Rada
Unii Europejskiej

**Bruksela, 23 maja 2022 r.**
**(OR. en)**

**9364/22**

| | |
|---|---|
| **CYBER 183** | **EUMC 170** |
| **COPEN 202** | **IPCR 54** |
| **COPS 228** | **HYBRID 46** |
| **COSI 142** | **DISINFO 45** |
| **DATAPROTECT 166** | **COTER 126** |
| **IND 189** | **CSDP/PSDC 304** |
| **JAI 698** | **CFSP/PESC 685** |
| **JAIEX 57** | **CIVCOM 93** |
| **POLMIL 120** | **RECH 262** |
| **RELEX 681** | **PROCIV 65** |
| **TELECOM 237** | |

**WYNIK PRAC**

| | |
|---|---|
| Od: | Sekretariat Generalny Rady |
| Data: | 23 maja 2022 r. |
| Do: | Delegacje |
| Dotyczy: | Konkluzje Rady w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni<br>– Konkluzje Rady zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. |

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni, w wersji zatwierdzonej przez Radę na posiedzeniu w dniu 23 maja 2022 r.

**ZAŁĄCZNIK**

**Konkluzje Rady w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni**

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC:

– konkluzje w sprawie wspólnego komunikatu z dnia 25 czerwca 2013 r. do Parlamentu Europejskiego i Rady pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń”[1],

– ramy polityki UE w zakresie cyberobrony[2],

– konkluzje w sprawie zarządzania internetem[3],

– konkluzje w sprawie dyplomacji elektronicznej[4],

– konkluzje w sprawie wzmacniania europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego[5],

– konkluzje w sprawie wspólnego komunikatu z dnia 20 listopada 2017 r. do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”[6],

– konkluzje w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”)[7],

– konkluzje w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę[8],

---

1 Dok. 12109/13.
2 Dok. 15585/14.
3 Dok. 16200/14.
4 Dok. 6122/15 + COR 1.
5 Dok. 14540/16.
6 Dok. 14435/17 + COR 1.
7 Dok. 10474/17.
8 Dok. 10086/18.

– konkluzje w sprawie wytycznych dotyczących budowania przez UE zewnętrznych zdolności cyfrowych[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[10],
– konkluzje w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa[11],
– konkluzje w sprawie znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczenia zagrożeń dla bezpieczeństwa związanych z 5G[12],
– konkluzje w sprawie przyszłości wysoce ucyfrowionej Europy po roku 2020: „Stymulowanie cyfrowej i gospodarczej konkurencyjności i spójności cyfrowej w całej Unii”[13],
– konkluzje w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych[14],
– konkluzje w sprawie kształtowania cyfrowej przyszłości Europy[15],
– konkluzje w sprawie cyberbezpieczeństwa urządzeń podłączonych do internetu[16],
– konkluzje w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[17],
– konkluzje w sprawie bezpieczeństwa i obrony[18],
– konkluzje w sprawie zbadania potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni – uzupełnienie skoordynowanego reagowania na szczeblu UE na cyberincydenty i cyberkryzysy na dużą skalę[19].
– Strategiczny kompas na rzecz bezpieczeństwa i obrony – dla Unii Europejskiej, która chroni swoich obywateli, swoje wartości i interesy oraz przyczynia się do międzynarodowego pokoju i bezpieczeństwa[20],

---

9 Dok. 10496/18.
10 Dz.U. L 320 z 17.12.2018, s. 28–34.
11 Dok. 7737/19.
12 Dok. 14517/19.
13 Dok. 9596/19.
14 Dok. 14972/19.
15 Dok. 8711/20.
16 Dok. 13629/20.
17 Dok. 7290/21.
18 Dok. 8396/21.
19 Dok. 13048/21.
20 Dok. 7371/22.

1. PODKREŚLA, że w ostatnich latach odnotowano nasilenie się szkodliwych zachowań w cyberprzestrzeni, zarówno ze strony podmiotów państwowych, jak i niepaństwowych, w tym gwałtowny i stały wzrost szkodliwych działań wymierzonych w infrastrukturę krytyczną, łańcuchy dostaw i własność intelektualną UE i jej państw członkowskich, podwyższone ryzyko wystąpienia skutków ubocznych oraz zwiększenie liczby ataków z użyciem oprogramowania szantażującego, których celem są przedsiębiorstwa, organizacje i obywatele. ODNOTOWUJE, że wraz z powrotem do polityki siłowej niektóre państwa w coraz większym stopniu próbują kwestionować i podważać w cyberprzestrzeni międzynarodowy ład oparty na zasadach, sprawiając, że sfera cyfrowa – obok morza pełnego, przestrzeni powietrznej i przestrzeni kosmicznej – staje się obszarem, w którym coraz częściej dochodzi do konfrontacji. DOSTRZEGA, że coraz powszechniejsze stają się zakrojone na szeroką skalę cyberataki lub próby ingerowania w sieć i systemy informatyczne oraz próby ich zakłócenia czy też zniszczenia mające systemowe skutki i że mogą one zagrażać naszemu bezpieczeństwu gospodarczemu oraz wpływać na nasze instytucje i procesy demokratyczne, a także że są one dowodem na to, że niektóre podmioty są gotowe narazić na szwank bezpieczeństwo i stabilność na świecie. PODKREŚLA, że agresja wojskowa Rosji na Ukrainę pokazała, że ofensywne działania w cyberprzestrzeni mogą być prowadzone jako integralna część strategii hybrydowych łączących zastraszanie, destabilizowanie i zakłócenia gospodarcze.

2. PONOWNIE STWIERDZA, że wobec bieżących zmian geopolitycznych siła naszej Unii leży w jedności, solidarności i determinacji i że wdrożenie Strategicznego kompasu zwiększy strategiczną autonomię UE i jej zdolność do współpracy z partnerami na rzecz ochrony jej wartości i interesów, także w dziedzinie cyfrowej. PODKREŚLA, że silniejsza UE o większych zdolnościach w dziedzinie bezpieczeństwa i obrony przyczyni się zdecydowanie do zapewnienia bezpieczeństwa światowego i transatlantyckiego i uzupełnia działania NATO, które pozostaje podstawą zbiorowej obrony swoich członków. POTWIERDZA, że UE zamierza zwiększyć wsparcie na rzecz międzynarodowego ładu opartego na zasadach, którego centralnym elementem jest Organizacja Narodów Zjednoczonych.

3. Zgodnie z konkluzjami Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa i ze Strategicznym kompasem PONOWNIE STWIERDZA, że należy rozwijać pozycję Unii w kwestiach cyberprzestrzeni w drodze zwiększenia naszej umiejętności zapobiegania cyberatakom poprzez budowanie i rozwój zdolności, szkolenia, ćwiczenia, zwiększoną odporność oraz w drodze zdecydowanej reakcji na cyberataki wymierzone w UE i jej państwa członkowskie, wykorzystującej wszystkie narzędzia dostępne UE. Obejmuje to m.in. dalsze wykazywanie przez UE determinacji w natychmiastowym i długoterminowym reagowaniu na działania podmiotów stwarzających zagrożenie, które starają się utrudnić nam bezpieczny i otwarty dostęp do cyberprzestrzeni i niekorzystnie oddziałują na nasze strategiczne interesy, w tym bezpieczeństwo naszych partnerów. W tym kontekście ZAZNACZA, że pozycja w kwestiach cyberprzestrzeni ma łączyć różne inicjatywy owocujące działaniami UE konsolidującymi pokój i stabilność w cyberprzestrzeni i sprzyjającymi jej otwartości, wolności, globalności, stabilności i bezpieczeństwu, a zarazem zapewniać lepszą koordynację krótko-, średnio- i długoterminowych działań na rzecz zapobiegania cyberzagrożeniom i cyberatakom, zniechęcania do ich inicjowania, powstrzymywania ich i reagowania na nie, jak również zapewniać wykorzystywanie zdolności cyfrowych. PODKREŚLA, że elementy te należy uwzględnić w pozycji UE w kwestiach cyberprzestrzeni, zgodnie z pięcioma zadaniami UE w tej dziedzinie, którymi są: wzmocnienie naszej cyberodporności i naszych zdolności do ochrony; wzmocnienie solidarnego i kompleksowego zarządzania kryzysowego; promowanie naszej wizji cyberprzestrzeni; międzynarodowa współpraca z państwami trzecimi i organizacjami międzynarodowymi; zapobieganie cyberatakom, obrona przed nimi i reagowanie na nie.

## I. WZMOCNIENIE NASZEJ CYBERODPORNOŚCI I NASZYCH ZDOLNOŚCI DO OCHRONY

4. PONOWNIE STWIERDZA, że należy podnieść ogólny poziom cyberbezpieczeństwa, OCZEKUJE na szybkie przyjęcie projektu dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS), projektu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) i projektu dyrektywy w sprawie odporności podmiotów krytycznych (CER) i PRZYJMUJE DO WIADOMOŚCI wniosek w sprawie rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii – z myślą o wspieraniu Unii Europejskiej, która chroni swoich obywateli, usługi publiczne i przedsiębiorstwa w cyberprzestrzeni. ZACHĘCA Komisję do sfinalizowania przyjęcia kluczowych wniosków służących zabezpieczeniu infrastruktury, technologii, produktów i usług cyfrowych, tak by dać wyraźny sygnał co do ambicji UE w tych kwestiach i by umożliwić wspieranie przedsiębiorstw w stawianiu czoła związanym z tym wyzwaniom. APELUJE do Komisji, aby w akcie dotyczącym cyberodporności, którego projekt Komisja powinna przedłożyć przed końcem 2022 r., zaproponowała wspólne unijne wymogi w zakresie cyberbezpieczeństwa dotyczące połączonych urządzeń oraz powiązanych procesów i usług, uwzględniając potrzebę zastosowania podejścia horyzontalnego i kompleksowego, które obejmie cały cykl życia produktów cyfrowych, a także obowiązujące przepisy, w szczególności w obszarze cyberbezpieczeństwa.

5. ZWRACA SIĘ do stosownych organów, takich jak Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC), Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), grupa współpracy ds. bezpieczeństwa sieci i informacji (NIS), oraz do Komisji Europejskiej o opracowanie – w oparciu o ocenę ryzyka – zaleceń dla państw członkowskich i Komisji Europejskiej w celu zwiększenia odporności sieci i infrastruktury łączności na terytorium Unii Europejskiej, w tym w celu stałego stosowania unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G.

6. APELUJE do UE i jej państw członkowskich, aby intensywniej dążyły do podniesienia ogólnego poziomu cyberbezpieczeństwa, np. poprzez ułatwianie podejmowania działalności przez zaufanych dostawców usług w zakresie cyberbezpieczeństwa, a także ZAZNACZA, że zachęcanie do rozwijania takiej działalności powinno być jednym z priorytetów unijnej polityki przemysłowej w obszarze cyberbezpieczeństwa. Z myślą o skuteczniejszym opieraniu się i przeciwdziałaniu atakom o potencjalnych systemowych skutkach i w oparciu o doświadczenia w radzeniu sobie z lukami w zabezpieczeniach Solarwinds, Microsoft Exchange i Apache Log4J ZWRACA SIĘ do Komisji, by zaproponowała, jak można zachęcić nowe podmioty do działalności w branży zaufanych dostawców usług w zakresie cyberbezpieczeństwa, zwiększyć cyberbezpieczeństwo w teleinformatycznym łańcuchu dostaw oraz wyeliminować potencjalny wpływ na UE i jej państwa członkowskie luk w oprogramowaniu, w tym w kontekście opracowywanego aktu dotyczącego cyberodporności, a także jak usprawnić wykrywanie cyberzagrożeń oraz zwiększyć zdolności dzielenia się informacjami na ich temat w państwach członkowskich i między nimi.

7. PONOWNIE STWIERDZAJĄC, że inwestowanie w innowacje oraz lepsze wykorzystywanie technologii cywilnej ma kluczowe znaczenie dla zwiększenia naszej technologicznej suwerenności, także w dziedzinie cyfrowej, APELUJE do Komisji o szybkie uruchomienie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w celu rozwijania silnego europejskiego ekosystemu badawczego, przemysłowego i technologicznego w cyberprzestrzeni, PODKREŚLA, że konieczne jest nasilenie badań i innowacji, większe inwestowanie w wymiarze cywilnym i obronnym z myślą o wzmocnieniu europejskiej bazy technologiczno-przemysłowej sektora obronnego (EDTIB) oraz tworzenie cyfrowych zdolności UE i jej państw członkowskich, w tym zdolności do wsparcia strategicznego. W związku z tym KŁADZIE NACISK na znaczenie intensywnego wykorzystywania nowych technologii, zwłaszcza informatyki kwantowej, sztucznej inteligencji i technologii dużych zbiorów danych, aby uzyskać przewagę komparatywną, w tym pod względem operacji reagowania na cyberzagrożenia.

8. UZNAJĄC, że zwiększanie naszego cyberbezpieczeństwa jest jednym ze sposobów podnoszenia skuteczności i bezpieczeństwa naszych działań na lądzie, w powietrzu, na morzu i w przestrzeni kosmicznej, PODKREŚLA wagę uwzględniania kwestii cyberbezpieczeństwa we wszystkich unijnych politykach publicznych, w tym w przepisach sektorowych stanowiących uzupełnienie dyrektywy NIS 2, oraz ZWRACA SIĘ do Komisji, by zbadała możliwości zwiększania cyberbezpieczeństwa w całym łańcuchu dostaw europejskiej bazy technologiczno-przemysłowej sektora obronnego (EDTIB).

9. STWIERDZA, że zadbanie o to, by na cyberbezpieczeństwo przeznaczano adekwatne zasoby finansowe i ludzkie, i zapewnienie środków służących tworzeniu warunków, które będą sprzyjać konkurencyjności sektora prywatnego, to elementy niezbędne do rozwijania pozycji UE w kwestiach cyberprzestrzeni, a także że zagadnienie stabilnego i długoterminowego finansowania cyberbezpieczeństwa powinno zostać uwzględnione również na szczeblu UE w drodze zaprojektowania i wdrożenia horyzontalnego mechanizmu łączącego wielorakie źródła finansowania, w tym pokrywania kosztu wysoko wykwalifikowanej kadry. W związku z tym APELUJE do Komisji, aby do końca 2022 r. przenalizowała warianty takiego mechanizmu, które następnie zostaną omówione na forum właściwych organów Rady.

10. ZWRACA UWAGĘ na potrzebę wzmożenia naszych wysiłków i zacieśnienia współpracy w walce z międzynarodową cyberprzestępczością, a w szczególności z oprogramowaniem szantażującym, za pośrednictwem EMPACT (europejskiej multidyscyplinarnej platformy przeciwko zagrożeniom przestępstwami), w drodze kontaktów między sektorem cyberbezpieczeństwa, sektorem ścigania przestępstw i sektorem dyplomacji, a także poprzez wzmocnienie zdolności organów ścigania w zakresie prowadzenia dochodzeń dotyczących cyberprzestępczości i w zakresie ścigania cyberprzestępczości. PONOWNIE ZOBOWIĄZUJE się do informowania społeczeństwa o cyberzagrożeniach i działaniach podejmowanych przeciwko nim na szczeblu krajowym i unijnym poprzez angażowanie społeczeństwa obywatelskiego, sektora prywatnego i środowiska akademickiego, w celu szerzenia wiedzy na ten temat i zachęcania do utrzymywania należytego poziomu cyberochrony i cyberhigieny. PODKREŚLA, że na szczeblu UE i państw członkowskich konieczne jest skoncentrowanie się na umiejętnościach i zdolnościach obywateli w zakresie cyberbezpieczeństwa oraz aktywne włączenie użytkowników w działania na rzecz ich własnej ochrony.

II. **WZMOCNIENIE SOLIDARNEGO I KOMPLEKSOWEGO ZARZĄDZANIA KRYZYSOWEGO**

11. Opierając się na corocznych ćwiczeniach w dziedzinie cyberbezpieczeństwa, innych ćwiczeniach dotyczących wymiaru związanego z cyberprzestrzenią oraz na ćwiczeniach EU CyCLES 2022, PODKREŚLA, jak ważne jest ustanowienie obejmującego różne społeczności i wielopoziomowego programu regularnych ćwiczeń w dziedzinie cyberbezpieczeństwa w celu testowania i rozwijania wewnętrznej i zewnętrznej reakcji UE na cyberincydenty na dużą skalę, z udziałem Rady, ESDZ, Komisji i odpowiednich zainteresowanych stron, takich jak ENISA i sektor prywatny, który to program będzie się wpisywał i wnosił wkład w ogólną politykę UE w zakresie ćwiczeń. PODKREŚLA znaczenie dalszego rozwijania ćwiczeń Cyber Europe i BlueOLEx, łączących reagowanie na różnych szczeblach. UZNAJE potrzebę oceny i konsolidacji istniejących ćwiczeń oraz rozważenia możliwość prowadzenia dalszych ćwiczeń w konkretnych segmentach cyberprzestrzeni, w szczególności wojskowych ćwiczeń CERT oraz ćwiczeń skupiających się na współpracy kryzysowej między instytucjami, organami i agencjami UE. UZNAJE, że pozycja Unii w kwestiach cyberprzestrzeni wzmocni naszą zdolność do zapobiegania cyberatakom poprzez różne działania, w tym szkolenia, i w związku z tym ZWRACA SIĘ do państw członkowskich o zacieśnienie współpracy cywilno-wojskowej w zakresie szkoleń i wspólnych ćwiczeń w dziedzinie cyberbezpieczeństwa.

12. PODKREŚLA potrzebę dalszego testowania i wzmacniania współpracy operacyjnej i wspólnej orientacji sytuacyjnej wśród państw członkowskich, w tym za pośrednictwem istniejących sieci, takich jak sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) i sieć organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU CyCLONe), aby zwiększyć gotowość UE do radzenia sobie z cyberincydentami na dużą skalę. PODKREŚLA znaczenie prac nad opracowaniem wspólnego języka wśród państw członkowskich i z instytucjami, organami i agencjami UE, dostosowanego do dyskusji na szczeblu politycznym, w celu wsparcia ustanowienia skonsolidowanej oceny dotkliwości i skutków odnośnych cyberincydentów, a także ewentualnych scenariuszy rozwoju i, w stosownych przypadkach, wynikających z nich potrzeb. PODKREŚLA w tej kwestii potrzebę zwiększenia komplementarności wspólnych sprawozdań z oceny sytuacyjnej, w tym sprawozdań EU CyCLONE na temat skutków i dotkliwości cyberincydentów na dużą skalę we wszystkich państwach członkowskich UE oraz ocen zagrożeń przedstawianych przez Centrum Analiz Wywiadowczych UE (INTCEN) w ramach unijnego zestawu narzędzi dla dyplomacji cyfrowej. ZWRACA SIĘ do Komisji, Wysokiego Przedstawiciela i grupy współpracy NIS, by do końca 2022 r. we współpracy z odpowiednimi cywilnymi i wojskowymi organami i agencjami oraz istniejącymi sieciami, w tym EU CyCLONe, przeprowadzili ocenę ryzyka i opracowali scenariusze ryzyka z perspektywy cyberbezpieczeństwa w sytuacji zagrożenia lub ewentualnego ataku na państwa członkowskie lub kraje partnerskie oraz by przedstawili je odpowiednim organom Rady. PODKREŚLA potrzebę odpowiedniej i skoordynowanej komunikacji publicznej na temat reakcji UE na cyberincydenty na dużą skalę.

13. W przypadku cyberincydentu na dużą skalę PODKREŚLA potrzebę wzmocnienia koordynacji oraz, w stosownych przypadkach – z wykorzystaniem osiągniętych postępów i prac zespołów szybkiego reagowania na cyberincydenty ustanowionych w ramach PESCO oraz, w oparciu o prace sieci CSIRT i EU CyCLONe – dobrowolnego łączenia przez państwa członkowskie zdolności reagowania na incydenty. UZNAJE, że rozwijanie powiązań z sektorem prywatnym mogłoby przyczynić się do wzmocnienia zdolności publicznych, w szczególności w kontekście niedoboru wykwalifikowanej siły roboczej w UE, oraz że wskazanie takich partnerów prywatnych i koordynowanie ich działań mogą odegrać istotną rolę w przypadku incydentów na dużą skalę. Aby zapewnić pełną gotowość na wypadek cyberincydentów na dużą skalę, ZWRACA SIĘ do Komisji, by do końca trzeciego kwartału 2022 r. przedstawiła wniosek w sprawie nowego funduszu reagowania kryzysowego w zakresie cyberbezpieczeństwa.

14. Zgodnie ze Strategicznym kompasem PRZYPOMINA o potrzebie inwestowania we wzajemną pomoc na mocy art. 42 ust. 7 Traktatu o Unii Europejskiej i solidarność na mocy art. 222 Traktatu o funkcjonowaniu Unii Europejskiej, w szczególności poprzez częste ćwiczenia. W tym kontekście PODKREŚLA potrzebę dalszych prac nad zapewnieniem i koordynacją dwustronnego wsparcia cywilnego i wojskowego, w tym poprzez zbadanie możliwości wsparcia udzielanego przez UE na wyraźny wniosek państw członkowskich, oraz nad określeniem odpowiednich środków reagowania, w tym poprzez rozwijanie strategii skoordynowanej komunikacji w kontekście wdrażania art. 42 ust. 7. ODNOTOWUJE, że powinno to również obejmować analizę powiązań z istniejącymi unijnymi mechanizmami zarządzania kryzysowego i Unijnym Mechanizmem Ochrony Ludności.

15. PODKREŚLA, że wzmocniona pozycja UE w kwestiach cyberprzestrzeni będzie wymagała lepszej bezpieczniej łączności. W tym celu PRZYPOMINA wskazówki nakreślone w Strategicznym kompasie w tym zakresie i ZWRACA SIĘ do Komisji i innych odpowiednich instytucji, organów i agencji, by do końca 2022 r. sporządziły zestawienie istniejących narzędzi bezpiecznej łączności w cyberprzestrzeni, które powinno zostać omówione przez odpowiednie organy Rady i odpowiednie grupy współpracy, takie jak sieć CSIRT i EU CyCLONe.

## III. PROMOWANIE NASZEJ WIZJI CYBERPRZESTRZENI

16. PRZYPOMINA, że wspólne i kompleksowe podejście UE do dyplomacji cyfrowej ma za zadanie przyczynić się do przeciwdziałania konfliktom, łagodzenia zagrożeń dla cyberbezpieczeństwa oraz do większej stabilności w stosunkach międzynarodowych. W tym kontekście PONOWNIE POTWIERDZA, że UE angażuje się na rzecz pokojowego rozstrzygania sporów międzynarodowych w cyberprzestrzeni oraz że prawo międzynarodowe, w tym międzynarodowe prawo dotyczące praw człowieka i międzynarodowe prawo humanitarne, ma zastosowanie do działań państw w cyberprzestrzeni. PODKREŚLA zobowiązanie UE i jej państw członkowskich do działania zgodnie z dobrowolnymi, niewiążącymi normami odpowiedzialnego zachowania państw w cyberprzestrzeni uzgodnionymi przez wszystkie państwa członkowskie ONZ. PODKREŚLA znaczenie otwartej, wolnej, globalnej, stabilnej i bezpiecznej cyberprzestrzeni, w której prawa człowieka, podstawowe wolności i praworządność mają pełne zastosowanie i przyczyniają się do wspierania dobrostanu społecznego, wzrostu gospodarczego, dobrobytu i integralności naszych wolnych i demokratycznych społeczeństw, oraz POTWIERDZA zobowiązanie UE i jej państw członkowskich do dalszego propagowania tych wartości i zasad. Z myślą o rozwijaniu kanałów konstruktywnego, szczerego i otwartego dialogu z kluczowymi zainteresowanymi stronami z sektora cyberprzestrzeni PODKREŚLA, jak ważne jest, by kwestie dotyczące cyberprzestrzeni, w tym unijny zestaw narzędzi dla dyplomacji cyfrowej, stały się integralną częścią unijnych negocjacji akcesyjnych oraz strategicznego i politycznego dialogu UE zarówno z partnerami międzynarodowymi, jak i z konkurentami, i jednocześnie WZYWA Wysokiego Przedstawiciela do dokonania przeglądu istniejących dwustronnych dialogów poświęconych cyberprzestrzeni i, w razie potrzeby, do zaproponowania rozpoczęcia podobnej współpracy z kolejnymi państwami lub odpowiednimi organizacjami międzynarodowymi.

17. PRZYPOMINA o znaczeniu współpracy obejmującej wiele zainteresowanych stron, ponieważ inne zainteresowane strony również ponoszą odpowiedzialność za cyberbezpieczeństwo, zwłaszcza jeśli chodzi o wdrażanie zaleceń i decyzji podjętych na forach międzynarodowych i regionalnych. ZWRACA się do UE i jej państw członkowskich, aby w dalszym ciągu promowały europejski model cyberprzestrzeni i internetu oparty na podejściu obejmującym wiele zainteresowanych stron, również poprzez inicjatywy takie jak paryskie wezwanie do zaufania i bezpieczeństwa w cyberprzestrzeni i deklaracja dotycząca przyszłości internetu, podkreślając wspólne korzyści ze stabilności w cyberprzestrzeni oraz podnosząc w skali globalnej świadomość zagrożeń wiążących się z państwocentryczną i autorytarną wizją internetu, a także WZYWA UE i jej państwa członkowskie do dalszego zacieśnienia współpracy z obejmującą wiele zainteresowanych stron społecznością, w tym poprzez wykorzystywanie stosownych projektów, takich jak unijna inicjatywa w zakresie dyplomacji cyfrowej będąca elementem instrumentu unijnej polityki zagranicznej.

18. ZOBOWIĄZUJE się stale angażować się w działania odpowiednich organizacji międzynarodowych, w szczególności w procesy związane z Pierwszym i Trzecim Komitetem ONZ, podkreślając jednocześnie, że obowiązujące prawo międzynarodowe ma, bez zastrzeżeń, zastosowanie w cyberprzestrzeni i w odniesieniu do niej. ZWRACA UWAGĘ na znaczenie nieustających wysiłków mających na celu utrzymanie i promowanie ram ONZ dotyczących odpowiedzialnego zachowania państw w cyberprzestrzeni oraz PODKREŚLA, że UE i jej państwa członkowskie będą aktywnie działać na rzecz wzmocnienia ich wdrażania, w tym poprzez ustanowienie programu działania na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni. PODKREŚLA, że UE i jej państwa członkowskie będą aktywnie angażować się w negocjacje w sprawie przyszłej konwencji ONZ, która ma służyć jako skuteczny instrument dla organów ścigania i organów sądowych w globalnej walce z cyberprzestępczością, przy pełnym uwzględnieniu istniejących ram międzynarodowych i regionalnych instrumentów w tej dziedzinie, w szczególności budapeszteńskiej Konwencji o cyberprzestępczości. ZWRACA UWAGĘ na znaczenie dalszego wspierania rozwoju i operacjonalizacji środków budowy zaufania na szczeblu regionalnym i międzynarodowym oraz dalszego zachęcania do korzystania z istniejących w ramach OBWE środków budowy zaufania w zakresie cyberprzestrzeni, w tym w czasach napięć międzynarodowych.

19. PRZYPOMINA, że przyjęcie proaktywnego podejścia opartego na prawach człowieka w celu zapewnienia międzynarodowych standardów w dziedzinie powstających technologii i podstawowej architektury internetowej, zgodnych z wartościami i zasadami demokratycznymi ma zasadnicze znaczenie dla zapewnienia, by internet pozostał globalny, niepodzielny i otwarty, oraz POPIERA zasadę, zgodnie z którą stosowanie i rozwój technologii są ukierunkowane na poszanowania praw człowieka i na ochronę prywatności oraz że korzystanie z nich ma się odbywać w sposób zgodny z prawem, bezpieczny i etyczny. ZACHĘCA Wysokiego Przedstawiciela i Komisję do opracowania strategicznej wizji kwestii technicznych w dziedzinie cyfrowej mających skutki dla polityki zagranicznej i mogących oddziaływać na stabilność cyberprzestrzeni, a w szczególności internetu, w tym na forum odpowiednich wyspecjalizowanych organizacji międzynarodowych (Międzynarodowy Związek Telekomunikacyjny itp.).

## IV. ZACIEŚNIENIE WSPÓŁPRACY Z KRAJAMI PARTNERSKIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

20. PODKREŚLA potrzebę lepszego powiązania unijnej strategii budowania zdolności cyfrowych z normami ONZ dotyczącymi odpowiedzialnego zachowania państw w cyberprzestrzeni, w tym poprzez opracowanie odpowiednio dostosowanych programów współpracy i budowania zdolności w celu wspierania państw trzecich w ich wysiłkach wdrożeniowych oraz kontynuowanie i rozszerzanie tym samym naszych wysiłków dotyczących promowania programu działania ONZ na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni. PODKREŚLA znaczenie pełnego włączenia budowania zdolności cyfrowych do oferty UE jako gwaranta bezpieczeństwa, przy odpowiedniej koordynacji wysiłków między państwami członkowskimi a instytucjami, organami i agencjami UE, a w szczególności Z ZADOWOLENIEM PRZYJMUJE współpracę między państwami członkowskimi, a także z partnerami z sektora publicznego i prywatnego, zwłaszcza za pośrednictwem unijnej sieci na rzecz budowania zdolności cyfrowych (EU CyberNet) i Globalnego Forum Wiedzy Cyfrowej (GFCE), aby zapewnić koordynację i uniknąć powielania działań.

WZYWA Wysokiego Przedstawiciela i Komisję do ustanowienia do trzeciego kwartału 2022 r. *Rady ds. Budowania Zdolności Cyfrowych* oraz do prowadzenia regularnej wymiany poglądów na forum Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni. ZWRACA SIĘ do

Komisji i Wysokiego Przedstawiciela o dalsze mobilizowanie Instrumentu Sąsiedztwa oraz Współpracy Międzynarodowej i Rozwojowej (ISWMR), Instrumentu Pomocy Przedakcesyjnej (IPA III) i innych narzędzi finansowych, takich jak Europejski Instrument na rzecz Pokoju (EPF) i inicjatywa „Global Gateway", aby wspierać wzmacnianie odporności naszych partnerów, ich zdolności do identyfikowania cyberzagrożeń i reagowania na nie oraz prowadzenia dochodzeń w sprawie cyberprzestępczości i ścigania jej, a także do opracowywania projektów współpracy, w tym w kontekście kryzysu, w szczególności ZACHĘCA do współpracy z partnerami na Bałkanach Zachodnich oraz we wschodnim i południowym sąsiedztwie UE, a także do rozmieszczenia ekspertów z UE i państw członkowskich w celu zaoferowania wsparcia w przypadku cyberkryzysów, z uwzględnieniem istniejących mandatów prawnych.

21. PODKREŚLA potrzebę wzmożenia wysiłków na rzecz opracowania ustrukturyzowanego i otwartego podejścia UE do działań informacyjnych na temat sposobów promowania globalnego wspólnego rozumienia stosowania prawa międzynarodowego w cyberprzestrzeni, ram ONZ dotyczących odpowiedzialnego zachowania państw w cyberprzestrzeni, w tym inicjatywy odnoszącej się do programu działania na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni, a także stanowiska UE i jej państw członkowskich w toczących się negocjacjach w sprawie konwencji ONZ o cyberprzestępczości; w ramach tych dążeń WZYWA też Wysokiego Przedstawiciela do przedstawienia Radzie do końca 2022 r. planu działań informacyjnych. ZACHĘCA Wysokiego Przedstawiciela i służby Komisji, by w pełni i systematycznie wykorzystywały 145 unijnych delegatur i rozwijały regularną, owocną współpracę między nimi a ambasadami państw członkowskich w państwach trzecich, pod auspicjami planowanej unijnej sieci dyplomacji cyfrowej. WZYWA Wysokiego Przedstawiciela do ustanowienia do trzeciego kwartału 2022 r. unijnej sieci dyplomacji cyfrowej, która przyczyni się do wymiany informacji, organizacji wspólnych szkoleń dla personelu z UE i państw członkowskich, uspójnienia wysiłków na rzecz budowania zdolności oraz skuteczniejszego wdrażania ram ONZ dotyczących odpowiedzialnego zachowania państw, a także środków budowy zaufania między państwami.

22. PODKREŚLA swoje zobowiązanie do dalszej współpracy z organizacjami międzynarodowymi i krajami partnerskimi w celu pogłębienia wspólnego zrozumienia krajobrazu cyberzagrożeń, opracowania mechanizmów współpracy i proaktywnego określenia wspólnych reakcji dyplomatycznych. PRZYPOMINAJĄC kluczowe osiągnięcia współpracy UE–NATO w obszarze cyberbezpieczeństwa w ramach wdrażania wspólnych deklaracji z Warszawy (2016 r.) i Brukseli (2018 r.), przy pełnym poszanowaniu autonomii procesu decyzyjnego i procedur obu organizacji oraz w oparciu o zasady przejrzystości, wzajemności i inkluzywności, PODKREŚLA potrzebę dalszego zacieśniania współpracy w dziedzinie cyberbezpieczeństwa z NATO poprzez ćwiczenia, wymianę informacji i wymiany między ekspertami, w tym w zakresie rozwijania zdolności, budowania zdolności partnerów oraz misji i operacji, a także w dziedzinie stosowania prawa międzynarodowego i norm ONZ dotyczących odpowiedzialnego zachowania państwa w cyberprzestrzeni i możliwych skoordynowanych reakcji na szkodliwe działania w cyberprzestrzeni.

## V. ZAPOBIEGANIE CYBERATAKOM, OBRONA PRZED NIMI I REAGOWANIE NA NIE

23. UZNAJE, że cyberprzestrzeń stała się areną rywalizacji geopolitycznej, i w związku z tym PRZYPOMINA, że UE musi być w stanie szybko i stanowczo reagować na cyberataki, takie jak finansowane przez państwo szkodliwe działania w cyberprzestrzeni wymierzone w UE i jej państwa członkowskie, i w związku z tym musi wzmocnić unijny zestaw narzędzi dla dyplomacji cyfrowej i w pełni wykorzystać wszystkie swoje instrumenty, w tym dostępne narzędzia polityczne, ekonomiczne, dyplomatyczne, prawne i w zakresie strategicznej komunikacji, aby zapobiegać szkodliwym działaniom w cyberprzestrzeni, zniechęcać do nich, powstrzymywać je i reagować na nie. PODKREŚLA, że wrogie podmioty muszą być świadome, że cyberataki na państwa członkowskie i instytucje UE będą wykrywane na wczesnym etapie, szybko identyfikowane i kontrowane za pomocą wszelkich niezbędnych narzędzi i strategii politycznych. Opierając się w szczególności na zawartych w nich elementach dotyczących pozycji w kwestiach cyberprzestrzeni, a także na wnioskach wyciągniętych z wdrażania zestawu narzędzi dla dyplomacji cyfrowej oraz z ćwiczeń EUCyCLES, ZWRACA SIĘ do państw członkowskich i Wysokiego Przedstawiciela, by przy wsparciu Komisji opracowali zmienioną wersję wytycznych wykonawczych do unijnego zestawu narzędzi dla dyplomacji cyfrowej do końca 2023 r., rozważając przy tym dodatkowe środki reagowania.

24. PODKREŚLA potrzebę prowadzenia regularnej wymiany informacji na temat krajobrazu cyberzagrożeń na forach odpowiednich organów i komitetów Rady przy jednoczesnym utrzymywaniu kontaktów z sektorem prywatnym, a także – opierając się na ocenie skutków i dotkliwości niedawnych incydentów – potrzebę zwiększenia ogólnej świadomości i gotowości, mając na względzie przyszłe zastosowania unijnego zestawu narzędzi dla dyplomacji cyfrowej oraz potrzebę opracowania dalszych narzędzi wspierających jego wdrażanie. Chociaż bezpieczeństwo narodowe pozostaje w wyłącznej gestii każdego państwa członkowskiego, ODNOTOWUJE potrzebę wzmocnienia wymiany danych wywiadowczych i informacji oraz współpracy między państwami członkowskimi, a także z INTCEN, aby stosowne organy mogły wymieniać między sobą dane wywiadowcze na początku procesu decyzyjnego, w tym w kwestii przydziału zadań, i by tym samym umożliwić szybką skuteczną i uzasadnioną reakcję na szkodliwe działania w cyberprzestrzeni wymierzone w UE i jej partnerów. PRZYPOMINA, jak ważne jest wzmocnienie zdolności INTCEN w dziedzinie cyberprzestrzeni w oparciu o informacje wywiadowcze dobrowolnie udostępniane przez państwa członkowskie i bez uszczerbku dla ich kompetencji, oraz przeanalizowanie wniosku dotyczącego ewentualnego utworzenia grupy roboczej państw członkowskich ds. wywiadu cyfrowego.

25. UZNAJĄC, że deklaracje UE i środki ograniczające podjęte w ramach unijnego zestawu narzędzi dla dyplomacji cyfrowej wysłały wyraźny sygnał, że szkodliwe działania w cyberprzestrzeni stanowiące zewnętrzne zagrożenie dla UE, jej państw członkowskich i partnerów są niedopuszczalne, i że tym samym te deklaracje i środki ograniczające przyczyniają się do zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania ich i reagowania na nie, POTWIERDZA swoje zobowiązanie do stosowania tych środków w celu przypominania o obowiązkach, które mają zastosowanie do cyberprzestrzeni na mocy prawa międzynarodowego, w tym całej Karty Narodów Zjednoczonych, w tym o spoczywającym na wszystkich państwach obowiązku zachowania należytej staranności, zgodnie z którym nie powinny one świadomie zezwalać na wykorzystywanie ich terytorium do szkodliwych i nielegalnych w świetle prawa międzynarodowego działań z wykorzystywaniem ICT, z myślą o dalszym rozwijaniu i promowaniu wspólnego stanowiska UE w sprawie stosowania prawa międzynarodowego w cyberprzestrzeni. Odnotowując, że odpowiednie i szybkie komunikaty łagodzą ryzyko eskalacji i mogą zniechęcać podmioty atakujące interesy europejskie, ZWRACA SIĘ do Wysokiego Przedstawiciela o opracowanie i przedłożenie państwom członkowskim spójnej strategii komunikacyjnej dotyczącej wykorzystywania unijnego zestawu narzędzi dla dyplomacji cyfrowej.

26. ZACHĘCA do opracowywania stopniowych, ukierunkowanych i trwałych podejść i reakcji na szkodliwe działania w cyberprzestrzeni, z wykorzystaniem szerokiego wachlarza narzędzi zapewnianych przez unijny zestaw narzędzi dla dyplomacji cyfrowej, w tym unijnego systemu sankcji za cyberataki, oraz do rozważenia dodatkowych środków. PODKREŚLA potrzebę zwiększenia możliwości mobilizowania, w poszczególnych przypadkach, wszystkich dostępnych narzędzi, wewnętrznych i zewnętrznych, aby zapobiegać cyberatakom, zniechęcać do nich, powstrzymywać je i reagować na nie, poprzez wdrażanie tych narzędzie zgodnie z szybkim, skutecznym, stopniowym, ukierunkowanym i trwałym podejściem opartym na długoterminowym strategicznym zaangażowaniu. WZYWA Wysokiego Przedstawiciela, by we współpracy z Komisją określił możliwe wspólne reakcje UE na cyberataki, w tym opcje dotyczące sankcji, z myślą o całym ich wachlarzu, tak aby przygotować się do podjęcia w razie potrzeby szybkich i skutecznych działań, i by przedstawił je Radzie do końca pierwszego kwartału 2023 r.

27. Odnotowując, że cyberobrona należy w głównej mierze do obowiązków krajowych, ZACHĘCA państwa członkowskie do dalszego rozwijania własnych zdolności do prowadzenia operacji w zakresie cyberobrony, w tym proaktywnych środków służących ochronie przed cyberatakami, wykrywaniu ich, bronieniu się przed nimi i zniechęcaniu do nich, a także ewentualnie środków wspierających inne państwa członkowskie i UE. Wszystkie państwa członkowskie zachęca się do zwiększenia, w razie potrzeby, własnych zdolności do udzielania i otrzymywania pomocy i wsparcia. PODKREŚLA, że dalszy rozwój tych zdolności powinien być jednym z kluczowych celów przyszłej polityki UE w zakresie cyberobrony. ZAUWAŻA, że polityka UE w zakresie cyberobrony powinna w większym stopniu uwzględniać rolę, jaką odpowiednie instytucje i organy UE mogą odegrać w zacieśnianiu współpracy między odpowiednimi unijnymi i krajowymi podmiotami ds. cyberobrony i rozwijaniu ich własnych zdolności, zgodne z ich odpowiednimi mandatami. ZWRACA SIĘ do Wysokiego Przedstawiciela, by wraz z Komisją uzupełnił rozwijanie pozycji UE w kwestiach cyberprzestrzeni poprzez przedstawienie w 2022 r. ambitnego wniosku dotyczącego polityki UE w zakresie cyberobrony, który utoruje drogę dalszemu rozwojowi tej pozycji przez Radę.

28. PODKREŚLA potrzebę zwiększenia interoperacyjności i wymiany informacji poprzez współpracę między wojskowymi zespołami reagowania na incydenty komputerowe (milCERT). ZWRACA SIĘ do państw członkowskich, by w oparciu o prace Europejskiej Agencji Obrony utworzyły sieć milCERT w celu rozwijania współpracy i ułatwiania wymiany informacji, co pomogłoby również w stymulowaniu koordynacji z innymi społecznościami zajmującymi się cyberprzestrzenią, a także sieć wojskowych dowódców ds. cyberprzestrzeni w celu wzmocnienia strategicznej współpracy między dowództwami ds. cyberprzestrzeni poszczególnych państw członkowskich UE lub innymi odpowiednimi organami. Utworzenie tych sieci, a także realizowanie projektów PESCO dotyczących cyberprzestrzeni, przyczyniłoby się do wzmocnienia cyberobrony na szczeblu UE. Podkreśla znaczenie współpracy między proponowaną siecią milCERT a już istniejącą siecią cywilną (CSIRT) w celu usprawnienia wymiany informacji i poprawy orientacji sytuacyjnej.

29. Na podstawie wojskowej wizji i strategii dotyczącej cyberprzestrzeni jako obszaru operacyjnego oraz biorąc pod uwagę trwający rozwój wojskowej koncepcji cyberobrony na potrzeby operacji i misji wojskowych dowodzonych przez UE, PONOWNIE PODKREŚLA potrzebę włączenia wymiaru cyberprzestrzeni do planowania i prowadzenia misji i operacji w dziedzinie WPBiO, w tym poprzez wzmocnienie ich zdolności cyfrowych, oraz ZAZNACZA, że przyczyni się to do lepszej orientacji sytuacyjnej w cyberprzestrzeni na szczeblu UE.

30. Podsumowując, ODNOTOWUJE, że pozycja w kwestiach cyberprzestrzeni będzie krokiem w kierunku ustanowienia unijnej doktryny działań w cyberprzestrzeni, opartej na zwiększonej odporności oraz zwiększonych zdolnościach i możliwościach reagowania, a także na wspólnym stanowisku w sprawie stosowania prawa międzynarodowego w cyberprzestrzeni. Aby zapewnić dalszy rozwój pozycji UE w kwestiach cyberprzestrzeni, w 2023 r. Rada PODSUMUJE postępy w realizacji niniejszych konkluzji.