I

(Uznesenia, odporúčania a stanoviská)

ODPORÚČANIA

RADA

ODPORÚČANIE RADY

z 8. decembra 2022

o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry

(Text s významom pre EHP)

(2023/C 20/01)

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114 a článok 292 prvú a druhú vetu,

so zreteľom na návrh Európskej komisie,

keďže:

(1) S cieľom zabezpečiť fungovanie vnútorného trhu je v záujme všetkých členských štátov a Únie ako celku, aby sa jasne identifikovala a chránila relevantná kritická infraštruktúra, ktorá poskytuje základné služby v rámci tohto trhu, najmä v kľúčových odvetviach, ako je energetika, digitálna infraštruktúra, doprava a vesmír, ako aj kritická infraštruktúra so značným cezhraničným významom ([1]), ktorej narušenie by mohlo významne ovplyvniť ostatné členské štáty.

(2) Toto odporúčanie, ktoré je nezáväzným aktom, preukazuje politickú vôľu členských štátov spolupracovať a ich záväzok vo vzťahu k odporúčaným opatreniam, ktoré sa zdôrazňujú v päťbodovom pláne vydanom predsedníčkou Európskej komisie, a to pri plnom rešpektovaní právomocí členských štátov. Toto odporúčanie nemá vplyv na ochranu základných záujmov národnej bezpečnosti, verejnej bezpečnosti a obrany členských štátov a od žiadneho členského štátu by sa nemalo očakávať, že bude zdieľať informácie, ktoré poškodzujú tieto záujmy.

(3) Hoci hlavnú zodpovednosť za zaistenie bezpečnosti a poskytovania základných služieb prostredníctvom kritickej infraštruktúry nesú členské štáty a ich prevádzkovatelia kritickej infraštruktúry, zvýšená koordinácia na úrovni Únie je vhodná najmä vzhľadom na vyvíjajúce sa hrozby, ktoré môžu mať vplyv na viaceré členské štáty súčasne, ako je napríklad útočná vojna Ruska voči Ukrajine a hybridná kampaň proti členským štátom, alebo môžu ovplyvniť odolnosť a dobré fungovanie hospodárstva Únie, jej vnútorného trhu a spoločnosti ako celku. Osobitná pozornosť by sa mala venovať kritickej infraštruktúre mimo územia členských štátov, ako je kritická podmorská infraštruktúra alebo energetická infraštruktúra na mori.

([1]) Členské štáty by mali posúdiť túto relevantnosť v súlade so svojimi vnútroštátnymi postupmi a môžu pri tom okrem iného vychádzať z posúdenia rizika, vplyvu udalosti alebo jej povahy.

(4) Európska rada vo svojich záveroch z 20. a 21. októbra 2022 dôrazne odsúdila sabotáž proti kritickej infraštruktúre, napríklad proti plynovodom Nord Stream, a vyjadrila vôľu Únie jednotne a rozhodne reagovať na akékoľvek úmyselné narušenie kritickej infraštruktúry alebo iné hybridné akcie.

(5) Vzhľadom na rýchlo sa vyvíjajúce hrozby by sa mali prioritne prijať opatrenia na zvýšenie odolnosti v kľúčových odvetviach, ako je energetika, digitálna infraštruktúra, doprava a vesmír, a v iných relevantných odvetviach, ktoré určia členské štáty. Takéto opatrenia by sa mali zamerať na posilnenie odolnosti kritickej infraštruktúry s ohľadom na príslušné riziká, najmä kaskádové účinky, narušenie dodávateľského reťazca, závislosť, vplyvy zmeny klímy, nespoľahlivých predajcov a partnerov a hybridné hrozby a kampane vrátane zahraničnej manipulácie s informáciami a zahraničného zasahovania. Pokiaľ ide o vnútroštátnu kritickú infraštruktúru, vzhľadom na možné dôsledky by sa mala venovať prioritná pozornosť infraštruktúre, ktorá má značný cezhraničný význam. Členské štáty sa nabádajú, aby vo vhodných prípadoch bezodkladne zabezpečili takéto opatrenia na zvýšenie odolnosti a zároveň zachovali prístup stanovený vo vyvíjajúcom sa právnom rámci.

(6) Ochranu európskej kritickej infraštruktúry v odvetví energetiky a dopravy v súčasnosti upravuje smernica Rady 2008/114/ES ([2]) a bezpečnosť sietí a informačných systémov v celej Únii s dôrazom na kybernetické hrozby zabezpečuje smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 ([3]). S cieľom zabezpečiť vyššiu spoločnú úroveň odolnosti a ochrany kritickej infraštruktúry, kybernetickej bezpečnosti a finančného trhu sa existujúci právny rámec mení a dopĺňa prijatím nových pravidiel uplatniteľných na kritické subjekty (smernica CER), posilnených pravidiel pre vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii (smernica NIS2) a nových pravidiel uplatniteľných na digitálnu prevádzkovú odolnosť finančného sektora (nariadenie DORA).

(7) Členské štáty by mali v súlade s právom Únie a vnútroštátnym právom využiť všetky dostupné nástroje na dosiahnutie pokroku a poskytnutie pomoci pri posilňovaní fyzickej a kybernetickej odolnosti. V tejto súvislosti by sa kritická infraštruktúra mala chápať tak, že zahŕňa relevantnú kritickú infraštruktúru identifikovanú členským štátom na vnútroštátnej úrovni alebo označenú za európsku kritickú infraštruktúru podľa smernice 2008/114/ES, ako aj kritické subjekty, ktoré sa identifikujú podľa smernice CER, alebo v príslušných prípadoch subjekty podľa smernice NIS2. Odolnosť by sa mala chápať ako schopnosť kritickej infraštruktúry predchádzať udalostiam, ktoré výrazne narúšajú alebo môžu významne narušiť poskytovanie základných služieb na vnútornom trhu, t. j. služieb, ktoré sú kľúčové pre zachovanie nevyhnutných spoločenských a hospodárskych funkcií, verejnú bezpečnosť a ochranu, zdravie obyvateľstva alebo životné prostredie, chrániť pred takýmito udalosťami, reagovať na ne, odolávať im, zmierňovať ich, absorbovať ich, prispôsobovať sa im alebo zotaviť sa z nich.

(8) Mali by sa zvolať národní experti s cieľom koordinovať prácu zameranú na dosiahnutie vyššej spoločnej úrovne odolnosti a ochrany kritickej infraštruktúry, ktorá sa má zaviesť pomocou nových pravidiel uplatniteľných na kritické subjekty. Táto koordinovaná práca by umožnila spoluprácu medzi členskými štátmi a zdieľanie informácií o činnostiach, ako je vypracovanie metodík na identifikáciu základných služieb poskytovaných kritickou infraštruktúrou. Komisia už začala zvolávať týchto expertov a uľahčovať ich prácu a má v úmysle v tom ďalej pokračovať. Po nadobudnutí účinnosti smernice CER a zriadení skupiny pre odolnosť kritických subjektov podľa tejto smernice by táto skupina mala pokračovať v tejto prípravnej práci v súlade so svojimi úlohami.

(9) Vzhľadom na zmenené prostredie hrozieb by sa mal ďalej rozvíjať potenciál vykonávania záťažových testov kritickej infraštruktúry na vnútroštátnej úrovni, keďže tieto testy by mohli byť užitočné na zvýšenie odolnosti kritickej infraštruktúry. Vzhľadom na osobitný význam odvetvia energetiky a dôsledky, ktoré by malo jeho možné narušenie pre celú Úniu, by vykonávanie záťažových testov na základe spoločne dohodnutých zásad pre toto odvetvie mohlo byť najväčším prínosom. Tieto testy patria do právomoci členských štátov, ktoré by mali nabádať a podporovať prevádzkovateľov kritickej infraštruktúry, aby tieto testy vykonávali, ak ich považujú za prospešné a zlučiteľné so svojimi vnútroštátnymi právnymi rámcami.

([2]) Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).

([3]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

(10) S cieľom zabezpečiť koordinovanú a účinnú reakciu na súčasné a očakávané hrozby sa Komisia nabáda, aby členským štátom poskytla dodatočnú podporu, najmä poskytovaním relevantných informácií vo forme brífingov, nezáväzných príručiek a usmernení. Európska služba pre vonkajšiu činnosť (ESVČ) by mala poskytovať posúdenia hrozieb najmä prostredníctvom Spravodajského a situačného centra EÚ a jeho strediska pre hybridné hrozby a s podporou riaditeľstva Vojenského štábu Európskej únie (EUMS) pre spravodajské informácie v rámci jednotnej kapacity na analýzu spravodajských informácií (SIAC). Komisia sa takisto vyzýva, aby v spolupráci s členskými štátmi presadzovala využívanie výskumných a inovačných projektov financovaných Úniou.

(11) Vzhľadom na rastúcu vzájomnú závislosť fyzickej a digitálnej infraštruktúry môžu škodlivé kybernetické činnosti zamerané na kritické oblasti viesť k narušeniu alebo poškodeniu fyzickej infraštruktúry, pričom sabotáž fyzickej infraštruktúry môže zase znemožniť prístup k digitálnym službám. Členské štáty sa vyzývajú, aby čo najskôr urýchlili prípravné práce zamerané na transpozíciu a uplatňovanie nového právneho rámca pre kritické subjekty a posilneného právneho rámca pre kybernetickú bezpečnosť, pričom by mali vychádzať zo skúseností získaných v rámci skupiny pre spoluprácu zriadenej smernicou (EÚ) 2016/1148 (ďalej len „skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti“), zohľadniť transpozičné lehoty a napredovať v tejto prípravnej práci súbežne a koherentne.

(12) Popri zvýšení pripravenosti je takisto dôležité posilniť spôsobilosti na rýchlu a účinnú reakciu na narušenie základných služieb poskytovaných kritickou infraštruktúrou. Toto odporúčanie preto obsahuje opatrenia na úrovni Únie aj na úrovni členských štátov, pričom zdôrazňuje aj podpornú úlohu a pridanú hodnotu, ktorú možno dosiahnuť zavedením posilnenej spolupráce a výmeny informácií v kontexte mechanizmu Únie v oblasti civilnej ochrany (UCPM) zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ ([4]) a využívaním príslušných prostriedkov Vesmírneho programu Únie zriadeného nariadením Európskeho parlamentu a Rady (EÚ) 2021/696 ([5]).

(13) Komisia, vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a zriadenými sieťami vrátane Európskej siete styčných organizácií pre kybernetické krízy (EU-CyCLONe) majú vykonávať hodnotenie rizík a vytvárať rizikové scenáre. V nadväznosti na spoločnú ministerskú výzvu z Nevers okrem toho skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v súčasnosti vykonáva posúdenie rizík s podporou Komisie a Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie (BEREC). Tieto dva procesy budú konzistentné a koordinované s vytváraním scenárov v rámci mechanizmu Únie v oblasti civilnej ochrany, ktorého súčasťou sú aj podujatia v oblasti kybernetickej bezpečnosti a ich skutočný vplyv a ktorý v súčasnosti vypracúva Komisia a členské štáty. V záujme efektívnosti, účinnosti, konzistentnosti a správneho uplatňovania tohto odporúčania by sa výsledky týchto procesov mali odzrkadliť na vnútroštátnej úrovni.

(14) S cieľom okamžite posilniť pripravenosť a schopnosť reagovať na rozsiahle kybernetickobezpečnostné incidenty Komisia vytvorila krátkodobý program na podporu členských štátov prostredníctvom dodatočných finančných prostriedkov pridelených agentúre ENISA. Navrhované služby okrem iného zahŕňajú opatrenia v oblasti pripravenosti, ako je penetračné testovanie subjektov s cieľom identifikovať zraniteľné miesta. Prostredníctvom programu sa môžu posilniť aj možnosti pomoci členským štátom v prípade rozsiahleho kybernetickobezpečnostného incidentu s vplyvom na kritické subjekty. Ide o prvý krok v súlade so závermi Rady z 23.mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti (ďalej len „závery Rady o prístupe EÚ ku kybernetickej bezpečnosti“), v ktorých sa od Komisie požaduje, aby predložila návrh fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti. Členské štáty by mali v plnej miere využívať tieto príležitosti v súlade s uplatniteľnými požiadavkami a nabádajú sa, aby pokračovali v práci v oblasti riadenia kybernetických kríz Únie, a to najmä pravidelným monitorovaním a hodnotením pokroku dosiahnutého pri vykonávaní plánu riadenia kybernetických kríz, ktorý nedávno vypracovala Rada. Tento plán je živým dokumentom a mal by sa v prípade potreby prehodnotiť a aktualizovať.

([4]) Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/696 z 28. apríla 2021, ktorým sa zriaďuje Vesmírny program Únie a Agentúra Európskej únie pre vesmírny program a ktorým sa zrušujú nariadenia (EÚ) č. 912/2010, (EÚ) č. 1285/2013 a (EÚ) č. 377/2014 a rozhodnutie č. 541/2014/EÚ (Ú. v. EÚ L 170, 12.5.2021, s. 69).

(15) Globálne podmorské komunikačné káble majú zásadný význam pre globálnu konektivitu i konektivitu v rámci EÚ. Vzhľadom na značnú dĺžku týchto káblov a ich inštaláciu na morskom dne je podmorské vizuálne monitorovanie väčšiny káblových úsekov mimoriadne náročné. Spoločná jurisdikcia a iné otázky týkajúce sa právomoci v súvislosti s týmito káblami predstavujú špecifický prípad európskej a medzinárodnej spolupráce v oblasti ochrany a obnovy infraštruktúry. Preto je potrebné doplniť prebiehajúce a plánované posúdenia rizík týkajúcich sa digitálnej a fyzickej infraštruktúry, ktorá podporuje digitálne služby, osobitnými posúdeniami rizík a možnosťami zmierňujúcich opatrení týkajúcich sa podmorských komunikačných káblov. Členské štáty vyzývajú Komisiu, aby na tento účel vykonala štúdie a svoje zistenia poskytla členským štátom.

(16) Hrozbami súvisiacimi s digitálnou infraštruktúrou môžu byť ovplyvnené aj odvetvia energetiky a dopravy, napríklad v súvislosti s energetickými technológiami, ktoré zahŕňajú digitálne komponenty. Bezpečnosť súvisiacich dodávateľských reťazcov je dôležitá pre kontinuitu poskytovania základných služieb a pre strategickú kontrolu kritickej infraštruktúry v odvetví energetiky. Tieto okolnosti by sa mali zohľadniť pri prijímaní opatrení na zvýšenie odolnosti kritickej infraštruktúry v súlade s týmto odporúčaním.

(17) Vzhľadom na rastúci význam vesmírnej infraštruktúry, pozemných prostriedkov súvisiacich s vesmírom vrátane výrobných zariadení, ako aj vesmírnych služieb pre činnosti súvisiace s bezpečnosťou je nevyhnutné zabezpečiť odolnosť a ochranu vesmírnych a súvisiacich pozemných prostriedkov a služieb v rámci Únie. Z rovnakých dôvodov je tiež nevyhnutné, aby sa v rámci tohto odporúčania štruktúrovanejšie využívali vesmírne údaje a služby poskytované vesmírnymi systémami a programami na dohľad nad kritickou infraštruktúrou v iných odvetviach a na sledovanie a ochranu tejto infraštruktúry. V pripravovanej vesmírnej stratégii EÚ pre bezpečnosť a obranu sa v tejto súvislosti navrhnú vhodné opatrenia, ktoré by sa mali zohľadniť pri vykonávaní tohto odporúčania.

(18) Na účinné riešenie rizík pre kritickú infraštruktúru je potrebná aj spolupráca na medzinárodnej úrovni, okrem iného aj v súvislosti s infraštruktúrou v medzinárodných vodách. Členské štáty sa preto vyzývajú, aby spolupracovali s Komisiou a vysokým predstaviteľom s cieľom podniknúť určité kroky smerom k nadviazaniu takejto spolupráce, pričom musia mať na pamäti, že všetky takéto kroky sa smú prijať len v súlade s ich príslušnými úlohami a povinnosťami podľa práva Únie, najmä podľa ustanovení zmlúv týkajúcich sa vonkajších vzťahov.

(19) Ako sa uvádza v oznámení Komisie z 15. februára 2022 s názvom „Príspevok Komisie k európskej obrane“, v nadväznosti na dokument „Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti“, Komisia do roku 2023 v spolupráci s vysokým predstaviteľom a členskými štátmi posúdi základné odvetvové scenáre hybridnej odolnosti s cieľom identifikovať nedostatky a potreby, ako aj kroky na ich riešenie. Táto iniciatíva by mala byť podkladom pre ďalšiu činnosť v rámci tohto odporúčania a mala by prispieť k posilneniu výmeny informácií a koordinácie opatrení na ďalšie zvyšovanie odolnosti vrátane odolnosti kritickej infraštruktúry.

(20) Stratégia námornej bezpečnosti EÚ z roku 2014 a jej revidovaný akčný plán obsahovali výzvu na zvýšenú ochranu kritickej námornej infraštruktúry vrátane podmorskej, a najmä infraštruktúry námornej dopravy a energetickej a komunikačnej infraštruktúry, okrem iného aj zvyšovaním informovanosti o námornej doprave prostredníctvom lepšej interoperability a zjednodušenej výmeny informácií (povinnej i dobrovoľnej). Táto stratégia a tento akčný plán sa v súčasnosti aktualizujú a budú zahŕňať posilnené opatrenia zamerané na ochranu kritickej námornej infraštruktúry. Tieto opatrenia by mali dopĺňať toto odporúčanie.

(21) Posilnenie odolnosti kritickej infraštruktúry prispieva k širšiemu úsiliu v boji proti hybridným hrozbám a kampaniam zameraným proti Únii a jej členským štátom. Toto odporúčanie vychádza zo spoločného oznámenia Európskemu parlamentu a Rade s názvom „Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie“. Opatrenie 1 tohto spoločného rámca, konkrétne prieskum hybridných rizík, zohráva kľúčovú úlohu pri identifikácii zraniteľných miest, ktoré môžu mať vplyv na vnútroštátne a celoeurópske štruktúry a siete. Vykonávaním záverov Rady z 21. júna 2022 o rámci pre koordinovanú reakciu EÚ na hybridné kampane sa okrem toho zabezpečí silnejšia koordinovaná činnosť prostredníctvom uplatňovania súboru nástrojov EÚ na boj proti hybridným hrozbám vo všetkých dotknutých oblastiach,

PRIJALA TOTO ODPORÚČANIE:

KAPITOLA I: CIEĽ, ROZSAH PÔSOBNOSTI A STANOVENIE PRIORÍT

1. V tomto odporúčaní sa stanovuje súbor cielených opatrení na úrovni Únie a na vnútroštátnej úrovni, ktoré majú na dobrovoľnom základe podporiť a zvýšiť odolnosť kritickej infraštruktúry so zameraním na kritickú infraštruktúru so značným cezhraničným významom a v identifikovaných kľúčových odvetviach, ako je energetika, digitálna infraštruktúra, doprava a vesmír. Tieto cielené opatrenia zahŕňajú lepšiu pripravenosť, posilnenú reakciu a medzinárodnú spoluprácu.

2. Informácie zdieľané v záujme plnenia cieľov toho odporúčania, ktoré sú dôverné podľa pravidiel Únie a vnútroštátnych pravidiel, ako aj podľa pravidiel dôvernosti v obchode, by sa mali vymieňať s Komisiou a inými príslušnými orgánmi len vtedy, ak je táto výmena potrebná na účely správneho uplatňovania tohto odporúčania. Toto odporúčanie nemá vplyv na ochranu základných záujmov národnej bezpečnosti, verejnej bezpečnosti či obrany členských štátov a od žiadneho členského štátu by sa nemalo očakávať, že bude zdieľať informácie, ktoré sú v rozpore s týmito záujmami.

KAPITOLA II: ZVÝŠENÁ PRIPRAVENOSŤ

Opatrenia na úrovni členských štátov

3. Keď členské štáty aktualizujú svoje posúdenia rizík alebo existujúce rovnocenné analýzy, mali by zvážiť prístup zohľadňujúci všetky riziká v súlade s vyvíjajúcou sa povahou súčasných hrozieb pre ich kritickú infraštruktúru, najmä v identifikovaných kľúčových odvetviach a podľa možnosti vo všetkých odvetviach, na ktoré sa vzťahuje pripravovaný nový právny rámec uplatniteľný na kritické subjekty.

4. Členské štáty sa vyzývajú, aby urýchlili prípravné práce a podľa možnosti prijali opatrenia na zvýšenie odolnosti, ako sa stanovuje v pripravovanom právnom rámci uplatniteľnom na kritické subjekty, s osobitným dôrazom na spoluprácu a výmenu relevantných informácií medzi členskými štátmi a s Komisiou, na identifikáciu kritických subjektov so značným cezhraničným významom a na posilnenie podpory identifikovaných kritických subjektov s cieľom zlepšiť ich odolnosť.

5. Členské štáty by mali podporovať odbornú prípravu a cvičenia expertov, ako aj vzájomnú výmenu najlepších postupov a získaných skúseností medzi expertmi. Členské štáty by mali nabádať expertov, aby sa zúčastňovali na existujúcich vnútroštátnych aj medzinárodných platformách odbornej prípravy, napríklad v rámci mechanizmu Únie v oblasti civilnej ochrany.

6. Členské štáty by mali nabádať a podporovať prevádzkovateľov kritickej infraštruktúry aspoň v odvetví energetiky, aby vykonávali záťažové testy podľa zásad spoločne dohodnutých na úrovni Únie, ak sú prospešné. Pomocou týchto stresových testov by sa mala posúdiť odolnosť kritickej infraštruktúry voči antagonistickým hrozbám súvisiacim s ľudskou činnosťou. Členské štáty by sa preto mali snažiť identifikovať príslušnú kritickú infraštruktúru, ktorá sa má testovať, a čo najskôr, najneskôr však do konca prvého štvrťroku 2023, konzultovať s prevádzkovateľmi príslušnej kritickej infraštruktúry. Okrem toho by členské štáty mali podporovať prevádzkovateľov kritickej infraštruktúry, aby vykonali tieto testy čo najskôr a snažili sa ich dokončiť do konca roka 2023, a to v súlade s vnútroštátnym právom. Rada má v úmysle posúdiť aktuálny stav záťažových testov do konca apríla 2023.

7. Vzhľadom na rýchlo sa vyvíjajúce hrozby pre kritickú infraštruktúru má zachovanie vysokej úrovne jej ochrany zásadný význam. Členské štáty sa nabádajú, aby vyčlenili dostatočné finančné zdroje na posilnenie kapacít svojich príslušných vnútroštátnych orgánov a podporovali ich, aby boli schopné zvýšiť odolnosť kritickej infraštruktúry. Členské štáty sa takisto nabádajú, aby vyčlenili dostatočné finančné zdroje pre orgány zodpovedné za riadenie rozsiahlych kybernetickobezpečnostných incidentov, podporovali ich a zabezpečili plnú mobilizáciu ich jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) a príslušných orgánov v rámci siete jednotiek CSIRT a siete EU-CyCLONe.

8. Členské štáty sa vyzývajú, aby v súlade s uplatniteľnými požiadavkami využili potenciálne možnosti financovania na úrovni Únie a na vnútroštátnej úrovni na zvýšenie odolnosti kritickej infraštruktúry v Únii pre seba a aby tiež nabádali prevádzkovateľov kritickej infraštruktúry, napríklad vrátane transeurópskych sietí, aby využívali takéto možnosti financovania proti celej škále závažných hrozieb, najmä v rámci programov financovaných z Fondu pre vnútornú bezpečnosť zriadeného nariadením Európskeho parlamentu a Rady (EÚ) 2021/1149 ([6]), Európskeho fondu regionálneho rozvoja zriadeného nariadením Európskeho parlamentu a Rady (EÚ) č. 1301/2013 ([7]), mechanizmu Únie v oblasti civilnej ochrany a plánu Komisie REPowerEU. Členské štáty sa takisto nabádajú, aby čo najlepšie využívali výsledky relevantných projektov v rámci výskumných programov, ako je Horizont Európa zriadený nariadením Európskeho parlamentu a Rady (EÚ) 2021/695 ([8]).

9. Pokiaľ ide o komunikačnú a sieťovú infraštruktúru v Únii, skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti sa vyzýva, aby v súlade s článkom 11 smernice (EÚ) 2016/1148 urýchlila svoju prebiehajúcu prácu na základe spoločnej ministerskej výzvy z Nevers zameranú na cielené posúdenie rizika a aby čo najskôr predložila prvé odporúčania. Toto posúdenie rizika by malo byť podkladom pre prebiehajúce medziodvetvové hodnotenie a scenáre kybernetických rizík, ktoré sa požadujú v záveroch Rady o prístupe EÚ ku kybernetickej bezpečnosti. Okrem toho by sa pri tejto práci mala zabezpečiť súdržnosť a komplementárnosť s prácou, ktorú vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, pokiaľ ide o bezpečnosť dodávateľského reťazca informačných a komunikačných technológií, ako aj iné relevantné skupiny.

10. Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti sa takisto vyzýva, aby s podporou Komisie a agentúry ENISA pokračovala v práci zameranej na bezpečnosť digitálnej infraštruktúry, a to aj v súvislosti s podmorskou infraštruktúrou, konkrétne podmorskými komunikačnými káblami. Takisto sa vyzýva, aby začala prácu zameranú na vesmírny sektor, v prípade potreby aj prípravou politických usmernení a metodík riadenia kybernetických rizík založených na prístupe zohľadňujúcom všetky hrozby a riziká pre prevádzkovateľov vo vesmírnom sektore, s cieľom zvýšiť odolnosť pozemnej infraštruktúry, ktorá podporuje poskytovanie vesmírnych služieb.

11. Členské štáty by mali v plnej miere využívať služby pripravenosti v oblasti kybernetickej bezpečnosti, ktoré ponúka program krátkodobej podpory Komisie realizovaný v spolupráci s agentúrou ENISA, napríklad penetračné testovanie na odhalenie zraniteľných miest, pričom sa v tejto súvislosti vyzývajú, aby sa prioritne zamerali na subjekty, ktoré prevádzkujú kritickú infraštruktúru v odvetviach energetiky, digitálnej infraštruktúry a dopravy.

12. Členské štáty by mali v plnej miere využívať Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC). Členské štáty by mali nabádať svoje národné koordinačné centrá, aby aktívne spolupracovali s členmi komunity kybernetickej bezpečnosti s cieľom budovať kapacity na úrovni Únie a na vnútroštátnej úrovni v záujme lepšej podpory prevádzkovateľov základných služieb.

13. Je dôležité, aby členské štáty dokončili vykonávanie opatrení odporúčaných v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, a najmä aby členské štáty zaviedli obmedzenia týkajúce sa vysokorizikových dodávateľov vzhľadom na to, že strata času môže zvýšiť zraniteľnosť sietí v Únii, a tiež aby posilnili fyzickú a nefyzickú ochranu kritických a citlivých častí sietí 5G, a to aj prostredníctvom prísnych kontrol prístupu. Okrem toho by mali členské štáty v spolupráci s Komisiou posúdiť potrebu doplnkových opatrení, aby sa zaistila jednotná úroveň bezpečnosti a odolnosti sietí 5G.

14. Členské štáty spolu s Komisiou a agentúrou ENISA by sa mali zamerať na vykonávanie záverov Rady zo 17. októbra 2022 o bezpečnosti dodávateľského reťazca IKT.

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1149 zo 7. júla 2021, ktorým sa zriaďuje Fond pre vnútornú bezpečnosť (Ú. v. EÚ L 251, 15.7.2021, s. 94).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1301/2013 zo 17. decembra 2013 o Európskom fonde regionálneho rozvoja a o osobitných ustanoveniach týkajúcich sa cieľa Investovanie do rastu a zamestnanosti, a ktorým sa zrušuje nariadenie (ES) č. 1080/2006 (Ú. v. EÚ L 347, 20.12.2013, s. 289).

([8]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/695 z 28. apríla 2021, ktorým sa zriaďuje Horizont Európa – rámcový program pre výskum a inovácie, stanovujú jeho pravidlá účasti a šírenia a zrušujú nariadenia (EÚ) č. 1290/2013 a (EÚ) č. 1291/2013 (Ú. v. EÚ L 170, 12.5.2021, s. 1).

15. Členské štáty by mali zohľadniť pripravovaný sieťový predpis o aspektoch kybernetickej bezpečnosti pri cezhraničných tokoch elektriny [...], pričom by mali vychádzať zo skúseností získaných pri vykonávaní smernice (EÚ) 2016/1148 a z príslušných usmernení vypracovaných skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, najmä z jej referenčného dokumentu o bezpečnostných opatreniach pre prevádzkovateľov základných služieb.

16. Členské štáty by mali rozvíjať používanie systémov Copernicus a Galileo a Európskej prekryvnej služby geostacionárnej navigácie (EGNOS) na účely dohľadu s cieľom zdieľať relevantné informácie s expertmi zvolanými v súlade s bodom 15. Mali by sa dobre využívať schopnosti, ktoré ponúka vládna satelitná komunikácia Únie (GOVSATCOM) Vesmírneho programu Únie na monitorovanie kritickej infraštruktúry, podporu predpovedania kríz a reakcie na ne.

Opatrenia na úrovni Únie

17. Mal by sa posilniť dialóg a spolupráca medzi určenými expertmi členských štátov a s Komisiou s cieľom zvýšiť fyzickú odolnosť kritickej infraštruktúry, a to najmä:

    a) prispením k príprave, vypracovaniu a propagácii spoločných dobrovoľných nástrojov na podporu členských štátov pri zvyšovaní odolnosti vrátane metodík a rizikových scenárov;

    b) podporou členských štátov pri vykonávaní nového právneho rámca uplatniteľného na kritické subjekty, okrem iného aj podnecovaním Komisie, aby včas prijala príslušný delegovaný akt;

    c) podporou vykonávania záťažových testov uvedených v bode 6 na základe spoločných zásad, počnúc testami zameranými na antagonistické hrozby súvisiace s ľudskou činnosťou v odvetví energetiky a následne aj v ďalších kľúčových odvetviach, ako aj podporou a poradenstvom pri vykonávaní takýchto záťažových testov na žiadosť členského štátu;

    d) využívaním bezpečnej platformy – po jej zriadení Komisiou – na dobrovoľné zhromažďovanie, hodnotenie a zdieľanie najlepších postupov, skúseností získaných z vnútroštátnych postupov a iných informácií súvisiacich s odolnosťou.

    Určení experti by mali pri tejto práci venovať osobitnú pozornosť medziodvetvovým závislostiam a kritickej infraštruktúre so značným cezhraničným významom a vo vhodných prípadoch by na ich prácu mala nadviazať Rada a Komisia.

18. Členské štáty sa nabádajú, aby využívali podporu, ktorú ponúka Komisia, napríklad prostredníctvom vypracúvania príručiek a usmernení, ako je príručka o ochrane kritickej infraštruktúry a verejných priestorov pred bezpilotnými leteckými systémami, a nástrojov na posudzovanie rizík. ESVČ sa vyzýva, aby najmä prostredníctvom Spravodajského a situačného centra EÚ a jeho strediska pre hybridné hrozby organizovala s podporou riaditeľstva EUMS pre spravodajské informácie v rámci SIAC brífingy o hrozbách pre kritickú infraštruktúru v Únii s cieľom zvýšiť situačnú informovanosť.

19. Členské štáty by mali podporovať opatrenia Komisie s cieľom využiť výsledky projektov zameraných na odolnosť kritickej infraštruktúry financovaných v rámci programov Únie pre výskum a inováciu. Rada berie na vedomie zámer Komisie zvýšiť v rámci rozpočtu vyčleneného na program Horizont Európa z viacročného finančného rámca na roky 2021 – 2027 finančné prostriedky na odolnosť bez toho, aby to malo negatívny vplyv na financovanie iných výskumných a inovačných projektov v oblasti civilnej bezpečnosti v rámci programu Horizont Európa.

20. Vzhľadom na úlohy stanovené v záveroch Rady o prístupe EÚ ku kybernetickej bezpečnosti sa Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti vyzývajú, aby v súlade so svojimi príslušnými úlohami a povinnosťami podľa práva Únie zintenzívnili spoluprácu s príslušnými sieťami a civilnými a vojenskými orgánmi a agentúrami pri vykonávaní hodnotenia rizík a vytváraní scenárov kybernetických rizík, pričom je potrebné zohľadniť najmä význam energetickej, digitálnej, dopravnej a vesmírnej infraštruktúry a vzájomnú závislosť medzi odvetviami a členskými štátmi. V tejto súvislosti by sa malo prihliadať aj na súvisiace riziká pre infraštruktúru, ktorú tieto odvetvia využívajú. Ak je hodnotenie rizík a vypracúvanie rizikových scenárov prínosom, mohlo by sa realizovať pravidelne, pričom by sa ním mali dopĺňať, rozvíjať a nezdvojovať existujúce alebo plánované posúdenia rizík v týchto odvetviach a poskytovať vstupy pre diskusie o tom, ako posilniť celkovú odolnosť subjektov prevádzkujúcich kritickú infraštruktúru a riešiť zraniteľné miesta.

21. Komisia sa vyzýva, aby v súlade so svojimi príslušnými úlohami v rámci riadenia kybernetických kríz urýchlila svoje činnosti zamerané na podporu pripravenosti a reakcie členských štátov na rozsiahle kybernetickobezpečnostné incidenty, a najmä aby:

a) s cieľom doplniť príslušné posúdenia rizík v kontexte bezpečnosti sietí a informácií vykonala komplexnú štúdiu ([9]), v ktorej zhodnotí podmorskú infraštruktúru, konkrétne podmorské komunikačné káble, ktoré spájajú členské štáty, ako aj Európu z globálneho hľadiska, pričom zistenia by sa mali zdieľať s členskými štátmi;

b) podporovala pripravenosť a reakcie členských štátov a inštitúcií, orgánov a agentúr Únie na rozsiahle kybernetickobezpečnostné incidenty alebo závažné incidenty v súlade s posilneným právnym rámcom pre kybernetickú bezpečnosť a inými príslušnými uplatniteľnými pravidlami ([10]);

c) urýchlila hlavnú koncepciu núdzového kybernetického fondu v rámci náležitej diskusie s členskými štátmi.

22. Komisia sa nabáda, aby intenzívnejšie pracovala na anticipačných opatreniach s výhľadom do budúcnosti vrátane spolupráce s členskými štátmi podľa článkov 6 a 10 rozhodnutia 1313/2013/EÚ, ako aj formou plánovania pre prípad nepredvídaných udalostí s cieľom podporiť operačnú pripravenosť Koordinačného centra pre reakcie na núdzové situácie (ERCC) a jeho reakciu na narušenia kritickej infraštruktúry; zvýšila investície do preventívnych prístupov a pripravenosti obyvateľstva a zvýšila podporu súvisiacu s budovaním kapacít v rámci vedomostnej siete Únie v oblasti civilnej ochrany.

23. Komisia by mala presadzovať používanie prostriedkov Únie na vykonávanie dohľadu (Copernicus, Galileo a EGNOS), aby tak podporila členské štáty pri monitorovaní kritickej infraštruktúry a v relevantných prípadoch aj jej bezprostredného okolia a aby zároveň podporila aj ďalšie možnosti dohľadu stanovené vo Vesmírnom programe Únie, ako je napríklad rámec získavania informácií o situácii vo vesmíre a rámec EÚ pre dohľad nad kozmickým priestorom a sledovanie tohto priestoru.

24. Agentúry Únie a iné príslušné subjekty sa vyzývajú, aby v relevantných prípadoch v súlade so svojimi mandátmi poskytli podporu v otázkach týkajúcich sa odolnosti kritickej infraštruktúry, a to najmä takto:

a) Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva (EUROPOL), pokiaľ ide o zhromažďovaní informácií, analýzu trestnej činnosti a podporu vyšetrovania pri cezhraničných opatreniach v oblasti presadzovania práva a v relevantných a vhodných prípadoch zdieľanie výsledkov s členskými štátmi;

b) Európska námorná bezpečnostná agentúra (EMSA), pokiaľ ide o záležitostí súvisiace s bezpečnosťou a ochranou námorného odvetvia Únie vrátane služieb námorného dozoru v záležitostiach súvisiacich s námornou bezpečnosťou a ochranou;

c) Agentúra Európskej únie pre vesmírny program (EUSPA) a Satelitné stredisko EÚ (Saten) môžu pomáhať prostredníctvom operácií v rámci Vesmírneho programu Únie;

d) Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC), pokiaľ ide o činnosti súvisiace s kybernetickou bezpečnosťou, pričom v spolupráci s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) by mohlo podporovať inováciu a priemyselnú politiku v oblasti kybernetickej bezpečnosti.

([9]) Táto štúdia by mala zahŕňať mapovanie kapacít a redundancií, zraniteľných miest, hrozieb a rizík pre dostupnosť služieb, vplyvu výpadkov (transatlantických) podmorských káblov na členské štáty a Úniu ako celok a zmierňovanie rizík, pričom by sa mala zohľadniť citlivosť takýchto informácií a potreba ich ochrany.

([10]) Osobitná pozornosť by sa mala venovať aj všetkým činnostiam zameraným na prípravu účinnej koordinovanej reakcie na úrovni Únie v prípade závažného cezhraničného kybernetickobezpečnostného incidentu alebo súvisiacej hrozby, ktorá by mohla mať systémový vplyv na finančný sektor Únie, ako sa stanovuje v novom právnom rámci pre digitálnu prevádzkovú odolnosť.

KAPITOLA III: POSILNENÁ REAKCIA

Opatrenia na úrovni členských štátov

25. Členské štáty sa vyzývajú, aby:

a) v relevantných prípadoch pokračovali v koordinácii svojej reakcie a udržiavali si prehľad o medziodvetvovej reakcii na akútne narušenia základných služieb poskytovaných kritickou infraštruktúrou. Mohlo by sa to uskutočniť v rámci budúcej koncepcie koordinovanej reakcie na narušenia kritickej infraštruktúry so značným cezhraničným významom; existujúcich integrovaných dojednaní o politickej reakcii na krízu (IPCR) na účely koordinácie politickej reakcie, pokiaľ ide o kritickú infraštruktúru s cezhraničným významom; koncepcie pre rozsiahle kybernetickobezpečnostné incidenty a krízy podľa odporúčania Komisie (EÚ) 2017/1584 ([11]); siete EU-CyCLONe; v rámci pre koordinovanú reakciu EÚ na hybridné kampane a v rámci súboru nástrojov EÚ na boj proti hybridným hrozbám v prípade hybridných hrozieb a kampaní; a v rámci systému včasného varovania v prípade dezinformácií.

b) zintenzívnili výmenu informácií na operačnej úrovni s ERCC v kontexte mechanizmu Únie v oblasti civilnej ochrany s cieľom posilniť včasné varovanie a koordinovať svoju reakciu v rámci mechanizmu Únie v oblasti civilnej ochrany v prípade narušenia kritickej infraštruktúry so značným cezhraničným významom, čím sa v prípade potreby zabezpečí rýchlejšia reakcia s podporou Únie;

c) zvýšili svoju pripravenosť reagovať, ak je to relevantné, prostredníctvom existujúcich alebo pripravovaných nástrojov na takéto závažné narušenia uvedené v písmene a);

d) sa angažovali v ďalšom rozvoji príslušných kapacít reakcie v rámci európskeho zoskupenia v oblasti civilnej ochrany (ECPP) a systému rescEU;

e) nabádali prevádzkovateľov kritickej infraštruktúry a príslušné vnútroštátne orgány, aby posilnili svoje kapacity tak, aby boli schopní rýchlo obnoviť základný výkon základných služieb, ktoré poskytujú títo prevádzkovateľmi kritickej infraštruktúry;

f) nabádali prevádzkovateľov kritickej infraštruktúry, aby pri obnove svojej kritickej infraštruktúry dbali na to, aby bola táto infraštruktúra čo najodolnejšia, berúc do úvahy primeranosť opatrení z hľadiska posúdení rizík a nákladov, celej škály významných rizík, ktoré sa na ňu môžu vzťahovať, a to aj v nepriaznivých klimatických scenároch.

26. Členské štáty sa vyzývajú, aby podľa možnosti urýchlili prípravné práce v súlade s posilneným právnym rámcom v oblasti kybernetickej bezpečnosti tým, že sa zamerajú na zlepšenie spôsobilostí vnútroštátnych jednotiek CSIRT vzhľadom na nové úlohy týchto jednotiek, ako aj na zvýšený počet subjektov z nových odvetví, tým, že včas preskúmajú a aktualizujú svoje stratégie kybernetickej bezpečnosti a čo najskôr prijmú vnútroštátne plány reakcie na kybernetickobezpečnostné incidenty a krízy, ak takéto plány ešte neexistujú.

27. Členské štáty sa vyzývajú, aby na vnútroštátnej úrovni zvážili najrelevantnejšie prostriedky na zabezpečenie toho, aby si boli príslušné zainteresované strany vedomé potreby zvýšiť odolnosť kritickej infraštruktúry prostredníctvom spolupráce s dôveryhodnými predajcami a partnermi. Je dôležité investovať do dodatočnej kapacity, najmä v odvetviach, v ktorých je súčasná infraštruktúra na konci životnosti, napríklad infraštruktúra podmorských komunikačných káblov, aby bolo možné zabezpečiť kontinuitu poskytovania základných služieb v prípade narušení a znížiť neželané závislosti.

28. Členské štáty sa nabádajú, aby venovali pozornosť proaktívnej strategickej komunikácii na vnútroštátnej úrovni v súvislosti s bojom proti hybridným hrozbám a kampaniam a vzhľadom na skutočnosť, že protivníci sa môžu snažiť zapojiť do zahraničnej manipulácie s informáciami a zasahovania ovplyvňovaním rétoriky v súvislosti s incidentmi zameranými na kritickú infraštruktúru.

Opatrenia na úrovni Únie

29. Komisia sa vyzýva, aby úzko spolupracovala s členskými štátmi na ďalšom rozvoji príslušných orgánov, nástrojov a kapacít v oblasti reakcie s cieľom zlepšiť operačnú pripravenosť na riešenie bezprostredných a nepriamych účinkov závažných narušení príslušných základných služieb poskytovaných kritickou infraštruktúrou, najmä pokiaľ ide o expertov a zdroje dostupné prostredníctvom európskeho zoskupenia v oblasti civilnej ochrany (ECPP) a systému rescEU v rámci mechanizmu Únie v oblasti civilnej ochrany alebo budúce tímy rýchlej reakcie na hybridné hrozby.

([11]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

30. Komisia sa vyzýva, aby vzhľadom na vyvíjajúce sa prostredie hrozieb v spolupráci s členskými štátmi v rámci mechanizmu Únie v oblasti civilnej ochrany:

a) nepretržite analyzovala a testovala primeranosť a operačnú pohotovosť existujúcich kapacít na reakciu;

b) pravidelne monitorovala a identifikovala potenciálne závažné nedostatky kapacity na reakciu v rámci ECPP a rescEU;

c) ďalej zintenzívňovala medziodvetvovú spoluprácu v snahe zabezpečiť primeranú reakciu na úrovni Únie a pravidelne organizovala odbornú prípravu alebo cvičenia zamerané na testovanie tejto spolupráce spolu s jedným alebo viacerými členskými štátmi;

d) ďalej rozvíjala ERCC ako medziodvetvové núdzové stredisko na úrovni Únie, ktorého úlohou je koordinovať podporu poskytovanú postihnutým členským štátom.

31. Rada je odhodlaná začať prácu s cieľom schváliť koncepciu koordinovanej reakcie na narušenia kritickej infraštruktúry so značným cezhraničným významom, v ktorej sa opisujú a stanovujú ciele a spôsoby spolupráce medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie pri reakcii na incidenty proti takejto kritickej infraštruktúre. Rada so záujmom očakáva návrh Komisie na takúto koncepciu, ktorý bude vychádzať z podpory a príspevkov príslušných agentúr Únie. Táto koncepcia musí byť plne zosúladená a interoperabilná s revidovaným operačným protokolom Únie na boj proti hybridným hrozbám (ďalej len „operačný protokol EÚ“) a musí zohľadňovať existujúcu koncepciu koordinovanej reakcie na cezhraničné kybernetickobezpečnostné incidenty ([12]) a krízy veľkého rozsahu a mandát siete EU-CyCLONe stanovený v smernici NIS2 a zabrániť duplicite štruktúr a činností. Táto koncepcia by mala v plnej miere rešpektovať existujúce dojednania IPCR zamerané na koordináciu reakcie.

32. Komisia sa vyzýva, aby konzultovala s relevantnými zainteresovanými stranami a expertmi o vhodných opatreniach v súvislosti s možnými závažnými incidentmi týkajúcimi sa podmorskej infraštruktúry, ktoré sa majú predložiť spoločne s hodnotiacou štúdiou uvedenou v bode 20 písm. a), ako aj aby ďalej rozpracovala plánovanie pre prípad nepredvídaných udalostí, scenáre rizík a ciele Únie v oblasti odolnosti voči katastrofám stanovené v rozhodnutí č. 1313/2013/EÚ.

KAPITOLA IV: MEDZINÁRODNÁ SPOLUPRÁCA

Opatrenia na úrovni členských štátov

33. Členské štáty by mali vo vhodných prípadoch a v súlade s právom Únie spolupracovať s relevantnými tretími krajinami v oblasti odolnosti kritickej infraštruktúry so značným cezhraničným významom.

34. Členské štáty sa nabádajú, aby spolupracovali s Komisiou a vysokým predstaviteľom s cieľom účinne riešiť riziká pre kritickú infraštruktúru v medzinárodných vodách.

35. Členské štáty sa vyzývajú, aby v spolupráci s Komisiou a vysokým predstaviteľom prispeli k urýchlenému vypracovaniu a zavedeniu súboru nástrojov EÚ na boj proti hybridným hrozbám a vykonávacích usmernení uvedených v záveroch Rady z 21. júna 2022 o rámci pre koordinovanú reakciu EÚ na hybridné kampane a aby ich následne používali v záujme plného uplatňovania uvedeného rámca najmä pri zvažovaní a príprave komplexnej a koordinovanej reakcie Únie na hybridné kampane a hybridné hrozby vrátane tých, ktoré sú namierené proti prevádzkovateľom kritickej infraštruktúry.

([12]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

Opatrenia na úrovni Únie

36. Komisia a vysoký predstaviteľ sa vyzývajú, aby vo vhodných prípadoch a v súlade so svojimi príslušnými úlohami a povinnosťami podľa práva Únie podporovali relevantné tretie krajiny s cieľom zvýšiť odolnosť kritickej infraštruktúry na ich území, a najmä kritickej infraštruktúry, ktorá je fyzicky prepojená s ich územím a územím členského štátu.

37. Komisia a vysoký predstaviteľ v súlade so svojimi príslušnými úlohami a povinnosťami podľa práva Únie posilnia koordináciu s NATO v oblasti odolnosti kritickej infraštruktúry spoločného záujmu prostredníctvom štruktúrovaného dialógu medzi EÚ a NATO o odolnosti pri plnom rešpektovaní právomocí Únie a členských štátov podľa zmlúv a kľúčových zásad, ktorými sa riadi spolupráca medzi EÚ a NATO, ktoré schválila Európska rada, najmä reciprocity, inkluzívnosti a autonómie rozhodovania. V tejto súvislosti sa v tejto spolupráci bude pokračovať v rámci štruktúrovaného dialógu medzi EÚ a NATO o odolnosti, ktorý je zakotvený v existujúcom mechanizme na vykonávanie spoločných vyhlásení na úrovni zamestnancov, pričom sa zabezpečí úplná transparentnosť a zapojenie všetkých členských štátov.

38. Komisia sa vyzýva, aby v potrebných a vhodných prípadoch zvážila účasť zástupcov relevantných tretích krajín v rámci spolupráce a výmeny informácií medzi členskými štátmi v oblasti odolnosti kritickej infraštruktúry, ktorá je fyzicky prepojená s územím členského štátu a územím tretej krajiny.

V Bruseli 8. decembra 2022

Za Radu
predseda
V. RAKUŠAN