Rada
Európskej únie

V Bruseli 6. júna 2025
(OR. en)

9794/25

Medziinštitucionálny spis:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	6. júna 2025
Komu:	Delegácie
Predmet:	Odporúčanie Rady týkajúce sa koncepcie EÚ pre riadenie kybernetickobezpečnostných kríz – odporúčanie Rady, ktoré Rada schválila na svojom zasadnutí 6. júna 2025

Delegáciám zasielame odporúčanie Rady, ktoré Rada schválila na svojom zasadnutí 6. júna 2025.

PRÍLOHA

ODPORÚČANIE RADY

týkajúce sa koncepcie EÚ pre riadenie kybernetických kríz

RADA EURÓPSKEJ ÚNIE

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

so zreteľom na návrh Európskej komisie,

keďže:

(1) Digitálne technológie a globálna pripojiteľnosť predstavujú základ hospodárskeho rastu, konkurencieschopnosti a transformácie kritickej infraštruktúry Únie. Prepojené a čoraz digitalizovanejšie hospodárstvo však zvyšuje aj riziko kybernetickobezpečnostných incidentov a kybernetických útokov. Rastúce geopolitické napätie, konflikty a strategické súperenie sa navyše odrážajú vo vplyve, objeme a sofistikovanosti škodlivých kybernetických činností. Takéto činnosti môžu byť súčasťou hybridných kampaní alebo vojenských operácií. Môžu takisto priamo ovplyvniť bezpečnosť, hospodárstvo a spoločnosť Únie. Okrem toho majú potenciál presahovania, najmä ak sú zamerané na medzinárodné strategické partnerské krajiny, ako sú kandidátske alebo susedné krajiny.

(2) Rozsiahly kybernetickobezpečnostný incident môže spôsobiť narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo môže mať významný vplyv na viac ako jeden členský štát. Takýto incident by sa mohol v závislosti od svojej príčiny a dosahu vystupňovať a prerásť do naplno prepuknutej krízy, ktorá ovplyvní riadne fungovanie vnútorného trhu alebo bude predstavovať vážne riziká pre verejnú bezpečnosť a ochranu subjektov alebo občanov vo viacerých členských štátoch alebo v Únii ako celku. Účinné krízové riadenie je nevyhnutné na zachovanie hospodárskej stability a ochranu európskych vlád, kritickej infraštruktúry, podnikov a občanov, pričom zároveň prispieva k medzinárodnej bezpečnosti a stabilite v kybernetickom priestore. Riadenie kybernetických kríz je preto neoddeliteľnou súčasťou celkového rámca EÚ pre krízové riadenie.

(3) Vzhľadom na vzájomnú závislosť a prepojenia medzi IKT prostrediami subjektov Únie a členských štátov by incident v rámci subjektu Únie mohol predstavovať kybernetickobezpečnostné riziko pre členské štáty a naopak. Výmena relevantných informácií a koordinácia v súvislosti s rozsiahlymi kybernetickobezpečnostnými incidentmi, ako aj závažnými incidentmi v zmysle vymedzenia v článku 3 bode 8 nariadenia (EÚ, Euratom) 2023/2841[1] má zásadný význam v kontexte koncepcie EÚ pre riadenie kybernetických kríz (ďalej len „kybernetická koncepcia“).

[1] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841 z 13. decembra 2023, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (Ú. v. EÚ L, 2023/2841, 18.12.2023, s. 1 – 27.).

(4) V prípade krízy, v dôsledku ktorej boli aktivované dojednania EÚ o integrovanej politickej reakcii na krízu podľa vykonávacieho rozhodnutia Rady (EÚ) 2018/1993[2] (ďalej len „dojednania o IPCR“), by sa v rámci kybernetickej koncepcie mali v plnej miere dodržiavať dojednania o IPCR týkajúce sa koordinácie a reakcie. Politická a strategická koordinácia by sa uskutočňovala v rámci IPCR. Dojednania o IPCR sú nástrojom horizontálnej koordinácie a reakcie na politickej úrovni Únie. Podľa dojednaní o IPCR rozhodnutie aktivovať alebo deaktivovať IPCR prijíma predsedníctvo Rady Európskej únie. Správy o integrovanej situačnej informovanosti a analýze (ISAA), ktoré vypracúvajú útvary Komisie a Európska služba pre vonkajšiu činnosť (ďalej len „ESVČ“), podporujú prácu v rámci IPCR v jej režime výmeny informácií, ako aj v režime úplnej aktivácie.

(5) Primárnu zodpovednosť za zvládanie kybernetickobezpečnostných incidentov a kybernetických kríz nesú členské štáty. Potenciálna cezhraničná a medziodvetvová povaha kybernetickobezpečnostných incidentov si však vyžaduje, aby členské štáty a príslušné subjekty Únie spolupracovali na technickej, operačnej a politickej úrovni s cieľom účinne koordinovať svoju činnosť v celej Únii. Celý životný cyklus riadenia kybernetickej krízy zahŕňa pripravenosť a spoločné situačné povedomie s cieľom predvídať rozsiahle kybernetickobezpečnostné incidenty, potrebné spôsobilosti odhaľovania na určenie potrebných nástrojov na reakciu a zotavenie s cieľom zmierňovať rozsiahle kybernetickobezpečnostné incidenty a zamedziť ich šíreniu, ako aj spôsobilosti reakcie na odrádzanie od ďalších incidentov a zabránenie ich vzniku.

[2] Vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu (Ú. v. EÚ L 320, 17.12.2018, s. 28 – 34).

(6) V odporúčaní Komisie (EÚ) 2017/1584[3] o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa stanovujú ciele a spôsoby spolupráce medzi členskými štátmi a subjektmi Únie pri reakcii na rozsiahle kybernetickobezpečnostné incidenty a kybernetické krízy. Zmapovali sa v ňom príslušní aktéri na technickej, operačnej a politickej úrovni a vysvetlilo sa, ako boli začlenení do existujúcich mechanizmov krízového riadenia Únie, ako sú dojednania o IPCR. Základné zásady stanovené v odporúčaní (EÚ) 2017/1584, konkrétne subsidiarita, komplementárnosť a dôvernosť informácií, ako aj trojúrovňový prístup (na technickej, operačnej a politickej úrovni), zostávajú v platnosti. Toto odporúčanie vychádza z uvedených základných zásad a jeho cieľom je nahradiť odporúčanie (EÚ) 2017/1584 a stanoviť nový rámec Únie pre riadenie kybernetickobezpečnostných kríz.

(7) Niektoré vymedzenia pojmov použité v tomto odporúčaní sú založené na vymedzeniach a pojmoch použitých v smernici (EÚ) 2022/2555[4]. Rozsah pôsobnosti tohto odporúčania sa však líši od rozsahu pôsobnosti smernice (EÚ) 2022/2555. V tomto odporúčaní sa stanovuje rámec Únie pre riadenie kybernetických kríz v kontexte celkovej pripravenosti EÚ na rozsiahle kybernetickobezpečnostné incidenty a kybernetické krízy vyplývajúce z takýchto incidentov – bez ohľadu na to, ktoré odvetvie alebo subjekt sú zasiahnuté. Pokiaľ je to možné, vymedzenia pojmov sú založené na vymedzeniach pojmov uvedených v smernici (EÚ) 2022/2555.

---

[3] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36 – 58).

[4] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80 – 152).

(8) Aktualizovaná kybernetická koncepcia je potrebná na poskytnutie jasných a prístupných usmernení, v ktorých sa vysvetľuje, čo je rozsiahly kybernetickobezpečnostný incident alebo kybernetická kríza na úrovni Únie, ako sa aktivuje rámec pre krízové riadenie, aké sú úlohy príslušných sietí, aktérov a mechanizmov na úrovni Únie a ako prebieha interakcia medzi týmito aktérmi a mechanizmami počas celého životného cyklu kybernetickej krízy. Cieľom kybernetickej koncepcie je podporiť širší rámec civilno-vojenských vzťahov EÚ v kontexte riadenia kybernetických kríz, a to aj v súvislosti s prehlbovaním vzťahov medzi EÚ a NATO, ak je to možné, aj prostredníctvom inkluzívnych, recipročných a nediskriminačných posilnených mechanizmov výmeny informácií v rámci riadenia kybernetických kríz.

(9) Malo by sa posilniť medziodvetvové krízové riadenie na úrovni Únie, aby sa umožnila integrovaná reakcia na krízu, najmä v prípadoch, keď majú rozsiahle kybernetickobezpečnostné incidenty a krízy fyzické následky. Týmto odporúčaním sa dopĺňajú dojednania o IPCR a iné mechanizmy krízového riadenia Únie vrátane všeobecného systému Komisie v oblasti rýchleho varovania ARGUS, mechanizmu Únie v oblasti civilnej ochrany (ďalej len „UCPM“) podporovaného Koordinačným centrom pre reakcie na núdzové situácie (ďalej len „ERCC“) zriadeným v rámci UCPM rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ o mechanizme Únie v oblasti civilnej ochrany[5] (ďalej len „rozhodnutie o UCPM“), mechanizmu reakcie ESVČ na krízy (ďalej len „CRM“), ako aj iných procesov, ako sú procesy opísané v súbore nástrojov kybernetickej diplomacie EÚ[6], súbor nástrojov na boj proti hybridným hrozbám[7] a v revidovanom protokole EÚ na boj proti hybridným hrozbám[8]. Zároveň sa ním dopĺňa odporúčanie Rady (EÚ) 2024/4371 o koncepcii koordinovanej reakcie Únie na narušenia kritickej infraštruktúry so značným cezhraničným významom[9] (ďalej len „koncepcia kritickej infraštruktúry EÚ“), ktorá sa vzťahuje na nekybernetickú fyzickú odolnosť a ktorej cieľom je zlepšiť koordináciu reakcie na úrovni Únie v tejto oblasti, a malo by s ním byť v súlade.

---

5 Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924 – 947).

6 Závery Rady o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti (9916/17).

7 Závery Rady o rámci pre koordinovanú reakciu EÚ na hybridné kampane, 21. júna 2022.

8 Spoločný pracovný dokument útvarov – Protokol EÚ na boj proti hybridným hrozbám [SWD(2023) 116 final].

9 Ú. v. EÚ C, C/2024/4371, 5.7.2024.

(10) Európska sieť styčných organizácií pre kybernetické krízy (ďalej len „sieť EU-CyCLONe“) je sieť na koordináciu riadenia rozsiahlych kybernetickobezpečnostných incidentov a kríz na operačnej úrovni, a to aj v prípade medziodvetvových rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz. S cieľom ďalej neskomplikovať existujúce rámce by sa malo zabrániť vytváraniu odvetvových štruktúr, ktorými by sa zdvojili úlohy siete EU-CyCLONe. Sieť EU-CyCLONe by mala dostávať operačné informácie týkajúce sa kybernetickej bezpečnosti aj od odvetví a poskytovať vstupy na politickej úrovni.

(11) Členské štáty sa nabádajú, aby v plnej miere využívali finančné zdroje, ktoré sú k dispozícii na kybernetickú bezpečnosť v rámci príslušných programov Únie. Malo by sa zabezpečiť, aby tieto programy predstavovali minimálne administratívne zaťaženie pre žiadateľov o financovanie a aby sa uľahčila účasť členských štátov na týchto programoch poskytnutím príslušných usmernení o reálnych možnostiach finančnej podpory.

(12) Toto odporúčanie prispieva k širším opatreniam v oblasti pripravenosti, ktoré sa vyžadujú od Únie v súvislosti s medziodvetvovými krízami v súlade so zásadami zakotvenými v stratégii Únie v oblasti pripravenosti, konkrétne k integrovanému prístupu zohľadňujúcemu všetky riziká, celú verejnú správu a celú spoločnosť, najmä pokiaľ ide o zlepšenie povedomia o rizikách a hrozbách a medziodvetvovú reakciu na krízu,

PRIJALA TOTO ODPORÚČANIE:

I: Cieľ, rozsah pôsobnosti a usmerňujúce zásady rámca EÚ pre riadenie kybernetických kríz

Cieľ a rozsah pôsobnosti

1. V tomto odporúčaní týkajúcom sa koncepcie EÚ pre riadenie kybernetických kríz (ďalej len „kybernetická koncepcia“) sa stanovuje rámec Únie pre riadenie kybernetických kríz v kontexte celkovej pripravenosti EÚ na rozsiahle kybernetickobezpečnostné incidenty a kybernetické krízy. Rámec odráža úlohy členských štátov aj inštitúcií, orgánov, úradov a agentúr Únie (ďalej len „subjekty Únie“) v medziach ich príslušných právomocí pri plnom rešpektovaní vnútroštátnych právnych predpisov a vnútorných pravidiel s cieľom zabezpečiť komplexnú a koordinovanú činnosť na úrovni Únie.

2. Kybernetická koncepcia by sa mala uplatňovať v súlade s koncepciou kritickej infraštruktúry EÚ, najmä v prípade incidentov, ktoré majú vplyv na fyzickú odolnosť aj kybernetickú bezpečnosť kritickej infraštruktúry[10].

3. Kybernetická koncepcia poskytuje usmernenia pre reakciu na rozsiahle kybernetickobezpečnostné incidenty alebo kybernetické krízy a mala by sa používať ako doplnok ku všetkým relevantným odvetvovým mechanizmom reakcie, ako sú mechanizmy uvedené v prílohe II. Príslušné zainteresované strany v oblasti kybernetickej bezpečnosti by mali pomáhať a asistovať pri dosahovaní cieľov týchto odvetvových mechanizmov na vnútroštátnej úrovni aj na úrovni Únie.

4. V prípade celoeurópskej medziodvetvovej krízy s kybernetickými aspektmi, v súvislosti s ktorou sa aktivuje IPCR, by koordináciu reakcie na politickej úrovni Únie mala vykonávať Rada prostredníctvom dojednaní o IPCR. V prípade aktivácie IPCR by opatrenia v rámci kybernetickej koncepcie mali podporovať reakciu EÚ na politickej úrovni a poskytovať konkrétnu podporu v oblasti kybernetickej bezpečnosti.

[10] Koordinácia v takýchto prípadoch sa v koncepcii kritickej infraštruktúry EÚ podrobnejšie opisuje v časti I oddiele 4 jej prílohy.

Usmerňujúce zásady

5. Pri riadení kybernetických kríz na úrovni Únie sa uplatňujú tieto usmerňujúce zásady:

a) *Proporcionalita*: väčšina kybernetickobezpečnostných incidentov, ktoré zasahujú členské štáty, nedosahuje úroveň, ktorá by sa mohla považovať za rozsiahly vnútroštátny alebo únijný kybernetickobezpečnostný incident alebo kybernetickú krízu. V prípade kybernetickobezpečnostných incidentov a hrozieb členské štáty dobrovoľne spolupracujú a vymieňajú si informácie, a to pravidelne v rámci siete jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „sieť jednotiek CSIRT“) a siete EU-CyCLONe v súlade so štandardnými operačnými postupmi (ďalej len „SOP“) týchto sietí.

b) *Subsidiarita*: Členské štáty nesú primárnu zodpovednosť za reakciu a nápravu v prípade kybernetickobezpečnostného incidentu, rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy, ktoré ich zasiahnu. Vzhľadom na potenciálne cezhraničné účinky by Rada, Komisia, vysoký predstaviteľ, Agentúra Európskej únie pre kybernetickú bezpečnosť (ďalej len „agentúra ENISA“), tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach Únie (ďalej len „CERT-EU“), Europol a všetky ostatné príslušné subjekty Únie mali spolupracovať počas celého životného cyklu krízy. Táto úloha vyplýva z práva Únie a odzrkadľuje, ako kybernetickobezpečnostné incidenty a kybernetické krízy ovplyvňujú jedno alebo viacero odvetví hospodárskej činnosti na jednotnom trhu, bezpečnosť a medzinárodné vzťahy Únie, ako aj samotné inštitúcie Únie.

c) *Komplementárnosť*: v tomto odporúčaní sa v plnej miere zohľadňujú existujúce mechanizmy krízového riadenia na úrovni Únie uvedené v prílohe II, konkrétne dojednania o IPCR, ARGUS a mechanizmus reakcie ESVČ na krízy. V tomto odporúčaní sa zohľadňujú mandáty siete jednotiek CSIRT a siete EU-CyCLONe, ako aj nariadenie (EÚ, Euratom) 2023/2841. V prípade aktivovania IPCR by mala práca príslušných sietí, subjektov a aktivovaných odvetvových mechanizmov pokračovať, mala by prispievať k politickej a strategickej koordinácii, ktorá prebieha v rámci IPCR, a mala by ju podporovať.

d) *Dôvernosť informácií*: pri každej výmene informácií v kontexte tohto odporúčania by sa mali rešpektovať platné pravidlá bezpečnosti a ochrany osobných údajov. Vo vhodných prípadoch by sa mali zohľadniť neformálne dohody o nezverejňovaní informácií, ako je napríklad semaforový protokol na označovanie citlivých informácií. Na výmenu utajovaných skutočností by sa bez ohľadu na použitý systém utajenia mali popri dostupných akreditovaných nástrojoch používať existujúce záväzné pravidlá a dohody o spracúvaní utajovaných skutočností.

6. V súlade s uvedenými usmerňujúcimi zásadami by členské štáty a subjekty Únie mali prehĺbiť svoju spoluprácu v oblasti riadenia kybernetických kríz, pričom by mali posilňovať vzájomnú dôveru a využívať existujúce siete a mechanizmy. Táto spolupráca v rámci kybernetickej koncepcie ťaží z vykonávania článkov 22 a 23 nariadenia (EÚ, Euratom) 2023/2841. Najmä plán riadenia kybernetických kríz vypracovaný na základe článku 23 nariadenia (EÚ, Euratom) 2023/2841 okrem iného prispieva k pravidelnej výmene relevantných informácií medzi subjektmi Únie a s členskými štátmi a vymedzuje dojednania týkajúce sa koordinácie a toku informácií medzi subjektmi Únie.

II: Vymedzenie pojmov

7. Na účely tejto kybernetickej koncepcie sa uplatňuje toto vymedzenie pojmov:

a) „incident“ je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov;

b) „významný incident“ je incident, ktorý:

a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu;

b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu;

c) „rozsiahly kybernetickobezpečnostný incident“ je incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty;

d) „kybernetická kríza“ je rozsiahly kybernetickobezpečnostný incident, ktorý sa vystupňuje do naplno prepuknutej krízy, ktorá neumožňuje riadne fungovanie vnútorného trhu alebo predstavuje vážne riziká pre verejnú bezpečnosť a ochranu subjektov alebo občanov v niekoľkých členských štátoch alebo v Únii ako celku.

III: Vnútroštátne štruktúry a zodpovednosť v oblasti riadenia kybernetických kríz

8. Členské štáty nesú primárnu zodpovednosť za reakciu v prípade rozsiahlych kybernetickobezpečnostných incidentov alebo kybernetických kríz, ktoré ich zasiahnu. Každý členský štát má v súlade so smernicou (EÚ) 2022/2555 jeden alebo viacero orgánov pre riadenie kybernetických kríz, ako aj jednu alebo viacero jednotiek CSIRT.

9. Prijatím smernice (EÚ) 2022/2555 a iných legislatívnych a nelegislatívnych nástrojov v oblasti kybernetickej bezpečnosti členské štáty zosúlaďujú svoje rámce kybernetickej bezpečnosti stanovením minimálnych pravidiel týkajúcich sa fungovania koordinovaného regulačného rámca, stanovením mechanizmov účinnej spolupráce medzi zodpovednými orgánmi v každom členskom štáte a zabezpečovaním účinných prostriedkov nápravy a opatrení na presadzovanie práva, ktoré sú kľúčové pre účinné presadzovanie týchto povinností.

10. V súlade s článkom 9 ods. 4 smernice (EÚ) 2022/2555 by členské štáty mali prijať národné plány reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy. Tieto plány zahŕňajú okrem iného vnútroštátne opatrenia v oblasti pripravenosti, postupy riadenia kybernetických kríz a vnútroštátne postupy a dojednania medzi vnútroštátnymi orgánmi a inštitúciami na zabezpečenie ich účinnej účasti na koordinovanom riadení rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz na úrovni Únie a jeho podpory. Postupy riadenia kybernetických kríz zahŕňajú aj ustanovenia o ich začlenení do všeobecného vnútroštátneho rámca krízového riadenia a kanálov na výmenu informácií.

11. V súlade s článkom 9 ods. 1 smernice (EÚ) 2022/2555 by členské štáty mali zabezpečiť súlad s platnými rámcami pre všeobecné vnútroštátne krízové riadenie. V prípade aktivácie IPCR by vnútroštátne orgány pre krízové riadenie mali na účely poskytovania informácií pre IPCR zhromažďovať vstupy od orgánov pre riadenie kybernetických kríz a vnútroštátnych odvetvových krízových mechanizmov.

12. V súlade s článkom 9 ods. 5 smernice (EÚ) 2022/2555 by si sieť EU-CyCLONe mala na žiadosť dotknutého členského štátu vymieňať informácie o príslušných častiach národných plánov reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy, najmä o ustanoveniach na zabezpečenie účinnej účasti na koordinovanom riadení rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz a jeho podpore na úrovni Únie, s cieľom vymieňať si najlepšie postupy a posúdiť, či by celkový rámec fungoval v praxi.

13. Sieť EU-CyCLONe a Medziinštitucionálna rada pre kybernetickú bezpečnosť (ďalej len „IICB“) sa vyzývajú, aby si vo vhodných prípadoch vymieňali informácie o súdržnosti plánu krízového riadenia vypracovaného IICB v súlade s článkom 23 nariadenia (EÚ, Euratom) 2023/2841 s národnými plánmi reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy.

14. Sieť EU-CyCLONe by mala s podporou agentúry ENISA ako svojho sekretariátu viesť aktualizovaný zoznam vnútroštátnych orgánov pre riadenie kybernetických kríz s kontaktnými údajmi úradníkov a vedúcich pracovníkov siete EU-CyCLONe a sprístupniť ho členom siete EU-CyCLONe.

IV: Hlavné siete a aktéri v ekosystéme EÚ pre riadenie kybernetických kríz

15. Sieť jednotiek CSIRT je hlavnou technickou sieťou na výmenu relevantných informácií o incidentoch, najmä v rozsahu pôsobnosti tohto odporúčania, v súlade s príslušnými úlohami opísanými v článku 15 ods. 3 smernice (EÚ) 2022/2555. Prispieva k zvyšovaniu dôvernosti a dôvery a podporuje rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi. Predseda siete jednotiek CSIRT sa môže zúčastňovať na činnosti IICB ako pozorovateľ.

16. CERT-EU je útvarom kybernetickej bezpečnosti pre všetky subjekty Únie. CERT-EU pôsobí ako centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti pre subjekty Únie v súlade s článkom 13 nariadenia (EÚ) 2023/2841. CERT-EU je členom siete jednotiek CSIRT a podporuje Komisiu v sieti EU-CyCLONe. CERT-EU pôsobí na technickej úrovni a je zodpovedný za koordináciu riadenia závažných incidentov, ktoré majú vplyv na subjekty Únie.

17. Sieť EU-CyCLONe pôsobí ako sprostredkovateľ medzi technickou a politickou úrovňou, najmä počas rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz. V súlade s článkom 16 smernice (EÚ) 2022/2555 podporuje koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz na operačnej úrovni a zabezpečuje pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Predseda siete EU-CyCLONe sa môže zúčastňovať na činnosti IICB ako pozorovateľ.

18. ENISA je agentúra Únie, ktorá vykonáva úlohy pridelené podľa nariadenia (EÚ) 2019/881[11] na účely dosiahnutia vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii, a to aj aktívnou podporou členských štátov a inštitúcií, orgánov a agentúr Únie. Agentúra ENISA okrem iného zabezpečuje sekretariát pre sieť jednotiek CSIRT a sieť EU-CyCLONe, služby situačného povedomia a pomáha členským štátom pravidelným organizovaním kybernetickobezpečnostných cvičení na úrovni Únie. V súlade so smernicou (EÚ) 2022/2555 a nariadením (EÚ) 2024/2847[12] agentúra ENISA dostáva informácie o významných cezhraničných incidentoch a aktívne využívaných zraniteľných miestach a incidentoch ovplyvňujúcich digitálne produkty.

19. Rada Európskej únie (ďalej len „Rada“) je inštitúcia, ktorá podľa článku 16 Zmluvy o Európskej únii (ďalej len „ZEÚ“) vykonáva funkcie tvorby politík a koordinačné funkcie a je poverená vykonávaním IPCR týkajúcej sa koordinácie a reakcie na politickej úrovni Únie. Rada pôsobí prostredníctvom zložení Rady, Výboru stálych predstaviteľov a príslušných prípravných orgánov Rady, najmä horizontálnej pracovnej skupiny pre kybernetické otázky (ďalej len „HWPCI“), a v relevantných prípadoch aj na základe dojednaní o IPCR.

---

11 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15 – 69).

12 Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, s.1 – 81).

20. Komisia ako inštitúcia, ktorá podporuje všeobecný záujem Únie a na tento účel prijíma vhodné iniciatívy, ako aj zabezpečuje uplatňovanie zmlúv a opatrení prijatých inštitúciami podľa článku 17 ZEÚ, je zodpovedná za určitú všeobecnú pripravenosť na úrovni Únie a určité opatrenia v oblasti situačného povedomia vrátane riadenia ERCC a spoločného systému komunikácie a poskytovania informácií v prípade núdzových situácií (ďalej len „CECIS“) v súlade s rozhodnutím o UCPM. Na operačnej úrovni uľahčuje súdržnosť a koordináciu medzi súvisiacimi opatreniami v oblasti reakcie na krízu na úrovni Únie. Konzultuje sa s ňou o rozhodnutiach aktivovať alebo deaktivovať IPCR. Útvary Komisie spolu s ESVČ vypracúvajú správy ISAA. Komisia je členom siete EU-CyCLONe v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetickobezpečnostný incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti, ktoré patria do rozsahu pôsobnosti smernice (EÚ) 2022/2555, a v ostatných prípadoch je pozorovateľom. Je kontaktným miestom v IICB pre sieť EU-CyCLONe. Je pozorovateľom v sieti jednotiek CSIRTS.

21. Vysoký predstaviteľ pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“), ktorému pomáha ESVČ, vykonáva spoločnú zahraničnú a bezpečnostnú politiku Únie (ďalej len „SZBP“) a svojimi návrhmi prispieva k rozvoju tejto politiky vrátane spoločnej bezpečnostnej a obrannej politiky (ďalej len „SBOP“). Patria sem diplomatické, spravodajské a vojenské štruktúry a mechanizmy, najmä jednotná kapacita na analýzu spravodajských informácií (ďalej len „SIAC“) ako jednotné kontaktné miesto vstupu pre spravodajské informácie členských štátov, Vojenský štáb EÚ (ďalej len „EUMS“) ako zdroj vojenských odborných znalostí, súbor nástrojov kybernetickej diplomacie EÚ, ako aj sieť delegácií EÚ, ktoré môžu prispievať ku krízovému riadeniu zvonka. ESVČ tiež pripravuje s Komisiou správy ISAA.

22. V prílohe II sa opisujú úlohy a právomoci príslušných aktérov na úrovni Únie v súvislosti s riadením kybernetických kríz vrátane hlavných sietí a aktérov.

V: Príprava na rozsiahle kybernetickobezpečnostné incidenty a kybernetickú krízu

Panoráma hrozieb

23. Členské štáty a príslušné subjekty Únie by mali prijať potrebné opatrenia na zvýšenie situačného povedomia, pričom by mali zohľadniť, že panoráma hrozieb a situačné povedomie v prípade konkrétnych incidentov si vyžadujú odlišné spôsoby činnosti. Členské štáty a príslušné subjekty Únie by mali spolupracovať na základe overených a spoľahlivých údajov, ktoré sa týkajú okrem iného trendov incidentov, taktík, techník a postupov a aktívne využívaných zraniteľných miest.

24. Pri výmene informácií na úrovni EÚ by členské štáty mali v plnej miere využívať existujúce platformy pre technickú a operačnú spoluprácu, ako sú platformy, ktoré používa sieť jednotiek CSIRT a sieť EU-CyCLONe.

25. S cieľom zlepšiť spoločné situačné povedomie a uľahčiť posudzovanie vplyvu na EÚ by sieť EU-CyCLONe a sieť jednotiek CSIRT s podporou agentúry ENISA mali využívať interne dohodnutý mechanizmus podávania správ na vytvorenie prehľadu EÚ o technických a operačných činnostiach na základe informácií zhromaždených na vnútroštátnej úrovni.

26. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali:

    a) spolupracovať s cieľom zlepšiť výmenu informácií medzi technickou a operačnou úrovňou a situačné povedomie ako celok;

    b) pokračovať v budovaní atmosféry dôvery medzi svojimi členmi a medzi sieťami;

    c) s podporou agentúry ENISA v plnej miere využívať dostupné nástroje na výmenu informácií, uvažovať o tom, ako tieto nástroje zlepšiť, a zabezpečiť interoperabilitu medzi sieťami.

27. Sieť EU-CyCLONe, sieť jednotiek CSIRT a IICB by mali spolupracovať s cieľom zabezpečiť účinnú výmenu relevantných informácií.

28. Agentúra ENISA ako sekretariát siete jednotiek CSIRT a siete EU-CyCLONe zohráva ústrednú úlohu pri podpore členských štátov a inštitúcií, orgánov a agentúr Únie pri dosahovaní spoločného situačného povedomia EÚ na technickej a operačnej úrovni s cieľom podporiť prípravu na rozsiahle kybernetickobezpečnostné incidenty a krízy.

29. V súlade so smernicou (EÚ) 2022/2555 a nariadením (EÚ) 2019/881 by členské štáty a príslušné subjekty Únie mali koordinovať svoju činnosť so súkromným sektorom vrátane komunít s otvoreným zdrojovým kódom a výrobcov s cieľom zlepšiť výmenu informácií. Agentúra ENISA by mala v tejto súvislosti využiť najmä svoj program partnerstva. Okrem toho by členské štáty a príslušné subjekty Únie mohli využívať aj existujúce strediská pre výmenu a analýzu informácií (ďalej len „ISAC“) na úrovni EÚ a na vnútroštátnej úrovni s cieľom posilniť kybernetickobezpečnostnú kapacitu a reagovať na kybernetickobezpečnostné incidenty, a to aj prostredníctvom spoločných zasadnutí súkromného sektora so sieťou EU-CyCLONe alebo sieťou jednotiek CSIRT.

30. S cieľom zlepšiť výmenu informácií v rámci sietí a medzi nimi a objasniť vzájomné očakávania týkajúce sa takejto výmeny by sa sieť EU-CyCLONe mala s podporou agentúry ENISA ako sekretariátu a po konzultácii so sieťou jednotiek CSIRT a skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti (skupina pre spoluprácu v oblasti NIS) do 24 mesiacov od prijatia tohto odporúčania dohodnúť na spoločnej zosúladenej taxonómii úrovní závažnosti incidentov. Táto taxonómia by mala umožniť porovnanie závažnosti incidentov vo všetkých členských štátoch s prihliadnutím na vplyv na poskytovanie služieb, počet dotknutých subjektov a ich príslušnú relevantnosť, vplyv na iné služby a infraštruktúru, ako aj na spôsobené peňažné škody, škody na dobrej povesti a politické škody. Mala by vychádzať z príslušných existujúcich stupníc alebo taxonómií, ako je taxonómia klasifikácie referenčných incidentov.

Technická úroveň

31. Sieť jednotiek CSIRT je platformou pre technickú spoluprácu a výmenu informácií medzi všetkými členskými štátmi a prostredníctvom CERT-EU so subjektmi Únie.

32. V súlade so smernicou (EÚ) 2022/2555 má každá jednotka CSIRT úlohu monitorovať a analyzovať kybernetické hrozby, zraniteľné miesta a incidenty na vnútroštátnej úrovni. Jednotky CSIRT by si mali v rámci siete jednotiek CSIRT, ako aj dvojstranne vymieňať relevantné informácie o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľných miestach s cieľom dosiahnuť spoločné situačné povedomie.

33. S cieľom posilniť operačnú spoluprácu na úrovni Únie by sieť jednotiek CSIRT mala zvážiť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je Europol, k účasti na svojej práci.

34. V súlade s nariadením 2023/2841 by mal CERT-EU zhromažďovať, spravovať, analyzovať a vymieňať si s inštitúciami, orgánmi, úradmi a agentúrami Únie informácie o kybernetických hrozbách, zraniteľných miestach a incidentoch v neutajovanej infraštruktúre IKT a v prípade potreby vydávať osobitné návrhy pre IICB na usmernenia a odporúčania pre inštitúcie, orgány, úrady a agentúry Únie. CERT-EU by mal spolupracovať a vymieňať si informácie s protistranami z členských štátov, a to aj prostredníctvom siete jednotiek CSIRT.

Operačná úroveň

35. V súlade so smernicou (EÚ) 2022/2555 by sieť EU-CyCLONe mala slúžiť ako platforma pre spoluprácu medzi orgánmi členských štátov pre riadenie kybernetických kríz a prostredníctvom Komisie s príslušnými subjektmi Únie s cieľom zvýšiť úroveň pripravenosti na riadenie rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz a rozvíjať spoločné situačné povedomie o rozsiahlych kybernetickobezpečnostných incidentoch a kybernetických krízach.

36. V súlade so smernicou (EÚ) 2022/2555 a nariadením (EÚ) 2024/2847 dostáva agentúra ENISA informácie o významných cezhraničných incidentoch a aktívne využívaných zraniteľných miestach a incidentoch ovplyvňujúcich digitálne produkty. Agentúra ENISA konajúca ako sekretariát by mala poskytovať poradenstvo sieti jednotiek CSIRT a sieti EU-CyCLONe s cieľom podporiť tieto siete pri určovaní toho, či by sa mali prijať ďalšie opatrenia, a prispieť k spoločnému situačnému povedomiu.

Politická úroveň

37. Členské štáty a príslušné subjekty Únie by mali monitorovať medzinárodný vývoj, ktorý ovplyvňuje kybernetickú bezpečnosť (v relevantných prípadoch vrátane kybernetických hrozieb, hybridných hrozieb a zahraničnej manipulácie s informáciami a zahraničného zasahovania vrátane dezinformácií). Mali by sa zohľadniť iniciatívy, ako sú spoločné správy o posúdení kybernetickej bezpečnosti (ďalej len „JCAR“), analýzy, ktoré poskytuje SIAC, a iné relevantné produkty poskytujúce špecializované poznatky.

38. Vysoký predstaviteľ by mal naďalej informovať členské štáty a zapájať ich do diplomatického úsilia Únie týkajúceho sa kybernetických hrozieb, najmä tých, ktoré zahŕňajú štátnych aktérov, do jej spolupráce s tretími krajinami a medzinárodnými organizáciami vrátane NATO a do vykonávania diplomatických opatrení vrátane reštriktívnych opatrení.

39. Predsedníctvo Rady Európskej únie môže iniciovať monitorovaciu stránku na webovej platforme IPCR, na ktorej si členské štáty a inštitúcie a orgány EÚ môžu vymieňať informácie o potenciálne sa vyvíjajúcej kríze.

Spoločné cvičenia

40. Komisia by v koordinácii s vysokým predstaviteľom s podporou agentúry ENISA a po konzultácii so sieťou EU-CyCLONe a sieťou jednotiek CSIRT mala zostaviť účinný ročný priebežný program kybernetických cvičení s cieľom pripraviť sa na kybernetické krízy a zvýšiť organizačnú efektívnosť. Priebežný program kybernetických cvičení by mal zohľadňovať cvičenia UCPM a iné cvičenia mechanizmov reakcie na krízu na úrovni Únie vrátane cvičenia uvedeného v koncepcii kritickej infraštruktúry EÚ. Prvý priebežný program by sa mal vypracovať do 12 mesiacov od prijatia kybernetickej koncepcie, pričom následné programy by sa mali dokončiť každý rok do 31. marca. Priebežný program by sa mal predložiť Rade na informovanie.

41. Priebežný program by sa mal vzťahovať aj na cvičenia vypracované na základe scenárov koordinovaného posudzovania rizík na úrovni EÚ. Mal by sa vzťahovať na cvičenia, do ktorých sú zapojení všetci príslušní aktéri, najmä súkromný sektor a NATO.

42. Agentúra ENISA by vo svojej úlohe sekretariátu siete jednotiek CSIRT a siete EU-CyCLONe mala zabezpečiť systematický zber poznatkov získaných z cvičení, ako aj identifikáciu a navrhovanie spôsobov implementácie výsledných opatrení s cieľom zaručiť ich účinné vykonávanie a pozitívny vplyv na spoločnú odolnosť EÚ vrátane príslušných štandardných operačných postupov.

43. Všetci aktéri a siete by mali zlepšiť koordináciu v prípade rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy na základe skúseností získaných z cvičení. Najmä sieť EU-CyCLONe a sieť jednotiek CSIRT by mali s cieľom zlepšiť koordináciu riešiť výzvy, ktoré boli identifikované počas cvičení, najmä tie, ktoré sa týkajú spolupráce medzi sieťami, a v prípade potreby urýchlene prispôsobiť štandardné operačné postupy.

44. Skupina pre spoluprácu v oblasti NIS by mala vyzvať sieť jednotiek CSIRT, sieť EU-CyCLONe a agentúru ENISA, aby predložili poznatky získané z cvičení, ako aj identifikáciu a navrhovaný spôsob vykonávania výsledných opatrení.

45. Rada môže vyzvať predsedov siete jednotiek CSIRT, siete EU-CyCLONe, skupiny pre spoluprácu v oblasti NIS a agentúry ENISA, aby prezentovali, ako sa využili skúsenosti získané z cvičení.

46. Agentúra ENISA sa vyzýva, aby v spolupráci s Komisiou a vysokým predstaviteľom zorganizovala cvičenie na testovanie kybernetickej koncepcie počas nasledujúceho cvičenia Cyber Europe. Do tohto cvičenia by sa mali zapojiť všetci príslušní aktéri vrátane politickej úrovne. Agentúra ENISA sa vyzýva, aby zapojenie politickej úrovne koordinovala s predsedníctvom Rady Európskej únie. Cvičenie môže zahŕňať aj súkromný sektor a NATO.

VI: Odhalenie incidentu, ktorý by mohol prerásť do rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy

47. Všetci aktéri by mali v súlade so svojimi príslušnými mandátmi a na základe prístupu zohľadňujúceho všetky riziká poskytovať príslušným sieťam informácie naznačujúce potenciálny rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu.

48. Ak v súlade s nariadením (EÚ) 2025/38[13] cezhraničné kybernetické centrá získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetickobezpečnostného incidentu, na účely spoločného situačného povedomia by mali zabezpečiť, aby sa relevantné informácie bez zbytočného odkladu poskytli orgánom členských štátov a Komisii prostredníctvom siete EU-CyCLONe a siete jednotiek CSIRT.

[13] Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite) (Ú. v. EÚ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49. Ak sa spozoruje významný incident, najmä taký, ktorý má okamžitý vplyv, možno ho oznámiť jednotke CSIRT, pričom táto jednotka, ako aj orgány členských štátov pre riadenie kybernetických kríz alebo iné odvetvové orgány ho môžu aj odhaliť. Členské štáty sa vyzývajú, aby si vymieňali informácie týkajúce sa takýchto incidentov v rámci sietí, ktoré by mali zvážiť prijatie vhodných opatrení. Aktivácia siete jednotiek CSIRT a siete EU-CyCLONe môže byť od seba nezávislá v závislosti od povahy incidentu a požadovanej reakcie. Obidve siete sa však nabádajú, aby pokračovali vo vzájomnej spolupráci na základe dohodnutých procesných opatrení. Rozhodnutie o aktivácii spočíva výlučne a nezávisle na každej príslušnej sieti.

50. Sieť jednotiek CSIRT by mala informovať sieť EU-CyCLONe o tom, či spozorovaný kybernetickobezpečnostný incident možno považovať za potenciálny alebo prebiehajúci rozsiahly kybernetickobezpečnostný incident.

51. Ako sa uvádza v smernici (EÚ) 2022/2555, sieť jednotiek CSIRT a sieť EU-CyCLONe by sa mali bezodkladne dohodnúť na procesných opatreniach v prípade potenciálneho alebo prebiehajúceho rozsiahleho kybernetickobezpečnostného incidentu, aby sa zabezpečila technicko-operatívna koordinácia a včasné a relevantné informovanie politickej úrovne.

VII: Reakcia na rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu na úrovni Únie

Reakcia na rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu, v prípade ktorých IPCR nie je aktivovaná v plnom režime

52. Účinná reakcia na rozsiahle kybernetickobezpečnostné incidenty alebo kybernetické krízy na úrovni EÚ závisí od účinnej technickej, operačnej a politickej spolupráce v rámci celovládneho prístupu, podľa možnosti vrátane orgánov presadzovania práva.

53. Zapojení aktéri by mali na každej úrovni vykonávať osobitné činnosti na dosiahnutie spoločného situačného povedomia a koordinovanej reakcie. Takýmito opatreniami sa zabezpečí riadne a účinné šírenie informácií.

54. Reakcia by mala byť primeraná vplyvu rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy. V súlade so smernicou (EÚ) 2022/2555 by orgány členských štátov pre riadenie kybernetických kríz mali zabezpečiť vnútroštátnu súdržnosť a koordináciu medzi odvetvovými reakciami na kybernetickú krízu.

55. V prípade rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy by všetci aktéri a siete mali v úzkej koordinácii reagovať takto:

a) na technickej úrovni:

i. zasiahnuté členské štáty a ich jednotky CSIRT by mali spolupracovať so zasiahnutými subjektmi s cieľom reagovať na incidenty a v náležitých prípadoch poskytovať pomoc;

ii. jednotky CSIRT by mali spolupracovať prostredníctvom siete jednotiek CSIRT s cieľom vymieňať si relevantné technické informácie o incidente; jednotky CSIRT spolupracujú vo svojom úsilí analyzovať dostupné technické artefakty a iné technické informácie súvisiace s incidentom s cieľom určiť príčinu a možné technické zmierňujúce opatrenia;

iii. jednotky CSIRT alebo orgány pre riadenie kybernetických kríz členského štátu sa vyzývajú, aby v prípade, že zistia významný incident, zdieľali informácie o ňom v rámci siete jednotiek CSIRT alebo siete EU-CyCLONe;

iv. sieť jednotiek CSIRT by s podporou agentúry ENISA mala pripraviť súhrn vnútroštátnych správ, ktoré poskytnú jednotky CSIRT a ktoré by sa mali predložiť sieti EU-CyCLONe;

v. ak má kybernetickobezpečnostný incident potenciál prerásť do rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy, sieť jednotiek CSIRT by si mala vymieňať primerané informácie so sieťou EU-CyCLONe; sieť EU-CyCLONe by mala tieto informácie použiť na informovanie Rady;

vi. sieť jednotiek CSIRT by mala byť v úzkom kontakte s Europolom, aby sa zabezpečila výmena príslušných technických informácií; sieť jednotiek CSIRT a Europol by mali zriadiť kontaktné miesta na zlepšenie výmeny informácií, ak je to relevantné v prípade rozsiahleho kybernetickobezpečnostného incidentu;

b) na operačnej úrovni:

i. členské štáty by mali zmierniť vplyv incidentu na vnútroštátnej úrovni pomocou vhodných opatrení;

ii. sieť jednotiek CSIRT by mala sieti EU-CyCLONe poskytovať technické posúdenia prebiehajúcich incidentov, ktoré môže sieť EU-CyCLONe využívať;

iii. sieť EU-CyCLONe by mala posúdiť dôsledky a vplyv relevantných rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz a navrhnúť možné zmierňujúce opatrenia a mala by podporovať koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kybernetických kríz, ako aj rozhodovanie na politickej úrovni;

iv. ak by si rozsiahly kybernetickobezpečnostný incident s medziodvetvovým vplyvom vyžadoval aktiváciu opatrení reakcie na úrovni Únie, najmä príslušných horizontálnych a odvetvových mechanizmov krízového riadenia na úrovni Únie uvedených v prílohe II,

a) v závislosti od typu odvetvových mechanizmov krízového riadenia na úrovni Únie môžu príslušní aktéri vyzvať na aktiváciu uvedeného mechanizmu;

b) v prípade aktivácie takéhoto odvetvového mechanizmu príslušné subjekty podporujú odvetvové subjekty pri zmierňovaní vplyvu incidentu;

c) Komisia by mala uľahčiť tok potrebných informácií medzi kontaktnými miestami pre príslušné horizontálne a odvetvové krízové mechanizmy na úrovni Únie uvedené v prílohe II a sieť EU-CyCLONe a mala by vykonať integrovanú medziodvetvovú analýzu a navrhnúť možnosti vhodného integrovaného plánu reakcie;

d) Komisia by mala v relevantných prípadoch prostredníctvom siete EU-CyCLONe v spolupráci s vysokým predstaviteľom zabezpečiť súdržnosť a koordináciu operačných opatrení na úrovni EÚ v kybernetickej oblasti so súvisiacimi opatreniami reakcie na úrovni Únie, najmä v súvislosti so žiadosťami o pomoc prostredníctvom UCPM;

e) ak bola iniciovaná monitorovacia stránka IPCR, prostredníctvom webovej platformy IPCR by sa mali vymieňať medzi členskými štátmi a subjektmi Únie aj informácie o incidente, jeho vplyvoch a prijatých opatreniach;

v. členské štáty môžu požiadať o služby z rezervy EÚ na účely kybernetickej bezpečnosti v súlade s článkom 15 nariadenia (EÚ) 2025/38; bez toho, aby boli dotknuté akékoľvek budúce vykonávacie akty podľa uvedeného nariadenia, by sa služby rezervy EÚ na účely kybernetickej bezpečnosti mali nasadiť do 24 hodín od podania žiadosti;

c) na politickej úrovni:

i. Rada môže v záujme primeranej politickej a strategickej reakcie požiadať kľúčové zainteresované strany, najmä Komisiu, vysokého predstaviteľa a sieť EU-CyCLONe, o brífingy;

ii. Rada by s podporou Komisie a vysokého predstaviteľa mohla rozhodnúť o vhodných opatreniach v reakcii na rozsiahly kybernetickobezpečnostný incident vrátane možných diplomatických reakcií v súlade s kapitolou IX;

iii. členské štáty môžu v závislosti od povahy a vplyvu incidentu aktivovať dodatočné mechanizmy alebo nástroje riadenia kybernetických kríz;

iv. keď sa IPCR aktivuje v režime výmeny informácií, spustí sa podporná spôsobilosť ISAA, čím sa zintenzívni výmena informácií prostredníctvom webovej platformy IPCR a zabezpečí sa spoločné situačné povedomie; situačné správy siete EU-CyCLONe a siete jednotiek CSIRT by mali zostať hlavnými nástrojmi prezentujúcimi spoločné situačné povedomie na operačnej a technickej úrovni; tieto správy môžu byť podkladom pre správy ISAA;

v. v prípade incidentu, ktorý si vyžaduje aktiváciu opatrení reakcie na úrovni Únie, najmä príslušných horizontálnych a odvetvových mechanizmov krízového riadenia na úrovni Únie uvedených v prílohe II, by Rada v spolupráci s Komisiou a vysokým predstaviteľom mala zabezpečiť súdržnosť a koordináciu medzi reakciami na kybernetickú krízu a súvisiacimi opatreniami reakcie na úrovni Únie;

vi. ak sa požadujú relevantné mechanizmy, najmä služby rezervy na účely kybernetickej bezpečnosti, útvary Komisie a vo vhodných prípadoch ESVČ, ako aj príslušné orgány Rady, najmä HWPCI a horizontálna pracovná skupina pre zvyšovanie odolnosti a boj proti hybridným hrozbám (HWP-ERCHT), by mali podľa potreby vykonávať koordináciu, pokiaľ ide o navrhovanie a vykonávanie opatrení, ako aj vhodný rozhodovací proces s dodatočnými opatreniami, a to v súlade so súborom nástrojov na boj proti hybridným hrozbám[14] v prípade škodlivých kybernetických činností, ktoré sú súčasťou širšej hybridnej kampane.

Reakcia na rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu, v prípade ktorých je IPCR aktivovaná v režime úplnej aktivácie

56. Mali by sa vykonať kroky uvedené v oddiele „*Reakcia na rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu, v prípade ktorých IPCR nie je aktivovaná v režime úplnej aktivácie“*.

57. Keď sa IPCR aktivuje v režime úplnej aktivácie, správy ISAA slúžia na zabezpečenie spoločného situačného povedomia na politickej úrovni. Situačné správy siete EU-CyCLONe a siete jednotiek CSIRT by mali zostať hlavnými nástrojmi prezentujúcimi spoločné situačné povedomie na operačnej a technickej úrovni. Tieto správy môžu byť podkladom pre správy ISAA.

58. V prípade rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy, ktoré vedú k aktivácii IPCR v režime úplnej aktivácie, by všetci aktéri mali reagovať v úzkej koordinácii v rámci celovládneho prístupu takto:

a) koordináciu reakcie na politickej úrovni Únie vykonáva Rada s využitím dojednaní o IPCR;

[14] Súbor nástrojov na boj proti hybridným hrozbám predstavuje rámec pre koordinovanú reakciu na hybridné kampane, ktoré majú vplyv na EÚ a jej členské štáty, a zahŕňa napríklad preventívne, kooperatívne, stabilizačné a reštriktívne opatrenia a opatrenia na zotavenie sa a podporu solidarity a vzájomnej pomoci.

b) sieť EU-CyCLONe by mala v spolupráci so sieťou jednotiek CSIRT poskytnúť politickej úrovni jasné informácie o vplyve a možných dôsledkoch incidentu a opatreniach reakcie a nápravy v súvislosti s incidentom, a to aj prostredníctvom príspevku do správ ISAA;

c) okrem spôsobilosti ISAA predsedníctvo Rady Európskej únie zvolá okrúhle stoly IPCR s cieľom umožniť politickú a strategickú koordináciu reakcie EÚ, pričom podkladom pre prácu IPCR sú činnosti v rámci kybernetickej koncepcie a práca príslušných odvetvových mechanizmov; tieto okrúhle stoly môžu okrem toho identifikovať niektoré konkrétne nedostatky v reakcii a vyzvať konkrétnych aktérov EÚ, aby ich riešili a podávali správy pri budúcich okrúhlych stoloch s cieľom podporiť politickú a strategickú koordináciu v rámci IPCR;

d) predsedníctvo Rady Európskej únie by malo zvážiť pozvanie siete EU-CyCLONe na príslušné zasadnutia vrátane okrúhlych stolov v rámci dojednaní o IPCR a iných relevantných zasadnutí Rady;

e) orgány členských štátov pre krízové riadenie by mali zabezpečiť súdržnosť a koordináciu medzi odvetvovými reakciami na kybernetickú krízu podporovanými orgánmi pre riadenie kybernetických kríz;

f) v súlade s kapitolou IX mali by sa zvážiť a vykonať možné diplomatické reakcie.

VIII: Úsilie v oblasti komunikácie s verejnosťou

59. Hoci informovanie obyvateľstva jednotlivých členských štátov o prebiehajúcom rozsiahlom kybernetickobezpečnostnom incidente alebo kybernetickej kríze, a to aj v rámci zvyšovania povedomia, je vo vnútroštátnej právomoci, členské štáty, Komisia a vysoký predstaviteľ by sa mali zamerať na čo najširšiu koordináciu svojej komunikácie s verejnosťou. V náležitých prípadoch sa môže zapojiť neformálna sieť krízových komunikátorov IPCR.

60. Na účely prípravy na rozsiahle kybernetickobezpečnostné incidenty a kybernetické krízy sa členské štáty a v príslušných prípadoch Komisia a tím CERT-EU vyzývajú, aby si vymieňali informácie o svojom komunikačnom úsilí v rámci siete EU-CyCLONe a siete jednotiek CSIRT vrátane najlepších postupov, ako sú poradenstvo alebo kampane na zvyšovanie povedomia. Agentúra ENISA by mala poskytnúť nástroje na podporu takejto výmeny a zabezpečenie ľahkého prístupu.

61. Členské štáty sa vyzývajú, aby si v prípade rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy vymieňali v rámci siete EU-CyCLONe informácie o svojom úsilí v oblasti komunikácie s verejnosťou s cieľom dospieť k spoločnému povedomiu a koordinovať opatrenia. Sieť EU-CyCLONe môže z vlastnej iniciatívy alebo na žiadosť Rady poskytnúť Rade prehľad takýchto prístupov.

IX: Diplomatická reakcia a spolupráca so strategickými partnermi

62. Vysoký predstaviteľ by mal v úzkej spolupráci s Komisiou a ostatnými príslušnými subjektmi Únie:

    a) podporovať rozhodovanie v Rade, a to aj prostredníctvom analýz, správ a návrhov, o využívaní možných opatrení ako súčasti súboru nástrojov kybernetickej diplomacie EÚ. Umožní sa tým využitie celého spektra dostupných nástrojov Únie na predchádzanie škodlivým kybernetickým činnostiam, odrádzanie od nich a reakciu na ne, čím sa posilní stav kybernetickej bezpečnosti a podporí sa medzinárodný mier, bezpečnosť a stabilita v kybernetickom priestore;

b) v prípade identifikácie relevantného incidentu uľahčovať tok potrebných informácií so strategickými partnermi, v relevantných prípadoch aj s NATO;

c) posilňovať koordináciu so strategickými partnermi, v relevantných prípadoch vrátane NATO, pri reakcii na škodlivé kybernetické činnosti trvalo pôsobiacich aktérov hrozieb, najmä pri využívaní súboru nástrojov kybernetickej diplomacie EÚ, a to v súlade s vykonávacími usmerneniami.

63. Členské štáty, vysoký predstaviteľ, Komisia a ďalšie príslušné subjekty Únie by mali spolupracovať so strategickými partnermi a medzinárodnými organizáciami s cieľom podporovať osvedčené postupy a zodpovedné správanie štátov v kybernetickom priestore a zabezpečiť rýchlu a koordinovanú reakciu v prípade potenciálnych alebo rozsiahlych kybernetickobezpečnostných incidentov.

64. Spolupráca Európskej únie a NATO by sa mala uskutočňovať v súlade s dohodnutými usmerňujúcimi zásadami, ktorými sú inkluzívnosť, reciprocita a transparentnosť, a pri plnom rešpektovaní autonómneho rozhodovania Únie.

65. Komisia a vysoký predstaviteľ by s prihliadnutím na existujúce dohody, ako je technická dohoda CERT-EU/NATO z roku 2016, mali zriadiť kontaktné miesta na koordináciu s NATO v prípade kybernetickej krízy s cieľom vymieňať si potrebné informácie o situácii a využívaní mechanizmov reakcie na krízu, aby zvýšili účinnosť reakcie a zintenzívnili spoluprácu v rámci nej. Na tento účel by Únia mala preskúmať spôsoby zlepšenia zdieľania informácií s NATO inkluzívnym, recipročným a nediskriminačným spôsobom, najmä prostredníctvom zabezpečenia nástrojov bezpečnej komunikácie pri zohľadnení noriem zdieľania informácií rôznych členských štátov.

66. V rámci priebežného programu kybernetických cvičení Únie uvedeného v kapitole V by útvary Komisie a ESVČ mali zvážiť zorganizovanie cvičenia na úrovni zamestnancov s NATO s cieľom otestovať spoluprácu medzi civilnými a vojenskými subjektmi v prípade rozsiahleho kybernetickobezpečnostného incidentu alebo kybernetickej krízy, v rámci ktorého sa členské štáty alebo spojenci v NATO snažia reagovať na kybernetický útok ovplyvňujúci ich bezpečnosť. Toto cvičenie by sa malo vykonávať inkluzívnym a nediskriminačným spôsobom a pri plnom dodržiavaní dohodnutých zásad parametrov spolupráce medzi EÚ a NATO. Malo by sa vykonávať v rámci cvičenia EU Integrated Resolve (paralelné a koordinované cvičenie, ďalej len „PACE“). Mali by sa prijať všetky potrebné opatrenia na zabezpečenie účasti všetkých aktérov uvedených v kybernetickej koncepcii.

67. Po konzultácii s Radou, Komisiou a vysokým predstaviteľom by sa mali zvážiť aj spoločné kybernetické cvičenia na úrovni Únie s krajinami západného Balkánu, Moldavskou republikou, Ukrajinou, ako aj inými strategickými partnermi a podobne zmýšľajúcimi tretími krajinami.

X. Koordinácia riadenia kybernetických kríz s vojenskými aktérmi na úrovni EÚ

68. Členské štáty by mali naďalej posilňovať spoluprácu medzi civilnými a vojenskými kybernetickými aktérmi na vnútroštátnej úrovni.

69. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali identifikovať možné spôsoby a postupy spolupráce s príslušnými vojenskými aktérmi EÚ, ako je konferencia veliteľov EÚ v oblasti kybernetickej bezpečnosti a operačná sieť pre vojenské tímy reakcie na počítačové núdzové situácie (ďalej len „MICNET“), s cieľom využívať spoločnú vojenské a civilné chápanie situácie, najmä prostredníctvom spoločných zasadnutí. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali Radu informovať o pokroku dosiahnutom v súvislosti s takouto spoluprácou.

70. Dotknutý členský štát sa vyzýva, aby informoval sieť EU-CyCLONe aj ESVČ, ak sa v súvislosti s rozsiahlym kybernetickobezpečnostným incidentom alebo kybernetickou krízou využívajú príslušné vnútroštátne alebo nadnárodné vojenské spôsobilosti reakcie, pričom na poskytnutí týchto informácií sa vzájomne dohodnú používateľ a poskytovateľ takejto spôsobilosti reakcie.

71. V rámci priebežného programu kybernetických cvičení Únie uvedeného v kapitole V by Komisia a vysoký predstaviteľ mali zvážiť zorganizovanie spoločného cvičenia s cieľom otestovať spoluprácu medzi civilnými aj vojenskými kybernetickými aktérmi v prípade rozsiahleho kybernetickobezpečnostného incidentu s vplyvom na členské štáty.

XI: Zotavenie a poznatky z kybernetickej krízy

72. Členské štáty, príslušné subjekty Únie a siete by mali spolupracovať počas fázy zotavenia po kybernetickej kríze s cieľom zabezpečiť rýchlu obnovu základných funkcií. Do takejto spolupráce by mali byť v relevantných prípadoch zapojené aj komunity presadzovania práva. V tejto fáze je kľúčová spolupráca so súkromným sektorom, najmä pokiaľ ide o uľahčenie obnovy údajov a opätovné sprevádzkovanie systémov. Účinnou koordináciou medzi zainteresovanými stranami by sa mala uprednostňovať minimalizácia narušenia a zabezpečenie kontinuity činností.

73. Členské štáty, príslušné subjekty Únie a siete by mali vo fáze zotavenia spolupracovať na základe poznatkov z kybernetických kríz alebo riešených kybernetickobezpečnostných incidentov z minulosti, ako aj správ o incidentoch, najmä v kontexte európskeho mechanizmu preskúmania kybernetických incidentov zriadeného nariadením (EÚ) 2025/38.

74. Sieť EU-CyCLONe by mala sieti jednotiek CSIRT, skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a Rade poskytnúť komplexný zoznam poznatkov získaných z kybernetických kríz alebo riešených kybernetickobezpečnostných incidentov z minulosti a najlepších postupov. Agentúra ENISA by mala zabezpečiť, aby sa tieto získané poznatky náležite zohľadnili v budúcich činnostiach v oblasti pripravenosti a pri zvažovaní plánovania budúcich cvičení.

XII: Bezpečná komunikácia

75. Na základe zmapovania existujúcich nástrojov bezpečnej komunikácie by[15]Komisia mala do konca roka 2026 navrhnúť interoperabilný súbor riešení bezpečnej komunikácie. Rada, Komisia, vysoký predstaviteľ, sieť EU-CyCLONe a sieť jednotiek CSIRT by sa mali na tomto súbore dohodnúť do konca roka 2027. Tieto riešenia by mali ťažiť z opatrení v oblasti bezpečnej komunikácie, ktoré by inštitúcie EÚ mohli prijať v rámci Európskej stratégie únie pripravenosti, a mali by sa vzťahovať na celú škálu požadovaných spôsobov komunikácie (hlas, údaje, videokonferencie, zasielanie správ, spoločná práca na dokumentoch, ich zdieľanie a nahliadanie do nich). Riešenia by mali spĺňať spoločne vymedzené požiadavky na ochranu citlivých neutajovaných skutočností. Mali by sa používať riešenia založené na otvorenom protokole s implementáciami s otvoreným zdrojovým kódom vhodnými na komunikáciu v reálnom čase, ktoré spravuje subjekt so sídlom v EÚ.

76. Sieť EU-CyCLONe a sieť jednotiek CSIRT by na účely výmeny utajovaných skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED mali mať v prípade potreby možnosť využívať bezpečné komunikačné kanály, ktoré budú pre inštitúcie, orgány, úrady a agentúry EÚ zaistené na výmenu utajovaných skutočností medzi sebou navzájom a s členskými štátmi.

---

15 WK 862/2023.

77. Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC) zriadené podľa nariadenia (EÚ) 2021/887[16] by malo bez toho, aby bol dotknutý budúci viacročný finančný rámec, zvážiť financovanie prostredníctvom programu Digitálna Európa s cieľom pomôcť členským štátom pri zavádzaní týchto nástrojov bezpečnej komunikácie. Malo by sa zabrániť akejkoľvek duplicite investícií do interoperabilných bezpečných systémov.

78. Subjekty EÚ a členské štáty by mali vypracovať najmä pohotovostné opatrenia pre prípad závažných kríz, keď sú narušené alebo nedostupné bežné komunikačné kanály spoliehajúce sa na internet alebo telekomunikačné siete.

79. Aby bolo možné účinne reagovať na kybernetické krízy, mali by sa zriadiť mechanizmy komunikácie a zdieľania informácií medzi orgánmi presadzovania práva a sieťami kybernetickej bezpečnosti, najmä na technickej úrovni. Tieto mechanizmy by mali rešpektovať úlohy jednotlivých strán, nemali by zasahovať do prebiehajúcich operácií a mala by sa nimi zaručiť redundantnosť komunikácie. Európsky kritický komunikačný systém (ďalej len „EUCCS“), ktorý sa v súčasnosti vyvíja, môže byť prínosom pre reakciu, ktorá sa prijme spoločne s príslušnými kybernetickými komunitami.

XIII: Záverečné ustanovenia

80. Sieť EU-CyCLONe by v spolupráci so sieťou jednotiek CSIRT a ďalšími hlavnými aktérmi v ekosystéme EÚ pre riadenie kybernetických kríz a s podporou agentúry ENISA mala do jedného roka od uverejnenia tohto odporúčania vypracovať podrobné diagramy toku procesov, v ktorých sa načrtnú informačné toky medzi príslušnými aktérmi, rozhodovacie procesy a správy vypracúvané počas riadenia rozsiahlych kybernetickobezpečnostných incidentov alebo kybernetických kríz, ako sa opisuje v tomto odporúčaní. Tieto diagramy tokov by mali zahŕňať rôzne spôsoby a úrovne spolupráce. Mali by sa podľa potreby aktualizovať.

---

[16] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887 z 20. mája 2021, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier, Ú. v. EÚ L 202, 8.6.2021, s. 1 – 31.

81. S cieľom podporiť účinné uplatňovanie revidovanej kybernetickej koncepcie a na základe skúseností získaných počas spoločných kybernetických cvičení vykonávaných v rámci nej môže Rada v prípade potreby vypracovať súbor vykonávacích usmernení. Tieto usmernenia by sa mohli zaoberať praktickými výzvami identifikovanými počas cvičení a mohli by sa nimi odstrániť zistené nedostatky a chýbajúce prepojenia v koordinácii, komunikácii a operačnej interakcii.

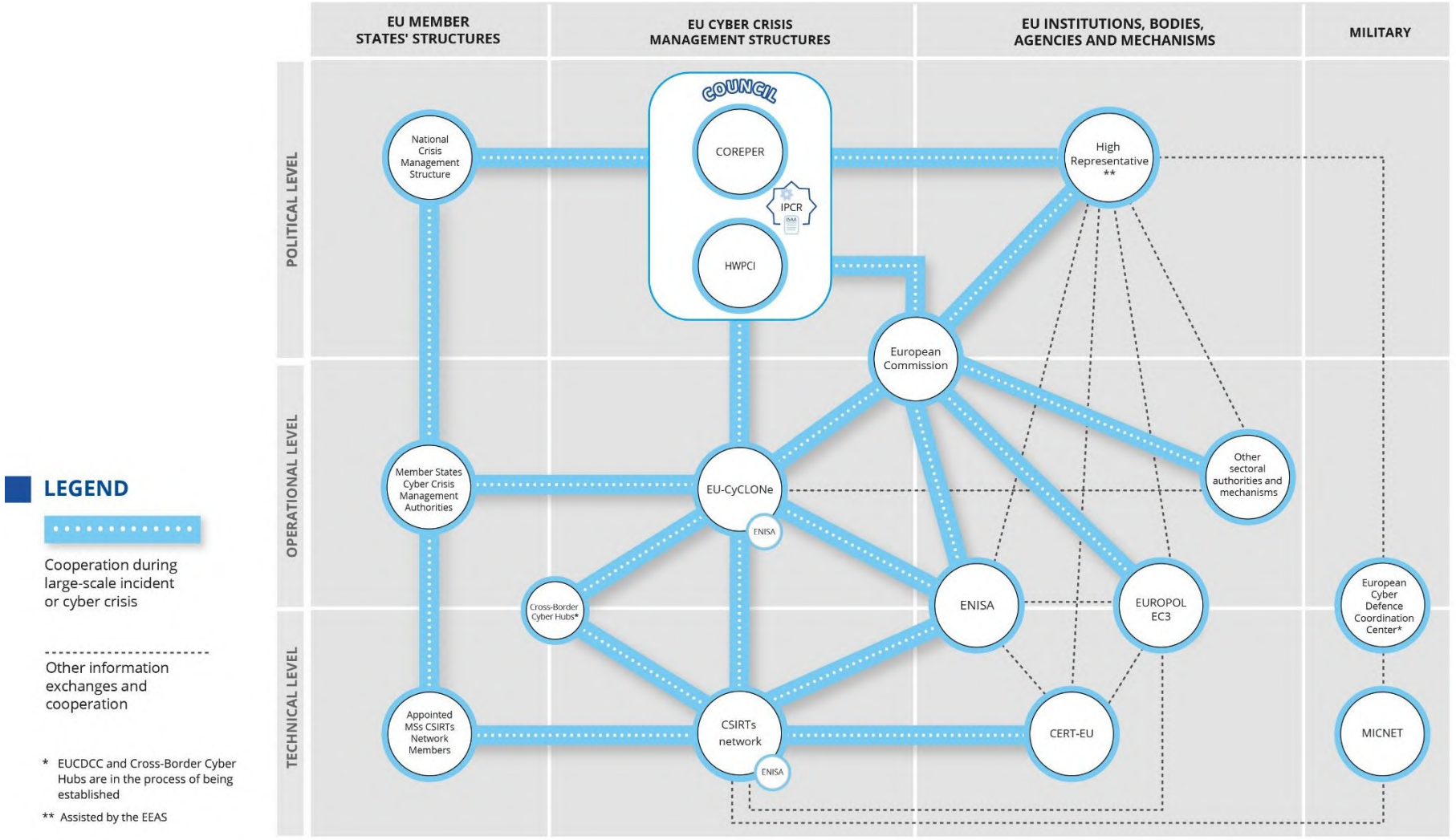
82. Toto odporúčanie by Komisia mala preskúmať v spolupráci s členskými štátmi aspoň každé štyri roky po jeho uverejnení. Po každom preskúmaní by Komisia mala uverejniť správu a predložiť ju Rade. Komisia a členské štáty by mali zohľadniť najmä vplyv meniacej sa panorámy hrozieb, výsledky spoločných cvičení a legislatívne zmeny – najmä akékoľvek zmeny vyplývajúce z revízie nariadenia (EÚ) 2019/881.

V Bruseli

Za Radu

predseda/predsedníčka

PRÍLOHA I – Koncepcia Únie pre reakciu na kybernetickú krízu



PRÍLOHA II – PRÍSLUŠNÍ AKTÉRI (SUBJEKTY A SIETE) NA ÚROVNI ÚNIE A MECHANIZMY KRÍZOVÉHO RIADENIA

1) Zapojenie hlavných aktérov do celého životného cyklu riadenia kybernetických kríz (rozsiahle kybernetickobezpečnostné incidenty a kybernetické krízy)

	Pripravenosť	Odhalenie	Reakcia na rozsiahly kybernetickobezpečnostný incident alebo kybernetickú krízu			Komunikácia s verejnosťou	Zotavenie a získané poznatky
			na technickej úrovni	na operačnej úrovni	na politickej úrovni		
Členské štáty	X	X	X	X	X	X	X
Komisia	X			X	X	X	
Vysoký predstaviteľ s pomocou ESVČ	X			X	X	X	
Rada	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Sieť jednotiek CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

2) Úlohy a právomoci príslušných aktérov a mechanizmov na úrovni Únie (v abecednom poradí) v súvislosti s riadením kybernetických kríz

Aktér	Úroveň	Úloha a právomoc	Odkaz
CERT-EU	technická/operačná	Koordinuje reakciu na krízu na technickej úrovni a riadenie závažných incidentov, ktoré majú vplyv na subjekty Únie. Vedie súpis dostupných odborných technických znalostí, ktoré by boli potrebné na reakciu na incident v prípade závažných incidentov, a pomáha IICB pri koordinácii plánov riadenia kybernetických kríz subjektov Únie pre prípad závažných incidentov. Člen siete jednotiek CSIRT. Podporuje Komisiu v sieti EU-CyCLONe pri koordinovanom riadení rozsiahlych kybernetickobezpečnostných incidentov a kríz. Pôsobí ako centrum pre výmenu informácií o kybernetickej bezpečnosti a koordináciu reakcie na incidenty, pričom uľahčuje výmenu informácií o incidentoch, kybernetických hrozbách, zraniteľnostiach a udalostiach odvrátených v poslednej chvíli	nariadenie (EÚ, Euratom) 2023/2841 nariadenie (EÚ) 2025/38

Aktér	Úroveň	Úloha a právomoc	Odkaz
		medzi subjektmi Únie a protistranami. Žiada o nasadenie rezervy EÚ na účely kybernetickej bezpečnosti v mene subjektov Únie. Spolupracuje s Centrom kybernetickej bezpečnosti NATO na základe vzájomnej technickej dohody.	
Rada Európskej únie	politická	Tvorba politík a koordinačné funkcie. Je poverená realizáciou IPCR, ktoré sa týkajú koordinácie a reakcie na politickej úrovni Únie.	článok 16 Zmluvy o Európskej únii
Predsedníctvo Rady Európskej únie	politická	Po konzultácii s prípadnými dotknutými členskými štátmi, ako aj s Komisiou a VP rozhoduje (s výnimkou prípadov, keď sa uplatní doložka o solidarite podľa článku 222 Zmluvy o fungovaní Európskej únie), či sa aktivujú IPCR.	článok 16 Zmluvy o Európskej únii vykonávacie rozhodnutie Rady (EÚ) 2018/1993
Cezhraničné kybernetické centrá	technická	„cezhraničné kybernetické centrum“ je platforma s účasťou viacerých krajín zriadená písomnou dohodou o konzorciu, ktorou sa v koordinovanej sieťovej štruktúre spájajú národné kybernetické centrá	nariadenie (EÚ) 2025/38

Aktér	Úroveň	Úloha a právomoc	Odkaz
		aspoň z troch členských štátov a ktorá je určená na zlepšenie monitorovania, odhaľovania a analýzy kybernetických hrozieb na predchádzanie incidentom a na podporu tvorby spravodajských informácií o kybernetických hrozbách, najmä prostredníctvom výmeny relevantných údajov a informácií, vo vhodných prípadoch anonymizovaných, ako aj prostredníctvom zdieľania najmodernejších nástrojov a spoločného rozvoja spôsobilostí v oblasti odhaľovania kybernetických hrozieb, ich analýzy, prevencie a ochrany pred nimi v dôveryhodnom prostredí; Úzko spolupracujú so sieťou jednotiek CSIRT pri výmene informácií. Poskytujú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetickobezpečnostného incidentu orgánom členských štátov a Komisii prostredníctvom siete EU-CyCLONe a siete jednotiek CSIRT.	

Aktér	Úroveň	Úloha a právomoc	Odkaz
Sieť jednotiek CSIRT	technická	Prispieva k zvyšovaniu dôvery a podporuje rýchlu operačnú spoluprácu medzi členskými štátmi. Je hlavnou sieťou na výmenu relevantných informácií o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľnostiach. Na žiadosť člena potenciálne zasiahnutého incidentom si sieť vymieňa informácie o danom incidente a súvisiacich kybernetických hrozbách a diskutuje o nich. Sieť môže takisto uľahčovať koordinovanú reakciu na incident, ktorý bol identifikovaný v rámci jurisdikcie žiadajúceho člena. Poskytuje pomoc členským štátom pri riadení cezhraničných incidentov a skúma ďalšie formy spolupráce vrátane vzájomnej pomoci. Prijíma informácie od členských štátov o ich žiadostiach o podporu z rezervy EÚ na účely kybernetickej bezpečnosti.	smernica (EÚ) 2022/2555 nariadenie (EÚ) 2025/38

Aktér	Úroveň	Úloha a právomoc	Odkaz
Konferencia veliteľov v oblasti kybernetickej bezpečnosti		Fórum pre veliteľov v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni v členských štátoch na účely spolupráce a výmeny dôležitých informácií týkajúcich sa prebiehajúcich operácií v kybernetickom priestore a stratégií na zmiernenie rozsiahlych kybernetickobezpečnostných incidentov. Organizuje ho rotujúce predsedníctvo Rady Európskej únie s podporou Európskej obrannej agentúry (EDA) a Európskej služby pre vonkajšiu činnosť (ESVČ) vrátane Vojenského štábu EÚ (EUMS).	spoločné oznámenie o politike EÚ v oblasti kybernetickej obrany (2022)
Komisia	operačná/politická	Výkonný orgán Európskej únie. Zabezpečovanie riadneho fungovania vnútorného trhu. Uľahčuje súdržnosť a koordináciu medzi súvisiacimi opatreniami v oblasti reakcie na krízu na úrovni Únie. Určité všeobecné opatrenia v oblasti pripravenosti na úrovni Únie podľa rozhodnutia o mechanizme UCPM vrátane	článok 17 Zmluvy o Európskej únii vykonávacie rozhodnutie (EÚ) 2018/1993 rozhodnutie č. 1313/2013/EÚ smernica (EÚ) 2022/2555

Aktér	Úroveň	Úloha a právomoc	Odkaz
		riadenia Koordinačného centra pre reakcie na núdzové situácie a spoločného systému komunikácie a poskytovania informácií v prípade núdzových situácií. Komisia je pozorovateľom v sieti EU-CyCLONe a jej členom v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetickobezpečnostný incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti, ktoré patria do rozsahu pôsobnosti smernice (EÚ) 2022/2555. Pozorovateľ v sieti jednotiek CSIRT. Celková zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti. Kontaktné miesto v Medziinštitucionálnej rade pre kybernetickú bezpečnosť na zdieľanie relevantných informácií o závažných incidentoch so sieťou EU-CyCLONe. Predsedníctvo Rady s ňou konzultuje o rozhodnutiach	nariadenie (EÚ) 2025/38 nariadenie (EÚ, Euratom) 2023/2841

Aktér	Úroveň	Úloha a právomoc	Odkaz
		aktivovať alebo deaktivovať IPCR (okrem prípadov, keď sa uplatňuje doložka o solidarite podľa článku 222 ZFEÚ). Útvary Komisie spolu s ESVČ vypracúvajú správy ISAA.	
Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA)	technická/operačná	Vykonáva úlohy na účely dosiahnutia vysokej úrovne kybernetickej bezpečnosti v celej Únii, a to aj aktívnou podporou členských štátov a inštitúcií Únie Zabezpečuje sekretariát pre sieť jednotiek CSIRT a sieť EU-CyCLONe. Pripravuje pravidelnú technickú situačnú správu o kybernetickej bezpečnosti v EÚ týkajúcu sa incidentov a kybernetických hrozieb (spolu s EC3 a CERT-EU a v úzkej spolupráci s členskými štátmi). Pomáha rozvíjať spoločnú reakciu na rozsiahle cezhraničné incidenty alebo krízy prostredníctvom: – agregácie a analýzy správ z vnútroštátnych zdrojov, – zabezpečenia toku informácií medzi technickou, operačnou a politickou úrovňou,	smernica (EÚ) 2022/2555 nariadenie (EÚ) 2019/881 nariadenie (EÚ) 2025/38 nariadenie (EÚ) 2024/2847

Aktér	Úroveň	Úloha a právomoc	Odkaz
		– uľahčovania riešenia incidentov (na požiadanie), – podpory subjektov Únie v oblasti komunikácie s verejnosťou, – podpory členských štátov v oblasti komunikácie s verejnosťou (na požiadanie), – testovania spôsobilostí reakcie na incidenty a pravidelného organizovania cvičení v oblasti kybernetickej bezpečnosti. Koná ako verejný obstarávateľ, ak bola poverená prevádzkou a správou rezervy EÚ na účely kybernetickej bezpečnosti, a to čiastočne alebo úplne. Každé dva roky organizuje rozsiahle komplexné kybernetickobezpečnostné cvičenie na úrovni Únie s technickými, operačnými alebo strategickými prvkami. V spolupráci s dotknutým členským štátom a inými príslušnými zainteresovanými stranami vypracúva správy o preskúmaní incidentu s cieľom posúdiť príčiny, dosah a zmierňovanie vplyvu incidentu (na žiadosť Komisie alebo siete EU-CyCLONe a so	

Aktér	Úroveň	Úloha a právomoc	Odkaz
		súhlasom dotknutého členského štátu). Informuje sieť EU-CyCLONe, ak sú informácie poskytnuté v rámci oznamovacích povinností vyplývajúcich z aktu o kybernetickej odolnosti relevantné pre koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kríz na operačnej úrovni.	
Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe)	operačná	Podporuje koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kríz na operačnej úrovni. Zabezpečuje pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Koordinuje riadenie rozsiahlych kybernetickobezpečnostných incidentov a kríz a podporuje rozhodovanie na politickej úrovni v súvislosti s takýmito incidentmi a krízami.	smernica (EÚ) 2022/2555 nariadenie (EÚ) 2025/38

Aktér	Úroveň	Úloha a právomoc	Odkaz
		Posudzuje dôsledky a vplyv relevantných rozsiahlych kybernetickobezpečnostných incidentov a kríz a navrhuje možné zmierňujúce opatrenia. Na žiadosť dotknutého členského štátu prerokúva národné plány reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy. Spolu s agentúrou ENISA a Komisiou vypracúva vzor na uľahčenie predkladania žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Prijíma informácie od členských štátov o ich žiadostiach o podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Prijíma informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetickobezpečnostného incidentu z cezhraničných kybernetických centier alebo siete jednotiek CSIRT.	

Aktér	Úroveň	Úloha a právomoc	Odkaz
Vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku s podporou Európskej služby pre vonkajšiu činnosť	politická	Vedie a koordinuje úsilie Únie o riešenie vonkajších bezpečnostných hrozieb v hybridnej a kybernetickej oblasti. Zodpovedá za nástroje kybernetickej diplomacie a kybernetickej obrany Únie s cieľom odrádzať od vonkajších hrozieb a reagovať na ne, a to aj prostredníctvom súboru nástrojov Únie na boj proti hybridným hrozbám a súboru nástrojov kybernetickej diplomacie. Spolupracuje s externými partnermi aj prostredníctvom zapájania sa do SBOP. Zabezpečuje úniu pripravenosti a situačné povedomie členských štátov v súvislosti s hybridnými a kybernetickými hrozbami, ako aj ich schopnosť reagovať na ne, napríklad prostredníctvom praktických cvičení, odbornej prípravy a sietí. Zaoberá sa bezpečnostnými a obrannými dôsledkami vesmírnych prostriedkov Únie, najmä v rámci spoločnej	rozhodnutie Rady 2010/427/EÚ

Aktér	Úroveň	Úloha a právomoc	Odkaz
		bezpečnostnej a obrannej politiky Únie (SBOP). Podporuje konferenciu veliteľov EÚ v oblasti kybernetickej bezpečnosti. Podporuje operačnú sieť EÚ pre vojenské tímy reakcie na počítačové núdzové situácie (MICNET). Predsedníctvo Rady s ním konzultuje o rozhodnutiach aktivovať alebo deaktivovať IPCR (okrem prípadov, keď sa uplatňuje doložka o solidarite podľa článku 222 ZFEÚ). ESVČ spolu s útvarmi Komisie vypracúva správu ISAA.	
Koordinačné centrum kybernetickej obrany EÚ	horizontálne	Jeho pôvodným cieľom je predovšetkým zlepšiť spoločné situačné povedomie Únie a jej členských štátov o škodlivých činnostiach v kybernetickom priestore, najmä pokiaľ ide o vojenské misie a operácie SBOP.	spoločné oznámenie o politike EÚ v oblasti kybernetickej obrany (2022)
Europol	operačná	Poskytuje operačnú a technickú podporu príslušným orgánom členských štátov pri predchádzaní počítačovej kriminalite a odrádzaní od nej.	nariadenie (EÚ) 2016/794 vrátane všetkých jeho zmien

Aktér	Úroveň	Úloha a právomoc	Odkaz
		Pomáha príslušným orgánom členských štátov na ich žiadosť pri reakcii na kybernetické útoky s podozrením na zločinecké pozadie.	
Medziinštitucionálna rada pre kybernetickú bezpečnosť		Vypracúva plán riadenia kybernetických kríz s cieľom podporiť koordinované riadenie závažných incidentov, ktoré majú vplyv na subjekty Únie, na operačnej úrovni a prispieť k pravidelnej výmene relevantných informácií. Koordinuje prijímanie plánov riadenia kybernetických kríz jednotlivých subjektov Únie. Na základe návrhu CERT-EU prijíma usmernenia alebo odporúčania k spolupráci pri reakcii na incidenty v prípade významných incidentov týkajúcich sa subjektov Únie.	nariadenie (EÚ, Euratom) 2023/2841
Operačná sieť pre vojenské tímy reakcie na počítačové núdzové situácie (MICNET)	technická	Podporuje silnejšiu a koordinovanejšiu reakciu na kybernetické hrozby ovplyvňujúce obranné systémy v Únii vrátane tých, ktoré sa používajú vo vojenských misiách	spoločné oznámenie o kybernetickej obrane z roku 2022

Aktér	Úroveň	Úloha a právomoc	Odkaz
		a operáciách SBOP. Podporuje ju Európska obranná agentúra.	
Jednotná kapacita na analýzu spravodajských informácií (SIAC)		Skladá sa zo 1. Spravodajského a situačného centra EÚ (EU INTCEN) a 2. útvaru SIAC riaditeľstva spravodajskej služby vojenského štábu EÚ (EUMS INT) SIAC. Poskytuje strategické spravodajské informácie o zahraničnej politike, terorizme a kybernetických a hybridných hrozbách. Spracúva vojenské spravodajstvo pre misie SBOP a podporuje operácie Únie v oblasti obrany a krízového riadenia. Podriadená vedeniu vysokého predstaviteľa.	články 38 a 42 až 46 Zmluvy o Európskej únii

3) Príslušné mechanizmy a platformy krízového riadenia na úrovni Únie

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
ARGUS	horizontálny	Koordinačný proces Komisie a všeobecný systém varovania pre súdržnú reakciu v prípade závažnej cezhraničnej krízy, ktorá si vyžaduje opatrenia na úrovni EÚ. Spája všetky príslušné útvary a kabinety, aby rozhodovali o opatreniach a koordinovali ich. Umožňuje Komisii vymieňať si relevantné informácie o vznikajúcich krízach zasahujúcich viacero odvetví alebo predvídateľných či bezprostredných hrozbách, ktoré si vyžadujú opatrenia na úrovni Únie.	oznámenie Komisie (2005)662
Centrum ESVČ pre reakciu na krízy (CRC)	horizontálny	Jednotné kontaktné miesto ESVČ pre všetky otázky súvisiace s krízami a nepretržitá 24/7 spôsobilosť reagovať na krízu v prípade núdzových situácií ohrozujúcich bezpečnosť zamestnancov v delegáciách EÚ a/alebo na krízy, ktoré postihujú občanov Únie v zahraničí. Združuje expertov na bezpečnosť, konzulárne záležitosti a situačné povedomie, pričom sa spolieha	Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti (21. marca 2022)

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
		na angažovaných odborníkov v delegáciách Únie.	
Koncepcia kritickej infraštruktúry	horizontálny	Koordinuje sa ňou reakcia na úrovni Únie na narušenia kritickej infraštruktúry so značným cezhraničným významom.	odporúčanie Rady C/2024/4371
Systém varovania pred kybernetickobezpečnostnými hrozbami	špecifický pre kybernetickú bezpečnosť	Zabezpečujú sa ním pokročilé spôsobilosti Únie s cieľom zlepšiť schopnosti odhaľovania, analýzy a spracúvania údajov v súvislosti s kybernetickými hrozbami a predchádzanie incidentom v Únii.	nariadenie (EÚ) 2025/38
Súbor nástrojov kybernetickej diplomacie (rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti)	špecifický pre kybernetickú bezpečnosť	Umožňuje spoločnú diplomatickú reakciu Únie na škodlivé kybernetické činnosti, ktorá prispieva k predchádzaniu konfliktom, zmierňovaniu kybernetických hrozieb a väčšej stabilite v medzinárodných vzťahoch.	závery Rady z 19. júna 2017 revidované vykonávacie usmernenia 10289/23, 8. júna 2023
Rezerva EÚ na účely kybernetickej bezpečnosti	špecifický pre kybernetickú bezpečnosť	Mobilizujú sa ňou odborníci a zdroje v oblasti kybernetickej bezpečnosti počas kríz s cieľom podporiť reakčné úsilie v členských štátoch, inštitúciách, orgánoch úradoch alebo agentúrach Únie	nariadenie (EÚ) 2025/38

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
Sieťový predpis pre odvetvové pravidlá týkajúce sa aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny	odvetvový	Stanovuje sa ním opakujúci sa proces posudzovania kybernetickobezpečnostných rizík v odvetví elektrickej energie na úrovni Únie, členských štátov, regiónov a subjektov. Obsahuje ustanovenia špecifické pre krízové riadenie a spoluprácu s jednotkami CSIRT a sieťou EU-CyCLONe v prípadoch, keď má rozsiahly kybernetickobezpečnostný incident vplyv na iné odvetvia závislé od bezpečnosti dodávok elektriny.	delegované nariadenie Komisie (EÚ) 2024/1366
Súbor nástrojov na boj proti hybridným hrozbám	horizontálny	Zahŕňa súbor ustanovení na zabezpečenie prehľadu o nástrojoch, ktoré sú k dispozícii na úrovni EÚ v reakcii na všetky druhy hybridných hrozieb, a o ich koordinovanom využívaní a zabezpečuje súdržnosť našich opatrení v rôznych oblastiach. Súbor nástrojov na boj proti hybridným hrozbám pomáha zabezpečiť, aby sa rozhodovanie zakladalo na komplexnom situačnom povedomí a získaných poznatkoch.	závery Rady o rámci pre koordinovanú reakciu EÚ na hybridné kampane, 22. júna 2022 vykonávacie usmernenia pre rámec pre koordinovanú reakciu EÚ na hybridné kampane, 14. decembra 2022

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
Tímy rýchlej reakcie na hybridné hrozby (EU HRRT)	horizontálny	Tímy rýchlej reakcie EÚ na hybridné hrozby ako súčasť súboru nástrojov EÚ na boj proti hybridným hrozbám čerpajú z príslušných odvetvových civilných a vojenských odborných znalostí na úrovni členských štátov aj EÚ s cieľom poskytovať prispôsobenú a cielenú krátkodobú pomoc členským štátom, misiám a operáciám spoločnej bezpečnostnej a obrannej politiky a partnerským krajinám v boji proti hybridným hrozbám a kampaniam.	usmerňujúci rámec pre praktické zriadenie tímov rýchlej reakcie EÚ na hybridné hrozby (21. mája 2024) operačné usmernenia pre nasadenie tímov rýchlej reakcie na hybridné hrozby, schválené Coreperom 4. decembra 2024
IPCR	horizontálny	Podporuje sa nimi rýchle a koordinované rozhodovanie na politickej úrovni Únie v prípade závažných a zložitých kríz. Rozhodnutie o aktivácii a deaktivácii prijíma predsedníctvo Rady, ktoré vedie konzultácie (okrem prípadov, keď sa uplatňuje doložka o solidarite) s dotknutými členskými štátmi, Komisiou a vysokým predstaviteľom. GSR, útvary Komisie a ESVČ sa môžu po konzultácii s predsedníctvom tiež dohodnúť na aktivácii IPCR v režime výmeny informácií. Práca v rámci IPCR vychádza zo správ ISAA, ktoré vypracúvajú útvary	vykonávacie rozhodnutie Rady (EÚ) 2018/1993

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
		Komisie a ESVČ. Takéto správy sa opierajú o relevantné informácie a analýzy poskytované členskými štátmi (napr. z príslušných národných krízových centier) a príslušnými agentúrami a orgánmi Únie.	
Protokol reakcie na núdzové situácie v rámci presadzovania práva EÚ	horizontálny	Nástroj na podporu orgánov presadzovania práva Únie pri poskytovaní okamžitej reakcie na závažné cezhraničné kybernetické útoky prostredníctvom rýchleho posúdenia, bezpečného a včasného zdieľania kritických informácií a účinnej koordinácie medzinárodných aspektov ich vyšetrovania.	závery Rady (26. júna 2018) o koordinovanej reakcii EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu
Tímy rýchlej kybernetickej reakcie PESCO (CRRT)	špecifický pre kybernetickú bezpečnosť	Tímy PESCO CRRT sú spoločne rozvíjanou civilno-vojenskou spôsobilosťou členských štátov EÚ v oblasti kybernetickej obrany s cieľom rýchlo reagovať na kybernetické incidenty a kybernetické krízy, ako aj vykonávať preventívne opatrenia, ako sú posúdenia zraniteľnosti a monitorovanie volieb. Poslaním PESCO CRRT je na požiadanie	článok 42 ods. 6 a článok 46 Zmluvy o Európskej únii a protokol č. 10 k nej

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
		poskytovať kybernetickú podporu členským štátom EÚ, inštitúciám, orgánom, úradom a agentúram EÚ, vojenským misiám a operáciám SBOP EÚ, ako aj partnerským krajinám.	

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
Architektúra reakcie na vesmírne hrozby (STRA)	odvetvový (vesmírne hrozby vrátane kybernetických)	Architektúra reakcie na vesmírne hrozby (STRA) týkajúca sa povinností, ktoré majú Rada a vysoký predstaviteľ vykonávať s cieľom odvrátiť hrozbu vyplývajúcu z nasadenia, prevádzky alebo používania systémov zriadených a služieb poskytovaných v rámci Vesmírneho programu Únie.	rozhodnutie Rady (SZBP) 2021/698
Rámec koordinácie systémových kybernetických incidentov (EU-SCICF)	odvetvový	Rámec, ktorý sa vyvíja na účely komunikácie a koordinácie a ktorým sa riešia a riadia potenciálne systémové kybernetické udalosti vo finančnom sektore. Bude vychádzať z jednej z plánovaných úloh európskych orgánov dohľadu (ESA) podľa nariadenia (EÚ) 2022/2554, ktorou je postupne umožniť účinnú koordinovanú reakciu na úrovni Únie v prípade závažného cezhraničného incidentu alebo hrozby súvisiacich s informačnými a komunikačnými technológiami (IKT), ktoré majú systémový vplyv na finančný sektor Únie ako celok.	odporúčanie Európskeho výboru pre systémové riziká z 2. decembra 2021 o celoeurópskom rámci koordinácie systémových kybernetických incidentov pre príslušné orgány (ESRB/2021/17)
Mechanizmus Únie v oblasti civilnej ochrany (UCPM)	horizontálny	Zabezpečuje spoluprácu v oblasti civilnej ochrany s cieľom zlepšiť prevenciu, pripravenosť a reakciu na katastrofy.	rozhodnutie 1313/2013

Mechanizmus	Horizontálny/ odvetvový/špecifický pre kybernetickú bezpečnosť	Opis	Odkaz
CISE – spoločné prostredie na výmenu informácií	špecifický pre námorný sektor, pokrýva sedem odvetví	CISE je sieť, ktorá spája systémy orgánov EÚ/EHP zodpovedných za námorný dozor. Umožňuje bezproblémovú a automatizovanú výmenu relevantných informácií cez hranice a naprieč rôznymi odvetviami.	Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti (21. marca 2022)

4) Odvetvia s vysokou úrovňou kritickosti a iné kritické odvetvia podľa smernice (EÚ) 2022/2555 a odvetvové krízové mechanizmy na úrovni Únie (v náležitých prípadoch)		
Odvetvia	**Pododvetvie**	**Uplatniteľné odvetvové krízové mechanizmy**
Energetika	elektrická energia	skupina pre koordináciu v oblasti elektrickej energie
	diaľkové vykurovanie a chladenie	neexistuje
	ropa	koordinačná skupina pre ropu skupina orgánov Európskej únie pre prieskum ložísk a ťažbu ropy a zemného plynu na mori (EUOAG)
	plyn	koordinačná skupina pre plyn
	vodík	neexistuje
Doprava	letecká doprava	Európska jednotka krízovej koordinácie v letectve (EACCC)
	železničná doprava	neexistuje
	vodná doprava	Európska agentúra pre kontrolu rybárstva (EFCA) SafeSeaNet (SSN) integrované námorné služby (IMS) dátové stredisko systému identifikácie a sledovania lodí na veľkú vzdialenosť (LRIT) námorné podporné služby EMSA

	cestná doprava	neexistuje
	horizontálna úroveň	sieť národných dopravných kontaktných miest zriadená v rámci pohotovostného plánu pre dopravu [COM(2022) 211 final]
Bankovníctvo		rámec EU-SCICF
Infraštruktúry finančných trhov		rámec EU-SCICF Európsky finančný stabilizačný mechanizmus

Zdravotníctvo		systém včasného varovania a reakcie (EWRS) systém rýchleho varovania pre tkanivá, bunky a zložky krvi (RATC/RAB) v rámci nástroja na riadenie krízových situácií v oblasti zdravia (HEOF) Rámec pre núdzové situácie v oblasti verejného zdravia systém rýchleho varovania pre chemické incidenty (RASCHEM) Európsky portál dohľadu pre infekčné choroby Úrad pre pripravenosť a reakcie na núdzové zdravotné situácie (HERA) Systém zdravotníckych spravodajských informácií (MediSys) výkonná riadiaca skupina na monitorovanie nedostatku zdravotníckych pomôcok (MDSSG) Rýchle varovanie v oblasti farmakovigilancie osobitná skupina EÚ pre oblasť zdravia (EUHTF) Výbor pre zdravotnú bezpečnosť
Pitná voda		neexistuje

Odpadová voda		neexistuje
Digitálna infraštruktúra		neexistuje
Riadenie služieb IKT		neexistuje
Verejná správa		neexistuje
Vesmír		Architektúra reakcie na vesmírne hrozby (STRA)
Poštové a kuriérske služby		neexistuje
Odpadové hospodárstvo		neexistuje
Výroba a distribúcia chemických látok		systém rýchleho varovania pre chemické incidenty (RASCHEM)

Výroba, spracovanie a distribúcia potravín		európsky systém monitorovania plodín globálne odhaľovanie kritických miest anomálií poľnohospodárskej výroby (ASAP) európska sieť informačných systémov o zdraví rastlín (EUROPHYT) núdzový tím EÚ pre oblasť veterinárnej medicíny (EUVET) systém rýchleho varovania pre potraviny a krmivá (RASFF) Európsky mechanizmus pripravenosti a reakcie na krízu potravinovej bezpečnosti (EFSCM) akt o núdzovej situácii na vnútornom trhu a jeho odolnosti (IMERA)
Výroba	zdravotnícke pomôcky	neexistuje
	počítačové, elektronické a optické výrobky	neexistuje
	stroje a zariadenia	neexistuje
	výroba motorových vozidiel, návesov a prívesov	neexistuje
	výroba ostatných dopravných prostriedkov	neexistuje

Poskytovatelia digitálnych služieb		neexistuje
Výskum		neexistuje

PRÍLOHA III – rámec EÚ pre reakciu na kybernetickobezpečnostnú krízu a súvisiace nástroje

Od roku 2017 Únia rozvíja svoj rámec pre kybernetickú bezpečnosť prostredníctvom niekoľkých nástrojov, ktoré obsahujú ustanovenia relevantné pre riadenie kybernetických kríz:

- nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[1],
- smernica Európskeho parlamentu a Rady (EÚ) 2022/2555[2],
- vykonávacie nariadenie Komisie 2024/2690[3], nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841[4],
- nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887[5],
- nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847[6],
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 (akt o kybernetickej solidarite)[7].

Medzi osobitné odvetvové krízové opatrenia v oblasti kybernetickej bezpečnosti patria delegované nariadenie Komisie (EÚ) 2024/1366[8] a pripravovaný rámec koordinácie systémových kybernetických incidentov (EU-SCICF) v kontexte nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554[9].

Smernica 2013/40[10] poskytuje odkaz na vymedzenie trestnej činnosti súvisiacej s kybernetickými útokmi a pravidlá Únie o cezhraničnom prístupe k elektronickým dôkazom; najmä nariadením Európskeho parlamentu a Rady (EÚ) 2023/1543[11] sa po jeho vykonaní výrazne uľahčí činnosť orgánov presadzovania práva v tejto oblasti.

V politike EÚ v oblasti kybernetickej obrany[12] sa uvádzajú úlohy operačnej siete EÚ pre vojenské tímy reakcie na počítačové núdzové situácie (MICNET) a konferencie veliteľov EÚ v oblasti kybernetickej bezpečnosti a predpokladá sa zriadenie Koordinačného centra kybernetickej obrany EÚ (EUCDCC).

V niektorých kritických odvetviach uvedených v prílohách I a II k smernici (EÚ) 2022/2555 existujú aj iné mechanizmy situačného povedomia a reakcie na krízu, ktoré nesúvisia s kybernetickou bezpečnosťou.

V odporúčaní Rady o koncepcii koordinovanej reakcie Únie na narušenia kritickej infraštruktúry so značným cezhraničným významom[13] sa stanovuje spolupráca medzi príslušnými aktérmi v prípadoch, keď má incident vplyv na fyzické aspekty aj kybernetickú bezpečnosť kritickej infraštruktúry.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb (Ú. v. EÚ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg/2023/2690/oj).

[4] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841 z 13. decembra 2023, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (Ú. v. EÚ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887 z 20. mája 2021, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu

a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite) (Ú. v. EÚ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Delegované nariadenie Komisie (EÚ) 2024/1366 z 11. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 stanovením sieťového predpisu pre odvetvové pravidlá týkajúce sa aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny (Ú. v. EÚ L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011(Ú. v. EÚ L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie a smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní (Ú. v. EÚ L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52022JC0049.

[13] *Ú. v. EÚ C, C/2024/4371, 5.7.2024,* https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:C_202404371.