I

(Usnesení, doporučení a stanoviska)

DOPORUČENÍ

RADA

DOPORUČENÍ RADY
ze dne 8. prosince 2022,
o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury

(Text s významem pro EHP)

(2023/C 20/01)

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 a čl. 292 první a druhou větu této smlouvy,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

(1) Má-li být zabezpečeno fungování vnitřního trhu, je v zájmu všech členských států a Unie jako celku jasně určit a chránit relevantní kritickou infrastrukturu, která v rámci uvedeného trhu poskytuje základní služby, zejména v klíčových odvětvích, jako je energetika, digitální infrastruktura, doprava a vesmír, jakož i kritickou infrastrukturu se značným přeshraničním významem ([1]), jejíž narušení by mohlo mít významný dopad na ostatní členské státy.

(2) Toto doporučení, které je nezávazným aktem, je důkazem politické vůle členských států vzájemně spolupracovat, jakož i jejich odhodlání provádět doporučená opatření, která jsou zdůrazněna v pětibodovém plánu vydaném předsedkyní Evropské komise, a to při plném respektování pravomocí členských států. Zároveň tímto doporučením není dotčena ochrana základních zájmů národní bezpečnosti, veřejné bezpečnosti nebo obrany členských států a od žádného členského státu by se nemělo očekávat, že bude sdílet informace, které uvedené zájmy poškozují.

(3) Přestože primární odpovědnost za zajištění bezpečnosti a poskytování základních služeb ze strany kritické infrastruktury nesou členské státy a provozovatelé jejich kritické infrastruktury, je vhodná zvýšená koordinace na úrovni Unie, zejména s ohledem na vyvíjející se hrozby, které mohou mít dopad na několik členských států současně, jako je útočná válka Ruska proti Ukrajině a hybridní kampaně namířené proti členským státům, nebo které mohou mít dopad na odolnost a řádné fungování unijní ekonomiky, vnitřního trhu a společnosti jako takové. Zvláštní pozornost by měla být věnována kritické infrastruktuře mimo území členských států, jako je podmořská kritická infrastruktura nebo energetická infrastruktura na moři.

([1]) Členské státy by měly posoudit tento význam v souladu se svými vnitrostátními postupy a mohou tak učinit mimo jiné na základě posouzení rizik, jakož i dopadu a povahy události.

(4) Evropská rada ve svých závěrech ze dne 20. a 21. října 2022 ostře odsoudila sabotáže páchané na kritické infrastruktuře, jako například poškození plynovodů Nord Stream, a uvedla, že Unie bude na jakékoli úmyslné poškození kritické infrastruktury nebo na jiné hybridní akce jednotně a důrazně reagovat.

(5) S ohledem na rychle se vyvíjející formy hrozeb by měla být přednostně přijata opatření ke zvýšení odolnosti v klíčových odvětvích, jako je energetika, digitální infrastruktura, doprava a vesmír, a v dalších relevantních odvětvích určených členskými státy. Tato opatření by se měla zaměřit na posílení odolnosti kritické infrastruktury s přihlédnutím k relevantním rizikům, zejména kaskádovým účinkům, narušení dodavatelských řetězců, závislosti, dopadům změny klimatu, nespolehlivým prodejcům a partnerům a hybridním hrozbám a kampaním, včetně zahraniční manipulace s informacemi a vměšování. Co se týče vnitrostátní kritické infrastruktury, měla by být vzhledem k možným důsledkům upřednostněna kritická infrastruktura, která má značný přeshraniční význam. Členské státy se vyzývají, aby ve vhodných případech tato opatření ke zvýšení odolnosti neprodleně zavedly a zároveň zachovaly přístup stanovený ve vyvíjejícím se právním rámci.

(6) Ochrana evropské kritické infrastruktury v odvětví energetiky a dopravy je v současné době upravena směrnicí Rady 2008/114/ES ([2]) a bezpečnost sítí a informačních systémů v celé Unii se zaměřením na kybernetické hrozby je zajištěna směrnicí Evropského parlamentu a Rady (EU) 2016/1148 ([3]). S cílem zajistit vyšší společnou úroveň odolnosti a ochrany kritické infrastruktury, kybernetické bezpečnosti a finančního trhu se stávající právní rámec mění a doplňuje prostřednictvím přijetí nových pravidel vztahujících se na kritické subjekty („směrnice CER“), posílených pravidel k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („směrnice NIS2“) a nových pravidel pro digitální provozní odolnost finančního sektoru („nařízení DORA“).

(7) Členské státy by měly v souladu s unijním a vnitrostátním právem využívat všechny dostupné nástroje, aby dosáhly pokroku a pomohly posílit fyzickou a kybernetickou odolnost. V tomto ohledu by měla být kritická infrastruktura chápána tak, že zahrnuje relevantní kritickou infrastrukturu, která byla určena členským státem na vnitrostátní úrovni nebo která byla označena za evropskou kritickou infrastrukturu podle směrnice 2008/114/ES, i kritické subjekty, které mají být určeny podle směrnice CER, nebo případně subjekty podle směrnice NIS2. Pojmem „odolnost“ by se měla rozumět schopnost kritické infrastruktury předcházet událostem, které významně narušují nebo mohou výrazně narušit poskytování základních služeb na vnitřním trhu, tj. služeb, které mají zásadní význam pro zachování životně důležitých společenských a ekonomických funkcí, veřejné bezpečnosti a bezpečnosti obecně, zdraví obyvatelstva nebo životního prostředí, chránit před těmito událostmi, reagovat na ně, odolávat jim, zmírňovat je, absorbovat je, přizpůsobovat se jim nebo se z nich zotavovat.

(8) Je třeba svolat vnitrostátní odborníky s cílem koordinovat činnost zaměřenou na dosažení vyšší společné úrovně odolnosti a ochrany kritické infrastruktury, která má být zavedena novými pravidly platnými pro kritické subjekty. Tato koordinovaná činnost by umožnila spolupráci mezi členskými státy a sdílení informací o činnostech, jako je vypracování metodik pro určení základních služeb poskytovaných kritickou infrastrukturou. Komise již uvedené odborníky začala svolávat a usnadňovat jejich činnost a má v úmyslu v této práci pokračovat. Jakmile vstoupí směrnice CER v platnost a bude zřízena skupina pro odolnost kritických subjektů podle této směrnice, měla by dotyčná skupina v této anticipační činnosti pokračovat v souladu se svými úkoly.

(9) S ohledem na změnu forem hrozeb by měl být dále rozvíjen potenciál provádění zátěžových testů kritické infrastruktury na vnitrostátní úrovni, neboť tyto testy by mohly být užitečné pro posílení odolnosti kritické infrastruktury. Vzhledem ke zvláštnímu významu odvětví energetiky a důsledkům, které z jeho možného narušení pro celou Unii vyplývají, by právě toto odvětví mohlo by mít z provádění zátěžových testů na základě společně dohodnutých zásad největší užitek. Uvedené testy spadají do pravomoci členských států, které by měly provozovatele kritické infrastruktury k provádění těchto testů podněcovat a podporovat je v něm, pokud je to vyhodnoceno jako přínosné a v souladu s jejich vnitrostátními právními rámci.

([2]) 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).

([3]) 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).

(10) V zájmu zajištění koordinované a účinné reakce na současné a předpokládané hrozby se Komise vyzývá, aby členským státům poskytla dodatečnou podporu, zejména poskytováním relevantních informací ve formě brífinků, nezávazných příruček a pokynů. Posouzení hrozeb by měla zajišťovat Evropská služba pro vnější činnost (ESVČ), zejména prostřednictvím Zpravodajského a informačního centra EU a jeho střediska pro hybridní hrozby, za podpory zpravodajského ředitelství Vojenského štábu EU (EUMS) v rámci společné zpravodajsko-analytické složky (SIAC). Komise se rovněž vyzývá, aby ve spolupráci s členskými státy podporovala využívání výzkumných a inovačních projektů financovaných Unií.

(11) Vzhledem k rostoucí vzájemné závislosti fyzické a digitální infrastruktury 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. Členské státy se vyzývají, aby co nejdříve urychlily přípravné práce zaměřené na provedení a uplatňování nového právního rámce vztahujícího se na kritické subjekty a posíleného právního rámce pro kybernetickou bezpečnost a vycházely přitom ze zkušeností získaných v rámci skupiny pro spolupráci, zřízené směrnicí (EU) 2016/1148 (dále jen „skupina pro spolupráci v oblasti bezpečnosti sítí a informací“), přičemž je třeba mít na paměti lhůty pro provedení ve vnitrostátním právu a skutečnost, že by tyto přípravné práce měly postupovat souběžným a soudržným způsobem.

(12) Kromě zlepšování připravenosti je rovněž důležité posílit schopnosti rychlé a účinné reakce v případě narušení základních služeb poskytovaných kritickou infrastrukturou. Toto doporučení proto obsahuje opatření na unijní i vnitrostátní úrovni, přičemž mimo jiné zdůrazňuje podpůrnou úlohu a přidanou hodnotu, jíž lze dosáhnout zavedením posílené spolupráce a výměny informací v rámci mechanismu civilní ochrany Unie, zřízeného rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU ([4]), a využíváním relevantních prostředků Kosmického programu Unie, zřízeného nařízením Evropského parlamentu a Rady (EU) 2021/696 ([5]).

(13) Komise, vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“) a skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s příslušnými civilními a vojenskými orgány a agenturami a zavedenými sítěmi, včetně Evropské sítě styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), mají provádět hodnocení rizik a vypracovávat rizikové scénáře. V návaznosti na společnou ministerskou výzvu z Nevers kromě toho skupina pro spolupráci v oblasti bezpečnosti sítí a informací za podpory Komise a Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) v současné době provádí posouzení rizik. Obě činnosti budou probíhat soudržně a v koordinaci s vypracováváním scénářů v rámci mechanismu civilní ochrany Unie, včetně událostí v oblasti kybernetické bezpečnosti a jejich reálného dopadu, na nichž v současné době pracují Komise a členské státy. Předpokládá se, že v zájmu účinnosti, účelnosti a soudržnosti a za účelem řádného uplatňování tohoto doporučení budou výsledky těchto činností zohledněny na vnitrostátní úrovni.

(14) Za účelem okamžitého posílení připravenosti a schopnosti reakce na rozsáhlé kybernetické bezpečnostní incidenty zřídila Komise prostřednictvím dalšího financování přiděleného agentuře ENISA krátkodobý program, který má členským státům poskytnout podporu. Navrhované služby mimo jiné zahrnují opatření v oblasti připravenosti, jako je penetrační testování subjektů s cílem určit zranitelná místa. Uvedený program rovněž může posílit možnosti pomoci členským státům v případě rozsáhlého kybernetického bezpečnostního incidentu s dopadem na kritické subjekty. Jedná se o první krok v souladu se závěry Rady ze dne 23. května 2022 o rozvoji kybernetické pozice Evropské unie („závěry Rady o kybernetické pozici EU“), v nichž se požaduje, aby Komise předložila návrh fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti. Členské státy by měly tyto příležitosti plně využívat v souladu s platnými požadavky a vyzývají se, aby pokračovaly v práci v oblasti řešení kybernetických krizí na úrovni Unie, zejména pravidelným sledováním a vyhodnocováním pokroku dosaženého při provádění plánu pro řešení kybernetických krizí, který v nedávné době vypracovala Rada. Tento plán je „živým dokumentem“ a v případě potřeby by měl být přezkoumán a aktualizován.

([4]) 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).

([5]) Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU (Úř. věst. L 170, 12.5.2021, s. 69).

(15) Zásadní význam pro celosvětovou konektivitu i konektivitu uvnitř EU mají globální podmořské komunikační kabely. 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 digitální a fyzické infrastruktury, na nichž jsou digitální služby založeny, o specifická posouzení rizik a o možnosti zmírňujících opatření týkajících se podmořských komunikačních kabelů. Členské státy vyzývají Komisi, aby za tímto účelem provedla studie a svá zjištění s nimi sdílela.

(16) Hrozby související s digitální infrastrukturou, například v souvislosti s energetickými technologiemi zahrnujícími digitální součásti, mohou mít dopad rovněž na odvětví energetiky a dopravy. Bezpečnost souvisejících dodavatelských řetězců je důležitá pro kontinuitu poskytování základních služeb a pro strategickou kontrolu nad kritickou infrastrukturou v odvětví energetiky. Uvedené okolnosti by měly být zohledněny při přijímání opatření ke zvýšení odolnosti kritické infrastruktury v souladu s tímto doporučením.

(17) Vzhledem k rostoucímu významu kosmické infrastruktury, pozemních prostředků souvisejících s oblastí kosmu, včetně výrobních zařízení, a služeb využívajících kosmického prostoru pro činnosti související s bezpečností je nezbytné zajistit odolnost a ochranu unijních kosmických prostředků a služeb a jejich pozemního segmentu v rámci Unie. Ze stejných důvodů je rovněž nezbytné v rámci tohoto doporučení také strukturovaněji využívat kosmická data a služby poskytované kosmickými systémy a programy pro účely dohledu a sledování a v zájmu ochrany kritické infrastruktury v jiných odvětvích. V připravované kosmické strategii EU pro bezpečnost a obranu budou v tomto ohledu navržena vhodná opatření, která by měla být při provádění tohoto doporučení zohledněna.

(18) Spolupráce na mezinárodní úrovni je rovněž nezbytná pro účinné řešení rizik pro kritickou infrastrukturu, mimo jiné v mezinárodních vodách. Členské státy se tudíž vyzývají, aby spolupracovaly s Komisí a vysokým představitelem a aby v zájmu dosažení uvedené spolupráce podnikly určité kroky, přičemž by měly mít na paměti, že veškeré takové kroky smí být učiněny pouze v souladu s jejich příslušnými úkoly a povinnostmi podle práva Unie, zejména podle ustanovení Smluv týkajících se vnějších vztahů.

(19) Jak je stanoveno ve sdělení ze dne 15. února 2022 nazvaném „Příspěvek Komise k evropské obraně“, v zájmu podpory „Strategického kompasu pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti“ Komise do roku 2023 posoudí ve spolupráci s vysokým představitelem a členskými státy základní hodnoty odvětvové hybridní odolnosti s cílem určit nedostatky a potřeby, jakož i kroky k jejich řešení. Uvedená iniciativa by měla být podkladem pro činnost v rámci tohoto doporučení a měla by pomoci posílit sdílení informací a koordinaci opatření pro další zvýšení odolnosti, včetně odolnosti kritické infrastruktury.

(20) Strategie EU pro námořní bezpečnost z roku 2014 a její revidovaný akční plán obsahovaly výzvu ke zvýšené ochraně kritické námořní infrastruktury, včetně podmořské, 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 i dobrovolné). Zmíněná strategie a akční plán se v současné době aktualizují a budou zahrnovat posílená opatření, jejichž cílem je ochrana kritické námořní infrastruktury. Uvedená opatření by měla doplňovat toto doporučení.

(21) Posílení odolnosti kritické infrastruktury přispívá k širšímu úsilí o boj proti hybridním hrozbám a kampaním namířeným proti Unii a jejím členským státům. Toto doporučení vychází ze společného sdělení Evropskému parlamentu a Radě nazvaného „Společný rámec pro boj proti hybridním hrozbám – reakce Evropské unie“. Opatření č. 1 společného rámce, tedy průzkum týkající se hybridních rizik, hraje klíčovou úlohu při určování zranitelných míst, která mohou potenciálně ovlivnit vnitrostátní a celoevropské struktury a sítě. Kromě toho provádění závěrů Rady ze dne 21. června 2022 o rámci pro koordinovanou reakci EU na hybridní kampaně zajistí důraznější koordinovanou činnost prostřednictvím uplatňování souboru hybridních nástrojů EU ve všech dotčených oblastech.

PŘIJALA TOTO DOPORUČENÍ:

KAPITOLA I: CÍL, OBLAST PŮSOBNOSTI A STANOVENÍ PRIORIT

1. Toto doporučení stanoví řadu cílených opatření na unijní i vnitrostátní úrovni na podporu a posílení odolnosti kritické infrastruktury, a to na dobrovolném základě, se zaměřením na kritickou infrastrukturu se značným přeshraničním významem a v rámci určených klíčových odvětvích, jako je energetika, digitální infrastruktura, doprava a vesmír. Tato cílená opatření spočívají v lepší připravenosti, posílené reakci a mezinárodní spolupráci.

2. Informace sdílené v zájmu naplnění cílů tohoto doporučení, které jsou důvěrné podle unijních a vnitrostátních pravidel, jakož i pravidel pro zachovávání důvěrnosti obchodních informací, by se měly vyměňovat s Komisí a dalšími relevantními orgány pouze v případě, že je taková výměna nutná pro řádné uplatňování tohoto doporučení. Tímto doporučením není dotčena ochrana základních zájmů národní bezpečnosti, veřejné bezpečnosti nebo obrany členských států a od žádného členského státu by se nemělo očekávat, že bude sdílet informace, které jsou s těmito zájmy v rozporu.

KAPITOLA II: LEPŠÍ PŘIPRAVENOST

Opatření na úrovni členských států

3. Členské státy by měly zvážit přístup zohledňující všechna rizika při aktualizaci svých posouzení rizik nebo svých stávajících rovnocenných analýz v souladu s vyvíjející se povahou stávajících hrozeb pro jejich kritickou infrastrukturu, zejména v určených klíčových odvětvích a pokud možno ve všech odvětvích, na něž se vztahuje připravovaný nový právní rámec použitelný na kritické subjekty.

4. Členské státy se vyzývají, aby urychlily přípravné práce a pokud možno přijaly opatření ke zvýšení odolnosti, jak je stanoveno v připravovaném právním rámci použitelném na kritické subjekty, se zvláštním zaměřením na spolupráci a sdílení relevantních informací mezi členskými státy a s Komisí, na určování kritických subjektů se značným přeshraničním významem a na posílení podpory pro určené kritické subjekty s cílem zlepšit jejich odolnost.

5. Členské státy by měly podporovat odbornou přípravu a cvičení odborníků a jejich vzájemné sdílení osvědčených postupů a získaných poznatků. Členské státy by měly odborníky vybízet k účasti na stávajících vzdělávacích vnitrostátních i mezinárodních platformách, například v rámci mechanismu civilní ochrany Unie.

6. Členské státy by měly podněcovat a podporovat provozovatele kritické infrastruktury alespoň v odvětví energetiky v tom, aby v případě, že to bude přínosné, prováděli zátěžové testy podle zásad společně dohodnutých na úrovni Unie. Zátěžové testy by měly posoudit odolnost kritické infrastruktury vůči nepřátelským hrozbám způsobeným člověkem. Členské státy by proto měly usilovat o určení relevantní kritické infrastruktury, která má být testována, a co nejdříve, nejpozději však do konce prvního čtvrtletí roku 2023, konzultovat příslušné provozovatele kritické infrastruktury. Kromě toho by členské státy měly podporovat provozovatele kritické infrastruktury tak, aby uvedené testy provedli co nejdříve a usilovali o jejich dokončení do konce roku 2023, a to v souladu s vnitrostátním právem. Rada má v úmyslu posoudit aktuální stav provádění zátěžových testů do konce dubna 2023.

7. Vzhledem k rychle se vyvíjejícím hrozbám pro kritickou infrastrukturu má zásadní význam zachování vysoké úrovně ochrany. Členské státy se vyzývají, aby vyčlenily dostatečné finanční zdroje na posílení kapacit svých relevantních vnitrostátních orgánů a podporovaly je tak, aby byly schopny zvýšit odolnost kritické infrastruktury. Členské státy se rovněž vyzývají, aby za účelem podpory orgánů odpovědných za řešení rozsáhlých kybernetických bezpečnostních incidentů pro ně vyčlenily dostatečné finanční zdroje a zajistily, aby jejich týmy pro reakci na počítačové bezpečnostní incidenty (týmy CSIRT) a příslušné orgány byly plně mobilizovány v rámci sítě CSIRT a EU-CyCLONe.

8. Členské státy se vyzývají, aby v souladu s platnými požadavky využily potenciálních možností financování na úrovni Unie a na vnitrostátní úrovni k posílení odolnosti kritické infrastruktury v Unii jednak samy a jednak aby vybízely provozovatele kritické infrastruktury, aby těchto možností financování, a to například pro účely transevropských sítí, využívali v zájmu řešení celé škály významných hrozeb, především v rámci programů financovaných z Fondu pro vnitřní bezpečnost, zřízeného nařízením Evropského parlamentu a Rady (EU) 2021/1149 ([6]), Evropského fondu pro regionální rozvoj, zřízeného nařízením Evropského parlamentu a Rady (EU) č. 1301/2013 ([7]), mechanismu civilní ochrany Unie a plánu Komise REPowerEU. Členské státy se rovněž vyzývají, aby co nejlépe využívaly výsledků příslušných projektů v rámci výzkumných programů, jako je Horizont Evropa, zřízený nařízením Evropského parlamentu a Rady (EU) 2021/695 ([8]).

9. Pokud jde o komunikační a síťovou infrastrukturu v Unii, skupina pro spolupráci v oblasti bezpečnosti sítí a informací se vyzývá, aby při současném plnění úkolů v souladu s článkem 11 směrnice (EU) 2016/1148 urychlila svou práci, která probíhá na základě společné ministerské výzvy z Nevers, na cíleném posuzování rizik a co nejdříve předložila první doporučení. Dotčené posouzení rizik by mělo poskytnout informace pro účely probíhajícího meziodvětvového hodnocení kybernetických rizik a scénářů, jak je požadováno v závěrech Rady o kybernetické pozici EU. Uvedená práce by navíc měla být prováděna při zajištění soudržnosti a doplňkovosti s prací, která je vykonávána v rámci pracovní osy skupiny pro spolupráci v oblasti bezpečnosti sítí a informací zaměřené na bezpečnost dodavatelského řetězce informačních a komunikačních technologií a v rámci dalších relevantních skupin.

10. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací se rovněž vyzývá, aby s podporou Komise a agentury ENISA pokračovala ve své práci v oblasti bezpečnosti digitální infrastruktury, a to i v souvislosti s podmořskou infrastrukturou, konkrétně podmořskými komunikačními kabely. Rovněž se vyzývá, aby zahájila svou práci týkající se kosmického odvětví, mimo jiné tím, že v případě potřeby vypracuje politické pokyny a metodiky pro řízení kybernetických bezpečnostních rizik na základě přístupu zohledňujícího všechna rizika a přístupu založeného na posouzení rizik pro subjekty působící v kosmickém odvětví s cílem zvýšit odolnost pozemní infrastruktury podporující poskytování služeb využívajících kosmického prostoru.

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

12. Členské státy by měly plně využívat Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC). Členské státy by měly vybízet svá národní koordinační centra k aktivní spolupráci s členy komunity v oblasti kybernetické bezpečnosti s cílem budovat na unijní i vnitrostátní úrovni kapacity za účelem lepší podpory provozovatelů základních služeb.

13. Je důležité, aby členské státy dokázaly provést opatření doporučená v souboru nástrojů EU pro kybernetickou bezpečnost sítí 5G, a zejména aby zavedly omezení týkající se vysoce rizikových dodavatelů vzhledem k tomu, že časová prodleva může zvýšit zranitelnost sítí v Unii, a rovněž aby posílily 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, aby byla zajištěna jednotná úroveň bezpečnosti a odolnosti sítí 5G.

14. Členské státy by se společně s Komisí a agenturou ENISA měly zaměřit na provedení závěrů Rady ze dne 17. října 2022 o bezpečnosti dodavatelského řetězce IKT.

([6]) Nařízení Evropského parlamentu a Rady (EU) 2021/1149 ze dne 7. července 2021, kterým se zřizuje Fond pro vnitřní bezpečnost (Úř. věst. L 251, 15.7.2021, s. 94).

([7]) Nařízení Evropského parlamentu a Rady (EU) č. 1301/2013 ze dne 17. prosince 2013 o Evropském fondu pro regionální rozvoj, o zvláštních ustanoveních týkajících se cíle Investice pro růst a zaměstnanost a o zrušení nařízení (ES) č. 1080/2006 (Úř. věst. L 347, 20.12.2013, s. 289).

([8]) Nařízení Evropského parlamentu a Rady (EU) 2021/695 ze dne 28. dubna 2021, kterým se zavádí rámcový program pro výzkum a inovace Horizont Evropa a stanoví pravidla pro účast a šíření výsledků a zrušují nařízení (EU) č. 1290/2013 a (EU) č. 1291/2013 (Úř. věst. L 170, 12.5.2021, s. 1).

15. Členské státy by měly zohlednit připravovaný síťový kodex pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny[...], a to na základě zkušeností získaných při provádění směrnice (EU) 2016/1148 a relevantních pokynů vypracovaných skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, zejména jejího referenčního dokumentu o bezpečnostních opatřeních pro provozovatele základních služeb.

16. Členské státy by měly rozvíjet využívání systémů Copernicus, Galileo a evropské služby pro pokrytí geostacionární navigací (EGNOS) pro účely dohledu s cílem sdílet relevantní informace s odborníky svolanými v souladu s bodem 15. Pro monitorování kritické infrastruktury a podporu předvídání krizí a reakce na ně by měly být účelně využívány schopnosti, které poskytuje unijní družicová komunikace v rámci státní správy (GOVSATCOM) Kosmického programu Unie.

Opatření na úrovni Unie

17. Je třeba posílit dialog a spolupráci mezi jmenovanými odborníky členských států a s Komisí za účelem zvýšení fyzické odolnosti kritické infrastruktury, a to zejména:

    a) přispěním k přípravě, vývoji a propagaci společných dobrovolných nástrojů na podporu členských států při zvyšování této odolnosti, včetně metodik a rizikových scénářů;

    b) podporou členských států při provádění nového právního rámce vztahujícího se na kritické subjekty, mimo jiné vybídnutím Komise k včasnému přijetí aktu v přenesené pravomoci;

    c) podporou provádění zátěžových testů uvedených v bodě 6 na základě společných zásad, přičemž jako první přijdou na řadu testy zaměřené na nepřátelské hrozby způsobené člověkem v odvětví energetiky a poté budou následovat testy v dalších klíčových odvětvích, jakož i poskytováním podpory a poradenství při provádění těchto zátěžových testů, a to na žádost členského státu;

    d) využíváním jakékoli bezpečné platformy – jakmile bude zřízena Komisí – ke shromažďování, hodnocení a dobrovolnému sdílení osvědčených postupů, poznatků získaných na základě vnitrostátních zkušeností a dalších informací souvisejících s touto odolností.

    Práce uvedených jmenovaných odborníků by měla být zaměřena obzvláště na meziodvětvové závislosti a kritickou infrastrukturu se značným přeshraničním významem a měla by na ni ve vhodných případech navazovat činnost v rámci Rady a Komise.

18. Členské státy se vyzývají, aby využívaly jakékoliv podpory poskytované Komisí, například v podobě vypracovávání příruček a pokynů, jako je příručka o ochraně kritické infrastruktury a veřejných prostor před systémy bezpilotních letadel, a nástrojů pro posuzování rizik. Evropská služba pro vnější činnost se vyzývá, aby zejména prostřednictvím Zpravodajského a informačního centra EU a jeho jednotky pro hybridní hrozby a za podpory zpravodajského ředitelství Vojenského štábu EU v rámci společné zpravodajsko-analytické složky (SIAC) pořádala brífinky o hrozbách pro kritickou infrastrukturu v Unii s cílem zlepšit situační povědomí.

19. Členské státy by měly podporovat opatření přijatá Komisí k využití výsledků projektů týkajících se odolnosti kritické infrastruktury, které jsou financovány v rámci programů Unie pro výzkum a inovace. Rada bere na vědomí záměr Komise zvýšit v rámci rozpočtu přiděleného na program Horizont Evropa v kontextu víceletého finančního rámce na období 2021–2027 financování tohoto typu odolnosti, aniž by to bylo na úkor financování jiných výzkumných a inovačních projektů v oblasti civilní bezpečnosti v rámci programu Horizont Evropa.

20. Vzhledem k úkolům stanoveným v závěrech Rady o kybernetické pozici EU se Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací vyzývají, aby v souladu se svými příslušnými úkoly a povinnostmi podle práva Unie zintenzivnili spolupráci s relevantními sítěmi a civilními a vojenskými orgány a agenturami při hodnocení rizik a vytváření scénářů rizik v oblasti kybernetické bezpečnosti, a to zejména s ohledem na význam energetiky, digitální infrastruktury, dopravy a kosmické infrastruktury a vzájemnou závislost mezi odvětvími a členskými státy. Tato činnost by měla zohlednit související rizika pro infrastrukturu, kterou uvedená odvětví využívají. Tam, kde je to přínosné, by se hodnocení rizik a vytváření scénářů mohly provádět pravidelně a měly by doplňovat stávající nebo plánovaná posouzení rizik v uvedených odvětvích a vycházet z nich, přičemž by nemělo docházet ke zdvojování úsilí, a měly by být zdrojem informací pro diskuse o tom, jak posílit celkovou odolnost subjektů provozujících kritickou infrastrukturu a jak řešit zranitelná místa.

21. Komise se vyzývá, aby v souladu se svými příslušnými úkoly v rámci řešení kybernetických krizí urychlila své činnosti na podporu připravenosti a reakce členských států na rozsáhlé incidenty v oblasti kybernetické bezpečnosti, a zejména aby:

    a) jako doplněk k relevantním posouzením rizik v kontextu bezpečnosti sítí a informací vypracovala komplexní studii ([9]), která zhodnotí podmořskou infrastrukturu, zejména podmořské komunikační kabely, jež propojují členské státy i Evropu globálně, přičemž závěry této studie by měly být sdíleny s členskými státy;

    b) podporovala připravenost a reakci členských států a orgánů, institucí a jiných subjektů Unie na rozsáhlé incidenty v oblasti kybernetické bezpečnosti nebo významné incidenty v souladu s posíleným právním rámcem pro kybernetickou bezpečnost a dalšími relevantními platnými pravidly ([10]);

    c) urychlila vypracování hlavní koncepce fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti, a to včetně řádné diskuse s členskými státy.

22. Komise se vyzývá, aby zintenzivnila práci na anticipačních opatřeních zaměřených do budoucna, včetně spolupráce 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) a její reakce na narušení kritické infrastruktury; zvýšila investice do preventivních přístupů a připravenosti obyvatelstva a posílila podporu v oblasti budování kapacit v rámci sítě znalostí Unie v oblasti civilní ochrany.

23. Komise by měla podporovat využívání unijních prostředků dohledu (Copernicus, Galileo a EGNOS) s cílem pomoci členským státům při monitorování kritické infrastruktury a v relevantních případech jejich bezprostředního okolí a podporovat i další možnosti dohledu stanovené v Kosmickém programu Unie, jako je rámec pro získávání poznatků o situaci ve vesmíru a rámec EU pro pozorování a sledování vesmíru.

24. V relevantních případech a v souladu se svými příslušnými mandáty se agentury Unie a další relevantní subjekty vyzývají, aby v záležitostech týkajících se odolnosti kritické infrastruktury poskytly podporu, zejména takto:

    a) Agentura Evropské unie pro spolupráci v oblasti prosazování práva (EUROPOL), pokud jde o shromažďování informací, analýzy trestné činnosti a podporu při vyšetřování v rámci přeshraničních donucovacích opatření a ve vhodných a relevantních případech sdílení výsledků s členskými státy;

    b) Evropská agentura pro námořní bezpečnost (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) Agentura Evropské unie pro Kosmický program (EUSPA) a Satelitní středisko Evropské unie (Satcen) mohou případně pomáhat prostřednictvím operací v rámci Kosmického programu Unie;

    d) Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC) by mohlo, pokud jde o činnosti související s kybernetickou bezpečností, i ve spolupráci s agenturou ENISA podporovat inovace a průmyslovou politiku v oblasti kybernetické bezpečnosti.

([9]) Tato studie by měla zahrnovat mapování jejích kapacit a redundancí, zranitelných míst, hrozeb a rizik pro dostupnost služeb, dopady výpadků ve fungování (transatlantických) podmořských kabelů na členské státy a Unii jako celek a zmírňování rizik, přičemž by měla zohledňovat citlivost těchto informací a potřebu je chránit.

([10]) Zvláštní pozornost by měla být rovněž věnována všem činnostem, které připravují účinnou koordinovanou reakci na úrovni Unie v případě závažného přeshraničního kybernetického incidentu nebo související hrozby, které by mohly mít systémový dopad na finanční sektor Unie, jak je stanoveno v novém právním rámci pro digitální provozní odolnost.

KAPITOLA III: POSÍLENÁ REAKCE

Opatření na úrovni členských států

25. Členské státy se vyzývají, aby:

a) v relevantních případech pokračovaly v koordinaci své reakce a udržovaly přehled o meziodvětvové reakci na akutní narušení základních služeb poskytovaných kritickou infrastrukturou. Tyto úkoly by bylo možné provádět v rámci budoucího plánu koordinované reakce na narušení kritické infrastruktury se značným přeshraničním významem; stávajících integrovaných opatření EU pro politickou reakci na krize (IPCR) pro koordinaci politické reakce v případě kritické infrastruktury s přeshraničním významem; plánu pro rozsáhlé kybernetické bezpečnostní incidenty a krize podle doporučení Komise (EU) 2017/1584 ([11]); sítě EU-CyCLONe; v rámci pro koordinovanou reakci EU na hybridní kampaně a souboru hybridních nástrojů EU v případě hybridních hrozeb a kampaní a v rámci systému včasného varování v případě dezinformací;

b) zintenzivnily výměnu informací na operační úrovni se střediskem ERCC v rámci mechanismu civilní ochrany Unie s cílem posílit včasné varování a koordinovat svou reakci v rámci tohoto mechanismu v případě narušení kritické infrastruktury se značným přeshraničním významem, čímž se v případě potřeby zajistí rychlejší reakce zprostředkovaná Unií;

c) zvýšily svou připravenost reagovat v relevantních případech prostřednictvím stávajících nástrojů nebo nástrojů, které budou vyvinuty, na tato významná narušení uvedená v písmenu a);

d) spolupracovaly na dalším rozvoji relevantních kapacit reakce v rámci Evropského souboru civilní ochrany (ECPP) a systému rescEU;

e) vybízely provozovatele kritické infrastruktury a relevantní vnitrostátní orgány, aby zvýšili své kapacity tak, aby bylo možné rychle obnovit elementární výkonnost základních služeb poskytovaných těmito provozovateli kritické infrastruktury;

f) vybízely provozovatele kritické infrastruktury, aby v případě přebudovávání své kritické infrastruktury vybudovali tuto infrastrukturu tak, aby byla co nejodolnější vůči kompletní řadě významných rizik, která pro ni mohou být relevantní, včetně při nepříznivých klimatických scénářích, a to při zohlednění přiměřenosti opatření, pokud jde o posouzení rizik a náklady.

26. Členské státy se vyzývají, aby tam, kde je to možné, urychlily přípravné práce, jak je stanoveno v posíleném právním rámci v oblasti kybernetické bezpečnosti, tím, že se zaměří na posílení schopností vnitrostátních týmů CSIRT s ohledem na nové úkoly týmů CSIRT i na rozšířený počet subjektů z nových odvětví, že včas přezkoumají a zaktualizují své strategie kybernetické bezpečnosti a že co nejdříve přijmou národní plány reakce na incidenty a krize v oblasti kybernetické bezpečnosti, pokud dosud neexistují.

27. Členské státy se vyzývají, aby na vnitrostátní úrovni zvážily nejvhodnější prostředky, jimiž zajistí, aby si relevantní zúčastněné strany byly vědomy nezbytnosti zvýšit odolnost kritické infrastruktury spoluprací s důvěryhodnými prodejci a partnery. Je důležité investovat do dodatečné kapacity, zejména v odvětvích, v nichž je stávající infrastruktura na konci své životnosti, např. infrastruktura podmořských komunikačních kabelů, aby bylo možné zajistit kontinuitu poskytování základních služeb v případě narušení a snížit nežádoucí závislost.

28. Členské státy se vyzývají, aby věnovaly pozornost proaktivní strategické komunikaci na vnitrostátní úrovni v souvislosti s bojem proti hybridním hrozbám a kampaním a s ohledem na skutečnost, že protivníci se mohou snažit zapojovat do zahraniční manipulace s informacemi a vměšování tím, že budou ovlivňovat narativy ohledně incidentů zaměřených na kritickou infrastrukturu.

Opatření na úrovni Unie

29. Komise se vyzývá, aby úzce spolupracovala s členskými státy na dalším rozvoji relevantních orgánů, nástrojů a kapacit pro reakci s cílem zvýšit operační připravenost k řešení bezprostředních a nepřímých dopadů významných narušení relevantních základních služeb poskytovaných kritickou infrastrukturou, zejména s odborníky a zdroji dostupnými prostřednictvím Evropského souboru civilní ochrany a systému rescEU v rámci mechanismu civilní ochrany Unie nebo budoucích týmů rychlé reakce na hybridní hrozby.

([11]) Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

30. Komise se vyzývá, aby s ohledem na vyvíjející se formy hrozeb a ve spolupráci s členskými státy v rámci mechanismu civilní ochrany Unie:

a) průběžně analyzovala a testovala adekvátnost a operační připravenost stávajících kapacit pro reakci;

b) pravidelně sledovala a zjišťovala potenciálně významné nedostatky kapacit pro reakci v rámci Evropského souboru civilní ochrany a kapacit rescEU;

c) dále zintenzivňovala meziodvětvovou spolupráci s cílem zajistit adekvátní reakci na úrovni Unie a ve spolupráci s jedním nebo více členskými státy organizovala pravidelná školení nebo cvičení pro testování této spolupráce;

d) dále rozvíjela středisko ERCC jako meziodvětvové centrum pro mimořádné situace na úrovni Unie ke koordinaci podpory pro postižené členské státy.

31. Rada je odhodlána zahájit práci s cílem schválit plán koordinované reakce na narušení kritické infrastruktury se značným přeshraničním významem, který popisuje a stanoví cíle a způsoby spolupráce mezi členskými státy a orgány, institucemi a jinými subjekty Unie při reakci na incidenty namířené proti uvedené kritické infrastruktuře. Rada se zájmem očekává návrh tohoto plánu, vypracovaný |Komisí, který bude vycházet z podpory a přispění relevantních agentur Unie. Plán musí být plně soudržný a interoperabilní s revidovaným operačním protokolem Unie pro boj proti hybridním hrozbám („EU Playbook“), má zohledňovat stávající plán pro koordinovanou reakci na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty ([12]) a krize a mandát sítě EU-CyCLONe stanovený ve směrnici NIS2 a zamezovat zdvojování struktur a činností. Tento plán by měl plně respektovat stávající opatření IPCR pro koordinaci reakce.

32. Komise se vyzývá, aby vedla konzultace s relevantními zúčastněnými stranami a odborníky ohledně vhodných opatření v souvislosti s možnými významnými incidenty týkajícími se podmořské infrastruktury, která mají být předložena spolu s hodnotící studií uvedenou v bodě 20 písm. a), a aby dále rozvíjela krizové plánování, rizikové scénáře a cíle Unie v oblasti odolnosti vůči katastrofám stanovené v rozhodnutí č. 1313/2013/EU.

KAPITOLA IV: MEZINÁRODNÍ SPOLUPRÁCE

Opatření na úrovni členských států

33. Členské státy by měly ve vhodných případech a v souladu s právem Unie spolupracovat s relevantními třetími zeměmi, pokud jde o odolnost kritické infrastruktury se značným přeshraničním významem.

34. Členské státy se vyzývají, aby spolupracovaly s Komisí a vysokým představitelem s cílem účinně řešit rizika pro kritickou infrastrukturu v mezinárodních vodách.

35. 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 ze dne 21. června 2022 o rámci pro koordinovanou reakci EU na hybridní kampaně a následně je používaly, aby byl uvedený rámec plně účinný, zejména při zvažování a přípravě komplexních a koordinovaných reakcí Unie na hybridní kampaně a hybridní hrozby, včetně hrozeb namířených proti provozovatelům kritické infrastruktury.

([12]) Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Opatření na úrovni Unie

36. Komise a vysoký představitel se vyzývají, aby ve vhodných případech a v souladu se svými příslušnými úkoly a povinnostmi podle práva Unie podporovaly relevantní třetí země s cílem zvýšit odolnost kritické infrastruktury na jejich území, a zejména kritické infrastruktury, která je fyzicky propojena s jejich územím a územím členského státu.

37. Komise a vysoký představitel v souladu se svými příslušnými úkoly a povinnostmi podle práva Unie posílí koordinaci s NATO v oblasti odolnosti kritické infrastruktury společného zájmu prostřednictvím strukturovaného dialogu mezi EU a NATO o odolnosti, a to při plném respektování pravomocí Unie a členských států v souladu se Smlouvami a klíčovými zásadami, jimiž se řídí spolupráce mezi EU a NATO, jak byly dohodnuty Evropskou radou, zejména zásadou reciprocity, inkluzivností a rozhodovací samostatností. V této souvislosti bude uvedená spolupráce pokračovat v rámci strukturovaného dialogu o odolnosti mezi EU a NATO, který je začleněn do stávajícího mechanismu fungujícího mezi zaměstnanci obou těchto subjektů a určeného pro provádění společných prohlášení, přičemž bude zajištěna plná transparentnost a účast všech členských států.

38. Komise se vyzývá, aby v nezbytných a vhodných případech zvážila účast zástupců relevantních třetích zemí v rámci spolupráce a výměny informací mezi členskými státy v oblasti odolnosti kritické infrastruktury, která je fyzicky propojena s územím členského státu a územím třetí země.

V Bruselu dne 8. prosince 2022.

Za Radu
předseda
V. RAKUŠAN