Eiropas Savienības
Padome

Briselē, 2022. gada 9. decembrī
(OR. en)

15623/22

Starpiestāžu lieta:
2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	13713/22, 15454/22
Temats:	PADOMES IETEIKUMS par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai

Pielikumā pievienots Padomes Ieteikums par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai, ko Padome pieņēma 3920. sanāksmē, kura notika 2022. gada 8. decembrī.

PIELIKUMS

PADOMES IETEIKUMS (ES) 2022/…

(... gada...)

par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai

(Dokuments attiecas uz EEZ)

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu un 292. panta pirmo un otro teikumu,

ņemot vērā Eiropas Komisijas priekšlikumu,

tā kā:

(1) Ar mērķi nodrošināt iekšējā tirgus darbību visu dalībvalstu un Savienības kopumā interesēs ir skaidri identificēt un aizsargāt attiecīgo kritisko infrastruktūru, kas minētajā tirgū nodrošina pamatpakalpojumus, jo īpaši svarīgajās nozarēs, piemēram, enerģētikas, digitālās infrastruktūras, transporta un kosmosa nozarēs, kā arī kritisko infrastruktūru ar būtisku pārrobežu nozīmi [1], kuras darbības traucējumi varētu ievērojami ietekmēt citas dalībvalstis.

[1] Šāda nozīme dalībvalstīm būtu jānovērtē atbilstoši savai valsts praksei, un tās to var darīt, pamatojoties cita starpā uz tādiem faktoriem kā riska novērtējums un notikuma ietekme un raksturs.

(2) Šajā ieteikumā, kurš ir nesaistošs akts, atspoguļota dalībvalstu politiskā griba kopīgi sadarboties un to apņemšanās attiecībā uz ieteiktajiem pasākumiem, kas uzsvērti Eiropas Komisijas priekšsēdētājas izdotajā piecu punktu plānā, vienlaikus pilnībā ievērojot dalībvalstu kompetenci. Šis ieteikums neskar dalībvalstu būtisko interešu aizsardzību nacionālās drošības, sabiedriskās drošības vai aizsardzības jomā, un ne no vienas dalībvalsts nebūtu jāsagaida, ka tā dalīsies ar informāciju, kas kaitē minētajām interesēm.

(3) Lai gan galvenā atbildība par kritiskās infrastruktūras drošības nodrošināšanu un tās nodrošināto pamatpakalpojumu sniegšanu gulstas uz dalībvalstīm un to kritiskās infrastruktūras operatoriem, ir lietderīgi pastiprināt koordināciju Savienības līmenī, jo īpaši ņemot vērā mainīgos apdraudējumus, kas vienlaikus var ietekmēt vairākas dalībvalstis, piemēram, Krievijas agresijas karu pret Ukrainu un pret dalībvalstīm vērstās hibrīdkampaņas, vai ietekmēt Savienības ekonomikas, iekšējā tirgus un sabiedrības kopumā noturību un sekmīgu darbību. Īpaša uzmanība būtu jāpievērš kritiskajai infrastruktūrai, kas atrodas ārpus dalībvalstu teritorijas, piemēram, zemūdens kritiskajai infrastruktūrai jūrās vai atkrastes energoinfrastruktūrai.

(4) Eiropadome savos 2022. gada 20. un 21. oktobra secinājumos stingri nosodīja sabotāžu pret kritisko infrastruktūru, piemēram, pret *Nord Stream* cauruļvadiem, norādot, ka uz jebkādiem tīšiem kritiskās infrastruktūras traucējumiem vai citām hibrīddarbībām Savienības atbildes reakcija būs vienota un apņēmīga.

(5) Ņemot vērā strauji mainīgo drošības apdraudējumu ainu, prioritārā kārtā būtu jāveic noturību uzlabojoši pasākumi svarīgajās nozarēs (piemēram, enerģētikas, digitālās infrastruktūras, transporta un kosmosa nozarēs) un citās nozīmīgās nozarēs, ko noteikušas dalībvalstis. Šādiem pasākumiem vajadzētu būt vērstiem uz kritiskās infrastruktūras noturības uzlabošanu, ņemot vērā attiecīgos riskus, jo īpaši kaskādes efektu, piegādes ķēžu traucējumus, atkarību, klimata pārmaiņu ietekmi, neuzticamus piegādātājus un partnerus, kā arī hibrīddraudus un kampaņas, tostarp ārvalstu īstenotu informācijas manipulāciju un iejaukšanos. Attiecībā uz valstu kritisko infrastruktūru, ņemot vērā iespējamās sekas, prioritāte būtu jāpiešķir tai kritiskajai infrastruktūrai, kurai ir būtiska pārrobežu nozīme. Dalībvalstis tiek mudinātas attiecīgā gadījumā steidzami nodrošināt šādus noturību uzlabojošus pasākumus, vienlaikus saglabājot mainīgajā tiesiskajā regulējumā izklāstīto pieeju.

(6) Eiropas kritiskās infrastruktūras aizsardzība enerģētikas un transporta nozarēs patlaban ir reglamentēta Padomes Direktīvā 2008/114/EK [2], savukārt tīklu un informācijas sistēmu drošība visā Savienībā, galveno uzmanību pievēršot kiberdraudiem, ir nodrošināta Eiropas Parlamenta un Padomes Direktīvā 2016/1148 [3]. Lai nodrošinātu augstāku kritiskās infrastruktūras, kiberdrošības un finanšu tirgus vispārējo noturības un aizsardzības līmeni, tiek veikti grozījumi un ieviesti papildinājumi esošajā tiesiskajā regulējumā, pieņemot jaunus noteikumus, ko piemēro kritiskām vienībām (Kritisko vienību noturības direktīva), pastiprinātus noteikumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (TID 2 direktīva) un jaunus noteikumus par finanšu sektora digitālās darbības noturību (*DORA*).

(7) Dalībvalstīm būtu saskaņā ar Savienības un valstu tiesību aktiem jāizmanto visi pieejamie rīki, lai virzītos uz priekšu un palīdzētu stiprināt fizisko noturību un kibernoturību. Šajā sakarā ar kritisko infrastruktūru būtu jāsaprot gan attiecīgā kritiskā infrastruktūra, ko dalībvalsts noteikusi valsts līmenī, gan infrastruktūra, kas noteikta par Eiropas kritisko infrastruktūru saskaņā ar Direktīvu 2008/114/EK, kā arī kritiskās vienības, kas jānosaka saskaņā ar Kritisko vienību noturības direktīvu, vai attiecīgā gadījumā vienības, uz kurām attiecas TID 2 direktīva. Noturība būtu jāsaprot kā jēdziens, kas attiecas uz kritiskās infrastruktūras spēju novērst notikumus, kuri būtiski traucē vai var būtiski traucēt attiecīgo pamatpakalpojumu sniegšanu iekšējā tirgū, t. i., pakalpojumu, kas ir būtiski, lai saglabātu svarīgas sabiedriskas un saimnieciskas funkcijas, sabiedrības veselību un drošību, iedzīvotāju veselību vai vidi, kā arī aizsargāt pret šādiem notikumiem, reaģēt uz tiem, pretoties tiem, mazināt to ietekmi, izturēt tos, pielāgoties tiem vai atgūties no tiem.

---

[2] Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (OV L 345, 23.12.2008., 75. lpp.).

[3] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

(8) Lai panāktu augstāku kritiskās infrastruktūras vispārējo noturības un aizsardzības līmeni, ko ieviesīs ar jaunajiem noteikumiem, kuri attieksies uz kritiskajām vienībām, būtu jāsasauc valstu eksperti šā darba koordinēšanai. Minētā darba koordinēšana palīdzētu nodrošināt sadarbību starp dalībvalstīm un informācijas apmaiņu par darbībām, piemēram, par metodiku izstrādi ar mērķi identificēt kritiskās infrastruktūras sniegtos pamatpakalpojumus. Komisija jau ir sākusi sasaukt minētos ekspertus un sekmēt viņu darbu un plāno šo darbu turpināt. Tiklīdz Kritisko vienību noturības direktīva būs stājusies spēkā un saskaņā ar to būs izveidota Kritisko vienību noturības grupa, šādi priekšdarbi būtu jāturpina minētajai grupai saskaņā ar tās uzdevumiem.

(9) Atzīstot, ka apdraudējumu aina ir mainījusies, būtu tālāk jāattīsta potenciāls kritiskās infrastruktūras stresa testu veikšanai valstu līmenī, jo šādi testi varētu būt noderīgi kritiskās infrastruktūras noturības uzlabošanai. Ņemot vērā enerģētikas nozares īpašo nozīmīgumu un sekas, kādas varētu rasties Savienības mērogā iespējamu traucējumu gadījumā, uz kopīgi atzītiem principiem balstītu stresa testu veikšana minētajai nozarei varētu sniegt vislielāko labumu. Šādi testi ir dalībvalstu kompetencē, un tām būtu jāatbalsta un jāmudina kritiskās infrastruktūras operatori šādus testus veikt, ja noskaidrots, ka tie sniedz ieguvumus un atbilst valsts tiesiskajam regulējumam.

(10) Lai nodrošinātu koordinētu un efektīvu reakciju uz pašreizējiem un gaidāmiem apdraudējumiem, Komisija tiek mudināta sniegt papildu atbalstu dalībvalstīm, jo īpaši sniedzot attiecīgu informāciju informatīvu paziņojumu, nesaistošu rokasgrāmatu un pamatnostādņu veidā. Eiropas Ārējās darbības dienestam (EĀDD) būtu jānodrošina draudu novērtējumi, konkrēti, ar ES Izlūkošanas un situāciju centra un tā Hibrīddraudu analīzes vienības starpniecību un ar Eiropas Savienības Militārā štāba (ESMŠ) Izlūkošanas direktorāta atbalstu saskaņā ar vienoto izlūkdatu analīzes procedūras (*SIAC*) satvaru. Komisija tiek arī aicināta sadarbībā ar dalībvalstīm veicināt Savienības finansētu pētniecības un inovācijas projektu īstenošanu.

(11) Palielinoties fiziskās un digitālās infrastruktūras savstarpējai atkarībai, ļaunprātīgas kiberdarbības, kas vērstas pret kritiskām jomām, var radīt traucējumus vai kaitējumu fiziskajai infrastruktūrai, vai arī fiziskās infrastruktūras sabotāža var padarīt nepieejamus digitālos pakalpojumus. Dalībvalstis tiek aicinātas pēc iespējas drīz paātrināt sagatavošanās darbu kritiskajām vienībām piemērojamā jaunā tiesiskā regulējuma transponēšanai un piemērošanai un pastiprinātā tiesiskā regulējuma kiberdrošības jomā transponēšanai un piemērošanai, balstoties uz sadarbības grupā, kas izveidota ar Direktīvu (ES) 2016/1148 ("TID sadarbības grupa"), gūto pieredzi, vienlaikus neaizmirstot par transponēšanas termiņiem un to, ka šādam sagatavošanās darbam būtu jāvirzās uz priekšu paralēli un saskaņoti.

(12) Papildus sagatavotības uzlabošanai ir svarīgi arī stiprināt spējas ātri un efektīvi reaģēt gadījumos, kad ir traucēti kritiskās infrastruktūras nodrošinātie pamatpakalpojumi. Tāpēc šajā ieteikumā ir iekļauti pasākumi gan Savienības, gan valstu līmenī, tostarp, uzsverot atbalstošo lomu un pievienoto vērtību, ko var gūt, ieviešot pastiprinātu sadarbību un informācijas apmaiņu saistībā ar Savienības civilās aizsardzības mehānismu (*UCPM*), kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES [4], un izmantojot attiecīgos aktīvus no Savienības kosmosa programmas, kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/696 [5].

(13) Komisijai, Savienības Augstajam pārstāvim ārlietās un drošības politikas jautājumos ("Augstais pārstāvis") un TID sadarbības grupai sadarbībā ar attiecīgām civilām un militārām struktūrām un aģentūrām un esošajiem tīkliem, tostarp Eiropas Kiberkrīžu sadarbības organizāciju tīklu (*EU CyCLONe*), jāveic riska izvērtējums un jāveido riska scenāriji. Turklāt turpmāko pasākumu ietvaros pēc Nevēras ministru kopīgā aicinājuma TID sadarbības grupa ar Komisijas un Eiropas Kiberdrošības aģentūras (*ENISA*) atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*) patlaban veic riska novērtējumu. Abi minētie pasākumi noritēs saskanīgi un koordinēti ar scenāriju izstrādes pasākumu Savienības civilās aizsardzības mehānisma (*UCPM*) ietvaros, tostarp attiecībā uz kiberdrošības notikumiem un to ietekmi uz reālo dzīvi, un ko Komisija un dalībvalstis pašlaik izstrādā. Efektivitātes, lietderības un konsekvences labad un šā ieteikuma labas piemērošanas nolūkā minēto pasākumu rezultāti būtu jāatveido valstu līmenī.

---

[4] 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.).

[5] 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.).

(14) Lai nekavējoties stiprinātu sagatavotību un spēju reaģēt uz liela mēroga kiberdrošības incidentu, Komisija ir izveidojusi īstermiņa atbalsta programmu dalībvalstīm, piešķirot papildu finansējumu aģentūrai *ENISA*. Ierosinātie pakalpojumi cita starpā ietver sagatavotības darbības, piemēram, vienību testēšanu pret ielaušanos, lai identificētu ievainojamību. Programma arī var stiprināt iespējas palīdzēt dalībvalstīm tādu liela mēroga kiberdrošības incidentu gadījumā, kas skar kritiskās vienības. Tas ir pirmais solis atbilstīgi Padomes 2022. gada 23. gada secinājumiem par Eiropas Savienības pozīcijas izstrādāšanu kiberjautājumos ("Padomes secinājumi par ES pozīciju kiberjautājumos"), kuros Komisija tiek aicināta nākt klajā ar priekšlikumu par ārkārtas reaģēšanas fondu kiberdrošības jomā. Dalībvalstīm būtu pilnībā jāizmanto minētās iespējas saskaņā ar piemērojamajām prasībām, un tās tiek mudinātas turpināt darbu Savienības kiberkrīžu pārvarēšanas jomā, jo īpaši, regulāri uzraugot un izvērtējot paveikto saistībā ar Padomē nesen izstrādātā kiberkrīžu pārvarēšanas ceļveža īstenošanu. Minētais ceļvedis ir adaptīvs dokuments, un tas būtu pēc vajadzības atkārtoti jāizskata un jāatjaunina.

(15) Globālie zemūdens sakaru kabeļi ir izšķiroši svarīgi globālajai un ES iekšējai savienojamībai. Ņemot vērā šādu kabeļu ievērojamo garumu un to novietojumu jūras gultnē, zemūdens vizuālā uzraudzība lielākajā daļā kabeļu posmu ir ārkārtīgi sarežģīta. Dalītā jurisdikcija un citi jurisdikcijas jautājumi, kas saistīti ar šādiem kabeļiem, ir specifisks gadījums Eiropas un starptautiskajā sadarbībā infrastruktūras aizsardzības un atjaunošanas jomā. Tāpēc iesāktie un plānotie riska novērtējumi attiecībā uz digitālo un fizisko infrastruktūru, kas ir digitālo pakalpojumu pamatā, ir jāpapildina ar īpašiem riska novērtējumiem un iespējām veikt riska mazināšanas pasākumus attiecībā uz zemūdens sakaru kabeļiem. Dalībvalstis aicina Komisiju šajā nolūkā veikt pētījumus un savus konstatējumus darīt zināmus dalībvalstīm.

(16) Ar digitālo infrastruktūru saistītie apdraudējumi var ietekmēt arī enerģētikas un transporta nozares, piemēram, attiecībā uz energotehnoloģijām, kas ietver digitālos komponentus. Saistīto piegādes ķēžu drošība ir svarīga pamatpakalpojumu sniegšanas nepārtrauktībai un enerģētikas nozares kritiskās infrastruktūras stratēģiskajai kontrolei. Minētie apstākļi būtu jāņem vērā, veicot pasākumus kritiskās infrastruktūras noturības uzlabošanai saskaņā ar šo ieteikumu.

(17) Ņemot vērā kosmosa infrastruktūras, ar kosmosu saistīto zemes aktīvu, tostarp ražošanas objektu, un kosmosā balstītu pakalpojumu pieaugošo nozīmi ar drošību saistītās darbībās, ir būtiski nodrošināt Savienības kosmosa un ar zemi saistīto aktīvu un pakalpojumu noturību un aizsardzību Savienībā. To pašu iemeslu dēļ ir būtiski arī, šā ieteikuma ietvaros, strukturētāk izmantot kosmosā balstītus datus un pakalpojumus, ko nodrošina kosmosa sistēmas un programmas kritiskās infrastruktūras novērošanai un uzraudzībai un tās aizsardzībai citās nozarēs. Gaidāmajā ES kosmosa stratēģijā drošībai un aizsardzībai šajā sakarā tiks ierosinātas attiecīgas darbības, kas būtu jāņem vērā, īstenojot šo ieteikumu.

(18) Ir vajadzīga arī sadarbība starptautiskā līmenī, lai efektīvi pārvaldītu riskus kritiskajai infrastruktūrai, cita starpā starptautiskajos ūdeņos. Tāpēc dalībvalstis tiek aicinātas sadarboties ar Komisiju un Augsto pārstāvi, lai veiktu konkrētus pasākumus šādas sadarbības panākšanai, paturot prātā, ka visus šādus pasākumus veic tikai saskaņā ar to attiecīgajiem uzdevumiem un pienākumiem, kas noteikti Savienības tiesību aktos, jo īpaši ES Līgumu noteikumos par ārējām attiecībām.

(19) Kā noteikts Komisijas 2022. gada 15. februāra paziņojumā "Komisijas ieguldījums Eiropas aizsardzībā", atbalstot "Stratēģisko drošības un aizsardzības kompasu – Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību", Komisija sadarbībā ar Augsto pārstāvi un dalībvalstīm līdz 2023. gadam novērtēs nozaru noturības pret hibrīddraudiem pamatlīmeņus, apzinot trūkumus un vajadzības, kā arī pasākumus, kā tiem pievērsties. Minētajai iniciatīvai būtu jāpalīdz virzīt darbs, kas tiek veikts saskaņā ar šo ieteikumu, palīdzot stiprināt informācijas apmaiņu un rīcības koordināciju, lai vēl vairāk stiprinātu noturību, tostarp kritiskās infrastruktūras noturību.

(20) ES 2014. gada Jūras drošības stratēģijā un tās pārskatītajā rīcības plānā ir pausts aicinājums apņēmīgāk aizsargāt kritisko jūras infrastruktūru, tostarp zemūdens infrastruktūru, un jo īpaši jūras transporta, enerģētikas un sakaru infrastruktūru, citstarp uzlabojot informētību par jūrlietām ar uzlabotas sadarbspējas un racionalizētas informācijas apmaiņas (obligātas un brīvprātīgas) palīdzību. Minētā stratēģija un rīcības plāns pašlaik tiek atjaunināti un ietvers pastiprinātas darbības, kuru mērķis ir aizsargāt kritisko jūras infrastruktūru. Minētajām darbībām būtu jāpapildina šis ieteikums.

(21) Kritiskās infrastruktūras noturības stiprināšana sniedz ieguldījumu plašākos centienos apkarot pret Savienību un tās dalībvalstīm vērstus hibrīddraudus un hibrīdkampaņas. Šā ieteikuma pamatā ir kopīgais paziņojums Eiropas Parlamentam un Padomei "Kopīgs regulējums hibrīddraudu apkarošanai – Eiropas Savienības reakcija". Kopīgā regulējuma 1. darbībai, proti, pētījumam par hibrīda veida riskiem, ir būtiska nozīme tādas ievainojamības apzināšanā, kas var ietekmēt valstu un Eiropas struktūras un tīklus. Turklāt, īstenojot Padomes 2022. gada 21. jūnija secinājumus par satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, tiks nodrošināta stingrāka koordinēta rīcība, visās skartajās jomās piemērojot ES hibrīddraudu novēršanas rīkkopu,

IR PIEŅĒMUSI ŠO IETEIKUMU.

I NODAĻA MĒRĶIS, DARBĪBAS JOMA UN PRIORITĀTES

1. Šajā ieteikumā ir izklāstīta virkne mērķorientētu darbību Savienības un valstu līmenī, lai brīvprātīgi atbalstītu un uzlabotu kritiskās infrastruktūras noturību, īpašu uzmanību pievēršot kritiskajai infrastruktūrai ar būtisku pārrobežu nozīmi un noteiktās svarīgās nozarēs, piemēram, enerģētikā, digitālajā infrastruktūrā, transportā un kosmosā. Minētās mērķorientētās darbības ietver labāku sagatavotību, pastiprinātu reaģēšanu un starptautisko sadarbību.

2. Ar informāciju, kas ir konfidenciāla, ievērojot Savienības un valsts noteikumus, kā arī ar noteikumus par uzņēmējdarbības konfidencialitāti, un ko kopīgo nolūkā sasniegt šā ieteikuma mērķus, būtu jāapmainās ar Komisiju un citām attiecīgajām iestādēm tikai tad, ja šāda apmaiņa ir nepieciešama šā ieteikuma labai piemērošanai. Šis ieteikums neskar dalībvalstu būtisko interešu aizsardzību nacionālās drošības, sabiedriskās drošības vai aizsardzības jomā un ne no vienas dalībvalsts nebūtu jāsagaida, ka tā dalīsies ar informāciju, kas ir pretrunā šīm interesēm.

II NODAĻA UZLABOTA SAGATAVOTĪBA

Darbības dalībvalstu līmenī

3. Dalībvalstīm, atjauninot savus riska novērtējumus vai to esošās līdzvērtīgās analīzes, būtu jāapsver visu apdraudējumu pieeja saskaņā ar pašreizējo kritisko infrastruktūru apdraudējumu mainīgo raksturu, jo īpaši apzinātajās svarīgajās nozarēs un, ja iespējams, visās nozarēs, uz kurām attiecas gaidāmais jaunais tiesiskais regulējums, kas piemērojams kritiskajām vienībām.

4. Dalībvalstis tiek aicinātas paātrināt sagatavošanās darbu un, ja iespējams, pieņemt noturības uzlabošanas pasākumus, kā noteikts gaidāmajā tiesiskajā regulējumā, kas piemērojams kritiskajām vienībām, īpašu uzmanību pievēršot sadarbībai un attiecīgās informācijas apmaiņai starp dalībvalstīm un ar Komisiju, attiecībā uz kritisko vienību, kurām ir būtiska pārrobežu nozīme, apzināšanu un atbalsta palielināšanu apzinātajām kritiskajām vienībām nolūkā uzlabot to noturību.

5. Dalībvalstīm būtu jāatbalsta ekspertu apmācība un mācības un ekspertu savstarpēja dalīšanās ar paraugpraksi un gūto pieredzi. Dalībvalstīm eksperti būtu jāmudina piedalīties esošajās valsts un starptautiskajās apmācības platformās, piemēram, *UCPM* ietvaros.

6. Dalībvalstīm būtu jāmudina un jāatbalsta kritiskās infrastruktūras operatori vismaz enerģētikas nozarē, lai tie veiktu stresa testus, ja tas ir lietderīgi, ievērojot principus, par kuriem panākta kopīga vienošanās Savienības līmenī. Stresa testos būtu jānovērtē kritiskās infrastruktūras noturība pret antagonistiskiem cilvēka radītiem apdraudējumiem. Tāpēc dalībvalstīm būtu jācenšas identificēt attiecīgo kritisko infrastruktūru, kurai jāveic tests, un pēc iespējas drīz un ne vēlāk kā 2023. gada pirmajā ceturksnī apspriesties ar attiecīgajiem kritiskās infrastruktūras operatoriem. Turklāt dalībvalstīm būtu jāatbalsta kritiskās infrastruktūras operatori, lai tie veiktu minētos testus pēc iespējas ātrāk un ar mērķi tos pabeigt līdz 2023. gada beigām saskaņā ar valsts tiesību aktiem. Padome plāno līdz 2023. gada aprīļa beigām izvērtēt pašreizējo stāvokli saistībā ar stresa testiem.

7. Ņemot vērā strauji mainīgos apdraudējumus kritiskajai infrastruktūrai, ir ļoti svarīgi saglabāt tās augsta līmeņa aizsardzību. Dalībvalstis tiek mudinātas piešķirt pietiekamus finanšu resursus nolūkā stiprināt savu attiecīgo valsts iestāžu spējas un tās atbalstīt, lai varētu uzlabot kritiskās infrastruktūras noturību. Dalībvalstis tiek arī mudinātas piešķirt pietiekamus finanšu resursus iestādēm, kas atbild par liela mēroga kiberdrošības incidentu pārvaldību, nolūkā tās atbalstīt, un nodrošināt, ka to datordrošības incidentu reaģēšanas vienības (*CSIRT*) un kompetentās iestādes tiek pilnībā mobilizētas attiecīgi *CSIRT* tīklā un *EU-CyCLONe*.

8. Dalībvalstis tiek aicinātas saskaņā ar piemērojamajām prasībām izmantot Savienības un valsts līmeņa potenciālās finansēšanas iespējas, lai uzlabotu kritiskās infrastruktūras noturību Savienībā sev pašām, kā arī mudināt kritiskās infrastruktūras operatorus izmantot šādas finansēšanas iespējas, tostarp, piemēram, Eiropas komunikāciju tīklus, pret visiem būtiskiem apdraudējumiem, jo īpaši tādu programmu ietvaros, ko finansē no Iekšējās drošības fonda, kas izveidots ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/1149 [6], Eiropas Reģionālās attīstības fonda, kas izveidots ar Eiropas Parlamenta un Padomes Regulu (ES) 1301/2013 [7], Savienības civilās aizsardzības mehānisma un Komisijas plāna *REPowerEU*. Dalībvalstis tiek arī mudinātas pēc iespējas labāk izmantot pētniecības programmu, piemēram, pamatprogrammas "Apvārsnis Eiropa", kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/695 [8], attiecīgo projektu rezultātus.

---

[6] Eiropas Parlamenta un Padomes Regula (ES) 2021/1149 (2021. gada 7. jūlijs) par Iekšējās drošības fonda izveidi (OV L 251, 15.7.2021., 94. lpp.).

[7] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1301/2013 (2013. gada 17. decembris) par Eiropas Reģionālās attīstības fondu un īpašiem noteikumiem attiecībā uz mērķi "Investīcijas izaugsmei un nodarbinātībai" un ar ko atceļ Regulu (EK) Nr. 1080/2006 (OV L 347, 20.12.2013., 289. lpp.).

[8] Eiropas Parlamenta un Padomes Regula (ES) 2021/695 (2021. gada 28. aprīlis), ar ko izveido pētniecības un inovācijas pamatprogrammu "Apvārsnis Eiropa", nosaka tās dalības un rezultātu izplatīšanas noteikumus un atceļ Regulas (ES) Nr. 1290/2013 un (ES) Nr. 1291/2013 (OV L 170, 12.5.2021., 1. lpp.).

9. Attiecībā uz sakaru un tīklu infrastruktūru Savienībā TID sadarbības grupa tiek aicināta, rīkojoties saskaņā ar Direktīvas (ES) 2016/1148 11. pantu, paātrināt pašreizējo darbu, kura pamatā ir Nevēras ministru kopīgais aicinājums sagatavot mērķorientētu riska novērtējumu, un tai būtu pēc iespējas drīz jānāk klajā ar pirmajiem ieteikumiem. Minētajā riska novērtējumā būtu jāsniedz informācija par notiekošo starpnozaru kiberrisku izvērtēšanu un scenārijiem, kas prasīti Padomes secinājumos par ES pozīciju kiberjautājumos. Turklāt minētais darbs būtu jāveic, nodrošinot saskaņotību un papildināmību ar darbu, ko veic TID sadarbības grupas darba grupa informācijas un komunikācijas tehnoloģiju piegādes ķēdes drošības jomā, kā arī citas attiecīgās grupas.

10. TID sadarbības grupa tiek arī aicināta ar Komisijas un *ENISA* atbalstu turpināt darbu digitālās infrastruktūras drošības jomā, arī saistībā ar zemūdens infrastruktūru, proti, zemūdens sakaru kabeļiem. Tā tiek arī aicināta sākt darbu kosmosa nozarē, tostarp, vajadzības gadījumā sagatavojot politikas norādes un kiberdrošības riska pārvaldības metodiku, kuru pamatā ir visu apdraudējumu pieeja un uz risku balstīta pieeja kosmosa nozares operatoriem ar mērķi palielināt tādas uz zemes izvietotas infrastruktūras noturību, kura atbalsta kosmosā balstītu pakalpojumu sniegšanu.

11. Dalībvalstīm būtu pilnībā jāizmanto kiberdrošības sagatavotības pakalpojumi, kas tiek piedāvāti Komisijas īstermiņa atbalsta programmā, kuru īsteno kopā ar *ENISA*, piemēram, ielaušanās testēšana ievainojamības noteikšanai, un šajā sakarā tās tiek mudinātas piešķirt prioritāti vienībām, kas ekspluatē kritisko infrastruktūru enerģētikas, digitālās infrastruktūras un transporta nozarē.

12. Dalībvalstīm būtu pilnībā jāizmanto Eiropas Kiberdrošības kompetences centrs (*ECCC*). Dalībvalstīm būtu jāmudina savi nacionālie koordinācijas centri proaktīvi sadarboties ar kiberdrošības kopienas locekļiem, lai Savienības un valstu līmenī veidotu spēju labāk atbalstīt pamatpakalpojumu sniedzējus.

13. Ir svarīgi, ka dalībvalstis panāk tādu pasākumu īstenošanu, kas ieteikti ES 5G kiberdrošības rīkkopā, un jo īpaši, ka dalībvalstis ievieš ierobežojumus augsta riska piegādātājiem, ņemot vērā, ka laika zaudēšana var palielināt tīklu ievainojamību Savienībā, un arī pastiprina kritiskās un sensitīvās 5G tīklu daļas fizisko un nefizisko aizsardzību, tostarp veicot stingru piekļuves kontroli. Turklāt dalībvalstīm sadarbībā ar Komisiju būtu jānovērtē, vai ir vajadzīga papildu rīcība, lai nodrošinātu 5G tīklu konsekventu drošības un noturības līmeni.

14. Dalībvalstīm kopā ar Komisiju un *ENISA* būtu jākoncentrējas uz to, lai īstenotu Padomes 2022. gada 17. oktobra secinājumus par IKT piegādes ķēdes drošību.

15. Dalībvalstīm būtu jāņem vērā gaidāmais tīkla kodekss attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem [...], pamatojoties uz pieredzi, kas gūta Direktīvas (ES) 2016/1148 īstenošanā, un attiecīgajiem norādījumiem, ko sagatavojusi TID sadarbības grupa, jo īpaši tās atsauces dokumentu par drošības pasākumiem pamatpakalpojumu sniedzējiem.

16. Dalībvalstīm būtu jāattīsta *Copernicus*, *Galileo* un Eiropas Ģeostacionārās navigācijas pārklājuma dienesta (*EGNOS*) izmantošana novērošanai, lai apmainītos ar attiecīgo informāciju ar ekspertiem, kas sasaukti saskaņā ar 15. punktu. Būtu pienācīgi jāizmanto Savienības kosmosa programmas Savienības valdības satelītsakaru (*GOVSATCOM*) sniegtās iespējas, lai uzraudzītu kritisko infrastruktūru un atbalstītu krīzes situāciju paredzēšanu un reaģēšanu krīzes situācijās.

Darbības Savienības līmenī

17. Būtu jāpastiprina dialogs un sadarbība starp dalībvalstu izraudzītajiem ekspertiem un ar Komisiju nolūkā uzlabot kritiskās infrastruktūras fizisko noturību, jo īpaši:

a) palīdzot sagatavot, izstrādāt un popularizēt kopīgus brīvprātīgus rīkus, ar ko atbalsta dalībvalstis šādas noturības uzlabošanā, ietverot metodiku un riska scenārijus;

b) palīdzot dalībvalstīm īstenot jauno tiesisko regulējumu, kas piemērojams kritiskajām vienībām, tostarp mudinot Komisiju laikus pieņemt deleģēto aktu;

c) atbalstot 6. punktā minēto stresa testu veikšanu, pamatojoties uz kopīgiem principiem, sākot ar šādiem testiem, kas vērsti uz antagonistiskiem cilvēka radītiem draudiem enerģētikas nozarē un pēc tam – citās svarīgajās nozarēs, kā arī pēc dalībvalsts pieprasījuma atbalstot šādu stresa testu veikšanu un konsultējot par to;

d) izmantojot jebkādu drošu platformu – tiklīdz Komisija tādu būs izveidojusi –, kur brīvprātīgi vākt, izvērtēt un apmainīties ar paraugpraksi, mācībām, kas gūtas no valstu pieredzes, un citu informāciju, kas saistīta ar šādu noturību.

Minēto izraudzīto ekspertu darbā īpaša uzmanība būtu jāpievērš starpnozaru atkarībai un kritiskajai infrastruktūrai ar ievērojamu pārrobežu nozīmību, un attiecīgā gadījumā būtu jāveic turpmāki pasākumi Padomē un Komisijā.

18. Dalībvalstis tiek mudinātas izmantot jebkādu atbalstu, ko piedāvā Komisija, piemēram, izstrādājot rokasgrāmatas un pamatnostādnes, piemēram, rokasgrāmatu par kritiskās infrastruktūras un publiskās telpas aizsardzību pret bezpilota gaisa kuģu sistēmām, un riska novērtēšanas rīkus. EĀDD, jo īpaši ar ES Izlūkošanas un situāciju centra un tā Hibrīddraudu analīzes vienības starpniecību un ar ESMŠ Izlūkošanas direktorāta atbalstu saskaņā ar *SIAC* satvaru, tiek aicināts sniegt informatīvus paziņojumus par kritiskās infrastruktūras apdraudējumu Savienībā, lai uzlabotu situācijas apzināšanos.

19. Dalībvalstīm būtu jāatbalsta darbības, ko Komisija veic, lai izmantotu to projektu rezultātus, kuri saistīti ar kritiskās infrastruktūras noturību un kurus finansē saskaņā ar Savienības pētniecības un inovācijas programmām. Padome pieņem zināšanai Komisijas nodomu budžetā, kas saskaņā ar daudzgadu finanšu shēmu 2021.–2027. gadam piešķirts pamatprogrammai "Apvārsnis Eiropa", palielināt finansējumu šādai noturībai, nemazinot finansējumu pārējiem ar civilo drošību saistītiem pētniecības un inovācijas projektiem pamatprogrammas "Apvārsnis Eiropa" ietvaros.

20. Saistībā ar Padomes secinājumos par ES pozīciju kiberjautājumos noteiktajiem uzdevumiem Komisija, Augstais pārstāvis un TID sadarbības grupa tiek aicināti saskaņā ar saviem attiecīgajiem uzdevumiem un pienākumiem, kas noteikti Savienības tiesību aktos, pastiprināt darbu ar attiecīgajiem tīkliem un civilajām un militārajām struktūrām un aģentūrām riska izvērtēšanā un kiberdrošības riska scenāriju izstrādē, ņemot vērā jo īpaši enerģētikas, digitālās infrastruktūras, transporta un kosmosa infrastruktūras nozīmību un nozaru un dalībvalstu savstarpējo atkarību. Veicot minēto izvērtēšanu, būtu jāņem vērā saistītie riski infrastruktūrai, uz kuru balstās minētās nozares. Ja tas ir lietderīgi, riska izvērtēšanu un scenāriju izstrādi varētu veikt regulāri, un ar to būtu jāpapildina esošie vai plānotie riska novērtējumi minētajās nozarēs, jābalstās uz tiem un jānovērš dublēšanās ar tiem, un tie būtu jāņem vērā diskusijās par to, kā stiprināt kritisko infrastruktūru ekspluatējošo vienību vispārējo noturību un pārvaldīt ievainojamību.

21. Komisija tiek aicināta saskaņā ar saviem attiecīgajiem uzdevumiem saistībā ar kiberkrīžu pārvarēšanu paātrināt savas darbības, kuru mērķis ir atbalstīt dalībvalstu sagatavotību un reaģēšanu uz liela mēroga kiberdrošības incidentiem, un jo īpaši:

a) lai papildinātu attiecīgos riska novērtējumus saistībā ar tīklu un informācijas drošību, veikt visaptverošu pētījumu [9], kurā tiktu izvērtēta zemūdens infrastruktūra, proti, zemūdens sakaru kabeļi, kas savieno dalībvalstis, kā arī Eiropu visā pasaulē, un kura konstatējumi būtu jādara zināmi dalībvalstīm;

b) atbalstīt dalībvalstu un Savienības iestāžu, struktūru un aģentūru gatavību liela mēroga kiberdrošības incidentiem vai būtiskiem incidentiem un to reaģēšanu uz tiem saskaņā ar pastiprināto kiberdrošības tiesisko regulējumu un citiem attiecīgiem piemērojamiem noteikumiem [10];

c) paātrināt Ārkārtas kiberfonda galvenās koncepcijas izstrādi, pienācīgi apspriežoties ar dalībvalstīm.

22. Komisija tiek mudināta pastiprināti veikt tālredzīgus priekšdarbus, tostarp sadarboties ar dalībvalstīm saskaņā ar Lēmuma 1313/2013/ES 6. un 10. pantu, un ārkārtas situāciju plānošanas veidā atbalstīt Ārkārtas reaģēšanas koordinēšanas centra (*ERCC*) operatīvo sagatavotību un reaģēšanu uz kritiskās infrastruktūras traucējumiem; palielināt investīcijas profilaktiskās pieejās un iedzīvotāju sagatavotībā; un palielināt atbalstu, kas saistīts ar spēju veidošanu Savienības Civilās aizsardzības zināšanu tīkla ietvaros.

---

9 Šajā pētījumā cita starpā būtu jāapzina tās spējas un rezerves, ievainojamība, draudi un riski attiecībā uz pakalpojumu pieejamību, (transatlantisko) zemūdens kabeļu dīkstāves ietekme uz dalībvalstīm un Savienību kopumā un riska mazināšana, vienlaikus ņemot vērā šādas informācijas sensitivitāti un nepieciešamību to aizsargāt.

10 Īpaša uzmanība būtu jāpievērš arī visām darbībām, ar ko gatavojas efektīvai un koordinētai Savienības līmeņa reakcijai liela pārrobežu kiberincidenta vai saistīta apdraudējuma gadījumā, kam varētu būt sistēmiska ietekme uz Savienības finanšu nozari, kā noteikts jaunajā tiesiskajā regulējumā par digitālās darbības noturību.

23. Komisijai būtu jāveicina Savienības novērošanas resursu (*Copernicus*, *Galileo* un *EGNOS*) izmantošana, lai atbalstītu dalībvalstis kritiskās infrastruktūras un attiecīgā gadījumā to tuvākās apkārtnes uzraudzībā un atbalstītu citas novērošanas iespējas, kas paredzētas Savienības kosmosa programmā, piemēram, kosmosa situācijas apzināšanās un ES kosmisko objektu novērošanas un uzraudzības sistēmas.

24. Attiecīgā gadījumā un saskaņā ar savām attiecīgajām pilnvarām Savienības aģentūras un citas attiecīgās struktūras tiek aicinātas sniegt atbalstu jautājumos, kas saistīti ar kritiskās infrastruktūras noturību, jo īpaši:

a) Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai (Eiropols) par informācijas vākšanu, kriminālizlūkošanas datu analīzi un izmeklēšanas atbalstu pārrobežu tiesībaizsardzības darbībās, un attiecīgā gadījumā rezultātu apmaiņu ar dalībvalstīm;

b) Eiropas Jūras drošības aģentūra (*EMSA*) par jautājumiem, kas saistīti ar jūrniecības nozares drošību un drošumu Savienībā, tostarp par jūras uzraudzības pakalpojumiem ar jūras drošību un drošumu saistītos jautājumos;

c) Eiropas Savienības Kosmosa programmas aģentūra (*EUSPA*) un ES Satelītcentrs (*SatCen*) var palīdzēt, veicot darbības Savienības kosmosa programmas ietvaros;

d) *ECCC* attiecībā uz darbībām, kas saistītas ar kiberdrošību, arī sadarbībā ar *ENISA* varētu atbalstīt inovāciju un rūpniecības politiku kiberdrošības jomā.

III NODAĻA. PASTIPRINĀTA REAĢĒŠANA

Darbības dalībvalstu līmenī

25. Dalībvalstis tiek aicinātas:

a) turpināt koordinēt savu reakciju, ja nepieciešams, un uzturēt pārskatu par starpnozaru reaģēšanu uz akūtiem kritiskās infrastruktūras sniegto pamatpakalpojumu traucējumiem. Šādā nolūkā varētu izmantot gaidāmo plānu koordinētai reaģēšanai uz tādas kritiskās infrastruktūras traucējumiem, kurai ir būtiska pārrobežu nozīme; pastāvošos integrētos krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismus – politiskai reakcijai gadījumos, kas skar kritisko infrastruktūru ar pārrobežu nozīmi; plānu reaģēšanai uz liela mēroga kiberdrošības incidentiem un krīzēm saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 [11]; *EU-CyCLONe*; satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām un ES hibrīddraudu novēršanas rīkkopu – hibrīddraudu un hibrīdkampaņu gadījumos; un ātrās brīdināšanas sistēmu – dezinformācijas gadījumos;

b) *UCPM* ietvaros palielināt operatīvā līmeņa informācijas apmaiņu ar Ārkārtas reaģēšanas koordinēšanas centru (*ERCC*), lai uzlabotu agrīno brīdināšanu un koordinētu savu reakciju *UCPM* ietvaros, ja traucēta kritiskā infrastruktūra ar būtisku pārrobežu nozīmi, tādējādi vajadzības gadījumā nodrošinot ātrāku Savienības atbalstītu reaģēšanu;

c) palielināt gatavību reaģēt, vajadzības gadījumā izmantojot esošos vai turpmāk izstrādātus rīkus, lai reaģētu uz šādiem a) punktā minētiem būtiskiem traucējumiem;

[11] 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.).

d) iesaistīties, lai pilnveidotu attiecīgās reaģēšanas spējas Eiropas civilās aizsardzības rezervē (*ECPP*) un *rescEU*;

e) mudināt kritisko infrastruktūru operatorus un attiecīgās valsts iestādes uzlabot spējas ātri atjaunot minēto kritiskās infrastruktūras operatoru sniegtos pamatpakalpojumus elementārā līmenī;

f) mudināt kritiskās infrastruktūras operatorus, kad tie atjauno kritisko infrastruktūru, to būvēt pēc iespējas noturīgāku un ņemt vērā to, cik lielā mērā pasākumi atbilst riska novērtējumiem un izmaksām, aptverot visus būtiskos riskus, kas uz to var attiekties, tostarp nelabvēlīgus klimata scenārijus.

26. Dalībvalstis tiek aicinātas paātrināt sagatavošanās darbu, kad iespējams, kā uzdots pastiprinātajā kiberdrošības tiesiskajā regulējumā, cenšoties uzlabot valstu *CSIRT* spējas, ņemot vērā *CSIRT* jaunos uzdevumus, kā arī vienību pieaugušo skaitu no jaunām nozarēm, savlaicīgi pārskatot un atjauninot savas kiberdrošības stratēģijas, un pēc iespējas drīz pieņemot valstu plānus reaģēšanai uz kiberdrošības incidentiem un krīzēm, ja tādu vēl nav.

27. Dalībvalstis tiek aicinātas valsts līmenī pārdomāt, kādi būtu paši piemērotākie paņēmieni, ar kuriem panākt, ka attiecīgās ieinteresētās personas apzinās nepieciešamību uzlabot kritiskās infrastruktūras noturību sadarbībā ar uzticamiem piegādātājiem un partneriem. Ir svarīgi ieguldīt papildu spējā, īpaši jomās, kur esošajai infrastruktūrai tuvojas ekspluatācijas beigu termiņš, piemēram, tāda ir zemūdens sakaru kabeļu infrastruktūra, lai varētu nodrošināt pamatpakalpojumu nepārtrauktu sniegšanu traucējumu gadījumā un samazināt nevēlamu atkarību.

28. Dalībvalstis tiek aicinātas pievērst uzmanību proaktīvai stratēģiskajai saziņai valsts līmenī saistībā ar hibrīddraudu un hibrīdkampaņu apkarošanu un ņemot vērā varbūtību, ka pretinieki var censties izmantot ārvalstu īstenotu informācijas manipulāciju un iejaukšanos,veidojot naratīvus saistībā ar incidentiem, kas vērsti pret kritisko infrastruktūru.

Darbības Savienības līmenī

29. Lai uzlabotu operatīvo gatavību novērst tūlītējās un netiešās sekas, ko rada būtiski kritiskās infrastruktūras sniegto attiecīgo pamatpakalpojumu traucējumi, Komisija tiek aicināta cieši sadarboties ar dalībvalstīm, lai pilnveidotu attiecīgās struktūras, instrumentus un reaģēšanas spējas, jo īpaši ekspertus un resursus, kas pieejami Eiropas civilās aizsardzības rezervē un *rescEU* no *UCPM* vai nākotnes hibrīddraudu novēršanas ātrās reaģēšanas vienībām.

30. Ņemot vērā, ka apdraudējumu aina mainās, un sadarbībā ar dalībvalstīm Komisija tiek aicināta saistībā ar *UCPM*:

a) pastāvīgi analizēt un testēt esošo reaģēšanas spēju piemērotību un operatīvo gatavību;

b) regulāri uzraudzīt, vai Eiropas civilās aizsardzības rezerves un *rescEU* spēju jomā pastāv potenciāli būtiski reaģēšanas spēju trūkumi, un tos apzināt;

c) vēl vairāk pastiprināt starpnozaru sadarbību, lai nodrošinātu pienācīgu reaģēšanu Savienības līmenī, un organizēt regulāru apmācību vai mācības, lai šo sadarbību testētu kopā ar vienu vai vairākām dalībvalstīm;

d) pilnveidot *ERCC* kā starpnozaru ārkārtas situāciju centru Savienības līmenī, kura uzdevums būtu koordinēt atbalsta sniegšanu skartajām dalībvalstīm.

31. Padome ir apņēmusies sākt darbu, lai apstiprinātu plānu koordinētai reaģēšanai uz kritiskās infrastruktūras ar būtisku pārrobežu nozīmi traucējumiem, kurā aprakstīti un noteikti mērķi un sadarbības veidi, kā tiek īstenota sadarbība starp dalībvalstīm un ES iestādēm, struktūrām, birojiem un aģentūrām, reaģējot uz incidentiem, kas vērsti pret šādu kritisko infrastruktūru. Padome gaida Komisijas sagatavotu šāda plāna projektu, kura izstrādē izmantots attiecīgu Savienības aģentūru atbalsts un ieguldījums. Plānā nodrošina pilnīgu saskaņotību un sadarbspēju ar pārskatīto Savienības operatīvo protokolu hibrīddraudu apkarošanai ("*EU Playbook*") un ņem vērā esošo plānu koordinētai reaģēšanai uz liela mēroga pārrobežu kiberdrošības incidentiem [12] un krīzēm, un *EU CyCLONe* pilnvaras, kas paredzētas TID 2 direktīvā, un nepieļauj struktūru un darbību dublēšanos. Minētajā plānā būtu pilnībā jāņem vērā esošie *IPCR* mehānismi, kas paredzēti reaģēšanas koordinēšanai.

[12] Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

32. Komisija tiek aicināta ar attiecīgajām ieinteresētajām personām un ekspertiem apspriest pasākumus, kas būtu piemēroti saistībā ar iespējamiem būtiskiem incidentiem, kuri skar zemūdens infrastruktūru – tie jāiesniedz kopā ar 20. punkta a) apakšpunktā minēto novērtēšanas pētījumu, – kā arī turpināt izstrādāt ārkārtas situāciju plānus, riska scenārijus un Savienības mērķus noturības pret katastrofām jomā, kas izklāstīti Lēmumā Nr. 1313/2013/ES.

IV NODAĻA. STARPTAUTISKĀ SADARBĪBA

Darbības dalībvalstu līmenī

33. Dalībvalstīm, attiecīgos gadījumos un saskaņā ar Savienības tiesību aktiem, būtu jāsadarbojas ar attiecīgajām trešām valstīm jautājumos, kas skar kritiskās infrastruktūras ar pārrobežu nozīmi noturību.

34. Dalībvalstis tiek mudinātas sadarboties ar Komisiju un Augsto pārstāvi, lai efektīvi pārvaldītu riskus, kas saistīti ar kritisko infrastruktūru starptautiskajos ūdeņos.

35. Dalībvalstis tiek aicinātas sadarbībā ar Komisiju un Augsto pārstāvi sniegt ieguldījumu, lai tiktu ātrāk izstrādātas un īstenotas un pēc tam izmantotas ES hibrīddraudu novēršanas rīkkopa un īstenošanas pamatnostādnes, kas minētas Padomes 2022. gada 21. jūnija secinājumos par satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, ar mērķi pilnībā īstenot satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, jo īpaši, kad tiek apsvērta un sagatavota visaptveroša un koordinēta Savienības reakcija uz hibrīdkampaņām un hibrīdapdraudējumiem, tostarp tādiem, kas vērsti pret kritiskās infrastruktūras operatoriem.

Darbības Savienības līmenī

36. Komisija un Augstais pārstāvis tiek aicināti attiecīgā gadījumā un saskaņā ar saviem attiecīgajiem uzdevumiem un pienākumiem, kuri noteikti Savienības tiesību aktos, atbalstīt attiecīgās trešās valstis, lai uzlabotu to teritorijā esošās kritiskās infrastruktūras noturību un jo īpaši tās kritiskās infrastruktūras noturību, kas ir fiziski savienota ar to teritoriju un kādas dalībvalsts teritoriju.

37. Komisija un Augstais pārstāvis saskaņā ar saviem attiecīgajiem uzdevumiem un pienākumiem, kuri noteikti Savienības tiesību aktos, stiprinās koordināciju ar NATO jautājumos, kas saistīti ar kopīgu interešu kritiskās infrastruktūras noturību, šādā nolūkā izmantojot ES un NATO strukturēto dialogu par noturību, pilnībā ievērojot Savienības un dalībvalstu kompetences atbilstoši Līgumiem un ES un NATO sadarbības pamatprincipus, par kuriem vienojusies Eiropadome, jo īpaši savstarpīgumu, iekļautību un lēmumu pieņemšanas autonomiju. Ņemot to vērā, minētā sadarbība tiks pilnveidota ES un NATO strukturētajā dialogā par noturību, kas iestrādāts esošajā personāla līmeņa mehānismā, kurš paredzēts kopīgo deklarāciju īstenošanai, vienlaikus nodrošinot pilnīgu pārredzamību un visu dalībvalstu iesaisti.

38. Komisija tiek aicināta apsvērt attiecīgo trešo valstu pārstāvju dalību, ja tas ir nepieciešams un lietderīgi, satvarā, kas paredzēts sadarbībai un informācijas apmaiņai starp dalībvalstīm saistībā ar tādas kritiskās infrastruktūras noturību, kas ir fiziski savienota ar kādas dalībvalsts teritoriju un kādas trešās valsts teritoriju.

[vieta], … [datums]

Padomes vārdā –

priekšsēdētājs