C/2024/1049

9.2.2024.

Eiropas Reģionu komitejas atzinums "ES Kibersolidaritātes akts un digitālā noturība"

(C/2024/1049)

Ziņotājs:	*Pehr GRANFALK* (*SE/PPE*), Solnas komūnas padomes loceklis
Atsauces dokuments:	Priekšlikums Eiropas Parlamenta un Padomes regulai, kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberapdraudējumu un kiberincidentus, tiem sagatavoties tiem un uz tiem reaģēt COM(2023) 209 final

I. **IETEIKUMI GROZĪJUMIEM**

COM(2023) 209

1. grozījums

1. apsvērums

Eiropas Komisijas ierosinātais teksts	RK grozījums
Informācijas un komunikācijas tehnoloģiju lietošana un izmantošana visās saimnieciskās dzīves nozarēs ir kļuvušas par fundamentāliem aspektiem laikā, kad mūsu pārvaldes, uzņēmumi un pilsoņi ir cits ar citu pāri nozarēm un robežām saistīti un savstarpēji atkarīgi vairāk nekā jebkad agrāk.	Informācijas un komunikācijas tehnoloģiju lietošana un izmantošana visās saimnieciskās dzīves nozarēs ir kļuvušas par fundamentāliem aspektiem***, bet arī padarījušas viegli ievainojamas*** mūsu pārvaldes, ***uzņēmumus*** un ***pilsoņus laikā, kad tie*** ir cits ar citu pāri nozarēm un robežām saistīti un savstarpēji atkarīgi vairāk nekā jebkad agrāk.

Pamatojums

Pašsaprotams.

2. grozījums

3. apsvērums

Eiropas Komisijas ierosinātais teksts	RK grozījums
Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu un vienību, kuras darbina kritisko infrastruktūru, noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. (..)	Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu***, valstu, reģionu un vietējā līmeņa publiskās pārvaldes*** un vienību, kuras darbina kritisko infrastruktūru, noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. (..)

Pamatojums

Vietējā un reģionālā pārvalde sniedz gan iedzīvotājiem, gan sabiedrībai ļoti nozīmīgus pakalpojumus, un tā ir viens no dinamiska Eiropas tirgus svarīgākajiem elementiem.

3. grozījums

29. apsvērums

Eiropas Komisijas ierosinātais teksts	RK grozījums
Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, jāsniedz atbalsts koordinētai tādu vienību kiberdrošības pārbaudei un novērtēšanai, kuras darbojas saskaņā ar Direktīvu (ES) 2022/2555 apzinātās ļoti kritiskās nozarēs. Šajā nolūkā Komisijai ar *ENISA* atbalstu un sadarbībā ar TID sadarbības grupu, kas izveidota ar Direktīvu (ES) 2022/2555, regulāri jānosaka attiecīgās nozares vai apakšnozares, kurām jābūt tiesīgām saņemt finansiālu atbalstu koordinētai pārbaudei Savienības līmenī. Nozares vai apakšnozares jāizraugās no Direktīvas (ES) 2022/2555 I pielikuma ("Sevišķi kritiskās nozares"). Koordinētās pārbaudes (..)	Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, jāsniedz atbalsts koordinētai tādu vienību kiberdrošības pārbaudei un novērtēšanai, kuras darbojas saskaņā ar Direktīvu (ES) 2022/2555 apzinātās ļoti kritiskās nozarēs. Šajā nolūkā Komisijai ar *ENISA* atbalstu un sadarbībā ar TID sadarbības grupu, kas izveidota ar Direktīvu (ES) 2022/2555, regulāri jānosaka attiecīgās nozares vai apakšnozares, kurām jābūt tiesīgām saņemt finansiālu atbalstu koordinētai pārbaudei Savienības līmenī. Nozares vai apakšnozares***, kā arī reģionālā un vietējā līmeņa publiskās pārvaldes iestādes neatkarīgi no tā, vai tās saskaņā ar valsts tiesību aktiem tiek uzskatītas par sevišķi kritiskām,*** jāizraugās no Direktīvas (ES) 2022/2555 I pielikuma ("Sevišķi kritiskās nozares"). Koordinētās pārbaudes (..)

Pamatojums

Tā kā dalībvalstīm ir iespēja vietējās un reģionālās pašvaldības izslēgt no TID2 direktīvas ([1]) īstenošanas, būtu jānodrošina, ka pašvaldības tiek ņemtas vērā Kibersolidaritātes aktā.

4. grozījums

30. apsvērums

Eiropas Komisijas ierosinātais teksts	RK grozījums
Turklāt kiberavārijas mehānismam jāsniedz atbalsts citām sagatavotības darbībām un jāatbalsta sagatavotība citās nozarēs, uz kurām neattiecas tādu vienību koordinēta pārbaude, kuras darbojas ***ļoti*** kritiskās nozarēs. Minētajās darbībās var ietilpt dažādi valstu gatavības pasākumi.	Turklāt kiberavārijas mehānismam jāsniedz atbalsts citām sagatavotības darbībām un jāatbalsta sagatavotība citās nozarēs, uz kurām neattiecas tādu vienību koordinēta pārbaude, kuras darbojas kritiskās nozarēs. ***Tas pats attiecas uz publisko pārvaldi neatkarīgi no tā, vai to uzskata par kritisku saskaņā ar valsts tiesību aktiem.*** Minētajās darbībās var ietilpt dažādi valstu gatavības pasākumi.

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

Pamatojums

Vietējām un reģionālajām pašvaldībām būtu jādod iespēja gūt labumu no kiberavārijas mehānisma sniegtā atbalsta.

5. grozījums

33. apsvērums

Eiropas Komisijas ierosinātais teksts	RK grozījums
Lai atbalstītu reaģēšanas un tūlītējas atkopšanas darbības ievērojamu vai plašu kiberincidentu gadījumos, pakāpeniski jāveido Savienības līmeņa kiberdrošības rezerves, kas sastāv no pārvaldīto drošības pakalpojumu privāto sniedzēju pakalpojumiem. ES kiberdrošības rezervēm jānodrošina dienestu pieejamība un gatavība. Pakalpojumiem no ES kiberdrošības rezervēm jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām***, kuras darbojas kritiskās vai ļoti kritiskās nozarēs***. Pieprasot atbalstu no ES kiberdrošības rezervēm, dalībvalstīm jāprecizē atbalsts, kas skartajai vienībai sniegts valsts līmenī, un tas jāņem vērā, novērtējot dalībvalsts pieprasījumu. Ar līdzīgiem nosacījumiem pakalpojumus no ES kiberdrošības rezervēm var izmantot arī Savienības iestāžu, struktūru un aģentūru atbalstīšanai.	Lai atbalstītu reaģēšanas un tūlītējas atkopšanas darbības ievērojamu vai plašu kiberincidentu gadījumos, pakāpeniski jāveido Savienības līmeņa kiberdrošības rezerves, kas sastāv no pārvaldīto drošības pakalpojumu privāto sniedzēju pakalpojumiem. ES kiberdrošības rezervēm jānodrošina dienestu pieejamība un gatavība. Pakalpojumiem no ES kiberdrošības rezervēm jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām. Pieprasot atbalstu no ES kiberdrošības rezervēm, dalībvalstīm jāprecizē atbalsts, kas skartajai vienībai sniegts valsts līmenī, un tas jāņem vērā, novērtējot dalībvalsts pieprasījumu. Ar līdzīgiem nosacījumiem pakalpojumus no ES kiberdrošības rezervēm var izmantot arī Savienības iestāžu, struktūru un aģentūru atbalstīšanai.

Pamatojums

Atbalsts no ES kiberdrošības rezervēm būtu jāsaņem visām skartajām vienībām, nevis tikai tām, kas darbojas kritiskās vai ļoti kritiskās nozarēs.

6. grozījums

1. panta 2. punkta b) apakšpunkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
visā Savienībā stiprināt to vienību gatavību, kuras darbojas kritiskās un ļoti kritiskās nozarēs, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt ievērojama vai plaša kiberincidenta gadījumā, arī darot pieejamu Savienības atbalstu ar programmu "Digitālā Eiropa" ("PDE") asociētajām trešajām valstīm reaģēšanai uz kiberincidentiem;	visā Savienībā stiprināt ***gan*** to vienību gatavību, kuras darbojas kritiskās un ļoti kritiskās nozarēs***, gan to publiskās pārvaldes iestāžu gatavību, kas darbojas valsts un tam pakārtotajos līmeņos***, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt ievērojama vai plaša kiberincidenta gadījumā, arī darot pieejamu Savienības atbalstu ar programmu "Digitālā Eiropa" ("PDE") asociētajām trešajām valstīm reaģēšanai uz kiberincidentiem;

Pamatojums

Šīs regulas darbības jomā būtu jāiekļauj arī vietējās un reģionālā līmeņa iestādes.

7. grozījums

4. panta 1. punkta otrā daļa

Eiropas Komisijas ierosinātais teksts	RK grozījums
Tam ir spēja būt par uzziņas avotu un vārteju citām publiskām un privātām organizācijām valsts līmenī, lai vāktu un analizētu informāciju par kiberdrošības apdraudējumu un incidentiem un sekmētu pārrobežu DOC izveidi. (..)	Tam ir spēja būt par uzziņas avotu un vārteju citām publiskām un privātām organizācijām valsts ***un tam pakārtotajos līmeņos***, lai vāktu un analizētu informāciju par kiberdrošības apdraudējumu un incidentiem un sekmētu pārrobežu DOC izveidi. (..)

Pamatojums

Valstu drošības operāciju centriem (DOC) būtu arī jāvāc un jāanalizē reģionālā un vietējā līmeņa iestāžu informācija.

8. grozījums

5. panta 2. punkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
Pēc uzaicinājuma izteikt ieinteresētību *ECCC* atlasa mitināšanas konsorciju dalībai ar *ECCC* kopīgā rīku un infrastruktūru iepirkumā. *ECCC* var mitināšanas konsorcijam piešķirt dotāciju rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet mitināšanas konsorcijs sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras *ECCC* un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.	Pēc uzaicinājuma izteikt ieinteresētību *ECCC* atlasa mitināšanas konsorciju dalībai ar *ECCC* kopīgā rīku un infrastruktūru iepirkumā. *ECCC* var mitināšanas konsorcijam piešķirt dotāciju rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet atlikušās izmaksas ***mitināšanas konsorcijs sedz ar citiem līdzekļiem, nevis tiem, kuri tiek nodrošināti ar Regulu (ES) Nr. 1060/2021 (Kopīgo noteikumu regulu)***. Pirms rīku un infrastruktūras iegādes procedūras *ECCC* un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

Pamatojums

Kibersolidaritātes aktā paredzētie pasākumi nebūtu jāfinansē no kohēzijas politikas programmām.

9. grozījums

9. panta 1. punkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
Lai uzlabotu Savienības noturību pret ***ievērojamu*** kiberdrošības apdraudējumu un solidāri sagatavotos ievērojamu un plašu kiberincidentu īslaicīgai ietekmei un to mazinātu, tiek izveidots kiberavārijas mehānisms (“mehānisms”).	Lai uzlabotu Savienības noturību pret kiberdrošības apdraudējumu un solidāri sagatavotos ievērojamu un plašu kiberincidentu īslaicīgai ietekmei un to mazinātu, tiek izveidots kiberavārijas mehānisms (“mehānisms”).

Pamatojums

Ar kiberavārijas mehānismu būtu jāgatavojas visu veidu kiberincidentu īstermiņa ietekmei un jāmazina šī ietekme.

10. grozījums

10. panta 2. punkts (jauns)

Eiropas Komisijas ierosinātais teksts	RK grozījums
	2. Komisija sagatavo gada ziņojumu, kurā novērtē mehānisma darbību un vajadzību pēc iespējamām papildu prasībām attiecībā uz sadarbību vai apmācību.

Pamatojums

Komisijai būtu jāsniedz regulāri ziņojumi, jo kiberdrošības joma ir dinamiska un prasības ir savlaicīgi jāpielāgo realitātei.

11. grozījums

11. panta 1. punkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
Lai visā Savienībā atbalstītu koordinētas 10. panta 1. punkta a) apakšpunktā minēto vienību gatavības pārbaudes, Komisija pēc apspriešanās ar TID sadarbības grupu un *ENISA* nosaka attiecīgās nozares vai apakšnozares no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām ļoti kritiskajām nozarēm, no kurām vienības var pakļaut koordinētai gatavības pārbaudei, ņemot vērā iegūtos un plānotos koordinētos riska novērtējumus un noturības pārbaudes Savienības līmenī.	Lai visā Savienībā atbalstītu koordinētas 10. panta 1. punkta a) apakšpunktā minēto vienību gatavības pārbaudes, Komisija pēc apspriešanās ar TID sadarbības grupu un *ENISA* nosaka attiecīgās nozares vai apakšnozares no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām ļoti kritiskajām nozarēm***, tostarp publiskās pārvaldes struktūras vietējā līmenī***, no kurām vienības var pakļaut koordinētai gatavības pārbaudei, ņemot vērā iegūtos un plānotos koordinētos riska novērtējumus un noturības pārbaudes Savienības līmenī.

Pamatojums

Vietējām un reģionālajām pašvaldībām būtu jādod iespēja gūt labumu no kiberārkārtas mehānisma. Ar šo grozījumu tiek iekļauta ziņotāja prasība, kas izteikta 3. grozījumā (attiecībā uz 30. apsvērumu).

12. grozījums

14. panta 2. punkta b) apakšpunkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
skartās vienības veids, augstāk prioritarizējot incidentus, kuri skar Direktīvas (ES) 2022/2555 3. panta 1. punktā definētās būtiskās vienības;	skartās vienības***, tostarp reģionālās un vietējās publiskās pārvaldes iestāžu*** veids, augstāk prioritarizējot incidentus, kuri skar Direktīvas (ES) 2022/2555 3. panta 1. punktā definētās būtiskās vienības;

Pamatojums

Darbības jomas precizēšana, iekļaujot vietējās un reģionālās iestādes.

13. grozījums

18. panta 1. punkts

Eiropas Komisijas ierosinātais teksts	RK grozījums
Pēc Komisijas, *EUCyCLONe* vai *CSIRT* tīkla pieprasījuma *ENISA* izskata un novērtē apdraudējumu, vājās vietas un apdraudējuma mazināšanas darbības, kas attiecas uz konkrētu ievērojamu vai plašu kiberincidentu. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* iesniedz incidenta pārskata ziņojumu *CSIRT* tīklam, *EU-CyCLONe* un Komisijai, lai palīdzētu tiem veikt to uzdevumus, sevišķi Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. Attiecīgā gadījumā Komisija ziņojumu iesniedz Augstajam pārstāvim.	Pēc Komisijas, *EUCyCLONe* vai *CSIRT* tīkla pieprasījuma *ENISA* izskata un novērtē apdraudējumu, vājās vietas un apdraudējuma mazināšanas darbības, kas attiecas uz konkrētu ievērojamu vai plašu kiberincidentu. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* iesniedz incidenta pārskata ziņojumu *CSIRT* tīklam, *EU-CyCLONe* un Komisijai, lai palīdzētu tiem veikt to uzdevumus, sevišķi Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. ***Ja iespējams, CSIRT tīkls iesniedz ziņojumu vietējā un reģionālā līmeņa iestādēm.*** Attiecīgā gadījumā Komisija ziņojumu iesniedz Augstajam pārstāvim.

Pamatojums

Darbības jomas precizēšana, iekļaujot vietējās un reģionālās iestādes.

II. **IETEIKUMI POLITIKAS JOMĀ**

EIROPAS REĢIONU KOMITEJAS NOSTĀJA

Eiropas Reģionu komiteja (RK) atzinīgi vērtē Eiropas Komisijas priekšlikumu regulai par Eiropas sadarbības stiprināšanu kiberdrošības jomā. Mūsdienās ES dalībvalstis ir cieši un digitāli savienotas, un šī tendence turpmākajos gados kļūs vēl spēcīgāka. Tāpēc Komiteja atzinīgi vērtē Komisijas iniciatīvu kopīgi vērsties pret kiberdraudiem, ko rada arvien straujākā digitalizācija. Priekšlikumā norādīts, ka pieaug kiberincidentu skaits, it īpaši pilsētu un reģionu kompetences jomās. Komisija uzsver, ka jāgatavojas incidentiem svarīgās sabiedrības darbības jomās, tie ir jāpārvar un no tiem ir jāmācās. RK uzskata, ka Komisijas priekšlikumi var sekmēt centienus stiprināt Savienības digitālo noturību.

1. Lai sasniegtu mērķi izveidot digitāli noturīgu Eiropu, politiķiem un iedzīvotājiem ir jāsaprot, ka spēki kiberdrošības jomā ir jāapvieno. Tāpēc RK aicina dalībvalstis, Komisiju un visas vietējās pašvaldības kopīgi palielināt informētību par rīcības nepieciešamību, tostarp par nepieciešamību palielināt investīcijas digitālās noturības veidošanā, it īpaši vietējā un reģionālajā līmenī, un apsvērt tādu aizsardzības instrumentu izstrādi, kas būtu vērsti pret finanšu izspiedējprogrammatūras uzbrukumiem. Lai to paveiktu, nepieciešami gan atbilstoši finansiāli un tehniski pasākumi, gan kvalificētu speciālistu apmācības pasākumi.

2. Komiteja secina, ka priekšlikums daudzviet atsaucas uz TID 2 direktīvu un ir uz to balstīts. Transponējot TID 2 direktīvu valsts līmenī, katra dalībvalsts nosaka, vai vietējās iestādes ietilpst TID 2 direktīvas darbības jomā ([2]). Tā kā katra dalībvalsts var lemt, vai TID 2 direktīvas īstenošanā pašvaldības uzskatāmas par būtiskām vai svarīgām vienībām, visa veida atšķirības starp valstīm ietekmēs pieeju, ko valstis izmantos attiecībā uz Kiberdsolidaritātes aktu tā pašreizējā redakcijā. Lai vietējās pašvaldības, kam dažās dalībvalstīs uzticēta būtisku pienākumu veikšana, netiktu izslēgtas no Kiberdsolidaritātes akta darbības jomas, tiesību akta tekstā būtu jāprecizē, ka šīs iestādes ietilpst tā darbības jomā neatkarīgi no tā, vai uz tām attiecas TID 2 direktīva.

3. Komiteja atzīst, ka kiberdrošība ir digitālās sadarbspējas stūrakmens, tāpēc ir svarīgi, lai reģionu sadarbspējas uzlabošanā ieguldītais darbs tiktu atbalstīts ar spēcīgiem kiberdrošības pasākumiem, kas nodrošinātu, lai kiberuzbrukumi nevājinātu Eiropas reģionu sadarbspēju.

4. Pilsētām un reģioniem jāsaņem konkrēts atbalsts no struktūrām, ko paredzēts izveidot, un nav pieļaujams, ka pienākums ziņot šīm struktūrām ir vienīgais pasākums, kas attiecas uz pilsētām un reģioniem. Tāpēc Komiteja aicina skaidrāk formulēt, kā reģioni tiek atbalstīti, it īpaši arī, lai paaugstinātu kiberdrošības līmeni mazās kopienās.

Viedokļi par priekšlikuma darbības jomām

Eiropas kibervairogs

Izveidot Eiropā drošības operāciju centru infrastruktūru, lai attīstītu un uzlabotu kopīgas spējas atklāt kiberdraudus un kiberincidentus, analizēt un apstrādāt datus par tiem.

5. Lai varētu gūt visaptverošu priekšstatu par pašreizējo kiberdrošības stāvokli Eiropas Savienībā, jāapkopo informācija, riska novērtējumi, draudi un incidenti, tostarp no vietējiem un valstu sistēmu nodrošinātājiem. RK uzskata, ka problēmas var radīt tas, ka nav skaidru stimulu un procedūru attiecībā uz to, kā pilsētas un reģioni var aktīvi veicināt digitālās noturības stiprināšanu. Vietējā un reģionālā līmeņa iesaiste ir ļoti svarīga, jo tam ir digitāli risinājumi, kas pakļauti uzbrukumiem. Tāpēc ir jārada vide, kurā pilsētas un reģionus var iesaistīt un kurā tie būtu jāiesaista kā partneri centienos vairot kiberdrošību Savienībā.

6. Komitejas pētījumos konstatēts, ka pastāv būtiskas valstu atšķirības tādā jomā kā aizsardzība un veiktie drošības pasākumi. Pat vienā valstī vērojamas būtiskas kiberdrošības spēju un mērķu atšķirības, piemēram, starp valsts iestādēm un mazākām vietējām iestādēm. Tāpēc Komiteja uzskata, ka regulai būtu jāpalīdz mazināt šīs atšķirības un jānodrošina, ka visiem iesaistītajiem dalībniekiem ir salīdzinoši līdzvērtīgas spējas un mērķi.

7. Komiteja vērš uzmanību uz risku, ka jaunā valstu un pārrobežu drošības operāciju centru tīkla uzdevumi varētu pārklāties ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīkla uzdevumiem ([3]). Ja līdztekus datordrošības incidentu reaģēšanas vienībām tiek veidoti valstu drošības centri, ir skaidri jādefinē, kā paredzēts sadarboties un kādi ir valstu drošības operāciju centru un *CSIRT* pienākumi incidenta gadījumā.

([2]) TID 2 direktīvas 2. panta 5. punkts. Dalībvalstis var paredzēt, ka šo direktīvu piemēro: a) valsts pārvaldes vienībām vietējā līmenī.

([3]) Saskaņā ar TID 2 direktīvas 11. panta 3. punktu *CSIRT* ir šādi uzdevumi:
a) kiberdraudu, ievainojamības un incidentu uzraudzība un analīze valsts līmenī un pēc pieprasījuma palīdzības sniegšana attiecīgajām būtiskajām un svarīgajām vienībām saistībā ar to tīklu un informācijas sistēmu uzraudzību reāllaikā vai tuvu reāllaikam;
b) agrīnu brīdinājumu, trauksmju, paziņojumu sniegšana un informācijas izplatīšana attiecīgajām būtiskajām un svarīgajām vienībām, kā arī kompetentajām iestādēm un citām attiecīgām ieinteresētajām personām par kiberdraudiem, ievainojamību un incidentiem, ja iespējams – gandrīz reāllaikā;
c) vajadzības gadījumā reaģēšana uz incidentiem un palīdzības sniegšana attiecīgajām būtiskajām un svarīgajām vienībām;
d) kriminālistikas datu vākšana un analīze un dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana attiecībā uz kiberdrošību;
e) pēc būtiskās vai svarīgās vienības pieprasījuma attiecīgās vienības tīklu un informācijas sistēmu proaktīva skenēšana, lai atklātu ievainojamības ar iespējamu būtisku ietekmi;
f) piedalīšanās *CSIRT* tīklā un savstarpējas palīdzības sniegšana atbilstīgi to spējām un kompetencei citiem *CSIRT* tīkla dalībniekiem pēc to lūguma;
g) attiecīgā gadījumā darbošanās kā koordinatorēm koordinētās ievainojamības izpaušanas saskaņā ar 12. panta 1. punktu vajadzībām;
h) līdzdalība drošu informācijas kopīgošanas rīku ieviešanā saskaņā ar 10. panta 3. punktu.

8. Komiteja atzinīgi vērtē regulas priekšlikuma un ierosināto pasākumu konkrētos mērķus. Vienlaikus pauž nožēlu par to, ka, neraugoties uz pieaugošo kiberuzbrukumu skaitu, pašreizējais priekšlikums pietiekami neaptver vietējās un reģionālās pašvaldības, un tādēļ ierosina vairākas izmaiņas tiesību aktos, lai novērstu šos trūkumus.

9. Pašlaik trūkst datu un skaidru mērījumu par incidentiem, apdraudējumiem un riskiem, kas skar vietējās pašvaldības un reģionus. Eiropas kiberdrošības vairogam būtu jāizstrādā rādītāji, lai varētu novērtēt, kā saistībā ar regulas īstenošanu norit attīstība un paaugstinās gatavības pakāpe. Ilgtermiņā rādītāji var tikt ietverti uz datiem balstītā risku kartē, kas var norādīt, kurās jomās vajadzīga steidzama rīcība.

Kiberavārijas mehānisms

Mērķis ir stiprināt gatavību, novērtēt kritiski svarīgu nozaru gatavību, stiprināt spējas atkopties pēc incidentiem un izveidot kiberdrošības rezervi.

10. Plaši kiberincidenti var būt izskaidrojami ar vietējām norisēm; priekšlikumā jānorāda, kā drošības operāciju centri un kiberdrošības rezerve var pievērsties ne tikai ievērojamiem un plašiem incidentiem, kas jau sākušies, bet arī nopietniem vietējiem traucējumiem. Informācijas apmaiņai nebūtu jāaprobežojas tikai ar plašiem incidentiem, bet tajā būtu jāaptver arī iespējamie draudi.

11. Ar incidentiem saistītā informācija bieži vien ir ļoti sensitīva un var ietvert tehniskus datus vai persondatus, kurus vēl nevar kopīgot bez līgumiem un vienošanās starp pusēm. Pašlaik informācijas apmaiņa valsts līmenī rada grūtības. Tāpēc pārrobežu apmaiņas jautājums ir ļoti sarežģīts. Lai Kiberavārijas mehānisms var darboties, Komisijai ir jānodrošina, ka visām ieinteresētajām personām – gan publiskajiem, gan privātajiem ES kiberdrošības rezerves dalībniekiem – ir juridiski un tehniski priekšnosacījumi informācijas apmaiņai un saņemšanai. Komiteja uzskata, ka galvenokārt tiek izplatīta informācija par incidentu likvidēšanu, t. i., par to, kā incidenta skartās struktūras var vislabāk pārvarēt nopietnu incidentu.

12. RK atzinīgi vērtē to, ka augsta līmeņa prasības noteiktas privātajiem pakalpojumu sniedzējiem, kuri iesaistīti ierosinātajā kiberdrošības rezervē. Tomēr nedrīkst formulēt tādas prasības, kas izslēdz noteiktas prasmes vai zināšanas par sistēmu, jo tikai daži ļoti lieli dalībnieki var izpildīt drošības pakalpojumu sniedzējiem noteiktās prasības. Lai ES būtu pēc iespējas noturīgāka, tai ir jāaptver plašs drošības pasākumu klāsts.

13. Priekšlikumā paredzēts, ka kiberdrošības rezervi veido pakalpojumi, ko sniedz uzticami pakalpojumu sniedzēji. Tie tiek sertificēti saskaņā ar Kiberdrošības aktu ([4]). Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir atbildīga par produktu un pakalpojumu atbilstību noteiktajām kiberdrošības prasībām. RK uzsver, ka Kiberdrošības aģentūrai ir ātri jāizstrādā sertifikācijas sistēmas, lai piegādātāji varētu sevi sertificēt, izmantojot mūsdienīgas tehnoloģijas ([5]).

14. Veidojot kiberdrošības rezervi, arī jānodrošina, ka netiek kropļota konkurence vai ka tiek atstumti dalībnieki, kas darbojas tikai dažās Savienības daļās. Lai varētu izveidot kiberdrošības rezervi un sertifikāciju, vajadzīgas ātras un skaidras procedūras, ar kurām šajā saistībā var apzināt viskompetentākos un svarīgākos dalībniekus.

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

([5]) Kiberdrošības aģentūra pašlaik izstrādā trīs sertifikācijas mehānismus, kas vēl nav pabeigti un aptver IKT, 5G un mākoņpakalpojumus: https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq.

15. RK uzskata, ka nacionālie kritiskām sistēmām vajadzīgo tehnoloģiju nodrošinātāji un pakalpojumu sniedzēji būtu jāapzina un jāreģistrē datubāzē. Šie dati var būt ļoti vērtīgi saistībā ar pasākumiem, kuros jāiesaista vietējie dalībnieki. Tos var izmantot arī Kiberdrošības akadēmijas darbā.

16. Incidenta gadījumā pretpasākumu efektivitāte ir atkarīga no reaģēšanas ātruma. Sarežģītajai informācijai par drošības incidentiem un riskiem īsā laikā jāsasniedz pareizās mērķgrupas. Priekšlikumā paredzēts izveidot jaunu informācijas apmaiņas organizāciju un struktūru. RK tomēr uzsver, ka, veidojot valsts un pārrobežu drošības centrus, ir jāizmanto un jāattīsta esošie informācijas kanāli, piemēram, *CyCLONe* ([6]) un *CSIRT*.

Kiberincidentu izskatīšanas mehānisms

Mērķis ir pārbaudīt kiberincidentus, it īpaši incidentus, kuriem bija būtiska ietekme.

17. Kiberdrošības jomā vajadzīgo prasmju pieprasījumu un to finansēšanas nepieciešamību nosaka straujā digitalizācija. RK atzinīgi vērtē to, ka Komisija izveidojusi Kiberprasmju akadēmiju, un aicina izstrādāt skaidru stratēģiju, kā stiprināt mazākas un finansiāli vājas pilsētas un reģionus, ņemot vērā prasmju trūkumu Eiropas Savienībā.

18. Komiteja uzsver: lai veidotu spēcīgu digitālo noturību, ir vajadzīga dažādu dalībnieku sadarbība, kurā iesaistās publiskas un privātas struktūras ar speciālām zināšanām, pieredzi un personālu. Tā uzsver vietējo un reģionālo pašvaldību lomu digitālās noturības veidošanā, jo tās var cita citu atbalstīt ar izpratnes veicināšanas kampaņām, paraugprakses piemēru apmaiņu un pieredzes apmaiņu. Jo vairāk uzņēmumu iegulda savā digitālajā noturībā, jo lielākas uzbrukumu izmaksas ir to pretiniekiem, un arī tas varētu būt atturošs faktors.

19. Pašlaik Eiropas pilsētas un reģioni sedz gan izmaksas, kas saistītas ar augsta kiberdrošības līmeņa nodrošināšanu, gan arī incidentu radītās izmaksas. RK uzskata, ka regula varētu radīt papildu spiedienu uz jau tā ierobežotajiem resursiem. Tāpēc regula nedrīkst radīt slogu, bet tai ar konkrētiem instrumentiem, procedūrām un atbalstu jāveicina visu iestāžu spēju stiprināšana.

20. RK nesaprot, kāpēc incidenta izskatīšanas ziņojumus nevar kopīgot valstu un pārrobežu drošības operāciju centru tīklā; priekšlikumā paredzēts, ka tikai valstu drošības operāciju centri var piekļūt publisko iestāžu informācijai. Lai dalībnieki varētu uzlabot un pilnveidot kiberdrošību, ir ļoti svarīgi mācīties no incidentos gūtās pieredzes. Sīka informācija būtu jādara pieejama visiem tīkla dalībniekiem.

21. Priekšlikumā finansēšana tiek traktēta pārāk vispārīgi. RK uzskata, ka jāprecizē, kā līdzekļi tiks izlietoti un kāda daļa tiek tieši piešķirta reģioniem un pašvaldībām.

([6]) TID 2 direktīvas 16. panta 1. un 3. punkts.
Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*)
1. *EU-CyCLONe* izveido, lai atbalstītu plašapmēra kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru relevantas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām.
3. *EU-CyCLONe* uzdevumi ir šādi:
   a) paaugstināt plašapmēra kiberdrošības incidentu un krīžu pārvaldības sagatavotības līmeni;
   b) veidot vienotu situācijas izpratni par plašapmēra kiberdrošības incidentiem un krīzēm;
   c) izvērtēt attiecīgo plašapmēra kiberdrošības incidentu un krīžu sekas un ietekmi un ierosināt iespējamos mitigācijas pasākumus;
   d) koordinēt plašapmēra kiberdrošības incidentu un krīžu pārvaldību un atbalstīt lēmumu pieņemšanu politiskā līmenī saistībā ar šādiem incidentiem un krīzēm;
   e) pēc attiecīgās dalībvalsts pieprasījuma apspriest 9. panta 4. punktā minētos valsts plānus reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm.

22. Visbeidzot Komiteja uzsver, ka priekšlikums atbilst subsidiaritātes un proporcionalitātes principiem.

Briselē, 2023. gada 30. novembrī

Eiropas Reģionu komitejas priekšsēdētājs

Vasco ALVES CORDEIRO