Rada
Evropské unie

Brusel 6. června 2025
(OR. en)

9794/25

Interinstitucionální spis:
2025/0036 (NLE)

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

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	6. června 2025
Příjemce:	Delegace
Předmět:	Doporučení Rady o plánu EU pro řešení kybernetických bezpečnostních krizí – doporučení Rady schválené Radou na zasedání dne 6. června 2025

Delegace naleznou v příloze doporučení Rady ve znění, které schválila Rada na svém zasedání konaném dne 6. června 2025.

PŘÍLOHA

DOPORUČENÍ RADY

o plánu EU pro řešení kybernetických bezpečnostních krizí

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na články 114 a 292 této smlouvy,

s ohledem na návrh Evropské komise,

vzhledem k těmto důvodům:

(1) Digitální technologie a globální konektivita jsou základem hospodářského růstu Unie, její konkurenceschopnosti a transformace kritické infrastruktury. Propojená a stále více digitální ekonomika však také zvyšuje riziko kybernetických bezpečnostních incidentů a útoků. Rostoucí geopolitické napětí, konflikty a strategické soupeření se navíc odrážejí v dopadu, objemu a sofistikovanosti nepřátelských kybernetických činností. Tyto činnosti mohou být součástí hybridních kampaní nebo vojenských operací. Mohou také přímo ovlivnit bezpečnost, hospodářství a společnost Unie. Kromě toho mají potenciál vedlejšího efektu, zejména pokud jsou tyto činnosti zaměřeny na země, které jsou mezinárodními strategickými partnery, například kandidátské nebo sousední země.

(2) Rozsáhlý kybernetický bezpečnostní incident může způsobit úroveň narušení, jež přesahuje schopnost členského státu na takový incident reagovat nebo má významný dopad na více než jeden členský stát. Takový incident by mohl v závislosti na své příčině a dopadu eskalovat a přejít ve skutečnou krizi, jež ovlivní řádné fungování vnitřního trhu nebo bude představovat vážná rizika pro veřejnou bezpečnost a ochranu subjektů nebo občanů v několika členských státech nebo v Unii jako celku. Pro zachování hospodářské stability a ochranu evropských vlád, kritické infrastruktury, podniků a občanů je zásadní účinné řešení krizí, jež zároveň přispívá k mezinárodní bezpečnosti a stabilitě v kyberprostoru. Řešení kybernetických krizí je proto nedílnou součástí celkového rámce EU pro řešení krizí.

(3) Vzhledem k vzájemné závislosti a propojení mezi prostředím IKT subjektů Unie a členských států by incident v rámci subjektu Unie mohl představovat kybernetické bezpečnostní riziko pro členské státy a naopak. Sdílení relevantních informací a koordinace v souvislosti s rozsáhlými kybernetickými bezpečnostními incidenty i závažnými incidenty, jak jsou definovány v čl. 3 odst. 8 nařízení (EU, Euratom) 2023/2841[1], má v kontextu plánu EU pro řešení kybernetických krizí (dále jen „kybernetický plán“) zásadní význam.

[1] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. prosince 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie, Úř. věst. L, 2023/2841, 18.12.2023, s. 1.

(4) V případě krize, v souvislosti s níž byla aktivována integrovaná politická reakce EU na krize (IPCR) podle prováděcího rozhodnutí Rady (EU)[2] 2018/1993 (dále jen „opatření IPCR“), by měl kybernetický plán plně respektovat opatření IPCR pro koordinaci a reakci. Politická a strategická koordinace by probíhala v rámci IPCR. Opatření IPCR jsou nástrojem pro horizontální koordinaci a reakci na politické úrovni Unie. V souladu s opatřeními IPCR přijímá rozhodnutí o aktivaci nebo deaktivaci IPCR předsednictví Rady Evropské unie. Zprávy o integrovaném situačním povědomí a analýze (ISAA) vypracované útvary Komise a Evropskou službou pro vnější činnost (dále jen „ESVČ“) jsou podporou činnosti v rámci IPCR jak v režimu sdílení informací, tak v režimu plné aktivace.

(5) Hlavní odpovědnost za řešení kybernetických bezpečnostních incidentů a kybernetických krizí nesou členské státy. Potenciální přeshraniční a meziodvětvová povaha kybernetických bezpečnostních incidentů však vyžaduje, aby členské státy a příslušné subjekty Unie spolupracovaly na technické, operační a politické úrovni s cílem účinně koordinovat činnost v celé Unii. Celý životní cyklus řešení kybernetických krizí zahrnuje připravenost a společné situační povědomí s cílem předvídat rozsáhlé kybernetické bezpečnostní incidenty, nezbytné schopnosti v oblasti odhalování s cílem určit potřebné nástroje pro reakci a zotavení, jejichž účelem je zmírňovat rozsáhlé kybernetické bezpečnostní incidenty a zamezit jejich šíření, jakož i schopnosti reakce pro odrazování od dalších incidentů a zabránění jejich vzniku.

[2] Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize, Úř. věst. L 320, 17.12.2018, s. 28.

(6) Doporučení Komise (EU) 2017/1584[3] o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize stanoví cíle a způsoby spolupráce mezi členskými státy a subjekty Unie při reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize. Zmapovalo příslušné aktéry na technické, operační a politické úrovni a vysvětlilo, jak jsou začleněni do stávajících mechanismů Unie pro řešení krizí, jako jsou opatření IPCR EU. Základní zásady stanovené v doporučení (EU) 2017/1584 zůstávají v platnosti, a to subsidiarita, komplementarita a důvěrnost informací, jakož i tříúrovňový přístup (v technické, operační a politické rovině). Toto doporučení, jímž se stanoví nový rámec Unie pro řešení kybernetických bezpečnostních krizí, vychází z uvedených základních zásad a jeho cílem je nahradit doporučení (EU) 2017/1584.

(7) Některé definice použité v tomto doporučení vycházejí z definic a pojmů použitých ve směrnici (EU) 2022/2555[4]. Oblast působnosti tohoto doporučení se však od oblasti působnosti směrnice (EU) 2022/2555 liší. V tomto doporučení se stanoví rámec Unie pro řešení kybernetických krizí v kontextu celkové připravenosti EU na rozsáhlé kybernetické bezpečnostní incidenty a kybernetické krize vyplývající z těchto incidentů – bez ohledu na to, které odvětví nebo subjekt jsou zasaženy. Definice v co největší možné míře vycházejí z definic uvedených ve směrnici (EU) 2022/2555.

---

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

[4] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), Úř. věst. L 333, 27.12.2022, s. 80.

(8) Aktualizovaný plán kybernetické bezpečnosti je nezbytný k poskytnutí jasných a přístupných pokynů vysvětlujících, co je rozsáhlý kybernetický bezpečnostní incident nebo kybernetická krize na úrovni Unie, jak se spouští rámec pro řešení krizí a jaké jsou úlohy příslušných sítí, aktérů a mechanismů na úrovni Unie a interakce mezi těmito aktéry a mechanismy v průběhu celého životního cyklu kybernetické krize. Cílem kybernetického plánu je podpořit širší rámec civilně-vojenských vztahů EU v kontextu řešení kybernetických krizí, a to i v souvislosti s prohlubováním vztahů mezi EU a NATO, pokud možno i prostřednictvím inkluzivních, recipročních a nediskriminačních posílených mechanismů sdílení informací při řešení kybernetických krizí.

(9) Mělo by být posíleno meziodvětvové řešení krizí na úrovni Unie, aby umožňovalo integrovanou reakci na krize, zejména v případech, kdy mají rozsáhlé kybernetické incidenty a krize fyzické dopady. Toto doporučení doplňuje opatření IPCR a další mechanismy Unie pro řešení krizí, včetně všeobecného systému rychlého varování Komise ARGUS, mechanismu civilní ochrany Unie (UCPM) podporovaného Střediskem pro koordinaci odezvy na mimořádné události (dále jen „ERCC“) zřízeným v rámci mechanismu civilní ochrany Unie rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU o mechanismu civilní ochrany Unie[5] (dále jen „rozhodnutí o UCPM“), mechanismu ESVČ pro reakci na krize (dále jen „CRM“), jakož i dalších procesů, jako jsou procesy popsané v souboru nástrojů EU pro diplomacii v oblasti kybernetiky[6], v souboru hybridních nástrojů[7] a v revidovaném protokolu EU pro boj proti hybridním hrozbám[8]. Doplňuje rovněž doporučení Rady (EU) 2024/4371 o plánu pro koordinaci reakce na úrovni Unie na narušení kritické infrastruktury se značným přeshraničním významem[9] (dále jen „plán EU pro kritickou infrastrukturu“), který se týká jiné než kybernetické (tedy fyzické) odolnosti a jehož cílem je zlepšit koordinaci reakce na úrovni Unie v této oblasti, a měl by s ním být v souladu.

---

5 Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

6 Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru (9916/17).

7 Závěry Rady o rámci pro koordinovanou reakci EU na hybridní kampaně, 22. června 2022.

8 Společný pracovní dokument útvarů Komise – Protokol EU pro boj proti hybridním hrozbám (SWD(2023)116 final).

9 Úř. věst. C, C/2024/4371, 5.7.2024.

(10) Evropská síť styčných organizací pro řešení kybernetických krizí (dále jen „EU-CyCLONe“) je síť pro koordinaci řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni, a to i v případě meziodvětvových rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí. Aby se dále nekomplikovaly stávající rámce, mělo by se zabránit vytváření odvětvových struktur, kterými by se zdvojovaly úkoly sítě EU-CyCLONe. Síť EU-CyCLONe by měla získávat operativní informace související s kybernetickou bezpečností i od odvětví a poskytovat vstupy na politické úrovni.

(11) Členské státy se vyzývají, aby plně využívaly finanční zdroje, které jsou pro kybernetickou bezpečnost k dispozici v rámci příslušných programů Unie. Je třeba zajistit, aby tyto programy představovaly pro žadatele o financování minimální administrativní zátěž a aby se usnadnila účast členských států v těchto programech poskytnutím příslušných pokynů ohledně reálných možností finanční podpory.

(12) Toto doporučení přispívá k širším opatřením v oblasti připravenosti, jež jsou od Unie vyžadována v případě meziodvětvových krizí v souladu se zásadami zakotvenými ve Strategii EU pro unii připravenosti, konkrétně k integrovanému přístupu zohledňujícímu veškerá rizika, všechny úrovně správy a celou společnost, zejména pokud jde o zvyšování povědomí o rizicích a hrozbách a meziodvětvovou reakci na krize.

PŘIJALA TOTO DOPORUČENÍ:

I: Cíl, oblast působnosti a hlavní zásady rámce EU pro řešení kybernetických krizí

Cíl a oblast působnosti

1) V tomto doporučení o plánu EU pro řešení kybernetických krizí (dále jen „kybernetický plán“) se stanoví rámec Unie pro řešení kybernetických krizí v kontextu celkové připravenosti EU na rozsáhlé kybernetické bezpečnostní incidenty a kybernetické krize. Rámec odráží úlohu členských států i orgánů, institucí a jiných subjektů Unie (dále jen „subjekty Unie“) podle jejich příslušných pravomocí, při plném dodržování vnitrostátních právních předpisů a vnitřních pravidel, s cílem zajistit komplexní a koordinovanou činnost na úrovni Unie.

2) Kybernetický plán by měl být používán v soudržnosti s plánem EU pro kritickou infrastrukturu, zejména v případě incidentů ovlivňujících jak fyzickou odolnost, tak i kybernetickou bezpečnost kritické infrastruktury[10].

3) Kybernetický plán poskytuje pokyny pro reakci na rozsáhlé kybernetické bezpečnostní incidenty nebo kybernetické krize a měl by být používán jako doplněk k případným relevantním odvětvovým mechanismům reakce, jako jsou mechanismy uvedené v příloze II. Příslušné zúčastněné strany v oblasti kybernetické bezpečnosti by měly pomáhat a asistovat při dosahování cílů těchto odvětvových mechanismů, a to jak na vnitrostátní úrovni, tak na unijní úrovni.

4) V případě celounijní meziodvětvové krize s kybernetickými aspekty, v souvislostí s níž je aktivována IPCR, by měla koordinaci reakce na politické úrovni Unie provádět Rada, a to s využitím opatření IPCR. V případě aktivace IPCR by měla opatření v rámci kybernetického plánu podporovat reakci EU na politické úrovni a poskytovat konkrétní podporu v oblasti kybernetické bezpečnosti.

[10] Plán EU pro kritickou infrastrukturu dále upřesňuje koordinaci pro takové případy v oddíle 4 části I své přílohy.

Hlavní zásady

5) Při řešení kybernetických krizí na úrovni Unie se uplatňují tyto hlavní zásady:

a) *Proporcionalita:* Většina kybernetických bezpečnostních incidentů postihujících členské státy nedosahuje úrovně, která by mohla být považována za rozsáhlý vnitrostátní nebo unijní kybernetický bezpečnostní incident nebo kybernetickou krizi. V případě kybernetických bezpečnostních incidentů a hrozeb členské státy dobrovolně spolupracují a vyměňují si informace, a to pravidelně v rámci sítě týmů pro reakci na počítačové bezpečnostní incidenty (dále jen „síť CSIRT“) a sítě EU-CyCLONe v souladu se standardními operačními postupy těchto sítí.

b) *Subsidiarita:* Členské státy jsou primárně odpovědné za reakci a nápravu v případě kybernetického bezpečnostního incidentu, rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize, které na ně mají dopad. S ohledem na potenciální přeshraniční dopady by Rada, Komise, vysoký představitel, Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“), Služba kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie (dále jen „CERT-EU“), Europol a všechny další příslušné subjekty Unie měly spolupracovat během celého životního cyklu krize. Tato úloha vyplývá z práva Unie a odráží dopad rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí na jedno nebo více odvětví hospodářské činnosti na jednotném trhu, bezpečnostní a mezinárodní vztahy Unie i na samotné subjekty Unie.

c) *Doplňkovost:* Toto doporučení plně zohledňuje stávající mechanismy řešení krizí na úrovni Unie uvedené v příloze II, zejména opatření IPCR EU, systém ARGUS a mechanismus ESVČ pro reakci na krize. V tomto doporučení jsou zohledněny mandáty sítě CSIRT a sítě EU-CyCLONe, jakož i nařízení (EU, Euratom) 2023/2841. V případě aktivace IPCR by měla práce příslušných sítí, subjektů a aktivovaných odvětvových mechanismů pokračovat a měla by poskytovat vstupy pro politickou a strategickou koordinaci probíhající v rámci IPCR a podporovat ji.

d) *Důvěrnost informací*: Veškerá výměna informací v kontextu tohoto doporučení by se měla řídit příslušnými bezpečnostními pravidly a pravidly ochrany osobních údajů. Ve vhodných případech by měly být zohledněny neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol) pro označování citlivých informací. Pro výměnu utajovaných informací by bez ohledu na použitý systém utajení měla být vedle dostupných akreditovaných nástrojů používána stávající závazná pravidla a dohody o zpracování utajovaných informací.

6) V souladu s výše uvedenými hlavními zásadami by členské státy a subjekty Unie měly prohloubit spolupráci v oblasti řešení kybernetických krizí, posilovat vzájemnou důvěru a vycházet ze stávajících sítí a mechanismů. Tato spolupráce v rámci kybernetického plánu těží z provádění článků 22 a 23 nařízení (EU, Euratom) 2023/2841. Zejména plán řešení kybernetických krizí vypracovaný na základě článku 23 nařízení (EU, Euratom) 2023/2841 mimo jiné přispívá k pravidelné výměně relevantních informací mezi subjekty Unie a s členskými státy a vymezuje ujednání týkající se koordinace a toku informací mezi subjekty Unie.

II: Definice

7) Pro účely tohoto kybernetického plánu se rozumí:

a) „incidentem“ událost narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné;

b) „významným incidentem“ incident, který:

   a. dotčenému subjektu způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty;

   b. způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značnou hmotnou nebo nehmotnou újmu;

c) „rozsáhlým kybernetickým bezpečnostním incidentem“ incident, který způsobí úroveň narušení, jež přesahuje schopnost členského státu na takový incident reagovat, nebo který má významný dopad na nejméně dva členské státy;

d) „kybernetickou krizí“ rozsáhlý kybernetický bezpečnostní incident, který eskaloval do skutečné krize, jež neumožňuje řádné fungování vnitřního trhu nebo představuje vážná rizika pro veřejnou bezpečnost a ochranu subjektů nebo občanů v několika členských státech nebo v Unii jako celku.

III: Vnitrostátní struktury a povinnosti pro řešení kybernetických krizí

8) Členské státy jsou primárně odpovědné za reakci v případě rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize, které na ně mají dopad. Každý členský stát má v souladu se směrnicí (EU) 2022/2555 jeden nebo více orgánů pro řešení kybernetických krizí a jeden nebo více týmů CSIRT.

9) Přijetím směrnice (EU) 2022/2555 a dalších legislativních a nelegislativních nástrojů v oblasti kybernetické bezpečnosti členské státy harmonizují své rámce kybernetické bezpečnosti stanovením minimálních pravidel týkajících se fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce mezi odpovědnými orgány v každém členském státě a stanovením účinných nápravných a donucovacích opatření, která jsou klíčová pro účinné prosazování těchto povinností.

10) V souladu s čl. 9 odst. 4 směrnice (EU) 2022/2555 by členské státy měly přijmout vnitrostátní plány reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize. Tyto plány zahrnují mimo jiné vnitrostátní opatření v oblasti připravenosti, postupy pro řešení kybernetických krizí a vnitrostátní postupy a ujednání mezi vnitrostátními orgány a subjekty pro zajištění jejich účinné účasti na koordinovaném řešení rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí na úrovni Unie a podpory tohoto řešení. Postupy řešení kybernetických krizí zahrnují rovněž ustanovení o jejich začlenění do rámce pro obecné vnitrostátní krizové řízení a kanály pro výměnu informací.

11) V souladu s čl. 9 odst. 1 směrnice (EU) 2022/2555 by členské státy měly zajistit soudržnost se stávajícími rámci pro obecné vnitrostátní krizové řízení. V případě aktivace IPCR by vnitrostátní orgány pro řešení krizí měly za účelem poskytování informací IPCR shromažďovat vstupy od orgánů pro řešení kybernetických krizí a z vnitrostátních odvětvových krizových mechanismů.

12) V souladu s čl. 9 odst. 5 směrnice (EU) 2022/2555 by si síť EU-CyCLONe měla na žádost dotčeného členského státu vyměňovat informace o příslušných částech vnitrostátních plánů reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, zejména o ustanoveních pro zajištění účinné účasti na koordinovaném řešení rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí na úrovni Unie a podpory tohoto řešení, s cílem vyměňovat si osvědčené postupy a posoudit, zda by v praxi fungoval celkový rámec.

13) Síť EU-CyCLONe a Interinstitucionální výbor pro kybernetickou bezpečnost (IICB) se vyzývají, aby si ve vhodných případech vyměňovaly informace o soudržnosti plánu pro řešení krizí vypracovaného výborem IICB v souladu s článkem 23 nařízení (EU, Euratom) 2023/2841 s vnitrostátními plány reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize.

14) Síť EU-CyCLONe by měla s podporou agentury ENISA jakožto svého sekretariátu vést aktualizovaný seznam vnitrostátních orgánů pro řešení kybernetických krizí s kontaktními údaji úředníků a vedoucích pracovníků sítě EU-CyCLONe a zpřístupnit ho členům sítě EU-CyCLONe.

IV: Hlavní sítě a aktéři v ekosystému EU pro řešení kybernetických krizí

15) Síť CSIRT je hlavní technickou sítí pro výměnu relevantních informací o incidentech, zejména v oblasti působnosti tohoto doporučení, v souladu s příslušnými úkoly popsanými v čl. 15 odst. 3 směrnice (EU) 2022/2555. Přispívá k budování důvěry a podporuje rychlou a účinnou operační spolupráci mezi členskými státy. Předseda sítě CSIRT se může účastnit činnosti výboru IICB jako pozorovatel.

16) CERT-EU je službou kybernetické bezpečnosti pro všechny subjekty Unie. Funguje jako centrum pro výměnu informací a koordinaci reakce na incidenty v oblasti kybernetické bezpečnosti pro subjekty Unie v souladu s článkem 13 nařízení (EU) 2023/2841. CERT-EU je členem sítě CSIRT a poskytuje podporu Komisi v síti EU-CyCLONe. Působí na technické úrovni a odpovídá za koordinaci řešení závažných incidentů s dopadem na subjekty Unie.

17) Síť EU-CyCLONe působí jako zprostředkovatel mezi technickou a politickou úrovní, a to zejména během rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí. V souladu s článkem 16 směrnice (EU) 2022/2555 podporuje koordinované řešení rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí na operativní úrovni a zajišťuje pravidelnou výměnu relevantních informací mezi členskými státy a orgány, institucemi a jinými subjekty Unie. Předseda sítě EU-CyCLONe se může účastnit činnosti výboru IICB jako pozorovatel.

18) ENISA je agentura Unie, která plní úkoly svěřené nařízením (EU) 2019/881[11] **za** účelem dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Unii, mimo jiné aktivní podporou členských států a orgánů, institucí a jiných subjektů Unie. Agentura ENISA mimo jiné zajišťuje sekretariát pro síť CSIRT a síť EU-CyCLONe, služby získávání poznatků o situaci a pomáhá členským státům tím, že pravidelně pořádá cvičení v oblasti kybernetické bezpečnosti na úrovni Unie. V souladu se směrnicí (EU) 2022/2555 a nařízením (EU) 2024/2847[12] agentura ENISA dostává informace o významných přeshraničních incidentech a aktivně využívaných zranitelných místech a incidentech s dopadem na digitální produkty.

19) Rada Evropské unie (dále jen „Rada“) je orgánem vykonávajícím funkce vymezování politik a koordinace v souladu s článkem 16 Smlouvy o Evropské unii (dále jen „Smlouva o EU“) a jsou jí svěřena opatření IPCR, která se týkají koordinace a reakce na úrovni Unie. Rada působí prostřednictvím složení Rady, Výboru stálých zástupců a příslušných přípravných orgánů Rady, zejména Horizontální pracovní skupiny pro otázky týkající se kybernetiky, jakož i v relevantních případech opatření IPCR.

---

[11] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (akt o kybernetické bezpečnosti), Úř. věst. L 151, 7.6.2019, s. 15.

[12] Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti), Úř. věst. L, 2024/2847, 20.11.2024. s. 1.

20) Komise jako orgán, který prosazuje obecný zájem Unie a za tímto účelem přijímá vhodné iniciativy, jakož i zajišťuje uplatňování Smluv a opatření přijatých orgány podle článku 17 Smlouvy o EU, je v souladu s rozhodnutím o mechanismu civilní ochrany Unie odpovědná za určitou obecnou připravenost na úrovni Unie a určitá opatření v oblasti situačního povědomí, včetně řízení střediska ERCC a společného komunikačního a informačního systému pro mimořádné události (dále jen „CECIS“). Na operativní úrovni usnadňuje soudržnost a koordinaci mezi souvisejícími opatřeními reakce na krize na úrovni Unie. Je konzultována ohledně rozhodnutí o aktivaci nebo deaktivaci opatření IPCR EU. Útvary Komise spolu s ESVČ vypracovávají zprávy v oblasti integrovaného situačního povědomí a analýzy (ISAA). Komise je členem sítě EU-CyCLONe v případech, kdy potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident má nebo pravděpodobně bude mít významný dopad na služby a činnosti spadající do oblasti působnosti směrnice (EU) 2022/2555; v ostatních případech je pozorovatelem. Je kontaktním místem v rámci výboru IICB pro síť EU-CyCLONe. Je pozorovatelem v rámci sítě CSIRT.

21) Vysoký představitel pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“), kterému je nápomocna ESVČ, provádí společnou zahraniční a bezpečnostní politiku Unie (dále jen „SZBP“) a svými návrhy přispívá k rozvoji této politiky včetně společné bezpečnostní a obranné politiky (dále jen „SBOP“). Patří sem diplomatické, zpravodajské a vojenské struktury a mechanismy, zejména společná zpravodajsko-analytická složka (SIAC) jako jednotné kontaktní místo pro zpravodajské služby členských států, Vojenský štáb EU (EUMS) jako zdroj vojenských odborných znalostí, soubor nástrojů EU pro diplomacii v oblasti kybernetiky, jakož i síť delegací EU, které mohou přispívat k řešení krizí z vnějšího rozměru. ESVČ rovněž spolu s Komisí vypracovává zprávy ISAA.

22) V příloze II jsou popsány úlohy a pravomoci příslušných aktérů na úrovni Unie v souvislosti s řešením kybernetických krizí, včetně hlavních sítí a aktérů.

V: Příprava na rozsáhlé kybernetické bezpečnostní incidenty a kybernetickou krizi

Prostředí hrozeb

23) Členské státy a příslušné subjekty Unie by měly přijmout nezbytná opatření ke zlepšení situačního povědomí, přičemž je třeba zohlednit, že prostředí hrozeb a situační povědomí v případě konkrétních incidentů si vyžadují odlišné způsoby fungování. Členské státy a příslušné subjekty Unie by měly spolupracovat na základě ověřených a spolehlivých údajů, týkajících se mimo jiné trendů, pokud jde o incidenty, taktiky, techniky a postupy a aktivně využívaná zranitelná místa.

24) Při sdílení informací na úrovni EU by členské státy měly plně využívat stávající platformy pro technickou a operativní spolupráci, jako jsou platformy používané sítí CSIRT a sítí EU-CyCLONe.

25) S cílem zlepšit společné situační povědomí a usnadnit posuzování dopadu na EU by síť EU-CyCLONe a síť CSIRT s podporou agentury ENISA měly využívat interně dohodnutý mechanismus podávání zpráv za účelem vytvoření přehledu EU o technických a operativních činnostech na základě informací shromážděných na vnitrostátní úrovni.

26) Síť EU-CyCLONe a síť CSIRT by měly:

a) spolupracovat na zlepšení sdílení informací mezi technickou a operační úrovní a na zlepšení situačního povědomí jako celku;

b) pokračovat v budování atmosféry důvěry mezi svými členy a mezi sítěmi;

c) plně využívat dostupné nástroje pro sdílení informací, a to s podporou agentury ENISA, zamyslet se nad tím, jak tyto nástroje zlepšit a zajistit interoperabilitu mezi sítěmi.

27) Síť EU-CyCLONe, síť CSIRT a výbor IICB by měly spolupracovat s cílem zajistit účinnou výměnu relevantních informací.

28) Agentura ENISA jako sekretariát sítě CSIRT a sítě EU-CyCLONe hraje ústřední úlohu při podpoře členských států a orgánů, institucí a jiných subjektů Unie při dosahování společného situačního povědomí EU na technické a operační úrovni s cílem podpořit přípravu na rozsáhlé kybernetické bezpečnostní incidenty a krize.

29) V souladu se směrnicí (EU) 2022/2555 a nařízením (EU) 2019/881 by členské státy a příslušné subjekty Unie měly koordinovat svou činnost se soukromým sektorem, včetně komunit uživatelů softwaru s otevřeným zdrojovým kódem a jeho výrobců, s cílem zlepšit sdílení informací. Agentura ENISA by v tomto ohledu měla využít zejména svůj program partnerství. Kromě toho by členské státy a příslušné subjekty Unie mohly rovněž navázat na stávající střediska pro sdílení a analýzu informací (dále jen „střediska ISAC“) na úrovni EU a na vnitrostátní úrovni za účelem zvýšení kapacity v oblasti kybernetické bezpečnosti a zlepšení reakce na kybernetické bezpečnostní incidenty, mimo jiné prostřednictvím společných setkání soukromého sektoru se sítí EU-CyCLONe nebo sítí CSIRT.

30) S cílem zlepšit sdílení informací v rámci sítí a mezi nimi a vyjasnit vzájemná očekávání ohledně tohoto sdílení by se síť EU-CyCLONe měla s podporou agentury ENISA jako sekretariátu a po konzultaci se sítí CSIRT a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací do 24 měsíců od přijetí tohoto doporučení dohodnout na společné sladěné taxonomii úrovní závažnosti incidentů. Tato taxonomie by měla umožnit srovnávání závažnosti incidentů napříč členskými státy prostřednictvím posouzení dopadu na poskytování služeb, počtu dotčených subjektů a jejich příslušného významu, dopadu na jiné služby a infrastrukturu, jakož i způsobené peněžní, reputační a politické újmy. Měla by vycházet z příslušných stávajících stupnic nebo taxonomií, jako je referenční taxonomie pro klasifikaci incidentů.

Technická úroveň

31) Síť CSIRT je platformou pro technickou spolupráci a sdílení informací mezi všemi členskými státy a prostřednictvím CERT-EU se subjekty Unie.

32) V souladu se směrnicí (EU) 2022/2555 má každý tým CSIRT za úkol monitorovat a analyzovat kybernetické hrozby, zranitelná místa a incidenty na vnitrostátní úrovni. Týmy CSIRT by si měly v rámci sítě CSIRT i na dvoustranné úrovni vyměňovat relevantní informace o incidentech, významných událostech, kybernetických hrozbách, rizicích a zranitelných místech s cílem dosáhnout společného situačního povědomí.

33) Za účelem posílení operativní spolupráce na úrovni Unie by síť CSIRT měla zvážit přizvání institucí a agentur Unie zapojených do politiky kybernetické bezpečnosti, jako je Europol, k účasti na své činnosti.

34) V souladu s nařízením 2023/2841 by měla služba CERT-EU shromažďovat, spravovat a analyzovat informace o kybernetických hrozbách, zranitelných místech a incidentech v neutajované infrastruktuře IKT a sdílet tyto informace s orgány, institucemi a jinými subjekty Unie a v případě potřeby vydávat výboru IICB konkrétní návrhy pokynů a doporučení pro orgány, instituce a jiné subjekty Unie. Služba CERT-EU by měla spolupracovat a vyměňovat si informace s protějšky z členských států, a to i prostřednictvím sítě CSIRT.

Operační úroveň

35) Síť EU-CyCLONe by měla v souladu se směrnicí (EU) 2022/2555 sloužit jako platforma pro spolupráci mezi orgány členských států pro řešení kybernetických krizí a prostřednictvím Komise s příslušnými subjekty Unie, s cílem zvýšit úroveň připravenosti na řešení rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí a rozvíjet společné situační povědomí o rozsáhlých kybernetických bezpečnostních incidentech a kybernetických krizích.

36) V souladu se směrnicí (EU) 2022/2555 a nařízením (EU) 2024/2847 agentura ENISA dostává informace o významných přeshraničních incidentech a aktivně využívaných zranitelných místech a incidentech s dopadem na digitální produkty. Agentura ENISA jednající jako sekretariát by měla poskytovat poradenství síti CSIRT a síti EU-CyCLONe, s cílem podpořit tyto sítě při rozhodování, zda je třeba přijmout další opatření, a přispět ke společnému situačnímu povědomí.

Politická úroveň

37) Členské státy a příslušné subjekty Unie by měly sledovat mezinárodní vývoj, který ovlivňuje kybernetickou bezpečnost (včetně kybernetických hrozeb, hybridních hrozeb a zahraniční manipulace s informacemi a vměšování, případně se zahrnutím dezinformací). Měly by být zohledňovány iniciativy, jako jsou společné zprávy o posouzení kybernetické bezpečnosti (JCAR), analýzy ze strany SIAC a další relevantní produkty poskytující odborné poznatky.

38) Vysoký představitel by měl i nadále informovat členské státy a zapojovat je do diplomatického úsilí Unie týkajícího se kybernetických hrozeb, zejména těch, jež zahrnují státní aktéry, do její spolupráce se třetími zeměmi a mezinárodními organizacemi včetně NATO a do provádění diplomatických opatření včetně omezujících opatření.

39) Předsednictví Rady Evropské unie může na internetové platformě IPCR spustit monitorovací stránku, na níž si členské státy a orgány a instituce EU budou moci vyměňovat informace o potenciálně se vyvíjející krizi.

Společná cvičení

40) Komise by měla v koordinaci s vysokým představitelem s podporou agentury ENISA a po konzultaci se sítí EU-CyCLONe a sítí CSIRT sestavit účinný roční průběžný program kybernetických cvičení s cílem připravit se na kybernetické krize a zvýšit organizační efektivitu. Průběžný program kybernetických cvičení by měl zohledňovat cvičení mechanismu civilní ochrany Unie a cvičení dalších mechanismů pro reakci na krize na úrovni Unie, včetně cvičení uvedeného v plánu EU pro kritickou infrastrukturu. První průběžný program by měl být vypracován do 12 měsíců od přijetí kybernetického plánu, přičemž následné programy by měly být dokončeny každý rok do 31. března. Průběžný program by měl být předložen Radě pro informaci.

41) Průběžný program by měl zahrnovat i cvičení vypracovaná na základě scénářů koordinovaného posuzování rizik na úrovni EU. Měl by zahrnovat cvičení se zapojením všech příslušných aktérů, zejména soukromého sektoru a NATO.

42) Agentura ENISA by z pozice sekretariátu sítě CSIRT a sítě EU-CyCLONe měla zajistit systematické shromažďování poznatků získaných z cvičení, jakož i určování a navrhování způsobů provádění výsledných opatření, s cílem zaručit jejich účinné uskutečnění a pozitivní dopad na společnou odolnost EU, a to včetně příslušných standardních operačních postupů.

43) Všichni aktéři a sítě by měli na základě zkušeností získaných ze cvičení zlepšit koordinaci pro případ rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize. Zejména síť EU-CyCLONe a síť CSIRT by se měly v zájmu zlepšení koordinace zabývat výzvami zjištěnými během cvičení, a to zejména pokud jde o spolupráci mezi sítěmi, a v případě potřeby urychleně přizpůsobit standardní operační postupy.

44) Skupina pro spolupráci v oblasti bezpečnosti sítí a informací by měla vyzvat síť CSIRT, síť EU-CyCLONe a agenturu ENISA, aby prezentovaly poznatky získané ze cvičení, jakož i určení a navrhovaný způsob provádění výsledných opatření.

45) Rada může vyzvat předsedy sítě CSIRT, sítě EU-CyCLONe, skupiny pro spolupráci v oblasti bezpečnosti sítí a informací a agentury ENISA, aby prezentovali, jak byly poznatky získané ze cvičení provedeny.

46) Agentura ENISA se vyzývá, aby ve spolupráci s Komisí a vysokou představitelkou uspořádala během příštího cvičení Cyber Europe cvičení zaměřené na otestování kybernetického plánu. Do cvičení by se měli zapojit všichni příslušní aktéři, včetně politické úrovně. Agentura ENISA se vyzývá, aby zapojení politické úrovně koordinovala s předsednictvím Rady Evropské unie. Cvičení může zahrnovat i soukromý sektor a NATO.

VI: Odhalení incidentu, který by mohl eskalovat v rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi

47) Všichni aktéři by měli v souladu se svými mandáty a na základě přístupu zohledňujícího veškerá rizika poskytovat příslušným sítím informace o potenciálním rozsáhlém kybernetickém bezpečnostním incidentu nebo kybernetické krizi.

48) Pokud přeshraniční kybernetická centra získají informace ohledně potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, měly by v souladu s nařízením (EU) 2025/38[13] zajistit pro účely získání společného situačního povědomí, aby byly orgánům členských států a Komisi prostřednictvím sítě EU-CyCLONe a sítě CSIRT neprodleně poskytnuty relevantní informace.

[13] Nařízení Evropského parlamentu a Rady (EU) 2025/38 ze dne 19. prosince 2024, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě), Úř. věst. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) Je-li zaznamenán významný incident, a to zejména incident s okamžitým dopadem, může být oznámen týmu CSIRT nebo může být týmem CSIRT, jakož i orgány členských států pro řešení kybernetických krizí nebo jinými odvětvovými orgány odhalen. Členské státy se vyzývají, aby informace ohledně takového incidentu sdílely v rámci sítí, které by měly zvážit přijetí vhodných opatření. Síť CSIRT a síť EU-CyCLONe mohou být aktivovány nezávisle na sobě podle povahy incidentu a požadované reakce. Obě sítě se však vyzývají, aby nadále vzájemně spolupracovaly na základě dohodnutých procesních ujednání. Rozhodnutí o aktivaci závisí výhradně a nezávisle na každé síti.

50) Síť CSIRT by měla síť EU-CyCLONe informovat o tom, zda lze pozorovaný kybernetický bezpečnostní incident považovat za potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident.

51) Jak se uvádí ve směrnici (EU) 2022/2555, měly by síť CSIRT a síť EU-CyCLONe stanovit procesní opatření pro případ potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, aby byla zajištěna technicko-operační koordinace a včasné a relevantní informování politické úrovně.

VII: Reakce na rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi na úrovni Unie

Reakce na rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi, u nichž nebyla aktivována IPCR v režimu plné aktivace

52) Účinná reakce na rozsáhlé kybernetické bezpečnostní incidenty nebo kybernetické krize na úrovni EU závisí na účinné technické, operativní a politické spolupráci v rámci přístupu zohledňujícího všechny úrovně správy, pokud možno včetně prosazování práva.

53) Zúčastnění aktéři by měli na každé úrovni provádět konkrétní činnosti s cílem dosáhnout společného situačního povědomí a koordinované reakce. Těmito opatřeními se zajistí řádné a účinné šíření informací.

54) Reakce by měla být přiměřená dopadu rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize. V souladu se směrnicí (EU) 2022/2555 by orgány členských států pro řešení kybernetických krizí měly zajistit vnitrostátní soudržnost a koordinaci mezi odvětvovými reakcemi na kybernetickou krizi.

55) V případě rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize by všichni aktéři a sítě měli v úzké koordinaci reagovat takto:

a) na technické úrovni:

i. dotčené členské státy a jejich týmy CSIRT by měly spolupracovat s dotčenými subjekty s cílem reagovat na incidenty a případně poskytovat pomoc;

ii. týmy CSIRT by měly spolupracovat prostřednictvím sítě CSIRT za účelem sdílení relevantních technických informací o incidentu; týmy CSIRT spolupracují ve svém úsilí analyzovat dostupné technické artefakty a další technické informace související s incidentem s cílem určit příčinu a možná technická zmírňující opatření;

iii. týmy CSIRT nebo orgány členského státu pro řešení kybernetických krizí se vyzývají, aby v případě, že se dozví o významném incidentu, sdílely informace v rámci sítě CSIRT nebo sítě EU-CyCLONe;

iv. síť CSIRT by měla s podporou agentury ENISA vypracovat souhrn vnitrostátních zpráv poskytovaných týmy CSIRT, který by měl být předložen síti EU-CyCLONe;

v. pokud má kybernetický bezpečnostní incident potenciál přerůst v rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi, měla by síť CSIRT sdílet příslušné informace se sítí EU-CyCLONe. Síť EU-CyCLONe by měla tyto informace využít k informování Rady;

vi. síť CSIRT by měla být v úzkém kontaktu s Europolem, aby byla zajištěna výměna relevantních technických informací. Síť CSIRT a Europol by měly zřídit kontaktní místa s cílem zlepšit sdílení informací, je-li to relevantní v případě rozsáhlého kybernetického bezpečnostního incidentu;

b) na operační úrovni:

i. členské státy by měly zmírnit dopad incidentu na vnitrostátní úrovni pomocí vhodných opatření;

ii. síť CSIRT by měla síti EU-CyCLONe poskytovat technická posouzení probíhajících incidentů, která může síť EU-CyCLONe využít;

iii. síť EU-CyCLONe by měla posoudit důsledky a dopad příslušných rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí a navrhnout možná zmírňující opatření a podporovat koordinované řešení rozsáhlých kybernetických bezpečnostních incidentů a kybernetických krizí, jakož i rozhodování na politické úrovni;

iv. pokud by rozsáhlý kybernetický bezpečnostní incident s meziodvětvovým dopadem vyžadoval aktivaci opatření reakce na úrovni Unie, a to zejména příslušných horizontálních a odvětvových mechanismů pro řešení krizí na úrovni Unie uvedených v příloze II,

a) mohou příslušní aktéři v závislosti na typu odvětvových mechanismů pro řešení krizí na úrovni Unie vyzvat k aktivaci uvedeného mechanismu;

b) v případě aktivace tohoto odvětvového mechanismu poskytují příslušné subjekty při zmírňování dopadu incidentu podporu odvětvovým subjektům;

c) Komise by měla usnadňovat tok nezbytných informací mezi kontaktními místy pro příslušné horizontální a odvětvové krizové mechanismy na úrovni Unie uvedené v příloze II a sítí EU-CyCLONe a měla by provádět integrovanou meziodvětvovou analýzu a navrhovat možnosti vhodného integrovaného plánu reakce;

d) Komise by měla v relevantních případech prostřednictvím sítě EU-CyCLONe ve spolupráci s vysokým představitelem zajišťovat soudržnost a koordinaci operativních opatření na úrovni EU v kybernetické oblasti se souvisejícími opatřeními reakce na úrovni Unie, a to zejména pokud jde o žádosti o pomoc prostřednictvím mechanismu civilní ochrany Unie;

e) pokud byla spuštěna monitorovací stránka IPCR, měly by být prostřednictvím internetové platformy IPCR mezi členskými státy a subjekty Unie sdíleny rovněž informace o incidentu, jeho dopadech a přijatých opatřeních;

v. členské státy mohou požádat o služby z rezervy EU pro kybernetickou bezpečnost v souladu s článkem 15 nařízení (EU) 2025/38. Aniž jsou dotčeny jakékoli budoucí prováděcí akty podle uvedeného nařízení, měly by být služby rezervy EU pro kybernetickou bezpečnost nasazeny do 24 hodin od podání žádosti;

c) na politické úrovni:

i. Rada si může v zájmu přijetí vhodné politické a strategické reakce vyžádat informace od klíčových zúčastněných stran, zejména od Komise, vysokého představitele a sítě EU-CyCLONe;

ii. Rada by s podporou Komise a vysokého představitele mohla rozhodnout o vhodných opatřeních v reakci na rozsáhlý kybernetický bezpečnostní incident včetně možných diplomatických reakcí v souladu s kapitolou IX;

iii. členské státy mohou v závislosti na povaze a dopadu incidentu aktivovat další mechanismy nebo nástroje pro řešení kybernetických krizí;

iv. je-li IPCR aktivována v režimu sdílení informací, aktivuje se podpůrná kapacita ISAA, čímž se posílí výměna informací prostřednictvím internetové platformy IPCR a zajistí se společný situační přehled. Situační zprávy sítě EU-CyCLONe a sítě CSIRT by měly zůstat hlavními nástroji prezentujícími společné situační povědomí na operativní, respektive na technické úrovni. Tyto zprávy mohou sloužit jako podklad pro zprávy ISAA;

v. v případě incidentu, který vyžaduje aktivaci opatření reakce na úrovni Unie, zejména příslušných horizontálních a odvětvových mechanismů pro řešení krizí na úrovni Unie uvedených v příloze II, by Rada ve spolupráci s Komisí a vysokým představitelem měla zajistit soudržnost a koordinaci mezi reakcemi na kybernetickou krizi a souvisejícími opatřeními reakce na úrovni Unie;

vi. jsou-li požadovány příslušné mechanismy, zejména služby rezervy pro kybernetickou bezpečnost, měly by útvary Komise a ve vhodných případech ESVČ, jakož i příslušné orgány Rady, zejména Horizontální pracovní skupina pro otázky týkající se kybernetiky a Horizontální pracovní skupina pro posilování odolnosti a boj proti hybridním hrozbám, podle potřeby koordinovat navrhování a provádění opatření, jakož i vhodný rozhodovací proces s dalšími opatřeními, a to v souladu se souborem hybridních nástrojů[14] pro případ nepřátelských činností v kyberprostoru, které jsou součástí širší hybridní kampaně.

Reakce na rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi, u nichž byla aktivována IPCR v režimu plné aktivace

56) Měly by být provedeny kroky obsažené ve výše uvedeném oddíle „*Reakce na rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi, u nichž nebyla aktivována IPCR v režimu plné aktivace“*.

57) Je-li IPCR aktivována v režimu plné aktivace, zprávy ISAA slouží k zajištění společného situačního povědomí na politické úrovni. Situační zprávy sítě EU-CyCLONe a sítě CSIRT by měly zůstat hlavními nástroji prezentujícími společné situační povědomí na operativní, respektive na technické úrovni. Tyto zprávy mohou sloužit jako podklad pro zprávy ISAA.

58) V případě rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize, jež vedou k aktivaci IPCR v režimu plné aktivace, by všichni aktéři měli reagovat v úzké koordinaci v rámci meziresortního přístupu takto:

a) koordinaci reakce na politické úrovni Unie provádí Rada za využití opatření IPCR;

[14] Soubor hybridních nástrojů je rámcem pro koordinovanou reakci na hybridní kampaně ovlivňující EU a její členské státy a zahrnuje například opatření v oblasti předcházení, spolupráce, stability, omezování a zotavení a podporuje solidaritu a vzájemnou pomoc.

b) síť EU-CyCLONe by měla ve spolupráci se sítí CSIRT poskytnout politické úrovni jasné informace o dopadu, možných důsledcích a opatřeních pro reakci na incident a jeho nápravu, a to i prostřednictvím přispění ke zprávám ISAA;

c) kromě kapacity ISAA předsednictví Rady Evropské unie svolá jednání u kulatého stolu IPCR s cílem umožnit politickou a strategickou koordinaci reakce EU, přičemž podkladem pro činnost IPCR budou opatření v rámci kybernetického plánu a práce příslušných odvětvových mechanismů. V rámci těchto jednání u kulatého stolu lze navíc identifikovat některé konkrétní nedostatky v reakci a vyzvat konkrétní aktéry EU, aby se jimi zabývali a podali o nich zprávu na budoucích jednáních u kulatého stolu s cílem podpořit politickou a strategickou koordinaci v rámci IPCR;

d) předsednictví Rady Evropské unie by mělo zvážit pozvání sítě EU-CyCLONe na příslušná zasedání včetně jednání u kulatého stolu v rámci opatření IPCR a dalších příslušných zasedání Rady;

e) orgány členských států pro řešení krizí by měly zajistit soudržnost a koordinaci mezi odvětvovými reakcemi na kybernetickou krizi podporovanými orgány pro řešení kybernetických krizí;

f) v souladu s kapitolou IX by měly být zváženy a prováděny případné diplomatické reakce.

VIII: Úsilí v oblasti komunikace s veřejností

59) Ačkoliv je informování obyvatelstva jednotlivých členských států o probíhajícím rozsáhlém kybernetickém bezpečnostním incidentu nebo kybernetické krizi, a to i v rámci zvyšování informovanosti, vnitrostátní pravomocí, měli by se členské státy, Komise a vysoký představitel při své komunikaci s veřejností zaměřit na co nejširší koordinaci. Ve vhodných případech je možné zapojit neformální síť krizových komunikátorů v rámci IPCR.

60) Pro účely přípravy na rozsáhlé kybernetické bezpečnostní incidenty a kybernetické krize se členské státy a v příslušných případech Komise a CERT-EU vyzývají, aby si vyměňovaly informace o svém komunikačním úsilí v rámci sítě EU-CyCLONe a sítě CSIRT, včetně osvědčených postupů, jako jsou poradenství nebo osvětové kampaně. Agentura ENISA by měla poskytnout nástroje na podporu této výměny a zajištění snadného přístupu.

61) Členské státy se vyzývají, aby v případě rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize sdílely v rámci sítě EU-CyCLONe informace o svém úsilí v oblasti komunikace s veřejností s cílem vybudovat společné povědomí a koordinovat opatření. Síť EU-CyCLONe může z vlastní iniciativy nebo na žádost Rady sdílet s Radou přehled těchto přístupů.

IX: Diplomatická reakce a spolupráce se strategickými partnery

62) Vysoký představitel by v úzké spolupráci s Komisí a dalšími příslušnými subjekty Unie měl:

a) podporovat rozhodování v Radě, a to i prostřednictvím analýz, zpráv a návrhů, o využití možných opatření v rámci souboru nástrojů EU pro diplomacii v oblasti kybernetiky. To umožní použít celé spektrum dostupných nástrojů Unie k předcházení nepřátelským kybernetickým činnostem, odrazování od nich a reakci na ně, což posílí její kybernetickou pozici a podpoří mezinárodní mír, bezpečnost a stabilitu v kyberprostoru;

b) v případě, že je identifikován relevantní incident, usnadnit tok potřebných informací mezi strategickými partnery, a to v relevantních případech včetně NATO;

c) posílit koordinaci se strategickými partnery, a to v relevantních případech včetně NATO, při reakci na nepřátelské kybernetické činnosti aktérů trvalé hrozby, zejména při používání souboru nástrojů EU pro diplomacii v oblasti kybernetiky, a to v souladu s prováděcími pokyny.

63) Členské státy, vysoký představitel, Komise a další příslušné subjekty Unie by měli spolupracovat se strategickými partnery a mezinárodními organizacemi s cílem prosazovat osvědčené postupy a odpovědné chování států v kyberprostoru a zajistit rychlou a koordinovanou reakci v případě potenciálních nebo rozsáhlých kybernetických bezpečnostních incidentů.

64) Spolupráce Evropské unie a NATO by měla probíhat v souladu s dohodnutými hlavními zásadami inkluzivnosti, reciprocity a transparentnosti a při plném respektování autonomního rozhodování Unie.

65) Komise a vysoký představitel by měli s přihlédnutím ke stávajícím dohodám, jako je technická dohoda CERT-EU/NATO z roku 2016, zřídit kontaktní místa pro koordinaci s NATO v případě kybernetické krize za účelem výměny nezbytných informací o situaci a využití mechanismů reakce na krize, aby zvýšili účinnost reakce a zlepšili spolupráci během ní. Za tímto účelem by Unie měla prozkoumat způsoby, jak zlepšit sdílení informací s NATO inkluzivním, recipročním a nediskriminačním způsobem, zejména prostřednictvím zajištění nástrojů pro bezpečnou komunikaci při současném zohlednění norem pro sdílení informací v různých členských státech.

66) V rámci průběžného programu kybernetických cvičení Unie uvedeného v kapitole V by útvary Komise a ESVČ měly zvážit uspořádání cvičení na úrovni zaměstnanců s NATO s cílem otestovat spolupráci mezi civilními a vojenskými subjekty v případě rozsáhlého kybernetického bezpečnostního incidentu nebo kybernetické krize, v rámci kterého se členské státy nebo spojenci NATO snaží reagovat na kybernetický útok s dopadem na jejich bezpečnost. Toto cvičení by mělo být prováděno inkluzivním a nediskriminačním způsobem a při plném dodržování dohodnutých zásad parametrů spolupráce mezi EU a NATO. Mělo by probíhat v rámci cvičení EU Integrated Resolve (paralelní a koordinované cvičení, dále jen „PACE“). Je třeba přijmout veškerá nezbytná opatření k zajištění účasti všech aktérů uvedených v kybernetickém plánu.

67) Po konzultaci s Radou, Komisí a vysokým představitelem by měla být zvážena také společná kybernetická cvičení na úrovni Unie se zeměmi západního Balkánu, Moldavskou republikou, Ukrajinou, jakož i dalšími strategickými partnery a podobně smýšlejícími třetími zeměmi.

X. Koordinace řešení kybernetických krizí s vojenskými aktéry na úrovni EU

68) Členské státy by měly pokračovat v posilování spolupráce mezi civilními a vojenskými aktéry v kybernetické oblasti na vnitrostátní úrovni.

69) Síť EU-CyCLONe a síť CSIRT by měly určit možné způsoby a postupy spolupráce s příslušnými vojenskými aktéry EU, jako je konference velitelů kybernetických sil EU a operační síť pro vojenské týmy pro reakci na počítačové hrozby (MICNET), aby bylo možné využít společné vojenské a civilní perspektivy, zejména prostřednictvím společných zasedání. Síť EU-CyCLONe a síť CSIRT by měly Radu informovat o pokroku dosaženém v této spolupráci.

70) Dotčený členský stát se vyzývá, aby informoval síť EU-CyCLONe, jakož i ESVČ, pokud jsou v souvislosti s rozsáhlým kybernetickým bezpečnostním incidentem nebo kybernetickou krizí využity příslušné vnitrostátní nebo nadnárodní vojenské schopnosti reakce, přičemž na poskytnutí těchto informací se vzájemně dohodnou uživatel a poskytovatel této schopnosti reakce.

71) V rámci průběžného programu kybernetických cvičení Unie uvedeného v kapitole V by Komise a vysoký představitel měli zvážit uspořádání společného cvičení s cílem otestovat spolupráci mezi civilními i vojenskými subjekty v kybernetické oblasti v případě rozsáhlého kybernetického bezpečnostního incidentu s dopadem na členské státy.

XI: Zotavení a zkušenosti získané z kybernetické krize

72) Členské státy, příslušné subjekty Unie a sítě by měly během fáze zotavení po kybernetické krizi spolupracovat v zájmu zajištění rychlého obnovení základních funkcí. Do této spolupráce by měly být v příslušných případech zapojeny i komunity v oblasti prosazování práva. V této fázi má zásadní význam spolupráce se soukromým sektorem, zejména pokud jde o usnadnění obnovy dat a opětovné zprovoznění systémů. Účinná koordinace mezi zúčastněnými stranami by se prioritně měla zaměřit na minimalizaci narušení a zajištění kontinuity činností.

73) Členské státy, příslušné subjekty Unie a sítě by měly ve fázi zotavení spolupracovat na základě zkušeností získaných z minulých kybernetických krizí nebo řešených kybernetických bezpečnostních incidentů, jakož i zpráv o incidentech, zejména v kontextu evropského mechanismu přezkumu kybernetických bezpečnostních incidentů zřízeného v souladu s nařízením (EU) 2025/38.

74) Síť EU- CyCLONe by měla síti CSIRT, skupině pro spolupráci v oblasti bezpečnosti sítí a informací a Radě poskytnout komplexní seznam zkušeností získaných z minulých kybernetických krizí nebo řešených kybernetických bezpečnostních incidentů a osvědčených postupů. Agentura ENISA by měla zajistit, aby byly tyto získané zkušenosti řádně zohledněny při budoucích činnostech v oblasti připravenosti a při zvažování plánování budoucích cvičení.

XII: Zabezpečená komunikace

75) Na základě zmapování stávajících nástrojů bezpečné komunikace[15] by Komise měla do konce roku 2026 navrhnout interoperabilní soubor řešení zabezpečené komunikace. Rada, Komise, vysoký představitel, síť EU-CyCLONe a síť CSIRT by se na tomto souboru měli dohodnout do konce roku 2027. Tato řešení by měla těžit z opatření v oblasti bezpečné komunikace, která by orgány EU mohly přijmout v rámci Strategii EU pro unii připravenosti, a měla by pokrývat celý rozsah požadovaných způsobů komunikace (hlasovou komunikaci, data, videokonference, zasílání zpráv, spolupráci a sdílení dokumentů a nahlížení do nich). Řešení by měla splňovat společně stanovené požadavky na ochranu citlivých neutajovaných informací. Měla by být používána řešení založená na otevřeném protokolu s implementacemi s otevřeným zdrojovým kódem vhodnými pro komunikaci v reálném čase, které spravuje subjekt se sídlem v EU.

76) Síť EU-CyCLONe a síť CSIRT by pro účely výměny informací se stupněm utajení RESTREINT UE/EU RESTRICTED měly mít v případě potřeby možnost používat zabezpečené komunikační kanály zajištěné pro orgány, instituce a jiné subjekty EU pro výměnu utajovaných informací mezi sebou navzájem a s členskými státy.

[15] Dokument WK 862/2023.

77) Aniž je dotčen budoucí víceletý finanční rámec, mělo by Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost (ECCC) zřízené podle nařízení (EU) 2021/887[16] zvážit financování z programu Digitální Evropa s cílem pomoci členským státům při zavádění nástrojů bezpečné komunikace. Je třeba zabránit jakémukoliv zdvojování investic do interoperabilních bezpečných systémů.

78) Subjekty EU a členské státy by měly zejména vypracovat pohotovostní plány pro případy závažných krizí, kdy jsou narušeny nebo nedostupné běžné komunikační kanály využívající internet nebo telekomunikační sítě.

79) Pro účinnou reakci na kybernetické krize by měly být vytvořeny mechanismy komunikace a sdílení informací mezi donucovacími orgány a sítěmi pro kybernetickou bezpečnost, zejména na technické úrovni. Tyto mechanismy by měly respektovat úlohu každé strany, neměly by zasahovat do probíhajících operací a měly by zaručovat redundanci komunikací. Přínosem pro společnou reakci s příslušnými kybernetickými komunitami může být v současnosti vyvíjený kritický komunikační systém EU.

XIII: Závěrečná ustanovení

80) Síť EU-CyCLONe by ve spolupráci se sítí CSIRT a dalšími hlavními aktéry v ekosystému EU pro řešení kybernetických krizí a s podporou agentury ENISA měla do jednoho roku od zveřejnění tohoto doporučení vypracovat podrobné vývojové diagramy procesů znázorňující toky informací mezi příslušnými aktéry, rozhodovací procesy a zprávy vypracované během řešení rozsáhlých kybernetických bezpečnostních incidentů nebo kybernetických krizí, jak je popsáno v tomto doporučení. Tyto vývojové diagramy by měly zahrnovat různé způsoby a úrovně spolupráce. Měly by být v případě potřeby aktualizovány.

[16] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, Úř. věst. L 202, 8.6.2021, s. 1.

81) Na podporu účinného uplatňování revidovaného kybernetického plánu a na základě zkušeností získaných při společných kybernetických cvičeních prováděných v jeho rámci může Rada v případě potřeby vypracovat soubor prováděcích pokynů. Tyto pokyny by mohly řešit praktické problémy zjištěné během cvičení a mohly by se pomocí nich odstranit zjištěné nedostatky a chybějící články v koordinaci, komunikaci a operativní interakci.

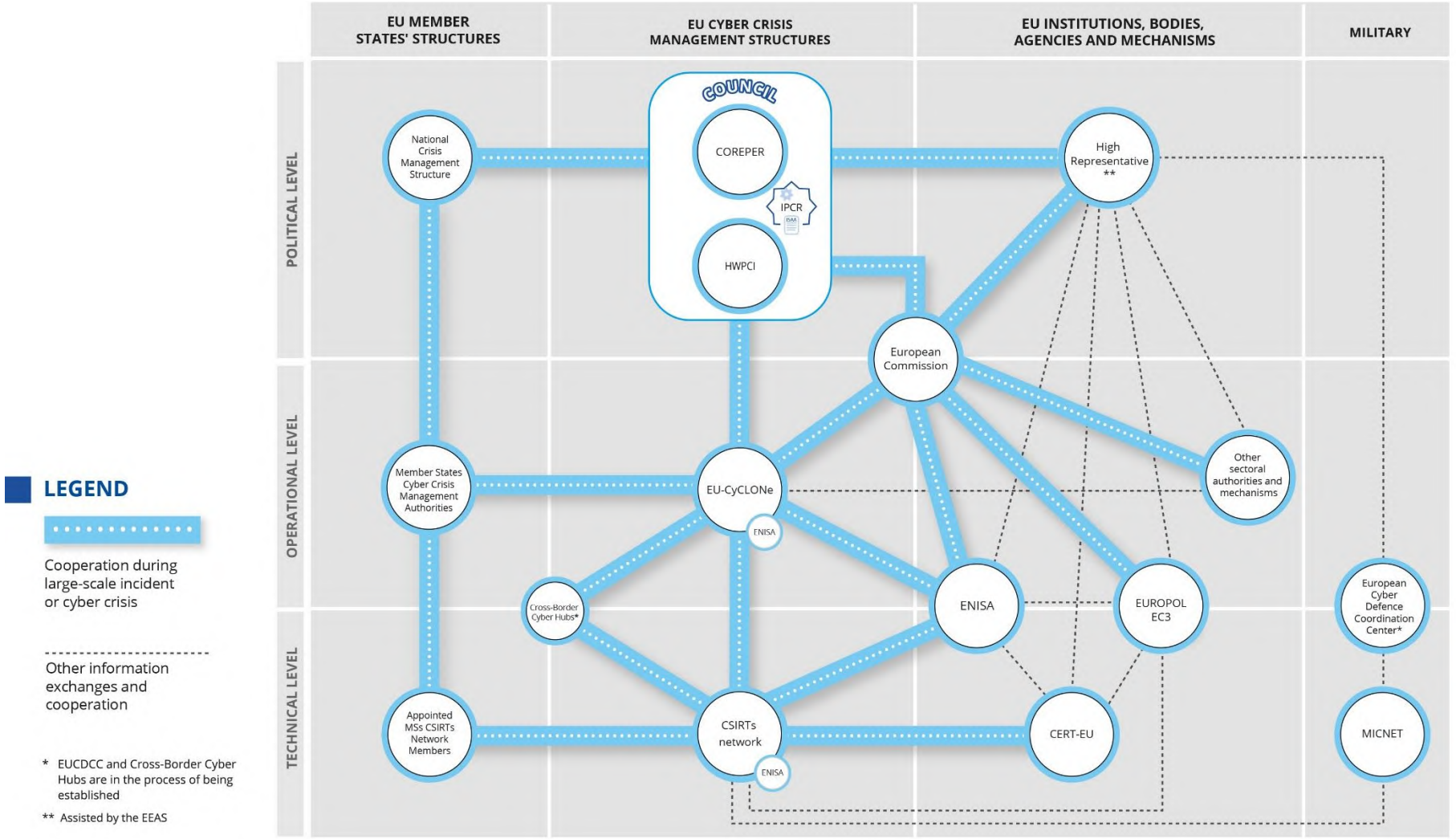
82) Komise by toto doporučení měla přezkoumat ve spolupráci s členskými státy nejméně jednou za čtyři roky po jeho zveřejnění. Po každém přezkumu by Komise měla zveřejnit zprávu a předložit ji Radě. Komise a členské státy by měly zohlednit zejména dopad měnícího se prostředí hrozeb, výsledky společných cvičení a legislativní změny – zejména jakékoliv případné změny vyplývající z revize nařízení (EU) 2019/881.

V Bruselu dne

Za Radu

předseda

PŘÍLOHA I – Plán Unie pro reakci na kybernetickou bezpečnostní krizi



PŘÍLOHA II – RELEVANTNÍ AKTÉŘI (SUBJEKTY A SÍTĚ) NA ÚROVNI UNIE A MECHANISMY PRO ŘEŠENÍ KRIZÍ

1) Zapojení hlavních aktérů do celého životního cyklu řešení kybernetických krizí (rozsáhlé kybernetické bezpečnostní incidenty a kybernetické krize)

	Připravenost	Odhalení	Reakce na rozsáhlý kybernetický bezpečnostní incident nebo kybernetickou krizi			Komunikace s veřejností	Zotavení a získané zkušenosti
			na technické úrovni	na operační úrovni	na politické úrovni		
Členské státy	X	X	X	X	X	X	X
Komise	X			X	X	X	
Vysoký představitel, jemuž je nápomocna ESVČ	X			X	X	X	
Rada	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Síť CSIRT	X	X	X				X
Síť EU-CyCLONe	X			X	X		X

2) Úlohy a pravomoci příslušných aktérů mechanismů na úrovni Unie (v abecedním pořadí) v souvislosti s řešením kybernetických krizí

Aktér	Úroveň	Úloha a pravomoc	Odkaz
CERT-EU	Technická/operační	Koordinuje reakci na krizi na technické úrovni a řešení závažných incidentů, které ovlivňují subjekty Unie. Vede seznam dostupných technických odborných znalostí, které by v případě závažných incidentů byly potřebné pro reakci, a pomáhá výboru IICB při koordinaci plánů subjektů Unie pro řešení kybernetických krizí v případě závažných incidentů. Člen sítě CSIRT. Podporuje Komisi v rámci sítě EU-CyCLONe, pokud jde o koordinované řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Působí jako centrum pro výměnu informací o kybernetické bezpečnosti a koordinaci reakce na incidenty, přičemž usnadňuje	Nařízení (EU, Euratom) 2023/2841 Nařízení (EU) 2025/38

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		výměnu informací o incidentech, kybernetických hrozbách, zranitelnostech a významných událostech mezi subjekty Unie a partnery. Žádá o použití rezervy EU pro kybernetickou bezpečnost jménem subjektů Unie. Spolupracuje s centrem NATO pro kybernetickou bezpečnost na základě technické dohody.	
Rada Evropské unie	Politická	Funkce obnášející tvorbu politik a koordinaci. Je pověřena prováděním opatření IPCR, které se týká koordinace a reakce na politické úrovni Unie.	Článek 16 Smlouvy o Evropské unii
Předsednictví Rady Evropské unie	Politická	Rozhoduje (s výjimkou případů, kdy je uplatněna doložka solidarity podle článku 222 Smlouvy o fungování Evropské unie) o aktivaci opatření IPCR EU, a to případně po konzultaci s dotčenými členskými státy, jakož i s Komisí a vysokým představitelem.	Článek 16 Smlouvy o Evropské unii Prováděcí rozhodnutí Rady (EU) 2018/1993

Aktér	Úroveň	Úloha a pravomoc	Odkaz
Přeshraniční kybernetická centra	Technická	Přeshraniční kybernetické centrum je platforma, které se účastní více zemí, zřízená prostřednictvím písemné dohody o konsorciu, která v koordinované síťové struktuře sdružuje národní kybernetická centra alespoň ze tří členských států a která je určena ke zlepšení monitorování, odhalování a analýzy kybernetických hrozeb s cílem předcházet incidentům a podporovat získávání poznatků o kybernetických hrozbách, zejména prostřednictvím výměny relevantních a případně anonymizovaných dat a informací, jakož i sdílením nejmodernějších nástrojů a společným vývojem schopností odhalování, analýzy a prevence a ochrany v oblasti kybernetické bezpečnosti v důvěryhodném prostředí; Úzce spolupracují se sítí CSIRT za účelem sdílení informací.	Nařízení (EU) 2025/38

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		Poskytují informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu orgánům členských států a Komisi prostřednictvím sítě EU-CyCLONe a sítě CSIRT.	
Síť CSIRT	Technická	Přispívá k budování důvěry a podporuje rychlou operační spolupráci mezi členskými státy. Jedná se o hlavní síť pro výměnu příslušných informací o incidentech, významných událostech, kybernetických hrozbách, rizicích a zranitelnostech. Na žádost člena potenciálně zasaženého incidentem si síť vyměňuje a projednává informace o tomto incidentu a souvisejících kybernetických hrozbách. Síť může rovněž usnadňovat koordinovanou reakci na incident, který byl zjištěn	Směrnice (EU) 2022/2555 Nařízení (EU) 2025/38

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		v oblasti spadající do pravomoci žádajícího člena. Poskytuje pomoc členským státům při zvládání přeshraničních incidentů a zkoumá další formy spolupráce včetně vzájemné pomoci. Přijímá informace od členských států o jejich žádostech o podporu z rezervy EU pro kybernetickou bezpečnost.	
Konference velitelů kybernetických sil		Fórum velitelů kybernetických sil na vnitrostátní úrovni v členských státech za účelem spolupráce a výměny důležitých informací o probíhajících operacích v kyberprostoru a strategiích pro zmírnění rozsáhlých kybernetických bezpečnostních incidentů. Pořádá ji rotující předsednictví Rady Evropské unie za podpory Evropské obranné agentury (EDA), Evropské služby pro vnější činnost (ESVČ), včetně Vojenského štábu EU (EUMS).	Společné sdělení o politice EU v oblasti kybernetické obrany (2022)

Aktér	Úroveň	Úloha a pravomoc	Odkaz
Komise	Operační/politická	Výkonný orgán Evropské unie. Zajištění bezproblémového fungování vnitřního trhu. Usnadňuje soudržnost a koordinaci mezi souvisejícími opatřeními reakce na krize na úrovni Unie. Některá obecná opatření v oblasti připravenosti na úrovni Unie v rámci mechanismu civilní ochrany Unie, včetně řízení Střediskem pro koordinaci odezvy na mimořádné události a společného komunikačního a informačního systému pro mimořádné události. Pozorovatel v síti EU-CyCLONe a člen v případě potenciálního nebo probíhajícího rozsáhlého incidentu, který má nebo pravděpodobně bude mít významný dopad na služby a činnosti spadající do oblasti	Článek 17 Smlouvy o Evropské unii Prováděcí rozhodnutí (EU) 2018/1993 Rozhodnutí č. 1313/2013/EU Směrnice (EU) 2022/2555 Nařízení (EU) 2025/38 Nařízení (EU, Euratom) 2023/2841

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		působnosti směrnice (EU) 2022/2555. Pozorovatel v rámci sítě CSIRT. Celková odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Kontaktní místo Interinstitucionálního výboru pro kybernetickou bezpečnost pro sdílení relevantních informací v souvislosti se závažnými incidenty se sítí EU-CyCLONe. Předsednictví Rady ji konzultuje v otázce rozhodnutí o aktivaci nebo deaktivaci opatření IPCR (s výjimkou případů, kdy je uplatněna doložka solidarity podle článku 222 SFEU). Útvary Komise spolu s ESVČ vypracovávají zprávy v oblasti integrovaného situačního povědomí a analýzy (ISAA).	

Aktér	Úroveň	Úloha a pravomoc	Odkaz
Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)	Technická/operační	Plní úkoly za účelem dosažení vysoké úrovně kybernetické bezpečnosti v celé Unii, mimo jiné aktivní podporou členských států a orgánů Unie Zajišťuje sekretariát pro síť CSIRT a síť EU-CyCLONe. Vypracovává pravidelnou technickou situační zprávu EU v oblasti kybernetické bezpečnosti týkající se incidentů a kybernetických hrozeb (spolu s EC3 a CERT-EU a v úzké spolupráci s členskými státy). Přispívá k vypracování společné reakce na rozsáhlé přeshraniční incidenty nebo krize, a to zejména: - shromažďováním a analýzou zpráv z vnitrostátních zdrojů; - zajišťováním toku informací mezi technickou, operační a politickou úrovní; - usnadňováním řešení incidentů, je-li požádána;	Směrnice (EU) 2022/2555 Nařízení (EU) 2019/881 Nařízení (EU) 2025/38 Nařízení (EU) 2024/2847

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		- podporou subjektů Unie v oblasti komunikace s veřejností; - podporou členských států, pokud jde o komunikaci s veřejností, je-li požádána; - testováním schopností reakce na incidenty a pravidelným pořádáním cvičení v oblasti kybernetické bezpečnosti. Jedná jako veřejný zadavatel, je-li pověřena, aby částečně nebo zcela provozovala a spravovala rezervu EU pro kybernetickou bezpečnost. Organizuje každé dva roky rozsáhlé komplexní cvičení v oblasti kybernetické bezpečnosti na úrovni Unie s technickými, operačními nebo strategickými prvky. Ve spolupráci s dotčeným členským státem a dalšími příslušnými zúčastněnými stranami vypracovává zprávu o přezkumu incidentu s cílem posoudit příčiny, dopad a zmírnění incidentu (na žádost	

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		Komise nebo sítě EU-CyCLONe a se souhlasem dotčeného členského státu). Informuje síť EU-CyCLONe, pokud jsou informace poskytnuté v rámci oznamovacích povinností podle aktu o kybernetické odolnosti relevantní pro koordinované řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operační úrovni.	
Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe)	Operační	Podporuje koordinované řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operační úrovni. Zajišťuje pravidelnou výměna příslušných informací mezi členskými státy a orgány, institucemi nebo jinými subjekty Unie. Koordinuje řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí a podporuje rozhodování na politické úrovni	Směrnice (EU) 2022/2555 Nařízení (EU) 2025/38

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		týkající se těchto incidentů a krizí. Posuzuje důsledky a dopad příslušných rozsáhlých kybernetických bezpečnostních incidentů a krizí a navrhuje případná opatření k jejich zmírnění. Na žádost dotčeného členského státu projednává národní plány reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize. Společně s agenturou ENISA a Komisí vypracovává šablonu pro usnadnění podávání žádostí o podporu z rezervy EU pro kybernetickou bezpečnost. Přijímá informace od členských států o jejich žádostech o podporu z rezervy EU pro kybernetickou bezpečnost. Přijímá informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu od přeshraničních	

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		kybernetických center nebo sítě CSIRT.	
Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku, jemuž je nápomocna Evropská služba pro vnější činnost	Politická	Řídí a koordinuje úsilí Unie o řešení vnějších hybridních a kybernetických bezpečnostních hrozeb. Je odpovědný za nástroje kybernetické diplomacie a kybernetické obrany Unie, jejichž úkolem je odrazovat od vnějších hrozeb a reagovat na ně mimo jiné s využitím souboru nástrojů Unie proti hybridním hrozbám a souborů nástrojů pro diplomacii v oblasti kybernetiky. Spolupracuje s externími partnery, a to i prostřednictvím zapojení do společné bezpečnostní a obranné politiky. Zajišťuje připravenost Unie a členských států, jejich situační povědomí a schopnost reagovat na hybridní a kybernetické hrozby, například	Rozhodnutí Rady 2010/427/EU

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		prostřednictvím praktických cvičení, vzdělávání a sítí. Zabývá se důsledky kosmických prostředků Unie pro bezpečnost a obranu, zejména v rámci společné bezpečnostní a obranné politiky (SBOP) Unie. Podporuje konferenci velitelů kybernetických sil EU. Podporuje operační síť EU pro vojenské týmy pro reakci na počítačové hrozby (MICNET). Předsednictví Rady jej konzultuje v otázce rozhodnutí o aktivaci nebo deaktivaci opatření IPCR (s výjimkou případů, kdy je uplatněna doložka solidarity podle článku 222 SFEU). ESVČ spolu s útvary Komise vypracovává zprávy ISAA.	
Koordinační středisko EU pro	Horizontální	Jeho původním cílem je především zlepšit společné situační povědomí Unie a jejích	Společné sdělení o politice EU v oblasti

Aktér	Úroveň	Úloha a pravomoc	Odkaz
kybernetickou obranu		členských států v oblasti nepřátelských činností v kyberprostoru, zejména pokud jde o vojenské mise a operace SBOP.	kybernetické obrany (2022)
Europol	Operační	Poskytuje operační a technickou podporu příslušným orgánům členských států při prevenci kyberkriminality a odrazování od ní. Napomáhá příslušným orgánům členských států na jejich žádost při reakci na kybernetické útoky, u nichž existuje podezření na jejich trestnou povahu.	Nařízení (EU) 2016/794 včetně všech změn
Interinstitucionální výbor pro kybernetickou bezpečnost		Vypracovává plán řešení kybernetických krizí s cílem podpořit na operativní úrovni koordinované řízení závažných incidentů s dopadem na subjekty Unie a přispět k pravidelné výměně příslušných informací, zejména pokud jde o dopady a závažnost závažných incidentů a možné způsoby jejich zmírnění.	Nařízení (EU, Euratom) 2023/2841

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		Koordinuje přijímání plánů jednotlivých subjektů Unie pro řešení kybernetických krizí. Přijímá na základě návrhu služby CERT-EU pokyny nebo doporučení týkající se spolupráce při reakci na významné incidenty týkající se subjektů Unie.	
Operační síť pro vojenské týmy pro reakci na počítačové hrozby (MICNET)	Technická	Podporuje důraznější a koordinovanější reakci na kybernetické hrozby ovlivňující obranné systémy v Unii, včetně systémů používaných při vojenských misích a operacích SBOP; podporuje ji Evropská obranná agentura.	Společné sdělení Kybernetická obrana z roku 2022
Společná zpravodajsko-analytická složka (SIAC)		Skládá se ze 1) Zpravodajského a informačního centra EU (EU INTCEN) a 2) společné zpravodajsko-analytické složky zpravodajského ředitelství Vojenského štábu EU (EUMS INT). Poskytuje strategické zpravodajské informace týkající	Články 38 a 42 až 46 Smlouvy o Evropské unii

Aktér	Úroveň	Úloha a pravomoc	Odkaz
		se zahraniční politiky, terorismu a kybernetických a hybridních hrozeb. Zpracovává vojenské zpravodajské informace pro mise SBOP a podporuje obranné operace a operace Unie pro řešení krizí. Je podřízena vedení vysokého představitele.	

3) Relevantní mechanismy a platformy pro řešení krizí na úrovni Unie

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
ARGUS	Horizontální	Koordinační proces Komise a obecný systém varování pro soudržnou reakci v případě závažné přeshraniční krize vyžadující opatření na úrovni EU. Sdružuje všechny relevantní útvary a kabinety, aby rozhodovaly o příslušných opatřeních a koordinovaly je. Umožňuje Komisi vyměňovat si relevantní informace o vznikajících víceodvětvových krizích nebo předvídatelných či bezprostředních hrozbách, které vyžadují opatření na úrovni Unie.	Sdělení Komise KOM(2005) 662
Středisko ESVČ pro reakci na krize	Horizontální	Jednotné kontaktní místo v ESVČ pro všechny záležitosti související s krizemi a stálá nepřetržitá kapacita pro reakci na krize v případě mimořádných událostí ohrožujících bezpečnost zaměstnanců delegací EU nebo v reakci na krize postihující občany Unie v zahraničí. Sdružuje odborníky na bezpečnost, konzulární	Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
		záležitosti a situační povědomí a zároveň se opírá o angažované odborníky na místě v delegacích Unie.	míru a bezpečnosti (21. března 2022)
Plán pro kritickou infrastrukturu	Horizontální	Koordinuje reakce na úrovni Unie na narušení kritické infrastruktury se značným přeshraničním významem.	Doporučení Rady C/2024/4371
Evropský systém varování v oblasti kybernetické bezpečnosti	Kybernetický	Zajišťuje pokročilé schopnosti Unie s cílem posílit schopnosti odhalování, analýzy a zpracování dat v souvislosti s kybernetickými hrozbami a prevencí incidentů v Unii.	Nařízení (EU) 2025/38
Soubor nástrojů pro diplomacii v oblasti kybernetiky (rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru)	Kybernetický	Umožňuje společnou diplomatickou reakci Unie na nepřátelské činnosti v kyberprostoru, která přispívá k předcházení konfliktům, zmírnění kybernetických bezpečnostních hrozeb a větší stabilitě mezinárodních vztahů.	Závěry Rady ze dne 19. června 2017 Revidované prováděcí pokyny 10289/23 ze dne 8. června 2023

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
Rezerva EU pro kybernetickou bezpečnost	Kybernetický	Mobilizuje odborníky na kybernetickou bezpečnost a zdroje během krizí s cílem podpořit úsilí reagovat v členských státech, institucích, orgánech nebo agenturách Unie.	Nařízení (EU) 2025/38
Kodex sítě pro odvětvová pravidla pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny	Odvětvový	Zavádí periodický proces posuzování kybernetických bezpečnostních rizik v odvětví elektřiny na úrovni Unie, členských států, regionů a subjektů. Obsahuje zvláštní ustanovení týkající se krizového řízení a spolupráce s týmy CSIRT a sítí EU-CyCLONe v případech, kdy má rozsáhlý kybernetický bezpečnostní incident dopad na jiná odvětví závislá na bezpečnosti dodávek elektřiny.	Nařízení Komise v přenesené pravomoci (EU) 2024/1366
Soubor hybridních nástrojů	Horizontální	Obsahuje soubor ustanovení, která mají zajistit přehled o všech nástrojích, které jsou k dispozici na úrovni EU, pokud jde o reakci na všechny druhy hybridních hrozeb, a o jejich koordinovaném používání s cílem zajistit soudržnost našich opatření napříč oblastmi. Soubor	Závěry Rady o rámci pro koordinovanou reakci EU na hybridní kampaně, 22. června 2022 Prováděcí pokyny k rámci pro koordinovanou reakci

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
		hybridních nástrojů pomáhá zajistit, aby byla rozhodnutí přijímána na základě komplexního situačního povědomí a získaných zkušeností.	EU na hybridní kampaně, 14. prosince 2022
Týmy rychlé reakce na hybridní hrozby (EU HRRT)	Horizontální	V rámci souboru hybridních nástrojů EU čerpají týmy rychlé reakce EU na hybridní hrozby z příslušných odvětvových civilních a vojenských odborných znalostí na vnitrostátní a unijní úrovni s cílem poskytnout přizpůsobenou a cílenou krátkodobou pomoc členským státům, misím a operacím společné bezpečnostní a obranné politiky a partnerským zemím v boji proti hybridním hrozbám a kampaním.	Obecný rámec pro praktické zřízení týmů rychlé reakce EU na hybridní hrozby (21. května 2024) Operační pokyny pro nasazení týmů rychlé reakce na hybridní hrozby, schválené Coreperem dne 4. prosince 2024
IPCR	Horizontální	Podporuje rychlé a koordinované rozhodování na politické úrovni Unie v případě závažných a složitých krizí. Rozhodnutí o aktivaci a deaktivaci přijímá předsednictví Rady, které konzultuje (s výjimkou případů, kdy byla uplatněna doložka solidarity)	Prováděcí rozhodnutí Rady (EU) 2018/1993

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
		postižené členské státy, Komisi a vysokého představitele. Generální sekretariát Rady, útvary Komise a ESVČ se mohou v konzultaci s předsednictvím rovněž dohodnout na aktivaci opatření IPCR EU v režimu sdílení informací. Práce IPCR vychází ze zpráv ISAA vypracovaných útvary Komise a ESVČ. Tyto zprávy vycházejí z relevantních informací a analýz poskytnutých členskými státy (například od příslušných vnitrostátních krizových středisek) a relevantními agenturami a subjekty Unie.	
Protokol pro reakci donucovacích orgánů EU na mimořádné situace	Horizontální	Nástroj na podporu donucovacích orgánů Unie při zajišťování okamžité reakce na závažné přeshraniční kybernetické útoky prostřednictvím rychlého posouzení, bezpečného, včasného sdílení kritických informací a účinné koordinace mezinárodních aspektů jejich vyšetřování.	Závěry Rady ze dne 26. června 2018 o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Mechanismus	Horizontální/ odvětvový/ kybernetický	Popis	Odkaz
Týmy rychlé kybernetické reakce (CRRT) v rámci PESCO	Kybernetický	Týmy CRRT v rámci PESCO jsou společně vytvořenou civilně-vojenskou schopností členských států EU v oblasti kybernetické obrany určenou k rychlé reakci na kybernetické incidenty a kybernetické krize, jakož i k provádění preventivních opatření, jako je hodnocení zranitelnosti a monitorování voleb. Úkolem uvedených týmů je poskytovat na požádání kybernetickou podporu členským státům EU, orgánům, institucím a jiným subjektům EU, vojenským misím a operacím SBOP EU, jakož i partnerským zemím.	Ustanovení čl. 42 odst. 6, článek 46 a protokol č. 10 ke Smlouvě o Evropské unii.

Architektura reakce na kosmické hrozby (STRA)	Odvětvový (Kosmické hrozby včetně hrozeb souvisejících s kybernetikou)	Architektura reakce na kosmické hrozby (STRA) týkající se odpovědnosti Rady a vysokého představitele za odvrácení hrozby vyplývající z rozmisťování, provozování nebo používání systémů zavedených a služeb poskytovaných v rámci Kosmického programu Unie	Rozhodnutí Rady (SZBP) 2021/698
Rámec pro koordinaci v případě systémových kybernetických bezpečnostních incidentů (EU-SCICF)	Odvětvový	Rámec, který je předmětem vývoje, je určený pro komunikaci a koordinaci a řeší a řídí potenciální systémové kybernetické události ve finančním sektoru. Bude vycházet z jedné z předpokládaných úloh evropských orgánů dohledu podle nařízení (EU) 2022/2554 a postupně umožní účinnou koordinovanou reakci na úrovni Unie v případě závažného přeshraničního incidentu souvisejícího s informačními a komunikačními technologiemi (IKT) nebo související hrozby se systémovým dopadem na finanční sektor Unie jako celek.	Doporučení Evropské rady pro systémová rizika ze dne 2. prosince 2021 o celoevropském rámci pro koordinaci příslušných orgánů v případě systémových kybernetických bezpečnostních incidentů (ESRB/2021/17)
Mechanismus civilní ochrany Unie (UCPM)	Horizontální	Zajišťuje spolupráci v oblasti civilní ochrany s cílem zlepšit prevenci, připravenost a reakci na katastrofy.	Rozhodnutí 1313/2013/EU.

CISE – společné prostředí pro sdílení informací	Specifické pro mořské prostředí, zahrnuje sedm odvětví.	CISE je síť, která propojuje systémy orgánů EU/EHP odpovědných za námořní dohled. CISE umožňuje bezproblémovou a automatizovanou výměnu relevantních informací napříč hranicemi a různými odvětvími.	Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti (21. března 2022).

4) Vysoce kritická odvětví a další kritická odvětví podle směrnice (EU) 2022/2555 a (případně) odvětvové mechanismy reakce na krize na úrovni Unie		
Odvětví	**Pododvětví**	**Použitelné odvětvové mechanismy reakce na krize**
Energetika	Elektřina	Koordinační skupina pro otázky elektřiny
	Dálkové vytápění a chlazení	není relevantní
	Ropa	Koordinační skupina pro otázky ropy Skupina orgánů dohledu nad pobřežními vodami Evropské unie (EUOAG)
	Plyn	Koordinační skupina pro otázky plynu
	Vodík	není relevantní
Doprava	Letecká	Koordinační krizová jednotka pro evropské letectví (EACCC)
	Železniční	není relevantní

	Vodní	Evropská agentura pro kontrolu rybolovu (EFCA) Systém Unie pro výměnu informací na moři (SafeSeaNet, SSN) Integrované námořní služby (IMS) Datové centrum pro identifikaci a sledování lodí na velké vzdálenosti (LRIT) Služby námořní podpory agentury EMSA
	Silniční	není relevantní
	Horizontální	Síť kontaktních míst pro dopravu zřízená Plánem pro mimořádné situace v dopravě (COM(2022) 211)
Bankovnictví		EU-SCICF
Infrastruktura finančních trhů		EU-SCICF Evropský mechanismus finanční stabilizace

Zdravotnictví		Systém včasného varování a reakce (EWRS) Nástroj pro činnosti při mimořádných situacích v oblasti zdraví (HEOF) Systém rychlého varování pro tkáňové, buněčné a krevní složky (RATC/RAB) Rámec pro mimořádné situace v oblasti veřejného zdraví Systém rychlého varování před chemickými incidenty (RASCHEM) Evropský portál pro dozor nad infekčními nemocemi Úřad pro připravenost a reakci na mimořádné situace v oblasti zdraví (HERA) Systém pro zpravodajské informace z oblasti zdravotnictví (MediSys) Výkonná řídící skupina pro nedostatek zdravotnických prostředků (MDSSG) Rychlé varování v oblasti farmakovigilance Pracovní skupina EU pro oblast zdraví (EUHTF) Výbor pro zdravotní bezpečnost

Pitná voda		není relevantní
Odpadní voda		není relevantní
Digitální infrastruktura		není relevantní
Řízení služeb IKT		není relevantní
Veřejná správa		není relevantní
Vesmír		Architektura reakce na kosmické hrozby (STRA)
Poštovní a kurýrní služby		není relevantní
Nakládání s odpady		není relevantní
Výroba, produkce a distribuce chemických látek		Systém rychlého varování před chemickými incidenty (RASCHEM)

Výroba, zpracování a distribuce potravin		Evropský systém monitorování plodin Globální systém odhalování anomálií v zemědělské produkci (ASAP) Evropská síť informačních systémů v oblasti zdraví rostlin (EUROPHYT) Nouzový veterinární tým EU (EUVET) Systém včasné výměny informací pro potraviny a krmiva (RASFF) Evropský mechanismus připravenosti a reakce na krize v oblasti potravinového zabezpečení (EFSCM) Akt pro odolnost a mimořádné situace na vnitřním trhu (IMERA)
Výroba	Zdravotnické prostředky	není relevantní
	Počítače a elektronické a optické přístroje a zařízení	není relevantní
	Stroje a zařízení	není relevantní
	Výroba motorových vozidel, přívěsů a návěsů	není relevantní
	Výroba ostatních dopravních prostředků a zařízení	není relevantní

Digitální poskytovatelé		není relevantní
Výzkum		není relevantní

Příloha III – Rámec EU pro řešení kybernetických bezpečnostních krizí a související nástroje

Od roku 2017 Unie pracuje na svém rámci kybernetické bezpečnosti skládajícím se z několika nástrojů, které obsahují ustanovení týkající se řešení kybernetických bezpečnostních krizí:

- Nařízení Evropského parlamentu a Rady (EU) 2019/881[1],
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555[2],
- Prováděcí nařízení Komise 2024/2690[3], nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841[4],
- Nařízení Evropského parlamentu a Rady (EU) 2021/887[5],
- Nařízení Evropského parlamentu a Rady (EU) 2024/2847[6] a
- nařízení Evropského parlamentu a Rady (EU) 2025/38 (nařízení o kybernetické solidaritě)[7].

Mezi konkrétní odvětvová opatření týkající se kybernetických bezpečnostních krizí patří nařízení Komise v přenesené pravomoci (EU) 2024/1366[8] a připravovaný rámec pro koordinaci v případě systémových kybernetických bezpečnostních incidentů (EU-SCICF) v kontextu nařízení Evropského parlamentu a Rady (EU) 2022/2554[9].

Směrnice 2013/40[10] poskytuje odkaz na definici trestné činnosti související s kybernetickými útoky a unijní pravidla pro přeshraniční přístup k elektronickým důkazům, zejména nařízení Evropského parlamentu a Rady (EU) 2023/1543[11], po svém provedení výrazně usnadní činnost související s vymáháním práva v této oblasti.

Politika kybernetické obrany EU[12] popisuje úlohu sítě EU pro vojenské týmy pro reakci na počítačové hrozby (dále jen „síť MICNET“) a konference velitelů kybernetických sil EU a předpokládá zřízení koordinačního střediska EU pro kybernetickou obranu (dále jen „EUCDCC“).

V některých kritických odvětvích uvedených v přílohách I a II směrnice (EU) 2022/2555 existují další mechanismy vytváření situačního povědomí a reakce na krize, které nesouvisejí s kybernetickou problematikou.

„Doporučení Rady o plánu pro koordinaci reakce na úrovni Unie na narušení kritické infrastruktury se značným přeshraničním významem“[13] stanoví spolupráci mezi příslušnými aktéry v případech, kdy incident ovlivňuje jak fyzické aspekty, tak kybernetickou bezpečnost kritické infrastruktury.

[1] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru, (OJ L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. prosince 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie (Úř. věst. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (Úř. věst. L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Nařízení Evropského parlamentu a Rady (EU) 2025/38 ze dne 19. prosince 2024, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě) (Úř. věst. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Nařízení Komise v přenesené pravomoci (EU) 2024/1366 ze dne 11. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2019/943 zavedením kodexu sítě pro odvětvová pravidla pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny (Úř. věst. L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení a směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení (Úř. věst. 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/CS/TXT/PDF/?uri=CELEX:52022JC0049

[13] *Úř. věst. C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:C_202404371