacyjnych, gdy 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 (wymienionych w Załączniku II do Cyber Blueprint), odpowiednie podmioty (tabela 2 Załącznika II) mogą zwrócić się o uruchomienie wybranego, wskazanego w Załączniku (tabela 3) mechanizmu, tym samym wspierając podmioty sektorowe w łagodzeniu skutków incydentu.

## 6.2. Reagowanie w przypadku IPCR aktywnego w pełnym trybie

Ten tryb uruchamia się w przypadku najpoważniejszych kryzysów, które wymagają pełnej mobilizacji politycznej Unii. W przypadku aktywacji IPCR w pełnym trybie, należy wdrożyć kroki wymienione w sekcji dotyczącej reagowania bez pełnej aktywacji IPCR, ale z podwyższeniem poziomu koordynacji działań.

Jednym z głównych źródeł informacji, umożliwiających podejmowanie decyzji na szczeblu politycznym są sprawozdania w zakresie zintegrowanej orientacji i analizy sytuacyjnej (ISAA). Służą zapewnieniu wspólnej świadomości sytuacyjnej na szczeblu politycznym, przy czym sprawozdania sytuacyjne EU-CyCLONe i sieci CSIRT pozostają głównymi instrumentami zapewniającymi wspólną świadomość sytuacyjną odpowiednio na poziomie operacyjnym i technicznym.

**Tabela 2. Reagowanie w przypadku IPCR aktywnego w pełnym trybie**

| Aspekt działania | Kto działa? (Główny podmiot) | Co się zmienia? (Dodatkowe działania i procedury) |
|---|---|---|
| **Koordynacja polityczna reagowania** | Rada UE | *Przejmuje centralne dowodzenie i koordynację całej reakcji Unii, wykorzystując pełne możliwości mechanizmu IPCR.* |
| **Przepływ informacji oraz raportowanie** | ISAA (jako narzędzie) | *Sprawozdania ISAA stają się głównym, oficjalnym źródłem informacji dla decydentów politycznych, zapewniając im wspólną świadomość sytuacyjną.* |
| **Dostarczanie danych, analiz oraz ocen** | EU-CyCLONe oraz sieć CSIRT | *Dostarczają kluczowe dane, analizy i oceny, które stanowią podstawę do tworzenia sprawozdań ISAA.* |
| **Spotkania w trybie kryzysowym** | Prezydencja Rady UE | *Może zwoływać specjalne posiedzenia okrągłego stołu IPCR, aby na bieżąco i w dynamiczny sposób koordynować reakcję polityczną.* |
| **Uczestnictwo w naradach** | EU-CyCLONe | *Jest zapraszana na kluczowe posiedzenia, w tym na spotkania w ramach okrągłego stołu IPCR, aby zapewnić bezpośrednie połączenie z poziomem operacyjnym.* |
| **Spójność na poziomie krajowym** | Organy państw członkowskich | *Muszą zapewnić, że ich krajowe działania są w pełni spójne ze scentralizowaną reakcją koordynowaną na poziomie Rady UE.* |
| **Reakcje dyplomatyczne** | Rada UE i inne odpowiednie podmioty | *Są rozważane i ewentualnie wdrażane zgodnie z wcześniej uzgodnionymi procedurami, a także zgodnie z przepisami Cyber Blueprint (rozdział IX).* |

# 7. Przywrócenie normalnego funkcjonowania po cyberkryzysie i analiza wniosków

Faza odzyskiwania pełnych zdolności technicznych i operacyjnych po cyberkryzysie jest równie istotna jak samo reagowanie, a jej skuteczność zależy od poziomu współpracy i zdolności do wyciągania wniosków z przebytego lub powstrzymanego cyberincydentu na dużą skalę lub cyberkryzysu. Na etapie przywracania normalnego funkcjonowania po cyberkryzysie, państwa członkowskie, odpowiednie podmioty unijne i sieci powinny współpracować, aby zapewnić szybkie przywrócenie podstawowych funkcji systemów i sieci. W taką współpracę powinny być również zaangażowane, w stosownych przypadkach, organy ścigania.

Na tym etapie kluczowa jest także współpraca z sektorem prywatnym, zwłaszcza w procesie ułatwiania odzyskiwania danych i przywracania systemów. W ramach skutecznej koordynacji między zainteresowanymi stronami priorytetowo należy traktować minimalizację zakłóceń i zapewnienie ciągłości działania.

Po zażegnaniu zagrożenia konieczne jest skupienie się na przeanalizowaniu przebiegu realnej lub potencjalnej sytuacji kryzysowej. Podstawą do wyciągnięcia wniosków, obok doświadczeń z poprzednich kryzysów, są także oficjalne zgłoszenia incydentów, zbierane m.in. w ramach europejskiego mechanizmu przeglądu incydentów w

cyberbezpieczeństwie. Sam proces wdrażania doświadczeń i wniosków z cyberkryzysu w Cyber Blueprint wygląda następująco:

1. EU-CyCLONe zbiera wnioski, analizy i najlepsze praktyki wypracowane podczas sytuacji kryzysowej.
2. Tworzony jest kompleksowy raport, który przedstawia się sieci CSIRT, grupie współpracy NIS oraz Radzie.
3. ENISA dba o to, aby wnioski zostały wykorzystane poprzez aktualizację planów gotowości i organizację dostosowanych ćwiczeń z zakresu reagowania i cyberobrony na wypadek przyszłych zagrożeń, kryzysów lub incydentów.

# 8. Działania w dziedzinie komunikacji

Ważnym elementem działań związanych z reagowaniem na cyberincydent na dużą skalę lub cyberkryzys jest odpowiednia komunikacja skierowana do ludności cywilnej. Jej prowadzenie należy do kompetencji państw członkowskich, jednak ze względu na transgraniczny charakter zdarzeń niezbędna jest koordynacja działań w tym obszarze, zarówno pomiędzy państwami, których dotyczą, jak i instytucjami unijnymi. Z tego względu, w zaleceniu podkreślono znaczenie wymiany informacji na temat działań komunikacyjnych w ramach EU-CyCLONe i sieci CSIRT. Rekomendacja ta obejmuje nie tylko prowadzenie wymiany informacji w trakcie już trwającego incydentu lub kryzysu, ale także w ramach działań przygotowawczych, jako dzielenie się najlepszymi praktykami w zakresie np. kampanii uświadamiających.

# 9. Reakcja dyplomatyczna i współpraca z partnerami strategicznymi oraz podmiotami wojskowymi

Kwestie komunikacji zewnętrznej podczas i po kryzysie bądź incydencie, w tym komunikacji strategicznej czy kontaktów z różnymi grupami i interesariuszami, stanowią jeden z kluczowych elementów procesu reagowania na incydenty. Z tego względu, reakcja na polu dyplomatycznym i współpraca z partnerami strategicznymi stanowią nieodzowny element unijnych ram zarządzania cyberkryzysami.

Wysoki Przedstawiciel, w ścisłej współpracy z Komisją i innymi odpowiednimi podmiotami UE, wspiera proces decyzyjny w Radzie. Obejmuje to sporządzanie analiz, sprawozdań i wniosków dotyczących stosowania ewentualnych środków w ramach unijnego zestawu narzędzi dla dyplomacji cyfrowej – *Diplomacy Toolbox*. W przypadku stwierdzenia incydentu, Wysoki Przedstawiciel ułatwia przepływ niezbędnych informacji z partnerami strategicznymi, w tym, w stosownych przypadkach, z NATO. Do jego zadań należy również wzmocnienie koordynacji z partnerami strategicznymi w zakresie reagowania na szkodliwe działania w cyberprzestrzeni prowadzone przez tzw. stałych agresorów.

W szerszym zakresie, państwa członkowskie, Wysoki Przedstawiciel, Komisja i inne odpowiednie podmioty UE współpracują z partnerami strategicznymi i organizacjami międzynarodowymi w celu propagowania dobrych praktyk i odpowiedzialnego zachowania państw w domenie cyberbezpieczeństwa oraz zapewnienia szybkiej, skoordynowanej reakcji w przypadku potencjalnych cyberincydentów. Współpraca na linii UE/NATO powinna przebiegać w myśl uzgodnionych zasad przewodnich dotyczących inkluzywności, wzajemności i przejrzystości oraz przy pełnym poszanowaniu autonomicznego procesu decyzyjnego w ramach wspólnoty europejskiej.

Ponadto, 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 działań i wymiany informacji z NATO w przypadku cyberkryzysu w celu zacieśniania współpracy w zakresie reagowania.

W tym celu UE przeanalizuje, jak poprawić wymianę informacji z NATO, w szczególności poprzez zapewnienie narzędzi do bezpiecznej komunikacji, przy jednoczesnym uwzględnieniu standardów wymiany informacji obowiązujących w poszczególnych państwach członkowskich.

W ramach unijnego, kroczącego programu ćwiczeń w dziedzinie cyberbezpieczeństwa służby Komisji i ESDZ powinny rozważyć zorganizowanie ćwiczenia z NATO. Celem powinno być przetestowanie współpracy między podmiotami cywilnymi i wojskowymi na wypadek cyberincydentu na dużą skalę lub cyberkryzysu. Ćwiczenie to powinno zostać przeprowadzone w ramach unijnego ćwiczenia *Integrated Resolve* (równoległe i skoordynowane ćwiczenie – PACE), z zapewnieniem udziału wszystkich podmiotów, o których mowa w planie na rzecz cyberbezpieczeństwa. Dodatkowo w porozumieniu z Radą, Komisją i Wysokim Przedstawicielem należy również rozważyć wspólne ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu unijnym z krajami Bałkanów Zachodnich, Republiką Mołdawii, Ukrainą, a także z innymi partnerami strategicznymi i państwami o podobnych do europejskich wartościach.

# 10. Koordynacja zarządzania cyberkryzysami z podmiotami wojskowymi

Współpraca między cywilnymi i wojskowymi podmiotami zajmującymi się cyberbezpieczeństwem jest kluczowa dla zbudowania, utrzymania i prawidłowego działania kompleksowego i skoordynowanego systemu cyberobrony. Rolą poszczególnych państw członkowskich jest zacieśnianie tej współpracy na poziomie krajowym.

EU-CyCLONe i sieć CSIRT określą możliwe sposoby i procedury współpracy z podmiotami wojskowymi UE, takimi jak unijna konferencja dowódców ds. obrony cyberprzestrzeni (*EU Cyber Commanders Conference*) i operacyjna sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET). EU-CyCLONe i sieć CSIRT powinny informować Radę o postępach poczynionych w odniesieniu do tego rodzaju współpracy.

W przypadku, gdy w kontekście cyberincydentu na dużą skalę lub cyberkryzysu wykorzystywane są odpowiednie krajowe lub międzynarodowe wojskowe zdolności reagowania, poszkodowane państwo członkowskie jest zachęcane do powiadomienia o tym EU-CyCLONe, a także ESDZ. Takie powiadomienie powinno być uzgodnione wspólnie przez użytkownika i podmiot zapewniający wspomnianą zdolność reagowania. W ramach 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.

# 11. Dalsze działania

W ciągu roku od publikacji zalecenia EU-CyCLONe, we współpracy z siecią CSIRT i innymi, głównymi podmiotami unijnego ekosystemu zarządzania cyberkryzysami oraz przy wsparciu ENISA, opracuje szczegółowe schematy przedstawiające przepływy informacji między odpowiednimi podmiotami, procesy decyzyjne i sprawozdania opracowane podczas zarządzania cyberincydentami na dużą skalę lub cyberkryzysami.

Ponadto, w przypadku, gdy w trakcie wspólnych ćwiczeń z cyberbezpieczeństwa zidentyfikowane zostaną wyzwania lub luki utrudniające stosowanie planu na rzecz cyberbezpieczeństwa przedstawionego w zaleceniu, Rada UE opracuje zestaw wytycznych wykonawczych, które zaadresują te trudności.

Przegląd zalecenia będzie dokonywany przez Komisję Europejską, we współpracy z państwami członkowskimi, co najmniej raz na cztery lata. Ma to na celu uwzględnienie zmieniającego się krajobrazu zagrożeń, wyników wspólnych ćwiczeń i zmian legislacyjnych.

# 12. Wnioski i rekomendacje

1. Cyber Blueprint ma strategiczne znaczenie dla kształtowania spójnych, zintegrowanych i efektywnych unijnych ram reagowania na cyberkryzysy i incydenty o dużej skali w obszarze cyberbezpieczeństwa, które mogą mieć dalekosiężne konsekwencje dla państw członkowskich i podmiotów unijnych. Zalecenie dzieli system reagowania cyberkryzysowego na trzy poziomy: techniczny, operacyjny i polityczny (strategiczny), jednocześnie nadając określonym podmiotom lub kategoriom podmiotów określone role i zadania.

2. Silny nacisk został położony na współpracę w zakresie przygotowania, reagowania i przywracania normalnego funkcjonowania po kryzysie – koordynacja w tym zakresie stanowi podstawę do efektywności zaproponowanego w dokumencie systemu. Wymaga to od państw członkowskich oraz instytucji UE podjęcia wysiłków w tym obszarze w jeszcze większym stopniu niż dotychczas.

3. Zalecenie stanowi impuls do przejścia od reaktywnego do proaktywnego zarządzania cyberkryzysami i cyberincydentami na dużą salę, kładąc nacisk na jasny podział kompetencji i ról, współpracę pomiędzy podmiotami, krajami i instytucjami UE, a także na działania przygotowawcze i regularne ćwiczenia.

4. W zaleceniu ENISA została wyznaczona jako instytucja odpowiedzialna za wdrażanie wniosków i rekomendacji z doświadczeń z reagowania na kryzysy. To elastyczne i dynamiczne podejście zapewnia, że plany na rzecz cyberbezpieczeństwa, procedury oraz programy ćwiczeń są aktualne i dostosowane do krajobrazu zagrożeń.

5. Cyber Blueprint, mimo niewiążącego charakteru, stanowi kolejną „cegiełkę” w ekosystemie cyberbezpieczeństwa i cyberobrony w UE, zarówno na poziomie instytucji, wspólnoty jako całości, jak i poszczególnych państw członkowskich. Przejawem tego są chociażby odwołania do już funkcjonujących instytucji, inicjatyw lub grup, powołanych na podstawie innych aktów prawnych (NIS 2, akt w sprawie cybersolidarności).

6. Korzystnym dla państw członkowskich byłoby podjęcie wspólnych inicjatyw mających na celu dalszą harmonizację działań takich jak tworzenie procedur reagowania, wymiana informacji o cyberzagrożeniach, opracowywanie wniosków z przebytych kryzysów oraz wymiana dobrych praktyk w zakresie wykorzystania ze środków unijnych (np. z UMOL, mechanizmu IPCR czy środków z rezerwy cyberbezpieczeństwa UE) na rzecz poprawy bezpieczeństwa.