Rada
Evropské unie

Brusel 7. září 2023
(OR. en)

12485/23
ADD 1

Interinstitucionální spis:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	6. září 2023
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2023) 526 final
Předmět:	PŘÍLOHA návrhu DOPORUČENÍ RADY o plánu pro koordinaci reakce na úrovni Unie na narušení kritické infrastruktury se značným přeshraničním významem

Delegace naleznou v příloze dokument COM(2023) 526 final.

Příloha: COM(2023) 526 final

EVROPSKÁ
KOMISE

V Bruselu dne 6.9.2023
COM(2023) 526 final

ANNEX

PŘÍLOHA

Návrh DOPORUČENÍ RADY

o plánu pro koordinaci reakce na úrovni Unie na narušení kritické infrastruktury se značným přeshraničním významem

PŘÍLOHA

Tato příloha popisuje zásady, cíle, hlavní aktéry, součinnost se stávajícími mechanismy reakce na krize a fungování plánu pro koordinaci reakce na významné incidenty v oblasti kritické infrastruktury (dále jen „plán pro kritickou infrastrukturu“) a zlepšení spolupráce mezi členskými státy a příslušnými orgány, institucemi a jinými subjekty Unie, pokud jde o tyto události, v souladu s platnými pravidly a postupy. Tímto plánem není nijak dotčena úloha a fungování jiných opatření.

ČÁST I: CÍLE, ZÁSADY, AKTÉŘI A DALŠÍ NÁSTROJE

1. Cíle

Plán pro kritickou infrastrukturu se zaměřuje na dosažení následujících tří hlavních cílů v reakci na významný incident v oblasti kritické infrastruktury:

a) **Sdílení informací o situaci**, neboť pro vhodnou koordinovanou reakci je nezbytné dobře porozumět významnému incidentu v oblasti kritické infrastruktury v členských státech, jeho původu a možným důsledkům pro všechny příslušné zúčastněné strany na provozní a strategické/politické úrovni.

b) **Koordinovaná komunikace s veřejností**, protože pomáhá zmírnit negativní dopady významného incidentu v oblasti kritické infrastruktury a minimalizovat nesrovnalosti ve sděleních předávaných veřejnosti v členských státech a mezi nimi. Jasná komunikace s veřejností je rovněž důležitá pro zmírnění následků dezinformací.

c) **Účinná reakce**, neboť posílení reakce členských států a spolupráce mezi členskými státy a s příslušnými orgány, institucemi, úřady a jinými subjekty Unie přispěje ke zmírnění dopadů významného incidentu v oblasti kritické infrastruktury a umožní rychlé obnovení základních služeb způsobem, který minimalizuje zranitelnost vůči dalším významným incidentům.

2. Zásady

Proporcionalita

Incidenty, které narušují kritickou infrastrukturu a/nebo poskytování základních služeb, často nesplňují kritérium významného incidentu v oblasti kritické infrastruktury, jak je uvedeno v bodě 2 tohoto doporučení. Jako takové je lze v zásadě účinně řešit na vnitrostátní úrovni. Proto se použití plánu pro kritickou infrastrukturu omezuje pouze na významné incidenty v oblasti kritické infrastruktury.

Subsidiarita

Hlavní odpovědnost za reakci na narušení kritické infrastruktury nebo základních služeb poskytovaných kritickými subjekty nesou v souladu s právem Unie členské státy. V případě významného incidentu v oblasti kritické infrastruktury se značným přeshraničním významem však plní důležitou doplňkovou úlohu také příslušné orgány, instituce a jiné subjekty Unie a Evropská služba pro vnější činnost (dále jen „ESVČ“), neboť takový incident může mít dopad na několik nebo dokonce na všechny oblasti hospodářské činnosti v rámci vnitřního trhu, na život občanů žijících v Unii, na bezpečnost a na mezinárodní vztahy Unie.

Doplňkovost

Plán pro kritickou infrastrukturu zohledňuje a odráží fungování stávajících mechanismů pro řešení krizí na úrovni Unie, konkrétně opatření Rady pro integrovanou politickou reakci na

krize (dále jen „IPCR“), vnitřní proces Komise pro koordinaci v krizových situacích, který je součástí systému ARGUS, mechanismus civilní ochrany Unie, a to za podpory Střediska pro koordinaci odezvy na mimořádné události (dále jen „ERCC“), a mechanismu ESVČ pro reakce na krize. Vychází rovněž z odvětvových opatření, včetně ustanovení o koordinovaném řešení rozsáhlých kybernetických bezpečnostních incidentů stanovených směrnicí Evropského parlamentu a Rady (EU) 2022/2555[1] a rámce stanoveného v Plánu koordinované reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize (dále jen „plán pro kybernetické incidenty“)[2], sítě kontaktních míst pro dopravu[3] a koordinační krizové jednotky pro evropské letectví[4].

Plán pro kritickou infrastrukturu dále vychází ze struktur a mechanismů stanovených směrnicí Evropského parlamentu a Rady (EU) 2022/2557[5], zejména pokud jde o spolupráci mezi příslušnými orgány a s Komisí a ve skupině pro odolnost kritických subjektů, a má být používán v souladu s nimi. Zohledňuje rovněž povinnosti příslušných orgánů, institucí a jiných subjektů Unie podle právního rámce, který se na ně vztahuje. Činnosti v oblasti reakce na krize kritické infrastruktury doplňují další mechanismy pro řešení krizí na úrovni Unie a na vnitrostátní a odvětvové úrovni, které podporují koordinaci více odvětví.

Důvěrnost informací

Plán pro kritickou infrastrukturu zohledňuje význam ochrany důvěrnosti utajovaných a citlivých neutajovaných informací týkajících se kritické infrastruktury a kritických subjektů.

3. Příslušní aktéři

Všechny členské státy a příslušné orgány, instituce a jiné subjekty Unie uvedené v písmenech a) až e) níže rozhodnou v souladu s pravidly a postupy, které se na ně vztahují, o příslušném aktérovi či aktérech pro každý významný incident v oblasti kritické infrastruktury v závislosti na dotčeném odvětví či odvětvích a typu incidentu.

a) členské státy

– příslušné orgány (např. orgány odpovědné za kritickou infrastrukturu, příslušné odvětvové orgány, jednotná kontaktní místa určená nebo zřízená podle čl. 9 odst. 2 směrnice (EU) 2022/2557, orgány určené nebo zřízené podle čl. 9 odst. 1 směrnice (EU) 2022/2557),

– případně Evropská síť styčných organizací pro řešení kybernetických krizí („EU-CyCLONe“), jak je uvedeno v článku 16 směrnice (EU) 2022/2555,

– skupina pro spolupráci podle článku 14 směrnice (EU) 2022/2555,

– případně další zúčastněné strany, včetně subjektů nebo osob ze soukromého sektoru, jako jsou provozovatelé kritické infrastruktury, včetně těch, které byly označeny za kritické subjekty,

[1] 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 (Úř. věst. L 333, 27.12.2022, s. 80).

[2] 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).

[3] Sdělení Komise – Plán pro mimořádné situace v dopravě (COM/2022/211 final).

[4] Zřízeny podle článku 19 prováděcího nařízení Komise (EU) 2019/123 ze dne 24. ledna 2019, kterým se stanoví prováděcí pravidla pro funkce sítě uspořádání letového provozu (ATM).

[5] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L 333, 27.12.2022, s. 164).

– ministři odpovědní za odolnost kritické infrastruktury a/nebo ministr či ministři odpovědní za odvětví, která jsou danou významnou událostí v kritické infrastruktuře nejvíce postižena.

b) Rada

– rotující předsednictví,

– příslušné pracovní skupiny, jako je Pracovní skupina pro civilní ochranu včetně podskupiny pro odolnost kritických subjektů (PROCIV-CER), a předseda (předsedové) příslušné pracovní skupiny (příslušných pracovních skupin) v závislosti na dotčeném odvětví (dotčených odvětvích) a povaze incidentu, jako je Horizontální pracovní skupina pro otázky týkající se kybernetiky a Horizontální pracovní skupina pro posílení odolnosti a boj s hybridními hrozbami,

– výbor COREPER, Politický a bezpečnostní výbor a IPCR, které podporuje generální sekretariát Rady.

c) Komise, včetně odborných skupin Komise

– určený vedoucí útvar (v závislosti na dotčeném odvětví) podporovaný střediskem ERCC jakožto operačním střediskem s nepřetržitým provozem, které řídí reakce na krize, a Generálním ředitelstvím pro migraci a vnitřní věci jako útvarem odpovědným v dané oblasti a v případě meziodvětvové události Generálním ředitelstvím pro migraci a vnitřní věci a dalšími příslušnými útvary Komise,

– Generální ředitelství pro komunikaci a útvar mluvčího,

– Generální ředitelství – Úřad pro připravenost a reakci na mimořádné situace v oblasti zdraví,

– skupina pro odolnost kritických subjektů, které předsedá zástupce Komise (Generální ředitelství pro migraci a vnitřní věci), zřízená směrnicí (EU) 2022/2557, a případně další příslušné odborné skupiny a výbory,

– středisko ERCC zřízené v rámci mechanismu civilní ochrany Unie rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU[6] (středisko s nepřetržitým provozem pro řešení mimořádných událostí v rámci mechanismu civilní ochrany Unie při Generálním ředitelství pro evropskou civilní ochranu a operace humanitární pomoci),

– skupina pro spolupráci podle článku 14 směrnice (EU) 2022/2555,

– středisko pro informování o situaci a analýzu v kybernetické oblasti,

– Výbor pro zdravotní bezpečnost podle článku 4 nařízení (EU) 2022/2371[7],

– generální sekretariát Komise (sekretariát systému ARGUS) a generální tajemník (příp. jeho zástupce) (postup v rámci systému ARGUS), Generální ředitelství pro lidské zdroje (ředitelství pro bezpečnost),

– další příslušné skupiny odborníků Komise, které jí pomáhají při koordinaci opatření v mimořádných nebo krizových situacích,

---

[6] 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).

[7] Nařízení Evropského parlamentu a Rady (EU) 2022/2371 ze dne 23. listopadu 2022 o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU (Úř. věst. L 314, 6.12.2022, s. 26).

– další sítě krizového řízení, včetně odvětvových (např. síť kontaktních míst pro dopravu řízená Generálním ředitelstvím pro mobilitu a dopravu, interinstitucionální pracovní skupina pro řešení kybernetických krizí[8], koordinační krizová jednotka pro evropské letectví),

– předseda a/nebo příslušný místopředseda/člen Komise.

d) ESVČ

– společná zpravodajsko-analytická složka („SIAC“), kterou tvoří Středisko pro analýzu zpravodajských informací („IntCen“) a zpravodajské ředitelství Vojenského štábu EU („EUMS Int“),

– středisko pro reakci na krize („CRC“),

– vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku / místopředseda Komise.

e) příslušné instituce a jiné subjekty Unie a příslušné agentury Unie, jako je Europol, v závislosti na dotčeném odvětví (dotčených odvětvích)[9].

4. Součinnost s dalšími příslušnými mechanismy a nástroji pro řešení krizí

Plán pro kritickou infrastrukturu je flexibilní nástroj, který mapuje různá opatření, jež by mohla být částečně nebo plně přijata s využitím různých stávajících opatření v závislosti na povaze a závažnosti významného incidentu v oblasti kritické infrastruktury a na potřebě provozní, strategické a politické koordinace.

a) Protokol EU o boji proti hybridním hrozbám[10] (dále jen „protokol EU“)

Protokol EU se vztahuje na případy hybridních hrozeb[11] a uvádí přehled postupů a nástrojů použitelných v případě takových hrozeb nebo kampaní.

V případě významného incidentu v oblasti kritické infrastruktury s hybridním rozměrem se protokol EU ve vhodných případech použije jako doplněk k plánu pro kritickou infrastrukturu, např. pokud jde o konkrétní informace, analýzu nebo komunikaci o hybridních aspektech významného incidentu v oblasti kritické infrastruktury a o spolupráci s vnějšími partnery.

---

[8] Neformální skupina zahrnující příslušné útvary Komise, ESVČ, Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA), skupinu CERT-EU a agenturu Europol, které spolupředsedají Generální ředitelství pro komunikační sítě, obsah a technologie a ESVČ.

[9] Jako je Europol; pro dopravu: Agentura Evropské unie pro bezpečnost letectví (EASA), Evropská agentura pro námořní bezpečnost (EMSA), Evropská agentura pro železnice (ERA); pro zdravotnictví: Evropské středisko pro prevenci a kontrolu nemocí (ECDC) a Evropská agentura pro léčivé přípravky (EMA); pro energetiku: Agentura pro spolupráci energetických regulačních orgánů (ACER); pro kosmické odvětví: Agentura EU pro kosmický program (EUSPA); pro potravinářské odvětví Evropský úřad pro bezpečnost potravin (EFSA); na moři: Evropská agentura pro kontrolu rybolovu (EFCA); v případě kybernetických incidentů: Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), týmy pro reakce na počítačové bezpečnostní incidenty (CSIRT), skupina pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-UE).

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

[11] Hybridní hrozby lze charakterizovat jako kombinaci nátlakových a podvratných činností a konvenčních i nekonvenčních metod, které mohou státní nebo nestátní aktéři koordinovaným způsobem využívat k dosažení konkrétních cílů, aniž by formálně vyhlásili válku, viz Protokol EU o hybridních hrozbách.

b) Plán koordinované reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize

Kybernetický plán se týká rozsáhlých přeshraničních incidentů, které způsobují narušení příliš rozsáhlé na to, aby je dotčený členský stát zvládnul sám, nebo které postihly více než jeden členský stát nebo orgán EU a jejichž dopad technického nebo politického významu je natolik rozsáhlý a významný, že vyžadují včasnou koordinaci politik a reakci na politické úrovni Unie.

V případě závažného incidentu v oblasti kritické infrastruktury, který se časově shoduje s rozsáhlým kybernetickým bezpečnostním incidentem nebo se zdá, že s ním souvisí, příslušné pracovní skupiny Rady stanoví vhodnou koordinaci na provozní úrovni, a to i se sítí EU-CyCLONe, nebo v rámci společného zasedání skupiny pro odolnost kritických subjektů se skupinou pro spolupráci. Účelem koordinace je určit, který subjekt, nástroj (nástroje) nebo mechanismus (mechanismy) by mohl/y co nejúčinněji přispět k reakci na významný incident v oblasti kritické infrastruktury, přičemž je třeba zabránit zdvojování a souběžným činnostem.

c) Mechanismus civilní ochrany Unie a Středisko pro koordinaci odezvy na mimořádné události

Operativní reakce v rámci mechanismu civilní ochrany Unie na aktuální nebo hrozící přírodní katastrofy a katastrofy způsobené člověkem (včetně katastrof zahrnujících narušení kritické infrastruktury) v Unii i mimo ni řídí v souladu s rozhodnutím č. 1313/2013/EU o mechanismu civilní ochrany Unie středisko ERCC, což je jediné operační středisko Komise s nepřetržitým provozem, které řídí reakce na krize. V takových případech může středisko ERCC poskytovat včasné varování, oznámení, provádět analýzy a podporovat sdílení informací a v případě aktivace mechanismu civilní ochrany Unie členským státem i vysílat operativní pomoc a odborníky do postižených oblastí. Kromě toho může středisko ERCC usnadňovat odvětvovou a meziodvětvovou koordinaci jak na úrovni Unie, tak mezi Unií a příslušnými vnitrostátními orgány, včetně orgánů odpovědných za civilní ochranu a odolnost kritické infrastruktury.

d) Další odvětvové nebo meziodvětvové mechanismy a nástroje

Plán pro kritickou infrastrukturu nezdvojuje jiné odvětvové nebo meziodvětvové nástroje pro řešení krizí nebo mechanismy koordinace. Pokud takové nástroje nebo mechanismy v dotčeném odvětví již existují, lze plán pro kritickou infrastrukturu v rámci jeho působnosti použít jako doplňkový nástroj k odvětvovým nebo meziodvětvovým nástrojům nebo mechanismům, který je však nenahrazuje. Aby se zabránilo zdvojování, bude třeba zajistit nezbytnou koordinaci mezi jednotlivými aktéry. Toho by mohlo být dosaženo například v rámci vnitřního procesu Komise pro koordinaci v krizových situacích, který je součástí systému ARGUS, za podpory střediska ERCC, a/nebo koordinačních schůzek IPCR.

ČÁST II: VÝMĚNA INFORMACÍ A KOORDINOVANÁ REAKCE

Níže popsaná opatření představují způsoby spolupráce, konkrétně výměnu informací, koordinovanou komunikaci a reakci. Tato struktura odpovídá způsobům fungování mechanismu krizové koordinace v rámci opatření IPCR zavedených Radou a v širším smyslu zohledňuje potenciální využití mechanismů krizové koordinace, které již na úrovni EU existují. Z této struktury je patrné, jak by se tyto způsoby spolupráce integrovaly, pokud by byly využity. Většinu těchto opatření však lze provádět i samostatně: na použití tohoto mechanismu nejsou závislá, ale spíše jej doplňují. Opatření jsou uvedena v chronologickém pořadí, přičemž se bere v úvahu, že v případě rozsáhlé krize, která představuje významný incident kritické infrastruktury, může být současně a průběžně prováděno několik opatření.

1. VÝMĚNA INFORMACÍ

a) Na provozní úrovni

Členské státy dotčené významným incidentem v oblasti kritické infrastruktury uplatňují svá vlastní pohotovostní opatření, zajišťují koordinaci s příslušnými vnitrostátními mechanismy pro řešení krizí a podle potřeby zapojují všechny příslušné vnitrostátní, regionální a místní subjekty.

Pokud jde o pomoc v oblasti civilní ochrany, koordinace mezi členskými státy a s Komisí je v případě potřeby zajištěna prostřednictvím střediska ERCC v rámci mechanismu civilní ochrany Unie

i) Sdílení informací a jejich oznamování příslušnými vnitrostátními orgány

Kromě oznamovací a informační povinnosti podle článku 15 směrnice (EU) 2022/2557 sdílejí příslušné vnitrostátní orgány odpovědné za kritickou infrastrukturu v členských státech dotčených významným incidentem v oblasti kritické infrastruktury prostřednictvím svých jednotných kontaktních míst a bez zbytečného odkladu s rotujícím předsednictvím Rady a Komisí příslušné informace, které obdržely od provozovatele (provozovatelů) kritické infrastruktury, kritických subjektů nebo z jiných zdrojů, jakož i informace týkající se mechanismů pro řešení krizí, které byly aktivovány. Pokud jde o Komisi, středisko ERCC zajišťuje nepřetržitý operační kontakt a kapacitu a koordinuje, sleduje a podporuje reakci na mimořádné události na úrovni Unie v reálném čase, přičemž slouží členským státům a Komisi jako operační centrum pro reakci na krizi a podporuje meziodvětvový přístup ke zvládání katastrof.

Takové sdílení informací se týká povahy významného incidentu v oblasti kritické infrastruktury, jeho příčiny, zjištěného či odhadovaného dopadu narušení na kritickou infrastrukturu a poskytování základních služeb, následků incidentu napříč odvětvími a hranicemi a opatření ke zmírnění následků, ať již přijatých nebo plánovaných, na vnitrostátní úrovni nebo s příslušnými dalšími členskými státy a Komisí prostřednictvím stávajících ujednání, např. ujednání o sdílení informací podle článků 9 a 15 směrnice (EU) 2022/2557. Toto oznámení je poskytováno, aniž by odvádělo zdroje kritické infrastruktury nebo v některých případech zdroje kritického subjektu nebo členského státu od činností souvisejících s řešením incidentu, které mají mít přednost.

Za účelem zajištění následných opatření informuje středisko ERCC nebo oznámené útvary Komise odpovědné za odvětví, v němž došlo k významnému incidentu v oblasti kritické infrastruktury, kontaktní místo na Generálním ředitelství pro migraci a vnitřní věci a Generální sekretariát Evropské komise. Mezitím středisko ERCC zahájí sledování dění, pokud již nebylo zahájeno, zejména v případě, že jeden nebo více dotčených členských států aktivuje mechanismus civilní ochrany Unie.

Mohou-li být informace relevantní pro řešení rozměru kybernetické bezpečnosti nebo souvisejí-li s kybernetickým bezpečnostním incidentem, sdílí Komise příslušné informace se sítí EU-CyCLONe.

Příslušné vnitrostátní orgány podle směrnice (EU) 2022/2557 bez zbytečného odkladu spolupracují a vyměňují si informace s příslušnými orgány podle směrnice (EU) 2022/2555, pokud jde o kybernetické incidenty a incidenty, které mají vliv na kritické subjekty, včetně kybernetických bezpečnostních a fyzických opatření přijatých kritickými subjekty.

V námořní oblasti příslušné vnitrostátní orgány zváží možnost využívat společné prostředí pro sdílení informací („CISE“) ke sdílení informací bez zbytečného prodlení.

ii) Organizace setkání odborníků

Komise co nejdříve svolá skupinu pro odolnost kritických subjektů s cílem usnadnit výměnu relevantních informací mezi příslušnými vnitrostátními orgány odpovědnými za kritickou infrastrukturu a příslušnými institucemi, orgány a jinými subjekty Unie týkajících se incidentu (povaha, příčina, dopad a důsledky napříč odvětvími a hranicemi) a opatření v oblasti reakce, včetně zmírňujících opatření a technické podpory dotčeným členským státům. V závislosti na těžišti incidentu budou příslušné útvary Komise úzce zapojeny do zasedání skupiny pro odolnost kritických subjektů s cílem sdílet informace shromážděné prostřednictvím stávajících odvětvových nástrojů. V případě incidentů, u nichž dochází ke kombinaci aspektů kybernetické bezpečnosti a fyzických nekybernetických aspektů, příslušné útvary Komise, skupina CERT-EU a případně ESVČ co nejdříve informují a konzultují pracovní skupinu pro řešení kybernetických krizí, jakož i příslušné předsedy skupiny pro spolupráci podle článku 14 směrnice (EU) 2022/2555 a případně síť EU-CyCLONe, o potřebě koordinačních činností. Po dohodě s příslušnými předsedy může Komise (Generální ředitelství pro migraci a vnitřní věci a Generální ředitelství pro komunikační sítě, obsah a technologie) navrhnout společné zasedání skupiny pro odolnost kritických subjektů se skupinou pro spolupráci s cílem sdílet informace o situaci a koordinovat příslušné reakce.

V případě významného meziodvětvového incidentu v kritické infrastruktuře, který vyžaduje nebo pravděpodobně bude vyžadovat zvládání následků na úrovni Unie, může Komise svolat meziodvětvové koordinační schůzky za účasti všech příslušných zúčastněných stran.

V případě, že jsou významným incidentem v oblasti kritické infrastruktury dotčeny i třetí zemi, Komise konzultuje příslušný orgán dotčené třetí země a může jej pozvat na zasedání skupiny pro odolnost kritických subjektů.

iii) Podpora ze strany Komise a agentur Unie

V případě potřeby a v souladu se svým mandátem předkládá agentura Europol na úrovni Unie situační zprávu o incidentu. Ostatní agentury Unie, je-li to vhodné a jednají-li v souladu se svými mandáty, podávají příslušné informace, které přispívají k informovanosti o situaci nebo ke koordinované reakci na významný incident v oblasti kritické infrastruktury, svým příslušným „mateřským“ generálním ředitelstvím, která následně podávají zprávy Komisi (Generální ředitelství pro migraci a vnitřní věci jako předsedající skupině pro odolnost kritických subjektů).

Komise může přispět k situačnímu povědomí s využitím prostředků vesmírného programu Unie[12], jako jsou program Copernicus, systém Galileo a služba EGNOS, je-li to vhodné a v souladu s platným právním rámcem.

b) Na strategické úrovni

i) Vypracovávání zpráv pro zajištění informovanosti o situaci

Na základě informací sdílených příslušnými vnitrostátními orgány na zasedání skupiny pro odolnost kritických subjektů nebo na společných zasedáních s příslušnými útvary, skupinami odborníků nebo sítěmi vypracuje Komise zprávu pro zajištění informovanosti o situaci, která vychází z příspěvků příslušných vnitrostátních orgánů a dalších dostupných informací.

Tato zpráva ve vhodných případech zohlední výsledky příslušných posouzení rizik, hodnocení a scénářů na úrovni EU z hlediska kybernetické bezpečnosti, včetně těch, které byly

[12] Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU (Úř. věst. L 170, 12.5.2021, s. 69).

provedeny Komisí, vysokým představitelem Unie pro zahraniční věci a bezpečnostní politiku a skupinou pro spolupráci.

V případě aktivace opatření IPCR může tato zpráva být přínosem pro analýzu integrovaného situačního povědomí („ISAA“), kterou připravují útvary Komise a ESVČ.

V případě potřeby předkládá složka SIAC aktuální posouzení incidentu založené na zpravodajských informacích.

ii) Aktivace mechanismů krizové koordinace Unie a využívání nástrojů Unie

Středisko ERCC začne v případě potřeby poskytovat podporu pro zajištění informovanosti o situaci ve vztahu k incidentu, zejména pokud incident vyvolá aktivaci mechanismu civilní ochrany Unie[13]. Kromě toho mohou dotčené členské státy požádat o satelitní snímky svého území prostřednictvím služby programu Copernicus pro podporu krizového řízení.

V případech, kdy je sdílení informací mezi Komisí, ESVČ a příslušnými agenturami Unie považováno za vhodné, aktivuje vedoucí generální ředitelství nebo Generální ředitelství pro migraci a vnitřní věci v koordinaci s generálním sekretariátem fázi I vnitřního procesu Komise pro koordinaci v krizových situacích v rámci systému ARGUS tím, že v nástroji IT systému Argus otevře příslušnou událost.

Rotující předsednictví Rady Unie může aktivovat opatření IPCR v režimu sdílení informací, což znamená, že Komise a ESVČ vypracovávají zprávy ISAA s případným přispěním příslušných vnitrostátních orgánů a dalších zdrojů. Za určitých podmínek může rotující předsednictví Rady nebo Komise založit monitorovací stránku na internetové platformě IPCR i bez aktivace opatření IPCR.

Další (odvětvové) mechanismy a nástroje Unie pro řešení krizí mohou být podle potřeby aktivovány na základě příslušných postupů. Komise zajistí koordinaci těchto mechanismů a nástrojů.

Pokud se fyzický incident časově shoduje s rozsáhlým kybernetickým bezpečnostním incidentem, jak je definován v čl. 6 odst. 7 směrnice (EU) 2022/2555, nebo se zdá, že s ním souvisí, může rotující předsednictví Rady využít plán pro kybernetické incidenty k určení vhodné koordinace na provozní úrovni, do níž se zapojí mimo jiné síť EU CyCLONe a skupina pro odolnost kritických subjektů.

iii) Koordinace komunikace s veřejností

Členské státy dotčené významným incidentem v oblasti kritické infrastruktury v co největší míře koordinují svou komunikaci ohledně krize s veřejností, přičemž v tomto ohledu respektují vnitrostátní pravomoci. V případě potřeby může být zapojena síť IPCR pro krizovou komunikaci.

Na základě sdílení informací o situaci podporují skupina pro odolnost kritických subjektů a dotčené členské státy případné vytvoření schválených komunikačních kanálů pro veřejnost.

Na základě sdílení informací o situaci pak Europol a další příslušné agentury Unie koordinují své činnosti v oblasti komunikace s veřejností s útvarem mluvčího Komise.

Pokud má významný incident v oblasti kritické infrastruktury vnější či hybridní rozměr nebo rozměr týkající se společné bezpečnostní a obranné politiky, je komunikace s veřejností

[13] Například zveřejňování výstupů z monitorování médií, zpráv civilní ochrany, analytických souhrnných zpráv, denních map GŘ ECHO, denních bleskových zpráv GŘ ECHO a dalších individuálně přizpůsobených produktů.

koordinována ve spolupráci s ESVČ a útvarem mluvčího Komise v souladu s protokolem EU pro boj proti hybridním hrozbám[14].

2. REAKCE (ZAHRNUJÍCÍ PRŮBĚŽNÉ ČINNOSTI POPSANÉ V ČÁSTI VÝMĚNA INFORMACÍ A DALŠÍ ČINNOSTI NA STRATEGICKÉ/POLITICKÉ ÚROVNI)

a) Na strategické úrovni

i) Průběžné vypracovávání situačních zpráv

Podskupina pro odolnost kritických subjektů v rámci Pracovní skupiny Rady pro civilní ochranu (PROCIV-CER) je informována o vypracování politicko-strategické situační zprávy (např. zprávy ISAA v případě aktivace IPCR nebo sdílené situační zprávy vypracované Komisí) a připravuje zasedání výboru COREPER, pokud tento výbor ještě nebyl svolán, případně zasedání Politického a bezpečnostního výboru.

Složka SIAC zintenzivňuje kontakt se zpravodajskými službami členských států, shromažďuje informace ze všech zdrojů a připravuje analýzu a posouzení incidentu a v případě potřeby i pravidelné aktualizace.

ii) Plná aktivace mechanismů krizové koordinace Unie a využívání nástrojů Unie

V případě, že předseda Komise aktivuje fázi II vnitřního procesu Komise pro koordinaci v krizových situacích, který je součástí systému ARGUS, svolá se v krátkém termínu zasedání krizového koordinačního výboru za účasti příslušných útvarů Komise, agentur a případně ESVČ s cílem zajistit koordinaci všech aspektů významného incidentu v oblasti kritické infrastruktury.

V případě, že předsednictví Rady aktivuje IPCR v plném režimu:

– Rotující předsednictví Rady vyzve k včasnému uspořádání neformálního jednání u kulatého stolu, jehož by se zúčastnili příslušní vnitrostátní, evropští a mezinárodní aktéři a na němž by zástupce Komise, který předsedá skupině pro odolnost kritických subjektů (Generální ředitelství pro migraci a vnitřní věci), mohl podat zprávu o dříve svolaném jednání skupiny (skupin), kterou by případně doplnily další útvary Komise a ESVČ.

– Složka SIAC a příslušné agentury Unie mohou být vyzvány, aby na tomto zasedání předložily aktuální informace o situaci v souvislosti s významným incidentem v oblasti kritické infrastruktury.

Zprávu ISAA připravuje vedoucí útvar (vedoucí útvar Komise nebo ESVČ) za přispění příslušných útvarů Komise, příslušných úřadů, orgánů a jiných subjektů Unie a příslušných vnitrostátních orgánů. Členské státy se vyzývají, aby prostřednictvím internetové platformy IPCR poskytly podklady pro vypracování zpráv ISAA.

V případě významného incidentu v oblasti kritické infrastruktury s mezinárodním bezpečnostním významem mohou útvary Komise a ESVČ svolat zasedání strukturovaného dialogu mezi EU a NATO o odolnosti, aby přispěly ke sdílení informací o situaci a k výměně informací o opatřeních přijatých Unií, respektive NATO.

iii) Komunikace s veřejností

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

Rada připravuje společná sdělení pro veřejnost. Tuto činnost může podpořit neformální síť krizových komunikátorů vytvořená v rámci IPCR. Sdělení pro veřejnost připravuje podle potřeby také útvar tiskového mluvčího Komise.

Pokud má významný incident v oblasti kritické infrastruktury vnější či hybridní rozměr nebo rozměr týkající se společné bezpečnostní a obranné politiky, je komunikace s veřejností koordinována ve spolupráci s ESVČ a útvarem mluvčího Komise.

iv) Podpora členským státům a účinná reakce

Rotující předsednictví může svolat zasedání podskupiny PROCIV-CER na podporu činností v rámci IPCR, jsou-li tato opatření aktivována.

Členské státy dotčené významným incidentem v oblasti kritické infrastruktury mohou prostřednictvím skupiny pro odolnost kritických subjektů požádat jiné členské státy nebo příslušné orgány, instituce a jiné subjekty Unie o technickou podporu, např. o specifické odborné poradenství s cílem zmírnit nepříznivé dopady významného incidentu v oblasti kritické infrastruktury.

Členské státy dotčené významným incidentem v oblasti kritické infrastruktury mohou rovněž požádat o technickou a/nebo finanční podporu ze strany Komise nebo příslušných agentur Unie. Komise v koordinaci s příslušnými agenturami Unie posoudí možnosti své podpory a případně aktivuje technická opatření ke zmírnění dopadů na úrovni Unie v souladu s jejich příslušnými postupy a koordinuje technické kapacity potřebné k tomu, aby se dopad významného incidentu v oblasti kritické infrastruktury podařilo odvrátit nebo zmírnit.

Konkrétně v rámci mechanismu civilní ochrany Unie by dotčené země mohly požádat o pomoc prostřednictvím společného komunikačního a informačního systému pro mimořádné události („CECIS“), načež by se středisko ERCC ujalo koordinace poskytování pomoci ze strany členských států a účastnických států mechanismu civilní ochrany Unie, jakož i prostřednictvím „rescEU“.

V rámci svých příslušných mandátů a na požádání podporuje členské státy dotčené významným incidentem v oblasti kritické infrastruktury při vyšetřování incidentu také Europol a další příslušné agentury Unie.

b) Na politické úrovni

Předsednictví Rady by mohlo zvážit nutnost svolat kulaté stoly IPCR, zasedání pracovních skupin Rady, výboru COREPER, Rady ministrů a/nebo vrcholné schůzky za účelem výměny informací o možném původu významného incidentu v oblasti kritické infrastruktury a jeho očekávaných důsledcích pro členské státy a Unii, dohodnout se na společných pokynech a přijmout nezbytná opatření na podporu členských států dotčených významným incidentem v oblasti kritické infrastruktury a zmírnění jeho dopadů.

Schéma 1: Schematický přehled plánu pro kritickou infrastrukturu

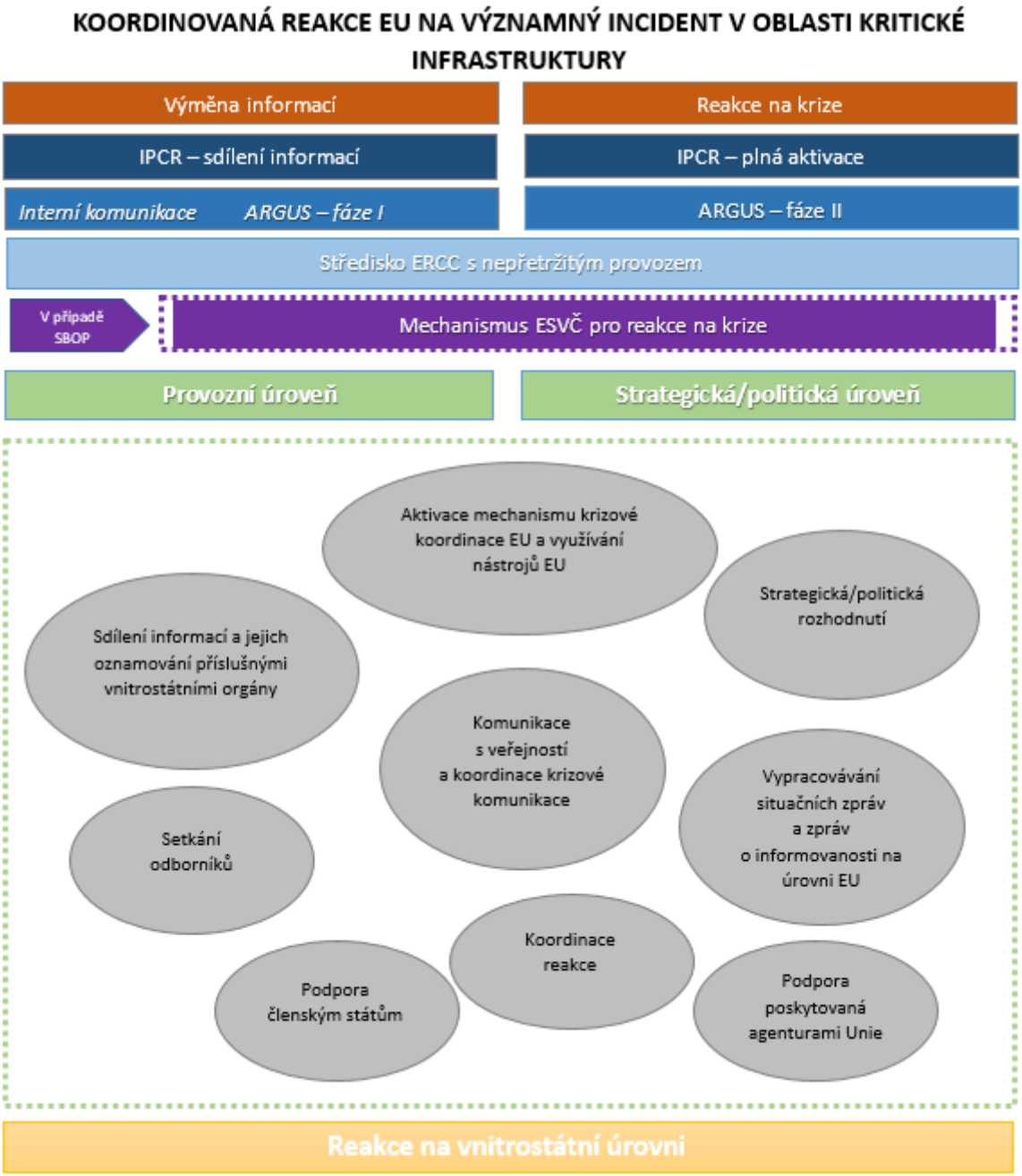
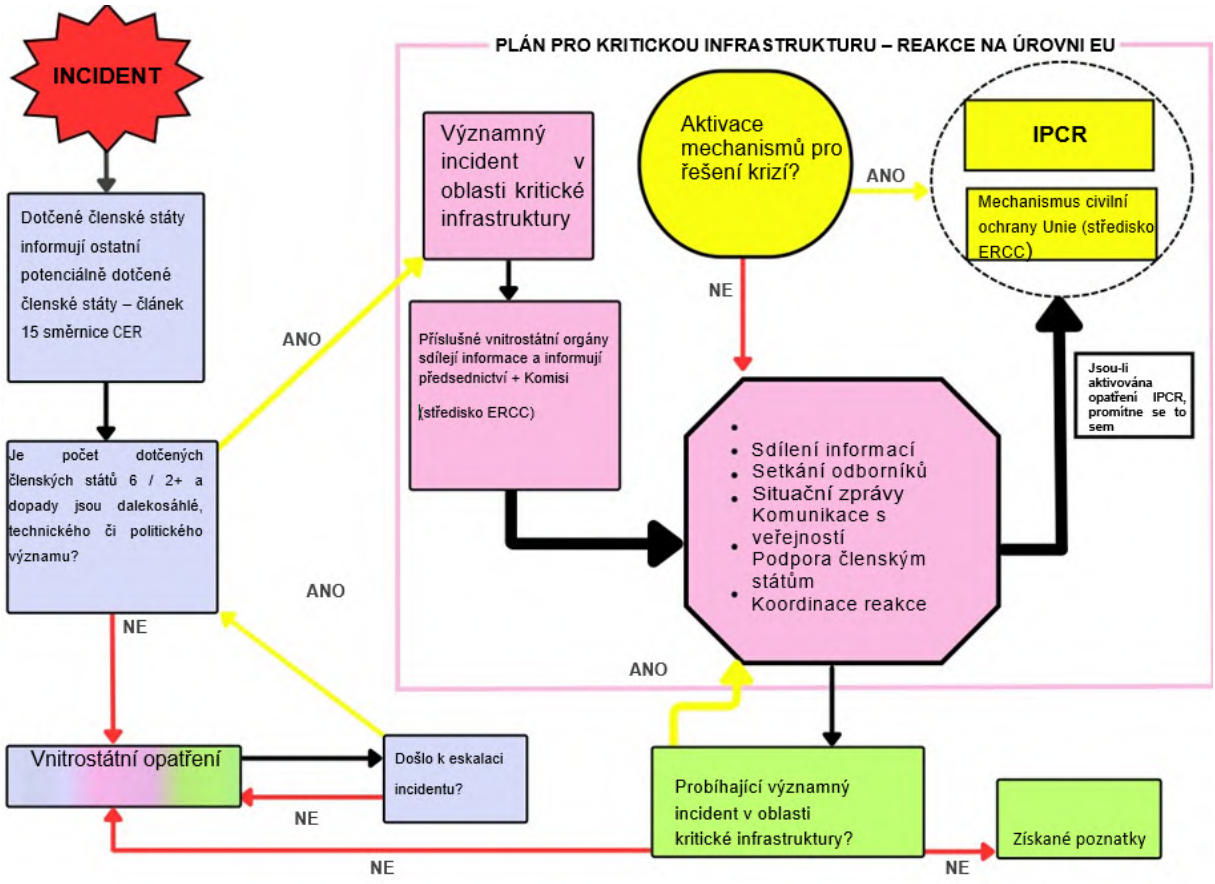


Schéma 2: Rozhodování v rámci plánu pro kritickou infrastrukturu



LEGENDA

- Fáze před použitím plánu
- Aktivace mechanismů pro řešení krizí
- V průběhu plánu
- Fáze po použití plánu