

V Bruseli 6. júna 2025
(OR. en)

9953/25

TELECOM 180
CYBER 160
COMPET 496
MI 361
PROCIV 66

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Komu:	Delegácie
Č. predch. dok.:	7929/25
Predmet:	Závery o spoľahlivej a odolnej konektivite – závery Rady (6. júna 2025)

Delegáciám v prílohe zasielame závery Rady o spoľahlivej a odolnej konektivite, ktoré schválila Rada pre dopravu, telekomunikácie a energetiku na zasadnutí 6. júna 2025.

Závery Rady o spoľahlivej a odolnej konektivite

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNAJÚC:

- smernicu Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií,
- smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2),
- smernicu Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES,
- spoločné oznámenie Európskemu parlamentu a Rade o aktualizácii stratégie námornej bezpečnosti EÚ a jej akčného plánu „Posilnená stratégia námornej bezpečnosti EÚ pre vyvíjajúce sa námorné hrozby“ z 10. marca 2023,
- závery Rady z 24. októbra 2023 o revidovanej stratégii námornej bezpečnosti EÚ (EUMSS) a jej akčnom pláne
- Lettovu správu „Oveľa viac než len trh – rýchlosť, bezpečnosť, solidarita. Posilnenie jednotného trhu s cieľom zabezpečiť udržateľnú budúcnosť a prosperitu pre všetkých občanov EÚ“ zo 17. apríla 2024,
- Draghiho správu „Budúcnosť európskej konkurencieschopnosti“ z 9. septembra 2024,
- Niinistöovu správu „Spoločne bezpečnejšie: posilnenie civilnej a vojenskej pripravenosti a pohotovosti“ z 30. októbra 2024,
- správu skupiny pre politiku rádiového frekvenčného spektra „Strategická vízia 6G“ z 12. februára 2025,
- spoločné oznámenie Európskemu parlamentu a Rade „Akčný plán EÚ na zaistenie bezpečnosti káblov“ z 21. februára 2025,

NADVÄZUJÚC NA:

- bielu knihu Komisie z 21. februára 2024 s názvom „Ako splniť potreby digitálnej infraštruktúry v Európe?“,
- odporúčanie Komisie z 26. februára 2024 o bezpečných a odolných podmorských káblových infraštruktúrach,
- závery Rady z 21. mája 2024 s názvom „Budúcnosť digitálnej politiky EÚ“,
- závery Rady zo 6. decembra 2024 o bielej knihe Komisie s názvom „Ako splniť potreby digitálnej infraštruktúry v Európe?“,

Všeobecný rámec

1. KONŠTATUJE, že infraštruktúra konektivity EÚ čelí novým a bezprecedentným výzvam vyplývajúcim z čoraz zložitejšej geopolitickej situácie, o čom svedčí vplyv útočnej vojny Ruska proti Ukrajine, ako aj rastúci počet fyzických, kybernetických a hybridných útokov a výskyt prírodných katastrof v dôsledku globálnej zmeny klímy. ZDÔRAZŇUJE, že hrozby pre infraštruktúru konektivity majú ďalekosiahle geopolitické dôsledky na zahraničnú politiku EÚ, ako aj na celkové bezpečnostné prostredie EÚ.
2. UZNÁVA, že tieto tlaky odhaľujú zraniteľnosť pozemných a iných ako pozemných sietí a podmorských káblov, čo si vyžaduje nové vymedzenie strategického prístupu EÚ k rozvoju komunikačných sietí vzhľadom na kritickú závislosť našej spoločnosti a hospodárstva od elektronických komunikácií a digitálnej infraštruktúry s cieľom otvorene chrániť digitálnu suverenitu a hospodársku prosperitu EÚ s osobitným dôrazom na vedúce postavenie v oblasti technológií a hospodársku odolnosť.
3. ZDÔRAZŇUJE, že na riešenie nových výziev súvisiacich s častejšími prírodnými katastrofami, škodlivými incidentmi, kybernetickými útokmi a geopolitickými hrozbami je nevyhnutný komplexný prístup k rozvoju spoľahlivej a odolnej sieťovej infraštruktúry. Tento prístup by sa mal zohľadniť a začleniť do možnej revízie existujúceho právneho rámca bez toho, aby bola dotknutá výlučná zodpovednosť členských štátov za národnú bezpečnosť.
4. UZNÁVA, že veľká väčšina medzikontinentálnej a časti vnútroeurópskej internetovej prevádzky prechádza cez podmorské káblivé infraštruktúry, ktoré tvoria kritickú chrbticovú sieť a sú čoraz viac ohrozené, o čom svedčia rôzne incidenty, najmä v Baltskom mori. V tejto súvislosti VÍTA opatrenia uvedené v odporúčaní Komisie o „bezpečných a odolných podmorských káblivých infraštruktúrach“ a SÚHLASÍ s tým, že je dôležité zabezpečiť vyššiu úroveň odolnosti a technickej integrácie všetkých komunikačných kanálov – pozemných, iných ako pozemných, a najmä podmorských – ako predpoklad spoľahlivej, odolnej a bezpečnej komunikácie, ako sa uvádza v bielej knihe Komisie s názvom „Ako zvládnuť potreby digitálnej infraštruktúry Európy?“.

5. BERIE NA VEDOMIE víziu prepojenej siete spolupráce (ďalej len „siet’ 3C“) stanovenú v uvedenej bielej knihe Komisie, ktorá má strategický význam pre ochranu a presadzovanie digitálnej suverenity EÚ otvoreným spôsobom a môže posilniť európske inovácie a zároveň posilniť ekosystém konektivity a výpočtovú kapacitu na podporu údajov a aplikácií založených na umelej inteligencii.

6. PRIPOMÍNA, že spoľahlivá a odolná konektivita prostredníctvom technickej integrácie rôznych typov sietí a diverzifikácie sa stala jednou z kľúčových priorít, čo si vyžaduje viacvrstvové, interoperabilné a redundantné siete. KONŠTATUJE, že je potrebné zmierniť narušenia komunikácie zlepšením fyzickej a geografickej redundancie sietí, ako aj dodávok energie pre infraštruktúru konektivity pre všetky chrbticové siete. UZNÁVA význam diverzifikácie infraštruktúry, najmä v núdzových situáciách.

7. VYZÝVA NA vytvorenie strategického prístupu pre spoľahlivú a odolnú konektivitu, v ktorom sa zohľadnia súčasné a vznikajúce technológie, najmä umelá inteligencia, 6G a kvantová komunikácia so zameraním na konvergenciu rôznych sieťových prvkov, ako sú pevné, mobilné a satelitné (a iné než pozemné prvky), do súdržného európskeho digitálneho ekosystému a trhu pre spoločnosti všetkých veľkostí.

8. POZNAMENÁVA, že v tomto strategickom prístupe by sa mala zohľadniť konvergencia rôznych typov sietí vrátane pozemných, iných ako pozemných a podmorských káblov, pričom by sa mali posúdiť rôzne obchodné modely a súčasné trendy, čím by sa podporila všadeprítomná a plynulá konektivita v celej Európe, zvýšila konkurencieschopnosť a posilnil európsky jednotný trh.

9. ZDÔRAZŇUJE, že konvergencia rôznych typov sietí poskytujúcich prístup predstavuje príležitosť využiť silné stránky rôznych technológií a kombinovať ich najlepšie charakteristiky, ale kľúčovým zameraním by malo zostať aj riešenie výziev v oblasti kybernetickej bezpečnosti.

10. VYZÝVA NA koordináciu s prebiehajúcimi výskumnými a pilotnými iniciatívami v oblasti konektivity, ako je spoločný podnik pre inteligentné siete a služby, ako aj s ďalšími relevantnými projektmi infraštruktúry konektivity podporovanými z fondov EÚ, ako sú Horizont Európa, Digitálna Európa a Nástroj na prepájanie Európy (CEF2 Digital), vrátane podmorských káblov, infraštruktúr chrbticovej konektivity, kapacít obnovy a opravy prostredníctvom využitia existujúcich kapacít káblových plavidiel a ich zlepšenia, ako aj s rozsiahlymi pilotnými projektmi pre projekty siete 3C. ZDÔRAZŇUJE význam možných programov financovania, ktoré by mohli prispieť k strategickým prioritám Únie.

11. UZNÁVA kľúčový význam medzinárodnej spolupráce pri zvyšovaní odolnosti a spoľahlivosti globálnej digitálnej infraštruktúry a zároveň pri podpore prístupu k digitálnej transformácii, ktorý je zameraný na človeka a založený na ľudských právach a zahŕňa viaceré zainteresované strany. ZDÔRAZŇUJE, že je potrebné podporovať kandidátske krajiny EÚ a iné partnerské krajiny prostredníctvom existujúcich platforiem a iniciatív EÚ, ako je Global Gateway, a v rámci príslušných medzinárodných fór, ako je ITU, poskytovať okrem iného technickú pomoc, budovanie kapacít a finančnú podporu a zároveň spolupracovať s partnerskými krajinami s cieľom hľadať konvergenciu, pokiaľ ide o politické prístupy a regulačné a normatívne príklady, a podporovať európske riešenia.

Odolnosť podľa typu siete – diverzifikácia a interoperabilita

12. ZDÔRAZŇUJE, že spoľahlivú a odolnú konektivitu možno zlepšiť diverzifikáciou typov siete spoliehaním sa na viacvrstvové, interoperabilné pozemné a iné ako pozemné komunikačné prostriedky podporované spoľahlivou chrbticovou infraštruktúrou, ako aj posúdeniami rizík a osvedčenými postupmi týkajúcimi sa zmierňujúcich opatrení v súlade so smernicou o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2) a smernicou o odolnosti kritických subjektov (CER).

13. UZNÁVA, že rýchly rozvoj systémov satelitnej komunikácie vrátane multikonštelračných sietí, z ktorých veľký počet prevádzkujú a vyvíjajú subjekty mimo EÚ, vytvára tlak na prístup k obežným dráham a spektru Zeme. Zároveň UZNÁVA komplementárne úlohy systémov satelitnej komunikácie a iných než pozemných spôsobilostí pre nepretržitú dostupnosť komunikačných služieb, najmä vo vzdialených regiónoch a regiónoch s nedostatočnou dostupnosťou služieb, ktoré zabezpečujú kritickú redundanciu a odolnosť voči pozemným narušeniam, ktoré sú za všetkých okolností mimoriadne dôležité pre poskytovanie služieb v oblasti bezpečnosti a zmierňovania následkov katastrof.

14. ZDÔRAZŇUJE strategický význam IRIS², ktorý bude integrovať EURO QCI, pre riešenie dlhodobých výziev v oblasti bezpečnosti, ochrany a odolnosti satelitnej komunikácie.

ZDÔRAZŇUJE úlohu IRIS² pri podpore existujúcej európskej technologickej a priemyselnej základne satelitnej komunikácie, preklenutí medzier v konektivite v celej Únii a zlepšovaní nezávislosti EÚ od mimoeurópskych poskytovateľov komunikačných služieb, najmä bezpečných, a prispieva k otvorenému posilneniu digitálnej suverenity Únie. ZDÔRAZŇUJE preto potrebu včasného zavedenia IRIS², ktorým sa doplní a začlení zložka vesmírneho programu GOVSATCOM v súlade s medzinárodnými a vnútroštátnymi regulačnými rámcami s cieľom poskytovať odolné komunikačné služby pre vládnych a komerčných používateľov.

15. ZDÔRAZŇUJE, že je dôležité zabezpečiť dostatočný, bezpečný, spoľahlivý, odolný a zabezpečený prístup ku geostacionárnym, stredným a nízkym obežným dráham Zeme a ku kapacitám rádiového frekvenčného spektra, ktoré závisia od uplatňovania pravidiel vymedzených v Rádiokomunikačnom poriadku ITU. ZDÔRAZŇUJE, že s cieľom zaručiť rovnaké podmienky pre všetkých prevádzkovateľov by stanovenie možných spoločných požiadaviek na satelitné konštelácie vstupujúce na vnútroštátne trhy a trhy EÚ vrátane tých, ktoré sú registrované v regulačných rámcoch mimo EÚ, malo vychádzať z výsledkov prebiehajúcej diskusie v rámci skupiny pre politiku rádiového spektra (RSPG). UZNÁVA prebiehajúci vývoj smerom ku konvergencii mobilných a satelitných technológií vrátane nedávnej normalizácie 5G a vývoja 6G, ktorý zabezpečuje plynulú dostupnosť služieb elektronickej komunikácie bez ohľadu na miesto a zároveň podporuje rozvoj európskych inovačných kapacít a hospodársku súťaž v EÚ v prospech koncových používateľov.

16. ĎALEJ UZNÁVA transformačný potenciál doplnkových satelitných služieb priamo na zariadenie (D2D), ktoré presahujú rámec aplikácií pre smartfóny pre spotrebiteľov, s cieľom riešiť vertikálne trhy súvisiace s mobilitou, ako sú dopravné, letecké a námorné odvetvia. BERIE NA VEDOMIE kľúčovú úlohu, ktorú môžu zohrávať služby D2D pri zlepšovaní verejných služieb vrátane civilnej ochrany s ďalekosiahlymi prínosmi vo viacerých oblastiach. UZNÁVA, že ďalšia konvergencia satelitných a mobilných technológií má potenciál stimulovať sociálno-ekonomický rast, zlepšiť odolnosť sietí, preklenúť digitálnu priepasť a riešiť globálne výzvy v oblasti konektivity. VYZÝVA na včasné začlenenie služieb D2D do globálneho komunikačného systému IRIS² s cieľom posilniť konkurencieschopnosť EÚ.

17. ZDÔRAZŇUJE rastúcu výzvu vyplývajúcu z úmyselného elektronického rušenia a „spoofingu“ globálnych navigačných satelitných systémov (GNSS), ktoré majú vplyv na širokú škálu kritickej infraštruktúry a služieb. UZNÁVA prácu osobitnej skupiny EÚ pre zasahovanie do GNSS. VYZÝVA NA koordinované úsilie EÚ o vytvorenie spoľahlivého mechanizmu na riadenie informácií súvisiacich s narušeniami GNSS, čím sa zabezpečí včasné podávanie správ, zdieľanie údajov v rámci požiadaviek na národnú bezpečnosť a právomocí členských štátov, ako aj koordinované opatrenia reakcie vo všetkých členských štátoch. ZDÔRAZŇUJE, že presná časová synchronizácia, ktorú poskytuje GNSS, je nevyhnutná pre mnohé kritické subjekty a strategické odvetvia vrátane letectva, financií a elektronických komunikácií, ako aj energetiky, dopravy a obchodu, a preto môže mať akýkoľvek druh narušenia týchto systémov ďalekosiahle hospodárske a spoločenské dôsledky. VYZÝVA na prijatie opatrení na zabezpečenie alternatívnych riešení k nepretržitej funkcionalite, ktorú poskytuje GNSS.

18. KONŠTATUJE, že investície do udržateľných technológií, ako sú dodávky energie z obnoviteľných zdrojov, uskladňovanie energie a inteligentné meranie, prispievajú nielen k zníženiu uhlíkovej stopy, ale aj k posilneniu odolnosti infraštruktúry konektivity, čím sa zabezpečuje nepretržitý prístup k zdroju energie v čase núdze.

19. VYZÝVA NA mobilizáciu strategických investícií na posilnenie ochrany a odolnosti digitálnej infraštruktúry s osobitným zameraním na kritické káble pre chrbticové siete, na ochranu životne dôležitých strategických záujmov EÚ v Atlantickom oceáne a Baltskom, Čiernom, Stredozemnom a Severnom mori, arktickom regióne, ako aj v najvzdialenejších regiónoch. ZDÔRAZŇUJE naliehavú potrebu komplexnej podpory podmorskej káblovej infraštruktúry, ako sa uvádza v Akčnom pláne EÚ na zaistenie bezpečnosti káblov, vrátane predchádzania hrozbám, odhaľovania rizík, rýchlej reakcie na incidenty, odrádzania, ako aj kapacít obnovy a opravy prostredníctvom využitia existujúcich kapacít káblových plavidiel a ich zlepšenia, a to na základe práce neformálnej expertnej skupiny pre podmorskú káblOVú infraštruktúru v koordinácii so skupinou pre odolnosť kritických subjektov (CER) a skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti. PODČIARKUJE význam zvýšených spôsobilostí s cieľom zotaviť sa z nezamýšľaných incidentov alebo sabotáže. ZDÔRAZŇUJE potrebu zabezpečiť redundanciu cezhraničných pozemných optických prepojení a podmorských káblOVých infraštruktúr v Európe pre globálnu prepojenosť. ZDÔRAZŇUJE, že je potrebné úzko spolupracovať s členskými štátmi v súlade s existujúcimi pravidlami vykonávania opatrení akčného plánu EÚ.

20. BERIE NA VEDOMIE prebiehajúce iniciatívy na podporu odolnosti, napríklad v rámci odporúčania Rady 2023/C 20/01 o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry a správy skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti o kybernetickej bezpečnosti a odolnosti európskych komunikačných infraštruktúr a sietí v nadväznosti na výzvu z Nevers z 9. marca 2022.

21. ZDÔRAZŇUJE kľúčový význam kybernetickej bezpečnosti pri rozvoji spoľahlivej a odolnej infraštruktúry konektivity, ako aj bezpečnosti, ktorá znižuje riziká vzájomnej technologickej a obchodnej závislosti. UZNÁVA význam posudzovania rizík s cieľom znížiť bezpečnostné riziká a závislosti, ako aj využívanie dôveryhodných dodávateľov pri zavádzaní komunikačných sietí. PODČIARKUJE význam transpozície a vykonávania smerníc NIS 2 a CER s cieľom zabezpečiť bezpečnosť digitálnych infraštruktúr a základných služieb. ZDÔRAZŇUJE, že je potrebné zmierniť riziká spojené s bezpečnosťou dodávateľského reťazca pre všetky typy sietí a informačných systémov a že je potrebné urýchlene prijať súbor opatrení na zníženie kritických rizík v dodávateľskom reťazci IKT. V tejto súvislosti VYZÝVA na urýchlenie úplného vykonávania súboru nástrojov kybernetickej bezpečnosti 5G, ako aj opatrení týkajúcich sa bezpečnosti dodávateľského reťazca v súlade so smernicou NIS 2 a smernicou CER, najmä koordinovaného posúdenia bezpečnostných rizík uvedených kritických dodávateľských reťazcov na úrovni Únie, a NABÁDA na diskusie o harmonizovanejšom prístupe k riešeniu vznikajúcich kybernetickobezpečnostných hrozieb v elektronických komunikáciách.

22. UZNÁVA strategický význam rozvoja európskych technicky integrovaných odolných komunikačných sietí, ktoré zabezpečia všadeprítomné pokrytie a budú maximalizovať odolnosť ich rôznych prvkov prostredníctvom diverzifikácie typu siete a redundancie. ZDÔRAZŇUJE, že rozvoj takýchto sietí by mal zohľadňovať osobitosti členských štátov a mal by sa riadiť dynamikou trhu sprevádzanou cieľenou podporou EÚ, a to aj prostredníctvom usmernení a financovania strategických projektov v oblasti konektivity.

Jednotný trh pre spoľahlivú a odolnú konektivitu

23. UZNÁVA, že spoľahlivá a odolná infraštruktúra konektivity je chrbtovou kosťou a základným stavebným prvkom jednotného trhu, ktorý je hlavnou hnacou silou konkurencieschopnosti a inovácií EÚ, pričom Únia je svetovým lídrom v digitálnom hospodárstve, čím sa otvoreným spôsobom posilňuje jej digitálna suverenita.

24. PODČIARKUJE, že jednotný trh s elektronickými komunikáciami by sa mal v prípade potreby prehĺbiť prostredníctvom ďalšej harmonizácie a zlepšenia cezhraničnej konektivity, pričom by sa mali uznať rôzne obchodné modely poskytovateľov služieb, regionálne okolnosti a vnútroštátne právomoci členských štátov pri uplatňovaní harmonizovaných pravidiel. ZDÔRAZŇUJE, že zlepšenia jednotného trhu s elektronickými komunikáciami otvorene posilnia konkurencieschopnosť a digitálnu suverenitu Únie a prispievajú k všadeprítomnému pokrytiu spoľahlivými a odolnými sieťami v prospech občanov a podnikov EÚ.

25. KONŠTATUJE, že podpora technicky integrovaných a odolných európskych komunikačných sietí môže otvoriť nové trhové možnosti v odvetví elektronických komunikácií, ako aj horizontálne v digitálnom hospodárstve, čím sa posilní globálna konkurencieschopnosť Únie stimulovaním technologických inovácií.

26. ZDÔRAZŇUJE, že rádiové frekvenčné spektrum zohráva kľúčovú úlohu v prospech jednotného trhu, hospodárstva EÚ a spoločnosti ako celku. ZDÔRAZŇUJE, že efektívne a koordinované využívanie rádiového frekvenčného spektra podporuje politiky EÚ a zároveň maximalizuje spoločenskú hodnotu a slúži na dosiahnutie cieľa zlepšenia jednotného trhu. PODPORUJE posúdenie potrieb frekvenčného spektra vrátane pásiem ako vhodných kandidátov na zavádzanie 6G na základe požiadaviek na pokrytie a kapacitu v prípadoch využívania pozemných a iných ako pozemných sietí.

27. UZNÁVA úspešný európsky model postupnej harmonizácie frekvenčného spektra a úlohu ITU pri správe rádiového frekvenčného spektra. VYZÝVA Komisiu, aby posilnila podporný mechanizmus na úrovni EÚ pre členské štáty, ktorý poskytne konštruktívny rámec umožňujúci členským štátom reagovať na prípady cezhraničného zasahovania v rámci EÚ a s tretími krajinami, a to nielen pri čisto technických otázkach.

28. NABÁDA na zavádzanie a ďalší rozvoj nadčasových, bezpečných a dôveryhodných noriem ako základu pre technologický vývoj, zachovanie digitálnej suverenity EÚ otvoreným spôsobom a podporu inovácií a súdržnosti sektora elektronických komunikácií EÚ. VYZÝVA Európsku komisiu, Európsku službu pre vonkajšiu činnosť a členské štáty, aby posilnili prístup Tímu Európa na medzinárodných fórach aktívnou účasťou na globálnych procesoch stanovovania noriem, podporou európskych noriem založených na základných hodnotách spoločných pre EÚ, ako sú ľudské práva, a zabezpečením koordinovanej európskej stratégie digitálnej infraštruktúry, ktorá zahŕňa všetky komunikačné vrstvy.

29. VYZÝVA NA vyššiu úroveň odolnosti diverzifikáciou a bezproblémovou, všadeprítomnou konektivitou prostredníctvom ďalšieho rozvoja technicky integrovaných a odolných európskych komunikačných sietí v rámci viacvrstvového prístupu, ktorý okrem iného zahŕňa: normalizačné činnosti, možné ciele finančné nástroje na podporu rozvoja takýchto sietí a usmernenia uľahčujúce trhové zavádzanie.

30. VYZÝVA Komisiu, aby Rade podala správu o významnom vývoji, pokiaľ ide o technicky integrované a odolné európske komunikačné siete. To by malo prispieť k výmene informácií a monitorovaniu pokroku pri dosahovaní plynulej a všadeprítomnej konektivity.

31. VYZÝVA Komisiu, aby nadviazala na prácu neformálnej expertnej skupiny pre podmorskú káblovú infraštruktúru v rámci strategického politického prístupu stanoveného v odporúčaní o bezpečných a odolných podmorských káblových infraštruktúrach, ako aj v Akčnom pláne EÚ na zaistenie bezpečnosti káblov a zvažila konkrétne návrhy na ďalšiu podporu spoľahlivosti a odolnosti týchto infraštruktúr ako kľúčovej súčasti európskych komunikačných sietí založených na práci skupiny pre odolnosť kritických subjektov (CER) a skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a neformálnej expertnej skupiny pre infraštruktúru podmorských káblov, pričom pripomína, že národná bezpečnosť je vo výlučnej zodpovednosti členských štátov.

32. UZNÁVA, že nepretržitá a neprerušovaná konektivita je nevyhnutná pre bezpečnú a riadne fungujúcu Úniu. BERIE NA VEDOMIE častejšie prírodné katastrofy a iné hrozby, v dôsledku ktorých je redundancia dodávok energie pre siete naliehavou výzvou. VYZÝVA Komisiu, aby analyzovala a navrhla vhodné opatrenia vrátane finančnej podpory bez toho, aby boli dotknuté rokovania o budúcom viacročnom finančnom rámci.

33. VYZÝVA Komisiu, aby posúdila možnosť koordinovanej iniciatívy na plánovanie a rozvoj spoľahlivej a odolnej siete digitálnych infraštruktúr a kapacít, ktorá by zahŕňala chrbticové pozemné, podmorské a satelitné siete v celej Únii a s medzinárodnými partnerskými krajinami, napríklad využitím rámca transeurópskych sietí a zriadením nástroja TEN-D (transeurópske siete – digitálna ekonomika). VÍTA prístup Komisie k iniciatíve v oblasti prepojenosti Arktídy, ako aj pokračujúce úsilie o posilnenie odolnosti digitálnej infraštruktúry námorných regiónov EÚ. ZDÔRAZŇUJE, že pri posudzovaní projektov európskeho záujmu v oblasti káblov, zlepšovaní bezpečnosti a odolnosti a podpore medzinárodných partnerstiev je potrebné vymedziť a dodržiavať jasné, integrované a hmatateľné kritériá s prihliadnutím na odporúčanie (EÚ) 2024/779.

34. ZAVÄZUJE sa neustále monitorovať a prispôbovať strategický prístup EÚ ku komunikačnej infraštruktúre s cieľom riešiť vznikajúce technologické, geopolitické a environmentálne výzvy a zabezpečiť spoľahlivú a odolnú konektivitu v celej Únii.
