Rada
Európskej únie

V Bruseli 20. októbra 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	19. októbra 2021
Komu:	Delegácie
Č. predch. dok.:	12534/21
Predmet:	Závery Rady o preskúmaní potenciálu iniciatívy na zriadenie spoločnej kybernetickej jednotky, ktorou sa dopĺňa koordinovaná reakcia EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu – závery Rady (19. októbra 2021)

Delegáciám v prílohe zasielame závery Rady o preskúmaní potenciálu iniciatívy na zriadenie spoločnej kybernetickej jednotky, ktorou sa dopĺňa koordinovaná reakcia EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu, ktoré Rada prijala na svojom zasadnutí 19. októbra 2021.

PRÍLOHA

Závery Rady o preskúmaní potenciálu iniciatívy na zriadenie spoločnej kybernetickej jednotky, ktorou sa dopĺňa koordinovaná reakcia EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNAJÚC:

– závery o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu[1],

– závery o koordinovanej reakcii EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu[2],

– závery o kybernetickej diplomacii[3],

– závery o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“)[4],

– závery o bezpečnosti a obrane[5],

– politický rámec EÚ pre kybernetickú obranu[6],

– závery o formovaní digitálnej budúcnosti Európy[7],

– vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu,

---

1 7290/21
2 10086/18
3 6122/15 + COR 1
4 10474/17
5 8396/21
6 15585/14
7 8711/20

– závery o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ[8],

– závery o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ[9],

1. ZDÔRAZŇUJE význam kybernetickej bezpečnosti pre budovanie odolnej, digitálnej a zelenej Európy. ZDÔRAZŇUJE, že kybernetická bezpečnosť je nevyhnutná pre prosperitu a bezpečnosť EÚ a jej členských štátov, jej obyvateľov, podnikov a inštitúcií, ako aj pre zachovanie integrity našich slobodných a demokratických spoločností.

2. UZNÁVA cezhraničný a medziodvetvový charakter mnohých kybernetickobezpečnostných hrozieb a rizík a potenciálne dôsledky škodlivých kybernetických činností, ktoré sa vykonávajú nepretržite a s väčším dosahom a ktoré sú čoraz viac rafinované, cielené, komplexné, trvácne a/alebo prenikavé[10]. Pandémia COVID-19 ešte viac odhalila zraniteľné miesta našich spoločností a potenciál škôd spôsobených rozsiahlymi kybernetickými incidentmi, pokiaľ ide o hospodárstvo, demokraciu, základné služby a kritickú infraštruktúru, najmä v sektore zdravotníctva. Zvýšil sa aj význam prepojenosti a závislosti spoločnosti od spoľahlivých, dôveryhodných a bezpečných sietí a informačných systémov. Pandémia napokon zdôraznila potrebu globálneho, otvoreného, slobodného, stabilného a bezpečného internetu, ako aj dôvery v produkty, procesy a služby informačných a komunikačných technológií (IKT) a ich bezpečnosť vrátane potreby zabezpečiť odolný dodávateľský reťazec.

---

8 14435/17 + COR 1

9 7737/19

10 Panoráma hrozieb 2020, ENISA.

3. Opätovne ZDÔRAZŇUJE význam kybernetickej odolnosti a ďalšieho rozvoja rámca EÚ pre krízové riadenie kybernetickej bezpečnosti[11] zameraného na účinnú a včasnú reakciu na úrovni EÚ na rozsiahle kybernetické incidenty a krízy a jeho hlbšie začlenenie do existujúcich horizontálnych a odvetvových mechanizmov reakcie EÚ na krízy. PODČIARKUJE úlohu Rady a integrovaných dojednaní o politickej reakcii na krízu (IPCR) pri zabezpečovaní včasnej koordinácie a reakcie na politickej úrovni Únie v prípade kríz, ktoré majú rozsiahly vplyv alebo politický význam, bez ohľadu na to, či vzniknú v Únii alebo mimo nej. VYZDVIHUJE význam testovania takýchto rámcov a mechanizmov počas pravidelných cvičení.

4. PRIPOMÍNA, že opatrenia na úrovni EÚ v súvislosti s rozsiahlymi kybernetickými incidentmi a krízami sa vykonávajú v súlade so zásadami subsidiarity, proporcionality, komplementárnosti, neduplicity a dôvernosti. OPAKUJE, že členské štáty nesú primárnu zodpovednosť za reakciu na rozsiahle kybernetickobezpečnostné incidenty a krízy, ktoré sa ich týkajú. PRIPOMÍNA, že je dôležité rešpektovať právomoci členských štátov a ich výhradnú zodpovednosť za národnú bezpečnosť v súlade s článkom 4 ods. 2 Zmluvy o Európskej únii, a to aj v oblasti kybernetickej bezpečnosti.

5. Zároveň PRIPOMÍNA, že je dôležité rešpektovať právomoci a mandáty inštitúcií, orgánov a agentúr EÚ. Vysoký predstaviteľ, Komisia a iné inštitúcie, orgány a agentúry EÚ takisto zohrávajú zásadnú úlohu vyplývajúcu z práva Únie, a to aj z dôvodu možného vplyvu rozsiahlych kybernetickobezpečnostných incidentov a kríz na jednotný trh, ako aj na fungovanie samotných inštitúcií, orgánov a agentúr EÚ.

[11] 10086/18

6. ZDÔRAZŇUJE, že pri ďalšom rozvoji rámca EÚ pre krízové riadenie kybernetickej bezpečnosti je potrebné vyhnúť sa zbytočnej duplicite, usilovať sa o komplementárnosť a pridanú hodnotu a zabezpečiť súlad s existujúcimi mechanizmami, iniciatívami, sieťami, procesmi a postupmi na vnútroštátnej a európskej úrovni. PODČIARKUJE význam racionalizácie existujúcich procesov a štruktúr s cieľom znížiť zložitosť a v záujme súdržnosti v Únii zlepšiť prístupnosť a schopnosť reagovať voči tým, ktorí žiadajú o pomoc a solidaritu.

7. UZNÁVA uplatniteľnosť medzinárodného práva vrátane Charty Organizácie Spojených národov v celom rozsahu, medzinárodného humanitárneho práva a práva v oblasti ľudských práv v kybernetickom priestore a PODPORUJE dodržiavanie dobrovoľných, nezáväzných noriem, pravidiel a zásad zodpovedného správania sa štátov v kybernetickom priestore, ktoré schválili všetky členské štáty OSN.

8. VÍTA pokrok, ktorý sa v posledných rokoch dosiahol v Rade, najmä v horizontálnej pracovnej skupine pre kybernetické otázky (HWPCI) a iných príslušných pracovných skupinách Rady, ako aj pri vytváraní ďalších iniciatív, sietí a mechanizmov spolupráce a výmeny informácií medzi členskými štátmi, najmä skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a siete CSIRT, ktorá bola zriadená smernicou Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016, ako aj v rámci siete styčných organizácií pre kybernetické krízy (CyCLONe), ako aj príslušných projektov v oblasti kybernetickej obrany v rámci stálej štruktúrovanej spolupráce (PESCO)[12], spoločnej pracovnej skupiny pre počítačovú kriminalitu (J-CAT), Európskej justičnej siete na boj proti počítačovej kriminalite (EJCN), dobrovoľných príspevkov členských štátov do EU INTCEN a koordinácie a spolupráce v kontexte súboru nástrojov kybernetickej diplomacie.

[12] Konkrétne projekt „tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti“ koordinovaný Litvou, projekt „koordinačné centrum pre kybernetickú a informačnú oblasť“ koordinované Nemeckom a projekt „platforma na výmenu informácií v oblasti reakcie na kybernetické hrozby a incidenty“, ktorý koordinuje Grécko.

9. PRIPOMÍNA existujúce rámce spolupráce medzi inštitúciami, orgánmi a agentúrami EÚ, ako je štruktúrovaná spolupráca medzi agentúrou ENISA a tímom CERT-EU, a memorandum o porozumení medzi agentúrou ENISA, Európskou obrannou agentúrou (EDA), Európskym centrom boja proti počítačovej kriminalite (EC3) Europolu a tímom CERT-EU. ZDÔRAZŇUJE význam pokračujúcej pravidelnej výmeny informácií s Radou o ďalšom vývoji v týchto rámcoch spolupráce.

10. PODČIARKUJE význam posilnenia spolupráce a výmeny informácií medzi rôznymi kybernetickými komunitami v EÚ a jej členských štátoch na všetkých potrebných úrovniach – technickej, operačnej a strategickej/politickej – a prepojenia existujúcich mechanizmov, sietí, štruktúr, procesov a postupov krízového riadenia tam, kde sa tým podporuje a zlepšuje riešenie rozsiahlych kybernetických incidentov a kríz.

11. UZNÁVA pokrok, ktorý dosiahla skupina členských štátov pri budovaní spoločnej operačnej kybernetickej spôsobilosti v podobe „tímov rýchlej kybernetickej reakcie“ v rámci PESCO s cieľom prehĺbiť dobrovoľnú spoluprácu v kybernetickej oblasti prostredníctvom vzájomnej pomoci, a to aj v reakcii na rozsiahle kybernetické incidenty a krízy.

12. UZNÁVA skúsenosti a spôsobilosť komunity orgánov presadzovania práva reagovať 24 hodín denne a 7 dní v týždni v oblasti operačnej spolupráce a zabezpečenej výmeny informácií, pokiaľ ide o boj proti závažným cezhraničným kybernetickým útokom, a to prostredníctvom protokolu reakcie na núdzové situácie v oblasti presadzovania práva v EÚ.

13. UZNÁVA pokračujúce vykonávanie rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor nástrojov kybernetickej diplomacie“). PRIPOMÍNA, že každý členský štát môže prijať vlastné zvrchované rozhodnutie, pokiaľ ide o pripísanie zodpovednosti za škodlivú kybernetickú činnosť, ktoré závisí od prípadu k prípadu. PRIPOMÍNA, že opatrenia prijaté v rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti by mali vychádzať zo spoločného situačného povedomia, na ktorom sa dohodnú členské štáty. EU INTCEN zohráva ústrednú úlohu ako centrum pre poskytovanie situačného povedomia a posudzovania hrozieb v kybernetických otázkach pre EÚ, a to na základe dobrovoľných spravodajských príspevkov členských štátov a bez toho, aby boli dotknuté ich právomoci.

14. Opätovne ZDÔRAZŇUJE význam vzájomnej pomoci a solidarity v súlade s článkom 42 ods. 7 Zmluvy o Európskej únii a článkom 222 Zmluvy o fungovaní Európskej únie a VYZÝVA na ďalšie cvičenia s kybernetickým rozmerom. PRIPOMÍNA, že je v prípade kybernetického incidentu alebo krízy veľkého rozsahu potrebné zvážiť prepojenia medzi rámcom EÚ pre krízové riadenie kybernetickej bezpečnosti, súborom nástrojov kybernetickej diplomacie a ustanoveniami uvedených článkov. Ďalej PRIPOMÍNA, že povinnosťami, ktoré pre členské štáty vyplývajú z článku 42 ods. 7 Zmluvy o Európskej únii, nie je dotknutá osobitná povaha bezpečnostnej a obrannej politiky niektorých členských štátov. PRIPOMÍNA tiež, že NATO zostáva základom kolektívnej obrany pre tie štáty, ktoré sú jeho členmi.

15. UZNÁVA spoluprácu medzi EÚ a NATO v oblasti kybernetickej bezpečnosti a obrany vrátane výmeny informácií medzi tímom CERT-EU a spôsobilosťou NATO pre reakciu na počítačové incidenty (NCIRC) pri plnom dodržiavaní zásad transparentnosti, reciprocity a inkluzívnosti, ako aj rozhodovacej autonómie oboch organizácií.

16. UZNÁVA význam prípadnej spolupráce so súkromným sektorom, pokiaľ ide o výmenu informácií a poskytovanie príslušných odborných znalostí, ako aj dôveryhodných riešení a služieb, a to napríklad aj pri podpore reakcie na incidenty a posilňovaní situačného povedomia medzi rôznymi kybernetickými komunitami.

17. ZDÔRAZŇUJE význam zabezpečených komunikačných kanálov na výmenu utajovaných skutočností a citlivých informácií. PODČIARKUJE potrebu ďalšieho pokroku.

V tejto súvislosti a so zreteľom na uvedené skutočnosti:

18. UZNÁVA odporúčanie Komisie o zriadení spoločnej kybernetickej jednotky ako iniciatívu, ktorá sa má zvážiť pri ďalšom rozvoji rámca EÚ pre krízové riadenie kybernetickej bezpečnosti[13].

19. VYZÝVA EÚ a jej členské štáty, aby pokračovali vo svojom úsilí o komplexnejší a účinnejší rámec EÚ pre krízové riadenie kybernetickej bezpečnosti, pričom by mali vychádzať z existujúcich mechanizmov a dosiahnutého pokroku, a aby postupným prístupom zohľadnili potenciál iniciatívy spoločnej kybernetickej jednotky dopĺňať tieto mechanizmy. ZDÔRAZŇUJE, že prírastkový, transparentný a inkluzívny proces je nevyhnutný na posilnenie dôvery, a preto je rozhodujúci pre ďalší rozvoj rámca EÚ pre krízové riadenie kybernetickej bezpečnosti. Tento proces by mal rešpektovať existujúce úlohy, právomoci a mandáty členských štátov a inštitúcií, orgánov a agentúr EÚ, ako aj zásady uvedené v týchto záveroch vrátane proporcionality, subsidiarity, inkluzívnosti, komplementárnosti, neduplicity a dôvernosti informácií. Zároveň PODČIARKUJE, že akákoľvek prípadná účasť členských štátov v spoločnej kybernetickej jednotke, ak sa zriadi, alebo ich súvisiace príspevky sú dobrovoľnej povahy.

[13] C(2021)4520 final (11155/21 a 11155/21 ADD1)

20. ZDÔRAZŇUJE, že je potrebné zaviesť primerané pracovné metódy a systém správy s cieľom umožniť zapojenie a účasť všetkých členských štátov na rokovaniach, rozvoji a účinných rozhodovacích procesoch týkajúcich sa rámca EÚ pre krízové riadenie kybernetickej bezpečnosti, a to aj pokiaľ ide o iniciatívu prípadnej spoločnej kybernetickej jednotky. VYZÝVA, aby sa rešpektovali výsadné práva Rady vyplývajúce zo zmlúv a zásada lojálnej spolupráce.

21. ZDÔRAZŇUJE, že je dôležité identifikovať a zapojiť všetky relevantné kybernetické komunity v EÚ a jej členských štátoch a zároveň zohľadniť ich rozdielne úlohy a povinnosti pri rôznych typoch rozsiahlych kybernetických incidentov a kríz. PODČIARKUJE kľúčovú úlohu Rady, najmä prostredníctvom HWPCI, pri tvorbe politík a koordinačnej funkcii v súvislosti s ďalším rozvojom rámca EÚ pre krízové riadenie kybernetickej bezpečnosti. VYZÝVA preto členské štáty, Komisiu, Európsku službu pre vonkajšiu činnosť (ESVČ), centrum EU INTCEN, tím CERT-EU, agentúru ENISA, Europol (EC3), Eurojust (EJCN), Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC), ako aj zástupcov siete jednotiek CSIRT, siete CyCLONe, skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, agentúry EDA a príslušných projektov PESCO, ako aj ďalších možných zainteresovaných strán, aby sa zapojili do tohto procesu. Mohla by sa bližšie preskúmať prípadná pracovná skupina, ako sa navrhuje v odporúčaní Komisie, v ktorej by sa zabezpečilo primerané zastúpenie všetkých členských štátov a ktorá by konala pod politickým usmernením Rady a slúžila by ako dočasné fórum združujúce zástupcov všetkých relevantných kybernetických komunít v členských štátoch a EÚ. Takáto pracovná skupina by mala pravidelne podávať správy o svojej činnosti a predkladať Rade prípadné návrhy na prerokovanie, schválenie a ďalšie usmernenie. Okrem toho by sa mohli zaviesť ďalšie formy dialógu v rámci komunít a medzi nimi, a to aj prostredníctvom workshopov, seminárov, spoločnej odbornej prípravy a cvičení.

22. ZDÔRAZŇUJE úlohu Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC) a siete národných koordinačných centier vo vzťahu k prípadnej spoločnej kybernetickej jednotke, najmä vzhľadom na jej úlohu podstatne zvýšiť technologické kapacity, technologické riešenia, spôsobilosti a zručnosti Únie v oblasti kybernetickej bezpečnosti.

23. VYZÝVA EÚ a jej členské štáty, aby sa zapojili do ďalšieho rozvoja rámca EÚ pre krízové riadenie kybernetickej bezpečnosti, a to aj preskúmaním potenciálu iniciatívy na zriadenie spoločnej kybernetickej jednotky, stanovením a vymedzením procesu vrátane míľnikov a harmonogramu, ako aj spresnením cieľov a prípadných úloh a povinností. ZDÔRAZŇUJE, že je potrebné prioritne konsolidovať existujúce siete a interakcie v každej komunite, ako aj dôkladne zmapovať prípadné nedostatky a potreby v oblasti výmeny informácií v rámci kybernetických komunít a medzi nimi, ako aj v rámci európskych inštitúcií, orgánov a agentúr a medzi nimi, a následne dospieť k dohode o možných hlavných cieľoch a prioritách prípadnej spoločnej kybernetickej jednotky. Bez toho, aby bol dotknutý výsledok, PODČIARKUJE, že je potrebné zamerať sa na identifikáciu potrieb v oblasti výmeny informácií s cieľom vybudovať spoločné situačné povedomie všetkých príslušných komunít. Pri identifikácii nedostatkov a potrieb v oblasti výmeny informácií vrátane prípadného využitia virtuálnych platforiem by sa mala naďalej venovať náležitá pozornosť zabezpečeným komunikačným kanálom na výmenu utajovaných skutočností a citlivých informácií, pričom ZDÔRAZŇUJE význam využívania už existujúcej infraštruktúry. Zavedenie postupného prístupu je zamerané na budovanie dôvery a základu pre prípadné ďalšie kroky týkajúce sa zlepšovania pripravenosti a operačnej spolupráce. UZNÁVA, že rôzne ciele si môžu vyžadovať rôzne riešenia a zapojenie iného súboru zástupcov príslušných kybernetických komunít v EÚ a jej členských štátoch.

24. VYZÝVA na ďalšie preskúmanie právneho základu pre prípadnú spoločnú kybernetickú jednotku počas celého procesu vrátane posúdenia úloh a povinností vo vzťahu k úlohám a povinnostiam, ktoré sa v odporúčaní pridelili agentúre ENISA, vzhľadom na článok 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019. VYZÝVA na ďalšie úvahy o jednotlivých prvkoch odporúčania o spoločnej kybernetickej jednotke, a to aj so zreteľom na myšlienku tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti a na plán reakcie EÚ na kybernetickobezpečnostné incidenty a krízy. ZDÔRAZŇUJE, že prípadná spoločná kybernetická jednotka musí rešpektovať kompetencie, mandáty a zákonné právomoci svojich možných budúcich účastníkov.

25. VYZÝVA EÚ a jej členské štáty, aby zvážili potenciál iniciatívy spoločnej kybernetickej jednotky, a to aj z pohľadu inštitúcií, orgánov a agentúr EÚ s cieľom doplniť úsilie, ktoré sa vyvíja na úrovni členských štátov. VÍTA zámer Komisie posilniť odolnosť príslušných inštitúcií, orgánov a agentúr EÚ prostredníctvom jej pripravovaného návrhu nariadenia o spoločných záväzných pravidlách v oblasti kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ.

26. Na záver OPÄTOVNE POTVRDZUJE svoj záväzok zvyšovať kybernetickú odolnosť a rozvíjať rámec EÚ pre krízové riadenie kybernetickej bezpečnosti a BUDE PRAVIDELNE MONITOROVAŤ pokrok v tejto súvislosti a poskytovať ďalšie usmernenia na dopĺňanie tohto rámca.