

Bruksela, 6 czerwca 2025 r.
(OR. en)

9953/25

TELECOM 180
CYBER 160
COMPET 496
MI 361
PROCIV 66

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	7929/25
Dotyczy:	Konkluzje w sprawie niezawodnej i odpornej łączności – Konkluzje Rady (6 czerwca 2025 r.)

Delegacje otrzymują w załączniku konkluzje Rady w sprawie niezawodnej i odpornej łączności w wersji zatwierdzonej przez Radę ds. Transportu, Telekomunikacji i Energii na jej posiedzeniu w dniu 6 czerwca 2025 r.

Konkluzje Rady w sprawie niezawodnej i odpornej łączności

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC:

- dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej,
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2),
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającą dyrektywę Rady 2008/114/WE,
- wspólny komunikat do Parlamentu Europejskiego i Rady w sprawie aktualizacji strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i jej planu działania „Udoskonalona strategia Unii Europejskiej w zakresie bezpieczeństwa morskiego w obliczu zmieniających się zagrożeń morskich” z dnia 10 marca 2023 r.,
- konkluzje Rady z dnia 24 października 2023 r. w sprawie zaktualizowanej strategii UE w zakresie bezpieczeństwa morskiego (EUMSS) i towarzyszącego jej planu działania,
- sprawozdanie Enrica Letty „Much more than a market – Speed, Security, Solidarity, Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens” [„Znacznie więcej niż rynek. Szybkość, bezpieczeństwo, solidarność – wzmocnienie jednolitego rynku w celu zapewnienia zrównoważonej przyszłości i dobrobytu wszystkim obywatelom UE”] z dnia 17 kwietnia 2024 r.,
- sprawozdanie Maria Draghiego na temat przyszłości europejskiej konkurencyjności z dnia 9 września 2024 r.,
- sprawozdanie Sauliego Niinistö „Safer together – Strengthening Europe’s Civilian and Military Preparedness and Readiness” [„Razem bezpieczniej – zwiększenie gotowości i przygotowania cywilnego i obronnego w Europie”] z dnia 30 października 2024 r.,
- sprawozdanie Zespołu ds. Polityki Spektrum Radiowego „6G Strategic vision” [„6G – wizja strategiczna”] z dnia 12 lutego 2025 r.,
- wspólny komunikat do Parlamentu Europejskiego i Rady „Plan działania UE na rzecz bezpieczeństwa kabli” z dnia 21 lutego 2025 r.,

OPIERAJĄC SIĘ NA:

- białej księdze Komisji z dnia 21 lutego 2024 r. pt. „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?”,
- zaleceniu Komisji z dnia 26 lutego 2024 r. w sprawie bezpiecznej i odpornej infrastruktury kabli podmorskich,
- konkluzjach Rady z dnia 21 maja 2024 r. w sprawie przyszłości unijnej polityki cyfrowej,
- konkluzjach Rady z dnia 6 grudnia 2024 r. w sprawie białej księgi zatytułowanej „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?”,

Ramy ogólne

1. ZAUWAŻA, że unijna infrastruktura łączności stoi w obliczu nowych i niespotykanych dotąd wyzwań wynikających z coraz bardziej złożonej sytuacji geopolitycznej, czego dowodem są skutki rosyjskiej wojny napastniczej przeciwko Ukrainie, a także z rosnącej liczby ataków fizycznych, cyberataków i ataków hybrydowych oraz klęsk żywiołowych spowodowanych zmianą klimatu na świecie. PODKREŚLA, że zagrożenia dla infrastruktury łączności mają daleko idące konsekwencje geopolityczne dla polityki zagranicznej UE, a także dla ogólnego środowiska bezpieczeństwa UE.
2. PRZYZNAJE, że presje te ujawniają słabości sieci naziemnych i nienaziemnych oraz kabli podmorskich; należy zatem przededefiniować strategiczne podejście UE do rozwoju sieci łączności w świetle krytycznej zależności naszego społeczeństwa i gospodarki od łączności elektronicznej i infrastruktury cyfrowej, aby chronić suwerenność cyfrową i dobrobyt gospodarczy UE przy zachowaniu otwartości, ze szczególnym naciskiem na uwzględnienie wiodącej pozycji technologicznej i odporności gospodarczej.
3. PODKREŚLA, że kompleksowe podejście do rozwoju niezawodnej i odpornej infrastruktury sieciowej ma zasadnicze znaczenie dla sprostania nowym wyzwaniom związanym z częstszym występowaniem klęsk żywiołowych, szkodliwych incydentów, cyberataków i zagrożeń geopolitycznych. Podejście to należy uwzględnić i zastosować podczas ewentualnego przeglądu istniejących ram prawnych, bez uszczerbku dla wyłącznej odpowiedzialności państw członkowskich za bezpieczeństwo narodowe.
4. UZNAJE, że znacząca większość międzykontynentalnego ruchu internetowego i część wewnątrzeuropejskiego ruchu internetowego odbywa się za pośrednictwem podmorskich infrastruktur kablowych, które tworzą krytyczną sieć szkieletową i są coraz bardziej zagrożone, o czym świadczą różne incydenty, zwłaszcza na Morzu Bałtyckim. Z ZADOWOLENIEM PRZYJMUJE w tym względzie środki zawarte w zaleceniu Komisji w sprawie bezpiecznej i odpornej infrastruktury kabli podmorskich i ZGADZA SIĘ co do znaczenia, jakie ma wyższy poziom odporności i integracji technicznej wszystkich kanałów komunikacyjnych – naziemnych, nienaziemnych i, co ważne, podmorskich – jako warunek wstępny niezawodnej, odpornej i bezpiecznej komunikacji, jak stwierdzono w białej księdze Komisji pt. „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?”.

5. ODNOTOWUJE wizję sieci połączonych systemów obliczeń zespołowych („sieć 3C”) przedstawioną we wspomnianej wyżej białej księdze Komisji, która ma strategiczne znaczenie dla ochrony i rozwoju suwerenności cyfrowej UE przy zachowaniu otwartości i może zwiększyć europejskie innowacje, wzmacniając jednocześnie ekosystem łączności i zdolności obliczeniowych w celu wsparcia zastosowań opartych na danych i sztucznej inteligencji.

6. PRZYPOMINA, że niezawodna i odporna łączność dzięki technicznemu zintegrowaniu różnych rodzajów sieci i dywersyfikacji stała się jednym z kluczowych priorytetów, wymagającym wielowarstwowych, interoperacyjnych i redundantnych sieci. ZAUWAŻA potrzebę łagodzenia zakłóceń w komunikacji poprzez poprawę fizycznej i geograficznej redundancji sieci, a także dostaw energii na potrzeby infrastruktury łączności dla wszystkich sieci szkieletowych. DOSTRZEGA, jak ważne jest, by infrastruktura była zdywersyfikowana, w szczególności w sytuacjach nadzwyczajnych.

7. WZYWA DO ustanowienia strategicznego podejścia do niezawodnej i odpornej łączności, uwzględniającego obecne i nowe technologie, zwłaszcza sztuczną inteligencję, 6G i komunikację kwantową, ze szczególnym naciskiem na ujednolicenie różnych elementów sieci, takich jak elementy stacjonarne, ruchome i satelitarne (oraz inne elementy nienaziemne), i ich przekształcenie w spójny europejski ekosystem cyfrowy i rynek dla przedsiębiorstw każdej wielkości.

8. ODNOTOWUJE, że to strategiczne podejście powinno uwzględniać konwergencję różnych rodzajów sieci – w tym kabli naziemnych, nienaziemnych i podmorskich – przy jednoczesnym uwzględnieniu różnych modeli biznesowych i obecnych tendencji, wspierając tym samym powszechną i płynną łączność w całej Europie, zwiększając konkurencyjność i wzmacniając jednolity rynek europejski.

9. PODKREŚLA, że konwergencja różnych rodzajów sieci zapewniających dostęp stanowi okazję do tego, by wykorzystać mocne strony poszczególnych technologii i połączyć najlepsze z ich cech, ale należy też dalej koncentrować się na przewyżnianiu wyzwań związanych z cyberbezpieczeństwem.

10. APELUJE O koordynację z trwającymi inicjatywami badawczymi i pilotażowymi w zakresie łączności, takimi jak Wspólne Przedsięwzięcie na rzecz Inteligentnych Sieci i Usług, a także z innymi odpowiednimi projektami infrastruktury w zakresie łączności wspieranymi z funduszy UE, takich jak „Horyzont Europa”, program „Cyfrowa Europa” i instrument „Łącząc Europę” – technologie cyfrowe, obejmującymi kable podmorskie, infrastrukturę łączności szkieletowej, zdolności w zakresie przywracania sprawności operacyjnej i gotowości do pracy dzięki wykorzystaniu zdolności istniejących statków do układania kabli i ich poprawie, a także z wielkoskalowymi projektami pilotażowymi na potrzeby projektów sieci 3C. PODKREŚLA znaczenie potencjalnych programów finansowania, które mogłyby przyczynić się do realizacji strategicznych priorytetów Unii.

11. UZNAJE kluczowe znaczenie współpracy międzynarodowej dla zwiększenia odporności i niezawodności globalnej infrastruktury cyfrowej przy jednoczesnym promowaniu wielostronnego, ukierunkowanego na człowieka i opartego na prawach człowieka podejścia do transformacji cyfrowej. PODKREŚLA potrzebę wspierania krajów kandydujących do UE i innych krajów partnerskich za pośrednictwem istniejących platform i inicjatyw UE, takich jak strategia Global Gateway, oraz w ramach odpowiednich forów międzynarodowych, takich jak ITU, przy zapewnieniu m.in. pomocy technicznej, budowania zdolności i wsparcia finansowego; AKCENTUJE, że równocześnie należy też prowadzić współpracę z krajami partnerskimi na rzecz poszukiwania konwergencji w zakresie podejść politycznych oraz przykładów regulacyjnych i normatywnych, a także promowania europejskich rozwiązań.

Odporność dzięki dywersyfikacji rodzajów sieci i interoperacyjności

12. PODKREŚLA, że niezawodną i odporną łączność można poprawić dzięki dywersyfikacji rodzajów sieci poprzez wykorzystanie wielowarstwowych, interoperacyjnych środków komunikacji naziemnej i nienaziemnej wspieranych przez solidną infrastrukturę szkieletową, a także dzięki ocenom ryzyka i dobrym praktykom w zakresie środków ograniczających ryzyko zgodnie z dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS 2) i dyrektywą w sprawie podmiotów krytycznych (CER).

13. PRZYZNAJE, że szybki rozwój systemów łączności satelitarnej, w tym sieci wielokonstelacyjnych, z których duża część jest eksploatowana i rozwijana przez podmioty spoza UE, wywiera presję na dostęp do orbit Ziemi i do widma. UZNAJE jednocześnie uzupełniające się role systemów łączności satelitarnej i innych zdolności nienaziemnych w zakresie nieprzerwanej dostępności usług łączności, w szczególności dla regionów oddalonych i regionów o niedostatecznym zasięgu sieci, zapewniające krytyczną redundancję i odporność na zakłócenia naziemne, co jest szczególnie ważne w kontekście świadczenia – w każdych okolicznościach – usług w zakresie bezpieczeństwa i pomocy w przypadku klęsk żywiołowych.

14. **PODKREŚLA** strategiczne znaczenie IRIS² – z którą zostanie zintegrowana EuroQCI – w kontekście długoterminowych wyzwań w zakresie ochrony, bezpieczeństwa i odporności łączności satelitarnej. Zwraca uwagę na rolę IRIS², jeśli chodzi o wspieranie istniejącej europejskiej bazy technologicznej i przemysłowej łączności satelitarnej, niwelowanie luk w łączności w całej Unii i zwiększanie niezależności UE od pozaeuropejskich dostawców usług komunikacyjnych – w szczególności usług bezpiecznych – oraz przyczynianie się do wzmacniania suwerenności cyfrowej Unii przy zachowaniu otwartości. **AKCENTUJE** zatem potrzebę terminowego wdrożenia IRIS² – infrastruktury, która uzupełnia i integruje komponent GOVSATCOM programu kosmicznego, zgodnie z międzynarodowymi i krajowymi ramami regulacyjnymi, aby zapewnić odporne usługi komunikacyjne dla użytkowników rządowych i użytkowników komercyjnych.

15. **PODKREŚLA** znaczenie zapewnienia wystarczającego, bezpiecznego, niezawodnego, odpornego i chronionego dostępu do orbity geostacjonarnej, do średniej i niskiej orbity okołozemskiej oraz do możliwości w zakresie widma radiowego, które opierają się na stosowaniu zasad określonych w Regulaminie Radiokomunikacyjnym ITU. **AKCENTUJE**, że aby wszystkim operatorom zagwarantować równe warunki działania, przy ustanawianiu ewentualnych wspólnych wymogów dotyczących konstelacji satelitarnych – także tych zarejestrowanych na podstawie ram regulacyjnych poza UE – mających dostęp do rynków krajowych i unijnych, należy opierać się na wynikach trwających dyskusji w ramach Zespołu ds. Polityki Spektrum Radiowego (RSPG). **DOSTRZEGA** stopniowe zmiany w kierunku konwergencji technologii mobilnych i satelitarnych, w tym niedawne znormalizowanie sieci 5G i rozwój 6G, które zapewniają ciągłą dostępność usług łączności elektronicznej niezależnie od miejsca, a jednocześnie wspierają rozwój europejskich zdolności w zakresie innowacji i konkurencji w UE z korzyścią dla użytkowników końcowych.

16. **UZNAJE PONADTO** transformacyjny potencjał, jaki w kontekście związanych z mobilnością rynków wertykalnych, takich jak sektory transportu, lotnictwa i gospodarki morskiej, mają uzupełniające usługi bezpośredniej łączności satelitarnej między urządzeniami (D2D) wykraczające poza konsumenckie aplikacje na smartfony. **ODNOTOWUJE** kluczową rolę, jaką usługi D2D mogą odegrać w zakresie poprawy usług publicznych, w tym ochrony ludności, przynosząc przy tym dalekosiężne korzyści w wielu dziedzinach. **PRZYZNAJE**, że dalsza konwergencja technologii satelitarnych i mobilnych może stymulować wzrost społeczno-gospodarczy, zwiększać odporność sieci, niwelować nierówności cyfrowe i pomóc w przezwyciężaniu globalnych wyzwań w zakresie łączności. **WZYWA** do włączenia usług D2D do globalnego systemu komunikacji IRIS² na wczesnym etapie, aby wzmocnić konkurencyjność UE.

17. ZWRACA UWAGĘ NA rosnące wyzwanie wynikające z celowego zagłuszania i spoofingu globalnych systemów nawigacji satelitarnej (GNSS), które mają wpływ na wiele rodzajów krytycznej infrastruktury i usług. DOCENIA pracę grupy zadaniowej UE ds. zakłóceń GNSS. WZYWA DO skoordynowanych unijnych wysiłków na rzecz ustanowienia solidnego mechanizmu zarządzania informacjami dotyczącymi zakłóceń GNSS, który będzie zapewniał terminową sprawozdawczość, wymianę danych w granicach krajowych wymogów bezpieczeństwa i kompetencji państw członkowskich, a także skoordynowane środki reagowania we wszystkich państwach członkowskich. PODKREŚLA, że zapewniana przez GNSS dokładna synchronizacja czasowa ma zasadnicze znaczenie dla wielu podmiotów krytycznych i strategicznych sektorów, w tym dla lotnictwa, finansów i łączności elektronicznej, a także sektora energetycznego, transportu i handlu, w związku z czym wszelkie zakłócenia w funkcjonowaniu tych systemów mogą mieć daleko idące konsekwencje gospodarcze i społeczne. WZYWA do podjęcia działań na rzecz zapewnienia rozwiązań alternatywnych dla ciągłości działania zapewnianej przez GNSS.

18. ZAUWAŻA, że inwestycje w zrównoważone technologie, takie jak dostawy energii ze źródeł odnawialnych, magazynowanie energii i inteligentne systemy opomiarowania, przyczyniają się nie tylko do zmniejszenia śladu węglowego, ale również do wzmocnienia odporności infrastruktury łączności, zapewniając niezakłócony dostęp do źródła energii w sytuacjach nadzwyczajnych.

19. WZYWA DO uruchomienia strategicznych inwestycji na rzecz zwiększenia ochrony i odporności infrastruktury cyfrowej, ze szczególnym naciskiem na kable krytyczne dla sieci szkieletowych, w celu ochrony kluczowych interesów strategicznych UE w Oceanie Atlantyckim oraz na Morzu Bałtyckim, Morzu Czarnym, Morzu Śródziemnym i Morzu Północnym, w regionie Arktyki, a także w regionach najbardziej oddalonych. PODKREŚLA pilną potrzebę kompleksowego wsparcia infrastruktury kabli podmorskich, na co zwrócono uwagę w planie działania UE na rzecz bezpieczeństwa kabli, w tym zapobiegania zagrożeniom, wykrywania ryzyka, szybkiego reagowania na incydenty, odstraszania, a także zdolności w zakresie przywracania sprawności operacyjnej i gotowości do pracy dzięki wykorzystaniu zdolności istniejących statków do układania kabli i ich poprawie, w oparciu o prace nieformalnej grupy ekspertów ds. infrastruktury kabli podmorskich, we współpracy z Grupą ds. Odporności Podmiotów Krytycznych (CER) i grupą współpracy NIS. AKCENTUJE znaczenie zwiększenia zdolności w celu przywrócenia sprawności operacyjnej po niezamierzonych incydentach lub sabotażu. UWYPUKLA potrzebę zapewnienia redundancji w odniesieniu do transgranicznych połączeń światłowodowych i infrastruktury kabli podmorskich w Europie na potrzeby globalnej łączności. PODKREŚLA potrzebę ścisłej współpracy z państwami członkowskimi zgodnie z obowiązującymi zasadami wdrażania środków przewidzianych w planie działania UE.

20. DOCENIA bieżące inicjatywy na rzecz wspierania odporności, takie jak inicjatywy prowadzone w ramach zalecenia Rady 2023/C 20/01 w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej oraz sprawozdania na temat cyberbezpieczeństwa i odporności europejskiej infrastruktury i sieci łączności przedstawionego przez grupę współpracy NIS w ramach działań następczych w związku z wezwaniem z Nevers z dnia 9 marca 2022 r.

21. PODKREŚLA kluczowe znaczenie cyberbezpieczeństwa dla rozwoju niezawodnej i odpornej infrastruktury łączności, a także bezpieczeństwa, które zmniejsza ryzyko współzależności technologicznych i handlowych. UZNAJE znaczenie ocen ryzyka w kontekście zmniejszenia zagrożeń dla bezpieczeństwa i zależności, a także korzystania z zaufanych dostawców przy uruchamianiu sieci łączności. PODKREŚLA znaczenie transpozycji i wdrożenia dyrektywy NIS 2 i dyrektywy CER w celu zapewnienia ochrony infrastruktury cyfrowej i podstawowych usług. AKCENTUJE potrzebę łagodzenia ryzyka związanego z bezpieczeństwem łańcucha dostaw w odniesieniu do wszystkich rodzajów sieci i systemów informatycznych oraz potrzebę szybkiego przyjęcia zestawu środków mających na celu ograniczenie krytycznego ryzyka w łańcuchu dostaw ICT. W tym kontekście APELUJE o przyspieszenie pełnego wdrożenia zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, a także środków w zakresie bezpieczeństwa łańcucha dostaw zgodnie z dyrektywą NIS 2 i dyrektywą CER, w szczególności skoordynowanej na szczeblu Unii oceny ryzyka dla bezpieczeństwa wyżej wymienionych krytycznych łańcuchów dostaw i ZACHEĆCA do dyskusji na temat bardziej zharmonizowanego podejścia do nowych zagrożeń dla cyberbezpieczeństwa w łączności elektronicznej.

22. UZNAJE strategiczne znaczenie rozwoju europejskich, zintegrowanych pod względem technicznym i odpornych sieci łączności, które będą zapewniały powszechny zasięg i maksymalizowały odporność swoich poszczególnych elementów poprzez dywersyfikację rodzajów sieci i redundancję. PODKREŚLA, że przy rozwoju takich sieci należy uwzględniać specyfikę państw członkowskich i kierować się dynamiką rynku, której towarzyszy ukierunkowane wsparcie UE, w tym poprzez wytyczne i finansowanie strategicznych projektów w zakresie łączności.

Jednolity rynek na rzecz niezawodnej i odpornej łączności

23. PRZYZNAJE, że niezawodna i odporna infrastruktura łączności stanowi kręgosłup i jeden z podstawowych elementów jednolitego rynku, który jest jednym z głównych czynników napędzających konkurencyjność i innowacje UE i stawia Unię na pozycji światowego lidera w gospodarce cyfrowej oraz wzmacnia jej suwerenność cyfrową przy zachowaniu otwartości.

24. PODKREŚLA, że jednolity rynek łączności elektronicznej należy w miarę potrzeby pogłębić poprzez dalszą harmonizację i poprawę łączności transgranicznej, przy jednoczesnym uznaniu różnych modeli biznesowych usługodawców, uwarunkowań regionalnych i krajowych kompetencji państw członkowskich w zakresie stosowania zharmonizowanych przepisów. ZAZNACZA, że usprawnienie jednolitego rynku łączności elektronicznej wzmocni konkurencyjność i suwerenność cyfrową Unii przy zachowaniu otwartości, a także przyczyni się do powszechnego występowania niezawodnych i odpornych sieci z korzyścią dla obywateli i przedsiębiorstw UE.

25. ZAUWAŻA, że wspieranie zintegrowanych pod względem technicznym i odpornych europejskich sieci łączności może otworzyć nowe możliwości rynkowe w sektorze łączności elektronicznej, a także horyzontalnie w gospodarce cyfrowej, zwiększając globalną konkurencyjność Unii poprzez stymulowanie innowacji technologicznych.

26. PODKREŚLA, że widmo radiowe odgrywa kluczową rolę z korzyścią dla jednolitego rynku, gospodarki UE i całego społeczeństwa. ZAZNACZA, że efektywne i skoordynowane korzystanie z widma radiowego wspiera politykę UE, a jednocześnie maksymalizuje wartość społeczną i służy osiągnięciu celu, jakim jest udoskonalenie jednolitego rynku. ZACHĘCA do oceny potrzeb w zakresie widma, w tym zakresów pasma jako odpowiednich kandydatów do wprowadzenia 6G, w oparciu o wymogi dotyczące zasięgu i przepustowości w odniesieniu do zastosowań sieci naziemnych i nienaziemnych.

27. UZNAJE udany europejski model stopniowej harmonizacji widma oraz rolę ITU w zarządzaniu widmem radiowym. APELUJE do Komisji, by wzmocniła na szczeblu UE mechanizm wsparcia dla państw członkowskich, który zapewni konstruktywne ramy umożliwiające państwom członkowskim reagowanie na przypadki transgranicznych ingerencji w UE i w państwach trzecich, bez ograniczania się do kwestii czysto technicznych.

28. ZACHECA do wdrażania i dalszego rozwoju dostosowanych do przyszłych wyzwań, bezpiecznych i wiarygodnych norm jako podstawy rozwoju technologicznego, utrzymania suwerenności cyfrowej UE przy zachowaniu otwartości oraz stymulowania innowacji i spójności unijnego sektora łączności elektronicznej. ZACHECA Komisję Europejską, Europejską Służbę Działań Zewnętrznych i państwa członkowskie do wzmocnienia podejścia „Drużyna Europy” na forach międzynarodowych poprzez aktywny udział w globalnych procesach ustanawiania norm, promowanie opracowanych na szczeblu europejskim norm opartych na podstawowych wartościach podzielanych przez UE, takich jak prawa człowieka, oraz zapewnienie skoordynowanej europejskiej strategii na rzecz infrastruktury cyfrowej, która będzie obejmowała wszystkie warstwy komunikacji.

29. APELUJE O wyższy poziom odporności poprzez dywersyfikację oraz płynną i powszechną łączność dzięki dalszemu rozwojowi technicznie zintegrowanych i odpornych europejskich sieci łączności w ramach wielowarstwowego podejścia obejmującego między innymi: działania normalizacyjne, ewentualne ukierunkowane instrumenty finansowe wspierające rozwój takich sieci oraz wytyczne ułatwiające wdrażanie na zasadach rynkowych.

30. ZWRACA SIĘ do Komisji, by złożyła Radzie sprawozdanie na temat istotnych zmian w zakresie zintegrowanych technicznie i odpornych europejskich sieci łączności. Powinno się to przyczynić do wymiany informacji i monitorowania postępów w osiągnięciu płynnej i powszechnej łączności.

31. ZWRACA SIĘ do Komisji, by wykorzystwała prace nieformalnej grupy ekspertów ds. infrastruktury kabli podmorskich w ramach strategicznego podejścia politycznego ustanowionego w zaleceniu w sprawie bezpiecznej i odpornej infrastruktury kabli podmorskich oraz w planie działania UE na rzecz bezpieczeństwa kabli podmorskich, a także rozważyła konkretne propozycje dalszego promowania niezawodności i odporności tej infrastruktury jako jednej z kluczowych części europejskich sieci łączności w oparciu o prace Grupy ds. Odporności Podmiotów Krytycznych (CER) i grupy współpracy NIS oraz nieformalnej grupy ekspertów ds. infrastruktury kabli podmorskich, przypominając jednocześnie, że bezpieczeństwo narodowe leży wyłącznie w gestii państw członkowskich.

32. UZNAJE, że ciągła i niezakłócona łączność ma zasadnicze znaczenie dla bezpiecznej i prawidłowo funkcjonującej Unii. ODNOTOWUJE częstsze klęski żywiołowe i inne zagrożenia, które sprawiają, że pilnym wyzwaniem staje się redundancja dostaw energii elektrycznej dla sieci. WZYWA Komisję, by przeanalizowała i zaproponowała odpowiednie środki, w tym wsparcie finansowe, bez przesądzania o wyniku negocjacji w sprawie kolejnych wieloletnich ram finansowych.

33. WZYWA Komisję do oceny możliwości przygotowania skoordynowanej inicjatywy na rzecz planowania i rozwoju niezawodnej i odpornej sieci infrastruktur i zdolności cyfrowych, obejmującej naziemne, podmorskie i satelitarne sieci szkieletowe, w całej Unii i z międzynarodowymi krajami partnerskimi, na przykład poprzez wykorzystanie ram sieci transeuropejskich i ustanowienie instrumentu TEN-D (transeuropejskie sieci cyfrowe). Z ZADOWOLENIEM PRZYJMUJE podejście Komisji do inicjatywy na rzecz łączności w Arktyce, a także bieżące wysiłki na rzecz wzmocnienia odporności infrastruktury cyfrowej w morskich regionach UE. PODKREŚLA, że przy ocenie projektów kablowych o znaczeniu europejskim należy określić i stosować jasne, zintegrowane i konkretne kryteria, z uwzględnieniem zalecenia (UE) 2024/779, służące poprawie bezpieczeństwa i odporności oraz promować partnerstwa międzynarodowe.

34. ZOBOWIĄZUJE SIĘ do stałego monitorowania i dostosowywania strategicznego podejścia UE do infrastruktury łączności w celu sprostania nowym wyzwaniom technologicznym, geopolitycznym i środowiskowym, przy zapewnieniu niezawodnej i odpornej łączności w całej Unii.
