EURÓPSKA
KOMISIA

V Štrasburgu 18. 10. 2022
COM(2022) 551 final

2022/0338 (NLE)

Návrh

ODPORÚČANIE RADY

týkajúce sa koordinovaného prístupu Únie k posilneniu odolnosti kritickej infraštruktúry

(Text s významom pre EHP)

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Bezpečnosť je základným cieľom Európskej únie. Hoci hlavnú zodpovednosť za ochranu občanov nesú členské štáty, kolektívne opatrenia na úrovni Únie významne prispievajú k bezpečnosti EÚ ako celku. Koordinácia pomáha posilniť odolnosť, zlepšiť ostražitosť a posilniť našu kolektívnu reakciu. V kontexte bezpečnostnej únie EÚ sa podnikli dôležité kroky na budovanie spôsobilostí a kapacít na predchádzanie mnohým bezpečnostným hrozbám, ich odhaľovanie a rýchlu reakciu na ne a na prepojenie aktérov vo verejnom a súkromnom sektore v spoločnom úsilí.

Aby bola EÚ pripravená na riešenie neustále sa meniacich hrozieb, je potrebná neustála ostražitosť a prispôsobovanie sa. Ruská útočná vojna proti Ukrajine priniesla nové riziká, často kombinované ako hybridná hrozba. Jedným z nich je riziko narušenia poskytovania základných služieb subjektmi prevádzkujúcimi kritickú infraštruktúru v Európe. Táto skutočnosť sa ešte viac zviditeľnila zrejmou sabotážou plynovodov Nord Stream a inými nedávnymi incidentmi. Spoločnosť sa vo veľkej miere spolieha na fyzickú aj digitálnu infraštruktúru a prerušenie základných služieb, či už prostredníctvom konvenčných fyzických útokov alebo kybernetických útokov alebo ich kombináciou, môže mať vážne dôsledky pre blaho občanov, naše hospodárstva a dôveru v naše demokratické systémy.

Zabezpečenie hladkého fungovania vnútorného trhu je ďalším kľúčovým cieľom EÚ, a to aj pokiaľ ide o základné služby poskytované subjektmi prevádzkujúcimi kritickú infraštruktúru. EÚ preto už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických subjektov, pokiaľ ide o kybernetické aj nekybernetické riziká.

Je naliehavo potrebné posilniť schopnosť EÚ čeliť potenciálnym útokom namiereným na kritickú infraštruktúru, a to najmä v samotnej EÚ, ale v prípade potreby aj v jej priamom susedstve.

Cieľom navrhovaného odporúčania Rady je zintenzívniť podporu EÚ zameranú na zvyšovanie odolnosti kritickej infraštruktúry a na zabezpečenie koordinácie na úrovni EÚ, pokiaľ ide o pripravenosť a reakciu. Jeho cieľom je maximalizovať a urýchliť prácu na ochrane tých aktív, zariadení a systémov, ktoré sú potrebné na fungovanie hospodárstva, a poskytovať základné služby na vnútornom trhu, ktoré občania nevyhnutne potrebujú, ako aj zmierniť vplyv akéhokoľvek útoku zaistením čo najrýchlejšej obnovy. Hoci by sa mala chrániť všetka takáto infraštruktúra, najvyššiu prioritu má v súčasnosti energetika, digitálna infraštruktúra, doprava a vesmír vzhľadom na ich obzvlášť horizontálny charakter pre spoločnosť a hospodárstvo a vzhľadom na súčasné posúdenia rizík.

EÚ zohráva osobitnú úlohu, pokiaľ ide o zabezpečenie odolnosti infraštruktúry, ktorá prekračuje pozemné alebo námorné hranice a ovplyvňuje záujmy viacerých členských štátov alebo ktorá sa využíva na poskytovanie základných služieb s cezhraničným dosahom. Kritická infraštruktúra s významom pre viaceré členské štáty sa však môže nachádzať samostatne v jednom členskom štáte alebo dokonca mimo územia členského štátu, napríklad v prípade podmorských káblov alebo potrubí. Jasná identifikácia kritickej infraštruktúry a subjektov, ktoré ju prevádzkujú, ako aj riziká, ktoré ich ohrozujú, a spoločný záväzok chrániť ich je v záujme všetkých členských štátov a EÚ ako celku.

Európsky parlament a Rada už dosiahli politickú dohodu o prehĺbení legislatívneho rámca pre EÚ s cieľom pomôcť posilniť odolnosť subjektov prevádzkujúcich kritickú infraštruktúru. V lete 2022 sa dosiahla dohoda o smernici o odolnosti kritických subjektov (ďalej len

„smernica CER“)[1] a o revidovanej smernici o bezpečnosti sietí a informačných systémov (ďalej len „smernica NIS2“)[2]. Obidve smernice budú predstavovať významné zintenzívnenie spôsobilostí v porovnaní s existujúcim legislatívnym rámcom – smernicou 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (ďalej len „smernica ECI“)[3] a smernicou Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“)[4]. Očakáva sa, že nové právne predpisy nadobudnú účinnosť koncom roka 2022 alebo začiatkom roka 2023 a členské štáty by mali dať ich transpozícii a ich uplatňovaniu prioritu, v súlade s právom Únie.

Vzhľadom na túto skutočnosť a vzhľadom na možnú naliehavosť riešenia hrozieb, ktoré vyplývajú z ruskej útočnej vojny proti Ukrajine, by sa kroky uvedené v nových právnych predpisoch mali, ak je to možné a vhodné, uskutočňovať už od dnešného dňa. Zintenzívnenie vzájomnej spolupráce realizované už teraz by tiež pomohlo vytvoriť impulz pre účinné vykonávanie predpisov až budú plne účinné.

Výsledkom by bolo, že by už teraz došlo k prekročeniu súčasných rámcov, a to tak z hľadiska hĺbky činnosti, ako aj z hľadiska rozsahu zahrnutých odvetví. V novej smernici CER sa zavádza nový rámec spolupráce, ako aj povinnosti členských štátov a kritických subjektov zamerané na posilnenie fyzickej nekybernetickej odolnosti – voči prírodným hrozbám a hrozbám spôsobeným ľudskou činnosťou – tých subjektov, ktoré poskytujú základné služby na vnútornom trhu, pričom sa uvádza jedenásť sektorov[5]. Smernicou NIS2 sa zavedie široké odvetvové pokrytie povinností v oblasti kybernetickej bezpečnosti. To bude zahŕňať novú požiadavku, aby členské štáty v prípade potreby zahrnuli podmorské káble do svojich stratégií kybernetickej bezpečnosti.

V právnych predpisoch sa vyžaduje, aby Komisia prevzala významnú koordinačnú úlohu. Podľa smernice CER má Komisia podpornú úlohu, ktorá sa má vykonávať s podporou a zapojením skupiny pre odolnosť kritických subjektov (CERG) zriadenej uvedenou smernicou, a mala by dopĺňať činnosti členských štátov vypracúvaním najlepších postupov, usmerňovacích materiálov a metodík. Pokiaľ ide o kybernetickú bezpečnosť, Rada už vo svojich záveroch o prístupe EÚ ku kybernetickej bezpečnosti z leta 2022 vyzvala Komisiu, vysokého predstaviteľa a skupinu pre spoluprácu NIS, aby pracovali na posúdení rizík a scenároch z hľadiska kybernetickej bezpečnosti. Takáto koordinácia môže inšpirovať prístup týkajúci sa ďalšej kľúčovej kritickej infraštruktúry.

Predsedníčka von der Leyenová 5. októbra 2022 predstavila 5-bodový plán, v ktorom sa stanovuje koordinovaný prístup k práci, ktorú je potrebné vykonať. Hlavnými prvkami sú: zlepšenie pripravenosti; spolupráca s členskými štátmi s cieľom uskutočniť záťažové testy ich kritickej infraštruktúry, a to najprv v odvetví energetiky a následne v ďalších vysokorizikových odvetviach; zvýšenie kapacity reakcie najmä prostredníctvom mechanizmu Únie v oblasti civilnej ochrany; dobré využívanie satelitnej kapacity na odhaľovanie potenciálnych hrozieb; a posilnenie spolupráce s NATO a kľúčovými partnermi v oblasti odolnosti kritickej infraštruktúry. V 5-bodovom pláne sa zdôraznila hodnota anticipácie právnych predpisov, ktoré už majú politickú dohodu.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 Ú. v. EÚ L 345, 23.12.2008.
4 Ú. v. EÚ L194, 19.7.2016.
5 Energetika, doprava, digitálna infraštruktúra, bankovníctvo, infraštruktúra finančného trhu, zdravotníctvo, pitná a odpadová voda, verejná správa, vesmír a potraviny.

V navrhovanom odporúčaní Rady sa víta tento prístup spočívajúci v štruktúrovaní podpory pre členské štáty a koordinácii ich úsilia v oblasti zvyšovania informovanosti o rizikách a v oblasti pripravenosti a reakcie na súčasné hrozby. V tejto súvislosti sa zvolávajú zasadnutia expertov s cieľom diskutovať o odolnosti subjektov prevádzkujúcich kritickú infraštruktúru v očakávaní nadobudnutia účinnosti smernice CER a ňou zriadenej skupiny CERG.

Zásadný význam bude mať posilnená spolupráca s kľúčovými partnermi a susednými a inými relevantnými tretími krajinami zameraná na odolnosť subjektov prevádzkujúcich kritickú infraštruktúru, a to najmä prostredníctvom štruktúrovaného dialógu medzi EÚ a NATO o odolnosti.

Toto odporúčanie sa zameriava na posilnenie schopnosti Únie predvídať nové hrozby vyplývajúce z ruskej útočnej vojny proti Ukrajine, predchádzať im a reagovať na ne. Navrhované odporúčania sa preto zameriavajú na riešenie bezpečnostných rizík a hrozieb pre kritickú infraštruktúru. Treba však poznamenať, že nedávne udalosti zdôraznili aj naliehavú potrebu venovať zvýšenú pozornosť vplyvom zmeny klímy na kritickú infraštruktúru a služby, napríklad pokiaľ ide o sezónne ohrozené a nepredvídateľné dodávky vody na chladenie pre jadrové elektrárne, ďalej pokiaľ ide o vodnú energiu a vnútrozemskú plavbu, alebo riziko materiálnych škôd na dopravnej infraštruktúre, čo môže spôsobiť vážne narušenie základných služieb. Tieto obavy sa budú ďalej riešiť prostredníctvom príslušných právnych predpisov a koordinácie.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Tento návrh odporúčania Rady je plne v súlade so súčasným a budúcim právnym rámcom pre odolnosť subjektov prevádzkujúcich kritickú infraštruktúru, smernicou ECI a smernicou CER, keďže je okrem iného zameraný na uľahčenie spolupráce medzi členskými štátmi v tejto oblasti a podporu konkrétnych opatrení na zvýšenie odolnosti voči súčasným bezprostredným hrozbám namiereným voči subjektom prevádzkujúcim kritickú infraštruktúru v EÚ.

Takisto dopĺňa a anticipuje smernicu CER tým, že už teraz vyzýva členské štáty, aby priorizovali včasnú transpozíciu smernice, a to prostredníctvom spolupráce formou zasadnutí expertov zvolaných v rámci 5-bodového plánu oznámeného Komisiou a prostredníctvom zamerania sa na koordináciu cesty k spoločnému prístupu k vykonávaniu záťažových testov kritickej infraštruktúry v EÚ.

Návrh je takisto v súlade so smernicou NIS a chystanou smernicou NIS2, ktorou sa zruší smernica NIS, a to tým, že sa v ňom vyzýva k skorému začatiu práce na vykonávaní a transpozícii. Zohľadňuje sa v ňom aj spoločná výzva z Nevers z marca 2022, ako aj závery Rady o prístupe EÚ ku kybernetickej bezpečnosti z mája 2022, pokiaľ ide o žiadosť členských štátov adresovanú Komisii, aby vypracovala posúdenia rizík a rizikové scenáre.

Návrh je takisto v súlade s politikou EÚ v oblasti civilnej ochrany, v rámci ktorej môžu členské štáty a tretie krajiny v prípade výrazného narušenia fungovania kritickej infraštruktúry/kritických subjektov požiadať o pomoc prostredníctvom Koordinačného centra pre reakcie na núdzové situácie (ERCC) v rámci mechanizmu Únie v oblasti civilnej ochrany (UCPM). V prípade aktivácie mechanizmu Únie v oblasti civilnej ochrany môže ERCC koordinovať a spolufinancovať nasadenie základného vybavenia, materiálov a odborných znalostí dostupných v členských štátoch (čiastočne v kontexte európskeho zoskupenia v oblasti civilnej ochrany) a v rámci rescEU pre postihnutú krajinu. Pomoc, ktorú možno poskytnúť na požiadanie, zahŕňa napríklad palivo, generátory, elektrickú infraštruktúru, kapacitu prístreškov, kapacitu čistenia vody a núdzové zdravotnícke kapacity.

Návrh je takisto v súlade s *acquis* EÚ v oblasti bezpečnosti dodávok energie.

Sektor jadrovej energie nie je v navrhovanom odporúčaní Rady osobitne zahrnutý, s výnimkou napríklad súvisiacej infraštruktúry (ako sú prenosové vedenia do jadrových elektrární), ktorá môže mať vplyv na bezpečnosť dodávok. Na konkrétne jadrové prvky sa vzťahujú príslušné právne predpisy v oblasti jadrovej energie podľa Zmluvy o Euratome a/alebo vnútroštátnych právnych predpisov[6]. Na základe ponaučení z havárie vo Fukušime sa posilnili európske právne predpisy v oblasti jadrovej bezpečnosti a vnútroštátne orgány preto musia vykonávať pravidelné preskúmania bezpečnosti každého zariadenia s cieľom zabezpečiť trvalý súlad s najprísnejšími bezpečnostnými požiadavkami a identifikovať ďalšie zlepšenia v oblasti bezpečnosti, ako aj šesť každoročných tematických partnerských hodnotení na úrovni EÚ.

Stratégia námornej bezpečnosti EÚ[7] a jej akčný plán[8] zdôrazňujú meniacu sa povahu hrozieb v námornej oblasti a vyzývajú na obnovenie záväzku chrániť kritickú námornú infraštruktúru vrátane podmorskej, a najmä infraštruktúru námornej dopravy a energetickú a komunikačnú infraštruktúru, a to aj zvyšovaním informovanosti o námornej doprave prostredníctvom lepšej interoperability a zjednodušenej výmeny informácií.

Návrh je tiež v súlade s inými príslušnými odvetvovými právnymi predpismi. Vykonávanie tohto odporúčania by preto malo byť v súlade s osobitnými opatreniami, ktoré regulujú alebo v budúcnosti môžu regulovať určité aspekty odolnosti subjektov pôsobiacich v dotknutých odvetviach, ako je doprava. Zahŕňa to aj ďalšie relevantné iniciatívy, ako je pohotovostný plán pre dopravu[9] alebo plán pre nepredvídané udalosti na zabezpečenie dodávok potravín a potravinovej bezpečnosti v čase krízy[10] a súvisiaci Európsky mechanizmus pripravenosti a reakcie na krízu potravinovej bezpečnosti. Z všeobecnejšieho pohľadu by sa odporúčanie malo vykonávať v plnom súlade so všetkými uplatniteľnými pravidlami práva EÚ vrátane tých, ktoré sú stanovené v smernici ECI a smernici NIS.

Návrh je takisto v súlade so Strategickým kompasom pre bezpečnosť a obranu, v ktorom sa zdôraznila potreba podstatne zvýšiť odolnosť a schopnosť bojovať proti hybridným hrozbám a kybernetickým útokom, ako aj potreba posilniť odolnosť partnerských krajín a spolupracovať s NATO. Je tiež v súlade s rámcom pre koordinovanú reakciu EÚ na hybridné hrozby a kampane, ktoré majú vplyv na EÚ, členské štáty a partnerov[11].

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Návrh vychádza z článku 114 Zmluvy o fungovaní Európskej únie (ZFEÚ), ktorý zahŕňa aproximáciu právnych predpisov na zlepšenie vnútorného trhu, spolu s článkom 292 ZFEÚ. Je to odôvodnené skutočnosťou, že cieľom navrhovaného odporúčania Rady je predovšetkým anticipovať opatrenia stanovené v nových smerniciach CER a NIS2, ktoré sú takisto založené na článku 114 ZFEÚ. V súlade s logikou odôvodňujúcou použitie uvedeného článku ako právneho základu pre uvedené smernice sú potrebné opatrenia EÚ na zabezpečenie hladkého fungovania vnútorného trhu, najmä vzhľadom na cezhraničnú povahu a rozsah dotknutých služieb a možné dôsledky v prípade narušení, ako aj súčasné a vznikajúce vnútroštátne

6 Odôvodnenie 9 smernice Rady 2008/114/ES (smernica ECI).
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.
11 Závery Rady Európskej únie 10016/22 z 21. júna 2022.

opatrenia zamerané na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru používanú na poskytovanie základných služieb na vnútornom trhu.

- **Subsidiarita (v prípade inej ako výlučnej právomoci)**

Ďalší postup na európskej úrovni v oblasti odolnosti subjektov prevádzkujúcich kritickú infraštruktúru je odôvodnený vzhľadom na vzájomnú závislosť, cezhraničnú povahu vzťahov medzi prevádzkou kritickej infraštruktúry a poskytovanými základnými službami, ako aj na potrebu jednotnejšieho a koordinovanejšieho európskeho prístupu s cieľom zabezpečiť dostatočnú odolnosť dotknutých subjektov v súčasnom geopolitickom kontexte. Mnohé zo spoločných výziev, ako je zjavná sabotáž plynovodov North Stream, sa riešia v prvom rade prostredníctvom vnútroštátnych opatrení alebo opatreniami subjektov prevádzkujúcich kritickú infraštruktúru; podpora EÚ, v prípade potreby aj príslušných agentúr, je však potrebná na posilnenie odolnosti, zlepšenie ostražitosti a posilnenie kolektívnej reakcie EÚ.

- **Proporcionalita**

Súčasný návrh je v súlade so zásadou proporcionality stanovenou v článku 5 ods. 4 Zmluvy o Európskej únii.

Ani obsah, ani forma tohto navrhovaného odporúčania Rady nepresahujú rámec nevyhnutný na dosiahnutie jeho cieľov. Navrhované opatrenia sú primerané sledovaným cieľom, keďže rešpektujú výsady a povinnosti členských štátov podľa vnútroštátneho práva.

V návrhu sa zohľadňuje potenciálny diferencovaný prístup, ktorý odráža rôznu vnútornú realitu členských štátov, pokiaľ ide o pripravenosť a reakciu na fyzické hrozby pre kritickú infraštruktúru.

- **Výber nástroja**

V záujme dosiahnutia uvedených cieľov sa v ZFEÚ, a to najmä v jeho článku 292, stanovuje, že Rada prijíma odporúčania na základe návrhu Komisie. Odporúčanie Rady je v tomto prípade vhodným nástrojom, a to aj so zreteľom na súčasný legislatívny kontext, ako je vysvetlené vyššie. Ako právny akt, hoci nezáväzný, signalizuje odporúčanie Rady záväzok členských štátov prijať zahrnuté opatrenia a poskytuje silný politický základ pre spoluprácu v týchto oblastiach pri plnom rešpektovaní právomocí členských štátov.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- **Konzultácie so zainteresovanými stranami**

Pri vypracúvaní tohto návrhu sa zohľadnili názory expertov členských štátov, ktoré vyjadrili na zasadnutí 12. októbra 2022. Dosiahol sa široký konsenzus o užitočnosti väčšej koordinácie na úrovni Únie, pokiaľ ide o pripravenosť a reakciu v súčasnom kontexte hrozieb a o anticipácii určitých prvkov smernice CER pred jej formálnym prijatím. Členské štáty vyjadrili ochotu vymieňať si skúsenosti a najlepšie postupy týkajúce sa opatrení a metodík na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru. Členské štáty tiež vyjadrili otvorenosť voči koordinovanému prístupu k záťažovým testom subjektov prevádzkujúcich kritickú infraštruktúru na dobrovoľnom základe a na základe spoločných zásad. Členské štáty uviedli, že subjekty prevádzkujúce kritickú infraštruktúru v odvetviach energetiky, digitálnej infraštruktúry a dopravy by sa mali na účely tohto odporúčania považovať za prioritu, a to najmä tie, ktoré sú relevantné pre viaceré členské štáty. Členské štáty tiež uvítali zámer Komisie zvolať v nadchádzajúcich týždňoch ďalšie zasadnutia expertov z členských štátov.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Obsah návrhu odporúčania Rady:

– V kapitole I sa stanovuje cieľ návrhu, uvádza sa tu, čoho sa týka, a je tu stanovená priorizácia odporúčaných opatrení.

– Kapitola II sa zameriava na opatrenia, ktoré by sa mali prijať v súvislosti s posilnenou pripravenosťou na úrovni Únie, ako aj na úrovni členských štátov.

– Kapitola III sa vzťahuje na posilnenú reakciu na úrovni EÚ, ako aj na úrovni členských štátov.

– Kapitola IV sa zaoberá medzinárodnou spoluprácou a opatreniami, ktoré by sa mali prijať na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru.

2022/0338 (NLE)

Návrh

ODPORÚČANIE RADY

týkajúce sa koordinovaného prístupu Únie k posilneniu odolnosti kritickej infraštruktúry

(Text s významom pre EHP)

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej články 114 a 292,

so zreteľom na návrh Európskej komisie,

keďže:

(1) Únia zohráva osobitnú úlohu, pokiaľ ide o infraštruktúru, ktorá prekračuje hranice a má vplyv na záujmy viacerých členských štátov alebo ktorú subjekty inak používajú na poskytovanie základných služieb s cezhraničným dosahom. Takéto poskytovanie služieb a kritická infraštruktúra s významom pre viaceré členské štáty sa však môžu nachádzať len v jednom členskom štáte alebo dokonca mimo územia členských štátov, napríklad v prípade podmorských káblov alebo potrubí. Jasná identifikácia takejto infraštruktúry a subjektov a hrozieb, ktorým čelia, ako aj spoločný záväzok chrániť ich je v záujme všetkých členských štátov a EÚ ako celku.

(2) Ochranu kritickej infraštruktúry v dvoch odvetviach v súčasnosti upravuje smernica Rady 2008/114/ES[12]. Uvedenou smernicou sa stanovuje postup identifikácie a označenia európskych kritických infraštruktúr (ECI) a spoločný prístup k zhodnoteniu potreby zlepšiť ochranu týchto infraštruktúr s cieľom prispieť k ochrane obyvateľov. Vzťahuje sa na odvetvia energetiky a dopravy. Aby sa zlepšila odolnosť kritických subjektov a základných služieb, ktoré poskytujú, a kritickej infraštruktúry, ktorú používajú, zákonodarca Únie v súčasnosti prijíma novú smernicu o odolnosti kritických subjektov[13] (ďalej len „smernica CER“), ktorá nahradí smernicu 2008/114/ES a bude sa vzťahovať na viac odvetví vrátane digitálnej infraštruktúry.

(3) Okrem toho sa smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii[14] zameriava na kybernetické hrozby. Uvedenú smernicu nahradí nová smernica o opatreniach na zabezpečenie vysokej spoločnej

[12] 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).

[13] COM(2020) 829.

[14] 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).

úrovne kybernetickej bezpečnosti v Únii[15] (ďalej len „smernica NIS2“), ktorá je takisto v procese prijímania zákonodarcom Únie.

(4) Vzhľadom na rýchlo sa vyvíjajúcu panorámu hrozieb, najmä v súvislosti so zjavnou sabotážou plynárenskej infraštruktúry Nord Stream 1 a 2, čelia subjekty prevádzkujúce kritickú infraštruktúru osobitným výzvam, pokiaľ ide o ich odolnosť voči nepriateľským činom a iným hrozbám spôsobeným ľudskou činnosťou, a zároveň dochádza k nárastu výziev vyplývajúcich z prírodných faktorov a zo zmeny klímy, ktoré môžu spolupôsobiť s nepriateľskými činmi. Preto musia uvedené subjekty prijať s podporou členských štátov vhodné opatrenia na zvýšenie odolnosti. Tieto opatrenia by sa mali prijať a táto podpora by sa mala poskytovať nad rámec opatrení podľa smernice 2008/114/ES a smernice (EÚ) 2016/1148, a to ešte pred prijatím, nadobudnutím účinnosti a transpozíciou nových smerníc CER a NIS2.

(5) Únia a členské štáty sa vyzývajú, aby do prijatia, nadobudnutia účinnosti a transpozície uvedených nových smerníc v súlade s právom Únie využili všetky dostupné nástroje na dosiahnutie pokroku a pomáhali posilniť fyzickú a kybernetickú odolnosť dotknutých subjektov a kritickej infraštruktúry, ktorú prevádzkujú, na poskytovanie základných služieb na vnútornom trhu, t. j. služieb, ktoré sú kľúčové pre zachovanie životne dôležitých spoločenských funkcií, hospodárskych činností, verejného zdravia a bezpečnosti alebo životného prostredia. V tejto súvislosti by sa pojem odolnosti mal chápať ako schopnosť subjektu predchádzať udalostiam, ktoré by mohli významne narušiť alebo významne narúšajú poskytovanie príslušných základných služieb, chrániť sa pred týmito udalosťami, reagovať na ne, odolávať im, zmierňovať ich, absorbovať ich, prispôsobovať sa im a zotavovať sa z nich.

(6) S cieľom zabezpečiť prístup, ktorý je účinný a čo najviac konzistentný s novou smernicou CER, by sa opatrenia uvedené v tomto odporúčaní mali vzťahovať na infraštruktúru, ktorú členský štát označil za kritickú infraštruktúru, a to tak na vnútroštátnu kritickú infraštruktúru, ako aj na európsku kritickú infraštruktúru, bez ohľadu na to, či subjekt prevádzkujúci kritickú infraštruktúru už bol označený za kritický subjekt podľa uvedenej novej smernice. Na účely tohto odporúčania by sa pojem „kritická infraštruktúra“ mal chápať v tomto zmysle.

(7) Vzhľadom na existujúce hrozby by sa opatrenia na zvýšenie odolnosti mali prioritne prijať v kľúčových odvetviach energetiky, digitálnej infraštruktúry, dopravy a vesmíru a takéto opatrenia by sa mali zamerať na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru voči rizikám spôsobeným ľudskou činnosťou. Pokiaľ ide o vnútroštátnu kritickú infraštruktúru, vzhľadom na možné dôsledky v prípade naplnenia rizík by sa mala uprednostniť infraštruktúra, ktorá má cezhraničný význam.

(8) Cieľom opatrení stanovených v tomto odporúčaní je preto najmä doplnenie nových smerníc CER a NIS2 založených na článku 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), a to anticipáciou a rozšírením opatrení, ktoré sa týmito novými smernicami stanovia. Preto a vzhľadom na cezhraničnú povahu a význam príslušných základných služieb a kritickej infraštruktúry a na existujúce a vznikajúce rozdiely medzi vnútroštátnymi právnymi predpismi, ktoré narúšajú vnútorný trh, je vhodné, aby sa aj toto odporúčanie zakladalo na článku 114 ZFEÚ v spojení s článkom 292 ZFEÚ.

---

[15] COM(2020) 823.

(9) Vykonávanie tohto odporúčania by sa nemalo chápať tak, že ovplyvňuje súčasné a budúce požiadavky práva Únie týkajúce sa určitých aspektov odolnosti dotknutých subjektov, a malo by byť s týmito požiadavkami v súlade. Takéto požiadavky sú stanovené vo všeobecných nástrojoch, ako je smernica 2008/114/ES a smernica (EÚ) 2016/1148 a nové smernice CER a NIS2, ktoré ich nahrádzajú, ale aj v určitých odvetvových nástrojoch, napríklad v oblasti dopravy, kde Komisia okrem iného prijala pohotovostný plán pre dopravu[16]. V súlade so zásadou lojálnej spolupráce by sa toto odporúčanie malo vykonávať pri plnom vzájomnom rešpektovaní a pomoci.

(10) Komisia 5. októbra 2022 oznámila päťbodový plán, v ktorom sa stanovuje koordinovaný prístup k riešeniu budúcich výziev, ktorý zahŕňa prácu na pripravenosti na základe novej smernice CER ešte pred jej prijatím a nadobudnutím účinnosti a ktorého súčasťou je aj spolupráca s členskými štátmi s cieľom vykonávať záťažové testy subjektov prevádzkujúcich kritickú infraštruktúru na základe spoločných zásad, počnúc odvetvím energetiky. Toto odporúčanie, ktoré k uvedenému plánu prispeje, víta navrhovaný prístup a stanovuje, ako ho možno premietnuť do konkrétnych opatrení.

(11) Vzhľadom na rýchlo sa vyvíjajúcu panorámu hrozieb a súčasné rizikové prostredie charakterizované rizikami spôsobenými ľudskou činnosťou, najmä pokiaľ ide o kritickú infraštruktúru s cezhraničným významom, je nevyhnutné mať presný, aktuálny a úplný obraz o najdôležitejších rizikách, ktorým subjekty prevádzkujúce kritickú infraštruktúru čelia. Členské štáty by preto mali prijať potrebné opatrenia na vykonanie alebo aktualizáciu svojich posúdení týchto rizík. Aj keď sa toto odporúčanie zameriava na bezpečnostné riziká, malo by sa okrem toho pokračovať v úsilí o riešenie zmeny klímy a environmentálnych rizík, najmä ak prírodné javy môžu ďalej zhoršovať riziká spôsobené ľudskou činnosťou.

(12) Vzhľadom na túto panorámu hrozieb by sa členské štáty mali vyzvať, aby čo najskôr prijali vhodné opatrenia na zvýšenie odolnosti kritickej infraštruktúry, a to aj nad rámec uvedených posúdení rizík, ktoré sa budú následne podľa novej smernice CER vyžadovať.

(13) V rámci vykonávania päťbodového plánu oznámeného Komisiou treba činnosť koordinovať zvolaním národných expertov, ktorí by sa mali spojiť ešte pred zriadením skupiny pre odolnosť kritických subjektov na základe novej smernice CER, aby sa umožnila spolupráca medzi členskými štátmi a výmena informácií, pokiaľ ide o odolnosť subjektov prevádzkujúcich kritickú infraštruktúru. To by malo zahŕňať spoluprácu a výmenu informácií týkajúcich sa činností, ako je identifikácia kritických subjektov a infraštruktúry, príprava a podpora spoločného súboru zásad na vykonávanie záťažových testov a získavanie spoločných poznatkov zo záťažových testov, identifikácia zraniteľných miest a možných spôsobilostí. Tieto procesy by mali byť prínosom aj pre odolnosť subjektov prevádzkujúcich kritickú infraštruktúru voči klimatickým a environmentálnym rizikám. Táto činnosť by umožnila aj spoločnú priorizáciu práce na záťažových testoch s dôrazom na odvetvia energetiky, digitálnej infraštruktúry, dopravy a vesmíru. Komisia už začala zvolávať týchto odborníkov a uľahčovať ich prácu a má v úmysle v tom ďalej pokračovať. Po nadobudnutí účinnosti novej smernice o CER a zriadení skupiny pre odolnosť kritických subjektov by táto skupina mala pokračovať v takejto anticipačnej práci v súlade so svojimi úlohami podľa smernice CER.

[16] COM(2022) 211.

(14) Záťažové testy by sa mali doplniť vypracovaním koncepcie pre incidenty a krízy v oblasti kritickej infraštruktúry, v ktorej sa opíšu a stanovia ciele a spôsoby spolupráce medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami EÚ pri reakcii na incidenty namierené proti kritickej infraštruktúre, a to najmä pokiaľ vedú k závažnému narušeniu poskytovania základných služieb na vnútornom trhu. Táto koncepcia by mala pri koordinácii reakcie vychádzať z existujúcich integrovaných dojednaní o politickej reakcii na krízu (IPCR), mala by fungovať súdržne s koncepciou pre kybernetické incidenty veľkého rozsahu a dopĺňať ju a mala by stanovovať aj dohodu o kľúčových posolstvách v rámci komunikácie s verejnosťou, keďže krízová komunikácia zohráva dôležitú úlohu pri zmierňovaní negatívnych účinkov incidentov a kríz v oblasti kritickej infraštruktúry.

(15) S cieľom zabezpečiť koordinovanú a účinnú reakciu na súčasné a predpokladané hrozby bude Komisia členským štátom poskytovať ďalšiu podporu v súvislosti so zvyšovaním odolnosti voči týmto hrozbám, ktorej súčasťou bude poskytovanie relevantných informácií vo forme brífingov, príručiek a usmernení, propagovanie využívania výskumných a inovačných projektov financovaných Úniou, prijímanie potrebných anticipačných opatrení a optimalizácia využívania prostriedkov Únie v oblasti dohľadu. Európska služba pre vonkajšiu činnosť by mala poskytovať posúdenia hrozieb, najmä prostredníctvom Spravodajského a situačného centra EÚ.

(16) Podporu v záležitostiach súvisiacich s odolnosťou by mali poskytovať aj agentúry Únie relevantné pre dané odvetvia a ďalšie relevantné subjekty, pokiaľ to umožňujú ich mandáty stanovené v príslušných nástrojoch práva Únie. Konkrétne Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) by mohla byť nápomocná v otázkach kybernetickej bezpečnosti, Európska námorná bezpečnostná agentúra (EMSA) by mohla byť nápomocná svojimi odbornými znalosťami pri podpore členských štátov prostredníctvom svojej služby námorného dozoru v záležitostiach súvisiacich s námornou bezpečnosťou a ochranou, Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva (EUROPOL) by mohla poskytovať podporu v súvislosti so zhromažďovaním informácií a vyšetrovaniami pri cezhraničných opatreniach na presadzovanie práva, zatiaľ čo Agentúra Európskej únie pre vesmírny program (EUSPA) a Satelitné stredisko Európskej únie (SatCen) môžu byť nápomocné prostredníctvom operácií v rámci Vesmírneho programu Únie.

(17) Aj keď hlavnú zodpovednosť za zaistenie bezpečnosti kritickej infraštruktúry a dotknutých subjektov nesú členské štáty, je vhodná zvýšená koordinácia na úrovni Únie, najmä vzhľadom na hrozby, ktoré môžu mať dosah na viaceré členské štáty súčasne, ako je ruská útočná vojna proti Ukrajine, alebo ktoré môžu ovplyvniť odolnosť a dobré fungovanie hospodárstva, jednotného trhu a spoločností Únie.

(18) Toto odporúčanie nezahŕňa poskytovanie informácií, ktorých zverejnenie je v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

(19) Vzhľadom na rastúcu vzájomnú závislosť fyzických a digitálnych infraštruktúr môžu škodlivé kybernetické činnosti zamerané na kritické oblasti viesť k narušeniu alebo poškodeniu fyzickej infraštruktúry, zatiaľ čo sabotáž fyzickej infraštruktúry môže znemožniť prístup k digitálnym službám. S ohľadom na zvýšenú hrozbu, ktorú predstavujú sofistikované hybridné útoky, by členské štáty mali tieto aspekty zahrnúť aj do svojej práce pri vykonávaní tohto odporúčania. Vzhľadom na vzájomné prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou prevádzkovateľov je dôležité, aby sa príprava transpozície a uplatňovania novej

smernice NIS2 začala čo najskôr a aby súbežne prebiehala takáto príprava aj v rámci novej smernice CER.

(20) Okrem zlepšenia pripravenosti je takisto dôležité posilniť schopnosť rýchlej a účinnej reakcie v prípade, že sa naplnia riziká ovplyvňujúce poskytovanie základných služieb subjektmi prevádzkujúcimi kritickú infraštruktúru. Toto odporúčanie by preto malo obsahovať opatrenia, ktoré by sa mali prijať tak na úrovni členských štátov, ako aj na úrovni Únie, vrátane posilnenej spolupráce a výmeny informácií v kontexte mechanizmu Únie v oblasti civilnej ochrany a využívania relevantných prostriedkov Vesmírneho programu Únie.

(21) Na základe výzvy Rady uvedenej v jej záveroch o prístupe EÚ ku kybernetickej bezpečnosti[17] Komisia, vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) a skupina pre spoluprácu zriadená smernicou (EÚ) 2016/1148 (skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, ďalej len „skupina pre spoluprácu NIS“) v koordinácii s príslušnými civilnými a vojenskými orgánmi a agentúrami a existujúcimi sieťami vrátane siete EU-CyCLONe v súčasnosti vykonávajú hodnotenie rizík a vypracúvajú scenáre rizík z hľadiska kybernetickej bezpečnosti v situácii hrozby alebo možného útoku voči členským štátom alebo partnerským krajinám. Táto činnosť sa zameriava na kritické odvetvia vrátane energetiky, digitálnej infraštruktúry, dopravy a vesmíru.

(22) V spoločnej ministerskej výzve z Nevers[18] a v záveroch Rady o prístupe EÚ ku kybernetickej bezpečnosti sa takisto vyzvalo na posilnenie odolnosti komunikačnej infraštruktúry a sietí v Únii, a to prostredníctvom odporúčaní pre členské štáty a Komisiu na základe posúdenia rizika. Toto posúdenie rizík v súčasnosti vykonáva skupina pre spoluprácu NIS s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie (BEREC). Posúdenie rizík a analýza nedostatkov sa zameriavajú na riziká kybernetických útokov v rôznych pododvetviach komunikačných infraštruktúr vrátane pevných a mobilných infraštruktúr, satelitov, podmorských káblov, internetového smerovania atď., a poskytujú tak základ pre činnosť v rámci tohto odporúčania. Toto posúdenie rizík bude podkladom pre prebiehajúce medziodvetvové hodnotenie kybernetických rizík a scenáre požadované Radou v jej záveroch z 23. mája 2022.

(23) Obe uvedené činnosti budú konzistentné a koordinované s vytváraním scenárov zameraných na civilnú ochranu v kontexte širokej škály prírodných katastrof a katastrof spôsobených ľudskou činnosťou vrátane kybernetickobezpečnostných udalostí a ich reálneho vplyvu. Tieto scenáre v súčasnosti vypracúva Komisia a členské štáty na základe rozhodnutia Európskeho parlamentu a Rady č. 1313/2013/EÚ[19]. V záujme efektívnosti, účinnosti a konzistentnosti by sa toto odporúčanie malo vykonať so zreteľom na výsledky uvedených činností.

(24) V súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G[20] sa stanovujú príslušné opatrenia a plány na zmiernenie rizík s cieľom posilniť bezpečnosť sietí 5G. Vzhľadom na závislosť mnohých základných služieb od sietí 5G a na vzájomne

---

17 Prístup ku kybernetickej bezpečnosti: Rada schválila závery – Consilium (europa.eu).

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

prepojenú povahu digitálnych ekosystémov je nevyhnutné, aby všetky členské štáty urýchlene vykonali opatrenia odporúčané v súbore nástrojov, a najmä aby uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov kľúčových aktív, ktoré sú v koordinovanom posúdení rizík na úrovni EÚ vymedzené ako kritické a citlivé.

(25) S cieľom okamžite posilniť pripravenosť a schopnosť reagovať na závažné kybernetické incidenty Komisia vytvorila krátkodobý program na podporu členských štátov prostredníctvom dodatočných finančných prostriedkov pridelených agentúre ENISA. Podporné služby v rámci programu budú zahŕňať opatrenia v oblasti pripravenosti, ako je penetračné testovanie kritických subjektov s cieľom identifikovať zraniteľné miesta. Posilnia sa tým aj možnosti pomoci členským štátom v prípade závažného incidentu s vplyvom na kritické subjekty. Ide o prvý krok v súlade so závermi Rady o prístupe 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 tieto príležitosti v súlade s uplatniteľnými požiadavkami v plnej miere využiť.

(26) Globálna podmorská dátová a elektronická komunikačná káblová sieť má zásadný význam pre globálnu konektivitu a 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 digitálnych a fyzických infraštruktúr, ktoré sú pre digitálne služby nevyhnutné, osobitnými posúdeniami rizík a možnosťami zmierňujúcich opatrení týkajúcich sa podmorských káblov. Komisia preto na tento účel vykoná štúdie a svoje zistenia poskytne členským štátom.

(27) Riziká súvisiace s digitálnou infraštruktúrou môžu mať vplyv aj na prioritné odvetvia energetiky a dopravy identifikované v tomto odporúčaní. Takýto vplyv môže existovať napríklad v súvislosti s energetickými technológiami zahŕňajúcimi digitálne komponenty. Bezpečnosť súvisiacich dodávateľských reťazcov je dôležitá pre kontinuitu poskytovania základných služieb a pre strategickú kontrolu kritickej infraštruktúry prevádzkovanej subjektmi v odvetví energetiky. Uvedené okolnosti by sa mali zohľadniť pri prijímaní opatrení na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru v súlade s týmto odporúčaním.

(28) Vzhľadom na rastúci význam vesmírnej infraštruktúry a vesmírnych služieb pre činnosti súvisiace s bezpečnosťou je nevyhnutné zabezpečiť odolnosť a ochranu vesmírnych prostriedkov a služieb v EÚ, ale v rámci tohto odporúčania takisto štruktúrovanejšie využívať vesmírne údaje a služby poskytované vesmírnymi systémami a programami na dohľad nad kritickou infraštruktúrou v iných odvetviach a na ochranu tejto infraštruktúry. V pripravovanej stratégii EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu sa v tejto súvislosti navrhnú vhodné opatrenia, ktoré by sa mali zohľadniť pri vykonávaní tohto odporúčania.

(29) Na účinné riešenie rizík, ktoré ohrozujú odolnosť subjektov prevádzkujúcich kritickú infraštruktúru buď v Únii, v príslušných tretích krajinách, alebo v medzinárodných vodách, je takisto nevyhnutná spolupráca na medzinárodnej úrovni. Členské štáty by sa preto mali vyzvať, aby spolupracovali s Komisiou a vysokým predstaviteľom s cieľom podniknúť určité kroky na tento účel, pričom sa rozumie, že všetky takéto

kroky sa smú prijať len v súlade s ich príslušnými úlohami a povinnosťami podľa práva Únie, najmä podľa ustanovení zmlúv EÚ týkajúcich sa vonkajších vzťahov.

(30) Ako sa uvádza v oznámení „Príspevok Komisie k európskej obrane“[21], 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“[22], 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.

(31) Stratégia námornej bezpečnosti EÚ z roku 2014 a jej akčný plán obsahovali výzvu na zvýšenú ochranu kritickej námornej infraštruktúry vrátane podmorskej, a najmä infraštruktúry námornej dopravy a energetickej a komunikačnej infraštruktúry, a to aj zvyšovaním informovanosti o námornej doprave prostredníctvom lepšej interoperability a zjednodušenej výmeny informácií. Táto stratégia a akčný plán sa v súčasnosti aktualizujú a budú zahŕňať posilnené opatrenia zamerané na ochranu kritickej námornej infraštruktúry. Uvedené opatrenia by mali byť podkladom pre toto odporúčanie a dopĺňať ho.

(32) Členské štáty by mali v plnej miere využiť potenciál programu Únie pre výskum v oblasti bezpečnosti a jeho prioritné zameranie na kritickú infraštruktúru, a to najmä v rámci programov financovaných z Fondu pre vnútornú bezpečnosť, ako aj ďalších potenciálnych možností financovania na úrovni Únie, napr. z Európskeho fondu regionálneho rozvoja, pokiaľ osobitné opatrenia spĺňajú príslušné požiadavky oprávnenosti. Možnosti na financovanie odolnosti môže ponúknuť aj plán REPowerEU. Každé takéto využitie možností financovania z prostriedkov Únie sa musí uskutočniť v súlade s uplatniteľnými právnymi požiadavkami,

PRIJALA TOTO ODPORÚČANIE:

KAPITOLA I: CIEĽ, ROZSAH PÔSOBNOSTI A STANOVENIE PRIORÍT

1. V tomto odporúčaní sa členské štáty vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, ako aj s Komisiou a inými príslušnými verejnými orgánmi či dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu.

2. Opatrenia stanovené v tomto odporúčaní sa týkajú infraštruktúry, ktorú členské štáty označili sa kritickú infraštruktúru vrátane európskej kritickej infraštruktúry.

3. Pri vykonávaní tohto odporúčania by sa prioritou malo stať zvýšenie odolnosti subjektov pôsobiacich v odvetví energetiky, digitálnej infraštruktúry, dopravy a vesmíru, ako aj kritickej infraštruktúry cezhraničného významu, ktorú tieto subjekty prevádzkujú, proti rizikám súvisiacim s ľudskou činnosťou.

KAPITOLA II ZVÝŠENÁ PRIPRAVENOSŤ

[21] com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu).

[22] Závery Rady Európskej únie 7371/22 z 21. marca 2022.

Opatrenia na úrovni členských štátov

4. Členské štáty sa vyzývajú, aby vykonali alebo aktualizovali posúdenie rizík z hľadiska odolnosti subjektov, ktoré prevádzkujú infraštruktúru v odvetví dopravy a energetiky, ktorá je podľa smernice 2008/114/ES označená za európsku kritickú infraštruktúru, a aby náležitým spôsobom a v súlade s uvedenom smernicou vzájomne spolupracovali pri vykonávaní takéhoto posúdenia rizík a pri prijímaní následných opatrení na zvýšenie odolnosti.

5. V snahe dosiahnuť vysokú úroveň odolnosti subjektov, ktoré prevádzkujú kritickú infraštruktúru, by členské štáty mali okrem toho zrýchliť prípravné činnosti, aby mohli čím skôr transponovať a uplatňovať novú smernicu CER, a to:

a) urýchlením prijatia alebo aktualizácie národných stratégií zvyšovania odolnosti subjektov prevádzkujúcich kritickú infraštruktúru s cieľom reagovať na súčasné hrozby. Relevantné časti tejto stratégie by mali byť oznámené Komisii;

b) vykonaním alebo aktualizovaním posúdenia rizík s prihliadnutím na vyvíjajúcu sa povahou súčasných hrozieb, pokiaľ ide o odolnosť subjektov, ktoré prevádzkujú kritickú infraštruktúru v relevantných odvetviach mimo energetiky, digitálnej infraštruktúry, dopravy a vesmíru, a pokiaľ možno v tých odvetviach, ktoré patria do rozsahu pôsobnosti novej smernice CER, teda v odvetví bankovníctva, infraštruktúry finančného trhu, digitálnej infraštruktúry, zdravotníctva, pitnej a odpadovej vody, verejnej správy, vesmíru a výroby, spracovania a distribúcie potravín, a to pri zohľadnení potenciálnej hybridnej povahy príslušných hrozieb, ako aj kaskádových účinkov či účinkov zmeny klímy;

c) informovaním Komisie o typoch rizík zistených pre jednotlivé odvetvia a pododvetvia a výsledkoch posúdení rizík, čo možno vykonať použitím spoločného vzoru na podávanie správ vypracovaného Komisiou v spolupráci s členskými štátmi;

d) zrýchlením procesu identifikácie a označovania kritických subjektov, pričom prioritou by mali byť kritické subjekty, ktoré:

a) využívajú kritickú infraštruktúru, ktorá je fyzicky prepojená medzi dvoma alebo viacerými členskými štátmi;

b) sú súčasťou podnikových štruktúr, ktoré sú prepojené s kritickými subjektmi v inom členskom štáte alebo ktoré sú na ne napojené;

c) boli ako také identifikované v jednom členskom štáte a poskytujú základné služby v šiestich alebo viacerých členských štátoch, resp. do šiestich alebo viacerých členských štátov, a ktoré sú preto osobitného európskeho významu, a informovali o tom Komisiu;

d) rozvíjaním vzájomnej spolupráce, najmä pokiaľ ide o kritické subjekty a základné služby a kritickú infraštruktúru cezhraničného významu, konkrétne zapájaním sa do vzájomných konzultácií na účely bodu 5 písm. d) a vzájomným informovaním sa v prípade incidentu so závažným alebo potenciálnym závažným cezhraničným rušivým vplyvom pri súbežnom informovaní Komisie;

e) zvyšovaním podpory pre označené kritické subjekty v snahe zlepšiť ich odolnosť, čo môže zahŕňať poskytovanie poradenského materiálu a metodiky, organizovanie cvičení na testovanie ich odolnosti a poskytovanie poradenstva a odbornej prípravy zamestnancom, ako aj umožnením vykonávať v súlade s právnymi predpismi Únie a vnútroštátnymi právnymi predpismi previerky osôb s citlivými úlohami v rámci opatrení kritických subjektov v oblasti riadenia bezpečnosti zamestnancov;

f) urýchlením procesu určenia alebo zriadenia miesta jednotného kontaktu v rámci príslušného orgánu, ktoré bude vykonávať funkciu styčného bodu na účely zabezpečenia cezhraničnej spolupráce v oblasti odolnosti subjektov prevádzkujúcich kritickú infraštruktúru s miestami jednotného kontaktu iných členských štátov.

6. Členské štáty sa nabádajú k tomu, aby vykonali záťažové testy subjektov, ktoré prevádzkujú kritickú infraštruktúru. Členské štáty sa vyzývajú najmä k tomu, aby pokročili vo svoje pripravenosti a v pripravenosti dotknutých subjektov v odvetví energetiky a aby v tomto odvetví vykonali záťažové testy, a to podľa možností v súlade so zásadami, ktoré boli spoločne dohodnuté na úrovni Únie, a aby pritom zabezpečili účinnú komunikáciu s dotknutými subjektmi. V prípade potreby by sa následne mohli zvážiť záťažové testy v iných prioritných odvetviach, konkrétne v odvetví digitálnej infraštruktúry, dopravy a vesmíru, s náležitým ohľadom na kontroly v leteckom a námornom pododvetví podľa práva Únie a s prihliadnutím na príslušné ustanovenia odvetvových právnych predpisov.

7. Členské štáty sa vyzývajú k tomu, aby v náležitých prípadoch v súlade s právom Únie spolupracovali s príslušnými tretími krajinami v oblasti odolnosti subjektov, ktoré prevádzkujú kritickú infraštruktúru cezhraničného významu.

8. Členské štáty sa vyzývajú, aby v súlade s platnými požiadavkami, vrátane ustanovení o zvýšení odolnosti proti zmene klímy, využili na zvýšenie odolnosti subjektov prevádzkujúcich kritickú infraštruktúru v Únii, a to napríklad aj pozdĺž transeurópskych sietí, proti celej škále závažných hrozieb, potenciálne možnosti financovania na úrovni Únie a vnútroštátnej úrovni, konkrétne v rámci programov financovaných z Fondu pre vnútornú bezpečnosť a Európskeho fondu regionálneho rozvoja, za predpokladu splnenia príslušných kritérií oprávnenosti, a z Nástroja na prepájanie Európy. Na tento účel možno v súlade s platnými požiadavkami využiť aj financovanie z mechanizmu Európskej únie v oblasti civilnej ochrany, a to najmä v prípade projektov týkajúcich sa posúdenia rizík, investičných plánov alebo štúdií, budovania kapacít alebo zlepšovania vedomostnej základne. Možnosti na financovanie odolnosti môže ponúknuť aj plán REPowerEU.

9. Pokiaľ ide o komunikačnú a sieťovú infraštruktúru v Únii, skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti (NIS) by v súlade s článkom 11 smernice (EÚ) 2016/1148 a následne s článkom 14 smernice NIS2 mala urýchliť prebiehajúcu prácu na cielenom posúdení rizika, pričom prvé odporúčania by mala predložiť začiatkom roka 2023. Táto činnosť by mala byť prepojená a komplementárna s činnosťou skupiny pre spoluprácu NIS v oblasti bezpečnosti dodávateľských reťazcov informačných a komunikačných technológií, ako aj s ďalšími relevantným skupinami, ako je skupina pre odolnosť kritických subjektov, ktorá má byť zriadená podľa novej smernice CER, a fórum pre dozor, ktoré má byť zriadené podľa nového aktu o digitálnej prevádzkovej odolnosti (DORA)[23].

10. Skupina pre spoluprácu NIS, ktoré má svoje úlohy vykonávať v súlade s článkom 11 smernice (EÚ) 2016/1148 a následne s článkom 14 smernice NIS2 sa vyzýva, aby ešte pred nadobudnutím účinnosti smernice NIS2 pracovala s podporou Komisie a agentúry ENISA prioritne na bezpečnosti odvetvia digitálnej infraštruktúry a vesmíru, a to aj prostredníctvom prípravy politického usmernenia a metodiky a opatrení v oblasti riadenia kybernetických bezpečnostných rizík na základe prístupu zohľadňujúceho všetky riziká v súvislosti s podmorskými komunikačnými

[23] COM(2020) 595 final.

káblami, ako aj na vypracovaní usmernení pre opatrenia v oblasti riadenia kybernetických bezpečnostných rizík určených pre prevádzkovateľov vo vesmírnom odvetví s cieľom zvýšiť odolnosť pozemnej infraštruktúry podporujúcej 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, konkrétne penetračné testovanie na odhalenie zraniteľných miest, pričom sa v tejto súvislosti vyzývajú, aby sa prioritne zamerali na subjekty, ktoré prevádzkujú kritickú infraštruktúru v odvetví energetiky, digitálnej infraštruktúry a dopravy.

12. Členské štáty by mali urýchlene vykonať opatrenia odporúčané v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G[24]. Tie členské štáty, ktoré ešte nestanovili obmedzenia týkajúce sa vysokorizikových dodávateľov, by tak mali urobiť bezodkladne, keďže oneskorenie v tejto oblasti môže viesť k vyššej zraniteľnosti sietí v Únii. Zároveň by mali posilniť fyzickú a nefyzickú ochranu kritických a citlivých častí sietí 5G, a to aj prísnymi kontrolami prístupu. Okrem toho by mali členské štáty v spolupráci s Komisiou posúdiť potrebu doplnkových opatrení vrátane právne záväzných požiadaviek na úrovni Únie, aby sa zaistila jednotná úroveň bezpečnosti a odolnosti sietí 5G.

13. Členské štáty by mali čím skôr implementovať pripravovaný sieťový predpis o aspektoch kybernetickej bezpečnosti pri cezhraničných tokoch elektriny, pričom by mali vychádzať zo skúseností získaných pri vykonávaní smernice NIS a z príslušných usmernení vypracovaných skupinou pre spoluprácu NIS, najmä z jej referenčného dokumentu o bezpečnostných opatreniach pre prevádzkovateľov základných služieb.

14. Členské štáty by mali rozvíjať používanie systémov Galileo a/alebo Copernicus na účely dohľadu a zdieľať relevantné informácie v rámci zasadnutia expertov zvolaného v súlade s bodom 15. Na monitorovanie kritickej infraštruktúry a podporu reakcie na krízu by sa mali náležitým spôsobom využívať spôsobilosti, ktoré ponúka vládna satelitná komunikácia (GOVSATCOM) Vesmírneho programu Únie.

Opatrenia na úrovni Únie

15. Komisia má v úmysle posilniť spoluprácu medzi expertmi členských štátov a prispieť tak k zvýšeniu fyzickej nekybernetickej odolnosti subjektov prevádzkujúcich kritickú infraštruktúru, a to:

a) prípravou vypracovania a propagácie spoločných nástrojov na podporu členských štátov pri zvyšovaní odolnosti, vrátane metodík a rizikových scenárov;

b) podporou vypracovania spoločných zásad vykonávania záťažových testov uvedených v bode 6 členskými štátmi, počnúc testami zameranými na riziká súvisiace s ľudskou činnosťou v odvetví energetiky a následne v ďalších kľúčových odvetviach, ako je digitálna infraštruktúra, doprava a vesmír; pričom sa zameria na ďalšie závažné riziká a hrozby a v relevantných prípadoch, aj na poskytovanie podpory a poradenstva pri vykonávaní takýchto záťažových testov;

c) poskytovaním bezpečnej platformy na zhromažďovanie, hodnotenie a zdieľanie najlepších postupov, poznatkov získaných na základe vnútroštátnych skúseností

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

a ďalších informácií týkajúcich sa odolnosti vrátane vykonávania uvedených záťažových testov a premietnutia ich výsledkov do protokolov a pohotovostných plánov.

Pri svojej činnosti by mali títo experti klásť osobitný dôraz na vzájomnú závislosť medzi odvetviami a na subjekty, ktoré prevádzkujú kritickú infraštruktúru cezhraničného významu, pričom na ich činnosť by mala po svojom zriadení nadviazať skupina pre odolnosť kritických subjektov.

16. Členské štáty by sa mali v plnej miere zapájať do posilnenej spolupráce uvedenej v bode 15, a to aj vymenovaním kontaktných miest s príslušnou odbornosťou a zdieľaním skúseností o metodikách používaných pri záťažových testoch a o protokoloch a pohotovostných plánoch vypracovaných na ich základe. Pri takejto výmene informácií by sa mal zachovať dôverný charakter predmetných informácií a mali by sa chrániť bezpečnostné a obchodné záujmy kritických subjektov, pričom by sa malo zároveň prihliadať na bezpečnosť členských štátov. Nezahŕňa to poskytovanie informácií, ktorých zverejnenie je v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

17. Komisia bude členské štáty podporovať poskytovaním príručiek a usmernení, napr. pripravovanou príručkou o ochrane kritickej infraštruktúry a verejných priestorov pred bezpilotnými leteckými systémami, či nástrojov na posúdenie rizík. ESVČ sa vyzýva, aby najmä prostredníctvom Spravodajského a situačného centra EÚ a svojho strediska pre hybridné hrozby zorganizovala informatívne stretnutia o hrozbách pre kritickú infraštruktúru v EÚ, ktorých cieľom bude zvýšiť situačnú informovanosť.

18. Komisia bude podporovať, aby sa výsledky projektov o odolnosti subjektov prevádzkujúcich kritickú infraštruktúru, ktoré sú financované v rámci programov Únie pre výskum a inovácie, využívali v praxi. Komisia má v úmysle zvýšiť financovanie odolnosti v rámci rozpočtu, ktorý je vo viacročnom finančnom rámci na roky 2021– 2027 vyčlenený na program Horizont Európa. Vďaka tomu by malo byť možné reagovať na súčasné a budúce výzvy v tejto oblasti, ako napr. zvýšenie odolnosti kritickej infraštruktúry proti zmene klímy, bez toho, aby to ohrozilo financovanie ďalšieho výskumu a inovácií v oblasti civilnej bezpečnosti v rámci programu Horizont Európa. Komisia sa bude zároveň viac zasadzovať o šírenie výsledkov príslušných výskumných projektov financovaných z prostriedkov Únie.

19. Skupina pre spoluprácu NIS sa vyzýva, aby v súčinnosti s Komisiou a vysokým predstaviteľom v súlade s ich príslušnými úlohami a právomocami podľa práva Únie intenzívnejšie spolupracovala s príslušnými sieťovými a civilnými i vojenskými subjektmi pri vykonávaní posúdenia rizika a pri vypracúvaní scenárov kybernetických bezpečnostných rizík, pričom by sa mala v počiatku zamerať na energetickú, komunikačnú, dopravnú a vesmírnu infraštruktúru a vzájomnú závislosť medzi odvetviami a členskými štátmi. V tejto súvislosti by sa malo prihliadať aj na súvisiace riziká z hľadiska fyzickej infraštruktúry, na ktorú sú tieto odvetvia odkázané. K posudzovaniu rizík a vypracúvaniu rizikových scenárov by malo dochádzať pravidelne, pričom táto činnosť by mala dopĺňať existujúce alebo plánované posúdenia rizík v týchto odvetviach a stavať na nich bez toho, aby dochádzalo k duplicite, a zároveň by mala byť východiskom pre diskusie o tom, ako posilniť celkovú odolnosť subjektov prevádzkujúcich kritickú infraštruktúru a riešiť zraniteľné miesta.

20. Komisia urýchli svoje činnosti na podporu pripravenosti členských štátov a reakcie na kybernetické bezpečnostné incidenty veľkého rozsahu, a to tým, že:

a) popri príslušných posúdeniach rizík v oblasti sieťovej a informačnej bezpečnosti vypracuje komplexnú štúdiu, v ktorej zhodnotí a zmapuje infraštruktúru podmorských káblov prepájajúcu členské štáty a Európu globálne, jej kapacity a redundanciu, zraniteľné miesta, riziká z hľadiska dostupnosti služieb a zmiernenie rizika. Svoje zistenia by mala zdieľať s členskými štátmi;

b) podporí pripravenosť členských štátov a reakciu inštitúcií, orgánov a agentúr EÚ (EUIBA) na kybernetické bezpečnostné incidenty veľkého rozsahu.

21. Komisia bude intenzívnejšie pracovať na anticipačných opatreniach s výhľadom do budúcnosti, a to aj v rámci mechanizmu Európskej únie, v oblasti civilnej ochrany v spolupráci s členskými štátmi podľa článkov 6 a 10 rozhodnutia 1313/2013/EÚ, ako aj formou pohotovostného plánovania s cieľom podporiť operačnú pripravenosť Koordinačného centra pre reakcie na núdzové situácie.

Konkrétne bude Komisia vykonávať tieto činnosti:

a) v rámci Koordinačného centra pre reakcie na núdzové situácie sa bude naďalej zameriavať na anticipáciu a medziodvetvové plánovanie prevencie, pripravenosti a reakcie s cieľom predvídať narušenie poskytovania základných služieb subjektmi, ktoré prevádzkujú kritickú infraštruktúru, a pripraviť sa naň;

b) zvýši investície do prevencie a pripravenosti obyvateľstva pre prípad takéhoto narušenia, pričom bude osobitný dôraz klásť na chemické, biologické, rádiologické a jadrové výbušniny a na iné vznikajúce hrozby spôsobené človekom;

c) posilní výmenu relevantných znalostí a najlepších postupov a zlepší koncepciu a vykonávanie činností v oblasti rozvoja spôsobilostí, ako sú kurzy odbornej prípravy a cvičenia so subjektmi prevádzkujúcimi kritickú infraštruktúru, a to prostredníctvom existujúcich štruktúr a expertízy, ako je napr. vedomostná sieť Únie v oblasti civilnej ochrany.

22. Komisia bude presadzovať používanie prostriedkov EÚ na vykonávanie dohľadu (Copernicus a Galileo), aby tak podporila členské štáty pri monitorovaní kritickej infraštruktúry a v relevantných prípadoch jej bezprostredného okolia, a aby zároveň podporila aj ďalšie možnosti dohľadu stanovené vo Vesmírnom programe Únie.

23. Agentúry Únie a iné príslušné subjekty sa vyzývajú, aby v otázkach odolnosti subjektov prevádzkujúcich kritickú infraštruktúru poskytli v relevantných prípadoch v súlade so svojim mandátom podporu, a to napríklad takto:

a) EUROPOL v oblasti zhromažďovania informácií, kriminálnej analýzy a podpory vyšetrovania v rámci cezhraničného presadzovania práva;

b) EMSA v oblasti bezpečnosti a ochrany odvetvia námorníctva v EÚ vrátane služieb námorného dozoru v záujme zaistenia námornej bezpečnosti a ochrany;

c) EUSPA v oblasti činností v rámci Vesmírneho programu Únie;

d) ENISA v oblasti činností týkajúcich sa kybernetickej bezpečnosti.

KAPITOLA III POSILNENÁ REAKCIA

Opatrenia na úrovni členských štátov

24. Členské štáty by mali:

a) koordinovať svoju reakciu a udržiavať si prehľad o medziodvetvovej reakcii na závažné narušenie poskytovania základných služieb subjektmi, ktoré prevádzkujú kritickú infraštruktúru, a to v rámci krízového mechanizmu Rady (IPCR), pokiaľ ide

o kritickú infraštruktúru cezhraničného významu, v rámci koncepcie zameranej na cezhraničné kybernetické incidenty a krízy veľkého rozsahu, resp. v rámci pre koordinovanú reakciu EÚ na hybridné kampane v prípade hybridných kampaní;

b) zintenzívniť výmenu informácií v rámci mechanizmu Európskej únie v oblasti civilnej ochrany a posilniť tak včasné varovanie a koordináciu svojej reakcie v rámci uvedeného mechanizmu v prípade takéhoto závažného narušenia, čím sa v prípade potreby zabezpečí rýchlejšia reakcia sprostredkovaná Úniou;

c) zvýšiť svoju pripravenosť reagovať na takéto závažné narušenie prostredníctvom mechanizmu Európskej únie v oblasti civilnej ochrany, najmä ak je pravdepodobné, že toto narušenie môže mať závažné cezhraničné alebo dokonca celoeurópske či medziodvetvové dosahy;

d) spoločne s Komisiou pracovať na ďalšom rozvoji príslušných kapacít reakcie v rámci európskeho zoskupenia v oblasti civilnej ochrany (ECPP) a rescEU;

e) vyzvať subjekty, ktoré prevádzkujú kritickú infraštruktúru, a príslušné vnútroštátne orgány, aby posilnili kapacitu uvedených subjektov v záujme rýchleho obnovenia základnej výkonnosti poskytovaných základných služieb;

f) zabezpečiť, aby v prípade, že je potrebné obnoviť kritickú infraštruktúru, bola takáto obnovená infraštruktúra odolná proti celej škále závažných rizík, ktoré sa na ňu môžu vzťahovať, a to aj v prípade nepriaznivých klimatických scenárov.

25. Členské štáty sa vyzývajú, aby urýchlili prípravu na transpozíciu a uplatňovanie smernice NIS2 tak, že bezodkladne začnú posilňovať spôsobilosti vnútroštátnych jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) vzhľadom na nové úlohy jednotiek CSIRT, ako aj na zvýšený počet subjektov z nových odvetví, urýchlene aktualizujú svoje stratégie kybernetickej bezpečnosti a čím skôr prijmú národné plány reakcie na kybernetické bezpečnostné incidenty a krízy.

Opatrenia na úrovni Únie

26. Reakcia na závažné narušenie poskytovania základných služieb subjektmi, ktoré prevádzkujú kritickú infraštruktúru, by mala byť koordinovaná na úrovni expertov členských štátov, pokiaľ ide o odolnosť uvedených subjektov a reakciu na takého narušenie, čo môže prispieť k fungovaniu krízového mechanizmu Rady (IPCR).

27. Komisia bude úzko spolupracovať s členskými štátmi na ďalšom rozvoji kapacít pre reakcie na núdzové situácie, ktoré bude možné nasadiť, vrátane expertov a rezerv v systéme rescEU v rámci mechanizmu Európskej únie v oblasti civilnej ochrany, aby tak bolo možné posilniť operačnú pripravenosť na riešenie bezprostredných a nepriamych účinkov závažného narušenia poskytovania základných služieb subjektmi, ktoré prevádzkujú kritickú infraštruktúru.

28. Vzhľadom na vyvíjajúce sa rizikové prostredie bude Komisia v spolupráci s členskými štátmi v rámci mechanizmu Európskej únie v oblasti civilnej ochrany:

a) kontinuálne analyzovať a testovať primeranosť a operačnú pripravenosť existujúcich kapacít pre reakcie;

b) pravidelne posudzovať prípadnú potrebu rozvoja nových kapacít pre reakcie na úrovni EÚ prostredníctvom rescEU;

c) intenzívnejšie rozvíjať medziodvetvovú spoluprácu v snahe zabezpečiť primeranú reakciu na úrovni EÚ a pravidelne organizovať cvičenia zamerané na testovanie tejto spolupráce;

d) pracovať na ďalšom rozvoji Koordinačného centra pre reakcie na núdzové situácie ako medziodvetvového krízového strediska na úrovni EÚ, ktorého úlohou je koordinovať podporu poskytovanú postihnutým členským štátom.

29. Komisia v spolupráci s vysokým predstaviteľom a v úzkej konzultácii s členskými štátmi vypracuje za podpory príslušných agentúr Únie koncepciu pre incidenty a krízy v oblasti kritickej infraštruktúry, v ktorej opíše a stanoví ciele a modely spolupráce medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami EÚ pri reakcii na incidenty namierené proti kritickej infraštruktúre, a to najmä pokiaľ vedú k závažnému narušeniu poskytovania základných služieb na vnútornom trhu. Táto koncepcia by mala vychádzať z existujúcich integrovaných dojednaní o politickej reakcii na krízu (IPCR) zameraných na koordináciu reakcie.

30. V súvislosti s infraštruktúrou podmorských káblov bude Komisia spolu so zainteresovanými stranami a expertmi pracovať na možných opatreniach obnovy po incidente, ktoré majú byť predložené spolu s hodnotiacou štúdiou uvedenou v bode 20 písm. a) a bude ďalej rozvíjať pohotovostné plánovanie a rizikové scenáre a pracovať na odolnosti Únie voči katastrofám v rámci mechanizmu Európskej únie v oblasti civilnej ochrany.

KAPITOLA IV MEDZINÁRODNÁ SPOLUPRÁCA

31. Komisia a vysoký predstaviteľ budú v súlade so svojimi príslušnými úlohami a právomocami podľa práva Únie v náležitých prípadoch podporovať partnerské krajiny v tom, aby zvyšovali odolnosť subjektov, ktoré prevádzkujú kritickú infraštruktúru na ich území.

32. Komisia a vysoký predstaviteľ budú v súlade so svojimi príslušnými úlohami a právomocami podľa práva Únie prostredníctvom štruktúrovaného dialógu medzi EÚ a NATO posilňovať koordináciu s NATO v oblasti odolnosti kritickej infraštruktúry a na tento účel zriadia pracovnú skupinu.

33. 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 o rámci pre koordinovanú reakciu EÚ na hybridné kampane[25] a aby ich následne používali, čím sa zabezpečí plné uplatňovanie uvedeného rámca najmä pri zvažovaní a príprave komplexnej a koordinovanej reakcie EÚ na hybridné kampane a hybridné hrozby vrátane tých, ktoré sú namierené proti subjektom prevádzkujúcim kritickú infraštruktúru.

34. Komisia v relevantných a vhodných prípadoch zváži účasť zástupcov tretích krajín na spolupráci a výmene informácií medzi expertmi členských štátov v oblasti odolnosti subjektov, ktoré prevádzkujú kritickú infraštruktúru.

[25] Závery Rady o rámci pre koordinovanú reakciu EÚ na hybridné kampane – Rada (europa.eu)

[…]

V Štrasburgu

Za Radu
predseda/predsedníčka