Rada
Unii Europejskiej

Bruksela, 9 marca 2021 r.
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

NOTA DO PUNKTU I/A

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli / Rada
Dotyczy:	Projekt konkluzji Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę

1. W dniu 16 grudnia 2020 r. Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa opublikowali wspólny komunikat do Parlamentu Europejskiego i Rady pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę”[1]. Nowa strategia w zakresie cyberbezpieczeństwa ma zwiększyć zbiorową odporność Europy na cyberzagrożenia i zapewnić wszystkim obywatelom i firmom możliwość pełnego korzystania z wiarygodnych i niezawodnych narzędzi i usług cyfrowych.

[1] 14133/20.

2. Komisja i ESDZ przedstawiły wspólny komunikat na nieformalnej wideokonferencji Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni (HWPCI) w dniu 17 grudnia 2020 r. oraz w dniu 12 stycznia 2021 r. Podczas nieformalnej wideokonferencji HWPCI w dniu 17 grudnia 2020 r. przyszła portugalska prezydencja Rady ogłosiła zamiar przygotowania projektu konkluzji Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę.

3. Prezydencja przedstawiła wstępny projekt konkluzji Rady na nieformalnej wideokonferencji HWPCI w dniu 2 lutego 2021 r. Konkluzje te zostały następnie omówione podczas nieformalnych wideokonferencji HWPCI w dniach 9 lutego 2021 r., 19 lutego 2021 r. oraz 1i 9 marca 2021 r.

4. Ponieważ projekt konkluzji zawiera również odniesienie do polityki obronnej UE (pkt 30), Grupa Polityczno-Wojskowa (PMG) przedyskutowała odnośny punkt na swym posiedzeniu w dniu 10 lutego 2021 r.

5. Szereg punktów odnosi się do wspólnej polityki zagranicznej i bezpieczeństwa (punkty 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 i 33) i w związku z tym zostały one przedłożone Komitetowi Politycznemu i Bezpieczeństwa, który poparł powyższe punkty na swym posiedzeniu w dniu 4 marca 2021 r.

6. Podczas nieformalnej wideokonferencji w dniu 9 marca 2021 r. HWPCI doszła do porozumienia co do projektu konkluzji Rady w brzmieniu przedstawionym w dokumencie 6722/21.

7. Z uwagi na powyższe Komitet Stałych Przedstawicieli proszony jest o przedłożenie Radzie załączonego projektu konkluzji Rady oraz o zasugerowanie, by przyjęła ona projekt konkluzji w jednym z punktów A porządku obrad.

ZAŁĄCZNIK

Projekt konkluzji Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC swoje 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”[2],

– zarządzania internetem[3],

– wspólnego komunikatu z dnia 20 listopada 2017 r. do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE”[4],

– budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa[5],

– znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczenia zagrożeń dla bezpieczeństwa związanych z 5G[6]

– przyszłości wysoce ucyfrowionej Europy po roku 2020: „Stymulowanie cyfrowej i gospodarczej konkurencyjności i spójności cyfrowej w całej Unii”[7],

– dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych[8],

– kształtowania cyfrowej przyszłości Europy[9],

---

2 12109/13.
3 16200/14.
4 14435/17 + COR 1.
5 7737/19.
6 14517/19.
7 9596/19.
8 14972/19.
9 8711/20.

– dyplomacji cyfrowej[10],

– wzmacniania odporności i zwalczania zagrożeń hybrydowych, w tym dezinformacji w kontekście pandemii COVID-19[11],

– dyplomacji elektronicznej[12],

– skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę[13],

– ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej")[14],

– wytycznych dotyczące budowania przez UE zewnętrznych zdolności cyfrowych[15],

– odbudowy przyspieszającej przechodzenie na bardziej dynamiczny, odporny i konkurencyjny przemysł europejski[16],

– cyberbezpieczeństwa urządzeń podłączonych do internetu[17],

– wzmacniania europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego[18],

– oraz swoją rezolucję w sprawie szyfrowania – Bezpieczeństwo dzięki szyfrowaniu i bezpieczeństwo pomimo szyfrowania[19],

---

10 12804/20.
11 14064/20.
12 6122/15 + COR 1.
13 10086/18.
14 10474/17.
15 10496/18.
16 13004/20.
17 13629/20.
18 14540/16.
19 13084/1/20 REV 1.

– oraz deklarację państw członkowskich z dnia 15 października 2020 r. pt. „Budowanie chmury obliczeniowej nowej generacji dla przedsiębiorstw i sektora publicznego w UE”;

PRZYWOŁUJĄC konkluzje Rady Europejskiej w sprawie COVID-19, jednolitego rynku, polityki przemysłowej, kwestii cyfrowych i stosunków zewnętrznych z dni 1–2 października 2020 r.[20] oraz w sprawie dezinformacji i zagrożeń hybrydowych oraz w sprawie nowego programu strategicznego na lata 2019–2024 z dnia 20 czerwca 2019 r.[21],

PRZYWOŁUJĄC „Globalną strategię na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej – wspólna wizja, wspólne działanie: silniejsza Europa” z dnia 28 czerwca 2016 r.,

PRZYWOŁUJĄC komunikat Komisji Europejskiej pt. „Kształtowanie cyfrowej przyszłości Europy” z dnia 19 grudnia 2020 r.[22] i komunikat w sprawie strategii UE w zakresie unii bezpieczeństwa z dnia 24 lipca 2020 r.[23],

PRZYWOŁUJĄC wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela pt. „Nowa agenda UE–USA na rzecz globalnych zmian” z dnia 2 grudnia 2020 r.[24],

1. PODKREŚLA, że cyberbezpieczeństwo ma zasadnicze znaczenie w budowaniu odpornej, ekologicznej i cyfrowej Europy, oraz Z ZADOWOLENIEM PRZYJMUJE wspólny komunikat do Parlamentu Europejskiego i Rady pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę”, który nakreśla nowe ramy działań UE w obszarze „odporności, suwerenności technologicznej i przywództwa” i wskazuje, jak chronić obywateli, firmy i instytucje przed cyberincydentami i cyberzagrożeniami, a jednocześnie zwiększyć zaufanie obywateli i organizacji do zdolności UE w zakresie promowania bezpiecznych i niezawodnych sieci i systemów informacyjnych, infrastruktury, łączności oraz w zakresie promowania i ochrony globalnej, otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni opierającej się na poszanowaniu praw człowieka, podstawowych wolności, demokracji i praworządności.

---

20 EUCO 13/20.
21 EUCO 9/19.
22 19.2.2020 COM(2020) 67 final.
23 24.7.2020 COM(2020) 605 final.
24 2.12.2020 JOIN(2020) 22 final.

2. UZNAJE, że pandemia COVID-19 podkreśliła, że w naszym codziennym życiu coraz bardziej potrzebne jest zaufanie do narzędzi i systemów wykorzystujących technologie informacyjno-komunikacyjne (ICT) oraz do ich bezpieczeństwa. PODKREŚLA, że cyberbezpieczeństwo oraz globalny i otwarty internet odgrywają podstawową rolę w funkcjonowaniu administracji publicznej i instytucji publicznych zarówno na poziomie krajowym, jak i UE oraz, ogólnie, naszego społeczeństwa i naszej gospodarki.

3. PODKREŚLA potrzebę dalszego poszerzania świadomości na temat kwestii dotyczących cyberprzestrzeni przy podejmowaniu decyzji na poziomie politycznym i strategicznym przez dostarczanie decydentom odpowiedniej wiedzy i odnośnych informacji oraz PODKREŚLA potrzebę poprawy świadomości ogółu społeczeństwa i promowania higieny cyberbezpieczeństwa.

4. WZYWA do promowania i ochrony kluczowych wartości UE, czyli demokracji, praworządności, praw człowieka i podstawowych wolności, w tym prawa do wolności wypowiedzi i informacji, prawa do wolności zgromadzania się i zrzeszania się oraz prawa do prywatności w cyberprzestrzeni. Z ZADOWOLENIEM PRZYJMUJE w związku z tym dalsze nieustające wysiłki, by chronić obrońców praw człowieka, społeczeństwo obywatelskie i środowisko akademickie pracujących nad takimi zagadnieniami, jak cyberbezpieczeństwo, prywatność danych, nadzór i cenzura online, przez przygotowywanie kolejnych praktycznych wytycznych, promowanie najlepszych praktyk i zwiększanie wysiłków UE na rzecz przeciwdziałania łamaniu i naruszaniu praw człowieka i niewłaściwemu wykorzystywaniu powstających technologii, zwłaszcza stosując, gdy to konieczne, środki dyplomatyczne, jak również kontrolę eksportu takich technologii. PODKREŚLA w tym kontekście znaczenie Planu działania UE dotyczącego praw człowieka i demokracji na lata 2020–2024 oraz zawartych w nim wytycznych w sprawie praw człowieka dotyczących wolności wypowiedzi w internecie i poza nim.
5. PODKREŚLA, że jednym z kluczowych celów Unii, który pozwoli jej samodzielnie określić własne ścieżki i interesy gospodarcze, jest osiągnięcie strategicznej autonomii przy zachowaniu otwartej gospodarki. Obejmuje to zwiększenie zdolności dokonywania samodzielnych wyborów w obszarze cyberbezpieczeństwa w celu wzmocnienia cyfrowego przywództwa UE i jej strategicznych zdolności. PRZYPOMINA, że obejmuje to zidentyfikowanie i ograniczenie strategicznych zależności oraz zwiększenie odporności najwrażliwszych ekosystemów przemysłowych i konkretnych obszarów. PODKREŚLA, że może to obejmować dywersyfikację łańcuchów produkcji i dostaw, zachęcanie do inwestycji i produkcji w Europie oraz przyciąganie ich, badanie alternatywnych rozwiązań imodeli o obiegu zamkniętym, a także propagowanie szerokiej współpracy przemysłowej w państwach członkowskich.

6. Biorąc pod uwagę niedobór umiejętności cyfrowych i umiejętności w zakresie cyberbezpieczeństwa wśród pracowników, PODKREŚLA znaczenie zaspokajania zapotrzebowania na pracowników wykwalifikowanych w dziedzinie cyfryzacji i cyberbezpieczeństwa, w szczególności przez rozwijanie, zatrzymywanie i przyciąganie najbardziej utalentowanych osób, na przykład przez kształcenie i szkolenia, tak by można było ucyfrowić nasze społeczeństwo w cyberbezpieczny sposób. ZACHĘCA do zwiększonego udziału kobiet i dziewcząt w zajęciach z nauk przyrodniczych, technologii, inżynierii i matematyki (STEM) oraz w podejmowania pracy w zawodach związanych z ICT poprzez podnoszenie dotychczasowych i nabywanie nowych kwalifikacji w zakresie umiejętności cyfrowych jako jednego ze sposobów niwelowania przepaści cyfrowej między kobietami a mężczyznami.

7. 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. PONOWNIE POTWIERDZA w tym kontekście swoje zobowiązanie do pokojowego rozstrzygania sporów międzynarodowych w cyberprzestrzeni oraz że wszystkie wysiłki dyplomatyczne UE powinny być w pierwszej kolejności ukierunkowane na propagowanie bezpieczeństwa i stabilności w cyberprzestrzeni przez zacieśnianie współpracy międzynarodowej oraz na ograniczanie ryzyka nieporozumień, eskalacji i konfliktów, które mogą wynikać z incydentów związanych z ICT, oraz POPIERA dalsze opracowywanie i wdrażanie środków budowy zaufania na poziomie regionalnym i międzynarodowym. PONOWNIE PODKREŚLA wezwanie Zgromadzenia Ogólnego Narodów Zjednoczonych, przyjęte w drodze konsensusu, by – korzystając z ICT – państwa członkowskie ONZ kierowały się zaleceniami zawartymi w sprawozdaniach grupy ekspertów rządowych ONZ oraz PONOWNIE POTWIERDZA stosowanie prawa międzynarodowego, w szczególności całej Karty Narodów Zjednoczonych, w cyberprzestrzeni.

8. PONOWNIE POTWIERDZA, że dalszy rozwój norm i standardów w Unii ma zasadnicze znaczenie, aby w istotny sposób kształtować normy i standardy międzynarodowe w obszarach nowych technologii oraz infrastruktury technicznej i logicznej o zasadniczym znaczeniu dla ogólnej dostępności i integralności publicznego rdzenia internetu, tak by były one zgodne z wartościami uniwersalnymi i unijnymi w ramach podejścia z udziałem wielu zainteresowanych stron. Pozwoli to zapewnić, że internet będzie mieć nadal światowy zasięg, będzie otwarty, wolny, stabilny i bezpieczny oraz że wykorzystywanie i rozwój technologii cyfrowych będzie odbywać się w poszanowaniu praw człowieka, a ich używanie będzie zgodne z prawem, bezpieczne i etyczne. PRZYJMUJE DO WIADOMOŚCI zapowiedź strategii normalizacyjnej i ZOBOWIĄZUJE się do proaktywnych i skoordynowanych działań promujących wiodącą rolę UE w tym zakresie oraz unijne cele na arenie międzynarodowej, w tym w szeregu międzynarodowych organów normalizacyjnych, oraz przez współpracę z partnerami o podobnym podejściu, społeczeństwem obywatelskim, środowiskiem akademickim i sektorem prywatnym.

9. STANOWCZO POPIERA oparty na porozumieniu wielu zainteresowanych stron model zarządzania internetem i cyberbezpieczeństwem oraz zobowiązuje się do zintensyfikowania regularnych i uporządkowanych wymian poglądów z zainteresowanymi podmiotami, w tym z sektorem prywatnym, środowiskiem akademickim i społeczeństwem obywatelskim, na forach międzynarodowych, również w kontekście paryskiej deklaracji w sprawie zaufania i bezpieczeństwa w cyberprzestrzeni. PROMUJE powszechny, przystępny cenowo i równy dostęp do internetu pozwalający zniwelować przepaść cyfrową, a w szczególności wzmocnienie pozycji kobiet i dziewcząt oraz osób znajdujących się w trudnej sytuacji lub zmarginalizowanych zarówno w rozwoju strategii politycznych, jak i w korzystaniu z internetu.

10. PODKREŚLA potrzebę uwzględniania cyberbezpieczeństwa w inwestycjach i inicjatywach dotyczących cyfryzacji w kolejnych latach i potrzebę dokonywania stałych postępów w tworzeniu równych zasad działania w dziedzinie cyberbezpieczeństwa oraz PRZYJMUJE DO WIADOMOŚCI plan Komisji, by zwiększyć wydatki publiczne oraz pozyskiwać prywatne inwestycje w tej dziedzinie. PODKREŚLA znaczenie małych i średnich przedsiębiorstw (MŚP) w ekosystemie cyberbezpieczeństwa i UZNAJE, że w okresie obowiązywania wieloletnich ram finansowych (WRF) na lata 2021–2027, jak również w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności (RRF) dostępne są właściwe instrumenty finansowe, by zdecydowanie wspierać cyberbezpieczeństwo podczas transformacji cyfrowej.

11. OCZEKUJE szybkiego wdrożenia rozporządzenia ustanawiającego Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji, w tym szybkiego utworzenia Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w Bukareszcie i rozpoczęcia przez nie działalności. Szybkie przyjęcie jego programu działania przyczyni się do maksymalnego wykorzystania skutków inwestycji we wzmocnienie wiodącej roli Unii i jej strategicznej autonomii w obszarze cyberbezpieczeństwa i wesprze zdolności i umiejętności techniczne, a także zwiększy konkurencyjność Unii na świecie przy zaangażowaniu przemysłu i środowisk akademickich w cyberbezpieczeństwo, w tym MŚP i ośrodków badawczych, które skorzystają z bardziej uporządkowanej, sprzyjającej włączeniu i strategicznej współpracy, biorąc pod uwagę spójność Unii i wszystkich jej państw członkowskich.

12. Z ZADOWOLENIEM PRZYJMUJE prace prowadzone obecnie przez agencję ENISA wraz z państwami członkowskimi i zainteresowanymi podmiotami, by przyjąć w UE systemy certyfikacji produktów, usług i procesów w zakresie ICT, co powinno przyczynić do podniesienia ogólnego poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. OCZEKUJE w tym kontekście unijnego kroczącego programu prac, którego celem będzie opracowanie unijnych systemów certyfikacji cyberbezpieczeństwa w ramach aktu o cyberbezpieczeństwie. UZNAJE w tym kontekście wiodącą rolę UE w opracowywaniu norm, które mogą kształtować otoczenie cyberbezpieczeństwa oraz przyczyniają się do zapewnienia uczciwej konkurencji w UE i na świecie, promując dostęp do rynku, jak również eliminując zagrożenia dla bezpieczeństwa, przy jednoczesnym zagwarantowaniu stosowania unijnych ram prawnych.

13. PONOWNIE PODKREŚLA, że z myślą o uwzględnieniu wszystkich istotnych aspektów cyberbezpieczeństwa urządzeń podłączonych do internetu, takich jak dostępność, integralność i poufność, ważne jest, by ocenić potrzebę wprowadzenia horyzontalnego prawodawstwa w długofalowej perspektywie, określając także warunki niezbędne do wprowadzenia do obrotu. Z ZADOWOLENIEM PRZYJMUJE w tym kontekście dyskusję na temat zakresu takiego prawodawstwa i jego powiązań z ramami certyfikacji cyberbezpieczeństwa, określonymi na mocy aktu o cyberbezpieczeństwie, z myślą o podniesieniu poziomu bezpieczeństwa na jednolitym rynku cyfrowym. PODKREŚLA, że wymogi w zakresie cyberbezpieczeństwa powinny zostać określone zgodnie z odpowiednim prawodawstwem Unii, w tym aktem o cyberbezpieczeństwie, nowymi ramami prawnymi, rozporządzeniem w sprawie normalizacji europejskiej oraz ewentualnym przyszłym prawodawstwem horyzontalnym, tak by uniknąć niejednoznaczności i fragmentacji prawnej.

14. UZNAJE znaczenie kompleksowego i horyzontalnego podejścia do cyberbezpieczeństwa w Unii, przy pełnym poszanowaniu kompetencji i potrzeb państw członkowskich, jak również znaczenie stałego wsparcia w obszarze pomocy technicznej i współpracy, by rozwijać zdolności państw członkowskich. Biorąc pod uwagę ewolucję cyberzagrożeń, PRZYJMUJE DO WIADOMOŚCI nowy wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, który czerpie z dyrektywy w sprawie bezpieczeństwa sieci i informacji, i ponownie podkreśla swoje poparcie dla wzmocnienia i harmonizacji krajowych ram dotyczących cyberbezpieczeństwa oraz stałej współpracy państw członkowskich. PODKREŚLA ponadto potrzebę uspójnienia i skoordynowania przepisów sektorowych w tej dziedzinie.

15. PRZYJMUJE DO WIADOMOŚCI wniosek Komisji wspierający państwa członkowskie w tworzeniu i umacnianiu centrów monitorowania bezpieczeństwa (SOC), by stworzyć sieć SOC w UE, co pozwoli kontynuować monitorowanie sieci i rejestrować oznaki ataków przygotowywanych na nie. OCZEKUJE w tym kontekście szczegółowych planów ze strony Komisji dotyczących sieci SOC, przy jednoczesnym poszanowaniu kompetencji państw członkowskich. PRZYPOMINA wysiłki podejmowane przez państwa członkowskie wspierane przez UE, by utworzyć sektorowe, krajowe i regionalne zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz krajowe lub europejskie ośrodki wymiany i analizy informacji jako część skutecznej sieci partnerstw w dziedzinie cyberbezpieczeństwa w Unii. OCZEKUJE zbadania potencjału tej sieci w zakresie wzmocnienia SOC, jak również ich komplementarności i koordynacji z istniejącymi sieciami i podmiotami (przede wszystkim siecią CSIRT), by promować kulturę skutecznej, bezpiecznej i niezawodnej wymiany informacji. PODKREŚLA, że proces ten będzie się opierał na pracach przeprowadzonych w kontekście inicjatyw związanych ze sztuczną inteligencją i z obliczeniami wielkiej skali oraz przez europejskie centra innowacji cyfrowych.

16. PRZYJMUJE DO WIADOMOŚCI ewentualne opracowanie bezpiecznego systemu łączności, korzystającego z doświadczeń europejskiej kwantowej infrastruktury komunikacyjnej (EuroQCI) oraz rządowej łączności satelitarnej w Unii Europejskiej (GOVSATCOM), oraz UZNAJE, że wszelkie ewentualne nowe rozwiązania w przyszłości powinny opierać się na solidnych ramach cyberbezpieczeństwa i brać pod uwagę całą infrastrukturę łączności elektronicznej, w tym kosmiczne, lądowe i podmorskie systemy sieciowe.

17. OCZEKUJE dyskusji z Komisją, agencją ENISA, dwoma unijnymi operatorami głównego serwera DNS i społecznością obejmującą wiele zainteresowanych stron, by ocenić rolę tych operatorów w zapewnieniu stałej dostępności internetu na całym świecie i przeciwdziałaniu jego fragmentacji. Z ZADOWOLENIEM PRZYJMUJE dalsze dyskusje nad planami Komisji, by stworzyć alternatywną europejską usługę dostępu do globalnego internetu (inicjatywa „DNS4EU”), w oparciu o przejrzysty model, który jest zgodny z najnowszymi normami i zasadami bezpieczeństwa, ochrony danych i prywatności w fazie programowania i domyślnie, by przyczynić się do zwiększonej odporności, przy jednoczesnym utrzymaniu i usprawnieniu łączności międzynarodowej wszystkich państw członkowskich.

18. UZNAJE potrzebę podjęcia przez Komisję i państwa członkowskie wspólnych wysiłków, by przyspieszyć przyjmowanie kluczowych norm kształtowania internetu, w tym IPv6, oraz solidnie ugruntowanych norm bezpieczeństwa internetu, które mają zasadnicze znaczenie w podnoszeniu ogólnego poziomu bezpieczeństwa, odporności, otwartości i interoperacyjności globalnego internetu, przy jednoczesnym zwiększaniu konkurencyjności przemysłu UE, a w szczególności operatorów infrastruktury internetowej.

19. PODKREŚLA znaczenie skoordynowanego podejścia, jak również opracowania i wdrożenia skutecznych środków na poziomie krajowym, by zwiększyć cyberbezpieczeństwo sieci 5G. POPIERA kolejne kroki proponowane w odniesieniu do cyberbezpieczeństwa sieci 5G w dodatku do strategii UE w zakresie cyberbezpieczeństwa i opierające się na wynikach sprawozdania ws. wpływu zaleceń Komisji na bezpieczeństwo sieci 5G, na przykład w odniesieniu do określenia długofalowego i kompleksowego podejścia biorącego pod uwagę cały łańcuch wartości i ekosystem 5G. W celu dalszego wzmocnienia skoordynowanego podejścia do bezpieczeństwa sieci 5G WZYWA państwa członkowskie, instytucje UE i inne odpowiednie zainteresowane podmioty, by kontynuowały okresowe analizy oraz wymieniały się informacjami i najlepszymi praktykami w ramach prac specjalnej grupy współpracy ds. bezpieczeństwa sieci i informacji w zakresie cyberbezpieczeństwa sieci 5G, oraz przygotowywały regularne sprawozdania dla Rady w zakresie postępów tych prac. Podkreślając odpowiedzialność państw członkowskich za ochronę bezpieczeństwa narodowego, ZWRACA UWAGĘ na swe stanowcze zobowiązanie do stosowania i szybkiego zakończenia wdrażania środków w ramach unijnego zestawu narzędzi na potrzeby sieci 5G oraz do stałego podejmowania wysiłków w celu zagwarantowania bezpieczeństwa sieci 5G i rozwijania sieci nowych generacji. Ścisła współpraca między państwami członkowskimi, Komisją i agencją ENISA w zakresie bezpieczeństwa sieci 5G mogłaby posłużyć jako przykład w innych kwestiach w obszarze cyberbezpieczeństwa, przy jednoczesnym poszanowaniu kompetencji państw członkowskich oraz zasad pomocniczości i proporcjonalności.

20. UZNAJE dalsze włączanie cyberbezpieczeństwa w unijne mechanizmy reagowania kryzysowego i testowanie tych rozwiązań w praktyce za zasadne oraz PODKREŚLA znaczenie wzmacniania współpracy i pogłębiania wymiany informacji między różnymi grupami zajmującymi się cyberbezpieczeństwem w UE oraz łączenia istniejących inicjatyw, struktur i procedur (takich jak zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych – IPCR, sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego – CSIRT, grupa współpracy ds. bezpieczeństwa sieci i informacji, europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa – CyCLONe, Europejskie Centrum ds. Walki z Cyberprzestępczością, Centrum Analiz Wywiadowczych Unii Europejskiej – INTCEN UE oraz inne właściwe organy UE) w przypadku ponadgranicznych cyberincydentów i cyberzagrożeń na dużą skalę. BIORĄC POD UWAGĘ już osiągnięte postępy w tej dziedzinie, OCZEKUJE wniosku Komisji w sprawie procesu, celów pośrednich i ram czasowych określania charakteru wspólnej jednostki ds. cyberprzestrzeni (JCU) w celu zwiększenia wartości dodanej unijnych ram zarządzania kryzysami w zakresie cyberbezpieczeństwa, jasnego skoncentrowania się na nich i uwzględnienia ich w głównym nurcie polityki, w tym przez gotowość, wspólną orientację sytuacyjną, wzmocnioną skoordynowaną reakcję oraz ćwiczenia praktyczne, stopniowo i w przejrzysty sposób, przy jednoczesnym unikaniu powielania i nakładania się podejmowanych działań oraz poszanowaniu kompetencji państw członkowskich.

21. PODKREŚLA zarówno znaczenie promowania współpracy i wymiany informacji między odnośnymi podmiotami zajmującymi się cyberbezpieczeństwem a właściwymi organami w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych, np. organów ścigania i sądowych, jak również potrzebę rozszerzenia i poprawy możliwości tych organów w zakresie prowadzenia dochodzeń i ścigania cyberprzestępstw oraz wpływania na przebieg międzynarodowych negocjacji i na zasady UE w odniesieniu do ponadgranicznego dostępu do elektronicznego materiału dowodowego. Niezależnie od otoczenia technologicznego w danym okresie kluczowe jest, aby zachować uprawnienia właściwych organów w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych opierające się na zgodnym z prawem dostępie umożliwiającym tym organom wykonywanie ich zadań, zgodnie z tym, co przewidują i dopuszczają przepisy. Takie przepisy przewidujące uprawnienia w zakresie egzekwowania muszą zawsze w pełni respektować należyte procedury i inne zabezpieczenia, a także prawa podstawowe, w szczególności prawo do poszanowania życia prywatnego i komunikowania się oraz prawo do ochrony danych osobowych.

22. PONOWNIE POTWIERDZA swoje poparcie dla opracowania, wdrożenia i wykorzystania zaawansowanego szyfrowania jako jednego z niezbędnych środków ochrony praw podstawowych i zapewniania cyfrowego bezpieczeństwa obywateli, rządów, przemysłu i społeczeństwa, a jednocześnie UZNAJE, że należy zapewnić właściwym organom w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych, np. organom ścigania i organom sądowym, możliwość korzystania z przysługujących im z mocy prawa uprawnień zarówno w internecie, jak i poza nim w celu ochrony społeczeństwa i obywateli. Właściwe organy muszą mieć możliwość dostępu do danych w sposób zgodny z prawem i ukierunkowany, w pełnym poszanowaniu praw podstawowych i odpowiednich przepisów o ochronie danych, przy jednoczesnym utrzymaniu cyberbezpieczeństwa. PODKREŚLA, że we wszystkich podejmowanych działaniach należy starannie wyważyć te interesy względem zasad konieczności, proporcjonalności i pomocniczości.

23. POPIERA i PROMUJE budapeszteńską Konwencję o cyberprzestępczości i bieżące prace nad drugim Protokołem dodatkowym do tej konwencji. Ponadto nadal angażuje się w wielostronną wymianę poglądów na temat cyberprzestępczości, w tym w ramach procesów związanych z Radą Europy, Biurem Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC) i Komisją ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Sądownictwa Karnego (CCPCJ), aby zapewnić usprawnioną współpracę międzynarodową ukierunkowaną na przeciwdziałanie cyberprzestępczości, w tym wymianę najlepszych praktyk i wiedzy technicznej oraz wspieranie rozwijania zdolności, a jednocześnie przy poszanowaniu, promowaniu i ochronie praw człowieka i podstawowych wolności.

24. UZNAJE, że choć to państwa członkowskie ponoszą wyłączną odpowiedzialność za bezpieczeństwo krajowe, strategiczna współpraca wywiadowcza w zakresie cyberzagrożeń i działań w cyberprzestrzeni ma zasadnicze znaczenie, i ZACHĘCA państwa członkowskie, by przez właściwe organy nadal angażowały się w prace INTCEN UE jako unijnego ośrodka zajmującego się orientacją sytuacyjną i oceną zagrożeń w kwestiach dotyczących cyberprzestrzeni oraz by przeanalizowały wniosek w sprawie ewentualnego utworzenia grupy roboczej państw członkowskich ds. wywiadu cyfrowego w celu zwiększenia możliwości INTCEN w tym obszarze, w oparciu o dobrowolne zaangażowanie wywiadowcze państw członkowskich i bez szkody dla ich kompetencji.

25. PODKREŚLA znaczenie solidnych i spójnych ram bezpieczeństwa, by chronić cały personel, wszystkie dane, sieci komunikacyjne i systemy informatyczne oraz procesy decyzyjne UE w oparciu o kompleksowe, spójne i jednolite zasady. W tym celu należy w szczególności zwiększyć odporność i poprawić kulturę bezpieczeństwa UE wobec cyberzagrożeń oraz zwiększyć bezpieczeństwo unijnych sieci wymiany informacji niejawnych i jawnych, przy jednoczesnym zapewnieniu adekwatnego zarządzania oraz dostępności wystarczających zasobów i zdolności, w tym w kontekście wzmocnienia mandatu CERT-UE. Z ZADOWOLENIEM PRZYJMUJE w tym kontekście toczące się dyskusje w sprawie utworzenia wspólnych zasad dotyczących bezpieczeństwa informacji, należycie uwzględniających zasady bezpieczeństwa Rady dotyczące ochrony informacji niejawnych UE, jak również określenia wspólnych wiążących zasad cyberbezpieczeństwa dla wszystkich instytucji, organów i jednostek UE.

26. OPIERAJĄC SIĘ NA wysiłkach UE w zakresie dyplomacji cyfrowej, ZOBOWIĄZUJE się do zwiększenia wydajności i skuteczności zestawu narzędzi dla dyplomacji cyfrowej i OCZEKUJE pogłębionych dyskusji nad ich zakresem i wykorzystywaniem, czerpiących zdoświadczeń z dotychczasowego stosowania tego narzędzia. Dyskusje te powinny przyczynić się do promowania bezpieczeństwa na poziomie międzynarodowym, stymulując dialog i sprzyjając wspólnej wizji zagadnień dotyczących cyberbezpieczeństwa, wzmacniając działania zapobiegawcze, stabilność i współpracę oraz pogłębiając zaufanie i budowanie potencjału, a w stosownych przypadkach stosując środki ograniczające, by przeciwdziałać szkodliwym działaniom w cyberprzestrzeni, które godzą w integralność i bezpieczeństwo UE i jej państw członkowskich, zniechęcać do takich działań, powstrzymywać je i odpowiadać na nie, przyczyniając się w ten sposób do bezpieczeństwa międzynarodowego i stabilności międzynarodowej oraz konsolidując pozycję UE w cyberprzestrzeni w pełnym poszanowaniu krajowych kompetencji i prerogatyw. W szczególności należy zwrócić szczególną uwagę na zapobieganie i przeciwdziałanie cyberatakom wpływającym na całe systemy, mogącym wpłynąć na nasze łańcuchy dostaw, infrastrukturę krytyczną i podstawowe usługi, demokratyczne instytucje i procesy oraz zagrażać naszemu bezpieczeństwu gospodarczemu, co obejmuje m.in. kradzież własności intelektualnej z wykorzystaniem cyberprzestrzeni. Państwa członkowskie i instytucje UE powinny również dalej zastanawiać się nad powiązaniami między unijnymi ramami zarządzania kryzysowego w cyberprzestrzeni, zestawem narzędzi dla dyplomacji cyfrowej a postanowieniami art. 42 ust. 7 TUE i art. 222 TFUE, w tym przez prace oparte na konkretnych scenariuszach, by przyjąć wspólne rozumienie praktycznych rozwiązań zmierzających do wdrożenia postanowień art. 42 ust. 7 TUE.

27. UZNAJE znaczenie wzmocnienia współpracy z organizacjami międzynarodowymi i krajami partnerskimi, by pogłębiać wzajemne zrozumienie pełnego obrazu cyberzagrożeń, rozwijać dialog i mechanizmy współpracy, w stosownych przypadkach określać wspólne reakcje dyplomatyczne, jak również usprawniać wymianę informacji, w tym przez edukację, szkolenia i ćwiczenia. W szczególności PODKREŚLA, że silne partnerstwo transatlantyckie w dziedzinie cyberbezpieczeństwa przyczynia się do naszej wspólnej stabilności oraz wspólnego bezpieczeństwa i dobrobytu, oraz PRZYJMUJE DO WIADOMOŚCI przepisy w sprawie współpracy w dziedzinie cyberbezpieczeństwa zawarte w umowie o handlu i współpracy między Zjednoczonym Królestwem a UE. PRZYPOMINAJĄC kluczowe osiągnięcia współpracy UE-NATO w obszarze cyberbezpieczeństwa w ramach wdrażania wspólnych deklaracji z Warszawy (2016 r,) i Brukseli (2018 r.), ponownie podkreśla znaczenie zwiększonej, wzajemnie się wzmacniającej i korzystnej współpracy przez edukację, szkolenia, ćwiczenia i skoordynowaną reakcję na szkodliwe działania w cyberprzestrzeni, przy pełnym poszanowaniu autonomii procesu decyzyjnego i procedur obu organizacji, w oparciu o zasady przejrzystości, wzajemności i inkluzywności.

28. Aby przyczynić się do powstania globalnej, otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni, która ma coraz większe znaczenie dla stałego dobrobytu, wzrostu, bezpieczeństwa, dobrostanu, łączności i integralności naszych społeczeństw, ZOBOWIĄZUJE się do ciągłego zaangażowania w procesy normotwórcze w organizacjach międzynarodowych, w szczególności w procesy związane z Pierwszym Komitetem Zgromadzenia Ogólnego ONZ, propagujące stosowanie prawa międzynarodowego w cyberprzestrzeni i przestrzeganie norm, przepisów i zasad odpowiedzialnego zachowania państw w cyberprzestrzeni oraz przyczyniające się do uznawania stosowania tych norm, przepisów i zasad, w tym przez promowanie szybkiego ustanowienia Programu działania dotyczącego propagowania odpowiedzialnego zachowania państw w cyberprzestrzeni, jako konstruktywnych, inkluzywnych i opartych na konsensusie działań następczych w odniesieniu do procesów realizowanych na forum ONZ zarówno przez grupę ekspertów rządowych, jak i przez Otwartą Grupę Roboczą.

29. PRZYPOMINA swoje stanowcze zaangażowanie na rzecz skutecznego multilateralizmu i międzynarodowego ładu opartego na zasadach, w którego centrum znajduje się Organizacja Narodów Zjednoczonych, swoje zdecydowane dążenie do wzmocnienia współpracy i koordynacji z organizacjami międzynarodowymi i regionalnymi, a mianowicie systemem ONZ, NATO, Radą Europy, OBWE, OECD, UA, OPA, ASEAN, Forum Regionalnym ASEAN, RWPZ i LPA w odniesieniu do dyskusji dotyczących cyberprzestrzeni, jak również w odniesieniu do kontynuacji i rozszerzenia usystematyzowanego dialogu UE w sprawach cyberprzestrzeni i konsultacji z państwami trzecimi. PODKREŚLA swoje aktywne poparcie dla ONZ, w szczególności w odniesieniu do oenzetowskiej Agendy 2030, w tym celów zrównoważonego rozwoju, i Z ZADOWOLENIEM PRZYJMUJE mapę drogową Sekretarza Generalnego ONZ w sprawie współpracy cyfrowej i agendę Sekretarza Generalnego ONZ w sprawie rozbrojenia, które propagują odpowiedzialność i przestrzeganie norm w cyberprzestrzeni oraz przyczyniają się do przeciwdziałania konfliktom wynikającym ze szkodliwych działań w cyberprzestrzeni oraz do ich pokojowego rozstrzygania. Z ZADOWOLENIEM PRZYJMUJE wniosek, by Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa ustanowił nieformalną unijną sieć dyplomacji cyfrowej w celu pogłębiania zaangażowania i rozwijania wiedzy eksperckiej – zarówno na poziomie UE, jak i jej państw członkowskich – w zakresie międzynarodowych kwestii dotyczących cyberprzestrzeni, tak by wzmocnić skoordynowane działania informacyjne.

30. OCZEKUJE na zapowiadany wniosek w sprawie przeglądu ram polityki UE w zakresie cyberobrony i ZOBOWIĄZUJE się do dołożenia wysiłków, by wzmocnić wymiar cyberbezpieczeństwa i cyberobrony w celu zapewnienia, że zostaną one w pełni włączone w szerszy obszar bezpieczeństwa i obrony, a w szczególności w kontekście prac nad Strategicznym kompasem. UWAŻA, że zapowiadana „wojskowa wizja i strategia dotycząca cyberprzestrzeni jako obszaru operacyjnego” przyczyni się do kontynuowania tych dyskusji. Z ZADOWOLENIEM PRZYJMUJE inicjatywę Europejskiej Agencji Obrony (EDA), by stymulować współpracę między wojskowymi zespołami reagowania na incydenty komputerowe, i WSPIERA wysiłki podejmowane w celu zwiększenia synergii cywilno-wojskowej oraz koordynacji w zakresie cyberobrony i cyberbezpieczeństwa, w tym aspektów dotyczących przestrzeni kosmicznej, między innymi przez specjalne projekty PESCO.

31. Z ZADOWOLENIEM PRZYJMUJE wniosek, by opracować program na rzecz budowania zewnętrznych zdolności cyfrowych UE, wniosek, by stworzyć Radę ds. Budowania Zdolności Cyfrowych UE, a także utworzenie i uruchomienie sieci na rzecz budowania zdolności cyfrowych UE (EU CyberNet) w celu zwiększenia odporności w cyberprzestrzeni i globalnych zdolności. Z ZADOWOLENIEM PRZYJMUJE w tym kontekście współpracę z państwami członkowskimi, jak również z partnerami z sektora prywatnego i publicznego, a mianowicie Globalnym Forum Wiedzy Cyfrowej (GFCE) i innymi odnośnymi podmiotami międzynarodowymi, by zapewnić koordynację i unikać powielania wysiłków. W szczególności ZACHĘCA do współpracy z partnerami na Bałkanach Zachodnich oraz partnerami ze wschodniego i południowego sąsiedztwa UE.

32. Aby zapewnić, by wszystkie kraje mogły czerpać ze społecznych, gospodarczych i politycznych korzyści wiążących się z internetem i stosowaniem technologii, ZOBOWIĄZUJE się do wspierania krajów partnerskich w stawianiu czoła nasilającym się wyzwaniom związanym ze szkodliwymi działaniami w cyberprzestrzeni, a mianowicie działaniami, które szkodzą rozwojowi gospodarek i społeczeństw tych krajów oraz integralności i bezpieczeństwu ustroju demokratycznego, w tym zgodnie z wysiłkami podejmowanymi w ramach Europejskiego planu działania na rzecz demokracji.

33. Aby zagwarantować rozwój, wdrożenie i monitorowanie propozycji przedstawionych w strategii Unii Europejskiej w zakresie cyberbezpieczeństwa, i biorąc pod uwagę wieloletni charakter niektórych inicjatyw, ZACHĘCA Komisję i Wysokiego Przedstawiciela do Spraw Zagranicznych i Polityki Bezpieczeństwa do opracowania szczegółowego planu wdrożenia, w którym ustalone zostaną priorytety i harmonogram planowanych działań. Będzie MONITOROWAĆ postępy we wdrażaniu niniejszych konkluzji za pomocą planu działania, który będzie poddawany regularnym przeglądom i aktualizacjom przez Radę w ścisłej współpracy z Komisją Europejską i Wysokim Przedstawicielem.