Rada
Unii Europejskiej

Bruksela, 8 października 2021 r.
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

NOTA DO PUNKTU I/A

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli (część II)/Rada
Dotyczy:	Konkluzje Rady w sprawie zbadania potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni – uzupełnienie skoordynowanego reagowania na szczeblu UE na cyberincydenty i cyberkryzysy na dużą skalę – Zatwierdzenie

1. 23 czerwca 2021 r. Komisja opublikowała zalecenie w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni[1], by przeciwdziałać rosnącej liczbie poważnych cyberincydentów mających wpływ na usługi publiczne, a także na funkcjonowanie przedsiębiorstw i życie obywateli w całej Unii Europejskiej.

2. 28 czerwca 2021 r. Komisja przedstawiła to zalecenie Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni. Kolejne dyskusje prowadzono pod przewodnictwem prezydencji słoweńskiej na posiedzeniach wspomnianej grupy roboczej 7 i 14 lipca 2021 r. w celu zebrania opinii państw członkowskich na temat przedmiotowego zalecenia Komisji.

[1] C(2021) 4520 final (dok. 11155/21 i 11155/21 ADD1).

3. 23 lipca 2021 r. na nieformalnej wideokonferencji członków Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni prezydencja przedstawiła pierwszy projekt konkluzji Rady pt. „Zbadanie potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni – uzupełnienie skoordynowanego reagowania na szczeblu UE na cyberincydenty i cyberkryzysy na dużą skalę”[2]. Projekt ten był następnie omawiany na posiedzeniach tej grupy roboczej 8 i 29 września 2021 r.

4. Na posiedzeniu 6 października 2021 r. Horyzontalna Grupa Robocza ds. Cyberprzestrzeni uzgodniła projekt konkluzji Rady w wersji przedstawionej w załączniku.

5. W związku z powyższym Komitet Stałych Przedstawicieli proszony jest o przedłożenie Radzie załączonego projektu konkluzji oraz o zaproponowanie, by przyjęła ona ten projekt konkluzji jako jeden z punktów A porządku obrad.

---

[2] Dok. 10975/21.

ZAŁĄCZNIK

Projekt konkluzji Rady pt. „Zbadanie potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni – uzupełnienie skoordynowanego reagowania na szczeblu UE na cyberincydenty i cyberkryzysy na dużą skalę”

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC:

– konkluzje Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[3],

– konkluzje Rady w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę[4],

– konkluzje Rady w sprawie dyplomacji elektronicznej[5],

– konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”)[6],

– konkluzje Rady w sprawie bezpieczeństwa i obrony[7],

– ramy polityki UE w zakresie cyberobrony[8],

– konkluzje Rady pt. „Kształtowanie cyfrowej przyszłości Europy”[9],

– decyzję wykonawczą Rady (UE) 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych

---

3 Dok. 7290/21.
4 Dok. 10086/18.
5 Dok. 6122/15 + COR 1.
6 Dok. 10474/17.
7 Dok. 8396/21.
8 Dok. 15585/14.
9 Dok. 8711/20.

– konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”[10],

– konkluzje Rady w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa[11],

1. PODKREŚLA znaczenie cyberbezpieczeństwa dla budowania odpornej, cyfrowej i ekologicznej Europy. ZAZNACZA, że cyberbezpieczeństwo jest niezbędne dla dobrobytu i bezpieczeństwa UE i jej państw członkowskich, jej obywateli, przedsiębiorstw i instytucji, a także dla utrzymania integralności naszych wolnych i demokratycznych społeczeństw.

2. DOSTRZEGA transgraniczny i międzysektorowy charakter wielu zagrożeń dla cyberbezpieczeństwa oraz ryzyko i potencjalne konsekwencje spowodowane ciągłym konfrontowaniem się ze zorganizowanymi szkodliwymi działaniami w cyberprzestrzeni, które mają większą siłę oddziaływania, są coraz bardziej wyrafinowane, ukierunkowane, złożone, uporczywe i rozpowszechnione[12]. Pandemia COVID-19 jeszcze bardziej ujawniła podatność naszych społeczeństw na zagrożenia i zakres potencjalnych szkód, jakie cyberincydenty na dużą skalę mogą wyrządzać w gospodarce i w sferze demokracji, usług podstawowych i infrastruktury krytycznej, zwłaszcza w sektorze opieki zdrowotnej. Zwiększyła również znaczenie konektywności i uzależnienia naszego społeczeństwa od niezawodnych, godnych zaufania i bezpiecznych sieci i systemów informatycznych. Pandemia podkreśliła też potrzebę globalnego, otwartego, wolnego, stabilnego i bezpiecznego internetu, a także potrzebę zaufania do produktów, procesów i usług z zakresu technologii informacyjno-komunikacyjnych i do poziomu ich bezpieczeństwa, w tym potrzebę zapewnienia odpornego łańcucha dostaw.

---

10 Dok. 14435/17 + COR 1.
11 Dok. 7737/19.
12 Sprawozdanie ENISA dotyczące krajobrazu zagrożeń za rok 2020.

3. PONOWNIE PODKREŚLA znaczenie cyberodporności i dalszego rozwijania unijnych ram zarządzania kryzysowego w cyberprzestrzeni[13] z myślą o podejmowaniu skutecznych działań na szczeblu UE w reakcji na cyberkryzysy i cyberincydenty na dużą skalę i znaczenie kontynuowania włączania cyberodporności w istniejące horyzontalne i sektorowe unijne mechanizmy reagowania kryzysowego. PODKREŚLA rolę Rady i zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) w zapewnianiu terminowej koordynacji i reagowania na szczeblu politycznym w sytuacjach kryzysowych o dalekosiężnych skutkach lub dużym znaczeniu politycznym, niezależnie od tego, czy źródło danego kryzysu leży w UE czy poza nią. WSKAZUJE, że istotne jest testowanie takich ram i mechanizmów w ramach regularnych ćwiczeń.

4. PRZYPOMINA, że działania na szczeblu UE w reakcji na cyberkryzysy i cyberincydenty na dużą skalę prowadzone są zgodnie z zasadami pomocniczości, proporcjonalności, komplementarności, niepowielania i poufności. PONOWNIE PODKREŚLA, że to państwa członkowskie mają w pierwszej kolejności obowiązek reagowania na dotyczące ich cyberincydenty i cyberkryzysy na dużą skalę. PRZYPOMINA o znaczeniu poszanowania kompetencji państw członkowskich i ich wyłącznej odpowiedzialności za bezpieczeństwo narodowe, zgodnie z art. 4 ust. 2 Traktatu o Unii Europejskiej, w tym również w dziedzinie cyberbezpieczeństwa.

5. PODKREŚLA jednocześnie znaczenie poszanowania kompetencji i uprawnień instytucji, organów i agencji UE. Wysoki Przedstawiciel, Komisja i inne unijne instytucje, organy i agencje również mają do odegrania istotną, wynikająca z prawa Unii rolę, m.in. ze względu na możliwe skutki cyberincydentów i cyberkryzysów na dużą skalę dla jednolitego rynku, a także dla funkcjonowania samych instytucji, organów i agencji UE.

---

[13] Dok. 10086/18.

6. AKCENTUJE potrzebę unikania zbędnego powielania działań i dążenia do komplementarności i wartości dodanej w dalszym rozwijaniu unijnych ram zarządzania kryzysowego w cyberprzestrzeni oraz potrzebę zapewnienia zgodności tych ram z istniejącymi mechanizmami, inicjatywami, procesami i procedurami na szczeblu krajowym i europejskim. PODKREŚLA znaczenie usprawnienia istniejących procesów i struktur w celu zmniejszenia złożoności oraz znaczenie poprawy – w interesie spójności w Unii – dostępności i zdolności reagowania na potrzeby osób, które zwracają się o pomoc i solidarność.

7. UZNAJE, że prawo międzynarodowe, w tym cała Karta Narodów Zjednoczonych, międzynarodowe prawo humanitarne i prawa człowieka, mają zastosowanie w cyberprzestrzeni i ZACHĘCA, by przestrzegać dobrowolnych, niewiążących norm, przepisów i zasad odpowiedzialnego zachowania państw w cyberprzestrzeni zatwierdzonych przez wszystkie państwa członkowskie ONZ.

8. Z ZADOWOLENIEM PRZYJMUJE postępy poczynione w ostatnich latach w Radzie, zwłaszcza w ramach prac Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni i innych odpowiednich grup roboczych Rady, a także postępy w zakresie ustanawiania przez państwa członkowskie innych inicjatyw, sieci i mechanizmów współpracy i wymiany informacji, szczególnie ustanowienie grupy współpracy NIS i sieci zespołów CSIRT na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r., europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), a także odpowiednich projektów związanych z cyberobroną zainicjowanych w ramach stałej współpracy strukturalnej (PESCO)[14], ustanowienie Wspólnej Grupy Zadaniowej ds. Przeciwdziałania Cyberprzestępczości (J-CAT), europejskiej sieci sądowej ds. cyberprzestępczości (EJCN), wyraża także zadowolenie z dobrowolnych wkładów państw członkowskich na rzecz Centrum Analiz Wywiadowczych UE (INTCEN) i z koordynacji działań i współpracy w kontekście zestawu narzędzi dla dyplomacji cyfrowej.

---

[14] W szczególności projekty dotyczące: zespołów szybkiego reagowania na cyberincydenty i pomocy wzajemnej w zakresie cyberbezpieczeństwa (projekt koordynowany przez Litwę), Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (projekt koordynowany przez Niemcy), Platformy wymiany informacji o cyberzagrożeniach i reagowaniu na cyberincydenty (projekt koordynowany przez Grecję).

9. PRZYPOMINA o istniejących ramach współpracy między instytucjami, organami i agencjami UE, takich jak współpraca strukturalna między agencją ENISA a CERT-UE i protokół ustaleń między agencją ENISA, Europejską Agencją Obrony (EDA), Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) i CERT-UE. PODKREŚLA znaczenie stałej i regularnej wymiany informacji z Radą na temat rozwijania tych form współpracy.

10. KŁADZIE NACISK na wagę wzmocnionej współpracy i wymiany informacji między różnymi podmiotami zajmującymi się cyberbezpieczeństwem, w UE i jej państwach członkowskich, na wszystkich niezbędnych szczeblach – technicznym, operacyjnym i strategicznym/politycznym – oraz wagę łączenia istniejących mechanizmów, sieci, struktur, procesów i procedur w zakresie zarządzania kryzysowego, tam gdzie wspiera to i usprawnia reagowanie na cyberincydenty i cyberkryzysy na duża skalę.

11. ODNOTOWUJE postępy osiągnięte przez grupę państw członkowskich w tworzeniu wspólnych operacyjnych cyberzdolności w formie „zespołów szybkiego reagowania na cyberincydenty" w ramach PESCO, których celem jest pogłębianie dobrowolnej współpracy w cyberprzestrzeni poprzez wzajemną pomoc, m.in. w zakresie reagowania na cyberincydenty i cyberkryzysy na dużą skalę.

12. UZNAJE doświadczenia i zdolności w zakresie reagowania 24 godziny na dobę przez 7 dni w tygodniu, jakimi dysponuje społeczność organów ścigania w dziedzinie współpracy operacyjnej i bezpiecznej wymiany informacji w przypadku poważnych transgranicznych cyberataków – zdobyte dzięki stosowaniu protokołu działań UE w zakresie egzekwowania prawa w sytuacjach kryzysowych.

13. DOSTRZEGA WYSIŁKI w zakresie wdrażania ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni (zestaw narzędzi dla dyplomacji cyfrowej). PRZYPOMINA, że każde państwo członkowskie ma swobodę podejmowania suwerennych decyzji w zakresie ustalenia podmiotu odpowiedzialnego za szkodliwe działanie w cyberprzestrzeni, indywidualnie dla każdego przypadku. PRZYPOMINA, że środki podejmowane w ramach wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni powinny być oparte na wspólnej orientacji sytuacyjnej uzgodnionej przez państwa członkowskie. EU INTCEN odgrywa centralną rolę jako ośrodek zapewniania na rzecz UE orientacji sytuacyjnej i oceny zagrożeń dotyczących cyberprzestrzeni w oparciu o dane wywiadowcze przekazywane dobrowolnie przez państwa członkowskie, bez uszczerbku dla kompetencji tych państw.

14. PONOWNIE PODKREŚLA znaczenie wzajemnej pomocy i solidarności, zgodnie z art. 42 ust. 7 Traktatu o Unii Europejskiej i art. 222 Traktatu o funkcjonowaniu Unii Europejskiej oraz WZYWA do przeprowadzania dalszych ćwiczeń dotyczących cyberprzestrzeni. PRZYPOMINA, że istnieje potrzeba przeanalizowania powiązań między unijnymi ramami zarządzania kryzysowego w cyberprzestrzeni, zestawem narzędzi dla dyplomacji cyfrowej a zapisami we wspomnianych powyżej artykułach – na wypadek wystąpienia cyberincydentu lub cyberkryzysu na dużą skalę. PRZYPOMINA ponadto, że obowiązki państw członkowskich wynikające z art. 42 ust. 7 Traktatu o Unii Europejskiej pozostają bez uszczerbku dla szczególnego charakteru polityki bezpieczeństwa i obrony niektórych państw członkowskich. PRZYPOMINA również, że NATO w dalszym ciągu jest fundamentem zbiorowej obrony dla tych państw, które są jego członkami.

15. DOCENIA współpracę UE–NATO w zakresie cyberbezpieczeństwa i cyberobrony, w tym wymianę informacji między CERT-UE a komórką NATO ds. reagowania na incydenty komputerowe (NCIRC), prowadzoną przy pełnym poszanowaniu zasad przejrzystości, wzajemności i inkluzywności, a także autonomii decyzyjnej obu organizacji.

16. UZNAJE znaczenie prowadzenia w stosownych przypadkach współpracy z sektorem prywatnym w zakresie działań na rzecz wymiany informacji oraz udostępniania odpowiedniej wiedzy fachowej, a także zaufanych rozwiązań i usług, w tym na przykład co udzielania wsparcia w zakresie reagowania na incydenty i wzmacniania orientacji sytuacyjnej wśród różnych społeczności zajmujących się cyberbezpieczeństwem.

17. PODKREŚLA znaczenie bezpiecznych kanałów komunikacji dla wymiany informacji niejawnych i szczególnie chronionych. WSKAZUJE na potrzebę dokonywania dalszych postępów.

W tym względzie i mając na uwadze powyższe:

18. UZNAJE zalecenie Komisji w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni za inicjatywę, którą należy uwzględnić przy dalszym rozwijaniu unijnych ram zarządzania kryzysowego w cyberprzestrzeni[15].

19. WZYWA UE i jej państwa członkowskie do kontynuowania ich wysiłków na rzecz bardziej kompleksowych i skutecznych unijnych ram zarządzania kryzysowego w cyberprzestrzeni, w oparciu o istniejące mechanizmy i już osiągnięte postępy, oraz do uwzględnienia potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni, uznając ją za uzupełnienie tych mechanizmów – poprzez stosowanie podejścia stopniowego. PODKREŚLA, że stopniowy, przejrzysty i inkluzywny proces jest niezbędny do zwiększenia zaufania, ma on więc zasadnicze znaczenie dla dalszego rozwoju unijnych ram zarządzania kryzysowego w cyberprzestrzeni. Proces ten powinien przebiegać przy poszanowaniu istniejących ról, kompetencji i uprawnień państw członkowskich i instytucji, organów i agencji UE, a także zasad określonych w niniejszych konkluzjach, w tym zasady proporcjonalności, pomocniczości, inkluzywności, komplementarności, niepowielania i poufności informacji. PRZYPOMINA jednocześnie, że wszelki potencjalny udział państw członkowskich w ewentualnej wspólnej jednostce ds. cyberprzestrzeni ma charakter dobrowolny.

---

[15] C(2021) 4520 final (dok. 11155/21 i 11155/21 ADD1).

20. PODKREŚLA potrzebę ustanowienia odpowiednich metod pracy i zarządzania, by umożliwić zaangażowanie i udział wszystkich państw członkowskich w dyskusjach, opracowywaniu i skutecznych procesach decyzyjnych dotyczących unijnych ram zarządzania kryzysowego w cyberprzestrzeni, w tym w odniesieniu do inicjatywy dotyczącej ewentualnej wspólnej jednostki ds. cyberprzestrzeni. APELUJE o poszanowanie uprawnień Rady wynikających z Traktatów oraz zasady lojalnej współpracy.

21. KŁADZIE NACISK na znaczenie identyfikowania i angażowania wszystkich odpowiednich społeczności zajmujących się cyberbezpieczeństwem w UE i jej państwach członkowskich, z uwzględnieniem ich różnych ról i obowiązków w przypadku różnych rodzajów cyberincydentów i cyberkryzysów na dużą skalę. PODKREŚLA zasadniczą rolę Rady, szczególnie za pośrednictwem Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni, w kształtowaniu polityki i pełnieniu funkcji koordynacyjnej w odniesieniu do dalszego rozwoju unijnych ram zarządzania kryzysowego w cyberprzestrzeni. ZACHĘCA zatem państwa członkowskie, Komisję, Europejską Służbę Działań Zewnętrznych (ESDZ), EU INTCEN, CERT-UE, agencję ENISA, Europol (EC3), Eurojust (EJCN), Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC), a także przedstawicieli sieci CSIRT, EU-CyCLONe, grupy współpracy NIS, EDA i przedstawicieli odpowiednich projektów PESCO oraz inne możliwe zainteresowane strony do zaangażowania się w ten proces. Należy poddać dalszej analizie zawartą w zaleceniu Komisji propozycję, by utworzyć grupę roboczą działającą pod politycznym kierownictwem Rady i gwarantującą odpowiednią reprezentację wszystkich państw członkowskich, która pełniłaby rolę tymczasowego forum skupiającego przedstawicieli wszystkich odpowiednich społeczności zajmującymi się cyberbezpieczeństwem w UE i jej państwach członkowskich. Taka grupa robocza powinna regularnie składać sprawozdania ze swojej działalności i przedstawiać Radzie ewentualne sugestie do dyskusji, zatwierdzenia lub prośby o dalsze wskazówki. Ponadto można ustanowić inne formy dialogu w obrębie społeczności i między społecznościami, m.in. w formie warsztatów, seminariów, wspólnych szkoleń i ćwiczeń.

22. PODKREŚLA rolę Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) i sieci krajowych ośrodków koordynacji w odniesieniu do ewentualnej wspólnej jednostki ds. cyberbezpieczeństwa, zwłaszcza biorąc pod uwagę, że jego zadaniem ma być istotne zwiększenie unijnych możliwości technologicznych, technologicznych rozwiązań, zdolności i umiejętności w dziedzinie cyberbezpieczeństwa.

23. ZACHĘCA UE i jej państwa członkowskie do zaangażowania w dalszy rozwój unijnych ram zarządzania kryzysowego w cyberprzestrzeni, w tym poprzez zbadanie potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberbezpieczeństwa, a więc do ustanowienia i zdefiniowania przedmiotowego procesu, w tym określenia etapów pośrednich i harmonogramu, oraz do sprecyzowania celów i ewentualnych ról i obowiązków. UWYPUKLA potrzebę skonsolidowania w pierwszej kolejności istniejących sieci i interakcji w ramach każdej społeczności, a także konieczność przeprowadzenia dokładnej identyfikacji ewentualnych luk i potrzeb w zakresie wymiany informacji, jakie istnieją w obrębie społeczności zajmujących się cyberbezpieczeństwem i między tymi społecznościami, a także w europejskich instytucjach, organach i agencjach i w ramach ich współpracy, co pociąga za sobą konieczność uzgodnienia potencjalnych głównych celów i priorytetów ewentualnej wspólnej jednostki ds. cyberbezpieczeństwa. Nie przesądzając o wyniku, PODKREŚLA konieczność skupienia się na określeniu potrzeb w zakresie wymiany informacji w celu budowania wspólnej orientacji sytuacyjnej wśród wszystkich odpowiednich społeczności. Przy identyfikacji luk i potrzeb w zakresie wymiany informacji, w tym w odniesieniu do ewentualnego wykorzystywania platform wirtualnych, należy zwrócić należytą uwagę na bezpieczne kanały komunikacji służące wymianie informacji niejawnych i szczególnie chronionych; Rada ZWRACA jednocześnie UWAGĘ na znaczenie wykorzystywania już istniejącej infrastruktury. Wprowadzenie podejścia stopniowego ma na celu zbudowanie zaufania i podstawy dla ewentualnych dalszych kroków związanych ze zwiększaniem gotowości i współpracy operacyjnej. DOSTRZEGA, że różne cele mogą wymagać różnych rozwiązań i zaangażowania różnorodnych przedstawicieli odpowiednich społeczności zajmujących się cyberbezpieczeństwem w UE i w państwach członkowskich.

24. WZYWA do prowadzenia dalszych analiz w zakresie podstawy prawnej dla ewentualnej wspólnej jednostki ds. cyberprzestrzeni w odniesieniu do całości procesu, w tym w kontekście zadań i ról tej jednostki w odniesieniu do zadań i ról przypisanych w zaleceniu agencji ENISA w świetle art. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. APELUJE o dalsze refleksje nad poszczególnymi elementami zalecenia w sprawie wspólnej jednostki ds. cyberprzestrzeni, w tym w odniesieniu do koncepcji unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa i unijnego planu reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa. PODKREŚLA, że ewentualna wspólna jednostka ds. cyberprzestrzeni musi respektować kompetencje, mandaty i uprawnienia swoich ewentualnych przyszłych uczestników.

25. WZYWA UE i jej państwa członkowskie, by rozważyły potencjał inicjatywy dotyczącej wspólnej jednostki ds, cyberprzestrzeni, również z perspektywy instytucji, organów i agencji UE, z myślą o uzupełnieniu bieżących wysiłków na szczeblu państw członkowskich. Z ZADOWOLENIEM PRZYJMUJE wyrażony przez Komisję zamiar wzmocnienia odporności odpowiednich instytucji, organów i agencji UE za pośrednictwem przyszłego wniosku dotyczącego rozporządzenia w sprawie wspólnych wiążących zasad cyberbezpieczeństwa dla instytucji, organów i agencji UE.

26. Na zakończenie POTWIERDZA swoje zaangażowanie na rzecz zwiększenia cyberodporności i dalszego rozwijania unijnych ram zarządzania kryzysowego w cyberprzestrzeni i BĘDZIE REGULARNIE MONITOROWAĆ postępy i przedstawiać dalsze wytyczne w celu uzupełniania wspomnianych unijnych ram.