Rada
Unii Europejskiej

Bruksela, 22 maja 2023 r.
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Dotyczy:	Konkluzje Rady w sprawie polityki UE w zakresie cyberobrony

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie polityki UE w zakresie cyberobrony, zatwierdzone przez Radę na posiedzeniu w dniu 22 maja 2023 r.

Konkluzje Rady w sprawie polityki UE w zakresie cyberobrony

1. Opierając się na ramach polityki w zakresie cyberobrony z 2014 r. i ich aktualizacji z 2018 r., Rada z zadowoleniem przyjmuje ambitny wspólny komunikat w sprawie polityki UE w zakresie cyberobrony, który przewiduje nie tylko dalsze inwestycje w nasze nowoczesne i interoperacyjne siły zbrojne, zaawansowane technologie i najnowocześniejsze zdolności w zakresie cyberobrony, ale także zacieśnianie partnerstw w celu sprostania wspólnym wyzwaniom. W czasach rosnącej zależności od technologii cyfrowych cyberprzestrzeń stała się polem strategicznej rywalizacji. Kwestią kluczową jest zatem utrzymanie otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni. Cyberoperacje, które umożliwiły niesprowokowaną i nieuzasadnioną wojnę napastniczą Rosji przeciwko Ukrainie i które jej towarzyszą, wpływają na stabilność i bezpieczeństwo na świecie, stanowią poważne ryzyko eskalacji i przyczyniają się do znacznego już wzrostu szkodliwych działań w cyberprzestrzeni, który w ostatnich latach wykraczał poza kontekst konfliktów zbrojnych.

2. Wojna w Ukrainie stworzyła nowy kontekst strategiczny i potwierdziła, że UE, jej państwa członkowskie i ich partnerzy muszą jeszcze bardziej wzmocnić odporność UE na zagrożenia cyberbezpieczeństwa i zwiększyć nasze wspólne cyberbezpieczeństwo i cyberobronę przed szkodliwymi zachowaniami i aktami agresji w cyberprzestrzeni. Wspólny komunikat w sprawie polityki UE w zakresie cyberobrony ukazuje naszą determinację w dążeniu do zapewnienia natychmiastowych i długoterminowych środków umożliwiających swobodę działań w cyberprzestrzeni oraz reagowanie na działania agresorów, którzy starają się m.in. ingerować w sieci i systemy informatyczne UE i jej partnerów, a także zakłócać je lub niszczyć. Wspólny komunikat, uzupełniający unijną strategię cyberbezpieczeństwa i zgodny ze Strategicznym kompasem, stanowi istotny krok na drodze ku temu, by UE stosowała podejście pełnego spektrum do odporności, reagowania, zapobiegania konfliktom, współpracy i stabilności w cyberprzestrzeni. W tym kontekście Rada podkreśla potrzebę odpowiednich i spójnych reakcji ze strony UE, jej państw członkowskich i ich partnerów, oczekując też na przegląd wytycznych wykonawczych dotyczących unijnego zestawu narzędzi dla dyplomacji cyfrowej, który byłby kolejnym kluczowym krokiem w kierunku rozwoju pozycji UE w cyberprzestrzeni.

3. Rada podkreśla, że niedawne cyberataki na europejską infrastrukturę krytyczną, gwałtownie zmieniający się krajobraz cyberzagrożeń i szybkie tempo rozwoju technologicznego również wskazują na potrzebę ściślejszej koordynacji i współpracy cywilno-wojskowej – zwraca jednocześnie uwagę na brak hierarchii między społecznościami cywilnymi i wojskowymi. Polityka UE w zakresie cyberobrony umożliwia UE i jej państwom członkowskim wzmocnienie ich zdolności do ochrony, wykrywania, obrony i powstrzymywania, przy odpowiednim wykorzystaniu całej gamy opcji obronnych dostępnych dla społeczności cywilnych i wojskowych na rzecz szerszego bezpieczeństwa i obrony UE, zgodnie z prawem międzynarodowym, w tym prawem praw człowieka i międzynarodowym prawem humanitarnym.

4. Chociaż bezpieczeństwo narodowe, w tym dziedzina cyberbezpieczeństwa, pozostaje – jak zauważono w art. 4 ust. 2 TUE – w wyłącznej gestii każdego państwa członkowskiego, Rada podkreśla jednak potrzebę znacznych inwestycji indywidualnych i wspólnych w zwiększenie odporności i wdrażanie zdolności obronnych w zakresie cyberobrony o pełnym spektrum oraz potrzebę wykorzystania unijnych ram współpracy i zachęt finansowych. Rada zwraca uwagę na potrzebę dalszego wzmacniania działań państw członkowskich oraz instytucji, organów i agencji UE (EUIBA) w celu ochrony Unii, naszych obywateli, EUIBA oraz misji i operacji w dziedzinie WPBiO w cyberprzestrzeni. Ponadto podkreśla, jak ważna jest odporność UE w cyberprzestrzeni, którą to odporność można rozwijać poprzez budowanie zdolności w zakresie cyberobrony i zacieśnianie współpracy z zaufanym ekosystemem prywatnym.

I. **Wspólne działanie na rzecz silniejszej cyberobrony**

5. Rada powtarza, 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, co należy wykonać zgodnie z opracowanym przez Radę planem działania w zakresie zarządzania kryzysami cyberbezpieczeństwa. Rada ponownie stwierdza, że należy umacniać nasze zdolności do ochrony i obrony przed cyberatakami, do ich wykrywania oraz powstrzymywania dzięki lepszej orientacji sytuacyjnej, budowaniu potencjału i rozwojowi zdolności, szkoleniom, ćwiczeniom i dzięki zwiększonej odporności, a także dzięki zdecydowanej i wykorzystującej wszystkie właściwe narzędzia reakcji na cyberataki wymierzone w UE, jej państwa członkowskie, EUIBA i misje w dziedzinie WPBiO. Tym samym Rada zachęca Wysokiego Przedstawiciela i Komisję do ograniczania złożoności w dziedzinie cyberbezpieczeństwa, unikania niepotrzebnego powielania działań oraz do zapewnienia współpracy i synergii z istniejącymi inicjatywami. Należy wzmocnić współpracę i koordynację między podmiotami zajmującymi się cyberobroną w UE i państwach członkowskich, a także między wojskowymi i cywilnymi społecznościami cybernetycznymi oraz między sektorem publicznym i zaufanym ekosystemem prywatnym. W tym kontekście zachęca się państwa członkowskie do dalszego badania i wzmacniania cywilno-wojskowych krajowych mechanizmów koordynacji, ułatwiania wspólnej dobrowolnej wymiany informacji, dzielenia się wyciągniętymi wnioskami, pomocy w opracowywaniu standardów interoperacyjnych oraz do przeprowadzania ocen ryzyka i opracowywania scenariuszy ryzyka, a także do wspólnych ćwiczeń, zwłaszcza na szczeblu europejskim, z pełnym poszanowaniem przepisów dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS 2).

6. Uznając wysiłki na rzecz dalszego zwiększenia odporności Unii za pomocą NIS 2 i dyrektywy w sprawie odporności podmiotów krytycznych (CER), Rada ponawia swoje zalecenie w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej[1]. Wezwano w nim do wprowadzenia środków służących dalszemu zwiększeniu odporności podmiotów krytycznych, infrastruktury, produktów i usług cyfrowych, a jednocześnie zwrócono uwagę, że właściwe wdrożenie NIS 2 pozostaje najważniejszym krokiem. Choć w przeważającej mierze wdrożenie to leży w gestii cywilnej, przyczynia się również do wzmocnienia cyberobrony. W tym kontekście zachęca się EUIBA oraz państwa członkowskie do wspierania dalszego rozwoju i wdrażania nowych i istniejących unijnych mechanizmów koordynacji, ocen, ewaluacji i scenariuszy ryzyka, wspólnej dobrowolnej wymiany informacji i ćwiczeń, w sposób, który wnosi wartość dodaną i pozwala uniknąć niepotrzebnego powielania prowadzonych inicjatyw.

7. Aby jeszcze bardziej wzmocnić zaufanie, skonsolidować współpracę i ułatwić terminową wymianę informacji na temat znaczących cyberincydentów na dużą skalę mających wpływ na systemy obronne, Rada z zadowoleniem przyjmuje inicjatywę dalszego rozwijania unijnej konferencji dowódców ds. obrony cyberprzestrzeni, która ma być organizowana przez każdą prezydencję Rady UE, przy wsparciu Europejskiej Agencji Obrony (EDA) i przy udziale Europejskiej Służby Działań Zewnętrznych (ESDZ). Rada zachęca wszystkie państwa członkowskie do wzięcia udziału w tych posiedzeniach. Aby wzmocnić odporność UE na cyberincydenty na dużą skalę, Rada zwraca się do europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) i do unijnej konferencji dowódców ds. obrony cyberprzestrzeni o zidentyfikowanie możliwych sposobów współpracy i czerpania korzyści ze wspólnej perspektywy wojskowej i cywilnej.

---

[1] Wniosek dotyczący zalecenia Rady w sprawie skoordynowanego podejścia Unii do kwestii wzmocnienia odporności infrastruktury krytycznej, COM/2022/551.

8. Aby promować bardziej solidną i skoordynowaną reakcję na szczeblu UE, Rada z zadowoleniem przyjmuje utworzenie do połowy 2024 r. unijnej operacyjnej sieci dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET) i oczekuje na osiągnięcie przez nią w tym samym terminie wstępnej zdolności operacyjnej, tak aby usprawnić wymianę informacji technicznych na temat cyberincydentów mających wpływ na systemy obronne między uczestniczącymi państwami członkowskimi. Rada zachęca wszystkie państwa członkowskie do udziału w MICNET, aby zapewnić skuteczność sieci. Ponadto Rada zachęca państwa członkowskie do korzystania z doświadczeń zdobytych w ramach sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) i zdecydowanie apeluje o utworzenie skutecznego mechanizmu współpracy i koordynacji między obiema sieciami w odpowiednim czasie, przy pełnym poszanowaniu mechanizmów zarządzania każdego podmiotu i ich składu.

9. W świetle wzrostu szkodliwych działań w cyberprzestrzeni prowadzonych przez podmioty państwowe i niepaństwowe wobec unijnych misji i operacji w dziedzinie WPBiO, Rada zwraca się do UE i jej państw członkowskich o wzmocnienie swoich zdolności w zakresie obrony i zabezpieczania misji i operacji w dziedzinie WPBiO. W związku z tym Rada z zadowoleniem przyjmuje cele dalszego zwiększania ochrony unijnych sieci i struktur wojskowych, m.in. zgodnie z unijną wojskową wizją i strategią dotyczącą cyberprzestrzeni jako obszaru operacyjnego[2].

[2] EEAS(2021) 706 REV 4

10. Rada przywołuje konkluzje Rady z maja 2022 r.[3] oraz potrzebę inwestowania we wzajemną pomoc na podstawie art. 42 ust. 7 TUE, a także klauzulę solidarności na mocy art. 222 TFUE. Rada podkreśla znaczenie dalszego pogłębiania wspólnego rozumienia przez UE i jej państwa członkowskie art. 42 ust. 7, w tym w złożonych sytuacjach obejmujących cyberataki, spójnie z właściwymi przepisami prawa międzynarodowego. Z zadowoleniem przyjmuje możliwość udzielenia wsparcia ze strony UE, na wyraźny wniosek zainteresowanych państw członkowskich, w przypadku wystąpienia cyberataku, bez uszczerbku dla szczególnego charakteru polityki bezpieczeństwa i obrony niektórych państw członkowskich.

11. Rada podkreśla postępy projektu stałej współpracy strukturalnej (PESCO) „Zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa (CRRT)" oraz osiągniętą w jego ramach gotowość do działania na żądanie jako zdolność do zaspokajania potrzeb państw członkowskich i UE z myślą o wsparciu misji i operacji w dziedzinie WPBiO oraz udzielaniu pomocy partnerom UE. Rada z zadowoleniem przyjmuje dalszy rozwój zdolności PESCO CRRT, krajowych zespołów reagowania na cyberincydenty oraz, w stosownych przypadkach, dodatkowe zdolności reagowania na incydenty np. przyszłe zespoły szybkiego reagowania na zagrożenia hybrydowe, jak przewidziano w Strategicznym kompasie, w tym poprzez wspieranie ich koordynacji i współpracy na szczeblu UE.

[3] Konkluzje Rady w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni, 23 maja 2022 r., 9364/22.

12. Rada z zadowoleniem przyjmuje działania w ramach projektu PESCO „Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (CIDCC)", którego celem jest zapewnienie zdolności wojskowych do gromadzenia i analizowania informacji istotnych dla wspólnego operacyjnego obrazu cyberbezpieczeństwa. Ponadto Rada wyraża zadowolenie w związku z propozycją, by od 2025 r. włączyć weryfikację poprawności tego projektu – przy założeniu dobrego funkcjonowania centrum koordynacji – do Centrum Koordynacji UE ds. Cyberobrony (EUCDCC), co zwiększy koordynację i orientację sytuacyjną, w szczególności w odniesieniu do dowódców misji i operacji UE w dziedzinie WPBiO, a także wzmocni szerzej pojętą unijną strukturę dowodzenia i kontroli. Rada wzywa Wysokiego Przedstawiciela, by przedstawił koncepcję i plan działania na rzecz ustanowienia EUCDCC, w oparciu o doświadczenia zdobyte przez podobne podmioty międzynarodowe, określając niezbędne zasoby, unikając niepotrzebnego powielania działań i dążąc do komplementarności z szerszymi unijnymi ramami cyberbezpieczeństwa.

13. Rada podkreśla znaczenie strategicznej współpracy wywiadowczej w zakresie cyberzagrożeń i działań w cyberprzestrzeni oraz zachęca państwa członkowskie, by za pośrednictwem swoich właściwych organów nadal wnosiły wkład w prace Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN), Dyrekcji Wywiadu (EUMS INT) i państw członkowskich w ramach pojedynczej komórki analiz wywiadowczych (SIAC). Rada ponadto zaznacza, jak ważne jest umocnienie naszych zdolności w zakresie cyberwywiadu w celu zwiększenia unijnej cyberodporności, reagowania i zapewnienia skutecznego wsparcia cywilnym i wojskowym misjom i operacjom w dziedzinie WPBiO, a także unijnym siłom zbrojnym i zdolności SIAC w dziedzinie cyberbezpieczeństwa, w oparciu o dobrowolne wkłady wywiadowcze państw członkowskich i bez uszczerbku dla ich kompetencji.

14. Rada odnotowuje działanie centrum ds. orientacji sytuacyjnej i analiz w zakresie cyberbezpieczeństwa Komisji Europejskiej, które to centrum ma na celu zwiększenie orientacji sytuacyjnej Komisji. Rada podkreśla znaczenie ustanowienia obopólnie korzystnej współpracy między tym centrum a innymi EUIBA, w szczególności Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE). Rada zaznacza, jak ważne podczas rozwijania orientacji sytuacyjnej jest zapewnienie ścisłej współpracy z unijnymi sieciami współpracy, a także poszanowanie poufności. Rada odnotowuje potrzebę wzmocnienia wspólnej orientacji sytuacyjnej na szczeblu UE i dalszego rozwijania unijnych ram zarządzania kryzysowego w cyberprzestrzeni, unikając przy tym niepotrzebnego powielania działań.

15. Rada przypomina, że kształcenie, szkolenie i ćwiczenia w dziedzinie cyberbezpieczeństwa mają zasadnicze znaczenie dla zapewnienia gotowości i skuteczności, i z zadowoleniem przyjmuje działania krajowe, a także działania prowadzone przez UE za pośrednictwem Europejskiego Kolegium Bezpieczeństwa i Obrony (EKBiO), EDA, ENISA i bieżących projektów PESCO, takich jak Federacje cyberpoligonowe oraz Cyberakademia i centrum innowacji UE (EU CAIH). Z myślą o dalszym zintensyfikowaniu tych wysiłków Rada oczekuje ustanowienia projektu ramowego EDA CyDef-X w celu synchronizacji i wspierania ćwiczeń w zakresie cyberobrony. Rada zachęca EDA do zbadania, w ścisłej współpracy z państwami członkowskimi i ESDZ, w jaki sposób CyDef-X mógłby dalej wspierać ćwiczenia takie jak CYBER PHALANX, w tym w zakresie wzajemnej pomocy na mocy art. 42 ust. 7 TUE i klauzuli solidarności na mocy art. 222 TFUE, a także w ścisłej współpracy z Komisją i ENISA w odniesieniu do ćwiczeń cywilnych. Ponadto Rada zachęca do wykorzystywania i dalszego rozwijania w ramach CyDef-X istniejących środowisk testowych i ćwiczebnych w dziedzinie cyberobrony, takich jak Federacje cyberpoligonowe. Aby zapewnić elastyczny i skuteczny proces decyzyjny w sprawach związanych z cyberkryzysami, Rada podkreśla, jak ważne jest organizowanie regularnych ćwiczeń symulacyjnych na szczeblu decyzyjnym państw członkowskich.

16. Rada odnotowuje wniosek dotyczący aktu o cybersolidarności oraz zamiar zwiększenia zdolności wykrywania zagrożeń cyberbezpieczeństwa i cyberincydentów w UE i reagowania na nie. Rada podkreśla, że wnioski w tej dziedzinie mogą być skuteczne tylko wtedy, gdy będą dostosowane do ram i potrzeb państw członkowskich w zakresie zarządzania kryzysowego. Rada podkreśla znaczenie testowania infrastruktury krytycznej pod kątem potencjalnych podatności na zagrożenia, jeżeli uzna się je za korzystne, w ramach kompetencji krajowych, z uwzględnieniem dostępnych unijnych ocen ryzyka.

17. Rada odnotowuje wniosek Komisji dotyczący ustanowienia Mechanizmu Reagowania Cyberkryzysowego, który mógłby wspierać dostępność usług w zakresie cyberbezpieczeństwa świadczonych przez zaufanych dostawców prywatnych, aby na żądanie pomóc państwom członkowskim w przypadku cyberincydentów na dużą skalę; podkreśla jednocześnie potrzebę zwiększenia skali europejskiego sektora cyberbezpieczeństwa przy wsparciu Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) jako podstawowego filaru funkcjonowania tego mechanizmu. Rada podkreśla kluczową rolę każdego państwa członkowskiego w monitorowaniu i ocenie potrzeb krajowych.

II. **Zabezpieczenie ekosystemu obronnego UE**

18. Rada przywołuje słowa zachęty kierowane przez nią do państw członkowskich, by nadal rozwijały swoje zdolności do prowadzenia operacji cyberobrony, w tym, w stosownych przypadkach, proaktywnych środków obronnych służących ochronie i obronie przed cyberatakami oraz wykrywaniu i powstrzymywaniu ich. Biorąc pod uwagę, że NIS 2 nie ma zastosowania do podmiotów administracji publicznej, które prowadzą działalność w dziedzinie obronności, Rada zwraca się do EDA, by – przy wsparciu Komisji i ESDZ, w stosownych przypadkach – pomagała państwom członkowskim w opracowywaniu niewiążących prawnie dobrowolnych zaleceń inspirowanych NIS 2 w celu zwiększenia cyberbezpieczeństwa w społeczności obronnej, i zachęca wszystkie państwa członkowskie do aktywnego zaangażowania się w te działania. Zalecenia te powinny uwzględniać podobne wysiłki podejmowane w innych ramach.

19. Jak stwierdzono w Strategicznym kompasie, zdolność UE do działania zależy od jej zdolności do ograniczenia jej strategicznych zależności w zakresie cyberobronnych zdolności i łańcuchów dostaw, a także od zdolności do rozwijania i opanowania najnowocześniejszych technologii cyberobrony. Obejmuje to wzmocnienie europejskiej bazy technologiczno-przemysłowej sektora obronnego (EDTIB) w całej UE oraz jej zdolności do współpracy z partnerami o podobnych poglądach na całym świecie, na zasadzie wzajemności, aby zapewnić wzajemne korzyści. Rada apeluje zatem, by sektor cyberbezpieczeństwa i sektor cyberobrony ściśle współpracowały nad tworzeniem synergii z myślą o rozwijaniu i zapewnianiu zdolności cyberobronnyvh obejmujących pełne spektrum. Rada zwraca się do Komisji, by w stosownych przypadkach w ścisłej współpracy z ECCC dalej wspierała rozwój silnej, sprawnej, konkurencyjnej i innowacyjnej w skali światowej europejskiej bazy technologiczno-przemysłowej sektora cyberobrony, w tym małych i średnich przedsiębiorstw (MŚP), poprzez dalsze inwestycje i działania polityczne.

20. Biorąc pod uwagę znaczenie interoperacyjności i wspólnego charakteru zdolności w zakresie cyberobrony, w tym w odniesieniu do wspólnego rozwoju zdolności cyberobronnych nowej generacji, Rada zachęca EDA i Sztab Wojskowy UE do pracy nad zestawem wymogów w zakresie interoperacyjności unijnej cyberobrony, które opierałyby się na istniejących zasadach, procesach i standardach ustanowionych w szczególności w ramach Organizacji Traktatu Północnoatlantyckiego (NATO) i były z nimi zgodne. Ponadto Rada zwraca się do państw członkowskich, by w ramach Europejskiego Komitetu Normalizacyjnego w dziedzinie Obronności zbadały, czy można by wymagać konkretnych dobrowolnych standardów dla systemów obronnych, w ścisłej współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym, w stosownych przypadkach, z europejskimi organizacjami normalizacyjnymi i NATO.

21. Rada z zadowoleniem przyjmuje wysiłki Komisji na rzecz przedstawienia planu promowania stosowania istniejących standardów w zakresie cywilnych zastosowań cyberbezpieczeństwa i cyberobrony, a także opracowania nowych dobrowolnych norm. Rada podkreśla, że w stosownych przypadkach należy dostosować standardy cyberbezpieczeństwa i cyberobrony. Rada uznaje, że takie dobrowolne normy mogłyby być przydatne dla unijnego sektora cyberbezpieczeństwa i cyberobrony, i wzywa do ściślejszej współpracy między cywilnymi i obronnymi organami normalizacyjnymi.

22. Rada apeluje o szybkie opracowanie przez Komisję i odpowiednie instytucje zaleceń opartych na mapowaniu istniejących narzędzi bezpiecznej komunikacji w dziedzinie cyberbezpieczeństwa. W miarę możliwości zalecenia powinny być dostosowane do istniejących inicjatyw w zakresie wymiany informacji i powinny również uwzględniać zagrożenia dla obecnych metod szyfrowania stwarzane przez powstające i przełomowe technologie.

23. Ponadto Rada z zadowoleniem przyjmuje wstępne prace nad ocenami i scenariuszami ryzyka podjęte na wniosek Rady przez Komisję, Wysokiego Przedstawiciela i grupę współpracy ds. bezpieczeństwa sieci i informacji, początkowo w odniesieniu do sektora energetycznego i telekomunikacyjnego. Rada uznaje, że przygotowywane są również ukierunkowane oceny cyberryzyka w odniesieniu do infrastruktury i sieci łączności w UE. Rada ponownie podkreśla, że sprawą najwyższej wagi jest wspólne rozumienie przez państwa członkowskie, ale także instytucje, organy i agencje UE, możliwych skutków cyberincydentów. W związku z tym Rada zwraca się do wyżej wymienionych podmiotów o dopilnowanie, by oceny i scenariusze ryzyka oraz późniejsze zalecenia w tym zakresie były brane pod uwagę przy określaniu i ustalaniu priorytetów środków i wsparcia, na szczeblu UE, a w stosownych przypadkach – na szczeblu krajowym. Rada apeluje ponadto, by scenariusze ryzyka były uwzględnianie przez wszystkie odpowiednie podmioty w procesach oceny ryzyka, a także przy opracowywaniu ćwiczeń w dziedzinie cyberbezpieczeństwa.

III. **Inwestowanie w zdolności w zakresie cyberobrony**

24. Rada zachęca państwa członkowskie do zwiększenia inwestycji na rzecz budowania, utrzymywania i dalszego rozwijania interoperacyjnych zdolności w zakresie cyberobrony. Rada popiera opracowanie zestawu dobrowolnych zobowiązań na rzecz dalszego rozwoju krajowych zdolności w zakresie cyberobrony, przy uwzględnieniu podobnych wysiłków podejmowanych w innych ramach.

25. Rada wzywa państwa członkowskie i EDA do wykorzystania okazji, jaką jest przegląd planu rozwoju zdolności, aby wyznaczyć wysoki poziom ambicji w odniesieniu do rozwoju współpracy w zakresie cyberobrony na szczeblu UE. Rada zachęca ponadto państwa członkowskie, by w celu zwiększenia swojego zaangażowania we wspólne unijne projekty rozwoju zdolności w zakresie cyberobrony opierały się na zaktualizowanym zestawie priorytetów i na zobowiązaniach podjętych w ramach PESCO, uznając bezpośrednie korzyści płynące ze wspólnych projektów na szczeblu UE w celu wspierania rozwoju krajowych zdolności w zakresie cyberobrony.

26. Rada z zadowoleniem przyjmuje wspólne wysiłki badawcze na szczeblu UE mające na celu zbadanie możliwych zastosowań powstających i przełomowych technologii w systemach związanych z obronnością, zauważając również potrzebę zapewnienia szybkiego włączenia tych zmian technologicznych do istniejących i przyszłych zdolności. Rada zachęca państwa członkowskie i przemysł UE do jak najlepszego wykorzystania możliwości współpracy w zakresie badań naukowych na szczeblu UE, na przykład w ramach EDA, bieżących projektów PESCO, takich jak Cyberakademia i centrum innowacji UE (CAIH), Europejski Fundusz Obronny oraz, w stosownych przypadkach, program „Horyzont Europa" i program „Cyfrowa Europa" w odniesieniu do projektów podwójnego zastosowania. Ponadto Rada z zadowoleniem przyjmuje wykorzystanie specjalnych ram w celu wspierania innowacji w dziedzinie obronności z wykorzystaniem rozwiązań z sektora cywilnego, w szczególności unijnego systemu innowacji w dziedzinie obronności i centrum innowacji w dziedzinie obronności. Ponadto Rada zachęca Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) i EDA do opracowania porozumienia roboczego w celu ułatwienia wymiany informacji między odpowiednimi pracownikami na temat poszczególnych priorytetów cywilnych, podwójnego zastosowania i technologii obronnych, z myślą o tworzeniu synergii i unikaniu powielania działań.

27. Rada z zadowoleniem przyjmuje zamiar opracowania przez Komisję – we współpracy z EDA i ECCC, zgodnie z ich odpowiednimi mandatami, z państwami członkowskimi i w porozumieniu z odpowiednimi zainteresowanymi stronami, takimi jak przemysł – planu działania w zakresie technologii w zakresie krytycznych cybertechnologii, który poprzez określenie tych technologii, mapowanie rozwoju technologicznego i strategicznych zależności pozwala te zależności ograniczyć, wspierając strategiczną autonomię i suwerenność technologiczną UE, przy jednoczesnym zachowaniu otwartej gospodarki. Rada odnotowuje, że techniczny plan działania w zakresie krytycznych cybertechnologii może stanowić podstawę strategicznych priorytetów unijnych instrumentów finansowania, a jednocześnie być zgodny z odpowiednimi warunkami tych instrumentów. Rada przypomina, że UE powinna realizować ambitną i asertywną europejską politykę przemysłową, aby stworzyć zrównoważone, atrakcyjne i konkurencyjne otoczenie biznesowe, które może również umożliwić europejskim podmiotom działającym w dziedzinie cyberbezpieczeństwa zwiększenie skali działalności.

28. Rada docenia zamiar zaradzenia znacznemu niedoborowi umiejętności w zakresie cyberbezpieczeństwa poprzez przyciąganie nowych specjalistów, w tym kobiet, podnoszenie i zmianę kwalifikacji, a także inwestowanie w szkolenia i ćwiczenia służące utworzeniu zróżnicowanej i inkluzywnej siły roboczej w sektorze cybernetycznym oraz organizowanie takich szkoleń i ćwiczeń. Uznając wyzwania, przed którymi stoi UE w odniesieniu do kapitału ludzkiego w zakresie cyberbezpieczeństwa i cyberobrony, Rada z zadowoleniem przyjmuje inicjatywę Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa, która może również przynieść korzyści pracownikom w dziedzinie cyberobrony.

29. Rada zwraca się do państw członkowskich o wymianę informacji na temat najlepszych praktyk z myślą o rozwoju wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa, przy wykorzystaniu synergii między inicjatywami wojskowymi, cywilnymi i w zakresie egzekwowania prawa, oraz wzywa EKBiO, by przy wsparciu i wiedzy fachowej EDA i ENISA rozważyły możliwości lepszej wymiany najlepszych praktyk i dalszej synergii między obszarami wojskowymi i cywilnymi dotyczących szkoleń i rozwoju umiejętności w zakresie cyberobrony.

30. Rada podkreśla, jak ważne jest wspólne rozumienie składu siły roboczej w dziedzinie cyberbezpieczeństwa i powiązanych umiejętności w celu zidentyfikowania i wyeliminowania luk na rynku pracy w dziedzinie cyberbezpieczeństwa; zwraca także uwagę na potrzebę zaangażowania wszystkich zainteresowanych stron, w tym państw członkowskich i przemysłu. Rada uznaje, że ustanowienie wskaźników monitorowania rynku pracy cyberbezpieczeństwa pomogłoby określić potrzeby w zakresie umiejętności w tej dziedzinie i odpowiednio ukierunkować fundusze, przyczyniając się jednocześnie do wypełnienia obowiązków związanych z polityką, w szczególności wynikających z NIS 2. Rada z zadowoleniem przyjmuje wniosek dotyczący ram certyfikacji umiejętności w zakresie cyberobrony i zwraca się do Wysokiego Przedstawiciela, jako szefa EKBiO, o opracowanie tych ram we współpracy z ESDZ, Komisją i państwami członkowskimi poprzez wykorzystanie inicjatyw cywilnych.

IV. **Partnerstwo w stawianiu czoła wspólnym wyzwaniom**

31. Rada wzywa Wysokiego Przedstawiciela i Komisję do umocnienia i zacieśnienia współpracy oraz do zbadania wzajemnie korzystnych i dostosowanych do potrzeb partnerstw w zakresie polityki cyberobrony, w tym dotyczących budowania zdolności w zakresie cyberobrony za pośrednictwem Europejskiego Instrumentu na rzecz Pokoju. W tym celu cyberobrona powinna zostać dodana jako punkt porządku obrad w dialogach i konsultacjach UE dotyczących cyberprzestrzeni, a także do ogólnych konsultacji z partnerami w dziedzinie bezpieczeństwa i obrony. Ponadto należy zintensyfikować dialogi i współpracę z sektorem prywatnym. Rada podkreśla, że międzynarodowa współpraca w zakresie standardów i certyfikacji cyberbezpieczeństwa stanowiłaby wartość dodaną dla przemysłu europejskiego. W związku z tym z zadowoleniem przyjmuje zobowiązanie Komisji do uczynienia z tego zasadniczego elementu dialogu, jaki UE prowadzi w sprawach cybeprzestrzeni z państwami trzecimi i organizacjami międzynarodowymi.

32. Rada podkreśla znaczenie współpracy międzynarodowej w celu zapobiegania ryzyku konfliktów w cyberprzestrzeni lub ograniczania tego ryzyka, zwłaszcza poprzez dalszy rozwój i operacjonalizację środków budowy zaufania na szczeblu regionalnym i międzynarodowym, w tym na szczeblu ONZ, oraz znaczenie dalszego zachęcania do korzystania z istniejących środków budowy zaufania, np. na forum Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), w tym w czasach napięć międzynarodowych.

    UE i jej państwa członkowskie podkreślają, że obowiązujące prawo międzynarodowe ma zastosowanie w cyberprzestrzeni i podkreślają, jak ważne są stałe wysiłki na rzecz utrzymania i promowania ram ONZ dotyczących odpowiedzialnego zachowania państw oraz działania na rzecz jego realizacji, w tym poprzez ustanowienie programu działania na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni.

33. Zgodnie ze wspólnymi deklaracjami w sprawie współpracy UE–NATO Rada zwraca się do Wysokiego Przedstawiciela jako do szefa EDA oraz do Komisji o dalsze zacieśnianie, pogłębianie i rozszerzanie partnerstwa z NATO w dziedzinie cyberbezpieczeństwa przy pełnym poszanowaniu zasad inkluzywności, wzajemności, wzajemnej otwartości i przejrzystości, a także autonomii decyzyjnej obydwu organizacji. Biorąc pod uwagę potrzebę zapewnienia komplementarnych i skoordynowanych wysiłków przy jak największym zaangażowaniu państw członkowskich nienależących do NATO i unikania niepotrzebnego powielania działań, Rada wzywa do ustanowienia powiązań na odpowiednich szczeblach między UE a NATO w zakresie szkoleń, edukacji, orientacji sytuacyjnej, ćwiczeń i platform badawczo-rozwojowych oraz do poszukiwania potencjalnych synergii między odpowiednimi dobrowolnymi zobowiązaniami na rzecz rozwoju krajowych zdolności w zakresie cyberobrony i ram zarządzania kryzysowego, ochrony infrastruktury krytycznej i zwiększenia wymiany informacji w dziedzinie orientacji sytuacyjnej, skoordynowanych reakcji na szkodliwe działania w cyberprzestrzeni, a także wysiłków na rzecz budowania zdolności w państwach trzecich. Obejmuje to porozumienie techniczne między komórką NATO ds. reagowania na incydenty komputerowe (NCIRC) a Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE), a także pogłębiony dialog polityczny na temat kwestii cyberobrony na wszystkich szczeblach.

V. **Wnioski**

34. W oparciu o konkluzje Rady w sprawie polityki UE w zakresie cyberobrony, Rada wzywa Wysokiego Przedstawiciela i Komisję, by przed drugim kwartałem 2023 r. opracowały do zatwierdzenia przez państwa członkowskie plan wdrożenia tej polityki. Rada zwraca się również do państw członkowskich o dobrowolne określenie swoich ambicji i działań w odniesieniu do cyberobrony w kontekście polityki UE w zakresie cyberobrony oraz o pełne wykorzystanie niewiążących prawnie dobrowolnych zaleceń i zobowiązań do zintensyfikowania krajowych i wielonarodowych działań w zakresie cyberobrony mających na celu osiągniecie maksymalnego wpływu na szczeblu UE. Wzywa się Wysokiego Przedstawiciela, Komisję i państwa członkowskie do corocznego składania sprawozdań i dyskusji na temat postępów w realizacji elementów wspólnego komunikatu i jego planu wdrażania, począwszy od drugiego kwartału 2024 r.