Eiropas Savienības
Padome

Briselē, 2023. gada 7. septembrī
(OR. en)

12485/23
ADD 1

Starpiestāžu lieta:
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**

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2023. gada 6. septembris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	COM(2023) 526 final
Temats:	PIELIKUMS dokumentam Priekšlikums PADOMES IETEIKUMAM par Plānu koordinētai Savienības līmeņa reaģēšanai uz kritiskās infrastruktūras ar būtisku pārrobežu nozīmi traucējumiem

Pielikumā ir pievienots dokuments COM(2023) 526 final.

Pielikumā: COM(2023) 526 final

EIROPAS
KOMISIJA

Briselē, 6.9.2023.
COM(2023) 526 final

ANNEX

PIELIKUMS

dokumentam

Priekšlikums PADOMES IETEIKUMAM

par Plānu koordinētai Savienības līmeņa reaģēšanai uz kritiskās infrastruktūras ar būtisku pārrobežu nozīmi traucējumiem

PIELIKUMS

Šajā pielikumā ir aprakstīti principi, mērķi, galvenie dalībnieki, mijiedarbība ar esošajiem krīzes reaģēšanas mehānismiem un tāda plāna ("Kritiskās infrastruktūras plāns") darbība, ko izmanto, lai reaģētu uz būtiskiem kritiskās infrastruktūras incidentiem un uzlabotu sadarbību starp dalībvalstīm un attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām attiecībā uz šādiem incidentiem, saskaņā ar piemērojamiem noteikumiem un procedūrām. Šis plāns nekādā veidā neietekmē citu pasākumu nozīmi un darbību.

I DAĻA. MĒRĶI, PRINCIPI, DALĪBNIEKI UN CITI INSTRUMENTI

1. Mērķi

Kritiskās infrastruktūras plāna mērķis reaģēšanā uz būtisku kritiskās infrastruktūras incidentu ir sasniegt šādus trīs galvenos mērķus:

(a) **kopīga situācijas apzināšanās**, jo laba izpratne par būtisko kritiskās infrastruktūras incidentu dalībvalstīs, tā izcelsmi un iespējamām sekām, ko tas rada visām attiecīgajām ieinteresētajām personām operatīvajā un stratēģiskajā/politiskajā līmenī, ir būtiska pienācīgā koordinētā reaģēšanā;

(b) **koordinēta sabiedrības informēšana**, jo tā palīdz mazināt būtiska kritiskās infrastruktūras incidenta negatīvo ietekmi un samazināt atšķirības vēstījumos, kas tiek sniegti sabiedrībai dalībvalstīs un starp tām. Skaidra sabiedrības informēšana ir svarīga arī dezinformācijas seku mazināšanā;

(c) **efektīva reaģēšana**, jo dalībvalstu reaģēšanas stiprināšana un sadarbība starp dalībvalstīm un ar attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām, palīdz mazināt būtiska kritiskās infrastruktūras incidenta ietekmi un ļauj ātri atjaunot pamatpakalpojumu sniegšanu tā, ka tiek mazināta neaizsargātība pret turpmākiem būtiskiem incidentiem.

2. Principi

Proporcionalitāte

Incidenti, kas traucē kritiskās infrastruktūras darbību un/vai pamatpakalpojumu sniegšanu, bieži vien ir zem būtiska kritiskās infrastruktūras incidenta robežvērtības, kas norādīta šā ieteikuma 2. punktā. Tāpēc tos principā var efektīvi risināt valsts līmenī. Tādējādi Kritiskās infrastruktūras plāna piemērošana attiecas tikai uz būtiskiem kritiskās infrastruktūras incidentiem.

Subsidiaritāte

Saskaņā ar Savienības tiesību aktiem dalībvalstis ir primāri atbildīgas par reaģēšanu uz traucējumiem kritiskās infrastruktūras darbībā vai kritisko vienību sniegtajos pamatpakalpojumos. Tomēr attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām un Eiropas Ārējās darbības dienestam (EĀDD) ir svarīga papildinoša nozīme tāda būtiska kritiskās infrastruktūras incidenta gadījumā, kam ir ievērojama pārrobežu nozīme, jo šāds incidents var ietekmēt vairākas vai pat visas saimnieciskās darbības jomas iekšējā tirgū, Savienībā dzīvojošo iedzīvotāju dzīvi, Savienības drošību un starptautiskās attiecības.

Papildināmība

Kritiskās infrastruktūras plānā ir ņemts vērā un atspoguļots darbs, ko Savienības līmenī veic esošie krīzes pārvarēšanas mehānismi, proti, Padomes integrētie krīzes situāciju politiskās

reaģēšanas (*IPCR*) mehānismi, Komisijas iekšējais krīzes koordinācijas process *ARGUS*, Savienības civilās aizsardzības mehānisms (*UCPM*), ko atbalsta Ārkārtas reaģēšanas koordinēšanas centrs (*ERCC*), un EĀDD mehānisms reaģēšanai krīzes situācijās. Tas ir arī izstrādāts, ņemot vērā nozaru pasākumus, tai skaitā noteikumus par plašapmēra kiberdrošības incidentu koordinētu pārvaldību, kas paredzēti Eiropas Parlamenta un Padomes Direktīvā (ES) 2022/2555[1], un satvaru, kurš izklāstīts Plānā, kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm ("Kiberdrošības plāns")[2], Transporta kontaktpunktu tīkls[3] un Eiropas aviācijas krīzes koordinācijas vienība[4].

Turklāt Kritiskās infrastruktūras plāns ir balstīts uz struktūrām un mehānismiem, kas izveidoti ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2022/2557[5], un tas ir jāpiemēro saskaņā ar tiem, jo īpaši attiecībā uz sadarbību starp kompetentajām iestādēm un ar Komisiju, kā arī Kritisko vienību noturības grupu. Tajā ir ņemti vērā arī attiecīgo Savienības iestāžu, struktūru, biroju un aģentūru pienākumi saskaņā ar tiem piemērojamo tiesisko regulējumu. Kritiskās infrastruktūras krīzes situācijās veicamās reaģēšanas darbības Savienības, valstu un nozaru līmenī papildina citus krīzes pārvarēšanas mehānismus, kuri atbalsta daudznozaru koordināciju.

Informācijas konfidencialitāte

Kritiskās infrastruktūras plānā ir ņemts vērā, ka svarīgi ir aizsargāt ar kritisko infrastruktūru un kritiskajām vienībām saistītās klasificētās un sensitīvās neklasificētās informācijas konfidencialitāti.

3. Iesaistītie dalībnieki

Katra dalībvalsts un attiecīgās Savienības iestādes, struktūras, biroji un aģentūras, kas minētas turpmāk a)–e) apakšpunktā, saskaņā ar tiem piemērojamiem noteikumiem un procedūru lems par saistīto(-ajiem) dalībnieku(-iem) katrā būtiskajā kritiskās infrastruktūras incidentā atkarībā no skartās(-ajām) nozares(-ēm) un incidenta veida.

a) Dalībvalstis

— Kompetentās iestādes (piemēram, par kritisko infrastruktūru atbildīgās iestādes, attiecīgās nozaru iestādes, vienotie kontaktpunkti, kas izraudzīti vai izveidoti saskaņā ar Direktīvas (ES) 2022/2557 9. panta 2. punktu, iestādes, kuras izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2557 9. panta 1. punktu),

— Attiecīgā gadījumā Eiropas Kiberkrīžu sadarbības organizāciju tīkls ("*EU-CyCLONe*"), kā minēts Direktīvas (ES) 2022/2555 16. pantā,

— Direktīvas (ES) 2022/2555 14. pantā minētā sadarbības grupa,

— Attiecīgā gadījumā citas ieinteresētās personas, tai skaitā vienības vai personas no privātā sektora, piemēram, kritiskās infrastruktūras operatori, tai skaitā tie, kas identificētas kā kritiskās vienības,

---

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (OV L 333, 27.12.2022., 80. lpp.).

[2] Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (OV L 239, 19.9.2017., 36. lpp.).

[3] Komisijas paziņojums "Ārkārtas rīcības plāns transporta nozarei" (COM(2022) 211 final).

[4] Izveidota saskaņā ar 19. pantu Komisijas Īstenošanas regulā (ES) 2019/123 (2019. gada 24. janvāris), ar ko nosaka sīki izstrādātus noteikumus gaisa satiksmes pārvaldības (*ATM*) tīkla funkciju īstenošanai.

[5] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un Padomes Direktīvas 2008/114/EK atcelšanu (OV L 333, 27.12.2022., 164. lpp.).

— Ministri, kas atbildīgi par kritiskās infrastruktūras noturību, un/vai ministrs(-i), kas ir atbildīgs(-i) par nozari vai nozarēm, kuras visvairāk ietekmējis attiecīgais būtiskais kritiskās infrastruktūras incidents.

b) Padome

— Rotējošā prezidentūra,

— Attiecīgās darba grupas, piemēram, Civilās aizsardzības jautājumu darba grupa, tai skaitā Kritisko vienību noturības apakšgrupa *PROCIV-CER*, un attiecīgās(-o) darba grupas(-u) priekšsēdētājs(-i) atkarībā no skartās(-ajām) nozares(-ām) un incidenta veida, piemēram, Kiberjautājumu horizontālā darba grupa un Horizontālā darba grupa noturības uzlabošanas un hibrīddraudu novēršanas jautājumos,

— Dalībvalstu valdību Pastāvīgo pārstāvju komiteja (*COREPER*), Politikas un drošības komiteja un *IPCR*, kuras visas atbalsta Padomes Ģenerālsekretariāts.

c) Komisija, kā arī Komisijas ekspertu grupas

— Izraudzītais vadošais dienests (atkarībā no skartās nozares), kuru atbalsta *ERCC* un kurš darbojas visu diennakti kā operatīvais centrs, kas pārvalda reaģēšanu krīzes situācijās, un Migrācijas un iekšlietu ģenerāldirektorāts kā par šo jomu atbildīgais dienests un starpnozaru incidenta gadījumā — Migrācijas un iekšlietu ģenerāldirektorāts un citi attiecīgie Komisijas dienesti,

— Komunikācijas ģenerāldirektorāts un preses dienests,

— Veselības ārkārtas situāciju gatavības un reaģēšanas iestādes (*HERA*) ģenerāldirektorāts,

— Kritisko vienību noturības grupa, ko vada Komisijas pārstāvis (Migrācijas un iekšlietu ģenerāldirektorāts), kas izveidota ar Direktīvu (ES) 2022/2557, un attiecīgā gadījumā citas attiecīgās ekspertu grupas un komitejas,

— *ERCC*, kas izveidots saskaņā ar Savienības civilās aizsardzības mehānismu (*UCPM*) ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES[6] (kas darbojas visu diennakti saskaņā ar *UCPM* un atrodas Eiropas Civilās aizsardzības un humānās palīdzības operāciju ģenerāldirektorātā),

— Direktīvas (ES) 2022/2555 14. pantā minētā sadarbības grupa,

— Kiberdraudu situācijas apzināšanās un analīzes centrs,

— Regulas (ES) 2022/2371[7] 4. pantā minētā Veselības drošības komiteja,

— Komisijas Ģenerālsekretariāts (*ARGUS* sekretariāts) un ģenerālsekretāra vietnieks (*ARGUS* process), Cilvēkresursu ģenerāldirektorāts (Drošības direktorāts),

— Citas attiecīgas Komisijas ekspertu grupas, kas palīdz Komisijai koordinēt pasākumus ārkārtas vai krīzes situācijā,

---

[6] Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības Civilās aizsardzības mehānismu (OV L 347, 20.12.2013., 924. lpp.).

[7] Eiropas Parlamenta un Padomes Regula (ES) 2022/2371 (2022. gada 23. novembris) par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 1082/2013/ES (OV L 314, 6.12.2022., 26. lpp.).

— Citi krīzes pārvarēšanas tīkli, tai skaitā nozaru tīkli (piemēram, Transporta kontaktpunktu tīkls, ko pārvalda Mobilitātes un transporta ģenerāldirektorāts, starpiestāžu Kiberkrīžu darba grupa[8], Eiropas aviācijas krīzes koordinācijas vienība),

– Priekšsēdētājs un/vai atbildīgais priekšsēdētāja vietnieks/komisārs.

d) EĀDD

— Vienotā izlūkdatu analīzes procedūra (*SIAC*), ko veido Izlūkošanas un situāciju centrs (*IntCen*) un ES Militārā štāba Izlūkošanas direktorāts (*EUMS Int*),

— Krīzes Reaģēšanas centrs (KRC),

— Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos / Komisijas priekšsēdētāja vietnieks.

e) Attiecīgās Savienības struktūras, biroji un attiecīgās Savienības aģentūras, piemēram, Eiropols, atkarībā no skartās(-ajām) nozares(-ām)[9].

4. Mijiedarbība ar citiem attiecīgiem krīzes pārvarēšanas mehānismiem un instrumentiem

Kritiskās infrastruktūras plāns ir elastīgs rīks, ar ko plāno dažādas darbības, kuras varētu veikt daļēji vai pilnībā, izmantojot dažādus esošos mehānismus, atkarībā no būtiskā kritiskās infrastruktūras incidenta veida un smaguma un no operatīvās, stratēģiskās/politiskās koordinēšanas nepieciešamības.

a) ES protokols hibrīddraudu apkarošanai[10] ("ES protokols")

ES protokolu piemēro hibrīddraudu gadījumā[11], un tajā izklāsta procesus un rīkus, kas piemērojami šādu draudu vai kampaņu gadījumā.

Būtiska kritiskās infrastruktūras incidenta ar hibrīddimensiju gadījumā papildus Kritiskās infrastruktūras plānam attiecīgā gadījumā piemēro ES protokolu, piemēram, attiecībā uz konkrētu informāciju, analīzi vai saziņu par būtiska kritiskās infrastruktūras incidenta hibrīdaspektiem un attiecībā uz sadarbību ar ārējiem partneriem.

---

[8] Neformāla grupa, kurā ietilpst attiecīgie Komisijas dienesti, EĀDD, Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība (*CERT-EU*) un Eiropols, kuras kopīgi vada Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts un EĀDD.

[9] Piemēram, Eiropols; attiecībā uz transportu: Eiropas Savienības Aviācijas drošības aģentūra (*EASA*), Eiropas Jūras drošības aģentūra (*EMSA*), Eiropas Dzelzceļa aģentūra (*ERA*); attiecībā uz veselības nozari: Eiropas Slimību profilakses un kontroles centrs (*ECDC*) un Eiropas Zāļu aģentūrai (*EMA*); attiecībā uz enerģētikas nozari: Eiropas Savienības Energoregulatoru sadarbības aģentūra (*ACER*); attiecībā uz kosmosa nozari: ES Kosmosa programmas aģentūra (*EUSPA*); attiecībā uz pārtikas nozari: Eiropas Pārtikas nekaitīguma iestāde (*EFSA*); attiecībā uz jūrniecības nozari: Eiropas Zivsaimniecības kontroles aģentūra (*EFCA*); attiecībā uz kiberincidentu nozari: Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), datordrošības incidentu reaģēšanas vienības (*CSIRT*), ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība (*CERT UE*).

[10] Komisijas dienestu darba dokuments "ES protokols hibrīddraudu apkarošanai", SWD(2023) 116 final.

[11] Hibrīddraudus var raksturot kā piespiedu un graujošu darbību, tradicionālu un netradicionālu metožu apvienojumu, ko koordinēti var izmantot valsts vai nevalstiski dalībnieki, lai panāktu konkrētus mērķus, bet nepārkāpjot oficiāli pieteikta kara robežu, sk. ES protokolu par hibrīddraudiem.

b) Plāns, kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm

Kiberdrošības plāns attiecas uz plašapmēra pārrobežu incidentiem, kuru izraisītie traucējumi ir pārāk plaši, lai skartā dalībvalsts varētu tos pārvarēt viena pati, vai kuri skar divas vai vairākas dalībvalstis vai ES iestādes un kuru ietekme tehniskajā vai politiskajā ziņā ir tik plaša un nozīmīga, ka ir vajadzīga savlaicīga politikas koordinēšana un reaģēšana Savienības politiskajā līmenī.

Tāda būtiska kritiskās infrastruktūras incidenta gadījumā, kas sakrīt ar plašapmēra kiberdrošības incidentu vai šķiet saistīts ar to, attiecīgās Padomes darba grupas nosaka pienācīgu koordināciju operatīvajā līmenī, tostarp ar *EU-CyCLONe* vai, rīkojot Kritisko vienību noturības grupas kopīgu sanāksmi ar sadarbības grupu. Koordinēšanas mērķis ir noteikt, kurš dalībnieks, rīks(-i) vai mehānisms(-i) varētu visefektīvāk palīdzēt reaģēt uz būtisko kritiskās infrastruktūras incidentu, vienlaikus izvairoties no dublēšanās un paralēliem darba virzieniem.

c) Savienības civilās aizsardzības mehānisms un tā Ārkārtējās reaģēšanas koordinēšanas centrs

Saskaņā ar Lēmumu Nr. 1313/2013/ES par Savienības civilās aizsardzības mehānismu operatīvo reaģēšanu saskaņā ar *UCPM* attiecībā uz faktiskām dabas un cilvēku izraisītām katastrofām vai katastrofas draudiem (tai skaitā tiem, kas rada kritiskās infrastruktūras darbības traucējumus) Savienībā un ārpus tās vada *ERCC*, kas ir Komisijas vienotais operatīvais centrs, kurš darbojas visu diennakti un pārvalda reaģēšanu krīzes situācijās. Šādos gadījumos *ERCC* var nodrošināt agrīno brīdināšanu, paziņošanu, analīzi un atbalstīt informācijas apmaiņu un, ja dalībvalsts aktivizē *UCPM*, operatīvās palīdzības un ekspertu izvietošanu skartajās teritorijās. Turklāt *ERCC* var veicināt nozaru un starpnozaru koordinēšanu gan Savienības līmenī, gan starp Savienības un attiecīgajām valstu iestādēm, tai skaitā tām, kas atbildīgas par civilo aizsardzību un kritiskās infrastruktūras noturību.

d) Citi nozaru vai starpnozaru mehānismi un instrumenti

Ar šo Kritiskās infrastruktūras plānu nedublē citus nozaru vai starpnozaru krīzes pārvarēšanas instrumentus vai koordinācijas mehānismus. Ja šādi rīki vai mehānismi jau pastāv skartajā nozarē, šo Kritiskās infrastruktūras plānu tā piemērošanas jomā var izmantot kā papildu rīku nozaru vai starpnozaru rīkiem vai mehānismiem, bet tas neaizstāj tos. Lai izvairītos no šādas dublēšanās, būtu jānodrošina nepieciešamā koordinācija starp dažādiem dalībniekiem. To varētu panākt, piemēram, Komisijas iekšējā krīzes koordinācijas procesā *ARGUS*, ko atbalsta *ERCC*, un/vai *IPCR* koordinācijas sanāksmēs.

II DAĻA. INFORMĀCIJAS APMAIŅA UN KOORDINĒTA REAĢĒŠANA

Turpmāk aprakstītās darbības ietver sadarbības veidus, proti, informācijas apmaiņu, koordinētu informēšanu un reaģēšanu. Šī struktūra atbilst Padomes krīzes situāciju koordinācijas mehānisma *IPCR* režīmiem, un tajā plašākā nozīmē ir ņemta vērā jau ES līmenī pastāvošo krīzes koordinācijas mehānismu iespējamā izmantošana. Šajā struktūrā ir parādīts, kā šie sadarbības veidi tajā tiktu integrēti, ja tos izmantotu. Tomēr lielāko daļu šo darbību var veikt arī autonomi: tās nav atkarīgas no minētā mehānisma izmantošanas, bet drīzāk to papildina. Darbības ir izklāstītas hronoloģiskā secībā, vienlaikus ņemot vērā, ka tādas plašapmēra krīzes gadījumā, kas ietver būtisku kritiskās infrastruktūras incidentu, vairākas darbības var veikt vienlaikus un pastāvīgi.

1. INFORMĀCIJAS APMAIŅA

(a) Operatīvajā līmenī

Dalībvalstis, kuras skāris būtisks kritiskās infrastruktūras incidents, piemēro savus ārkārtas pasākumus, nodrošina koordināciju ar attiecīgajiem valsts krīzes pārvarēšanas mehānismiem un attiecīgā gadījumā iesaista visus attiecīgos valsts, reģionālos un vietējos dalībniekus.

Attiecīgā gadījumā attiecībā uz civilās aizsardzības palīdzību koordinācija starp dalībvalstīm un ar Komisiju tiek nodrošināta, izmantojot *ERCC* saskaņā ar *UCPM*.

i) Informācijas apmaiņa un paziņošana, ko veic valstu kompetentās iestādes

Papildus paziņošanas un informēšanas pienākumiem, kuri paredzēti Direktīvas (ES) 2022/2557 15. pantā, valstu kompetentās iestādes, kas atbildīgas par kritisko infrastruktūru dalībvalstīs, kuras skāris būtisks kritiskās infrastruktūras incidents, bez nepamatotas kavēšanās, izmantojot savus vienotos kontaktpunktus, apmainās ar Padomes rotējošo prezidentvalsti un Komisiju ar attiecīgo informāciju, kas saņemta no kritiskās infrastruktūras operatora(-iem), kritiskajām vienībām vai no citiem avotiem, kā arī ar informāciju par aktivizētajiem krīzes pārvarēšanas mehānismiem. Komisijai *ERCC* nodrošina operatīvos kontaktus un spējas 24 stundas diennaktī un reāllaikā koordinē, uzrauga un atbalsta reaģēšanu uz ārkārtas situācijām Savienības līmenī, vienlaikus kalpojot dalībvalstīm un Komisijai kā operatīvajam centram reaģēšanai krīzes situācijās, veicinot starpnozaru pieeju katastrofu pārvarēšanai.

Šāda informācijas apmaiņa attiecas uz būtiska kritiskās infrastruktūras incidenta veidu, tā cēloni, novēroto vai aplēsto traucējumu ietekmi uz kritisko infrastruktūru un pamatpakalpojumu sniegšanu, incidenta sekām nozarēs un pāri robežām un ietekmes mazināšanas pasākumiem, kas jau veikti vai plānoti valsts līmenī vai ar attiecīgajām citām dalībvalstīm un Komisiju, izmantojot esošos mehānismus, piemēram, informācijas apmaiņas kārtību saskaņā ar Direktīvas (ES) 2022/2557 9. un 15. pantu. Šādas ziņas sniedz, nenovirzot kritiskās infrastruktūras vai dažos gadījumos kritiskās vienības vai dalībvalsts resursus no darbībām, kuras saistītas ar incidenta risināšanu, kam jābūt noteiktai par prioritāti.

Lai nodrošinātu turpmākus pasākumus, *ERCC* vai informāciju saņēmušie Komisijas dienesti, kas ir atbildīgi par nozari(-ēm), kurā(-ās) notika būtisks kritiskās infrastruktūras incidents, informē Migrācijas un iekšlietu ģenerāldirektorāta kontaktpunktu un Komisijas Ģenerālsekretariātu. Tikmēr, ja vēl nav uzsākts, *ERCC* sāk uzraudzīt notikumus, jo īpaši gadījumā, ja *UCPM* aktivizē viena vai vairākas skartās dalībvalstis.

Ja informācija varētu būt būtiska kiberdrošības dimensijas risināšanai vai saistīta ar kiberdrošības incidentu, Komisija apmainās ar attiecīgo informāciju ar *EU-CyCLONe*.

Valstu kompetentajām iestādēm saskaņā ar Direktīvu (ES) 2022/2557 bez nepamatotas kavēšanās ir jāsadarbojas un jāapmainās ar informāciju ar kompetentajām iestādēm saskaņā ar Direktīvu (ES) 2022/2555 saistībā ar kiberincidentiem un incidentiem, kas skar kritiskās vienības, tai skaitā kiberdrošības un fiziskiem pasākumiem, kurus veikušas kritiskās vienības.

Jūrlietu jomā valstu kompetentās iestādes apsver iespēju izmantot vienoto informācijas apmaiņas vidi (*CISE*), lai bez nepamatotas kavēšanās apmainītos ar informāciju.

ii) Ekspertu sanāksmju organizēšana

Komisija pēc iespējas ātrāk sasauc Kritisko vienību noturības grupu, lai veicinātu attiecīgās informācijas apmaiņu starp valstu kompetentajām iestādēm, kas atbildīgas par kritisko infrastruktūru, un attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām par incidentu (veidu, cēloni, ietekmi un sekām nozarēs un pāri robežām) un par reaģēšanas

darbībām, tai skaitā seku mazināšanas pasākumiem un tehnisko atbalstu skartajām dalībvalstīm. Atkarībā no incidenta smagumcentra attiecīgie Komisijas dienesti būs cieši saistīti ar Kritisko vienību noturības grupas sanāksmi, lai apmainītos ar informāciju, kas iegūta, izmantojot esošos nozaru instrumentus. Tādu incidentu gadījumā, kuros apvienoti kiberdrošības un fiziski ar kiberdrošību nesaistīti aspekti, attiecīgie Komisijas dienesti, *CERT-EU* un EĀDD, attiecīgā gadījumā pēc iespējas ātrāk ziņo un apspriežas Kiberkrīžu darba grupā, kā arī ar attiecīgajiem sadarbības grupas priekšsēdētājiem, kā minēts Direktīvas (ES) 2022/2555 14. pantā, un attiecīgā gadījumā *EU-CyCLONe* par koordinēšanas pasākumu nepieciešamību. Vienojoties ar attiecīgajiem priekšsēdētājiem, Komisija (Migrācijas un iekšlietu ģenerāldirektorāts un Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts) var ierosināt Kritisko vienību noturības grupas kopīgu sanāksmi ar sadarbības grupu, lai panāktu kopīgu situācijas apzināšanos un koordinētu attiecīgos reaģēšanas pasākumus.

Būtiska starpnozaru kritiskās infrastruktūras incidenta gadījumā, kura dēļ ir nepieciešama vai varētu būt nepieciešama seku pārvaldība Savienības līmenī, Komisija var sasaukt starpnozaru koordinācijas sanāksmes, kurās piedalās visas attiecīgās ieinteresētās personas.

Ja nozīmīgs kritiskās infrastruktūras incidents skar arī trešo valsti, Komisija apspriežas ar skartās trešās valsts kompetento iestādi un var uzaicināt to uz Kritisko vienību noturības grupas sanāksmi.

iii) Komisijas un Savienības aģentūru sniegtais atbalsts

Attiecīgā gadījumā un rīkojoties saskaņā ar savām pilnvarām, Eiropols Savienības līmenī sniedz incidenta situāciju ziņojumu. Citas Savienības aģentūras, attiecīgā gadījumā un rīkojoties saskaņā ar savām attiecīgajām pilnvarām, sniedz attiecīgo informāciju, kas veicina situācijas apzināšanos vai koordinētu reaģēšanu uz būtisku kritiskās infrastruktūras incidentu, atbildīgajiem ģenerāldirektorātiem, kuri savukārt ziņo Komisijai (Migrācijas un iekšlietu ģenerāldirektorātam kā Kritisko vienību noturības grupas priekšsēdētājam).

Komisija attiecīgā gadījumā un saskaņā ar piemērojamo tiesisko regulējumu var veicināt situācijas apzināšanos, izmantojot tādus Savienības kosmosa programmas[12] līdzekļus kā *Copernicus*, *Galileo* un *EGNOS*.

(b) Stratēģiskajā līmenī

i) Situācijas apzināšanās ziņojumu sagatavošana

Pamatojoties uz informāciju, ar ko valstu kompetentās iestādes ir apmainījušās Kritisko vienību noturības grupas sanāksmē vai kopīgās sanāksmēs ar attiecīgajiem dienestiem, ekspertu grupām vai tīkliem, Komisija sagatavo situācijas apzināšanās ziņojumu, kura pamatā ir valstu kompetento iestāžu sniegtā informācija un cita pieejamā informācija.

Šajā ziņojumā attiecīgā gadījumā no kiberdrošības viedokļa tiks ņemti vērā rezultāti, kas gūti attiecīgajos ES līmeņa riska novērtējumos, izvērtējumos un scenārijos, tai skaitā tajos, ko veikusi Komisija, Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos un sadarbības grupa.

IPCR aktivizēšanas gadījumā šis ziņojums var sniegt ieguldījumu integrētajā situācijas apzināšanās analīzē (ISAA), ko sagatavo Komisijas dienesti un EĀDD.

[12] Eiropas Parlamenta un Padomes Regula (ES) 2021/696 (2021. gada 28. aprīlis), ar ko izveido Savienības kosmosa programmu un Eiropas Savienības Kosmosa programmas aģentūru un atceļ Regulas (ES) Nr. 912/2010, (ES) Nr. 1285/2013 un (ES) Nr. 377/2014 un Lēmumu Nr. 541/2014/ES (OV L 170, 12.5.2021., 69. lpp.).

Attiecīgā gadījumā *SIAC* sniedz jaunāko uz izlūkdatiem balstītu novērtējumu par incidentu.

ii) Savienības krīzes koordinācijas mehānismu aktivizēšana un Savienības rīku izmantošana

ERCC attiecīgā gadījumā sāk sniegt situācijas apzināšanās atbalstu saistībā ar incidentu, jo īpaši, ja notikuma dēļ jāaktivizē *UCPM*[13]. Turklāt skartās dalībvalstis var pieprasīt savas teritorijas satelītattēlus, izmantojot *Copernicus* ārkārtas situāciju pārvaldības pakalpojumu.

Ja to uzskata par vajadzīgu, lai Komisijā apmainītos ar informāciju ar EĀDD un attiecīgajām Savienības aģentūrām, vadošais ģenerāldirektorāts vai Migrācijas un iekšlietu ģenerāldirektorāts sadarbībā ar Ģenerālsekretariātu aktivizē Komisijas iekšējā krīzes koordinācijas procesa *ARGUS* I posmu, uzsākot pasākumu *ARGUS* IT rīkā.

Savienības Padomes rotējošā prezidentvalsts var aktivizēt *IPCR* mehānismus informācijas apmaiņas režīmā, kas nozīmē, ka Komisija un EĀDD ar valstu kompetento iestāžu un attiecīgā gadījumā citu avotu atbalstu izstrādā *ISAA* ziņojumus. Pat neaktivizējot *IPCR*, Padomes rotējošā prezidentvalsts vai Komisija var noteiktos apstākļos izveidot *IPCR* tīmekļa platformas uzraudzības lapu.

Citus (nozaru) Savienības krīzes pārvarēšanas mehānismus un rīkus attiecīgā gadījumā var aktivizēt, ievērojot attiecīgās procedūras. Komisija nodrošinās koordināciju starp šiem mehānismiem un rīkiem.

Ja fiziskais incidents sakrīt vai šķiet saistīts ar plašapmēra kiberdrošības incidentu, kā definēts Direktīvas (ES) 2022/2555 6. panta 7. punktā, Padomes rotējošā prezidentvalsts var izmantot Kiberdrošības plānu, lai noteiktu pienācīgu koordināciju operatīvajā līmenī, cita starpā iesaistot *EU-CyCLONe* un Kritisko vienību noturības grupu.

iii) Sabiedrības informēšana koordinēšana

Būtiska kritiskās infrastruktūras incidenta skartās dalībvalstis, cik vien iespējams, koordinē sabiedrības informēšanu par krīzi, vienlaikus ievērojot valsts kompetenci šajā jomā. Attiecīgā gadījumā var iesaistīt *IPCR* krīzes saziņas tīklu.

Pamatojoties uz kopīgo situācijas apzināšanos, Kritisko vienību noturības grupa un skartās dalībvalstis attiecīgā gadījumā atbalsta saskaņotu sabiedrības informēšanas virzienu formulēšanu.

Eiropols un citas attiecīgās Savienības aģentūras savas sabiedrības informēšanas darbības koordinē ar Komisijas preses dienestu, pamatojoties uz kopīgu situācijas apzināšanos.

Ja būtiskais kritiskās infrastruktūras incidents ietver ārējo, hibrīdo vai kopējās drošības un aizsardzības politikas dimensiju, sabiedrības informēšanu koordinē ar EĀDD un Komisijas preses dienestu saskaņā ar ES protokolu hibrīddraudu apkarošanai[14].

2. REAĢĒŠANA (KAS IETVER NEPĀRTRAUKTAS DARBĪBAS, KURAS APRAKSTĪTAS SADAĻĀ "INFORMĀCIJAS APMAIŅA", UN PAPILDU DARBĪBAS STRATĒĢISKAJĀ/POLITISKAJĀ LĪMENĪ)

(a) Stratēģiskajā līmenī

i) Pastāvīga situācijas ziņojumu sagatavošana

[13] Piemēram, publicējot mediju monitoringa produktus, civilās aizsardzības ziņojumus, analītiskos kopsavilkumus, *ECHO* ikdienas kartes, *ECHO* ikdienas ziņas un citus pielāgotus produktus.

[14] Komisijas dienestu darba dokuments "ES protokols hibrīddraudu apkarošanai", SWD(2023) 116 final.

Padomes Civilās aizsardzības jautājumu darba grupa — Kritisko vienību noturība (*PROCIV-CER*) tiek informēta par politiskās/stratēģiskās situācijas ziņojuma sagatavošanu (piemēram, *IPCR* aktivizēšanas gadījumā *ISAA* vai Komisijas sagatavoto situācijas apzināšanās ziņojumu) un sagatavo Dalībvalstu valdību Pastāvīgo pārstāvju komiteju (*COREPER*), ja tā vēl nav sasaukta, vai attiecīgā gadījumā Politikas un drošības komitejas sanāksmi.

SIAC pastiprina saziņu ar dalībvalstu izlūkdienestiem, apkopo visu avotu informāciju un sagatavo incidenta analīzi un novērtējumu, kā arī vajadzības gadījumā regulārus atjauninājumus.

ii) Savienības krīzes koordinācijas mehānismu pilnīga aktivizēšana un Savienības instrumentu izmantošana

Ja Komisijas priekšsēdētājs aktivizē Komisijas iekšējā krīzes koordinācijas procesa *ARGUS* II posmu, īsā laikā sasauc Krīzes koordinācijas komitejas sanāksmi(-es), kurā(-ās) iesaista attiecīgos Komisijas dienestus, aģentūras un attiecīgā gadījumā EĀDD, lai koordinētu visus būtiskā kritiskās infrastruktūras incidenta aspektus.

Ja Padomes prezidentvalsts aktivizē *IPCR* pilnā režīmā:

— Padomes rotējošā prezidentvalsts aicina savlaicīgi rīkot neformālu apaļā galda sanāksmi, pulcējot attiecīgos valstu, Eiropas un starptautiskos dalībniekus, kurā Komisijas pārstāvis, kas darbojas kā Kritisko vienību noturības grupas priekšsēdētājs (Migrācijas un iekšlietu ģenerāldirektorāts), var ziņot par iepriekš sasaukto(-ajām) grupas sanāksmi(-ēm), un ko attiecīgā gadījumā papildina citi Komisijas dienesti un EĀDD,

— šajā sanāksmē var uzaicināt *SIAC* un attiecīgās Savienības aģentūras sniegt jaunāko informāciju par būtisko kritiskās infrastruktūras incidentu.

ISAA vadošais dienests (Komisijas vadošais dienests vai EĀDD) ar attiecīgo Komisijas dienestu, attiecīgo Savienības biroju, struktūru un aģentūru un valstu kompetento iestāžu palīdzību sagatavo *ISAA* ziņojumu. Dalībvalstis tiek aicinātas sniegt ieguldījumu, izmantojot *IPCR* tīmekļa platformu, *ISAA* ziņojumu sagatavošanā.

Tāda būtiska kritiskās infrastruktūras incidenta gadījumā, kam ir nozīme starptautiskajā drošībā, Komisijas dienesti un EĀDD var sasaukt ES un NATO strukturētā dialoga par noturību sanāksmi, lai veicinātu kopīgu situācijas apzināšanos un informācijas apmaiņu par pasākumiem, kurus attiecīgi veic Savienība un NATO.

iii) Sabiedrības informēšana

Padome sagatavo kopīgus sabiedrības informēšanas ziņojumus. Šo darbu var atbalstīt neformālais krīzes saziņas koordinatoru tīkls, kas izveidots ar *IPCR*. Attiecīgā gadījumā sabiedrības informēšanas ziņojumus sagatavo arī Komisijas preses dienests.

Ja būtiskais kritiskās infrastruktūras incidents ietver ārējo, hibrīdo vai kopējās drošības un aizsardzības politikas dimensiju, sabiedrības informēšanu koordinē ar EĀDD un Komisijas preses dienestu.

iv) Atbalsts dalībvalstīm un efektīva reaģēšana

Rotējošā prezidentvalsts var sasaukt *PROCIV-CER* sanāksmi, lai atbalstītu darbības *IPCR* ietvaros, ja tas ir aktivizēts.

Dalībvalstis, kuras skāris būtisks kritiskās infrastruktūras incidents, ar Kritisko vienību noturības grupas starpniecību var lūgt tehnisko atbalstu citām dalībvalstīm vai attiecīgajām Savienības iestādēm, struktūrām un aģentūrām, piemēram, īpašas zināšanas, lai mazinātu būtiskā kritiskās infrastruktūras incidenta negatīvo ietekmi.

Dalībvalstis, kuras skāris būtisks kritiskās infrastruktūras incidents, var arī lūgt tehnisko un/vai finansiālo atbalstu Komisijai vai attiecīgajām Savienības aģentūrām. Komisija sadarbībā ar attiecīgajām Savienības aģentūrām novērtē tās iespējamo atbalstu un attiecīgā gadījumā Savienības līmenī aktivizē tehniskos seku mazināšanas pasākumus saskaņā ar savām attiecīgajām procedūrām un koordinē tehniskās spējas, kas vajadzīgas, lai apturētu vai samazinātu būtiska kritiskās infrastruktūras incidenta ietekmi.

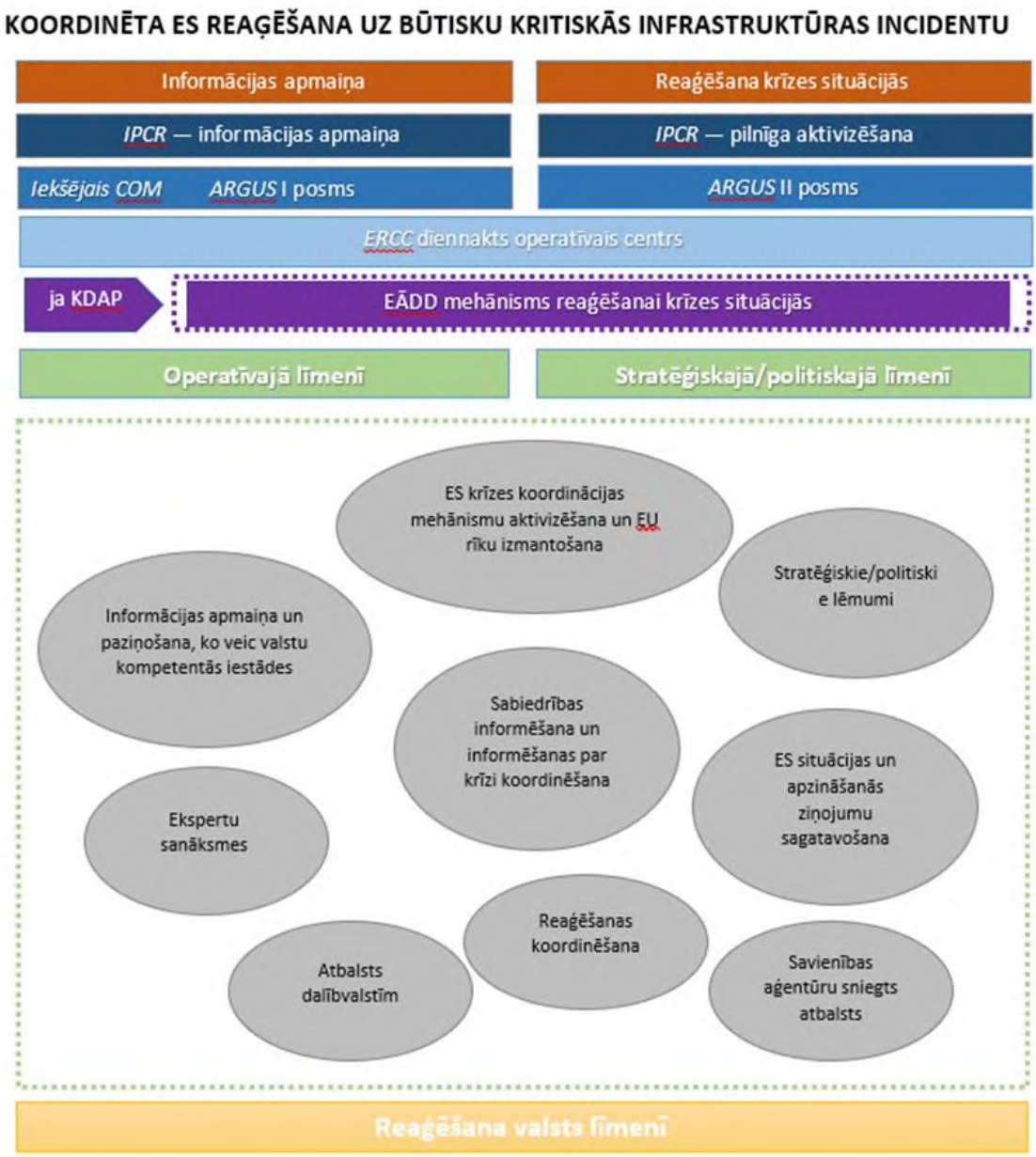
Jo īpaši *UCPM* kontekstā skartās valstis varētu lūgt palīdzību, izmantojot Kopīgo ārkārtējo situāciju sakaru un informācijas sistēmu (*CECIS*), un pēc tam *ERCC* strādātu, lai koordinētu palīdzības sniegšanu no dalībvalstīm un *UCPM* iesaistītajām valstīm, kā arī izmantojot *rescEU*.

Eiropols un citas attiecīgās Savienības aģentūras saskaņā ar savām attiecīgajām pilnvarām un pēc pieprasījuma atbalsta dalībvalstis, kuras skāris būtisks kritiskās infrastruktūras incidents, incidenta izmeklēšanā.

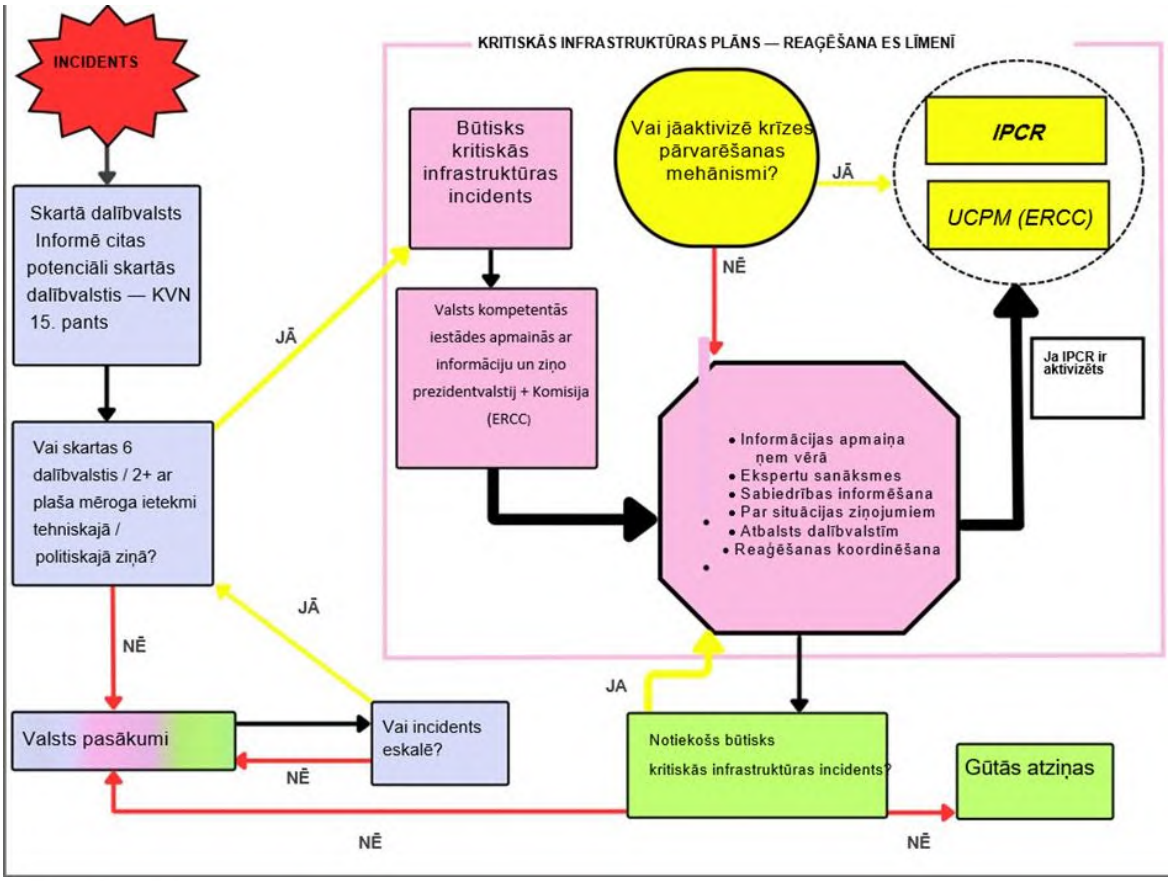
(b) Politiskajā līmenī

Padomes prezidentvalsts varētu apsvērt nepieciešamību sasaukt *IPCR* apaļā galda sanāksmes, Padomes darba grupu, *COREPER*, Ministru padomes un/vai samitu sanāksmes, lai apmainītos ar informāciju par būtiskā kritiskās infrastruktūras incidenta iespējamo izcelsmi un paredzamajām sekām dalībvalstīs un Savienībā, vienotos par kopējām pamatnostādnēm un pieņemtu vajadzīgos pasākumus, lai atbalstītu dalībvalstis, kuras skāris būtisks kritiskās infrastruktūras incidents, un mazinātu tā sekas.

1. diagramma. Kritiskās infrastruktūras plāna shematisks pārskats



3. DIAGRAMMA. KRITISKĀS INFRASTRUKTŪRAS PLĀNA LĒMUMU PIEŅEMŠANA



APZĪMĒJUMI

Posmi pirms plāna

Krīzes pārvarēšanas mehānismu aktivizēšana

Plāns

Posmi pēc plāna