Rada
Evropské unie

Brusel 8. října 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

POZNÁMKA K BODU „I/A“

Odesílatel:	Generální sekretariát Rady
Příjemce:	Výbor stálých zástupců (část II)/Rada
Předmět:	Závěry Rady o prozkoumání potenciálu iniciativy ke zřízení společné kybernetické jednotky, která by doplnila koordinovanou reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize – schválení

1. Dne 23. června 2021 zveřejnila Komise své doporučení o vybudování společné kybernetické jednotky[1] pro řešení rostoucího počtu závažných kybernetických incidentů, které mají dopad na veřejné služby, jakož i na život podniků a občanů v celé Evropské unii.

2. Komise toto doporučení předložila na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 28. června 2021. V průběhu slovinského předsednictví proběhla další jednání během zasedání Pracovní skupiny pro mezinárodní spolupráci na vysoké úrovni (HWPCI) ve dnech 7. a 14. července 2021 s cílem shromáždit názory členských států na doporučení Komise.

[1] Dokument C(2021)4520 final (11155/21 a 11155/21 ADD1).

3. Na neformální videokonferenci členů HWPCI dne 23. července 2021 předložilo předsednictví první návrh závěrů Rady o prozkoumání potenciálu iniciativy ke zřízení společné kybernetické jednotky, která by doplnila koordinovanou reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[2]. Tento návrh závěrů byl dále projednán na zasedáních členů Pracovní skupiny na vysoké úrovni pro mezinárodní spolupráci ve dnech 8. a 29. září 2021.

4. Na zasedání dne 6. října 2021 se Pracovní skupina na vysoké úrovni pro mezinárodní spolupráci dohodla na návrhu závěrů Rady ve znění uvedeném v příloze.

5. S ohledem na výše uvedené skutečnosti se Výbor stálých zástupců vyzývá, aby návrh závěrů Rady ve znění uvedeném v příloze předložil Radě a navrhl jí, aby tento návrh závěrů přijala v rámci bodů „A“ pořadu jednání.

---

[2] Dokument 10975/21.

PŘÍLOHA

Návrh závěrů Rady o prozkoumání potenciálu iniciativy ke zřízení společné kybernetické jednotky, která by doplnila koordinovanou reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize

RADA EVROPSKÉ UNIE,

PŘIPOMÍNAJÍC své závěry o:

– strategii kybernetické bezpečnosti EU pro digitální dekádu[3],

– koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[4],

– kybernetické diplomacii[5],

– rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“)[6],

– bezpečnosti a obraně[7],

– politický rámec EU pro kybernetickou obranu[8],

– utváření digitální budoucnosti Evropy[9],

– prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize,

---

3 Dokument 7290/21.
4 Dokument 10086/18.
5 Dokument 6122/15 + COR 1.
6 Dokument 10474/17.
7 Dokument 8396/21.
8 Dokument 15585/14.
9 Dokument 8711/20.

– společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“[10],

– budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU[11],

1. ZDŮRAZŇUJE význam kybernetické bezpečnosti pro budování odolné, digitální a zelené Evropy. ZDŮRAZŇUJE, že kybernetická bezpečnost je nezbytná pro prosperitu a bezpečnost EU a jejích členských států, jejích občanů, podniků a institucí, jakož i pro zachování integrity našich svobodných a demokratických společností.

2. UZNÁVÁ přeshraniční a meziodvětvovou povahu mnoha hrozeb v oblasti kybernetické bezpečnosti a rizika a potenciální důsledky soustavných kampaní nepřátelských činností v kyberprostoru, které mají větší dopad, jsou sofistikovanější, cílenější, komplexnější, trvalejší a ve větší míře všudypřítomné[12]. Pandemie COVID-19 dále odhalila slabiny našich společností a potenciální škody způsobené rozsáhlými kybernetickými incidenty na hospodářství, demokracii, základních službách a kritické infrastruktuře, zejména ve zdravotnictví. Zvýšila rovněž význam konektivity a závislosti společnosti na spolehlivých, důvěryhodných a bezpečných sítích a informačních systémech. V konečném důsledku zdůraznila potřebu globálního, otevřeného, svobodného, stabilního a bezpečného internetu, jakož i důvěru v produkty, procesy a služby informačních a komunikačních technologií a jejich bezpečnost, včetně potřeby zajistit odolný dodavatelský řetězec.

---

10 Dokument 14435/17 + COR 1.
11 Dokument 7737/19.
12 Zpráva agentury ENISA o typech ohrožení za rok 2020.

3. ZNOVU ZDŮRAZŇUJE význam kybernetické odolnosti a dalšího rozvoje rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti[13] s cílem účinně a včas reagovat na úrovni EU na rozsáhlé kybernetické bezpečnostní incidenty a krize a dále jej začlenit do stávajících horizontálních a odvětvových mechanismů EU pro řešení krizí. ZDŮRAZŇUJE úlohu Rady a integrovaných opatření EU pro politickou reakci na krize (IPCR) při zajišťování včasné koordinace a reakce na politické úrovni Unie v případě krizí, které vznikly uvnitř Unie nebo mimo ni a které mají dalekosáhlý dopad nebo politický význam. ZDŮRAZŇUJE význam testování takových rámců a mechanismů při pravidelných cvičeních.

4. PŘIPOMÍNÁ, že činnosti na úrovni EU v souvislosti s rozsáhlými kybernetickými bezpečnostními incidenty a krizemi probíhají v souladu se zásadami subsidiarity, proporcionality, doplňkovosti, nezdvojování a důvěrnosti. OPAKUJE, že primární odpovědnost za reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize, které se jich týkají, nesou členské státy. PŘIPOMÍNÁ, že je důležité respektovat pravomoci členských států a jejich výlučnou odpovědnost za národní bezpečnost v souladu s čl. 4 odst. 2 Smlouvy o Evropské unii, a to i v oblasti kybernetické bezpečnosti.

5. Zároveň PŘIPOMÍNÁ, že je důležité respektovat pravomoci a mandáty orgánů, institucí a jiných subjektů EU. Vysoký představitel, Komise a další orgány, instituce a jiné subjekty EU hrají rovněž zásadní úlohu vyplývající z právních předpisů Unie, mimo jiné z důvodu možného dopadu rozsáhlých kybernetických bezpečnostních incidentů a krizí na jednotný trh, jakož i na fungování samotných orgánů, institucí a jiných subjektů EU.

[13] Dokument 10086/18.

6. ZDŮRAZŇUJE, že je třeba zabránit zbytečnému zdvojování činností a usilovat o doplňkovost a přidanou hodnotu při dalším rozvoji rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti a zajistit soulad se stávajícími mechanismy, iniciativami, sítěmi, procesy a postupy na vnitrostátní a evropské úrovni. ZDŮRAZŇUJE, že je důležité zjednodušit stávající procesy a struktury s cílem snížit složitost a v zájmu soudržnosti v Unii zlepšit dostupnost a schopnost reagovat na žádosti o pomoc a solidaritu.

7. UZNÁVÁ použitelnost mezinárodního práva, včetně Charty Organizace spojených národů jako celku, mezinárodního humanitárního práva a lidských práv v kyberprostoru, a PODPORUJE dodržování dobrovolných nezávazných norem, pravidel a zásad odpovědného chování státu v kyberprostoru, které schválily všechny členské státy OSN.

8. VÍTÁ pokrok, jehož bylo v posledních letech dosaženo v Radě, zejména v Horizontální pracovní skupině pro otázky kybernetiky (HWPCI) a dalších příslušných pracovních skupinách Rady, jakož i při přípravě dalších iniciativ, sítí a mechanismů v oblasti spolupráce a sdílení informací mezi členskými státy, zejména v rámci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací a sítě CSIRT zřízené směrnicí Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, dále v rámci Sítě styčných organizací pro řešení kybernetických krizí (CyCLONe), jakož i v rámci příslušných projektů souvisejících s kybernetickou obranou zahájených v rámci stálé strukturované spolupráce (PESCO)[14], v rámci společné pracovní skupiny pro kyberkriminalitu (J-CAT), Evropské justiční sítě pro boj proti kyberkriminalitě (EJCN), dobrovolných příspěvků členských států Zpravodajskému a informačnímu centru EU (EU INTCEN) a konečně v rámci koordinace a spolupráce v souvislosti se souborem nástrojů pro diplomacii v oblasti kybernetiky.

[14] Zejména projekt „týmů rychlé kybernetické reakce a vzájemné pomoci v oblasti kybernetické bezpečnosti“ koordinovaný Litvou, „Koordinační středisko pro kybernetický a informační prostor“ koordinované Německem a „platforma pro sdílení informací o kybernetických hrozbách a reakci na incidenty“ koordinovaná Řeckem.

9. PŘIPOMÍNÁ stávající rámce pro spolupráci mezi orgány, institucemi a jinými subjekty EU, jako je strukturovaná spolupráce mezi agenturou ENISA a skupinou CERT-EU, a memorandum o porozumění mezi agenturou ENISA, Evropskou obrannou agenturou (EDA), Evropským centrem Europolu pro boj proti kyberkriminalitě (EC3) a skupinou CERT-EU. ZDŮRAZŇUJE, že je důležité pokračovat v pravidelném sdílení informací s Radou o dalším vývoji v těchto rámcích pro spolupráci.

10. ZDŮRAZŇUJE, že je důležité posílit spolupráci a sdílení informací mezi různými kybernetickými komunitami v rámci EU a jejích členských států na všech nezbytných úrovních – technické, operační a strategické/politické – a propojit stávající mechanismy krizového řízení, sítě, struktury, procesy a postupy, pokud to podporuje a zlepšuje řešení rozsáhlých kybernetických incidentů a krizí.

11. BERE NA VĚDOMÍ pokrok dosažený skupinou členských států při vytváření společné operační kybernetické schopnosti „týmy rychlé kybernetické reakce“ v rámci PESCO, jejímž cílem je prohloubit dobrovolnou spolupráci v kybernetické oblasti prostřednictvím vzájemné pomoci, a to i v reakci na rozsáhlé kybernetické incidenty a krize.

12. BERE NA VĚDOMÍ zkušenosti donucovacích orgánů a jejich schopnost reagovat 24 hodin denně a sedm dní v týdnu v oblasti operativní spolupráce a bezpečné výměny informací v boji proti přeshraničním kybernetickým útokům prostřednictvím protokolu EU o vymáhání práva v případě nouze.

13. UZNÁVÁ pokračující provádění rámce pro společnou diplomatickou reakci EU na nepřátelskou činnost v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“). PŘIPOMÍNÁ, že každý členský stát může v jednotlivých případech přijmout své vlastní svrchované rozhodnutí ohledně připisování nepřátelské činnosti v kyberprostoru. PŘIPOMÍNÁ, že opatření přijatá v rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru by měla být založena na sdílených poznatcích o situaci dohodnutých mezi členskými státy. Středisko EU INTCEN plní pro EU ústřední úlohu jakožto centra pro poskytování poznatků o situaci a posuzování hrozeb v oblasti kybernetických otázek, a to na základě dobrovolných zpravodajských příspěvků členských států a aniž jsou dotčeny jejich pravomoci.

14. ZNOVU ZDŮRAZŇUJE význam vzájemné pomoci a solidarity v souladu s čl. 42 odst. 7 Smlouvy o Evropské unii a s článkem 222 Smlouvy o fungování Evropské unie a VYZÝVÁ k dalším cvičením s kybernetickým rozměrem. PŘIPOMÍNÁ, že je třeba uvažovat o propojení rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti, souboru nástrojů pro diplomacii v oblasti kybernetiky a ustanovení výše uvedených článků v případě rozsáhlých kybernetických incidentů nebo krizí. Dále PŘIPOMÍNÁ, že povinnostmi členských států vyplývajícími z čl. 42 odst. 7 Smlouvy o Evropské unii není dotčena zvláštní povaha bezpečnostní a obranné politiky některých členských států. PŘIPOMÍNÁ také, že NATO zůstává základem kolektivní obrany pro státy, které jsou jeho členy.

15. UZNÁVÁ spolupráci mezi EU a NATO v oblasti kybernetické bezpečnosti a obrany, včetně sdílení informací mezi skupinou CERT-EU a složkou NATO pro schopnost reakce na počítačové incidenty (NCIRC), a to při plném respektování zásad transparentnosti, reciprocity a inkluzivnosti, jakož i rozhodovací samostatnosti obou organizací.

16. UZNÁVÁ význam případné spolupráce se soukromým sektorem, pokud jde o sdílení informací, a poskytování příslušných odborných znalostí, jakož i důvěryhodných řešení a služeb, a to i například při podpoře reakce na incidenty a posilování poznatků o situaci mezi různými kybernetickými komunitami.

17. ZDŮRAZŇUJE význam zabezpečených komunikačních kanálů pro výměnu utajovaných a citlivých informací. ZDŮRAZŇUJE, že je třeba dosáhnout dalšího pokroku.

V tomto ohledu a s ohledem na výše uvedené,

18. BERE NA VĚDOMÍ doporučení Komise o vybudování společné kybernetické jednotky jakožto iniciativu, kterou je třeba při dalším rozvíjení rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti zvážit[15].

19. VYZÝVÁ EU a její členské státy, aby pokračovaly ve svém úsilí o vytvoření komplexnějšího a účinnějšího rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti, který bude vycházet ze stávajících mechanismů a z již dosaženého pokroku, a aby postupným přístupem vzaly pro doplnění těchto mechanismů v úvahu potenciál iniciativy ke zřízení společné kybernetické jednotky. ZDŮRAZŇUJE, že postupný, transparentní a inkluzivní proces má zásadní význam pro posílení důvěry, a je proto nepostradatelný pro další rozvíjení rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti. Tento proces by měl respektovat stávající úlohy, pravomoci a mandáty členských států a orgánů, institucí a jiných subjektů EU, jakož i zásady uvedené v těchto závěrech, včetně proporcionality, subsidiarity, inkluzivnosti, doplňkovosti, nezdvojování a důvěrnosti informací. Zároveň ZDŮRAZŇUJE, že jakákoli případná účast na případné společné kybernetické jednotce nebo příspěvek k ní ze strany členských států je dobrovolné povahy.

[15] Dokument C(2021)4520 final (11155/21 a 11155/21 ADD1).

20. ZDŮRAZŇUJE, že je třeba zavést odpovídající pracovní metody a řízení s cílem umožnit zapojení a účast všech členských států na jednáních, rozvoji a účinných rozhodovacích procesech týkajících se rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti, včetně případné iniciativy ke zřízení společné kybernetické jednotky. VYZÝVÁ, aby bylo respektováno právo Rady vyplývající ze Smluv a zásady loajální spolupráce.

21. ZDŮRAZŇUJE, že je důležité identifikovat a zapojit všechny příslušné kybernetické komunity v rámci EU a jejích členských států a zároveň zohlednit jejich různé úlohy a povinnosti v různých typech rozsáhlých kybernetických incidentů a krizí. ZDŮRAZŇUJE zásadní úlohu Rady, zejména prostřednictvím Horizontální pracovní skupiny pro otázky týkající se kybernetiky, při tvorbě politik a koordinační funkci, pokud jde o další rozvoj rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti. VYZÝVÁ proto členské státy, Komisi, Evropskou službu pro vnější činnost (ESVČ), středisko EU INTCEN, skupinu CERT-EU, agenturu ENISA, Europol (EC3), Eurojust (EJCN), Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost (ECCC), jakož i zástupce sítě CSIRT, sítě CyCLONe, skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, Evropské obranné agentury a příslušných projektů PESCO, jakož i další možné zúčastněné strany, aby se do tohoto procesu zapojily. Mohla by být podrobněji prozkoumána možnost vytvoření pracovní skupiny, jak je navrženo v doporučení Komise, a to při zajištění odpovídajícího zastoupení všech členských států a pod politickým vedením Rady, přičemž by tato skupina sloužila jako dočasné fórum sdružující zástupce všech příslušných kybernetických komunit v členských státech a v rámci EU. Tato pracovní skupina by měla pravidelně podávat zprávy o své činnosti a předkládat Radě případné návrhy k projednání, potvrzení a návrhy dalšího postupu. Kromě toho by mohly být zavedeny další formy dialogu v rámci komunit i mezi nimi, mimo jiné prostřednictvím workshopů, seminářů, společné odborné přípravy a cvičení.

22. ZDŮRAZŇUJE úlohu Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (ECCC) a sítě národních koordinačních center ve vztahu k případné společné kybernetické jednotce, zejména s ohledem na její úlohu při podstatném zvýšení technologických kapacit, technologických řešení, schopností a dovedností Unie v oblasti kybernetické bezpečnosti.

23. VYZÝVÁ EU a její členské státy, aby se zapojily do dalšího rozvíjení rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti, mimo jiné prozkoumáním potenciálu iniciativy ke zřízení společné kybernetické jednotky, stanovením a vymezením procesu, včetně milníků a harmonogramu, jakož i vyjasněním cílů a možných úloh a povinností. ZDŮRAZŇUJE, že je třeba prioritně konsolidovat stávající sítě a interakce v rámci každé komunity a provést důkladné zmapování možných nedostatků a potřeb ohledně sdílení informací v rámci kybernetických komunit i mezi nimi a rovněž v rámci evropských orgánů, institucí a agentur i mezi nimi, a následně se dohodnout na možných hlavních cílech a prioritách případné společné kybernetické jednotky. Aniž by byl předjímán výsledek, ZDŮRAZŇUJE, že je třeba se zaměřit na určení potřeb v oblasti sdílení informací s cílem vytvořit společné poznatky o situaci mezi všemi příslušnými komunitami. Při zjišťování nedostatků a potřeb v oblasti sdílení informací, včetně možného využívání virtuálních platforem, by měla být i nadále věnována náležitá pozornost zabezpečeným komunikačním kanálům pro výměnu utajovaných a citlivých informací, přičemž ZDŮRAZŇUJE význam využití již existující infrastruktury. Zavedení postupného přístupu má vybudovat důvěru a základ pro možné další kroky související se zlepšením připravenosti a operativní spolupráce. UZNÁVÁ, že různé cíle by mohly vyžadovat různá řešení a zapojení různých skupin zástupců příslušných kybernetických komunit v rámci EU a jejích členských států.

24. VYZÝVÁ k dalšímu posouzení právního základu pro případné zřízení společné kybernetické jednotky během celého procesu, včetně posouzení úkolů a úloh ve vztahu k úkolům a úlohám přiděleným agentuře ENISA v doporučení s ohledem na článek 7 nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019. VYZÝVÁ k dalšímu zamyšlení nad jednotlivými prvky doporučení o vybudování společné kybernetické jednotky, mimo jiné s ohledem na myšlenku týmů pro rychlou reakci EU v oblasti kybernetické bezpečnosti a na plán reakce EU na kybernetické bezpečnostní incidenty a krize. ZDŮRAZŇUJE, že případná společná kybernetická jednotka musí respektovat pravomoci, mandáty a právní pravomoci svých případných budoucích účastníků.

25. VYZÝVÁ EU a její členské státy, aby zvážily potenciál iniciativy ke zřízení společné kybernetické jednotky, a to i z pohledu orgánů, institucí a agentur EU, s cílem doplnit stávající úsilí na úrovni členských států. VÍTÁ záměr Komise posílit odolnost příslušných orgánů, institucí a agentur EU prostřednictvím jejího připravovaného návrhu nařízení o společných závazných pravidlech pro kybernetickou bezpečnost pro orgány, instituce a jiné subjekty EU.

26. Závěrem POTVRZUJE svůj závazek posílit kybernetickou odolnost a dále rozvíjet rámec EU pro řešení krizí v oblasti kybernetické bezpečnosti a BUDE PRAVIDELNĚ MONITOROVAT pokrok a poskytovat další pokyny pro doplnění rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti.