EIROPAS
KOMISIJA

Strasbūrā, 18.10.2022.
COM(2022) 551 final

2022/0338 (NLE)

Priekšlikums

PADOMES IETEIKUMS

par koordinētu Savienības pieeju kritiskās infrastruktūras noturības stiprināšanai

(Dokuments attiecas uz EEZ)

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Drošība ir būtisks Eiropas Savienības mērķis. Lai gan par pilsoņu aizsardzību galvenokārt ir atbildīgas dalībvalstis, kolektīva rīcība Savienības līmenī sniedz būtisku ieguldījumu visas ES drošībā. Koordinācija palīdz attīstīt noturību, uzlabot modrību un stiprināt mūsu kolektīvo reaģēšanu. ES drošības savienības kontekstā ir veikti svarīgi pasākumi, lai uzkrātu spēkus un spējas novērst un atklāt daudzus drošības apdraudējumus un ātri reaģēt uz tiem, kā arī iesaistīt kopīgos centienos publiskā un privātā sektora dalībniekus.

Lai ES spētu tikt galā ar mūžam mainīgo drošības apdraudējuma ainu, ir vajadzīga pastāvīga modrība un pielāgošanās. Krievijas agresijas karš pret Ukrainu ir radījis jaunus riskus, kas bieži vien izpaužas apvienoti kā hibrīdapdraudējums. Viens no tiem ir risks, ka vienībām, kas Eiropā ekspluatē kritisko infrastruktūru, varētu traucēt pamatpakalpojumu sniegšanu. Tas ir kļuvis vēl skaidrāks līdz ar *Nord Stream* gāzes cauruļvadu acīmredzamo sabotāžu un citiem neseniem incidentiem. Sabiedrība lielā mērā ir atkarīga gan no fiziskās, gan digitālās infrastruktūras, un pamatpakalpojumu pārtraukšana, izmantojot vai nu konvencionālus fiziskus uzbrukumus, vai kiberuzbrukumus, vai abu apvienojumu, var nopietni ietekmēt iedzīvotāju labklājību, mūsu ekonomiku un uzticēšanos mūsu demokrātiskajām sistēmām.

Turklāt vēl viens svarīgs ES mērķis ir iekšējā tirgus netraucētas darbības nodrošināšana, t. sk. attiecībā uz pamatpakalpojumiem, ko sniedz vienības, kuras ekspluatē kritisko infrastruktūru. Tāpēc ES jau ir veikusi vairākus pasākumus, lai samazinātu kritisko vienību ievainojamību un palielinātu to noturību gan attiecībā uz kiberriskiem, gan riskiem, kas nav saistīti ar kiberdrošību.

Ir steidzami jārīkojas, lai palielinātu ES spēju stāties pretī iespējamiem uzbrukumiem kritiskajai infrastruktūrai, galvenokārt pašā ES, bet attiecīgos gadījumos arī tās tiešajās kaimiņvalstīs.

Ierosinātā Padomes ieteikuma mērķis ir pastiprināt ES atbalstu kritiskās infrastruktūras noturības palielināšanai un nodrošināt ES līmeņa koordināciju attiecībā uz sagatavotību un reaģēšanu. Tā mērķis ir maksimāli izvērst un paātrināt darbu, lai aizsargātu ekonomikas darbībai nepieciešamos aktīvus, objektus un sistēmas un iekšējā tirgū sniegtu pamatpakalpojumus, uz kuriem paļaujas iedzīvotāji, kā arī mazināt jebkura uzbrukuma ietekmi, nodrošinot pēc iespējas drīzu atveseļošanu. Lai gan būtu jāaizsargā visa šāda veida infrastruktūra, pašlaik galvenā prioritāte ir tādas nozares kā enerģētika, digitālā infrastruktūra, transports un kosmoss, ņemot vērā to īpaši horizontālo raksturu attiecībā uz sabiedrību un ekonomiku, kā arī pašreizējos riska novērtējumus.

ES ir īpaša loma tādas infrastruktūras noturības nodrošināšanā, kas šķērso sauszemes vai jūras robežas un ietekmē vairāku dalībvalstu intereses vai ko izmanto pārrobežu pamatpakalpojumu sniegšanai. Tomēr vairākām dalībvalstīm būtiska kritiskā infrastruktūra, kā, piemēram, zemūdens kabeļi vai cauruļvadi, var atrasties tikai vienā dalībvalstī vai pat ārpus dalībvalsts teritorijas. Visu dalībvalstu un visas ES interesēs ir skaidri apzināt kritisko infrastruktūru un vienības, kas to ekspluatē, kā arī riskus, kas tām draud, un kolektīvi apņemties tās aizsargāt.

Eiropas Parlaments un Padome jau ir panākuši politisku vienošanos padziļināt ES tiesisko regulējumu, lai palīdzētu stiprināt to vienību noturību, kuras ekspluatē kritisko infrastruktūru. 2022. gada vasarā tika panākta vienošanās par Direktīvu par kritiskās infrastruktūras noturību

("*CER* direktīva")[1] un pārskatīto Tīklu un informācijas sistēmu drošības direktīvu ("TID 2 direktīva")[2]. Salīdzinājumā ar spēkā esošo tiesisko regulējumu, 2008. gada 8. decembra Direktīvu 2008/114/EK par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību ("EKI direktīva")[3], un Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā ("TID direktīva")[4], tās nozīmēs spēju uzlabojumu ievērojamā apmērā. Paredzams, ka jaunie tiesību akti stāsies spēkā 2022. gada beigās vai 2023. gada sākumā, un dalībvalstīm to transponēšana un piemērošana saskaņā ar Savienības tiesību aktiem būtu jānosaka par prioritāti.

Tādējādi un ņemot vērā iespējamo steidzamo vajadzību pārvaldīt apdraudējumus, ko rada Krievijas agresijas karš pret Ukrainu, jaunajos tiesību aktos izklāstītie pasākumi, ja iespējams, būtu jāveic jau no šodienas. Savstarpējās sadarbības pastiprināšana jau tagad arī palīdzētu radīt impulsu efektīvai īstenošanai, kad jaunie tiesību akti būs pilnībā stājušies spēkā.

Rezultātā gan attiecībā uz darbības dziļumu, gan aptverto nozaru plašumu jau tagad tiktu pārsniegts pašreizējais regulējums. Jaunajā *CER* direktīvā, konkrēti norādot vienpadsmit nozares[5], ir ierosināts jauns sadarbības satvars, kā arī pienākumi dalībvalstīm un kritiskajām vienībām, kuru mērķis ir stiprināt fizisko noturību, kas nav kibernoturība, pret dabas un cilvēka izraisītiem apdraudējumiem vienībām, kuras sniedz pamatpakalpojumus iekšējā tirgū. Ar TID 2 direktīvu tiks ieviests plašs kiberdrošības pienākumu nozaru aptvērums. Tas ietvers jaunu prasību dalībvalstīm attiecīgā gadījumā iekļaut savās kiberdrošības stratēģijās zemūdens kabeļus.

Tiesību aktos ir noteikts, ka Komisijai jāuzņemas ievērojama koordinatores loma. Saskaņā ar *CER* direktīvu Komisijai ir atbalstītājas un veicinātājas loma, kas jāīsteno, izmantojot ar minēto direktīvu izveidotās Kritisko vienību noturības grupas (*CERG*) atbalstu un iesaisti, un Komisijai būtu jāpapildina dalībvalstu darbības, izstrādājot paraugpraksi, norādījumus un metodiku. Attiecībā uz kiberdrošību Padome jau savos secinājumos par ES pozīciju kiberjautājumos 2022. gada vasarā aicināja Komisiju, Augsto pārstāvi un TID sadarbības grupu strādāt pie riska novērtējumiem un scenārijiem no kiberdrošības viedokļa. Šāda koordinācija var iedvesmot pieeju attiecībā uz citu svarīgu kritisko infrastruktūru.

2022. gada 5. oktobrī Komisijas priekšsēdētāja fon der Leiena nāca klajā ar piecu punktu plānu, kurā izklāstīta koordinēta pieeja nepieciešamajam turpmākajam darbam. Tā galvenie elementi bija šādi: uzlabot sagatavotību; sadarboties ar dalībvalstīm, lai veiktu to kritiskās infrastruktūras stresa testus, sākumā enerģētikas nozarei un pēc tam — citām augsta riska nozarēm; palielināt reaģēšanas spējas, jo īpaši izmantojot Savienības civilās aizsardzības mehānismu; pienācīgi izmantot satelītu spējas, lai atklātu iespējamos apdraudējumus; kā arī stiprināt sadarbību ar NATO un galvenajiem partneriem kritiskās infrastruktūras noturības jomā. Piecu punktu plānā tika uzsvērts, cik svarīgi ir virzīt tiesību aktus, par kuriem jau ir panākta politiska vienošanās.

Ierosinātajā Padomes ieteikumā šī pieeja ir novērtēta atzinīgi, lai strukturētu atbalstu dalībvalstīm un koordinētu to centienus palielināt informētību par risku, sagatavotību un spēju reaģēt uz pašreizējiem apdraudējumiem. Šajā sakarā tiek sasauktas ekspertu sanāksmes, lai

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 OV L 345, 23.12.2008.
4 OV L 194, 19.7.2016.
5 Enerģētika, transports, digitālā infrastruktūra, bankas, finanšu tirgus infrastruktūra, veselība, dzeramais ūdens, notekūdeņi, publiskā pārvalde, kosmoss un pārtika.

apspriestu kritisko infrastruktūru ekspluatējošo vienību noturību, gaidot *CER* direktīvas un ar to izveidotās *CERG* stāšanos spēkā.

Būtiska nozīme būs pastiprinātai sadarbībai ar galvenajiem partneriem un kaimiņvalstīm un citām iesaistītajām trešām valstīm to vienību noturības jomā, kuras ekspluatē kritisko infrastruktūru, jo īpaši izmantojot ES un NATO strukturēto dialogu par noturību.

Šā ieteikuma mērķis ir stiprināt Savienības spēju paredzēt un novērst jaunos apdraudējumus, ko rada Krievijas agresijas karš pret Ukrainu, un reaģēt uz tiem. Tāpēc ierosinātajos ieteikumos galvenā uzmanība pievērsta ar drošību saistīto risku un kritiskās infrastruktūras apdraudējumu pārvaldībai. Tomēr jāatzīmē, ka nesenie notikumi ir arī uzsvēruši neatliekamo vajadzību pievērst pastiprinātu uzmanību klimata pārmaiņu ietekmei uz kritisko infrastruktūru un pakalpojumiem, piemēram, uz sezonāli traucētu un neprognozējamu ūdensapgādi kodolelektrostaciju dzesēšanai, hidroenerģijai un iekšzemes kuģošanai, vai arī būtiska kaitējuma riskam transporta infrastruktūrā, kurš var radīt nozīmīgus traucējumus pamatpakalpojumu sniegšanā. Šie problēmjautājumi arī turpmāk tiks risināti ar attiecīgiem tiesību aktiem un koordināciju.

- **Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā**

Šis Padomes ieteikuma priekšlikums pilnībā atbilst pašreizējam un gaidāmajam tiesiskajam regulējumam par kritisko infrastruktūru ekspluatējošo vienību noturību, attiecīgi EKI direktīvai un *CER* direktīvai, jo tā mērķis citstarp ir veicināt sadarbību starp dalībvalstīm šajā jomā un atbalstīt konkrētus pasākumus, lai uzlabotu noturību pret pašreizējiem tūlītējiem apdraudējumiem vienībām, kas ekspluatē kritisko infrastruktūru ES.

Tas arī papildina *CER* direktīvu un veic tai priekšdarbus, jau aicinot dalībvalstis par prioritāti noteikt direktīvas savlaicīgu transponēšanu, sadarbojoties ekspertu sanāksmēs, kas tiek sasauktas kā daļa no Komisijas izziņotā 5 punktu plāna, un cenšoties koordinēt ceļu uz kopīgu pieeju kritiskās infrastruktūras noturības testu veikšanai ES.

Aicinot drīz sākt īstenošanas un transponēšanas darbu, priekšlikums atbilst arī TID direktīvai un gaidāmajai TID 2 direktīvai, ar ko atcels TID direktīvu. Tas atspoguļo arī Nevēras 2022. gada marta kopīgo aicinājumu, kā arī Padomes 2022. gada maija secinājumus par ES pozīciju kiberjautājumos attiecībā uz dalībvalstu lūgumu Komisijai izstrādāt riska novērtējumus un riska scenārijus.

Priekšlikums atbilst arī ES civilās aizsardzības politikai, kura nosaka: ja tiek būtiski traucēta kritiskās infrastruktūras vai kritisko vienību darbība, dalībvalstis un trešās valstis Savienības civilās aizsardzības mehānisma (*UCPM*) ietvaros var lūgt palīdzību, izmantojot Ārkārtas reaģēšanas koordinēšanas centru (*ERCC*). *UCPM* aktivizācijas gadījumā *ERCC* spēj koordinēt un līdzfinansēt būtiska dalībvalstīs (daļēji saistībā ar Eiropas civilās aizsardzības rezervi) un *rescEU* ietvaros pieejamā aprīkojuma, materiālu un ekspertu izvietošanu attiecīgajā valstī. Palīdzība, ko var sniegt pēc lūguma, ietver, piemēram, degvielu, ģeneratorus, elektroenerģijas infrastruktūru, patvēruma spējas, ūdens attīrīšanas spējas un neatliekamās medicīniskās palīdzības spējas.

Priekšlikums atbilst arī ES *acquis*, kas attiecas uz energoapgādes drošību.

Kodolenerģētikas nozare nav konkrēti iekļauta ierosinātajā Padomes ieteikumā, izņemot, piemēram, saistīto infrastruktūru (kā pārvades līnijas uz kodolelektrostacijām), kas var ietekmēt piegādes drošību. Uz konkrētiem kodolelementiem attiecas atbilstošie tiesību akti kodolenerģijas jomā saskaņā ar *Euratom* līgumu un/vai valsts tiesību aktiem[6]. Ņemot vērā

[6] Padomes Direktīvas 2008/114/EK (EKI direktīva) 9. apsvērums.

Fukusimas avārijā gūto pieredzi, tika pastiprināti Eiropas kodoldrošības tiesību akti, un līdz ar to valstu iestādēm attiecībā uz katru iekārtu ir regulāri jāveic periodiskas drošības pārbaudes, lai nodrošinātu pastāvīgu atbilstību augstākajām drošības prasībām un apzinātu tālākus drošības uzlabojumus, kā arī jāveic seši gadskārtēji tematiski salīdzinoši novērtējumi ES līmenī.

ES Jūras drošības stratēģijā[7] un tās rīcības plānā[8] ir uzsvērta apdraudējumu mainīgā būtība jūrlietu jomā un pausts aicinājums no jauna apņemties aizsargāt kritisko jūras infrastruktūru, tostarp zem ūdens, un jo īpaši jūras transporta, enerģētikas un sakaru infrastruktūru, citstarp uzlabojot informētību par jūrlietām ar uzlabotas sadarbspējas un racionalizētas informācijas apmaiņas palīdzību.

Priekšlikums atbilst arī citiem attiecīgajiem nozaru tiesību aktiem. Tāpēc šā ieteikuma īstenošanai vajadzētu noritēt saskanīgi ar konkrētiem pasākumiem, kas reglamentē vai nākotnē var reglamentēt konkrētus noturības aspektus attiecībā uz vienībām, kuras darbojas attiecīgajās nozarēs, piemēram, transporta nozarē. Tas ietver citas attiecīgas iniciatīvas, piemēram, ārkārtas rīcības plānu transporta nozarei[9] vai ārkārtas rīcības plānu par pārtikas apgādi un nodrošinātību ar pārtiku krīzes laikā[10] un ar to saistīto Eiropas Pārtikas nodrošinājuma krīžgatavības un reaģēšanas mehānismu. Kopumā ieteikums, protams, būtu jāīsteno, pilnībā ievērojot visus piemērojamos ES tiesību aktu noteikumus, ieskaitot tos, kas paredzēti EKI un TID direktīvā.

Priekšlikums atbilst arī Stratēģiskajam kompasam drošībai un aizsardzībai, kurā uzsvērta nepieciešamība būtiski uzlabot noturību un spēju apkarot hibrīdapdraudējumus un kiberuzbrukumus, kā arī nepieciešamība stiprināt partnervalstu noturību un sadarboties ar NATO. Tas atbilst arī satvaram koordinētai ES reaģēšanai uz hibrīdapdraudējumu un hibrīdkampaņām, kas skar ES, dalībvalstis un partnerus[11].

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Priekšlikuma pamatā ir Līguma par Eiropas Savienības darbību (LESD) 114. pants, kas paredz tiesību aktu tuvināšanu iekšējā tirgus uzlabošanai, kā arī LESD 292. pants. To pamato fakts, ka ierosinātā Padomes ieteikuma galvenais mērķis ir veikt priekšdarbus pasākumiem, kas paredzēti jaunajā *CER* un TID2 direktīvā, kuras arī ir balstītas uz LESD 114. pantu. Saskaņā ar loģiku, ar ko pamato minētā panta izmantošanu par minēto direktīvu juridisko pamatu, ir vajadzīga ES rīcība, lai nodrošinātu netraucētu iekšējā tirgus darbību, jo īpaši ņemot vērā attiecīgo pakalpojumu pārrobežu raksturu un tvērumu un iespējamās sekas traucējumu gadījumā, kā arī pašreizējos un jaunos valstu pasākumus, kuru mērķis ir uzlabot to vienību noturību, kuras ekspluatē kritisko infrastruktūru, ko izmanto pamatpakalpojumu sniegšanai iekšējā tirgū.

• Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Eiropas līmeņa turpmākās darbības kritisko infrastruktūru ekspluatējošo vienību noturības jomā ir pamatotas, ņemot vērā kritiskās infrastruktūras darbību un sniegto pamatpakalpojumu

[7] 11205/14.
[8] 10494/18.
[9] COM(2022) 211.
[10] COM(2021) 689.
[11] Eiropas Savienības Padome 10016/22, 2022. gada 21. jūnijs.

saiknes savstarpēji atkarīgo pārrobežu raksturu un vajadzību pēc vienotākas un koordinētākas Eiropas pieejas, lai nodrošinātu, ka attiecīgās vienības pašreizējā ģeopolitiskajā kontekstā ir pietiekami noturīgas. Tā kā daudzas no kopīgajām problēmām, piemēram, *Nord Stream* gāzes cauruļvadu acīmredzamā sabotāža, pirmkārt un galvenokārt tiek risinātas ar valstu pasākumiem vai darbojoties vienībām, kas ekspluatē kritisko infrastruktūru, ir nepieciešams ES atbalsts, tostarp vajadzības gadījumā attiecīgo aģentūru atbalsts, lai stiprinātu noturību, uzlabotu modrību un stiprinātu ES kolektīvo reaģēšanu.

- **Proporcionalitāte**

Šis priekšlikums ir saskaņā ar proporcionalitātes principu, kas paredzēts Līguma par Eiropas Savienību 5. panta 4. punktā.

Ierosinātā Padomes ieteikuma saturs un forma nepārsniedz tā mērķu sasniegšanai nepieciešamo. Ierosinātās darbības ir proporcionālas izvirzītajiem mērķiem, jo tajās ir ievērotas dalībvalstu prerogatīvas un pienākumi saskaņā ar valsts tiesību aktiem.

Visbeidzot, priekšlikumā ir paredzēta iespējama diferencēta pieeja, kas atspoguļo dalībvalstu atšķirīgo iekšējo realitāti attiecībā uz sagatavotību un reaģēšanu uz fiziskiem kritiskās infrastruktūras apdraudējumiem.

- **Juridiskā instrumenta izvēle**

Lai sasniegtu iepriekš minētos mērķus, LESD, konkrēti, tā 292. pantā, ir paredzēts, ka Padome, pamatojoties uz Komisijas priekšlikumu, pieņem ieteikumus. Padomes ieteikums šajā gadījumā ir derīgs instruments, ņemot vērā arī pašreizējo tiesisko kontekstu, kas paskaidrots iepriekš. Padomes ieteikums, lai gan ir nesaistošs tiesību akts, norāda uz dalībvalstu apņemšanos īstenot tajā iekļautos pasākumus un nodrošina stingru politisko pamatu sadarbībai šajās jomās, vienlaikus pilnībā respektējot dalībvalstu pilnvaras.

3. *EX POST* IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- **Apspriešanās ar ieinteresētajām personām**

Izstrādājot šo priekšlikumu, tika ņemti vērā dalībvalstu ekspertu viedokļi, kas tika pausti 2022. gada 12. oktobra sanāksmē. Valdīja plaša vienprātība par to, ka būtu lietderīga plašāka koordinācija Savienības līmenī attiecībā uz sagatavotību un reaģēšanu pašreizējā apdraudējuma kontekstā, un par to, ka pirms *CER* direktīvas oficiālās pieņemšanas ir jāveic priekšdarbi saistībā ar dažiem tās elementiem. Dalībvalstis pauda gatavību dalīties pieredzē un paraugpraksē, kuras saistītas ar pasākumiem un metodiku kritisko infrastruktūru ekspluatējošo vienību noturības uzlabošanai. Dalībvalstis arī pauda atvērtību ieviest koordinētu pieeju kritisko infrastruktūru ekspluatējošo vienību stresa testiem, kas veicami brīvprātīgi un pamatojoties uz kopīgiem principiem. Dalībvalstis norādīja, ka šajā ieteikumā par prioritārām būtu jāuzskata vienības, kas ekspluatē kritisko infrastruktūru enerģētikas, digitālās infrastruktūras un transporta nozarē, respektīvi, tajās nozarēs, kas ir aktuālas vairākām dalībvalstīm. Dalībvalstis arī pauda gandarījumu par Komisijas nodomu tuvākajās nedēļās sasaukt turpmākas dalībvalstu ekspertu sanāksmes.

- **Detalizēts konkrētu priekšlikuma noteikumu skaidrojums**

Priekšlikums Padomes ieteikumam ir šāds.

– I nodaļā ir izklāstīts priekšlikuma mērķis, priekšmets un ieteikto pasākumu prioritātes.

– II nodaļā uzmanība tiek pievērsta pasākumiem, kas būtu jāveic, lai uzlabotu sagatavotību gan Savienības, gan dalībvalstu līmenī.

– III nodaļā ir runa par pastiprinātu reaģēšanu gan ES, gan dalībvalstu līmenī.

– IV nodaļa attiecas uz starptautisko sadarbību un darbībām, kas būtu jāveic, lai uzlabotu to vienību noturību, kuras ekspluatē kritisko infrastruktūru.

2022/0338 (NLE)

Priekšlikums

PADOMES IETEIKUMS

par koordinētu Savienības pieeju kritiskās infrastruktūras noturības stiprināšanai

(Dokuments attiecas uz EEZ)

EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

tā kā:

(1) Savienībai ir īpaša loma attiecībā uz tādu infrastruktūru, kas šķērso robežas un ietekmē vairāku dalībvalstu intereses, vai ko citādi izmanto vienības, kas sniedz pamatpakalpojumus pārrobežu kontekstā. Tomēr tāda vairākām dalībvalstīm būtiska vai pakalpojumu sniegšanā izmantota kritiskā infrastruktūra kā, piemēram, zemūdens kabeļi vai cauruļvadi, var atrasties tikai vienā dalībvalstī vai ārpus dalībvalsts teritorijas. Visu dalībvalstu un visas Savienības interesēs ir skaidri apzināt šo infrastruktūru un vienības, kā arī apdraudējumus, ar ko tās saskaras, un kolektīvi apņemties tās aizsargāt.

(2) Kritiskās infrastruktūras aizsardzību divās nozarēs pašlaik reglamentē Padomes Direktīva 2008/114/EK[12]. Ar minēto direktīvu izveido procedūru, kā apzināt un noteikt Eiropas kritisko infrastruktūru, un vienotu pieeju, kā izvērtēt vajadzību uzlabot šādas infrastruktūras aizsardzību, tādējādi veicinot cilvēku aizsardzību. Tā attiecas uz enerģētikas un transporta nozari. Lai uzlabotu kritisko vienību un to sniegto pamatpakalpojumu un infrastruktūras, uz kuru tās balstās, noturību, Savienības likumdevējs pašlaik pieņem jaunu direktīvu par kritisko vienību noturību[13] (“*CER* direktīva”), un tā aizstās Direktīvu 2008/114/EK, aptverot vairāk nozaru, tostarp digitālo infrastruktūru.

(3) Vēl arī Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā[14] koncentrējas uz kiberapdraudējumiem. Minētā direktīva tiks aizstāta ar jaunu direktīvu par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā[15] (“TID 2 direktīva”), kuru arī pašlaik pieņem Savienības likumdevējs.

---

12 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.).

13 COM(2020) 829.

14 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.).

15 COM(2020) 823.

(4) Ņemot vērā strauji mainīgo drošības apdraudējuma ainu, sevišķi saistībā ar *Nord Stream 1* un *Nord Stream 2* gāzes infrastruktūras acīmredzamo sabotāžu, vienības, kas ekspluatē kritisko infrastruktūru, saskaras ar īpašām problēmām saistībā ar noturību pret naidīgu rīcību un citiem cilvēka radītiem apdraudējumiem, turklāt dabas faktoru un klimata pārmaiņu radītās problēmas pieaug un var mijiedarboties ar naidīgu rīcību. Tāpēc tām ar dalībvalstu atbalstu ir jāveic atbilstoši noturības uzlabošanas pasākumi. Minētie pasākumi būtu jāveic un atbalsts būtu jāsniedz papildus pasākumiem, kas paredzēti Direktīvā 2008/114/EK un Direktīvā (ES) 2016/1148, un pat pirms jaunās *CER* un TID 2 direktīvas pieņemšanas, stāšanās spēkā un transponēšanas.

(5) Līdz tiek pieņemtas, stājas spēkā un tiek transponētas minētās jaunās direktīvas, Savienība un dalībvalstis tiek mudinātas izmantot visus pieejamos instrumentus saskaņā ar Savienības tiesību aktiem, lai virzītos uz priekšu un palīdzētu stiprināt attiecīgo vienību fizisko un kibernoturību un kritisko infrastruktūru, ko tās ekspluatē, lai sniegtu pamatpakalpojumus iekšējā tirgū, t. i., pakalpojumus, kas ir būtiski, lai saglabātu svarīgas sabiedriskas funkcijas, saimnieciskās darbības, sabiedrības veselību un drošību vai vidi. Šajā sakarā noturība būtu jāsaprot kā jēdziens, kas attiecas uz vienības spēju novērst notikumus, kuri var būtiski traucēt attiecīgo pamatpakalpojumu sniegšanu, aizsargāt pret šādiem notikumiem, reaģēt uz tiem, pretoties tiem, mazināt to ietekmi, izturēt tos, pielāgoties tiem un atgūties no tiem.

(6) Lai nodrošinātu pieeju, kas ir gan efektīva, gan pēc iespējas saskanīga ar jauno *CER* direktīvu, šajā ieteikumā ietvertajiem pasākumiem būtu jāattiecas uz infrastruktūru, ko dalībvalsts noteikusi par kritisko infrastruktūru, aptverot gan valsts kritisko infrastruktūru, gan Eiropas kritisko infrastruktūru neatkarīgi no tā, vai vienība, kas ekspluatē kritisko infrastruktūru, jau ir izraudzīta par kritisko vienību saskaņā ar minēto jauno direktīvu. Šajā ieteikumā termins "kritiskā infrastruktūra" būtu jāsaprot šādi.

(7) Ņemot vērā pastāvošos apdraudējumus, noturību veicinoši pasākumi pret cilvēka radītiem riskiem prioritārā kārtā būtu jāveic svarīgajās nozarēs, proti, enerģētikas, digitālās infrastruktūras, transporta un kosmosa nozarē, un šādiem pasākumiem vajadzētu būt vērstiem uz to vienību noturības uzlabošanu, kuras ekspluatē kritisko infrastruktūru. Attiecībā uz valstu kritisko infrastruktūru, ņemot vērā iespējamās sekas, ja riski materializēsies, prioritāte būtu jāpiešķir infrastruktūrai, kurai ir pārrobežu nozīme.

(8) Attiecīgi šajā ieteikumā noteikto pasākumu galvenais mērķis ir papildināt jauno *CER* un TID 2 direktīvu, kuru pamatā ir Līguma par Eiropas Savienības darbību (LESD) 114. pants, veicot priekšdarbus un papildinot pasākumus, ko nodrošinās minētās jaunās direktīvas. Tādēļ un ņemot vērā attiecīgo pamatpakalpojumu un kritiskās infrastruktūras pārrobežu raksturu un būtiskumu, kā arī pašreizējās un turpmākās valstu tiesību aktu atšķirības, kuras kropļo iekšējo tirgu, ir lietderīgi šo ieteikumu balstīt arī uz LESD 114. pantu kopā ar LESD 292. pantu.

(9) Šā ieteikuma īstenošana nebūtu jāsaprot kā tāda, kas ietekmē Savienības tiesību aktu pašreizējās un turpmākās prasības attiecībā uz konkrētiem attiecīgo vienību noturības aspektiem, un tai vajadzētu būt arī saskanīgai ar šiem aktiem. Šādas prasības ir noteiktas vispārīgos instrumentos, piemēram, Direktīvā 2008/114/EK un Direktīvā (ES) 2016/1148 un jaunajā *CER* un TID 2 direktīvā, ar kurām tās aizstāj, kā arī dažos nozaru instrumentos, piemēram, transporta jomā, kur Komisija citstarp ir uzņēmusies

iniciatīvu attiecībā uz ārkārtas rīcības plānu transporta jomā[16]. Saskaņā ar lojālas sadarbības principu šis ieteikums būtu jāīsteno ar pilnīgu savstarpēju cieņu un atbalstu.

(10) Komisija 2022. gada 5. oktobrī nāca klajā ar piecu punktu plānu, kurā nākotnes problēmu risināšanai izklāstīta koordinēta pieeja, kas ietver darbu pie sagatavotības, pamatojoties uz jaunās *CER* direktīvas pieņemšanu un stāšanos spēkā un veicot attiecīgus priekšdarbus, kā arī sadarbību ar dalībvalstīm ar mērķi, pamatojoties uz kopīgiem principiem, sākot ar enerģētikas nozari, veikt noturības testus vienībām, kuras ekspluatē kritisko infrastruktūru. Šajā ieteikumā, kas palīdzēs īstenot minēto plānu, atzinīgi novērtēta ierosinātā pieeja un izklāstīts, kā to var pārvērst rīcībā.

(11) Ņemot vērā strauji mainīgo drošības apdraudējuma ainu un pašreizējo riska vidi, ko raksturo cilvēka radīti riski, sevišķi attiecībā uz kritisko infrastruktūru ar pārrobežu nozīmi, ir būtiski iegūt precīzu, konkrētajai situācijai atbilstošu un pilnīgu priekšstatu par vissvarīgākajiem riskiem, ar kuriem saskaras vienības, kas ekspluatē kritisko infrastruktūru. Tāpēc dalībvalstīm būtu jāveic vajadzīgie pasākumi, lai sagatavotu vai atjauninātu minēto risku novērtējumus. Lai gan šis ieteikums ir koncentrēts uz riskiem, kas saistīti ar drošību, būtu jāturpina arī centieni pārvaldīt klimata pārmaiņu un vidiskos riskus, sevišķi, kad norises dabā var vēl vairāk saasināt cilvēka radītos riskus.

(12) Ņemot vērā šo drošības apdraudējumu ainu, dalībvalstis būtu jāaicina pēc iespējas drīz veikt atbilstošus pasākumus, lai uzlabotu kritiskās infrastruktūras noturību, arī papildus minētajiem riska novērtējumiem, kas vēlāk būs jāveic saskaņā ar jauno *CER* direktīvu.

(13) Īstenojot Komisijas izziņoto piecu punktu plānu, ir jākoordinē darbs, sapulcinot valstu ekspertus, kuri jāsaaicina kopā, gaidot Kritisko vienību noturības grupas izveidi ar jauno *CER* direktīvu, lai nodrošinātu sadarbību starp dalībvalstīm un informācijas apmaiņu par to vienību noturību, kuras ekspluatē kritisko infrastruktūru. Tam būtu jāietver sadarbība un informācijas apmaiņa par tādām darbībām kā kritisko vienību un infrastruktūras apzināšana, vienota principu kopuma izstrāde un popularizēšana stresa testu veikšanai un kopīga pieredzes gūšana no stresa testiem, kā arī ievainojamības un iespējamo spēju apzināšana. Šiem procesiem būtu arī jāveicina kritiskās infrastruktūras ekspluatētāju noturība pret klimata un vidiskajiem riskiem. Šis darbs arī ļautu kopīgi noteikt prioritātes darbam pie stresa testiem, īpašu uzmanību pievēršot enerģētikas, digitālās infrastruktūras un transporta nozarei. Komisija jau ir sākusi pulcēt šos ekspertus un sekmēt viņu darbu un plāno šo darbu turpināt. Tiklīdz jaunā *CER* direktīva būs stājusies spēkā un Kritisko vienību noturības grupa būs izveidota, minētajai grupai šādi priekšdarbi būtu jāturpina saskaņā ar saviem uzdevumiem, kas noteikti *CER* direktīvā.

(14) Stresa tests būtu jāpapildina ar kritiskās infrastruktūras incidentu un krīžu plāna izstrādi, kurā aprakstīts un izklāstīts, kādu mērķu labad un kādos veidos sadarbojas dalībvalstis un ES iestādes, struktūras, biroji un aģentūras, reaģējot uz incidentiem, kas vērsti pret kritisko infrastruktūru, sevišķi gadījumos, kad tie rada būtiskus traucējumus pamatpakalpojumu sniegšanai iekšējā tirgū. Šajā plānā būtu jāizmanto esošie integrētie krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismi reaģēšanas koordinēšanai, tam būtu jādarbojas saskaņā un savstarpēji papildinoši ar plānu par plaša mēroga kiberincidentiem, kā arī būtu jāparedz vienošanās par galvenajiem publiskās

[16] COM(2022) 211.

komunikācijas vēstījumiem, ņemot vērā, ka krīzes komunikācijai ir svarīga nozīme kritiskās infrastruktūras incidentu un krīžu negatīvās ietekmes mazināšanā.

(15) Lai nodrošinātu koordinētu un efektīvu reaģēšanu uz pašreizējiem un gaidāmajiem apdraudējumiem, Komisija sniegs papildu atbalstu dalībvalstīm ar mērķi uzlabot noturību, ņemot vērā minētos apdraudējumus, sevišķi nodrošinot attiecīgu informāciju informatīvu paziņojumu, rokasgrāmatu un pamatnostādņu veidā, veicinot Savienības finansētu pētniecības un inovācijas projektu ieviešanu, veicot nepieciešamos priekšdarbus un optimizējot Savienības uzraudzības līdzekļu izmantošanu. EĀDD būtu jānodrošina apdraudējumu novērtējumi, sevišķi ar ES Izlūkošanas un situāciju centra starpniecību.

(16) Ar attiecīgajām nozarēm saistītām Savienības aģentūrām un citām attiecīgām struktūrām arī būtu jāsniedz atbalsts ar noturību saistītos jautājumos, ciktāl atļauj to atbilstošās pilnvaras, kas noteiktas attiecīgajos Savienības tiesību aktos. Konkrēti, Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) varētu palīdzēt kiberdrošības jautājumos, Eiropas Jūras drošības aģentūras (*EMSA*) eksperti ar sava jūras uzraudzības dienesta starpniecību varētu atbalstīt dalībvalstis jautājumos, kas saistīti ar jūras drošību un drošumu, Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai (Eiropols) varētu sniegt atbalstu saistībā ar informācijas vākšanu un izmeklēšanu pārrobežu tiesībaizsardzības darbībās, savukārt Eiropas Savienības Kosmosa programmas aģentūra (*EUSPA*) un ES Satelītcentrs (*Satcen*) varētu palīdzēt, veicot darbības Savienības kosmosa programmas ietvaros.

(17) Lai gan galvenā atbildība par kritiskās infrastruktūras un attiecīgo vienību drošības nodrošināšanu gulstas uz dalībvalstīm, ir lietderīga pastiprināta koordinācija Savienības līmenī, jo īpaši ņemot vērā apdraudējumus, kas vienlaikus var ietekmēt vairākas dalībvalstis, piemēram, Krievijas agresijas karu pret Ukrainu, vai ietekmēt Savienības ekonomikas, vienotā tirgus un sabiedrības noturību un sekmīgu darbību.

(18) Šis ieteikums nerosina tādas informācijas sniegšanu, kuras izpaušana ir pretrunā būtiskām valsts drošības, sabiedrības drošības vai aizsardzības interesēm dalībvalstīs.

(19) Palielinoties fiziskās un digitālās infrastruktūras savstarpējai atkarībai, ļaunprātīgas kiberdarbības, kas vērstas pret kritiskām jomām, var radīt traucējumus vai kaitējumu fiziskajai infrastruktūrai, savukārt fiziskās infrastruktūras sabotāža var padarīt nepieejamus digitālos pakalpojumus. Ņemot vērā pieaugošo apdraudējumu, ko rada sarežģīti hibrīduzbrukumi, dalībvalstīm šādi apsvērumi arī būtu jāiekļauj savā darbā, ko tās veic, īstenojot šo ieteikumu. Ņemot vērā savstarpējo saikni starp kiberdrošību un operatoru fizisko drošību, ir svarīgi, lai darbs pie jaunās TID 2 direktīvas transponēšanas un piemērošanas sagatavošanas tiktu sākts pēc iespējas drīz un lai paralēli noritētu šāds darbs arī saskaņā ar jauno *CER* direktīvu.

(20) Papildus sagatavotības uzlabošanai ir svarīgi arī uzlabot spējas ātri un efektīvi reaģēt gadījumā, ja īstenojas risks, kas ietekmē to pamatpakalpojumu sniegšanu, kurus nodrošina vienības, kas ekspluatē kritisko infrastruktūru. Tāpēc šajā ieteikumā būtu jāietver pasākumi, kas jāveic gan dalībvalstu, gan Savienības līmenī, tostarp pastiprināta sadarbība un informācijas apmaiņa saistībā ar Savienības civilās aizsardzības mehānismu un attiecīgo Savienības kosmosa programmas aktīvu izmantošana.

(21) Pēc Padomes aicinājuma, ko tā paudusi secinājumos par ES pozīciju kiberjautājumos[17], Komisija, Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos ("Augstais pārstāvis") un ar Direktīvu (ES) 2016/1148 izveidotā sadarbības grupa ("TID sadarbības grupa") koordinācijā ar attiecīgām civilām un militārām struktūrām un aģentūrām un esošajiem tīkliem, tostarp *EU CyCLONe*, veic riska izvērtēšanu un veido riska scenārijus no kiberdrošības viedokļa situācijai, kad pastāv apdraudējums vai iespējams uzbrukums dalībvalstīm vai partnervalstīm. Šis pasākums ir koncentrēts uz kritiskajām nozarēm, t. sk. enerģētiku, digitālo infrastruktūru, transportu un kosmosu.

(22) Nevēras ministru kopīgajā aicinājumā[18] un Padomes secinājumos par ES pozīciju kiberjautājumos arī tika aicināts stiprināt komunikācijas infrastruktūras un tīklu noturību Savienībā, sniedzot dalībvalstīm un Komisijai ieteikumus, kuru pamatā ir riska novērtējums. Šo riska novērtējumu pašlaik veic TID sadarbības grupa ar Komisijas un *ENISA* atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*). Riska novērtējumā un nepilnību analīzē aplūkoti kiberuzbrukumu riski dažādām sakaru infrastruktūras apakšnozarēm, tostarp fiksēto un mobilo sakaru infrastruktūrai, satelītiem, zemūdens kabeļiem, interneta maršrutētājiem u. c., tādējādi nodrošinot pamatu darbam saskaņā ar šo ieteikumu. Šis riska novērtējums tiks izmantots pašlaik notiekošajā starpnozaru kiberrisku izvērtēšanā un Padomes 2022. gada 23. maija secinājumos pieprasītajos scenārijos.

(23) Abi pasākumi noritēs saskanīgi un koordinēti ar scenāriju izstrādi, kas koncentrējas uz civilo aizsardzību saistībā ar plašu dabas un cilvēka izraisītu katastrofu klāstu, tostarp kiberdrošības incidentiem un to ietekmi uz reālo dzīvi, un ko Komisija un dalībvalstis pašlaik izstrādā saskaņā ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES[19]. Efektivitātes, racionalitātes un konsekvences labad šis ieteikums būtu jāīsteno, ņemot vērā minēto pasākumu rezultātus.

(24) ES 5G kiberdrošības rīkkopā[20] ir izklāstīti attiecīgi pasākumi un ietekmes mazināšanas plāni 5G tīklu drošības stiprināšanai. Ņemot vērā daudzu pamatpakalpojumu atkarību no 5G tīkliem un digitālo ekosistēmu savstarpējo saistību, ir būtiski, lai visas dalībvalstis steidzami īstenotu rīkkopā ieteiktos pasākumus, un jo īpaši piemērotu attiecīgos ierobežojumus augsta riska piegādātājiem attiecībā uz svarīgākajiem aktīviem, kas ES koordinētajā riska novērtējumā atzīti par kritiskiem un sensitīviem.

(25) Lai nekavējoties stiprinātu sagatavotību un spējas reaģēt uz smagiem kiberincidentiem, Komisija ir izveidojusi īstermiņa atbalsta programmu dalībvalstīm, piešķirot papildu finansējumu aģentūrai *ENISA*. Aptvertie pakalpojumi ietvers sagatavotības darbības, piemēram, kritisko vienību ielaušanās testēšanu, lai identificētu ievainojamību. Tā arī stiprinās iespējas palīdzēt dalībvalstīm tādu nopietnu incidentu gadījumā, kas skar kritiskās vienības. Tas ir pirmais solis, kas sperts saskaņā ar Padomes secinājumiem par pozīciju kiberjautājumos, kuros Komisija tiek aicināta nākt klajā ar priekšlikumu par Ārkārtas kiberfondu. Dalībvalstīm būtu pilnībā jāizmanto minētās iespējas saskaņā ar piemērojamajām prasībām.

---

17 *Cyber posture: Council approves conclusions - Consilium* (europa.eu)

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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.).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(26) Globālais datu un elektronisko sakaru zemūdens kabeļu tīkls ir izšķiroši svarīgs globālajai un ES iekšējai savienojamībai. Ņemot vērā šo kabeļu lielo garumu un to novietojumu uz jūras gultnes, zemūdens vizuālā uzraudzība lielākajā daļā kabeļu posmu ir ārkārtīgi sarežģīta. Dalītā jurisdikcija un citi jurisdikcijas jautājumi, kas saistīti ar šiem kabeļiem, ir Eiropas un starptautiskās sadarbības infrastruktūras aizsardzības un atjaunošanas jomā īpašs gadījums. 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 kabeļiem. Tāpēc Komisija šajā nolūkā veiks pētījumus un savus konstatējumus darīs zināmus dalībvalstīm.

(27) Šajā ieteikumā noteiktās prioritārās nozares – enerģētiku un transportu – var ietekmēt arī riski, kas saistīti ar digitālo infrastruktūru. Šāda ietekme var pastāvēt, piemēram, attiecībā uz energotehnoloģijām, kas ietver digitālos komponentus. Saistīto piegādes ķēžu drošība ir svarīga pamatpakalpojumu sniegšanas nepārtrauktībai un enerģētikas nozares vienību ekspluatētās kritiskās infrastruktūras stratēģiskajai kontrolei. Minētie apstākļi būtu jāņem vērā, veicot pasākumus saskaņā ar šo ieteikumu to vienību noturības uzlabošanai, kuras ekspluatē kritisko infrastruktūru.

(28) Ņemot vērā kosmosa infrastruktūras un ar kosmosu saistīto pakalpojumu pieaugošo nozīmi ar drošību saistītās darbībās, ir būtiski nodrošināt Savienības kosmosa resursu un pakalpojumu noturību un aizsardzību gan ES, gan šā ieteikuma ietvaros, lai strukturētāk izmantotu kosmosā balstītus datus un pakalpojumus, ko sniedz kosmosa sistēmas un programmas kritiskās infrastruktūras novērošanai un aizsardzībai citās nozarēs. Gaidāmajā ES kosmosa stratēģijā drošībai un aizsardzībai šajā sakarā tiks ierosinātas attiecīgas darbības, kas būtu jāņem vērā, īstenojot šo ieteikumu.

(29) Ir vajadzīga arī sadarbība starptautiskā līmenī, lai efektīvi pārvaldītu riskus to vienību noturībai, kuras ekspluatē kritisko infrastruktūru Savienībā, attiecīgajās trešās valstīs vai starptautiskajos ūdeņos. Tāpēc dalībvalstis būtu jāaicina sadarboties ar Komisiju un Augsto pārstāvi, lai veiktu konkrētus pasākumus šā mērķa sasniegšanai, saprotot, 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.

(30) Kā noteikts paziņojumā "Komisijas ieguldījums Eiropas aizsardzībā"[21], atbalstot "Stratēģisko drošības un aizsardzības kompasu — Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību"[22], Komisija sadarbībā ar Augsto pārstāvi un dalībvalstīm izvērtēs nozaru noturības pret hibrīddraudiem pamatlīmeņus, apzinot trūkumus un vajadzības, kā arī pasākumus to risināšanai līdz 2023. gadam. Šai iniciatīvai būtu jānodrošina informācija darbam, kas tiek veikts saskaņā ar šo ieteikumu, palīdzot stiprināt informācijas apmaiņu un rīcības koordināciju, lai vēl vairāk stiprinātu noturību, tostarp kritiskās infrastruktūras noturību.

(31) ES 2014. gada Jūras drošības stratēģijā un tās rīcības plānā ir pausts aicinājums apņēmīgāk aizsargāt kritisko jūras infrastruktūru, tostarp zem ūdens, 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. Stratēģija un rīcības plāns pašlaik tiek atjaunināti un ietvers

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu).

22 Eiropas Savienības Padome, 7371/22, 2022. gada 21. marts.

pastiprinātas darbības, kuru mērķis ir aizsargāt kritisko jūras infrastruktūru. Šīm darbībām būtu jānodrošina informācija šim ieteikumam un tas jāpapildina.

(32) Dalībvalstīm būtu pilnībā jāņem vērā Savienības drošības pētniecības programmas potenciāls, sevišķi pievēršoties tās īpašajai prioritātei kritiskās infrastruktūras jomā, jo īpaši izmantojot Iekšējās drošības fonda finansētās programmas, kā arī citas potenciālās finansēšanas iespējas Savienības līmenī, proti, Eiropas Reģionālās attīstības fondu, ciktāl konkrētie pasākumi atbilst tā atbilstības prasībām. Noturības finansēšanas iespējas var piedāvāt arī *REPowerEU*. Ikvienai šādai Savienības finansējuma piedāvāto iespēju izmantošanai jānotiek saskaņā ar piemērojamajām tiesību aktu prasībām,

IR PIEŅĒMUSI ŠO IETEIKUMU.

I NODAĻA. MĒRĶIS, DARBĪBAS JOMA UN PRIORITĀTES

(1) Ar šo ieteikumu dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un lojāli, efektīvi, solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgajām publiskajām iestādēm, kā arī attiecīgajām vienībām, lai uzlabotu to vienību noturību, kuras Savienībā ekspluatē kritisko infrastruktūru, lai sniegtu pamatpakalpojumus iekšējā tirgū.

(2) Šajā ieteikumā izklāstītie pasākumi attiecas uz infrastruktūru, ko kāda dalībvalsts noteikusi par kritisko infrastruktūru, tostarp par Eiropas kritisko infrastruktūru.

(3) Īstenojot šo ieteikumu, prioritāte būtu jāpiešķir to vienību noturības uzlabošanai pret cilvēka radītiem riskiem, kuras darbojas enerģētikas, digitālās infrastruktūras, transporta un kosmosa nozarē, un tās kritiskās infrastruktūras noturības uzlabošanai, ko šīs vienības ekspluatē un kam ir pārrobežu nozīme.

II NODAĻA. UZLABOTA SAGATAVOTĪBA

Darbības dalībvalstu līmenī

(4) Dalībvalstis tiek aicinātas veikt vai atjaunināt riska novērtējumus par to vienību noturību, kuras ekspluatē Eiropas kritisko infrastruktūru, kas saskaņā ar Direktīvu 2008/114/EK noteikta transporta un enerģētikas nozarē, un attiecīgā gadījumā un saskaņā ar minēto direktīvu savstarpēji sadarboties attiecībā uz šādiem riska novērtējumiem un no tiem izrietošajiem noturības uzlabošanas pasākumiem.

(5) Turklāt, lai panāktu to vienību augstu noturības līmeni, kuras ekspluatē kritisko infrastruktūru, dalībvalstīm būtu jāpaātrina sagatavošanas darbs, lai pēc iespējas drīz transponētu un piemērotu jauno *CER* direktīvu, veicot šādas darbības:

(a) paātrināt tādu valsts stratēģiju pieņemšanu vai atjaunināšanu, kuru mērķis ir uzlabot to vienību noturību, kuras ekspluatē kritisko infrastruktūru, lai reaģētu uz pašreizējo apdraudējumu. Šīs stratēģijas attiecīgās daļas būtu jāpaziņo Komisijai;

(b) veikt vai atjaunināt riska novērtējumus atbilstoši pašreizējo apdraudējumu mainīgajam raksturam attiecībā uz to vienību noturību, kuras ekspluatē kritisko infrastruktūru atbilstošajās nozarēs, kas nav enerģētika, digitālā infrastruktūra un transports, un iespēju robežās – nozarēs, uz kurām attiecas jaunā *CER* direktīva, proti, banku, finanšu tirgus infrastruktūras, digitālās infrastruktūras, veselības, dzeramā ūdens, notekūdeņu, publiskās pārvaldes, kosmosa un pārtikas ražošanas, pārstrādes un izplatīšanas nozarē, ņemot vērā attiecīgo apdraudējumu iespējamo hibrīdo raksturu, t. sk. kaskādes efektu un klimata pārmaiņu ietekmi;

(c) informēt Komisiju par apzināto risku veidiem pa nozarēm un apakšnozarēm un riska novērtējumu rezultātiem, ko var veikt, izmantojot vienotu ziņošanas paraugu, kuru Komisija izstrādājusi sadarbībā ar dalībvalstīm;

(d) paātrināt kritisko vienību apzināšanas un noteikšanas procesu, prioritāti piešķirot kritiskajām vienībām, kas:

(a) izmanto kritisko infrastruktūru, kura ir fiziski savienota starp vismaz divām dalībvalstīm;

(b) pieder pie korporatīvajām struktūrām, kas ir savienotas ar kritiskajām vienībām citās dalībvalstīs vai ir ar tām saistītas;

(c) ir identificētas kā tādas vienā dalībvalstī un sniedz pamatpakalpojumus vismaz sešās dalībvalstīs vai vismaz sešām dalībvalstīm un tāpēc ir īpaši nozīmīgas Eiropai, un attiecīgi informē Komisiju;

(d) savstarpēji sadarboties, īpaši attiecībā uz kritiskajām vienībām un pamatpakalpojumiem un kritisko infrastruktūru, kam ir pārrobežu nozīme, proti, iesaistīties savstarpējās konsultācijās 5. punkta d) apakšpunkta nolūkā un informēt citai citu tāda incidenta gadījumā, kam ir būtiska vai potenciāli būtiska traucējoša pārrobežu ietekme, vienlaikus attiecīgi informējot Komisiju;

(e) palielināt atbalstu izraudzītajām kritiskajām vienībām, lai uzlabotu to noturību, kas var ietvert norādījumu un metodikas nodrošināšanu, praktisku pasākumu organizēšanu to noturības pārbaudei, konsultāciju sniegšanu un šo vienību darbinieku apmācību, kā arī iespēju veikt drošības pārbaudes personām ar sensitīviem pienākumiem saskaņā ar Savienības un valstu tiesību aktiem kā daļu no darbinieku drošības pārvaldības pasākumiem, ko veic kritiskās vienības;

(f) paātrināt vienota kontaktpunkta izraudzīšanos vai izveidi kompetentajā iestādē, lai pildītu koordinācijas funkciju nolūkā nodrošināt pārrobežu sadarbību ar citu dalībvalstu vienotajiem kontaktpunktiem saistībā ar to vienību noturību, kuras ekspluatē kritisko infrastruktūru.

(6) Dalībvalstis tiek mudinātas veikt stresa testus vienībām, kas ekspluatē kritisko infrastruktūru. Dalībvalstis sevišķi tiek aicinātas uzlabot savu un attiecīgo vienību sagatavotību enerģētikas nozarē un veikt noturības testus šajā nozarē, ja iespējams, ievērojot principus, par kuriem kopīgi panākta vienošanās Savienības līmenī, vienlaikus nodrošinot efektīvu saziņu ar attiecīgajām vienībām. Noturības testus citās prioritārās nozarēs, proti, digitālās infrastruktūras, transporta un kosmosa nozarē, vajadzības gadījumā varētu apsvērt pēc tam, veltot pienācīgu uzmanību pārbaudēm gaisa un jūras apakšnozarē saskaņā ar Savienības tiesību aktiem un ņemot vērā atbilstošos noteikumus nozaru tiesību aktos.

(7) Dalībvalstis tiek aicinātas attiecīgos gadījumos un saskaņā ar Savienības tiesību aktiem sadarboties ar atbilstošajām trešām valstīm attiecībā uz to vienību noturību, kuras ekspluatē pārrobežu nozīmes kritisko infrastruktūru.

(8) Dalībvalstis tiek aicinātas saskaņā ar piemērojamajām prasībām izmantot potenciālās finansēšanas iespējas Savienības un valsts līmenī, lai uzlabotu to vienību noturību, kuras Savienībā ekspluatē kritisko infrastruktūru, tostarp, piemēram, Eiropas sakaru tīklos, pret būtisku apdraudējumu pilnu spektru, jo īpaši to programmu ietvaros, ko finansē no Iekšējās drošības fonda un Eiropas Reģionālās attīstības fonda, ja ir izpildīti attiecīgie atbilstības kritēriji, un no Eiropas infrastruktūras savienošanas instrumenta, tostarp pēc noteikumiem par klimatdrošināšanu. Šim nolūkam var

izmantot arī Savienības civilās aizsardzības mehānisma finansējumu saskaņā ar piemērojamajām prasībām, jo īpaši projektiem, kas saistīti ar riska novērtējumiem, investīciju plāniem vai pētījumiem, spēju veidošanu vai zināšanu bāzes uzlabošanu. Noturības finansēšanas iespējas var piedāvāt arī *REPowerEU*.

(9) Attiecībā uz sakaru un tīklu infrastruktūru Savienībā TID sadarbības grupai, rīkojoties saskaņā ar Direktīvas (ES) 2016/1148 11. pantu un pēc tam TID 2 direktīvas 14. pantu, būtu jāpaātrina darbs pie mērķorientēta riska novērtējuma un pirmie ieteikumi būtu jāiesniedz 2023. gada sākumā. 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, piemēram, Kritisko vienību noturības grupa, kas jāizveido saskaņā ar jauno *CER* direktīvu, un grupa, kas jāizveido saskaņā ar jauno Digitālās darbības noturības aktu (*DORA*)[23].

(10) TID sadarbības grupa, kurai jāveic savi uzdevumi saskaņā ar Direktīvas (ES) 2016/1148 11. pantu un pēc tam TID 2 direktīvas 14. pantu, tiek aicināta ar Komisijas un *ENISA* atbalstu piešķirt prioritāti darbam pie digitālās infrastruktūras un kosmosa nozares drošības, tostarp sagatavojot norādījumus par politiku un kiberdrošības riska pārvaldības metodiku un pasākumus, kuru pamatā ir visu apdraudējumu pieeja attiecībā uz zemūdens sakaru kabeļiem, gaidot TID 2 direktīvas stāšanos spēkā, kā arī izstrādājot norādījumus par kiberdrošības riska pārvaldības pasākumiem kosmosa nozares operatoriem, kuru mērķis ir 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*, proti, 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 steidzami jāīsteno pasākumi, kas ieteikti ES 5G kiberdrošības rīkkopā[24]. Dalībvalstīm, kuras vēl nav ieviesušas ierobežojumus augsta riska piegādātājiem, tas būtu jādara bez turpmākas kavēšanās, ņemot vērā, ka zaudētais laiks var palielināt tīklu ievainojamību Savienībā. Tām būtu arī jāstiprina kritiskās un sensitīvās 5G tīklu daļas fiziskā un nefiziskā aizsardzība, tostarp veicot stingru piekļuves kontroli. Turklāt dalībvalstīm sadarbībā ar Komisiju būtu jānovērtē, vai ir vajadzīga papildu rīcība, tostarp juridiski saistošas prasības Savienības līmenī, lai nodrošinātu 5G tīklu konsekventu drošības un noturības līmeni.

(13) Dalībvalstīm pēc iespējas drīz būtu jāīsteno gaidāmais tīkla kodekss attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem, pamatojoties uz pieredzi, kas gūta TID direktīvas īstenošanā, un attiecīgajiem norādījumiem, ko sagatavojusi TID sadarbības grupa, jo īpaši tās atsauces dokumentu par drošības pasākumiem pamatpakalpojumu sniedzējiem.

(14) Dalībvalstīm būtu jāattīsta *Galileo* un/vai *Copernicus* izmantošana uzraudzībai un jāapmainās ar attiecīgo informāciju starp ekspertiem, kas sasaukti saskaņā ar 15. punktu. Būtu pienācīgi jāizmanto Savienības kosmosa programmas Savienības

---

23 COM(2020) 595 final.

24 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

valdības satelītsakaru (*GOVSATCOM*) sniegtās iespējas, lai uzraudzītu kritisko infrastruktūru un atbalstītu reaģēšanu krīzes situācijās.

Darbības Savienības līmenī

(15) Komisija plāno stiprināt sadarbību starp dalībvalstu ekspertiem, lai palīdzētu uzlabot kritisko infrastruktūru ekspluatējošo vienību fizisko noturību, kas nav kibernoturība, veicot šādas darbības:

(a) sagatavot kopīgu instrumentu izstrādi un popularizēšanu, lai atbalstītu dalībvalstis šādas noturības uzlabošanā, tostarp metodiku un riska scenārijus;

(b) atbalstīt to, ka dalībvalstis izstrādā kopīgus principus 6. punktā minēto noturības testu veikšanai, sākot ar testiem, kas vērsti uz cilvēka radītiem riskiem enerģētikas nozarē un pēc tam – citās svarīgās nozarēs, piemēram, digitālajā infrastruktūrā un transportā; pārvaldīt citus būtiskus riskus un bīstamības; kā arī attiecīgā gadījumā atbalstīt un konsultēt par šādu stresa testu veikšanu;

(c) izveidot drošu platformu, kur vākt, izvērtēt un apmainīties ar paraugpraksi, mācībām, kas gūtas no valstu pieredzes, un citu informāciju, kas saistīta ar šādu noturību, tostarp par minēto stresa testu veikšanu un to rezultātu iestrādāšanu protokolos un ārkārtas rīcības plānos.

Minēto ekspertu darbā īpaša uzmanība būtu jāpievērš starpnozaru atkarībai un vienībām, kas ekspluatē kritisko infrastruktūru ar pārrobežu nozīmi, un tas būtu jāturpina Kritisko vienību noturības grupai, tiklīdz tā būs izveidota.

(16) Dalībvalstīm būtu pilnībā jāpiedalās 15. punktā minētajā pastiprinātajā sadarbībā, tostarp nozīmējot kontaktpunktus ar attiecīgām speciālajām zināšanām un apmainoties ar pieredzi par metodēm, ko izmanto noturības testos un protokolos, un ārkārtas situāciju plānos, kas izstrādāti, pamatojoties uz tiem. Informācijas apmaiņā būtu jāievēro minētās informācijas konfidencialitāte un jāaizsargā kritisko vienību drošība un komerciālās intereses, vienlaikus saglabājot dalībvalstu drošību. Tas nenozīmē tādas informācijas sniegšanu, kuras izpaušana ir pretrunā būtiskām valsts drošības, sabiedrības drošības vai aizsardzības interesēm dalībvalstīs.

(17) Komisija atbalstīs dalībvalstis, nodrošinot rokasgrāmatas un pamatnostādnes, piemēram, izstrādājot 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 savas Hibrīddraudu analīzes vienības starpniecību, tiek aicināts sniegt informatīvus paziņojumus par kritiskās infrastruktūras apdraudējumu Eiropas Savienībā, lai uzlabotu situācijas apzināšanos.

(18) Komisija atbalstīs to projektu rezultātu pārņemšanu, kuri saistīti ar to vienību noturību, kas ekspluatē kritisko infrastruktūru, un kurus finansē saskaņā ar Savienības pētniecības un inovācijas programmām. Komisija gatavojas palielināt finansējumu šādai noturībai budžetā, kas daudzgadu finanšu shēmā 2021.–2027. gadam piešķirts pamatprogrammai "Apvārsnis Eiropa". Tam būtu jāļauj risināt pašreizējās un turpmākās problēmas šajā jomā, piemēram, kritiskās infrastruktūras klimatdrošināšanu Savienībā, nesamazinot finansējumu, kas paredzēts citiem ar civilo drošību saistītiem pētniecības un inovācijas virzieniem pamatprogrammas "Apvārsnis Eiropa" ietvaros. Komisija arī pastiprinās centienus izplatīt attiecīgo Savienības finansēto pētniecības projektu rezultātus.

(19) TID sadarbības grupa sadarbībā ar Komisiju un Augsto pārstāvi tiek aicināta saskaņā ar to attiecīgajiem uzdevumiem un pienākumiem, kas noteikti Savienības tiesību

aktos, pastiprināt darbu ar attiecīgajiem tīkliem un civilajām un militārajām struktūrām riska novērtēšanā un kiberdrošības riska scenāriju izstrādē, sākotnēji koncentrējoties uz enerģētikas, sakaru, transporta un kosmosa infrastruktūru un nozaru un dalībvalstu savstarpējo atkarību. Veicot šo novērtēšanu, būtu jāņem vērā saistītie riski fiziskajai infrastruktūrai, uz kuriem balstās šīs nozares. Riska novērtējumi un scenāriji būtu jāsagatavo regulāri, un tiem būtu jāpapildina esošie vai plānotie riska novērtējumi šajās 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.

(20) Komisija paātrinās savas darbības, lai atbalstītu dalībvalstu sagatavotību un reaģēšanu uz liela mēroga kiberdrošības incidentiem, proti:

(a) papildus attiecīgajiem riska novērtējumiem tīklu un informācijas drošības kontekstā veiks visaptverošu pētījumu, kurā novērtēta zemūdens kabeļu infrastruktūra, kas savieno dalībvalstis un savieno Eiropu visā pasaulē, t. sk. veiks kartēšanu, noteiks tās spējas un rezerves, ievainojamību, pakalpojumu pieejamības riskus un riska mazināšanu. Konstatējumi būtu jādara zināmi dalībvalstīm;

(b) atbalstīs dalībvalstu un ES iestāžu, struktūru un aģentūru (*EUIBA*) sagatavotību reaģēt uz liela mēroga kiberdrošības incidentiem.

(21) Komisija pastiprinās tālredzīgus priekšdarbus, tostarp ES civilās aizsardzības mehānisma ietvaros, sadarbībā ar dalībvalstīm saskaņā ar Lēmuma 1313/2013/ES 6. un 10. pantu un ārkārtas situāciju plānošanas veidā, lai atbalstītu Ārkārtas reaģēšanas koordinēšanas centra operatīvo sagatavotību.

Komisija uzņemsies šādas konkrētas saistības:

(a) turpināt darbu Ārkārtas reaģēšanas koordinēšanas centrā saistībā ar priekšdarbiem un starpnozaru novēršanas, sagatavotības un reaģēšanas plānošanu, lai paredzētu un sagatavotos pamatpakalpojumu sniegšanas traucējumiem, kas skar vienības, kuras ekspluatē kritisko infrastruktūru;

(b) palielināt investīcijas profilaktiskā pieejā un iedzīvotāju sagatavotībā šādu traucējumu gadījumā, īpašu uzmanību pievēršot ķīmiskiem, bioloģiskiem, radioloģiskiem, kodola un sprāgstvielu aģentiem vai citiem jauniem cilvēka izraisītiem apdraudējumiem;

(c) pastiprināt attiecīgo zināšanu un paraugprakses apmaiņu un uzlabot struktūru un vadību spēju veidošanas pasākumiem, piemēram, apmācības kursiem un mācībām ar vienībām, kas ekspluatē kritisko infrastruktūru, izmantojot esošās struktūras un speciālās zināšanas, piemēram, Savienības Civilās aizsardzības zināšanu tīklu.

(22) Komisija veicinās ES uzraudzības līdzekļu (*Copernicus* un *Galileo*) izmantošanu tam, lai atbalstītu dalībvalstis kritiskās infrastruktūras un attiecīgā gadījumā to tuvākās apkārtnes uzraudzībā un atbalstītu citas uzraudzības iespējas, kas paredzētas Savienības kosmosa programmā.

(23) Attiecīgā gadījumā un saskaņā ar savām attiecīgajām pilnvarām Savienības aģentūras un citas attiecīgās struktūras tiek aicinātas sniegt atbalstu jautājumos, kas saistīti ar kritisko infrastruktūru ekspluatējošo vienību noturību, piemēram:

(a) Eiropols par informācijas vākšanu, kriminālizmeklēšanas datu analīzi un izmeklēšanas atbalstu pārrobežu tiesībaizsardzības darbībās;

(b) *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) *EUSPA* attiecībā uz Savienības kosmosa programmas darbībām;

(d) *ENISA* attiecībā uz darbībām, kas saistītas ar kiberdrošību.

III NODAĻA. PASTIPRINĀTA REAĢĒŠANA

Darbības dalībvalstu līmenī

(24) Dalībvalstīm būtu jāveic šādas darbības:

(a) koordinēt savu reaģēšanu un uzturēt pārskatu par starpnozaru reaģēšanu uz būtiskiem traucējumiem pamatpakalpojumu sniegšanā, ko veic vienības, kuras ekspluatē kritisko infrastruktūru, Padomes krīzes mehānisma (*IPCR*) ietvaros attiecībā uz kritisko infrastruktūru ar pārrobežu nozīmi, Plāna par liela mēroga kiberdrošības incidentiem un krīzēm ietvaros vai Satvara koordinētai ES reaģēšanai uz hibrīdkampaņām ietvaros hibrīdkampaņas gadījumā;

(b) palielināt informācijas apmaiņu Savienības civilās aizsardzības mehānisma ietvaros, lai uzlabotu agrīno brīdināšanu un koordinētu to, kā tās reaģē šā mehānisma ietvaros šādu būtisku traucējumu gadījumā, tādējādi vajadzības gadījumā nodrošinot ātrāku Savienības atbalstītu reaģēšanu;

(c) palielināt savu gatavību reaģēt uz šādiem būtiskiem traucējumiem, izmantojot Savienības civilās aizsardzības mehānismu, jo īpaši, ja tiem varētu būt būtiska pārrobežu vai pat Eiropas mēroga, kā arī starpnozaru ietekme;

(d) sadarboties ar Komisiju, lai turpinātu attīstīt attiecīgās reaģēšanas spējas Eiropas civilās aizsardzības rezervē (*ECPP*) un *rescEU*;

(e) aicināt vienības, kas ekspluatē kritisko infrastruktūru, un attiecīgās valsts iestādes uzlabot minēto vienību spēju ātri atjaunot pamatpakalpojumu sniegšanu elementārā līmenī;

(f) nodrošināt, ka tad, kad kritisko infrastruktūru ir nepieciešams atjaunot, šāda atjaunota infrastruktūra būs noturīga pret visiem būtiskajiem riskiem, kas uz to var attiekties, tostarp nelabvēlīgu klimata scenāriju gadījumā.

(25) Dalībvalstis tiek aicinātas paātrināt sagatavošanās darbu TID 2 direktīvas transponēšanai un piemērošanai, nekavējoties sākot uzlabot valstu datordrošības incidentu reaģēšanas vienību (*CSIRT*) spējas, ņemot vērā *CSIRT* jaunos uzdevumus, kā arī vienību pieaugušo skaitu no jaunām nozarēm, ātri atjauninot savas kiberdrošības stratēģijas un pēc iespējas drīz pieņemot valstu plānus reaģēšanai uz kiberdrošības incidentiem un krīzēm.

Darbības Savienības līmenī

(26) Reaģēšana uz būtiskiem traucējumiem pamatpakalpojumu sniegšanā, ko veic vienības, kuras ekspluatē kritisko infrastruktūru, būtu jākoordinē starp dalībvalstu ekspertiem attiecībā uz minēto vienību noturību un reaģēšanu uz šādiem traucējumiem – tas var veicināt Padomes krīzes mehānisma (*IPCR*) darbību.

(27) Komisija cieši sadarbosies ar dalībvalstīm, lai turpinātu attīstīt izvietojamas ārkārtas reaģēšanas spējas, tostarp ekspertus un *rescEU* krājumus *UCPM* ietvaros, lai uzlabotu operatīvo sagatavotību nolūkā pārvaldīt tūlītējās un netiešās sekas, ko rada

būtiski traucējumi pamatpakalpojumu sniegšanā, ko veic vienības, kuras ekspluatē kritisko infrastruktūru.

(28) Ņemot vērā mainīgo riska ainu un sadarbojoties ar dalībvalstīm, Komisija saistībā ar *UCPM*:

(a) pastāvīgi analizēs un testēs esošās reaģēšanas spējas piemērotību un darbības gatavību;

(b) regulāri pārskatīs iespējamo vajadzību izstrādāt jaunas reaģēšanas spējas ES līmenī, izmantojot *rescEU*;

(c) vēl vairāk pastiprinās starpnozaru sadarbību, lai nodrošinātu pienācīgu reaģēšanu ES līmenī, un organizēs regulāras mācības, lai testētu šo sadarbību;

(d) turpinās attīstīt *ERCC* kā starpnozaru krīzes centru ES līmenī, lai koordinētu atbalstu skartajām dalībvalstīm.

(29) Komisija sadarbībā ar Augsto pārstāvi un intensīvi konsultējoties ar dalībvalstīm un ar atbilstošo Savienības aģentūru atbalstu izstrādās kritiskās infrastruktūras incidentu un krīžu plānu, kurā aprakstīts un izklāstīts, kādu mērķu labad un kādos veidos sadarbojas dalībvalstis un ES iestādes, struktūras, biroji un aģentūras, reaģējot uz incidentiem, kas vērsti pret kritisko infrastruktūru, sevišķi gadījumos, kad tie rada būtiskus traucējumus pamatpakalpojumu sniegšanai iekšējā tirgū. Šajā plānā būtu jāizmanto esošie integrētie krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismi reaģēšanas koordinēšanai.

(30) Komisija sadarbosies ar ieinteresētajām personām un ekspertiem saistībā ar iespējamiem atjaunošanas pasākumiem pēc incidentiem attiecībā uz zemūdens kabeļu infrastruktūru – tie jāiesniedz kopā ar 20. punkta a) apakšpunktā minēto novērtēšanas pētījumu, kā arī turpinās ārkārtas situāciju plānu un riska scenāriju izstrādi un strādās pie Savienības noturības pret katastrofām Savienības civilās aizsardzības mehānisma ietvaros.

IV NODAĻA. STARPTAUTISKĀ SADARBĪBA

(31) Komisija un Augstais pārstāvis vajadzības gadījumā un saskaņā ar to attiecīgajiem uzdevumiem un pienākumiem, kas noteikti Savienības tiesību aktos, atbalstīs partnervalstis, lai uzlabotu to vienību noturību, kuras to teritorijā ekspluatē kritisko infrastruktūru.

(32) Komisija un Augstais pārstāvis atbilstoši saviem attiecīgajiem uzdevumiem un pienākumiem, kas noteikti Savienības tiesību aktos, stiprinās koordināciju ar NATO kritiskās infrastruktūras noturības jomā, izmantojot ES un NATO strukturēto dialogu par noturību, un šim nolūkam izveidos darba grupu.

(33) Dalībvalstis tiek aicinātas sadarbībā ar Komisiju un Augsto pārstāvi sniegt ieguldījumu ES hibrīddraudu novēršanas rīkkopas un Padomes secinājumos par satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām[25] minēto īstenošanas pamatnostādņu paātrinātā izstrādē un īstenošanā un pēc tam tās izmantot, lai pilnībā īstenotu satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, jo īpaši apsverot un sagatavojot visaptverošu un koordinētu ES reaģēšanu uz hibrīdkampaņām un

[25] *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns - Consilium (europa.eu)*

hibrīdapdraudējumu, tostarp tiem, kas vērsti pret vienībām, kuras ekspluatē kritisko infrastruktūru.

(34) Nepieciešamības gadījumā Komisija apsvērs trešo valstu pārstāvju dalību sadarbībā un informācijas apmaiņā starp dalībvalstu ekspertiem kritisko infrastruktūru ekspluatējošo vienību noturības jomā.

[…]

Strasbūrā,

Padomes vārdā –
priekšsēdētājs