Rada
Unii Europejskiej

Bruksela, 6 grudnia 2024 r.
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Dotyczy:	Konkluzje Rady w sprawie ENISA

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie ENISA, w wersji zatwierdzonej przez Radę na jej posiedzeniu w dniu 6 grudnia 2024 r.

ZAŁĄCZNIK

Projekt konkluzji Rady w sprawie ENISA

RADA UNII EUROPEJSKIEJ,

1. PODKREŚLA, że wyzwania pochodzące z globalnej cyberprzestrzeni nigdy nie były tak złożone, zróżnicowane i poważne, jak obecnie, ze względu na wyrafinowanie pojawiających się zagrożeń cyberbezpieczeństwa, stale zmieniające się środowisko bezpieczeństwa i obecne napięcia geopolityczne. W związku z tym UE i jej państwa członkowskie powinny kontynuować wysiłki na rzecz zwiększenia odporności z myślą o skutecznym identyfikowaniu obecnych i pojawiających się zagrożeń i wyzwań oraz reagowaniu na nie. ZWRACA UWAGĘ, że prace na rzecz podwyższenia poziomu cyberodporności powinny być kontynuowane w ramach podejścia obejmującego całe społeczeństwo. PODKREŚLA, że w nadchodzących latach UE i jej państwa członkowskie powinny skupić się na skutecznym wdrażaniu inicjatyw ustawodawczych i nieustawodawczych stanowiących podstawę wszystkich działań podjętych dotychczas w tym zakresie i przyczyniających się do ich realizacji.

2. PRZYPOMINAJĄC, że bezpieczeństwo narodowe pozostaje w wyłącznej gestii każdego państwa członkowskiego, POTWIERDZA, że w ostatnich latach UE i jej państwa członkowskie podjęły wspólne działania na wielką skalę nad ustanowieniem niezbędnej struktury instytucjonalnej i form współpracy w dziedzinie cyberprzestrzeni zarówno na szczeblu krajowym, jak i unijnym. PRZYJMUJE Z ZADOWOLENIEM różne inicjatywy ustawodawcze i nieustawodawcze, które zapewniły UE i jej państwom członkowskim mocne i solidne ramy w tej dziedzinie, zwiększające ogólną cyberodporność Unii. Ramy te ewoluowały, obejmując rozmaite aspekty cyberbezpieczeństwa: bezpieczeństwo, dyplomację, egzekwowanie prawa i obronę. ODNOTOWUJE, że duża liczba podmiotów – w tym organy państw członkowskich ds. cyberbezpieczeństwa, grupa współpracy ds. bezpieczeństwa sieci i informacji (NIS CG), sieć CSIRT, europejska sieć organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU-CyCLONe), sieć krajowych ośrodków koordynacji (NCC), Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa (ECCG), Komisja, Europejska Służba Działań Zewnętrznych (ESDZ), Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), CERT-UE, Europejska Agencja Obrony (EDA) oraz działające w strukturach Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) – wchodzi w skład ekosystemu cyberbezpieczeństwa UE, przy czym każdy z tych podmiotów pełni swoją rolę we wdrażaniu ogólnounijnych ram cyberbezpieczeństwa.

3. UZNAJE, że w ciągu ostatnich dwudziestu lat ENISA okazała się nieocenionym elementem europejskiego ekosystemu cyberbezpieczeństwa, odgrywając kluczową rolę w aktywnym wspieraniu państw członkowskich oraz instytucji, organów, urzędów i agencji UE (EUIBA) we wdrażaniu i opracowywaniu polityki cyberbezpieczeństwa, w budowaniu zdolności i gotowości, we współpracy oraz w promowaniu świadomości i certyfikacji cyberbezpieczeństwa.

OGÓLNE ZALECENIA DOTYCZĄCE POLITYKI

4. ZWRACA SIĘ do Komisji, by wykorzystała **ocenę aktu o cyberbezpieczeństwie** jako okazję do zbadania, w jaki sposób ocena ta może przyczynić się do uproszczenia złożonego ekosystemu cyberbezpieczeństwa, zwiększając tym samym skuteczność i efektywne wykorzystanie zasobów. W związku z tym WZYWA Komisję do zapewnienia, aby mandat ENISA w zakresie wspierania państw członkowskich oraz instytucji, organów, urzędów i agencji UE (EUIBA) był ukierunkowany i jasno określony, z wyszczególnieniem konkretnych celów strategicznych i priorytetowych zadań, obok bardziej precyzyjnego podziału zadań i kompetencji w odniesieniu do innych podmiotów. W tym kontekście ZWRACA SIĘ do Komisji o przeanalizowanie i dalsze wzmocnienie roli ENISA we wspieraniu współpracy operacyjnej na szczeblu UE i między państwami członkowskimi w zakresie zwiększania cyberodporności, z uwzględnieniem kompetencji państw członkowskich w tej dziedzinie. Ponadto WZYWA Komisję do wzmocnienia doradczej roli ENISA w zapewnianiu eksperckich i opartych na dowodach wytycznych i zaleceń w odniesieniu do wdrażania obecnych i przyszłych inicjatyw ustawodawczych i nieustawodawczych UE, przy jednoczesnym zapewnieniu spójnych unijnych ram cyberbezpieczeństwa.

5. W tym samym duchu ZACHĘCA Komisję, by rozważyła optymalizację roli ENISA w odniesieniu do zadań, które nie leżą u podstaw jej misji. PODKREŚLA, że **obowiązki** ENISA **zostały znacznie rozszerzone** w następstwie niedawnych inicjatyw ustawodawczych, w tym m.in. dyrektywy NIS 2, aktu dotyczącego cyberodporności i aktu w sprawie cybersolidarności. ODNOTOWUJĄC, że ENISA otrzymała dodatkowe zasoby w wyniku niektórych z tych inicjatyw, PODKREŚLA, że rozszerzenie obowiązków ENISA oraz rosnąca złożoność zagrożeń cyberbezpieczeństwa i wyzwań na tym polu doprowadziły do znacznego zwiększenia zadań Agencji, co powinno znaleźć odzwierciedlenie w **odpowiednich zasobach** – ludzkich, finansowych i technicznych – aby w pełni umożliwić jej wykonywanie wszystkich zadań wchodzących w zakres jej kompetencji, nie przesądzając o wynikach negocjacji w sprawie wieloletnich ram finansowych. W tym celu WZYWA Komisję, by podczas przygotowywania projektu budżetu ogólnego Unii priorytetowo potraktowała działania i zadania związane ze wspieraniem państw członkowskich w zwiększaniu ich cyberodporności i współpracy operacyjnej oraz w rozwijaniu i wdrażaniu przez nie prawa Unii.

WSPARCIE UDZIELANE PRZEZ ENISA NA RZECZ OPRACOWYWANIA I WDRAŻANIA POLITYKI

6. PRZYPOMINA, że w obecnych ramach prawnych dotyczących cyberbezpieczeństwa ENISA powierzono szereg kluczowych obowiązków w zakresie wsparcia i doradztwa w całej UE. PRZYJMUJE Z ZADOWOLENIEM rolę ENISA w tym zakresie w zapewnianiu **pomocy państwom członkowskim** w skutecznym wdrażaniu inicjatyw ustawodawczych i nieustawodawczych. WZYWA ENISA, aby w ścisłej współpracy z grupą ds. bezpieczeństwa sieci i informacji (NIS CG) i Komisją nadal przedstawiała ogólne spostrzeżenia i analizy na temat obecnego otoczenia prawnego w zakresie cyberbezpieczeństwa. ZACHĘCA ENISA, aby regularnie i w sposób ustrukturyzowany udostępniała i aktywnie promowała wytyczne techniczne i najlepsze praktyki, pomagając państwom członkowskim we wdrażaniu polityki i przepisów w zakresie cyberbezpieczeństwa.

7. UZNAJE kluczową rolę ENISA w opracowywaniu **europejskich systemów certyfikacji cyberbezpieczeństwa**, które stanowią podstawę zaufania do produktów, usług i procesów ICT, a ponadto do usług zarządzanych w zakresie bezpieczeństwa w świetle zbliżającej się ukierunkowanej zmiany aktu o cyberbezpieczeństwie. PODKREŚLA, że państwa członkowskie i przemysł są zaniepokojone długotrwałym procesem wyboru, opracowywania i przyjmowania systemów certyfikacji cyberbezpieczeństwa; w związku z tym PILNIE WZYWA Komisję do wykorzystania możliwości, jaką stwarza ocena aktu o cyberbezpieczeństwie, aby znaleźć sposoby na przyjęcie prostszego, opartego na analizie ryzyka, a także bardziej przejrzystego i szybszego podejścia do opracowywania unijnych systemów certyfikacji cyberbezpieczeństwa, a jednocześnie ZWRACA UWAGĘ NA ważną rolę państw członkowskich w tym procesie. Ponadto PODKREŚLA znaczenie wyraźnego przypisania odpowiedzialności za utrzymywanie każdego systemu certyfikacji. PRZYPOMINA również, że ENISA powinna terminowo konsultować się ze wszystkimi odpowiednimi zainteresowanymi stronami w drodze formalnego, otwartego, przejrzystego i inkluzywnego procesu podczas przygotowywania propozycji systemów oraz że Komisja powinna konsultować się w sposób otwarty, przejrzysty i inkluzywny przy ocenie efektywności i wykorzystania przyjętych systemów. ZACHĘCA ENISA do dalszego zacieśniania współpracy ze środowiskami ochrony danych, w szczególności z Europejską Radą Ochrony Danych, w stosownych przypadkach, oraz z właściwymi organami krajowymi, ze szczególnym uwzględnieniem wspierania synergii w kontekście opracowywania przyszłych europejskich systemów certyfikacji cyberbezpieczeństwa.

8. Aby zapobiec niepotrzebnym obciążeniom administracyjnym, które mogłyby wynikać ze złożonych ram sprawozdawczości, WZYWA ENISA, by we współpracy z Komisją kontynuowała wymianę informacji z państwami członkowskimi na temat praktycznych aspektów, uproszczenia i usprawnienia procedury sprawozdawczej. Ponadto PRZYPOMINA o swoim zaproszeniu skierowanym do Komisji, by przy wsparciu ENISA i innych odpowiednich unijnych podmiotów przygotowała zestawienie odpowiednich obowiązków sprawozdawczych określonych w odpowiednich aktach ustawodawczych UE dotyczących cyberprzestrzeni i kwestii cyfrowych. PRZYPOMINA, że wymiana informacji między ENISA a państwami członkowskimi opiera się na relacji opartej na zaufaniu, w której bezpieczeństwo i poufność są gwarantowane zgodnie z aktem o cyberbezpieczeństwie oraz odpowiednimi przepisami i protokołami, i powinna być ograniczona do tego, co jest istotne i proporcjonalne w świetle celu wymiany informacji. PODKREŚLA, że dane i informacje muszą być traktowane z należytą starannością.

9. PODKREŚLA, że ENISA jest odpowiedzialna za ustanowienie i utrzymywanie **jednolitej platformy sprawozdawczej na mocy aktu dotyczącego cyberodporności**, która będzie wnosiła konkretną operacyjną wartość dodaną, zwłaszcza w przypadku aktywnie wykorzystywanych podatności i poważnych incydentów mających wpływ na bezpieczeństwo produktów z elementami cyfrowymi. Biorąc pod uwagę szeroki zakres tych przepisów horyzontalnych, jednolita platforma sprawozdawcza powinna być skutecznym i bezpiecznym narzędziem ułatwiającym wymianę informacji między krajowymi zespołami CSIRT a ENISA. W związku z tym PILNIE WZYWA ENISA do przydzielenia wystarczających zasobów ludzkich, aby przyspieszyć ustanowienie platformy jako jeden z kluczowych priorytetów, tak by zapewnić jej gotowość w terminie określonym w akcie dotyczącym cyberodporności.

10. UZNAJE rolę ENISA w tworzeniu **europejskiej bazy danych dotyczących podatności**, której celem jest zapewnienie większej przejrzystości w odniesieniu do ujawniania podatności, przy jednoczesnym zapewnieniu odpowiedniego postępowania z danymi wrażliwymi. Biorąc pod uwagę koniec okresu transpozycji dyrektywy NIS 2, PILNIE WZYWA ENISA do zintensyfikowania wszelkich niezbędnych prac w celu zapewnienia sprawnego funkcjonowania tej bazy danych. Jednocześnie ZACHĘCA grupę współpracy ds. bezpieczeństwa sieci i informacji (NIS CG) do dalszego rozpowszechniania, z pomocą ENISA, wytycznych, polityk i procedur dotyczących ujawniania podatności.

11. DOCENIA korzyści płynące z **działania wspierającego cyberbezpieczeństwo** realizowanego przez ENISA, które funkcjonuje jako pula usług w zakresie cyberbezpieczeństwa dostępnych dla państw członkowskich w celu uzupełnienia ich wysiłków, a także doświadczenie ENISA zdobyte podczas jego wdrażania. W związku z tym PODKREŚLA, że ENISA powinna odgrywać centralną rolę w zarządzaniu unijną rezerwą cyberbezpieczeństwa i jej obsłudze. ZACHĘCA ENISA do rozpoczęcia przygotowywania zestawienia potrzebnych usług i ich dostępności natychmiast po wejściu w życie aktu w sprawie cybersolidarności, aby unijna rezerwa cyberbezpieczeństwa była jak najbardziej użyteczna i dostosowana do potrzeb użytkowników we wszystkich państwach członkowskich. ZACHĘCA ENISA, by – gdy zostanie jej powierzone to zadanie – angażowała państwa członkowskie, w szczególności poprzez gromadzenie informacji na temat wymaganych kryteriów i informowanie o przyszłych przetargach, na wczesnym etapie procesu tworzenia unijnej rezerwy cyberbezpieczeństwa. ZACHĘCA ENISA, by – gdy zostanie jej powierzone to zadanie – zapewniła, aby proces wyboru zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa był przejrzysty, otwarty, sprawiedliwy i umożliwiał udział dostawców ze wszystkich państw członkowskich, niezależnie od wielkości. Ponadto PRZYPOMINA, że ENISA ma obowiązek bez zbędnej zwłoki wydać wytyczne dotyczące interoperacyjności dla transgranicznych centrów cyberbezpieczeństwa.

12. PODKREŚLA, że **monitorowanie tendencji w zakresie powstających technologii** w szybko zmieniającej się dziedzinie, jaką jest cyberbezpieczeństwo, ma kluczowe znaczenie dla utrzymania i dalszego wzmacniania naszej pozycji w cyberprzestrzeni. DOCENIA działania, które prowadzi ENISA, aby zwrócić uwagę społeczeństwa na zagrożenia i możliwości związane z takimi technologiami, jak sztuczna inteligencja i obliczenia kwantowe, ułatwiając w ten sposób lepsze zrozumienie obecnych wyzwań. Zachęca ENISA do dalszego przyczyniania się do realizacji tych zadań, do aktywnego propagowania wdrażania jej zaleceń oraz, w stosownych przypadkach, do doradzania ECCC i współpracy z tym ośrodkiem.

WSPARCIE UDZIELANE PRZEZ ENISA PAŃSTWOM CZŁONKOWSKIM NA RZECZ ZWIĘKSZANIA CYBERODPORNOŚCI I ULEPSZANIA WSPÓŁPRACY OPERACYJNEJ

13. PODKREŚLA, że ENISA odgrywa ważną rolę **jako sekretariat dwóch sieci współpracy w dziedzinie cyberbezpieczeństwa prowadzonych przez państwa członkowskie na szczeblu UE: sieci CSIRT i EU-CyCLONe**. PODKREŚLA cenny wkład ENISA w działania grupy koordynacyjnej ds. bezpieczeństwa sieci i informacji, zwłaszcza w formie aktywnego zaangażowania i wkładu technicznego w różne obszary prac. ZACHĘCA ENISA do dalszego wspierania funkcjonowania i współpracy tych sieci w przyszłości, ponieważ stanowią one podstawowe kanały współpracy państw członkowskich na różnych szczeblach.

14. PRZYPOMINA o potrzebie ulepszenia **wspólnej orientacji sytuacyjnej** na szczeblu UE, która przyczynia się do wzmacniania pozycji UE w cyberprzestrzeni w związku z wykrywaniem cyberincydentów, zapobieganiem im i reagowaniem na nie. W związku z tym PODKREŚLA znaczenie działań prognostycznych ENISA, regularnych sprawozdań i ocen zagrożenia, które to elementy przyczyniają się wszystkie do poprawy orientacji sytuacyjnej. ZACHĘCA ENISA, by blisko współpracowała z państwami członkowskimi na rzecz rozwoju orientacji sytuacyjnej na szczeblu UE. W tym kontekście DOCENIA ważną rolę ENISA wraz z CERT-UE i Europolem we wspieraniu Rady za pomocą briefingów sytuacyjnych w kontekście zestawu narzędzi dla dyplomacji cyfrowej uzupełniających orientację sytuacyjną zapewnianą przez pojedynczą komórkę analiz wywiadowczych (SIAC) i PODKREŚLA potrzebę stworzenia kompleksowego obrazu zagrożeń na podstawie różnych źródeł, w tym z sektora prywatnego. ZACHĘCA w związku z tym do dalszego rozwijania współpracy ENISA z ESDZ, a w szczególności z Intcen, przy pełnym poszanowaniu ich odpowiednich mandatów.

15. PODKREŚLA, że centrum ds. orientacji sytuacyjnej i analiz w zakresie cyberbezpieczeństwa przy Komisji pełni wewnętrzną funkcję w Komisji i jest wspierane przez współpracę z ENISA i CERT-UE. ZWRACA SIĘ do Komisji, by – z myślą o zmaksymalizowaniu potencjału synergii i zmniejszeniu złożoności ekosystemu cyberbezpieczeństwa UE – wzięła pod uwagę wyniki oceny aktu o cyberbezpieczeństwie, a także dyskusji na temat oceny planu na rzecz cyberbezpieczeństwa („Cyber Blueprint”), aby zoptymalizować zadania centrum ds. orientacji sytuacyjnej i analiz w zakresie cyberbezpieczeństwa przy Komisji oraz powiązane zadania ENISA. ZACHĘCA Komisję do unikania niepotrzebnego powielania zadań, przy jednoczesnym zachowaniu centralnej roli ENISA w rozwijaniu wspólnej orientacji sytuacyjnej na szczeblu Unii w celu wsparcia państw członkowskich, z należytym poszanowaniem ich kompetencji krajowych.

16. ZWRACA UWAGĘ, że rozwijanie wspólnej orientacji sytuacyjnej jest warunkiem koniecznym terminowego i skutecznego zarządzania kryzysowego w całej Unii. PODKREŚLA, że w **reagowaniu na cyberincydenty na dużą skalę** zaangażowane są na szczeblu UE różne kluczowe podmioty oraz że w razie wystąpienia takich incydentów skuteczna współpraca między państwami członkowskimi opiera się głównie na sieciach CSIRT i EU-CyCLONe. ENISA odgrywa ważną rolę w zarządzaniu kryzysami cyberbezpieczeństwa jako sekretariat sieci CSIRT i EU-CyCLONe. ZWRACA SIĘ do Komisji, by w ocenie planu na rzecz cyberbezpieczeństwa znalazły należyte odzwierciedlenie dodatkowe zadania i obowiązki związane z wkładem w opracowanie wspólnej reakcji na transgraniczne cyberincydenty lub kryzysy cyberbezpieczeństwa na dużą skalę, a także rola powierzona ENISA jako sekretariatowi sieci CSIRT i EU-CyCLONe oraz na mocy najnowszych przepisów dotyczących cyberbezpieczeństwa.

17. PODKREŚLA znaczenie organizowania regularnych **ćwiczeń w dziedzinie cyberbezpieczeństwa**, które znacznie podnoszą gotowość UE do reagowania na incydenty i kryzysy. UZNAJE, że ENISA zebrała cenne i rozległe doświadczenie w tej dziedzinie, wspierając państwa członkowskie. UZNAJE ważną rolę ENISA na etapach planowania, przygotowania, realizacji i oceny ćwiczeń w dziedzinie cyberbezpieczeństwa i PODKREŚLA, że powinna ona pozostać jednym z głównych podmiotów na szczeblu UE, pamiętając, że takie ćwiczenia powinny być przeprowadzane w oparciu o ustrukturyzowane ramy i wspólną terminologię. ZACHĘCA ENISA oraz sieci CSIRT i EU-CyCLONe do jak najefektywniejszego wykorzystania istniejących regularnych ćwiczeń w celu testowania i udoskonalania unijnych ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa oraz do zapewnienia jak najpełniejszego wykorzystania wyciągniętych wniosków.

WSPÓŁPRACA ENISA Z INNYMI PODMIOTAMI W EKOSYSTEMIE CYBERBEZPIECZEŃSTWA

18. PRZYPOMINA, że ze względu na horyzontalny charakter cyberbezpieczeństwa **współpraca między wszystkimi podmiotami na szczeblu państw członkowskich i Unii** ma zasadnicze znaczenie, i w związku z tym PODKREŚLA, że zwiększenie ogólnej cyberodporności na szczeblu europejskim wymaga również współpracy ENISA z innymi odpowiednimi podmiotami w dziedzinie cyberbezpieczeństwa.

19. PODKREŚLA, że zdolność instytucji, organów, urzędów i agencji UE do zachowania cyberbezpieczeństwa jest ważna dla ogólnej cyberodporności na szczeblu UE, a rola CERT-UE jest w tym kontekście bezcenna. W związku z tym PRZYJMUJE Z ZADOWOLENIEM ugruntowaną współpracę strukturalną między CERT-UE a ENISA i ZACHĘCA te podmioty do kontynuowania ścisłej współpracy w przyszłości.

20. Dzięki osiągniętej autonomii finansowej ECCC w znacznym stopniu przyczyni się do rozwoju silnego europejskiego ekosystemu badań przemysłowych i technologicznych w dziedzinie cyberbezpieczeństwa, obejmującego umiejętności w zakresie rozwoju siły roboczej zgodnie ze swoim mandatem. ZACHĘCA ENISA i ECCC do dalszej ścisłej współpracy, zwłaszcza w odniesieniu do potrzeb i priorytetów w zakresie badań naukowych i innowacji, a także umiejętności w dziedzinie cyberbezpieczeństwa, w celu zwiększenia konkurencyjności unijnego sektora cyberbezpieczeństwa. ZWRACA SIĘ do Komisji, by przeanalizowała, w jaki sposób można jeszcze bardziej zoptymalizować synergie w pracy ENISA i ECCC oraz jak lepiej usprawnić działania zgodnie z ich odpowiednimi mandatami.

21. PODKREŚLA, że regularne aktualizowanie krajobrazu zagrożeń pozwala lepiej określić, jakie środki i narzędzia są potrzebne do skutecznego zwalczania cyberprzestępczości. ZWRACA UWAGĘ na wartość dodaną sprawozdań UE dotyczących wspólnej oceny cyberbezpieczeństwa (EU JCAR), które są wynikiem współpracy między ENISA, EC3 Europolu i CERT-UE, i które już wniosły cenny wkład w stawianie czoła różnym wyzwaniom, w tym w zakresie walki z cyberprzestępczością. ZACHĘCA ENISA i Europol do dalszej ustrukturyzowanej współpracy w przyszłości.

22. PODKREŚLA, że cyberobrona stanowi ważny i stale rozwijający się składnik przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni. ZWRACA UWAGĘ na potrzebę współpracy ENISA z ESDZ i Komisją w przypadkach, w których ENISA ma do odegrania rolę we wspieraniu wdrażania polityki UE w zakresie cyberobrony, w ścisłej współpracy z EAO, ECCC i środowiskami zajmującymi się cyberobroną. KŁADZIE NACISK na rolę ENISA jako agencji cywilnej. PODKREŚLA znaczenie pogłębiania i usprawniania współpracy cywilno-wojskowej w dziedzinie cyberbezpieczeństwa w UE, w tym jasnego podziału ról i obowiązków między obiema społecznościami oraz między UE a NATO, przy pełnym poszanowaniu zasad inkluzywności, wzajemności, wzajemnej otwartości i przejrzystości, a także autonomii decyzyjnej obu organizacji. ZACHĘCA ENISA do kontynuowania współpracy z Agencją NATO ds. Łączności i Informatyki.

23. ZACHĘCA UE do dalszego promowania naszych wspólnych wartości i wspólnych wysiłków na forach światowych, aby stać na straży wolnej, globalnej, otwartej i bezpiecznej cyberprzestrzeni. PODKREŚLA, że transgraniczny charakter cyberzagrożeń i cyberincydentów wymaga ścisłej i skutecznej współpracy nie tylko na szczeblu UE, ale również **z organizacjami i partnerami międzynarodowymi**. ZAUWAŻA, że międzynarodowe zaangażowanie ENISA powinno koncentrować się na strategicznych partnerach i krajach kandydujących do UE, zgodnie ze wspólną polityką zagraniczną i bezpieczeństwa UE. PODKREŚLA, że w ramach swojego międzynarodowego zaangażowania ENISA powinna działać zgodnie ze swoim mandatem i odpowiednimi przepisami aktu o cyberbezpieczeństwie. UZNAJE konieczność wyjaśnienia, zgodnie z odpowiednimi procedurami, kwestii międzynarodowego zaangażowania ENISA, a w szczególności zapewnienia, aby jej zarząd był należycie i terminowo informowany o powiązanych działaniach. ZACHĘCA ENISA do angażowania się w odpowiednie międzynarodowe ramy współpracy w dziedzinie cyberbezpieczeństwa, w tym z organizacjami takimi jak NATO i OBWE.

24. PRZYPOMINA, że UE i jej państwa członkowskie często zwracały uwagę na luki w **umiejętnościach w zakresie cyberbezpieczeństwa**. PRZYPOMINA, że Komisja i ENISA wprowadziły szerokie i kompleksowe ramy zapewniające wytyczne dla wszystkich zainteresowanych stron, takie jak europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa, komunikat w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa oraz corocznie organizowana Europejska Konferencja na temat Umiejętności w dziedzinie Cyberbezpieczeństwa, oraz ZACHĘCA Komisję i ENISA do wykorzystania tych inicjatyw, ze szczególnym uwzględnieniem trwających dyskusji na temat konsorcjum na rzecz europejskiej infrastruktury cyfrowej (EDIC). W tym celu ZWRACA SIĘ do Komisji, by utrzymywała kontakty z państwami członkowskimi zainteresowanymi utworzeniem EDIC. UZNAJE, że zarówno ENISA, jak i ECCC, są upoważnione do promowania umiejętności w całej Unii. ZWRACA SIĘ do ENISA, by priorytetowo potraktowała wspieranie wysiłków państw członkowskich w zakresie umiejętności i edukacji, zwiększając ogólną świadomość społeczną, i by w stosownych przypadkach współpracowała z ECCC.

25. ODNOTOWUJE, że w ostatnich latach ENISA rozwinęła **współpracę z sektorem prywatnym**. PRZYPOMINA, że ponieważ sektor prywatny stale monitoruje krajobraz cyberzagrożeń, informacje gromadzone przez branżę mogłyby przyczynić się do poprawy wspólnej orientacji sytuacyjnej. W związku z tym ZACHĘCA ENISA, by w ścisłej współpracy z państwami członkowskimi i między podmiotami UE zacieśniała współpracę z sektorem prywatnym.

26. WZYWA Komisję i ENISA do rozważenia sposobów zacieśnienia współpracy między ENISA a europejskimi organami **normalizacyjnymi**. PODKREŚLA, że ENISA musi zwiększać swoją wiedzę fachową w zakresie europejskiej normalizacji cyberbezpieczeństwa m.in. poprzez monitorowanie działań normalizacyjnych i udział w takich działaniach.

27. PILNIE WZYWA Komisję i ENISA do zbadania, w jaki sposób można jeszcze bardziej zoptymalizować funkcjonowanie unijnych ram cyberbezpieczeństwa, z uwzględnieniem zaleceń i propozycji przedstawionych w niniejszych konkluzjach. Stała współpraca, ustalanie priorytetów w zakresie zadań i zasobów, a także uproszczenie złożonego ekosystemu cyberbezpieczeństwa stanowić będą kluczowe elementy umożliwiające sprostanie obecnym i przyszłym wyzwaniom.