EVROPSKÁ
KOMISE

Ve Štrasburku dne 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Návrh

DOPORUČENÍ RADY

o koordinovaném přístupu Unie za účelem posílení odolnosti kritické infrastruktury

(Text s významem pro EHP)

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Bezpečnost je základním cílem Evropské unie. Zatímco primární odpovědnost za ochranu občanů nesou členské státy, kolektivní činnost na úrovni Unie významně přispívá k bezpečnosti EU jako celku. Koordinace pomáhá zvýšit odolnost, zlepšit ostražitost a posílit naši kolektivní reakci. V souvislosti s bezpečnostní unií EU byly učiněny důležité kroky k budování schopností a kapacit pro prevenci a odhalování řady bezpečnostních hrozeb a rychlou reakci na ně a k propojení subjektů veřejného a soukromého sektoru ve společném úsilí.

Vybavení EU pro řešení neustále se měnících forem hrozeb vyžaduje neustálou ostražitost a přizpůsobování. Útočná válka Ruska proti Ukrajině přinesla nová rizika, která jsou často kombinována ve formě hybridní hrozby. Jedním z nich je riziko narušení poskytování základních služeb subjekty provozujícími kritickou infrastrukturu v Evropě. To je ještě zřetelnější v souvislosti se zjevnou sabotáží plynovodů Nord Stream a dalšími nedávnými incidenty. Společnost je silně závislá na fyzické i digitální infrastruktuře a přerušení základních služeb, ať už prostřednictvím konvenčních fyzických útoků nebo kybernetických útoků, nebo jejich kombinace, může mít vážné důsledky pro blahobyt občanů, naše ekonomiky a důvěru v naše demokratické systémy.

Dalším klíčovým cílem EU je zajištění hladkého fungování vnitřního trhu, a to i pokud jde o základní služby poskytované subjekty provozujícími kritickou infrastrukturu. EU proto již přijala řadu opatření ke snížení zranitelnosti a zvýšení odolnosti kritických subjektů, a to jak v souvislosti s kybernetickými, tak nekybernetickými riziky.

Je naléhavě nutné přijmout opatření k posílení schopnosti EU čelit možným útokům na kritickou infrastrukturu, zejména v samotné EU, ale případně i v jejím bezprostředním sousedství.

Cílem navrhovaného doporučení Rady je zintenzivnit podporu EU zaměřenou na zvyšování odolnosti kritické infrastruktury a zajistit koordinaci na úrovni EU, pokud jde o připravenost a reakci. Jeho cílem je maximalizovat a urychlit práci na ochraně těchto prostředků, zařízení a systémů, které jsou nezbytné pro fungování ekonomiky, a poskytovat na vnitřním trhu základní služby, na nichž jsou občané závislí, a zmírnit dopad jakéhokoli útoku zajištěním co nejrychlejší obnovy. I když by měla být chráněna veškerá tato infrastruktura, v současnosti jsou hlavní prioritou odvětví energetiky, digitální infrastruktury, dopravy a vesmíru vzhledem k jejich obzvláště horizontálnímu charakteru pro společnost a ekonomiku a k posouzení současných rizik.

EU hraje specifickou úlohu v případě zajištění odolnosti infrastruktury, která přesahuje pozemní nebo námořní hranice, a má tak dopad na zájmy několika členských států, nebo která je využívána k poskytování základních přeshraničních služeb. Kritická infrastruktura s významem pro několik členských států se však může nacházet pouze v jednom členském státě, nebo dokonce mimo území členského státu, například v případě podmořských kabelů nebo potrubí. Jasné určení kritické infrastruktury a subjektů, které ji provozují, i rizik, která je ohrožují, a kolektivní závazek k jejich ochraně je v zájmu všech členských států a EU jako celku.

Evropský parlament a Rada již dosáhly politické dohody o prohloubení legislativního rámce EU s cílem pomoci posílit odolnost subjektů provozujících kritickou infrastrukturu. V létě 2022 bylo dosaženo dohody ohledně směrnice o odolnosti kritické infrastruktury („směrnice

CER“)[1] a revidované směrnice o bezpečnosti sítí a informačních systémů („směrnice NIS2“)[2]. Ve srovnání se stávajícím legislativním rámcem – směrnicí 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu („směrnice ECI“)[3] a směrnicí Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii („směrnice NIS“)[4] budou výše uvedené směrnice představovat významné posílení schopností. Očekává se, že nové právní předpisy vstoupí v platnost koncem roku 2022 nebo začátkem roku 2023, a členské státy by měly jejich provedení ve vnitrostátním právu a uplatňování upřednostnit, v souladu s právem Unie.

Vzhledem k výše uvedenému a k potenciální naléhavosti řešení hrozeb vyplývajících z útočné války Ruska proti Ukrajině by měla být opatření nastíněná v nových právních předpisech realizována dříve, pokud je to možné a vhodné. Posílení vzájemné spolupráce již nyní by rovněž pomohlo dát impuls k účinnému provádění těchto nových právních předpisů, jakmile budou plně v platnosti.

Výsledkem by bylo jít nad rámec stávajících opatření již nyní, a to jak z hlediska hloubky opatření, tak z hlediska rozsahu zahrnutých odvětví. Nová směrnice CER obsahuje nový rámec pro spolupráci a povinnosti členských států a kritických subjektů zaměřené na posílení fyzické nekybernetické odolnosti subjektů, které poskytují základní služby na vnitřním trhu, vůči přírodním a člověkem způsobeným hrozbám a specifikuje jedenáct odvětví[5]. Směrnice NIS2 zavede povinnosti v oblasti kybernetické bezpečnosti pro širokou škálu odvětví. Patří sem i nový požadavek, aby členské státy v příslušném případě zahrnuly do svých strategií kybernetické bezpečnosti i podmořské kabely.

Uvedené právní předpisy vyžadují, aby Komise převzala významnou koordinační úlohu. Podle směrnice CER má Komise podpůrnou a usnadňující úlohu, která má být plněna za podpory a zapojení skupiny pro odolnost kritických subjektů (CERG) zřízené uvedenou směrnicí, a měla by doplňovat činnosti členských států tím, že bude vypracovávat osvědčené postupy, pokyny a metodiky. Pokud jde o kybernetickou bezpečnost, Rada již ve svých závěrech o kybernetické pozici EU v létě 2022 vyzvala Komisi, vysokého představitele a skupinu pro spolupráci NIS, aby pracovali na posouzení rizik a rizikových scénářích z hlediska kybernetické bezpečnosti. Tato koordinace může být inspirací pro to, jaký přístup zvolit u další klíčové kritické infrastruktury.

Dne 5. října 2022 představila předsedkyně Komise von der Leyenová pětibodový plán, který nastiňuje koordinovaný přístup k nezbytné další práci. Klíčovými prvky tohoto plánu jsou: zlepšení připravenosti, spolupráce s členskými státy s cílem provést zátěžové testování jejich kritické infrastruktury – nejprve odvětví energetiky a poté dalších vysoce rizikových odvětví, zvýšení schopnosti reakce, zejména prostřednictvím mechanismu civilní ochrany Unie, účelné využívání družicové kapacity k odhalování potenciálních hrozeb a posílení spolupráce s NATO a klíčovými partnery v oblasti odolnosti kritické infrastruktury. Uvedený pětibodový plán zdůraznil význam dřívější realizace právních předpisů, u nichž již bylo dosaženo politické dohody.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 Úř. věst. L 345, 23.12.2008.
4 Úř. věst. L 194, 19.7.2016.
5 Energetika, doprava, digitální infrastruktura, bankovnictví, infrastruktura finančních trhů, zdravotnictví, pitná voda, odpadní voda, veřejná správa, vesmír a potraviny.

Navrhované doporučení Rady vítá tento přístup s cílem strukturovat podporu členských států a koordinovat jejich úsilí při zvyšování povědomí o rizicích, připravenosti a reakce na současné hrozby. V tomto ohledu jsou svolávána setkání odborníků, aby projednali odolnost subjektů provozujících kritickou infrastrukturu ještě před tím, než směrnice CER vstoupí v platnost a bude zřízena skupina CERG stanovená v uvedené směrnici.

Zásadní význam bude mít posílená spolupráce s klíčovými partnery a sousedními a dalšími relevantními třetími zeměmi, pokud jde o odolnost subjektů provozujících kritickou infrastrukturu, zejména prostřednictvím strukturovaného dialogu o odolnosti mezi EU a NATO.

Toto doporučení se zaměřuje na posílení schopnosti Unie předvídat nové hrozby vyplývající z útočné války Ruska proti Ukrajině, předcházet jim a reagovat na ně. Navrhovaná doporučení se proto zaměřují na řešení bezpečnostních rizik a hrozeb pro kritickou infrastrukturu. Nicméně nedávné události rovněž vyzdvihly naléhavou potřebu věnovat zvýšenou pozornost dopadům změny klimatu na kritickou infrastrukturu a služby, například pokud jde o sezónně ohrožené a nepředvídatelné dodávky vody pro chlazení jaderných elektráren, vodní energii a vnitrozemskou plavbu nebo riziko materiálních škod na dopravní infrastruktuře, které mohou způsobit významné narušení základních služeb. Tyto obavy budou i nadále řešeny prostřednictvím příslušných právních předpisů a koordinace.

- **Soulad s platnými předpisy v této oblasti politiky**

Tento návrh doporučení Rady je plně v souladu se stávajícím a budoucím právním rámcem pro odolnost subjektů provozujících kritickou infrastrukturu, směrnicí ECI a směrnicí CER, neboť jeho cílem je mimo jiné usnadnit v této oblasti spolupráci mezi členskými státy a podpořit konkrétní opatření ke zvýšení odolnosti proti stávajícím bezprostředním hrozbám vůči subjektům provozujícím kritickou infrastrukturu v EU.

Návrh rovněž doplňuje a předjímá směrnici CER tím, že již vyzývá členské státy, aby upřednostnily její včasné provedení ve vnitrostátním právu, a to tak, že budou spolupracovat prostřednictvím setkání odborníků svolaných v rámci pětibodového plánu oznámeného Komisí a budou usilovat o koordinaci dosažení společného přístupu k provádění zátěžových testů kritické infrastruktury v EU.

Návrh je rovněž v souladu se směrnicí NIS a připravovanou směrnicí NIS2, která směrnici NIS zruší, protože vyzývá k brzkému zahájení práce na jejím a provedení ve vnitrostátním právu a uplatňování. Odráží rovněž společnou výzvu z Nevers z března 2022 i závěry Rady o kybernetické pozici EU z května 2022, pokud jde o žádost členských států, aby Komise vypracovala posouzení rizik a rizikové scénáře.

Návrh je rovněž v souladu s politikou EU v oblasti civilní ochrany, kdy v případě rozsáhlého narušení operací kritické infrastruktury/subjektů mohou členské státy a třetí země požádat o pomoc prostřednictvím Střediska pro koordinaci odezvy na mimořádné události (ERCC) v rámci mechanismu civilní ochrany Unie. V případě aktivace mechanismu civilní ochrany Unie je středisko ERCC schopno koordinovat a spolufinancovat nasazení základního vybavení, materiálu a expertizy dostupných v členských státech (částečně v rámci Evropského souboru civilní ochrany) a v rámci rescEU v postižené zemi. Pomoc, která může být poskytnuta na požádání, zahrnuje například palivo, generátory, elektrickou infrastrukturu, ubytovací kapacitu, kapacitu pro čištění vody a kapacity pro rychlou zdravotnickou pomoc.

Návrh je rovněž v souladu s *acquis* EU týkajícím se zabezpečení dodávek energie.

Odvětví jaderné energie není do navrhovaného doporučení Rady konkrétně zahrnuto, s výjimkou například související infrastruktury (jako jsou přenosová vedení do jaderných elektráren), která může mít vliv na zabezpečení dodávek. Na specifické jaderné prvky se

vztahují příslušné právní předpisy v oblasti jaderné energie podle Smlouvy o Euratomu a/nebo vnitrostátních právních předpisů[6]. Na základě zkušeností z havárie ve Fukušimě byly posíleny evropské právní předpisy pro jadernou bezpečnost, a proto musí vnitrostátní orgány pro každé zařízení provádět pravidelná periodická hodnocení bezpečnosti, aby se zajistilo nepřetržité dodržování nejvyšších bezpečnostních požadavků a identifikovaly se další možnosti zlepšení bezpečnosti, a dále musí provádět šest ročních tematických vzájemných hodnocení na úrovni EU.

Strategie EU pro námořní bezpečnost[7] a její akční plán[8] zdůrazňují měnící se povahu hrozeb v námořní oblasti a vyzývají k obnovení závazku k ochraně kritické námořní infrastruktury, včetně podvodní, a zejména infrastruktury námořní dopravy a energetické a komunikační infrastruktury, mimo jiné zvyšováním povědomí o situaci na moři prostřednictvím lepší interoperability a zjednodušené výměny informací.

Návrh je rovněž v souladu s dalšími příslušnými odvětvovými právními předpisy. Provádění tohoto doporučení by proto mělo být v souladu se zvláštními opatřeními, která regulují nebo v budoucnu mohou regulovat určité aspekty odolnosti subjektů působících v dotčených odvětvích, například v dopravě. To zahrnuje další relevantní iniciativy, jako je plán pro mimořádné situace v dopravě[9] nebo plán pro nepředvídané události pro zajištění dodávek potravin a potravinového zabezpečení v dobách krize[10] a související evropský mechanismus připravenosti a reakce na krize v oblasti potravinového zabezpečení. Obecněji by toto doporučení mělo být přirozeně prováděno při plném dodržování všech platných pravidel práva EU, včetně pravidel stanovených ve směrnicích ECI a NIS.

Návrh je rovněž v souladu se Strategickým kompasem pro bezpečnost a obranu, který zdůraznil potřebu podstatně posílit odolnost a schopnost bojovat proti hybridním hrozbám a kybernetickým útokům, a potřebu posílit odolnost partnerských zemí a spolupracovat s NATO. Je rovněž v souladu s rámcem pro koordinovanou reakci EU na hybridní hrozby a kampaně, které se dotýkají EU, členských států a jejich partnerů[11].

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Návrh je založen na článku 114 Smlouvy o fungování Evropské unie, který zahrnuje sbližování právních předpisů, jejichž účelem je zlepšení fungování vnitřního trhu, spolu s článkem 292 Smlouvy o fungování EU. To je odůvodněno skutečností, že cílem navrhovaného doporučení Rady je především dřívější realizace opatření stanovených v nových směrnicích CER a NIS2, které jsou obě rovněž založeny na článku 114 Smlouvy o fungování EU. V souladu s logikou, která odůvodňuje použití uvedeného článku jako právního základu uvedených směrnic, je potřeba přijmout opatření na úrovni EU, aby se zajistilo hladké fungování vnitřního trhu, zejména s ohledem na přeshraniční povahu a rozsah dotčených služeb a na možné důsledky v případě jejich narušení a s ohledem na stávající a nově vznikající vnitrostátní opatření zaměřená na posílení odolnosti subjektů provozujících kritickou infrastrukturu používanou k poskytování základních služeb na vnitřním trhu.

---

6 9. bod odůvodnění směrnice Rady 2008/114/ES (směrnice ECI).
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.
11 Rada Evropské unie, 10016/22, 21. června 2022.

- **Subsidiarita (v případě nevýlučné pravomoci)**

Další postup na evropské úrovni v oblasti odolnosti subjektů provozujících kritickou infrastrukturu je odůvodněn vzájemnou závislostí a přeshraniční povahou vztahů mezi operacemi kritické infrastruktury a poskytovanými základními službami a potřebou jednotnějšího a koordinovanějšího evropského přístupu s cílem zajistit, aby dotčené subjekty byly v současném geopolitickém kontextu dostatečně odolné. Vzhledem k tomu, že mnohé ze společných problémů, jako je zjevná sabotáž plynovodů Nord Stream, jsou v první řadě řešeny prostřednictvím vnitrostátních opatření nebo subjekty provozujícími kritickou infrastrukturu, je podpora ze strany EU, případně jejích relevantních agentur, nezbytná pro zvýšení odolnosti, zlepšení ostražitosti a posílení kolektivní reakce EU.

- **Proporcionalita**

Tento návrh je v souladu se zásadou proporcionality stanovenou v čl. 5 odst. 4 Smlouvy o Evropské unii.

Obsah ani forma tohoto navrhovaného doporučení Rady nepřesahují rámec toho, co je nezbytné k dosažení jeho cílů. Navrhovaná opatření jsou přiměřená sledovaným cílům, neboť respektují výsady a povinnosti členských států podle vnitrostátního práva.

Návrh rovněž zohledňuje potenciální diferencovaný přístup, který odráží rozdílné vnitřní podmínky členských států, pokud jde o připravenost a reakci na fyzické hrozby pro kritickou infrastrukturu.

- **Volba nástroje**

Aby bylo výše uvedených cílů dosaženo, Smlouva a fungování EU stanoví, zejména v článku 292, že Rada může přijmout na základě návrhu Komise doporučení. Doporučení Rady je v tomto případě vhodným nástrojem i s ohledem na stávající legislativní kontext vysvětlený výše. Jakožto právní akt, i když je nezávazný, doporučení Rady signalizuje závazek členských států přijmout v něm uvedená opatření a poskytuje pevný politický základ pro spolupráci v těchto oblastech, přičemž plně respektuje pravomoci členských států.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Konzultace se zúčastněnými stranami**

Při vypracovávání tohoto návrhu byly zohledněny názory odborníků z členských států vyjádřené na zasedání dne 12. října 2022. O užitečnosti větší koordinace na úrovni Unie, pokud jde o připravenost a reakci v současném kontextu hrozeb, a o dřívější realizaci některých prvků směrnice CER před jejím formálním přijetím panovala široká shoda. Členské státy vyjádřily ochotu sdílet zkušenosti a osvědčené postupy týkající se opatření a metodik ke zvýšení odolnosti subjektů provozujících kritickou infrastrukturu. Členské státy rovněž vyjádřily otevřenost vůči koordinovanému přístupu k zátěžovým testům subjektů provozujících kritickou infrastrukturu, které by probíhaly na dobrovolném základě a na základě společných zásad. Členské státy uvedly, že pro účely tohoto doporučení by měly být za prioritu považovány subjekty provozující kritickou infrastrukturu v odvětví energetiky, digitální infrastruktury a dopravy, zejména subjekty s významem pro několik členských států. Členské státy rovněž uvítaly záměr Komise svolat v nadcházejících týdnech další zasedání odborníků z členských států.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Návrh doporučení Rady zní takto:

– Kapitola I uvádí cíl návrhu, jeho rozsah a stanovení priorit doporučených opatření.

– Kapitola II se zaměřuje na opatření, která by měla být přijata v zájmu lepší připravenosti jak na úrovni Unie, tak na úrovni členských států.

– Kapitola III se zabývá posílenou reakcí jak na úrovni EU, tak na úrovni členských států.

– Kapitola IV se zabývá mezinárodní spoluprací a opatřeními, která by měla být přijata za účelem posílení odolnosti subjektů provozujících kritickou infrastrukturu.

2022/0338 (NLE)

Návrh

DOPORUČENÍ RADY

o koordinovaném přístupu Unie za účelem posílení odolnosti kritické infrastruktury

(Text s významem pro EHP)

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na články 114 a 292 této smlouvy,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

(1) Unie hraje specifickou úlohu v případě infrastruktury, která přesahuje hranice, a má tak dopad na zájmy několika členských států, nebo která je jinak využívána subjekty k poskytování základních přeshraničních služeb. Toto poskytování služeb a kritická infrastruktura s významem pro několik členských států se však mohou nacházet pouze v jednom členském státě nebo mimo území členských států, například v případě podmořských kabelů nebo potrubí. Jasné určení této infrastruktury a subjektů a hrozeb, jimž čelí, i kolektivní závazek k jejich ochraně je v zájmu všech členských států a Unie jako celku.

(2) Ochrana kritické infrastruktury ve dvou odvětvích je v současnosti upravena směrnicí Rady 2008/114/ES[12]. Uvedenou směrnicí se zavádí postup pro určování a označování evropských kritických infrastruktur a společný přístup k posouzení potřeby zvýšit ochranu těchto infrastruktur s cílem přispět k ochraně obyvatel. Vztahuje se na odvětví energetiky a dopravy. Aby se zlepšila odolnost kritických subjektů a základních služeb, které poskytují, a kritické infrastruktury, na niž jsou odkázány, normotvůrce Unie právě provádí proces přijímání nové směrnice o odolnosti kritických subjektů[13] („směrnice CER“), která nahradí směrnici 2008/114/ES a bude se vztahovat na více odvětví, včetně digitální infrastruktury.

(3) Kromě toho se směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[14] zaměřuje na kybernetické hrozby. Uvedená směrnice bude nahrazena novou směrnicí o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii[15] („směrnice NIS2“), která se rovněž nachází v procesu přijímání normotvůrcem Unie.

---

12 Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008, s. 75).

13 COM(2020) 829.

14 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

15 COM(2020) 823.

(4) S ohledem na rychle se vyvíjející formy hrozeb, zejména v souvislosti se zjevnou sabotáží plynárenské infrastruktury Nord Stream 1 a 2, čelí subjekty provozující kritickou infrastrukturu specifickým výzvám, pokud jde o jejich odolnost vůči nepřátelským činům a dalším člověkem způsobeným hrozbám, a současně dochází k nárůstu výzev vyplývajících z přírodních faktorů a změny klimatu, které mohou mít vliv společně s nepřátelskými činy. Proto musí uvedené subjekty přijmout za podpory členských států vhodná opatření ke zvýšení odolnosti. Uvedená opatření by měla být přijata a uvedená podpora by měla být poskytnuta nad rámec opatření ve směrnici 2008/114/ES a směrnici (EU) 2016/1148, a to i před přijetím nových směrnic CER a NIS2, jejich vstupem v platnost a provedením ve vnitrostátním právu.

(5) Do přijetí, vstupu v platnost a provedení uvedených nových směrnic se Unie a členské státy v souladu s právem Unie vyzývají, aby k dosažení pokroku využívaly všechny dostupné nástroje a pomáhaly posílit fyzickou a kybernetickou odolnost dotčených subjektů a kritické infrastruktury, kterou provozují za účelem poskytování základních služeb na vnitřním trhu, tj. služeb, které mají zásadní význam pro zachování životně důležitých společenských funkcí, ekonomických činností, veřejného zdraví a bezpečnosti nebo životního prostředí. V tomto ohledu by pojem odolnosti měl být chápán tak, že odkazuje na schopnost subjektu předcházet událostem, které mohou významně narušit nebo které narušují poskytování dotčených základních služeb, chránit se před těmito událostmi, reagovat na ně, odolávat jim, zmírňovat je a absorbovat, přizpůsobovat se jim a zotavovat se z nich.

(6) V zájmu zajištění přístupu, který je jak účinný, tak co nejkonzistentnější s novou směrnicí CER, by se opatření obsažená v tomto doporučení měla vztahovat na infrastrukturu označenou členským státem za kritickou infrastrukturu, zahrnující jak vnitrostátní, tak evropskou kritickou infrastrukturu, bez ohledu na to, zda byl subjekt provozující kritickou infrastrukturu již označen za kritický subjekt podle uvedené nové směrnice. Pro účely tohoto doporučení by měl být pojem „kritická infrastruktura“ chápán odpovídajícím způsobem.

(7) S ohledem na stávající hrozby by měla být přednostně přijata opatření ke zvýšení odolnosti v klíčových odvětvích energetiky, digitální infrastruktury, dopravy a vesmíru a tato opatření by se měla zaměřit na posílení odolnosti subjektů provozujících kritickou infrastrukturu z hlediska rizik způsobených člověkem. Co se týče vnitrostátní kritické infrastruktury, měla by být vzhledem k možným důsledkům, pokud se rizika naplní, upřednostněna infrastruktura, která má přeshraniční význam.

(8) Cílem opatření v tomto doporučení je proto především doplnit nové směrnice CER a NIS2, které jsou založeny na článku 114 Smlouvy o fungování Evropské unie, tím, že doporučují dřívější realizaci a rozšíření opatření, která stanoví uvedené nové směrnice. Proto a s ohledem na přeshraniční povahu a význam dotčených základních služeb a kritické infrastruktury a na stávající a vznikající rozdíly mezi vnitrostátními právními předpisy, které narušují vnitřní trh, je vhodné založit toto doporučení též na článku 114 a dále na článku 292 Smlouvy o fungování EU.

(9) Provádění tohoto doporučení by nemělo být chápáno tak, že ovlivňuje stávající a budoucí požadavky práva Unie týkající se určitých aspektů odolnosti dotčených subjektů, a mělo by být s uvedenými požadavky v souladu. Tyto požadavky jsou stanoveny v obecných nástrojích, jako jsou směrnice 2008/114/ES a směrnice (EU) 2016/1148 a nové směrnice CER a NIS2, které je nahradí, ale také v některých

odvětvově specifických nástrojích, například v oblasti dopravy, kde Komise mimo jiné přijala plán pro mimořádné situace v dopravě[16]. V souladu se zásadou loajální spolupráce by toto doporučení mělo být prováděno za plného vzájemného respektu a pomoci.

(10) Komise dne 5. října 2022 oznámila pětibodový plán, který nastiňuje koordinovaný přístup k řešení budoucích výzev a zahrnuje práci na připravenosti na základě nové směrnice CER a její realizaci ještě před jejím přijetím a vstupem v platnost a který rovněž zahrnuje spolupráci s členskými státy s cílem provádět zátěžové testy subjektů provozujících kritickou infrastrukturu na základě společných zásad, počínaje odvětvím energetiky. Toto doporučení, které k uvedenému plánu přispěje, vítá navrhovaný přístup a stanoví, jak jej lze převést do praxe.

(11) Vzhledem k rychle se vyvíjejícím formám hrozeb a k současnému rizikovému prostředí charakterizovanému riziky způsobenými člověkem, zejména pokud jde o kritickou infrastrukturu s přeshraničním významem, je nezbytné mít přesný, aktuální a úplný obraz o nejdůležitějších rizicích, jimž subjekty provozující kritickou infrastrukturu čelí. Členské státy by proto měly přijmout nezbytná opatření k provedení nebo aktualizaci svých posouzení uvedených rizik. Ačkoli se toto doporučení zaměřuje na bezpečnostní rizika, mělo by se navíc pokračovat v úsilí o řešení změny klimatu a environmentálních rizik, zejména pokud mohou přírodní jevy rizika způsobená člověkem dále zhoršit.

(12) S ohledem na uvedené formy hrozeb by členské státy měly být vyzvány, aby ke zvýšení odolnosti kritické infrastruktury, a to i nad rámec uvedených posouzení rizik, co nejdříve přijaly vhodná opatření, která budou následně vyžadována podle nové směrnice CER.

(13) V rámci realizace pětibodového plánu oznámeného Komisí je nezbytné práci koordinovat svoláním národních odborníků, kteří by se měli sejít ještě před zřízením skupiny pro odolnost kritických subjektů stanovené v nové směrnici CER, aby byla umožněna spolupráce mezi členskými státy a výměna informací, pokud jde o odolnost subjektů provozujících kritickou infrastrukturu. To by mělo zahrnovat spolupráci a výměnu informací týkající se činností, jako je určení kritických subjektů a infrastruktury, příprava na vypracování a prosazování společného souboru zásad pro provádění zátěžových testů a získávání společných poznatků ze zátěžových testů, identifikace zranitelných míst a možných schopností. Tyto procesy by rovněž měly být přínosem pro odolnost subjektů provozujících kritickou infrastrukturu vůči klimatickým a environmentálním rizikům. Tato činnost by rovněž umožnila společné upřednostnění práce na zátěžových testech s důrazem na odvětví energetiky, digitální infrastruktury, dopravy a vesmíru. Komise již uvedené odborníky začala svolávat a usnadňovat jejich činnost a má v úmyslu v této práci pokračovat. Jakmile vstoupí nová směrnice CER v platnost a bude zřízena skupina pro odolnost kritických subjektů, měla by tato skupina v této anticipační činnosti pokračovat v souladu se svými úkoly podle směrnice CER.

(14) Zátěžové testy by měly být doplněny vypracováním plánu pro incidenty a krize v oblasti kritické infrastruktury, který popíše a stanoví cíle a způsoby spolupráce mezi členskými státy a orgány, institucemi a jinými subjekty EU při reakci na incidenty namířené proti kritické infrastruktuře, zejména pokud vedou k významnému narušení poskytování základních služeb pro vnitřní trh. Tento plán by měl pro koordinaci

[16] COM(2022) 211.

reakce využívat stávající integrovaná opatření pro politickou reakci na krize (IPCR), měl by fungovat soudržně s plánem pro rozsáhlé kybernetické incidenty a doplňovat jej a měl by rovněž zajistit dohodu na hlavních sděleních v rámci komunikace s veřejností, neboť tato krizová komunikace hraje důležitou úlohu při zmírňování negativních dopadů incidentů a krizí v oblasti kritické infrastruktury.

(15) V zájmu zajištění koordinované a účinné reakce na současné a předpokládané hrozby poskytne Komise členským státům další podporu s cílem zvýšit odolnost z hlediska uvedených hrozeb, zejména jim bude poskytovat relevantní informace ve formě brífinků, příruček a pokynů, bude propagovat využívání výzkumných a inovačních projektů financovaných Unií, přijímat nezbytná anticipační opatření a optimalizovat využívání unijních prostředků dohledu. Evropská služba pro vnější činnost by měla poskytovat posouzení hrozeb, zejména prostřednictvím svého Zpravodajského a informačního centra EU.

(16) Podporu v záležitostech týkajících se odolnosti by měly poskytovat rovněž agentury Unie relevantní pro daná odvětví a další relevantní subjekty, pokud to jejich mandáty stanovené v příslušných nástrojích práva Unie umožňují. Konkrétně by Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) mohla být nápomocna v otázkách kybernetické bezpečnosti, Evropská agentura pro námořní bezpečnost (EMSA) by mohla členským státům pomáhat svou expertizou prostřednictvím své služby námořního dohledu nad záležitostmi souvisejícími s námořní bezpečností a ochranou, Agentura Evropské unie pro spolupráci v oblasti prosazování práva (EUROPOL) by mohla poskytovat podporu v souvislosti se shromažďováním informací a vyšetřováním při přeshraničních donucovacích opatřeních a Agentura Evropské unie pro Kosmický program (EUSPA) a Satelitní středisko Evropské unie (Satcen) mohou případně pomáhat prostřednictvím operací v rámci Kosmického programu Unie.

(17) Přestože primární odpovědnost za zajištění bezpečnosti kritické infrastruktury a dotčených subjektů nesou členské státy, je vhodná zvýšená koordinace na úrovni Unie, zejména s ohledem na hrozby, které mohou mít dopad na několik členských států současně, jako je útočná válka Ruska proti Ukrajině, nebo mohou mít dopad na odolnost a řádné fungování ekonomiky, jednotného trhu a společnosti v Unii.

(18) Toto doporučení nezahrnuje poskytování informací, jejichž zpřístupnění je v rozporu se základními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

(19) Vzhledem k rostoucí vzájemné závislosti fyzických a digitálních infrastruktur mohou nepřátelské činnosti v kyberprostoru zaměřené na kritické oblasti vést k narušení nebo poškození fyzické infrastruktury a sabotáž fyzické infrastruktury může znemožnit přístup k digitálním službám. S ohledem na zvýšenou hrozbu, kterou představují sofistikované hybridní útoky, by členské státy měly tyto skutečnosti rovněž zahrnout do své práce na provedení tohoto doporučení. Vzhledem k vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností provozovatelů je důležité, aby přípravy na provedení nové směrnice NIS2 ve vnitrostátním právu a její uplatňování byly zahájeny co nejdříve a aby souběžně probíhaly rovněž přípravy na novou směrnici CER.

(20) Kromě zlepšování připravenosti je rovněž důležité posílit schopnosti rychlé a účinné reakce v případě, že se naplní rizika ovlivňující základní služby poskytované subjekty provozujícími kritickou infrastrukturu. Toto doporučení by proto mělo obsahovat opatření, která by měla být přijata jak na úrovni členských států, tak na úrovni Unie,

včetně posílené spolupráce a výměny informací v rámci mechanismu civilní ochrany Unie a využívání příslušných prostředků Kosmického programu Unie.

(21) V návaznosti na výzvu Rady obsaženou v jejích závěrech o kybernetické pozici EU[17] provádějí Komise, vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku („vysoký představitel“) a skupina pro spolupráci zřízená směrnicí (EU) 2016/1148 („skupina pro spolupráci NIS“) v koordinaci s příslušnými civilními a vojenskými orgány a subjekty a zřízenými sítěmi, včetně sítě EU CyCLONe, hodnocení rizik a vytvářejí rizikové scénáře z hlediska kybernetické bezpečnosti pro situaci hrozby nebo možného útoku na členské státy nebo partnerské země. Tato činnost se zaměřuje na kritická odvětví, včetně energetiky, digitální infrastruktury, dopravy a vesmíru.

(22) Podnět k posílení odolnosti komunikační infrastruktury a sítí v Unii obsahovaly rovněž společná ministerská výzva z Nevers[18] a závěry Rady o kybernetické pozici EU, a sice prostřednictvím doporučení členským státům a Komisi na základě posouzení rizik. Toto posouzení rizik v současnosti provádí skupina pro spolupráci NIS za podpory Komise a agentury ENISA a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací (BEREC). Posouzení rizik a analýza nedostatků se zaměřují na rizika kybernetických útoků v různých pododvětvích komunikačních infrastruktur, včetně pevných a mobilních infrastruktur, satelitů, podmořských kabelů, internetového směrování atd., a poskytují tak základ pro činnost podle tohoto doporučení. Toto posouzení rizik bude podkladem pro probíhající meziodvětvové hodnocení kybernetických rizik a scénáře požadované Radou v jejích závěrech ze dne 23. května 2022.

(23) Zmíněné dvě činnosti budou konzistentní a koordinované s vytvářením scénářů zaměřených na civilní ochranu v kontextu široké škály přírodních a člověkem způsobených katastrof, včetně událostí v oblasti kybernetické bezpečnosti a jejich reálného dopadu; tyto scénáře v současnosti vypracovává Komise a členské státy podle rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU[19]. V zájmu účinnosti, účelnosti a konzistentnosti by toto doporučení mělo být zavedeno do praxe s ohledem na výsledky uvedených činností.

(24) Soubor nástrojů EU pro kybernetickou bezpečnost sítí 5G[20] stanoví příslušná opatření a zmírňující plány s cílem posílit bezpečnost sítí 5G. Vzhledem k závislosti mnoha základních služeb na sítích 5G a k propojené povaze digitálních ekosystémů je nezbytné, aby všechny členské státy opatření doporučená v uvedeném souboru nástrojů urychleně zrealizovaly, a zejména aby zavedly příslušná omezení týkající se vysoce rizikových dodavatelů u klíčových prostředků, které jsou v koordinovaném posouzení rizik EU vymezeny jako kritické a citlivé.

(25) Za účelem okamžitého posílení připravenosti a kapacit reakce na závažné kybernetické incidenty vytvořila Komise prostřednictvím dalšího financování přiděleného agentuře ENISA krátkodobý program, který má členským státům poskytnout podporu. Poskytované služby budou zahrnovat opatření v oblasti připravenosti, jako je

---

17 Kybernetická pozice:Rada schválila závěry – Consilium (europa.eu)

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

19 Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

penetrační testování kritických subjektů s cílem identifikovat zranitelná místa. Rovněž budou posíleny možnosti pomoci členským státům v případě závažného incidentu s dopadem na kritické subjekty. Jedná se o první krok v souladu se závěry Rady o kybernetické pozici, v nichž se požaduje, aby Komise předložila návrh fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti. Členské státy by měly těchto příležitostí v souladu s příslušnými požadavky plně využít.

(26) Zásadní význam pro celosvětovou a vnitrounijní konektivitu má globální podmořská datová a elektronická komunikační kabelová síť. Vzhledem ke značné délce těchto kabelů a jejich instalaci na mořském dně je podmořské vizuální monitorování většiny kabelových úseků mimořádně náročné. Sdílená jurisdikce a další jurisdikční otázky týkající se těchto kabelů představují specifický případ pro evropskou a mezinárodní spolupráci v oblasti ochrany a obnovy infrastruktury. Je proto nezbytné doplnit probíhající a plánovaná posouzení rizik týkající se digitálních a fyzických infrastruktur, na nichž jsou digitální služby založeny, o zvláštní posouzení rizik a o možnosti zmírňujících opatření týkající se podmořských kabelů. Komise proto za tímto účelem provede studie a svá zjištění sdělí členským státům.

(27) Na prioritní odvětví energetiky a dopravy identifikovaná v tomto doporučení mohou být rizika související s digitální infrastrukturou rovněž dopad. Takový dopad může existovat například ve vztahu k energetickým technologiím zahrnujícím digitální součásti. Bezpečnost souvisejících dodavatelských řetězců je důležitá pro kontinuitu poskytování základních služeb a pro strategickou kontrolu kritické infrastruktury provozované subjekty v odvětví energetiky. Uvedené okolnosti by měly být při přijímání opatření pro zvýšení odolnosti subjektů provozujících kritickou infrastrukturu v souladu s tímto doporučením zohledněny.

(28) Vzhledem k rostoucímu významu kosmické infrastruktury a kosmických služeb pro činnosti související s bezpečností je nezbytné zajistit odolnost a ochranu unijních kosmických prostředků a služeb v EU, ale také v rámci tohoto doporučení, a strukturovaněji využívat kosmická data a služby poskytované kosmickými systémy a programy pro účely dohledu nad kritickou infrastrukturou v jiných odvětvích a její ochrany. V připravované kosmické strategii EU pro bezpečnost a obranu budou v tomto ohledu navrženy vhodná opatření, která by měla být při provádění tohoto doporučení zohledněna.

(29) K účinnému řešení rizik ohrožujících odolnost subjektů provozujících kritickou infrastrukturu buď v Unii, nebo v relevantních třetích zemích nebo v mezinárodních vodách je rovněž nezbytná spolupráce na mezinárodní úrovni. Členské státy by proto měly být vyzvány, aby spolupracovaly s Komisí a vysokým představitelem a aby za uvedeným účelem podnikly určité kroky, přičemž se rozumí, že veškeré takové kroky smí být učiněny pouze v souladu s jejich příslušnými úkoly a povinnostmi podle práva Unie, zejména podle ustanovení Smluv EU týkajících se vnějších vztahů.

(30) Jak je stanoveno ve sdělení „Příspěvek Komise k evropské obraně“[21], v návaznosti na dokument „Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti“[22], Komise do roku 2023 posoudí ve spolupráci s vysokým představitelem a členskými státy referenční hodnoty odvětvové hybridní odolnosti s cílem určit nedostatky a potřeby, jakož i kroky k jejich řešení. Tato iniciativa by měla být

[21] com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

[22] Rada Evropské unie, 7371/22, 21. března 2022.

podkladem pro další činnost v rámci tohoto doporučení a měla by pomoci posílit sdílení informací a koordinaci opatření pro další zvýšení odolnosti, včetně odolnosti kritické infrastruktury.

(31) Strategie EU pro námořní bezpečnost z roku 2014 a její akční plán obsahovaly výzvu ke zvýšené ochraně kritické námořní infrastruktury, včetně podvodní, a zejména infrastruktury námořní dopravy a energetické a komunikační infrastruktury, mimo jiné zvýšením povědomí o situaci na moři prostřednictvím lepší interoperability a zjednodušené výměny informací (povinné a dobrovolné). Zmíněná strategie a akční plán se v současné době aktualizují a budou zahrnovat posílená opatření zaměřená na ochranu kritické námořní infrastruktury. Uvedená opatření by měla být podkladem pro toto doporučení a doplňovat jej.

(32) Členské státy by měly zohlednit plný potenciál programu Unie pro výzkum v oblasti bezpečnosti, konkrétně využít jeho prioritní zaměření na kritickou infrastrukturu, zejména v rámci programů financovaných z Fondu pro vnitřní bezpečnost, i další potenciální možnosti financování na úrovni Unie, konkrétně z Evropského fondu pro regionální rozvoj, pokud specifická opatření splňují jeho požadavky na způsobilost. Odolnost by bylo případně možné financovat i v rámci REPowerEU. Veškeré využití možností financování z prostředků Unie se musí uskutečnit v souladu s příslušnými právními požadavky,

PŘIJALA TOTO DOPORUČENÍ:

KAPITOLA I: CÍL, OBLAST PŮSOBNOSTI A STANOVENÍ PRIORIT

1) V rámci tohoto doporučení se členské státy vyzývají, aby urychleně přijaly účinná opatření a aby loajálně, efektivně, solidárně a koordinovaně spolupracovaly mezi sebou navzájem a s Komisí a dalšími příslušnými veřejnými orgány i s dotčenými subjekty s cílem posílit odolnost kritické infrastruktury používané k poskytování základních služeb na vnitřním trhu.

2) Opatření stanovená v tomto doporučení se týkají infrastruktury označené členským státem za kritickou infrastrukturu, včetně evropské kritické infrastruktury.

3) Při provádění tohoto doporučení by mělo být prioritou posílení odolnosti subjektů působících v odvětvích energetiky, digitální infrastruktury, dopravy a vesmíru a kritické infrastruktury s přeshraničním významem, kterou uvedené subjekty provozují, s ohledem na rizika způsobená člověkem.

KAPITOLA II LEPŠÍ PŘIPRAVENOST

Opatření na úrovni členských států

4) Členské státy se vyzývají, aby provedly nebo zaktualizovaly posouzení rizik týkající se odolnosti subjektů provozujících evropskou kritickou infrastrukturu označenou v odvětví dopravy a energetiky podle směrnice 2008/114/ES a aby podle potřeby a v souladu s uvedenou směrnicí na těchto posouzeních rizik a výsledných opatřeních k posílení odolnosti vzájemně spolupracovaly.

5) Kromě toho a v zájmu dosažení vysoké úrovně odolnosti subjektů provozujících kritickou infrastrukturu by členské státy měly urychlit přípravné práce s cílem provést novou směrnici CER co nejdříve ve vnitrostátním právu a začít ji uplatňovat tím, že:

a) urychlí přijetí nebo aktualizaci svých národních strategií pro posílení odolnosti subjektů provozujících kritickou infrastrukturu s cílem reagovat na současné hrozby. Relevantní části této strategie by měly být sděleny Komisi;

b) provedou nebo zaktualizují posouzení rizik v souladu s vyvíjející se povahou současných hrozeb, pokud jde o odolnost subjektů provozujících kritickou infrastrukturu v relevantních odvětvích nad rámec energetiky, digitální infrastruktury, dopravy a vesmíru a pokud možno v odvětvích spadajících do oblasti působnosti nové směrnice CER, což jsou konkrétně bankovnictví, infrastruktura finančních trhů, digitální infrastruktura, zdravotnictví, pitná voda, odpadní voda, veřejná správa, vesmír a zpracování, výroba a distribuce potravin, s přihlédnutím k potenciální hybridní povaze příslušných hrozeb, včetně kaskádových efektů a dopadů změny klimatu;

c) budou informovat Komisi o typech rizik zjištěných v jednotlivých odvětvích a pododvětvích a o výsledcích posouzení rizik, což bude možné s využitím společného vzoru pro podávání zpráv vypracovaného Komisí ve spolupráci s členskými státy;

d) urychlí proces určení a označení kritických subjektů, přičemž prioritu budou mít kritické subjekty, které:

a) využívají kritickou infrastrukturu, která je fyzicky propojena mezi dvěma nebo více členskými státy;

b) jsou součástí korporátních struktur, které jsou propojeny s kritickými subjekty v jiných členských státech nebo na ně mají vazby;

c) byly jako kritické subjekty určeny v jednom členském státě a poskytují základní služby v šesti či více členských státech nebo do šesti či více členských států, a mají proto zvláštní evropský význam, a budou o tom informovat Komisi;

d) budou vzájemně spolupracovat, zejména pokud jde o kritické subjekty a základní služby a kritickou infrastrukturu s přeshraničním významem, zejména tak, že se pro účely bodu 5 písm. d) budou vzájemně konzultovat a že se v případě incidentu s významným nebo potenciálně významným přeshraničním rušivým účinkem budou vzájemně informovat, přičemž podle potřeby budou informovat i Komisi;

e) posílí podporu označených kritických subjektů s cílem zlepšit jejich odolnost, což může zahrnovat poskytování pokynů a metodik, organizaci cvičení k otestování jejich odolnosti a poskytování poradenství a školení jejich personálu, a dále v souladu s unijními a vnitrostátními právními předpisy umožní kontroly spolehlivosti osob s citlivými úlohami jako součást opatření kritických subjektů v oblasti řízení bezpečnosti zaměstnanců;

f) urychlí určení nebo zřízení jednotného kontaktního místa v rámci příslušného orgánu pro výkon styčné funkce za účelem zajištění přeshraniční spolupráce týkající se odolnosti subjektů provozujících kritickou infrastrukturu s jednotnými kontaktními místy jiných členských států.

6) Členské státy se vyzývají, aby prováděly zátěžové testy subjektů provozujících kritickou infrastrukturu. Členské státy se zejména vyzývají, aby pokročily ve své připravenosti a připravenosti dotčených subjektů v odvětví energetiky a prováděly v tomto odvětví zátěžové testy, pokud možno v souladu se zásadami společně dohodnutými na úrovni Unie, a zároveň zajistily efektivní komunikaci s dotčenými subjekty. Následně by mohly být v případě potřeby zváženy zátěžové testy v jiných prioritních odvětvích, konkrétně v digitální infrastruktuře, dopravě a vesmíru, s

náležitým ohledem na inspekce v leteckém a námořním pododvětví podle práva Unie a s přihlédnutím k příslušným ustanovením odvětvových právních předpisů.

7) Členské státy se vyzývají, aby ve vhodných případech a v souladu s právem Unie spolupracovaly s relevantními třetími zeměmi, pokud jde o odolnost subjektů provozujících kritickou infrastrukturu s přeshraničním významem.

8) Členské státy se vyzývají, aby v souladu s příslušnými požadavky využily potenciálních možností financování na úrovni Unie a na vnitrostátní úrovni ke zvýšení odolnosti subjektů provozujících kritickou infrastrukturu v Unii, mimo jiné například podél transevropských sítí, vůči celé škále závažných hrozeb, zejména v rámci programů financovaných z Fondu pro vnitřní bezpečnost a Evropského fondu pro regionální rozvoj a dále z Nástroje pro propojení Evropy, přičemž je potřeba splnit příslušná kritéria způsobilosti, včetně ustanovení o zajištění odolnosti vůči změně klimatu. K tomuto účelu lze v souladu s příslušnými požadavky rovněž využít financování z mechanismu civilní ochrany Unie, zejména u projektů souvisejících s posuzováním rizik, investičními plány nebo studiemi, budováním kapacit nebo zlepšováním znalostní základny. Odolnost by bylo případně možné financovat i v rámci REPowerEU.

9) Pokud jde o komunikační a síťovou infrastrukturu v Unii, skupina pro spolupráci NIS by měla při plnění úkolů v souladu s článkem 11 směrnice (EU) 2016/1148 a následně s článkem 14 směrnice NIS2 urychlit svou probíhající práci na cíleném posuzování rizik a měla by začátkem roku 2023 předložit první doporučení. Uvedená práce by měla být prováděna při zajištění soudržnosti a doplňkovosti s prací, kterou vykonávají pracovní osa skupiny pro spolupráci NIS zaměřená na bezpečnost dodavatelského řetězce informačních a komunikačních technologií a další relevantní skupiny, jako je skupina pro odolnost kritických subjektů, která má být zřízena podle nové směrnice CER, a fórum dohledu, které má být zřízeno podle nového aktu o digitální provozní odolnosti (DORA)[23].

10) Skupina pro spolupráci NIS, která má plnit své úkoly v souladu s článkem 11 směrnice (EU) 2016/1148 a následně s článkem 14 směrnice NIS2, se vyzývá, aby s podporou Komise a agentury ENISA upřednostnila svou práci v oblasti bezpečnosti digitální infrastruktury a kosmického odvětví, mimo jiné aby připravila strategické pokyny a metodiky a opatření k řízení kybernetických bezpečnostních rizik na základě přístupu zohledňujícím všechna rizika v souvislosti s podmořskými komunikačními kabely, v očekávání vstupu směrnice NIS2 v platnost, a dále práci na přípravě pokynů pro opatření k řízení kybernetických bezpečnostních rizik určených pro subjekty působící v kosmickém odvětví, aby se zvýšila odolnost pozemní infrastruktury podporující poskytování kosmických služeb.

11) Členské státy by měly plně využít služeb připravenosti v oblasti kybernetické bezpečnosti, které jsou nabízeny v rámci krátkodobého podpůrného programu Komise realizovaného ve spolupráci s agenturou ENISA, zejména penetračního testování za účelem identifikace zranitelných míst, a v této souvislosti se vyzývají, aby upřednostnily subjekty provozující kritickou infrastrukturu v odvětví energetiky, digitální infrastruktury a dopravy.

[23] COM(2020) 595 final.

12) Členské státy by měly urychleně realizovat opatření doporučená v souboru nástrojů EU pro kybernetickou bezpečnost sítí 5G[24]. Členské státy, které dosud nepřijaly omezení týkající se vysoce rizikových dodavatelů, by tak měly bezodkladně učinit vzhledem k tomu, že časová prodleva může zvýšit zranitelnost sítí v Unii. Měly by rovněž posílit fyzickou a nefyzickou ochranu kritických a citlivých částí sítí 5G, mimo jiné prostřednictvím přísných kontrol přístupu k nim. Kromě toho by členské státy ve spolupráci s Komisí měly posoudit potřebu doplňkových opatření, včetně právně závazných požadavků na úrovni Unie, aby byla zajištěna jednotná úroveň bezpečnosti a odolnosti sítí 5G.

13) Členské státy by měly co nejdříve zavést připravovaný síťový kodex pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny, a to na základě zkušeností získaných při provádění směrnice NIS a příslušných pokynů vypracovaných skupinou pro spolupráci NIS, zejména jejího referenčního dokumentu o bezpečnostních opatřeních pro provozovatele základních služeb.

14) Členské státy by měly rozvíjet využívání systémů Galileo a/nebo Copernicus pro účely dohledu a sdílet relevantní informace v rámci okruhu odborníků svolaných v souladu s bodem 15. Pro monitorování kritické infrastruktury a podporu reakce na krize by měly být účelně využívány schopnosti, které poskytuje družicová komunikace v rámci státní správy (GOVSATCOM) Kosmického programu Unie.

Opatření na úrovni Unie

15) Komise má v úmyslu posílit spolupráci mezi odborníky z členských států s cílem pomoci zvýšit fyzickou nekybernetickou odolnost subjektů provozujících kritickou infrastrukturu, a to zejména tak, že:

a) připraví vývoj a propagaci společných nástrojů na podporu členských států při zvyšování této odolnosti, včetně metodik a rizikových scénářů;

b) podpoří vypracování společných zásad pro provádění zátěžových testů uvedených v bodě 6 členskými státy, přičemž jako první přijdou na řadu testy zaměřené na rizika způsobená člověkem v odvětví energetiky a poté budou následovat testy v dalších klíčových odvětvích, jako je digitální infrastruktura, doprava a vesmír, dále se zaměří na jiná významná rizika a nebezpečí a v relevantních případech bude při provádění těchto zátěžových testů poskytovat podporu a poradenství;

c) poskytne bezpečnou platformu pro shromažďování, hodnocení a sdílení osvědčených postupů, poznatků získaných na základě vnitrostátních zkušeností a dalších informací týkajících se tohoto typu odolnosti, včetně informací o provádění uvedených zátěžových testů a převádění jejich výsledků do protokolů a krizových plánů.

Práce těchto odborníků by měla být zaměřena obzvláště na meziodvětvové závislosti a subjekty provozující kritickou infrastrukturu s přeshraničním významem a měla by v ní pokračovat skupina pro odolnost kritických subjektů, jakmile bude zřízena.

16) Členské státy by se měly do posílené spolupráce uvedené v bodě 15 plně zapojit, mimo jiné tak, že určí kontaktní místa s příslušnou expertizou a budou sdílet zkušenosti s metodikami používanými pro zátěžové testy a protokoly a krizové plány vypracované na jejich základě. Při těchto výměnách informací by měla být zachovávána důvěrnost předmětných informací a bezpečnost a obchodní zájmy kritických subjektů a zároveň respektována bezpečnost členských států. Nespadá sem

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

poskytování informací, jejichž zpřístupnění je v rozporu se základními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

17) Komise bude podporovat členské státy tím, že poskytne příručky a pokyny, například připraví příručku o ochraně kritické infrastruktury a veřejných prostor před systémy bezpilotních letadel, a dále poskytne nástroje pro posuzování rizik. Evropská služba pro vnější činnost se vyzývá, aby zejména prostřednictvím Zpravodajského a informačního centra EU a jeho jednotky pro hybridní hrozby pořádala brífinky o hrozbách pro kritickou infrastrukturu v EU s cílem zlepšit situační povědomí.

18) Komise bude podporovat využívání výsledků projektů týkajících se odolnosti subjektů provozujících kritickou infrastrukturu financovaných v rámci programů Unie pro výzkum a inovace. Komise má v úmyslu v rámci rozpočtu přiděleného na program Horizont Evropa v kontextu víceletého finančního rámce na období 2021–2027 financování tohoto typu odolnosti zvýšit. To by mělo umožnit řešit současné a budoucí výzvy v této oblasti, jako je zajištění odolnosti kritické infrastruktury vůči změně klimatu, aniž by to bylo na úkor dalšího financování výzkumu a inovací v oblasti civilní bezpečnosti v rámci programu Horizont Evropa. Komise rovněž zvýší své úsilí o šíření výsledků příslušných relevantních projektů financovaných Unií.

19) Skupina pro spolupráci NIS se vyzývá, aby ve spolupráci s Komisí a vysokým představitelem v souladu s jejich příslušnými úkoly a povinnostmi podle práva Unie zintenzivnila kooperaci s relevantními sítěmi a civilními a vojenskými subjekty při posuzování rizik a vytváření scénářů rizik v oblasti kybernetické bezpečnosti s počátečním zaměřením na energetickou, komunikační, dopravní a kosmickou infrastrukturu a vzájemnou závislost mezi odvětvími a členskými státy. Tato činnost by měla zohlednit související rizika pro fyzickou infrastrukturu, na níž jsou tato odvětví odkázána. Posuzování rizik a vytváření scénářů by měly být prováděny pravidelně a měly by doplňovat stávající nebo plánovaná posouzení rizik v těchto odvětvích, stavět na nich a nedublovat je a měly by být zdrojem informací pro diskuse o tom, jak posílit celkovou odolnost subjektů provozujících kritickou infrastrukturu a jak řešit zranitelná místa.

20) Komise urychlí své činnosti na podporu připravenosti členských států a reakce na rozsáhlé incidenty v oblasti kybernetické bezpečnosti, a zejména:

a) jako doplněk k příslušným posouzením rizik v kontextu bezpečnosti sítí a informací vypracuje ucelenou studii zhodnocení infrastruktury podmořských kabelů, která propojuje členské státy a dále propojuje Evropu celosvětově (včetně zmapování), jejích kapacit a redundancí, zranitelných míst, rizik pro dostupnost služeb a zmírňování rizik. Její zjištění by měla být sdílena s členskými státy;

b) podpoří připravenost členských států a orgánů, institucí a jiných subjektů EU na rozsáhlé incidenty v oblasti kybernetické bezpečnosti.

21) Komise zintenzivní práci na výhledových předběžných opatřeních, včetně v rámci mechanismu civilní ochrany Unie, ve spolupráci s členskými státy podle článků 6 a 10 rozhodnutí 1313/2013/EU a ve formě krizového plánování na podporu operační připravenosti Střediska pro koordinaci odezvy na mimořádné události (ERCC).

Komise bude provádět zejména tyto činnosti:

a) v rámci střediska ERCC bude dále pracovat na anticipaci a meziodvětvovém plánování prevence, připravenosti a reakce s cílem předvídat narušení základních služeb poskytovaných subjekty provozujícími kritickou infrastrukturu a připravit se na taková narušení;

b) zvýší investice do preventivních přístupů a připravenosti obyvatelstva v případě takových narušení, se zvláštním zaměřením na chemické, biologické a radiologické jaderné výbušniny nebo jiné nové hrozby způsobené člověkem;

c) posílí výměnu relevantních znalostí a osvědčených postupů a zlepší koncepci a realizaci činností v oblasti rozvoje kapacit, jako jsou školicí kurzy a cvičení se subjekty provozujícími kritickou infrastrukturu, a to prostřednictvím stávajících struktur a expertizy, jako je unijní síť znalostí v oblasti civilní ochrany.

22) Komise bude podporovat využívání unijních prostředků dohledu (Copernicus a Galileo) s cílem pomoci členským státům při monitorování kritické infrastruktury a v relevantních případech jejich bezprostředního okolí a bude podporovat i další možnosti dohledu stanovené v Kosmickém programu Unie.

23) V relevantních případech a v souladu se svými mandáty se agentury Unie a další příslušné subjekty vyzývají, aby v záležitostech týkajících se odolnosti subjektů provozujících kritickou infrastrukturu poskytly podporu, zejména následovně:

a) EUROPOL, pokud jde o shromažďování informací, analýzy trestné činnosti a investigativní podporu při přeshraničních donucovacích opatřeních;

b) EMSA, pokud jde o záležitosti týkající se bezpečnosti a ochrany námořního odvětví v Unii, včetně služeb námořního dohledu v záležitostech týkajících se námořní bezpečnosti a ochrany;

c) EUSPA, pokud jde o činnosti v rámci Kosmického programu Unie;

d) ENISA, pokud jde o činnosti související s kybernetickou bezpečností.

KAPITOLA III: POSÍLENÁ REAKCE

Opatření na úrovni členských států

24) Členské státy by měly:

a) koordinovat svou reakci a udržovat přehled o meziodvětvové reakci na významná narušení základních služeb, které poskytují subjekty provozující kritickou infrastrukturu, v rámci krizového mechanismu Rady (IPCR) v případě kritické infrastruktury s přeshraničním významem, plánu pro rozsáhlé incidenty a krize v oblasti kybernetické bezpečnosti nebo v rámci pro koordinovanou reakci EU na hybridní kampaně v případě hybridních kampaní;

b) zintenzivnit výměnu informací v rámci mechanismu civilní ochrany Unie s cílem posílit včasné varování a v případě takto významných narušení koordinovat svou reakci v rámci zmíněného mechanismu, čímž se v případě potřeby zajistí rychlejší reakce zprostředkovaná Unií;

c) zvýšit svou připravenost reagovat na takto významná narušení prostřednictvím mechanismu civilní ochrany Unie, zejména pokud je pravděpodobné, že tato narušení budou mít významné přeshraniční nebo dokonce celoevropské i meziodvětvové důsledky;

d) spolupracovat s Komisí na dalším rozvoji relevantních kapacit reakce v rámci Evropského souboru civilní ochrany (ECPP) a rescEU;

e) vyzvat subjekty provozující kritickou infrastrukturu a příslušné vnitrostátní orgány, aby zvýšily kapacitu uvedených subjektů umožňující rychlé obnovení elementární výkonnosti poskytovaných základních služeb;

f) zajistit, aby v případě nutnosti znovuvýstavby kritické infrastruktury byla tato obnovená infrastruktura odolná vůči kompletní řadě významných rizik, která pro ni mohou být relevantní, včetně v nepříznivých klimatických scénářích.

25) Členské státy se vyzývají, aby urychlily přípravné práce pro provedení směrnice NIS2 ve vnitrostátním právu a její uplatňování tak, že okamžitě zahájí posilování kapacit vnitrostátních týmů pro reakci na počítačové bezpečnostní incidenty (CSIRT) s ohledem na nové úkoly týmů CSIRT i na rozšířený počet subjektů z nových odvětví, že urychleně zaktualizují své strategie kybernetické bezpečnosti a že co nejdříve přijmou národní plány reakce na incidenty a krize v oblasti kybernetické bezpečnosti.

Opatření na úrovni Unie

26) Reakce na významná narušení základních služeb poskytovaných subjekty provozujícími kritickou infrastrukturu by měla být koordinována mezi odborníky z členských států, pokud jde o odolnost uvedených subjektů a reakce na tato narušení, které by mohly přispět k fungování krizového mechanismu Rady (IPCR).

27) Komise bude úzce spolupracovat s členskými státy na dalším rozvoji nasaditelných kapacit reakce na mimořádné situace, včetně odborníků a zásob z rescEU v rámci mechanismu civilní ochrany Unie, aby se posílila operační připravenost k řešení bezprostředních a nepřímých dopadů významných narušení základních služeb poskytovaných subjekty provozujícími kritickou infrastrukturu.

28) S ohledem na vyvíjející se rizikové prostředí a ve spolupráci s členskými státy bude Komise v rámci mechanismu civilní ochrany Unie:

a) průběžně analyzovat a testovat adekvátnost a operační připravenost stávající kapacity reakce;

b) pravidelně přezkoumávat případnou potřebu vyvinout na úrovni EU nové kapacity reakce prostřednictvím rescEU;

c) dále zintenzivňovat meziodvětvovou spolupráci s cílem zajistit adekvátní reakci na úrovni EU a organizovat pravidelná cvičení pro testování této spolupráce;

d) dále rozvíjet středisko ERCC jako meziodvětvové krizové centrum na úrovni EU ke koordinaci podpory pro postižené členské státy.

29) Komise ve spolupráci s vysokým představitelem, v úzké konzultaci s členskými státy a za podpory příslušných agentur Unie vypracuje plán pro incidenty a krize v oblasti kritické infrastruktury, který popíše a stanoví cíle a způsoby spolupráce mezi členskými státy a orgány, institucemi a jinými subjekty EU při reakci na incidenty namířené proti kritické infrastruktuře, zejména pokud vedou k významnému narušení poskytování základních služeb pro vnitřní trh. Zmíněný plán by měl pro koordinaci reakce využít stávající integrovaná opatření pro politickou reakci na krize (IPCR).

30) Komise bude spolupracovat se zúčastněnými stranami a odborníky na možných opatřeních k nápravě incidentů týkajících se infrastruktury podmořských kabelů, která mají být předložena ve spojení s hodnotící studií uvedenou v bodě 20 písm. a), a v rámci mechanismu civilní ochrany Unie dále rozvíjet krizové plánování, rizikové scénáře a pracovat na odolnosti Unie vůči katastrofám.

KAPITOLA IV: MEZINÁRODNÍ SPOLUPRÁCE

31) Komise a vysoký představitel budou ve vhodných případech a v souladu se svými příslušnými úkoly a povinnostmi podle práva Unie podporovat partnerské země s cílem zvýšit odolnost subjektů provozujících kritickou infrastrukturu na jejich území.

32) Komise a vysoký představitel v souladu se svými příslušnými úkoly a povinnostmi podle práva Unie posílí v oblasti odolnosti kritické infrastruktury koordinaci s NATO prostřednictvím strukturovaného dialogu mezi EU a NATO o odolnosti a za tímto účelem zřídí pracovní skupinu.

33) Členské státy se vyzývají, aby ve spolupráci s Komisí a vysokým představitelem přispěly k urychlenému vývoji a zavedení souboru nástrojů EU proti hybridním hrozbám a prováděcích pokynů zmíněných v závěrech Rady o rámci pro koordinovanou reakci EU na hybridní kampaně[25] a následně je používaly, aby byl uvedený rámec plně účinný, zejména při zvažování a přípravě ucelených a koordinovaných reakcí EU na hybridní kampaně a hybridní hrozby, včetně hrozeb namířených proti subjektům provozujícím kritickou infrastrukturu.

34) Komise v rámci spolupráce a výměny informací mezi odborníky z členských států v oblasti odolnosti subjektů provozujících kritickou infrastrukturu zváží účast zástupců třetích zemí, bude-li to relevantní a vhodné.

[…]

Ve Štrasburku dne

Za Radu
předseda/předsedkyně

[25] Závěry Rady o rámci pro koordinovanou reakci EU na hybridní kampaně – Consilium (europa.eu)