EURÓPSKA
KOMISIA

V Bruseli 24. 2. 2025
COM(2025) 66 final

2025/0036 (NLE)

Návrh

ODPORÚČANIE RADY

o koncepcii EÚ týkajúcej sa riadenia kybernetických kríz

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Rada vo svojich záveroch o budúcnosti kybernetickej bezpečnosti z 22. mája 2024

> *„[vyzvala] Komisiu, aby urýchlene vyhodnotila súčasnú koncepciu kybernetickej bezpečnosti a na tomto základe navrhla revidovanú koncepciu kybernetickej bezpečnosti vo forme odporúčania Rady, v ktorom sa pozornosť bude venovať súčasným výzvam a komplexnej panoráme kybernetických hrozieb, posilnia sa v ňom existujúce siete, zlepší spolupráca a odstránia bariéry medzi organizáciami, pričom sa na tento účel využijú predovšetkým existujúce štruktúry. Okrem toho by sa revidovaná koncepcia mala opierať o časom overené hlavné zásady spolupráce (proporcionalita, subsidiarita, komplementárnosť a dôvernosť informácií) a rozšíriť ich na celý životný cyklus krízového riadenia a mala by prispieť k zosúladeniu a posilneniu zabezpečenej komunikácie v oblasti kybernetickej bezpečnosti. Pri revidovanej koncepcii by sa malo zabezpečiť, aby bola zlučiteľná s existujúcimi rámcami, ako sú dojednania EÚ o integrovanej politickej reakcii na krízu (IPCR), súbor nástrojov kybernetickej diplomacie EÚ, súbor nástrojov EÚ na boj proti hybridným hrozbám, protokol reakcie na núdzové situácie v rámci presadzovania práva v EÚ (LERP), novými rámcami, ako je koncepcia kritickej infraštruktúry, sektorové postupy a celkové štruktúry krízového riadenia v rámci subjektov Únie, a to aj so zapojením vysokého predstaviteľa a Europolu. V tejto revidovanej koncepcii by sa úloha Komisie, vysokého predstaviteľa a agentúry ENISA v súlade s ich právomocami mala zamerať najmä na podporu horizontálnej koordinácie.“*

Cieľom tohto návrhu odporúčania Rady o koncepcii Únie pre riadenie kybernetických kríz (ďalej len „kybernetická koncepcia“) je jasným, jednoduchým a prístupným spôsobom predstaviť rámec Európskej únie (EÚ) pre riadenie kybernetických kríz. To by malo príslušným aktérom Únie (teda jednotlivým subjektom a sieťam subjektov na úrovni Únie) umožniť pochopiť, ako vzájomne spolupracovať a čo najlepšie využívať dostupné mechanizmy počas celého životného cyklu krízového riadenia. Jeho zámerom je vysvetliť, čo je kybernetická kríza a čo aktivuje mechanizmus na riešenie kybernetických kríz na úrovni Únie. Vysvetľuje sa v ňom využitie dostupných mechanizmov, ako je mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií vrátane rezervy EÚ na účely kybernetickej bezpečnosti, pri príprave na zvládnutie krízy vyplývajúcej z rozsiahleho kybernetického incidentu, reakciu na ňu a zotavenie sa z nej. Okrem toho sa zameriava na podporu štruktúrovanejšej spolupráce medzi civilnými a vojenskými aktérmi vrátane spolupráce s Organizáciou Severoatlantickej zmluvy (NATO), keďže rozsiahly kybernetický incident, ktorý by zasiahol civilnú infraštruktúru Únie, na ktorú sa spolieha armáda, môže aktivovať aj mechanizmy reakcie NATO.

Kybernetická koncepcia je nezáväzný nástroj, ktorým sa určujú konkrétne opatrenia pre príslušných aktérov v prípade kybernetickej krízy a ktorým sa môže zvýšiť celková účinnosť rámca pre riadenie kybernetických kríz. Aktualizuje sa ním koncepcia stanovená v odporúčaní Komisie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu a vychádza z výsledkov a poznatkov získaných z cvičení na úrovni Únie od prijatia uvedeného odporúčania. Tvorí súčasť širších politických priorít v oblasti pripravenosti a bezpečnosti.

Podľa vymedzenia v smernici (EÚ) 2022/2555 (smernica NIS 2) je rozsiahly kybernetický incident taký incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty. Takýto

incident sa môže v závislosti od svojej príčiny a dosahu vystupňovať a naplno prerásť do 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.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Návrh je v súlade s príslušnými nástrojmi Únie v oblasti kybernetickej bezpečnosti, najmä so smernicou NIS 2 a s nariadením (EÚ) 2023/2841, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie. Takisto je v súlade s rámcom mechanizmu Únie v oblasti civilnej ochrany (UCPM), ktorý bol zriadený rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ, s vykonávacím rozhodnutím (EÚ) 2018/1993 o dojednaniach EÚ o integrovanej politickej reakcii na krízu (IPCR) a s odvetvovými nástrojmi pre situačné povedomie a krízové riadenie vrátane odvetvia elektrickej energie.

- **Súlad s ostatnými politikami Únie**

Kybernetická koncepcia dopĺňa nedávno prijaté odporúčanie Rady o koncepcii koordinovanej reakcie Únie s cieľom riešiť narušenia kritickej infraštruktúry so značným cezhraničným významom a je s ním v súlade, keďže táto koncepcia sa vzťahuje na narušenia súvisiace s nekybernetickou fyzickou odolnosťou. Je v úzkej súčinnosti s mechanizmami a nástrojmi krízového riadenia v rámci spoločnej zahraničnej a bezpečnostnej politiky (SZBP) a spoločnej bezpečnostnej a obrannej politiky (SBOP), ako sa uvádza v Strategickom kompase Rady pre bezpečnosť a obranu. Iniciatívy Únie zamerané na boj proti počítačovej kriminalite môžu okrem toho podporiť ciele sledované v tomto odporúčaní.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právny základ**

Pri návrhu sa vychádza z článku 292 ZFEÚ, v ktorom sa stanovujú príslušné pravidlá týkajúce sa prijímania odporúčaní.

Návrh by doplnil celý legislatívny rámec v oblasti kybernetickej bezpečnosti vytvorený na úrovni Únie. V tomto návrhu sa nerieši riadenie závažných incidentov, ktoré majú vplyv na subjekty Únie v zmysle nariadenia 2023/2841 prijatého na základe článku 298 ZFEÚ. Rieši sa v ňom však výmena informácií medzi subjektmi Únie a členskými štátmi vrátane ustanovení nariadenia 2023/2841 o tom, že zástupca Komisie v Medziinštitucionálnej rade pre kybernetickú bezpečnosť (IICB) má byť kontaktnou osobou na uľahčenie výmeny relevantných informácií súvisiacich so závažnými incidentmi medzi IICB a Európskou sieťou styčných organizácií pre kybernetické krízy EU-CyCLONe, čo má prispieť k spoločnému situačnému povedomiu.

- **Subsidiarita (v prípade inej ako výlučnej právomoci)**

Zatiaľ čo za reakciu na narušenia kritickej infraštruktúry alebo služieb poskytovaných základnými a dôležitými subjektmi sú v prvom rade zodpovedné členské štáty, určité škodlivé kybernetické činnosti cezhraničnej povahy môžu narušiť a poškodiť kritickú informačnú infraštruktúru, od ktorej závisí bezproblémové fungovanie vnútorného trhu. Únia preto zohráva dôležitú úlohu v prípade významného incidentu alebo krízy. Takéto narušenie môže mať vplyv na viaceré alebo dokonca všetky časti hospodárskej činnosti v rámci jednotného trhu a mohlo by ovplyvniť bezpečnosť a medzinárodné vzťahy Únie. Koordinácia na úrovni Únie v prípade narušení kritickej infraštruktúry s významným cezhraničným vplyvom je

nielen vhodná, ale aj potrebná v záujme zabezpečenia fungovania vnútorného trhu. Koordinované reakcie na úrovni Únie podporia reakcie členských štátov na narušenie prostredníctvom spoločného situačného povedomia, koordinovanej komunikácie s verejnosťou a zmierňovania dôsledkov narušenia na vnútorný trh.

- **Proporcionalita**

Tento návrh je v súlade so zásadou proporcionality stanovenou v článku 5 ods. 4 Zmluvy o Európskej únii. Ani obsah, ani forma tohto navrhovaného odporúčania Rady nepresahujú rámec nevyhnutný na dosiahnutie jeho cieľov. Navrhované opatrenia sú primerané sledovaným cieľom, ktoré sa zameriavajú na zabezpečenie koordinovaného riadenia kybernetických kríz v Únii.

- **Výber nástroja**

V záujme dosiahnutia uvedených cieľov sa v ZFEÚ, a to najmä v jej článku 292 stanovuje, že Rada prijíma odporúčania na základe návrhu Komisie. V súlade s článkom 288 ZFEÚ odporúčania nie sú záväzné. Odporúčanie Rady je v tomto prípade vhodným nástrojom, pretože signalizuje záväzok členských štátov k opatreniam, ktoré sú v ňom zahrnuté, a poskytuje pevný základ pre spoluprácu pri koordinácii riadenia rozsiahlych kybernetických incidentov a kríz. Navrhované odporúčanie by tak doplnilo záväzný právny rámec (najmä smernicu NIS 2).

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- **Konzultácie so zainteresovanými stranami**

Pri vypracúvaní tohto návrhu Komisia konzultovala revíziu kybernetickej koncepcie a vyzvala členské štáty a príslušné subjekty Únie, aby sa k nej vyjadrili. Zohľadnila názory expertov členských štátov, ako aj agentúry ENISA prednesené na seminári, ktorý 5. septembra 2024 v Karpaczi spoločne zorganizovali Komisia a Poľsko.

Komisia viedla konzultácie so zástupcami členských štátov v sieti jednotiek CSIRT, sieti EÚ-CyCLONe a v skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v septembri 2024 a vyzvala ich na predloženie písomných príspevkov.

Komisia predstavila a získala spätnú väzbu od Rady počas dvoch špecializovaných diskusií v rámci horizontálnej pracovnej skupiny pre kybernetické otázky, ktoré sa konali v októbri a novembri 2024.

Komisia viedla konzultácie so zástupcami súkromného sektora, ako aj členských štátov, Európskej služby pre vonkajšiu činnosť (ESVČ) a agentúry ENISA na seminári, ktorý v novembri 2024 v Bruseli zorganizovalo Stále zastúpenie Poľska pri EÚ.

Komisia viedla konzultácie s príslušnými subjektmi Únie, konkrétne s ESVČ, agentúrou ENISA, Europolom a CERT-EU, a to aj prostredníctvom diskusií na vysokej úrovni na zasadnutiach pracovnej skupiny pre kybernetické krízy[1], ktoré sa konali v júli a novembri 2024.

Dosiahol sa konsenzus v tom, že je potrebný aktuálny, jasný, jednoduchý a operatívny dokument, ktorý umožní príslušným aktérom pochopiť rámec pre riadenie kybernetických

[1] Neformálna skupina zložená z útvarov Komisie a iných útvarov EÚ.

kríz a účinne využívať dostupné mechanizmy. Zhoda sa dosiahla, aj pokiaľ ide o potrebu vyhnúť sa duplicite nástrojov a dobre využiť existujúce mechanizmy na úrovni Únie na koordináciu, výmenu informácií a reakciu, a to bez vytvárania nových štruktúr alebo zasahovania do vnútorných štandardných operačných postupov existujúcich sietí a existujúcich odvetvových mechanizmov.

2025/0036 (NLE)

Návrh

ODPORÚČANIE RADY

o koncepcii EÚ týkajúcej sa riadenia kybernetických kríz

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 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 hospodárstvo, ktoré je čoraz závislejšie od digitálnych technológií, však zvyšuje aj riziko kybernetických 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 viacrozmerných hybridných hrozieb 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 kybernetický incident môže spôsobiť narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo má významný vplyv na viac ako jeden členský štát. Takýto incident by sa mohol v závislosti od svojej príčiny a dosahu vystupňovať a naplno prerásť do 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 udržanie hospodárskej stability a ochranu európskych vlád, kritickej infraštruktúry, občanov a podnikov, ako aj na prispievanie k medzinárodnej bezpečnosti a stabilite v kybernetickom priestore. Riadenie kybernetických kríz je preto neoddeliteľnou súčasťou celkového rámca EÚ pre riadenie kybernetických kríz.

(3) V súlade s postupmi stanovenými vo vykonávacom rozhodnutí Rady (EÚ) 2018/1993[2] prijíma predsedníctvo Rady rozhodnutie o aktivácii a deaktivácii integrovanej politickej reakcie na krízu (IPCR), pričom vedie konzultácie s dotknutými členskými štátmi, Komisiou a vysokým predstaviteľom (VP) (s výnimkou prípadov, keď došlo k dovolaniu sa doložky o solidarite). Okrem toho sa v súlade s postupmi IPCR môžu generálny sekretariát Rady, útvary Komisie a Európska služba pre vonkajšiu činnosť (ďalej len „ESVČ“) po konzultácii s predsedníctvom dohodnúť na aktivácii IPCR v režime výmeny informácií. Pri diskusiách v rámci IPCR sa vychádza zo správ o

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

integrovanej situačnej informovanosti a analýze, ktoré vypracovali útvary Komisie a ESVČ.

(4) Členské štáty nesú primárnu zodpovednosť za riadenie vnútroštátnych kybernetických kríz, avšak potenciálna cezhraničná a medziodvetvová povaha kybernetických incidentov si vyžaduje, aby členské štáty a príslušné subjekty Únie spolupracovali na technickej, operačnej a politickej úrovni s cieľom účinne koordinovať svoju činnosť v celej Únii. Reakcia na krízu a zotavenie sa z nej sú zároveň pre dotknuté subjekty a odvetvia nákladné. Celý životný cyklus krízového riadenia preto zahŕňa pripravenosť a spoločné situačné povedomie na predvídanie kybernetických incidentov, potrebné spôsobilosti odhaľovania na ich identifikáciu a potrebné nástroje na reakciu a zotavenie na zmierňovanie kybernetických incidentov, odrádzanie od nich a zamedzenie ich šírenia.

(5) 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 reagovaní na rozsiahle kybernetické incidenty a krízy. Zmapovali sa v ňom príslušní aktéri na technickej, operačnej a politickej úrovni a vysvetlilo sa, ako boli začlenené do širšieho 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.

(6) Od roku 2017 Únia vypracovala svoj rámec pre kybernetickú bezpečnosť prostredníctvom niekoľkých nástrojov, ktoré obsahujú ustanovenia relevantné pre riadenie kybernetických kríz: nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[4], smernica Európskeho parlamentu a Rady (EÚ) 2022/2555[5], vykonávacie nariadenie Komisie 2024/2690[6], nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841[7], nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887[8],

---

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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 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).

5 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).

6 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).

7 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).

8 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

nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847[9] a nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 („akt o kybernetickej solidarite“)[10]. Medzi osobitné odvetvové krízové opatrenia v oblasti kybernetickej bezpečnosti patria delegované nariadenie Komisie (EÚ) 2024/1366[11] a pripravovaný rámec koordinácie systémových kybernetických incidentov (EU-SCICF) v kontexte nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554[12]. Smernica 2013/40[13] poskytuje odkaz na vymedzenie trestnej činnosti súvisiacej s kybernetickými útokmi a pravidlá Únie o cezhraničnom prístupe k elektronickým dôkazom a najmä nariadením Európskeho parlamentu a Rady (EÚ) 2023/1543[14] sa po vykonaní výrazne uľahčí činnosť orgánov presadzovania práva v tejto oblasti. V politike EÚ v oblasti kybernetickej obrany[15] 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[16] sa stanovuje spolupráca medzi príslušnými aktérmi v prípadoch, keď má incident vplyv na fyzické aspekty aj kybernetickú bezpečnosť kritickej infraštruktúry.

(7) Medzi príslušných aktérov, ktorí majú zodpovednosť za riadenie kybernetických kríz na úrovni Únie, patria Komisia, ESVČ vrátane jednotnej kapacity na analýzu spravodajských informácií (SIAC), Agentúra Európskej únie pre kybernetickú

---

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).

9 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).

10 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).

11 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).

12 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).

13 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).

14 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).

15 JOIN(2022) 49 final.

16 Ú. v. EÚ C/2024/4371, 5.7.2024.

bezpečnosť (ENISA), tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU), Europol prostredníctvom svojho Európskeho centra boja proti počítačovej kriminalite (EC3), Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe), Sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT), Satelitné stredisko EÚ (SATCEN), Stredisko na monitorovanie bezpečnosti systému Galileo a sieť delegácií Únie. Títo aktéri Únie by mali spoločne určiť oblasti spolupráce a prispievania k vykonávaniu rámca Únie pre riadenie kybernetických kríz v súlade so svojimi právomocami podľa platných právnych predpisov.

(8) Aktualizované odporúčanie, v ktorom sa stanovuje koncepcia kybernetickej bezpečnosti (ďalej len „kybernetická koncepcia“), je potrebné na poskytnutie jasných a prístupných usmernení, v ktorých sa vysvetľuje, čo je kybernetická kríza na úrovni Únie, ako sa aktivuje rámec pre riadenie kybernetických kríz a aké sú úlohy príslušných aktérov a mechanizmov na úrovni Únie, ako aj interakcia medzi týmito aktérmi a mechanizmami počas celého životného cyklu kybernetickej krízy. Kybernetickú koncepciu je potrebné vnímať v širšom kontexte civilno-vojenských vzťahov a vzťahov medzi EÚ a NATO.

(9) Toto odporúčanie dopĺňa dojednania o integrovanej politickej reakcii na krízu EÚ (IPCR) a širšie krízové mechanizmy Únie vrátane spoločného systému rýchleho varovania Komisie ARGUS, mechanizmu Únie v oblasti civilnej ochrany (UCPM) podporovaného Koordinačným centrom pre reakcie na núdzové situácie (ERCC), mechanizmu reakcie Európskej služby pre vonkajšiu činnosť na krízy (CRM), ako aj ďalších procesov, ako sú procesy opísané v súbore nástrojov EÚ na boj proti hybridným hrozbám[17] a v revidovanom protokole EÚ na boj proti hybridným hrozbám. Zároveň dopĺňa odporúčanie Rady o koncepcii koordinovanej reakcie Únie na narušenia kritickej infraštruktúry so značným cezhraničným významom (ďalej len „koncepcia kritickej infraštruktúry“), ktorá sa vzťahuje na nekybernetickú fyzickú odolnosť a ktorej cieľom je zlepšiť koordináciu reakcie na úrovni Únie v tejto oblasti, a malo by byť s ním v súlade.

(10) Komplexný a integrovaný prístup ku krízovému riadeniu by sa mal podporovať vo všetkých odvetviach a na všetkých úrovniach riadenia. Malo by sa posilniť medziodvetvové krízové riadenie na úrovni Únie, aby sa umožnila integrovaná reakcia na krízu, najmä v prípadoch, keď kybernetické incidenty spôsobia reálne následky. Ak sú kybernetické incidenty súčasťou širšej hybridnej kampane alebo krízy, príslušní aktéri by mali podporovať úsilie o vytvorenie jednotného situačného prehľadu vo viacerých odvetviach a oblastiach. Odporúčanie prispieva k širším opatreniam v oblasti pripravenosti Únie na viacrozmerné hybridné hrozby (v súlade so zásadami zakotvenými v stratégii únie pripravenosti).

(11) Bezpečnosť kritickej digitálnej infraštruktúry má zásadný význam pre odolnosť hospodárstva, spoločnosti a obrany Únie. Subjekty, ktoré patria do rozsahu pôsobnosti smernice (EÚ) 2022/2555, vrátane tých, ktoré poskytujú podmorské komunikačné káble, musia prijať opatrenia na ochranu fyzickej a environmentálnej bezpečnosti sietí a informačných systémov na základe prístupu zohľadňujúceho všetky riziká, ako sú zlyhania systému, ľudské chyby, zlomyseľné konanie alebo prírodné javy. Okrem toho by tieto subjekty mali hlásiť incidenty vrátane tých, ktoré sa týkajú podmorských komunikačných káblov, tímom CSIRT alebo prípadne príslušnému orgánu. Hoci

[17] Závery Rady o rámci pre koordinovanú reakciu EÚ na hybridné kampane, 22. júna 2022.

základné zásady, z ktorých kybernetická koncepcia vychádza, sú relevantné pre bezpečnosť podmorských káblov, mechanizmy, ktoré sú v nej stanovené, nie sú dostatočne komplexné na to, aby pokryli celý cyklus odolnosti voči krízam. Jej špecifická povaha si vyžaduje spoločné a prispôsobené úsilie na riešenie potrieb integrovaného dohľadu nad hrozbami a situačného povedomia pre morské oblasti okolo EÚ, strategické investície na vytvorenie redundantných kapacít a spoločný európsky prístup na posilnenie spôsobilostí v oblasti nápravy a obnovy. Stratégia námornej bezpečnosti EÚ zahŕňa opatrenia na zvýšenie kybernetickej bezpečnosti v námornej oblasti a na zlepšenie dohľadu nad kritickou námornou infraštruktúrou vrátane podmorských káblov a jej ochrany. V prípade krízového riadenia na úrovni Únie by bolo vhodné zvážiť vytvorenie osobitnej siete národných kontaktných miest a úzke civilno-vojenské interakcie, a to aj s NATO.

(12) Pripravenosť na krízu si vyžaduje komplexné posúdenie zohľadňujúce všetky riziká a všetky hrozby vzhľadom na zbližovanie hospodárskych a bezpečnostných záujmov EÚ. Spoločné situačné povedomie Únie medzi členskými štátmi a subjektmi Únie, uľahčené dohodou o spoločnej taxonómii a bezpečných komunikačných kanáloch, by malo umožniť koordinovanú a informovanú reakciu na potenciálne rozsiahle kybernetické incidenty, ako aj odstrašenie aktérov pretrvávajúcich hrozieb. Na základe zásady „need-to-know“ (potreba poznať) a vzhľadom na význam dôvery pri výmene informácií by skupiny členských štátov v rôznych zloženiach a prípadne príslušné subjekty Únie mohli chcieť spolupracovať a vymieňať si informácie dôležité pre riadenie kybernetických incidentov. Členské štáty a subjekty Únie, ktoré si vymieňajú informácie o hrozbách, rizikách a nedostatkoch vo vyspelosti by mali umožniť identifikáciu správnych priorít pre rozumné investície a konkrétne opatrenia, ktoré by viedli k lepšej kybernetickej odolnosti.

(13) V súlade s článkom 6 nariadenia (EÚ) 2019/881 agentúra ENISA v úzkej spolupráci s členskými štátmi pripravuje pravidelnú hĺbkovú technickú situačnú správu o kybernetickej bezpečnosti v EÚ, ktorá sa týka incidentov a kybernetických hrozieb. Táto správa sa nazýva správa o spoločnom posúdení kybernetickej bezpečnosti EÚ (EU-JCAR) a pripravuje sa v spolupráci s Europolom/EC3 a CERT-EU s cieľom posilniť pripravenosť Únie, keďže poskytuje situačné povedomie založené na analýze incidentov a kybernetických hrozieb.

(14) Kľúčovú kritickú infraštruktúru, ako sú energetika, doprava, digitálna infraštruktúra, zdravotníctvo alebo finančné služby, ako aj bezpečnostné riešenia nasadené na jej ochranu, zvyčajne prevádzkujú súkromné spoločnosti. Ochrana tejto infraštruktúry pred rozsiahlymi kybernetickými incidentmi si vyžaduje úzku spoluprácu medzi verejnými a súkromnými subjektmi vrátane výrobcov a vývojárov otvorených zdrojov, ktorá je založená na dôvere a jasných a špecializovaných postupoch výmeny informácií, šírenia informácií a koordinácie reakcie.

(15) Kybernetické cvičenia na úrovni Únie sú veľmi účinným nástrojom na testovanie postupov a mechanizmov spolupráce, a tým zvyšujú pripravenosť. Keďže cvičenia sú náročné na zdroje, program cvičení musí byť čo najjednoduchší a najkonsolidovanejší a musia sa v ňom zohľadňovať scenáre vypracované v koordinovanom posúdení rizík Únie a iných príslušných iniciatívach.

(16) Európske digitálne infraštruktúry majú mnoho dôkladne začlenených technických závislostí. Tieto by sa mali riešiť s cieľom zabezpečiť kontinuitu operácií v prípade krízy. Týka sa to napríklad systému názvov domén (DNS), ktorý je kľúčovou zložkou fungovania internetu. Rezolvery DNS sú nevyhnutné pre prístup na internet, a to aj

počas závažnej kybernetickej krízy, pretože prekladajú názvy internetových domén na IP adresy. V smernici (EÚ) 2022/2555 sa príslušné zainteresované strany vyzývajú, aby prijali stratégiu diverzifikácie rozlišovania DNS. Zároveň sa v nej členské štáty nabádajú, aby podporovali rozvoj a využívanie verejnej a bezpečnej európskej služby rezolverov DNS ako kľúčového opatrenia na zabezpečenie pripravenosti a odolnosti voči krízam.

(17) Okrem toho je nutné, aby sa v záujme zvýšenia odolnosti ďalších kritických komponentov, ako je napríklad systém smerovania, a zabezpečenia ich funkčnosti počas závažných kybernetických kríz včas zaviedli príslušné najlepšie postupy a najnovšie dostupné normy. Vo vykonávacom nariadení (EÚ) 2024/2690 sa preto nariaďuje zriadenie multilaterálneho fóra s cieľom určiť najlepšie dostupné normy a techniky zavádzania základných prvkov kybernetickej bezpečnosti a podporuje sa účasť príslušných subjektov na tomto fóre.

(18) Na účinné odhaľovanie škodlivej činnosti v čoraz zložitejších globálnych dodávateľských reťazcoch, ktorá môže mať vplyv na celú Úniu, je potrebný koordinovaný prístup. Je to dôležité najmä v oblastiach, v ktorých sa Únia spolieha na technológie od vysoko rizikových dodávateľov podliehajúcich jurisdikcii tretej krajiny, ktorá vyžaduje nahlasovanie informácií o zraniteľnostiach softvéru alebo hardvéru orgánom danej krajiny skôr, ako sa zistí, že ich možno zneužiť. Štátom sponzorovaní aktéri takisto môžu predbežne zaujať pozíciu v kritickej infraštruktúre so zámerom spôsobiť narušenie neskôr, napríklad počas konfliktu. To sa dá ťažko odhaliť tradičnými metódami, pretože aktéri hrozieb maskujú svoje aktivity tým, že splývajú s legitímnou prevádzkou a používajú techniky „living off the land“, ktoré sa spoliehajú na legitímne nástroje a procesy, aby skryli škodlivé činnosti. To isté platí aj pre tretie krajiny, v ktorých podľa verejných vyhlásení Únie alebo jej členských štátov aktéri hrozieb pôsobiaci z územia týchto krajín vykonávali škodlivé kybernetické činnosti proti Únii. Dodávateľské reťazce by mali zvýšiť svoju odolnosť a viac sa diverzifikovať, pričom by sa mala zachovať spoločná základná úroveň pripravenosti.

(19) Pokiaľ ide o technickú úroveň, pri odhaľovaní incidentov, kybernetických hrozieb a zraniteľností, podpore technických atribútov a zotavovaní sa z kybernetických útokoch zohrávajú zásadnú úlohu tímy CSIRT, orgány presadzovania práva, ako aj národné a cezhraničné kybernetické centrá (ďalej len „kybernetické centrá“), ktoré sa majú zriadiť podľa nariadenia (EÚ) 2025/38. Zásadný význam majú účinné procesné opatrenia pre spoluprácu medzi sieťou jednotiek CSIRT a sieťou EU-CyCLONe, ako sa to vyžaduje v smernici (EÚ) 2022/2555. Cieľom európskeho mechanizmu varovania v oblasti kybernetickej bezpečnosti je podporiť rozvoj pokročilých spôsobilostí Únie s cieľom posilniť schopnosti odhaľovania, analýzy a spracovania údajov v súvislosti s kybernetickými hrozbami a predchádzaním incidentom v Únii.

(20) Pokiaľ ide o okamžitú reakciu, mechanizmy, ktoré majú členské štáty k dispozícii, zahŕňajú rezervu EÚ na účely kybernetickej bezpečnosti a opatrenia podporujúce vzájomnú pomoc zriadené podľa nariadenia (EÚ) 2025/38, tímy rýchlej reakcie na hybridné hrozby a tímy rýchlej kybernetickej reakcie (CRRT) v rámci stálej štruktúrovanej spolupráce (PESCO), ako aj mechanizmy určené pre spojencov NATO. Protokol reakcie na núdzové situácie v rámci presadzovania práva v EÚ (LEERP) okrem toho podporuje orgány presadzovania práva EÚ pri poskytovaní okamžitej reakcie na závažné cezhraničné kybernetické útoky prostredníctvom rýchleho posúdenia, bezpečnej a včasnej výmeny dôležitých informácií a účinnej koordinácie medzinárodných aspektov ich vyšetrovania vrátane zosúladenia činnosti na úrovni orgánov presadzovania práva a koordinácie s partnermi, ktorí nepôsobia ako orgány

presadzovania práva. Získanie jasného prehľadu o tom, aké možnosti reakcie sú k dispozícii v prípade kybernetických incidentov a hybridných činností a ako sa využívajú, môže zabezpečiť efektívne prideľovanie zdrojov a predísť ich duplicite. Podľa nariadenia (EÚ) 2025/38 sú preto členské štáty povinné informovať sieť jednotiek CSIRT a sieť EU-CyCLONe, keď žiadajú o služby rezervy EÚ na účely kybernetickej bezpečnosti.

(21) Účinný boj proti počítačovej kriminalite je pre kybernetickú bezpečnosť nevyhnutný. Odstrašenie sa nedá dosiahnuť len prostredníctvom odolnosti, ale vyžaduje si aj identifikáciu, trestné stíhanie a reakciu na páchateľov. Preto je nevyhnutná spolupráca prostredníctvom prispôsobených technických systémov a platforiem a výmena relevantných informácií medzi aktérmi kybernetickej bezpečnosti, subjektmi kybernetickej diplomacie a orgánmi presadzovania práva v záujme zabezpečenia komplexného pochopenia panorámy hrozieb a schopnosti reagovať súdržným a koordinovaným spôsobom.

(22) Krízy vyvolávajú neistotu, ktorú môžu protivníci ľahko využiť na šírenie dezinformácií a zasievanie nedôvery. S cieľom zabrániť takýmto javom je nutné jasne a dôsledne informovať verejnosť o situácii a o krokoch, ktoré sa prijímajú na jej nápravu. Koordinovanou strategickou komunikáciou možno podporiť aj diplomatické kroky voči aktérom pretrvávajúcich hrozieb a rozvoj opisu hrozieb pre Úniu, ich odstrašujúcich opatrení a potreby podporovať zodpovedné správanie štátov v kybernetickom priestore.

(23) V záujme účinného krízového riadenia je potrebné určiť spoločné bezpečné komunikačné riešenia pre kybernetickú oblasť a zaviesť ich v celej Únii, a to aj na výmenu utajovaných skutočností EÚ, ak to bude nutné. Na základe žiadosti Rady Komisia a ďalšie príslušné subjekty Únie zmapovali existujúce bezpečné komunikačné nástroje a výsledky mapovania predstavili v decembri 2022. V súčasnosti existuje niekoľko samostatných snáh subjektov Únie o vybudovanie bezpečných komunikačných kapacít v krízových situáciách, ktoré si vyžadujú lepšiu koordináciu a využitie. Patrí medzi ne aj zriadenie európskeho kritického komunikačného systému (EUCCS) na zvýšenie odolnosti verejnej komunikačnej infraštruktúry voči škodlivému zasahovaniu a zlepšenie každodennej operačnej spolupráce, a to aj cezhraničnej.

(24) Bezpečnostné prostredie Únie si vyžaduje nadrezortný a celospoločenský prístup k civilnej a vojenskej pripravenosti a pohotovosti zohľadňujúci všetky riziká. Vojenské orgány sa spoliehajú na civilnú kritickú infraštruktúru, ako sú komunikácie, energetika, zdravotníctvo, doprava a logistika. V súlade s tým a ako sa zdôrazňuje v rámci politiky EÚ v oblasti kybernetickej obrany[18], kybernetická bezpečnosť EÚ si vyžaduje väčšiu spoluprácu a súčinnosť medzi kapacitami civilných a vojenských sietí v oblasti pripravenosti a reakcie, a to aj v prípade ozbrojeného útoku. Aktéri kybernetickej bezpečnosti by mali spolupracovať naprieč inštitucionálnymi a operačnými jednotkami s cieľom predvídať hrozbu narušenia zasahujúceho viacero odvetví a viacero dimenzií a reagovať na ňu v súlade so zásadami, ktoré (majú byť zakotvené) v stratégii únie pripravenosti. Okrem toho škodlivá kybernetická činnosť zohráva čoraz väčšiu úlohu v širších hybridných kampaniach proti Únii, jej členským štátom a strategickým partnerom. Preto je potrebná silnejšia spolupráca medzi Úniou a NATO.

[18] Politika EÚ v oblasti kybernetickej obrany, JOIN(2022) 49 final.

(25) Vo vojenskej komunite budúce Koordinačné centrum kybernetickej obrany EÚ a jednotná kapacita na analýzu spravodajských informácií (SIAC) v rámci Európskej služby pre vonkajšiu činnosť, operačná sieť pre vojenské tímy reakcie na počítačové núdzové situácie (MICNET) a konferencia veliteľov EÚ v oblasti kybernetickej bezpečnosti, ktorú sprostredkúva Európska obranná agentúra (EDA), ako aj príslušné projekty v rámci stálej štruktúrovanej spolupráce (PESCO) predstavujú dôležitých aktérov a iniciatívy pre koordináciu a spoluprácu v oblasti pripravenosti na odhaľovanie kybernetických hrozieb, ktoré majú vplyv na Úniu a členské štáty, odrádzanie od nich a obranu pred nimi, ako aj na zotavenie sa z nich. Preto by sa mala podporovať spolupráca medzi civilnými a vojenskými aktérmi, ako je napríklad spolupráca medzi sieťou EU-CyCLONe a konferenciou veliteľov EÚ v oblasti kybernetickej bezpečnosti, ako aj potenciálna spolupráca medzi sieťou MICNET a sieťou jednotiek CSIRT.

(26) Spoluprácou so strategickými medzinárodnými partnerskými krajinami a organizáciami mimo Únie sa posilňujú spôsobilosti Únie v oblasti kybernetickej bezpečnosti. Prostredníctvom podpory medzinárodnej spolupráce môžu Únia a jej partneri zabezpečiť spoločné situačné povedomie a súdržnosť v riadení kybernetických kríz a spoľahlivý stav kybernetickej bezpečnosti a prispieť tak k celosvetovému, otvorenému, stabilnému, bezpečnému a odolnému kybernetickému priestoru. Táto spolupráca by mala byť založená na dôvere a spoločnom cieli chrániť kritickú infraštruktúru a základné služby pred kybernetickými hrozbami, a to aj prostredníctvom podpory zodpovedného správania štátov v kybernetickom priestore založeného na rámci Organizácie Spojených národov (OSN) a vyvodzovania zodpovednosti voči aktérom hrozieb za ich nezodpovedné a nezákonné správanie v kybernetickom priestore. Opatrenia kybernetickej diplomacie prispievajú k odstrašeniu a reakcii na škodlivé kybernetické činnosti a zabezpečujú koordináciu a spoluprácu so strategickými medzinárodnými partnerskými krajinami,

PRIJALA TOTO ODPORÚČANIE:

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

1. V tomto odporúčaní sa stanovuje rámec Únie pre riadenie kybernetických kríz v kontexte celkovej pripravenosti EÚ na viacrozmerné hybridné hrozby. Ako môže incident prerásť do rozsiahleho kybernetického incidentu a následne do krízy na úrovni EÚ, je znázornené a zhrnuté v prílohe 1, a to vrátane prípadov, keď k takémuto incidentu dôjde súbežne s inými hybridnými hrozbami, čo si vyžaduje interakciu medzi potrebnými reakciami. Rámec riadenia kybernetických kríz by mal príslušným aktérom na úrovni Únie vrátane subjektov a sietí umožniť pochopiť, ako vzájomne spolupracovať a čo najlepšie využívať existujúce mechanizmy uvedené v prílohe II v rámci celého životného cyklu krízového riadenia. Okrem toho sa v ňom týmto aktérom na úrovni Únie odporúčajú možné spôsoby zvýšenia účinnosti existujúcich mechanizmov.

2. Únia a jej členské štáty by pri riadení krízy, ktorá vznikla z rozsiahleho kybernetického incidentu v zmysle vymedzenia v článku 6 bode 7 smernice (EÚ) 2022/2555, ktorý má vplyv na riadne fungovanie vnútorného trhu alebo predstavuje vážne riziko pre verejnú bezpečnosť a ochranu subjektov alebo občanov vo viacerých členských štátoch alebo v Únii ako celku (ďalej len „kybernetická kríza“), mali postupovať podľa kybernetickej koncepcie.

3. Ak kybernetický incident, ktorý na technickej úrovni zistila jednotka CSIRT alebo kybernetické centrum, vedie k eskalácii podľa vnútorných postupov siete jednotiek

CSIRT, príslušné informácie by sa mali v súlade s príslušnými procesnými opatreniami poskytnúť sieti EU-CyCLONe, ktorá by mala následne zvážiť, či ide o potenciálny alebo prebiehajúci rozsiahly kybernetický incident v zmysle vymedzenia v článku 6 bode 7 smernice (EÚ) 2022/2555. Určenie toho, či v dôsledku tohto rozsiahleho kybernetického incidentu existuje alebo prestáva existovať kybernetická kríza, by sa malo vykonať v súlade s vykonávacím rozhodnutím (EÚ) 2018/1993, a najmä s jeho článkami 4 a 5.

4. V súlade so zásadami proporcionality, subsidiarity, komplementárnosti a dôvernosti informácií stanovenými v prílohe III by členské štáty a subjekty Únie mali prehĺbiť svoju spoluprácu v oblasti riešenia kybernetických kríz, posilňovať vzájomnú dôveru a opierať sa o existujúce siete a mechanizmy. Hoci kybernetická koncepcia nezasahuje do spôsobu, akým subjekty vymedzujú svoje interné postupy, každý subjekt by mal jasne vymedziť rozhrania používané na spoluprácu s ostatnými subjektmi. Na týchto rozhraniach by sa mali medzi sebou spoločne dohodnúť príslušné subjekty a mali by ich jasne zdokumentovať.

5. Kybernetická koncepcia by sa mala uplatňovať v súlade s koncepciou kritickej infraštruktúry, najmä v prípade incidentov, ktoré majú vplyv na fyzickú odolnosť aj kybernetickú bezpečnosť kritickej infraštruktúry[19]. Ak existujú opatrenia krízového riadenia v jednotlivých odvetviach, ktoré sa vzťahujú na kybernetické incidenty, tieto opatrenia by sa mali vykonávať v súlade s týmto odporúčaním.

II. Príprava na kybernetickú krízu na úrovni Únie

a) Situačné povedomie a výmena informácií

6. Overené a spoľahlivé údaje vrátane trendov v oblasti incidentov, taktík, techník a postupov a aktívne zneužívaných zraniteľností by mali byť základom spoločného situačného povedomia členských štátov a subjektov Únie o panoráme kybernetických hrozieb. Tieto spoločné poznatky by mali členské štáty a subjekty Únie využívať na predvídanie kybernetických útokov, prípravu na ne a ich odhaľovanie v súlade so svojimi príslušnými oblasťami zodpovednosti. Toto spoločné situačné povedomie by malo:

   a) vzťahovať sa na všetky kritické odvetvia uvedené v smernici (EÚ) 2022/2555, najmä na komunikácie, digitálnu infraštruktúru, energetiku, dopravu, financie, vesmír a zdravotníctvo, a prostredníctvom CERT-EU aj na siete a systémy subjektov Únie v súlade s nariadením (EÚ, Euratom) 2023/2841;

   b) vychádzať z vysokokvalitných diverzifikovaných a integrovaných súborov údajov, ktoré sa zbierajú, spracúvajú a vymieňajú v reálnom čase;

   c) zohľadniť sa v správe o spoločnom posúdení kybernetickej bezpečnosti (JCAR) a v ďalších relevantných dokumentoch;

   d) zohľadniť súvisiace hybridné hrozby vrátane zahraničnej manipulácie s informáciami a zahraničného zasahovania a dezinformácií;

   e) podporovať krátkodobé akcie a opatrenia v oblasti reakcie, ako aj prispievať k dlhodobému politickému plánovaniu v kontexte pripravenosti a odstrašovania;

[19] Koordinácia v takýchto prípadoch sa podrobnejšie opisuje v časti I oddiele 4 prílohy ku koncepcii kritickej infraštruktúry.

f) [prepojenie na ďalšie posúdenia rizík a hrozieb, ktoré sa pravidelne vypracúvajú a posilňujú v rámci stratégie únie pripravenosti s cieľom zabezpečiť synergie a zjednodušenie oznamovacích povinnosti členských štátov].

7. 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) naďalej budovať atmosféru dôvery medzi členmi;

c) plne využívať dostupné nástroje na výmenu informácií.

8. Členské štáty a príslušné subjekty Únie by mali zlepšiť spôsoby koordinácie a partnerstva so súkromným sektorom vrátane komunít a výrobcov otvorených zdrojov s cieľom zlepšiť výmenu informácií na základe existujúcich stredísk pre výmenu a analýzu informácií na úrovni EÚ a na vnútroštátnej úrovni, posilniť kapacity v oblasti kybernetickej bezpečnosti a reagovať na kybernetické incidenty, a to aj prostredníctvom diskusií za okrúhlym stolom so sieťou EÚ-CyCLONe a sieťou jednotiek CSIRT.

9. Členské štáty a príslušné subjekty Únie by sa mohli rozhodnúť, že na účely rozvoja spolupráce a posilnenia dôvery a na základe opatrení na výmenu informácií o kybernetickej bezpečnosti podľa smernice (EÚ) 2022/2555 a ustanovení nariadenia (EÚ) 2025/38 týkajúcich sa kybernetických centier vytvoria dobrovoľné zoskupenia spolupráce na základe zásady „need-to-know“ (potreba poznať), ak existujú spoločné záujmy, ako je napríklad odrádzanie od určitého typu hrozby, ktorému čelia, jeho odhaľovanie alebo reakcia naň. Všetky takéto zoskupenia by mali rešpektovať mandát príslušných aktérov, ako aj doteraz vytvorené štruktúry. Tieto spolupracujúce zoskupenia by mohli vyzvať subjekty Únie, aby im uľahčili spoluprácu, a to aj prostredníctvom vhodnej infraštruktúry.

10. Členské štáty by prostredníctvom skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenej smernicou (EÚ) 2022/2555 mali do 12 mesiacov od prijatia kybernetickej koncepcie vypracovať spoločnú taxonómiu v súvislosti s riadením kybernetických kríz a poskytnúť príručku o bezpečnom spracúvaní a výmene informácií týkajúcich sa kybernetických incidentov a kríz vrátane oddielu venovaného určovaniu úrovne dôvernosti týchto informácií (kategorizácia).

11. Pri určovaní úrovne dôvernosti dostupných informácií by členské štáty a príslušné subjekty Únie mali zvážiť potenciálny vplyv, ktorý môže mať nadmerné utajovanie na dobrovoľnú výmenu informácií a dosiahnutie spoločného situačného povedomia. Pri výmene neutajovaných informácií by členské štáty mali v plnej miere využívať existujúce platformy pre technickú a operačnú spoluprácu, ako sú platformy, ktoré používajú sieť jednotiek CSIRT a sieť EU-CyCLONe.

b) Spoločné cvičenia

12. Členské štáty a príslušné subjekty Únie by mali vypracovať účinný rotujúci cyklus kybernetických cvičení s cieľom pripraviť sa na kybernetické krízy a zvýšiť organizačnú efektívnosť. Pri týchto cvičeniach by sa malo vychádzať zo scenárov vypracovaných na základe koordinovaných posúdení rizík EÚ vrátane tých, ktoré sa týkajú kríz zasahujúcich viacero odvetví. V rámci rotujúceho cyklu kybernetických cvičení by sa mal zohľadňovať mechanizmus UCPM a ďalšie mechanizmy reakcie

na krízy na úrovni Únie. Malo by sa zabezpečiť účinné uplatňovanie poznatkov získaných z cvičení.

13. Príslušní aktéri Únie by mohli vykonávať menšie cvičenia na otestovanie svojich interakcií a rozhraní v prípade eskalácie kybernetických incidentov.

14. Útvary Komisie, ESVČ a agentúra ENISA sa vyzývajú, aby do 18 mesiacov od prijatia kybernetickej koncepcie zorganizovali cvičenie na jej otestovanie, do ktorého sa zapoja všetci príslušní aktéri vrátane súkromného sektora.

c) Spôsobilosti rozlišovania DNS

15. Členské štáty, príslušné subjekty Únie, ako aj súkromné subjekty, napríklad prevádzkovatelia kritickej infraštruktúry, by mali posilniť svoju stratégiu diverzifikácie rozlišovania DNS v rámci systémov názvov domén (DNS) vrátane využívania aspoň jednej infraštruktúry DNS na úrovni Únie, ako je napríklad DNS4EU, aby sa zabezpečilo spoľahlivé rozlišovanie DNS počas závažných kríz. Agentúra ENISA a sieť EU-CyCLONe by mali vypracovať a sprístupniť usmernenia pre núdzový prechod, v ktorých sa uvedú kroky pre prepnutie na infraštruktúru DNS na úrovni Únie v prípade zlyhania iných služieb DNS, čím sa zabezpečí kontinuita kritických služieb počas krízy.

16. Okrem toho by si národné kybernetické centrá a cezhraničné kybernetické centrá mali vymieňať príslušné informácie o hrozbách s takýmito infraštruktúrami DNS na úrovni Únie, aby ich podporili pri poskytovaní vysokej úrovne ochrany pred hrozbami špecifickými pre Úniu, a tým ďalej zvyšovali kapacity na odhaľovanie a zmierňovanie hrozieb špecifických pre Úniu.

17. S cieľom všeobecne posilniť bezpečnosť a dostupnosť kritickej internetovej infraštruktúry, a to aj počas kríz, by členské štáty mali aktívne podporovať účasť všetkých príslušných zainteresovaných strán – vrátane tých, ktoré nie sú priamo uvedené vo vykonávacom akte NIS2 – na poverenom multilaterálnom fóre, ktorého úlohou je identifikovať najlepšie dostupné normy a techniky zavádzania kľúčových opatrení v oblasti bezpečnosti siete. Okrem toho by členské štáty mali zvážiť zapojenie sa do fóra a samy prijať odporúčané usmernenia.

d) Zdroje

18. Členské štáty by mali v plnej miere využívať finančné zdroje, ktoré sú k dispozícii na kybernetickú bezpečnosť v rámci príslušných programov Únie.

III. Odhalenie incidentu, ktorý by mohol prerásť do kybernetickej krízy

19. V záujme riešenia stupňujúcej sa zložitosti kybernetických incidentov a rastúcich výziev pri ich odhaľovaní by verejné aj súkromné subjekty mali vo svojich digitálnych infraštruktúrach zaviesť stratégie odhaľovania na základe informácií o hrozbách, aby sa identifikovali možné predbežné pozície, ktoré môžu byť následne využité na účely narušenia. V prípade identifikácie tajných operácií by sa subjekty mali proaktívne podeliť o príslušné informácie so svojimi partnermi oveľa skôr, ako situácia prerastie do krízy.

20. Všetci aktéri by mali v súlade so svojimi príslušnými mandátmi a na základe prístupu zohľadňujúceho všetky riziká poskytovať príslušným sieťam informácie naznačujúce potenciálnu kybernetickú krízu.

21. Sieť jednotiek CSIRT a sieť EU-CyCLONe by mali stanoviť procesné opatrenia v prípade potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu,

aby sa zabezpečila technicko-operatívna koordinácia a včasné a relevantné informovanie politickej úrovne.

22. Sieť jednotiek CSIRT by mala informovať sieť EU-CyCLONe o tom, či pozorovaný kybernetický incident možno považovať za potenciálny alebo prebiehajúci rozsiahly kybernetický incident.

23. Cezhraničné kybernetické centrá, ktoré už boli zriadené alebo sa majú zriadiť podľa nariadenia (EÚ) 2025/38, by mali prispievať príslušnými informáciami do mechanizmov na úrovni Únie v prípadoch potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu na základe prístupu zohľadňujúceho všetky riziká vrátane fyzického poškodenia kritickej infraštruktúry, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo služieb ponúkaných sieťami a informačnými systémami alebo prístupných prostredníctvom nich.

24. Ak sa zistí potenciálny alebo rozsiahly kybernetický incident s vplyvom na viaceré odvetvia:

a) 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 sieťou EU-CyCLONe;

b) príslušné subjekty Únie by mali podporovať sieť EU-CyCLONe pri posudzovaní dôsledkov pre odvetvia a obyvateľstvo.

IV. Reakcia na kybernetickú krízu na úrovni Únie

25. V prípade kybernetickej krízy stanovenej podľa IPCR by mali všetci aktéri reagovať v úzkej koordinácii s ostatnými subjektmi reagujúcimi na širšie hybridné hrozby v rámci nadrezortného prístupu takto:

a) postihnutý (-é) členský (-é) štát (-y) a sieť jednotiek CSIRT by mali spolupracovať na rýchlom obnovení ohrozených systémov, aby sa zabezpečilo minimálne narušenie prevádzky;

b) sieť EU-CyCLONe by mala v spolupráci so sieťou jednotiek CSIRT poskytnúť politickej úrovni jasné informácie o vplyve, možných dôsledkoch a opatreniach na reakciu a nápravu incidentu, a to aj prostredníctvom príspevku do správy o integrovanej situačnej informovanosti a analýze (ISAA) v rámci dojednaní o IPCR;

c) Komisia by mala v prípade potreby v spolupráci s vysokým predstaviteľom zabezpečiť súdržnosť a koordináciu medzi reakciami na krízu a súvisiacimi opatreniami na úrovni Únie týkajúcimi sa reakcie, najmä príslušnými odvetvovými mechanizmami krízového riadenia na úrovni Únie uvedenými v prílohe 2, a v súvislosti so žiadosťou o pomoc prostredníctvom mechanizmu UCPM;

d) predsedníctvo Rady by malo zvážiť pozvanie predsedu siete EU-CyCLONe na neformálne stretnutia za okrúhlym stolom a iné príslušné zasadnutia Rady v rámci dojednaní o IPCR;

e) Rada by mala s podporou siete EU-CyCLONe a príslušných subjektov Únie koordinovať úsilie v oblasti komunikácie s verejnosťou, a to aj s cieľom zabezpečiť, aby sa krízová situácia nevyužívala na šírenie nepresných informácií;

f) vysoký predstaviteľ by mal v úzkej spolupráci s Komisiou a ďalšími príslušnými subjektmi Únie podporovať rozhodovanie v Rade o využívaní možných opatrení v rámci súboru nástrojov kybernetickej diplomacie, a to aj prostredníctvom analýz a správ. 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 Únie a podporí sa medzinárodný mier, bezpečnosť a stabilita v kybernetickom priestore;

g) Komisia, vysoký predstaviteľ a členské štáty by mali účinnejšie využívať aj ekonomické nástroje, ako sú zákazy obchodovania, aby lepšie predchádzali pretrvávajúcim škodlivým kybernetickým činnostiam štátnych aktérov, odrádzali od nich a reagovali na ne.

26. Ak používateľ služieb poskytovaných rezervou EÚ na účely kybernetickej bezpečnosti[20] požiada o služby rezervy EÚ na účely kybernetickej bezpečnosti v súlade s článkom 15 nariadenia (EÚ) 2025/38 a bez toho, aby boli dotknuté akékoľvek budúce vykonávacie akty podľa uvedeného nariadenia:

a) služby by mali byť nasadené do 24 hodín od podania žiadosti;

b) Komisia a vysoký predstaviteľ by mali zabezpečiť koordináciu s ďalšími opatreniami v súlade so súborom nástrojov EÚ na boj proti hybridným hrozbám[21] v prípade škodlivých kybernetických činností, ktoré sú súčasťou širšej hybridnej kampane;

c) v prípade škodlivej kybernetickej činnosti s vojenským rozmerom by mal žiadajúci členský štát o svojej žiadosti informovať konferenciu veliteľov EÚ v oblasti kybernetickej bezpečnosti Únie.

27. V prípade rozsiahleho kybernetického incidentu, ktorý má vplyv na riadne fungovanie vesmírnych služieb, ktoré sú nevyhnutné pre bezpečnosť Únie alebo jej členských štátov, by sieť EU-CyCLONe mala informovať vysokého predstaviteľa s cieľom koordinovať prípadnú reakciu s architektúrou reakcie na vesmírne hrozby zriadenou v súlade s rozhodnutím Rady (SZBP) 2021/698.

V. Zotavenie z kybernetickej krízy

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

VI. Bezpečná komunikácia

---

[20] Rezerva EÚ na účely kybernetickej bezpečnosti je mechanizmus pozostávajúci zo služieb dôveryhodných poskytovateľov riadených bezpečnostných služieb s cieľom na požiadanie podporiť reakciu a iniciovať opatrenia na zotavenie sa v prípadoch významných kybernetických incidentov, rozsiahlych kybernetických incidentov alebo rozsiahlych rovnocenných kybernetických incidentov, ktoré majú vplyv na členské štáty, inštitúcie, orgány, úrady alebo agentúry Únie alebo tretie krajiny pridružené k programu Digitálna Európa.

[21] Súbor nástrojov EÚ 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.

29. Na základe mapovania existujúcich nástrojov bezpečnej komunikácie[22] by sa Komisia, vysoký predstaviteľ, sieť EU-CyCLONe, sieť jednotiek CSIRT a príslušné subjekty Únie mali do konca roka 2026 dohodnúť na interoperabilnom súbore riešení v oblasti bezpečnej komunikácie pre príslušných aktérov Únie. Tieto riešenia by mali pokrývať celú škálu požadovaných spôsobov komunikácie [hlasová, dátová, videokonferencia (VTC), posielanie správ, spolupráca a výmena dokumentov a konzultácie]. V rámci riešení by sa mali zohľadňovať hlavné zásady, ako sú bezpečnostné záujmy Únie, technologická suverenita a dôvernosť, ako aj prvky, ako sú použiteľnosť, bezpečnosť už v štádiu návrhu, certifikácia európskymi orgánmi pre informačnú bezpečnosť, šifrovanie bez medzifáz, autentifikácia, dostupnosť a postkvantová kryptografia. Riešenia by mali spĺňať spoločne vymedzené požiadavky na ochranu citlivých neutajovaných informácií a mali by obsahovať nástroje na výmenu informácií so stupňom utajenia RESTREINT UE/EU RESTRICTED.

30. Na tomto základe by aktéri na úrovni Únie mali používať riešenia založené na protokole Matrix na komunikáciu v reálnom čase. Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC) zriadené podľa nariadenia (EÚ) 2021/887 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.

31. 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.

32. V strednodobom horizonte by sa mali zriadiť mechanizmy komunikácie a výmeny informácií medzi orgánmi presadzovania práva a sieťami kybernetickej bezpečnosti, najmä na technickej úrovni, aby bolo možné účinne reagovať na krízy. Tieto mechanizmy by mali rešpektovať úlohy jednotlivých strán a nemali by zasahovať do prebiehajúcich operácií. Komisia spolupracuje s členskými štátmi na vytvorení európskeho kritického komunikačného systému (EUCCS), ktorý by mal do roku 2030 prepojiť komunikačné siete orgánov presadzovania práva a civilnej ochrany v celom schengenskom priestore, aby bolo možné používať kritické komunikačné zariadenia na území iných členských štátov. EUCCS preto môže byť prínosom aj pre spoločnú reakciu s príslušnými kybernetickými komunitami. Tento systém by mal zahŕňať záložnú komunikáciu napríklad prostredníctvom satelitnej komunikácie.

VII. Koordinácia kybernetických kríz s vojenskými aktérmi

33. Sieť EU-CyCLONe a konferencia veliteľov EÚ v oblasti kybernetickej bezpečnosti, sieť MICNET a sieť jednotiek CSIRT, ako aj budúce Koordinačné centrum kybernetickej obrany EÚ a jeho civilné protistrany z Únie by mali spolupracovať na rozvoji spoločného situačného povedomia medzi civilnými a vojenskými aktérmi.

34. Únia by sa s prihliadnutím na existujúce dohody, ako je technická dohoda CERT-EU/NATO z roku 2016, mala usilovať o zriadenie kontaktných miest na koordináciu s NATO v prípade kybernetickej krízy s cieľom vymieňať si potrebné informácie o situácii a využívaní mechanizmov reakcie na krízu. Na tento účel by Únia mala preskúmať spôsoby, ako zlepšiť schopnosti výmeny informácií s NATO, a to aj

[22] HWPCI WK 862/23.

prostredníctvom možného prepojenia príslušných komunikačných a informačných systémov.

35. Ak členský štát v súvislosti s kybernetickým incidentom využíva príslušné obranné iniciatívy, ako sú napríklad CRRT PESCO, alebo iné relevantné iniciatívy, ako sú napríklad tímy rýchlej reakcie EÚ na hybridné hrozby (HRRT), mal by o tom informovať sieť EU-CyCLONe, ako aj konferenciu veliteľov EÚ v oblasti kybernetickej bezpečnosti.

VIII. Spolupráca so strategickými partnermi

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

a) v prípade identifikácie relevantného incidentu uľahčiť tok potrebných informácií so strategickými partnermi;

b) posilniť koordináciu so strategickými partnermi pri reakcii na pretrvávajúce škodlivé kybernetické činnosti aktérov pretrvávajúcich hrozieb, najmä pri využívaní súboru nástrojov kybernetickej diplomacie, a to v súlade s jeho vykonávacími usmerneniami.

37. 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 kybernetických incidentov.

38. V rámci rotujúceho cyklu cvičení uvedeného v oddiele II by útvary Komisie a ESVČ mali zvážiť zorganizovanie spoločného cvičenia zamestnancov s cieľom otestovať spoluprácu medzi civilnými a vojenskými zložkami v prípade rozsiahleho kybernetického incidentu, ktorý by postihol členské štáty Únie a spojencov NATO, vrátane prípadov, keď sa aktivovali alebo by sa pravdepodobne mohli aktivovať články 4 alebo 5 Zmluvy o NATO.

39. Vzhľadom na expozíciu kandidátskych krajín a možnosť kybernetických incidentov v susedstve Únie by sa mali zvážiť spoločné cvičenia s účasťou kandidátskych krajín.

V Bruseli

Za Radu

predseda/predsedníčka