Eiropas Savienības
Padome

Briselē, 2021. gada 20. oktobrī
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2021. gada 19. oktobris
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	12534/21
Temats:	Padomes secinājumi "Izpētīt kopējās kibervienības iniciatīvas potenciālu – papildināt koordinētu ES reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm" – Padomes secinājumi (2021. gada 19. oktobris)

Pielikumā pievienoti Padomes secinājumi "Izpētīt kopējās kibervienības iniciatīvas potenciālu – papildināt koordinētu ES reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm", kurus Padome pieņēma 2021. gada 19. oktobra sanāksmē.

PIELIKUMS

Padomes secinājumi "Izpētīt kopējās kibervienības iniciatīvas potenciālu – papildināt koordinētu ES reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm"

EIROPAS SAVIENĪBAS PADOME,

ATGĀDINOT savus secinājumus:

– par ES kiberdrošības stratēģiju digitālajai desmitgadei [1],

– par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm [2],

– par kiberdiplomātiju [3],

– par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums") [4],

– par drošību un aizsardzību [5],

– ES kiberaizsardzības politikas satvaru [6],

– par Eiropas digitālās nākotnes veidošanu [7],

– Padomes Īstenošanas lēmumu (ES) 2018/1993 (2018. gada 11. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" [8],

– par kiberdrošības spēju un spēju veidošanu ES [9],

1. UZSVER kiberdrošības nozīmi noturīgas, digitālas un zaļas Eiropas veidošanā. UZSVER, ka kiberdrošība ir obligāti nepieciešama ES un tās dalībvalstu, tās iedzīvotāju, uzņēmumu un iestāžu labklājībai un drošībai, kā arī mūsu brīvo un demokrātisko sabiedrību integritātes saglabāšanai.

2. ATZĪST daudzu kiberdrošības apdraudējumu pārrobežu un pārnozaru raksturu, kā arī riskus un iespējamās sekas nemitīgām ietekmīgākām, izsmalcinātākām, mērķtiecīgākām, sarežģītākām, noturīgākām un/vai uzmācīgākām ļaunprātīgu kiberdarbību kampaņām [10]. Covid-19 pandēmija ir vēl vairāk atklājusi mūsu sabiedrības ievainojamību un iespēju liela mēroga kiberincidentiem kaitēt ekonomikai, demokrātijai, pamatpakalpojumiem un kritiskajai infrastruktūrai, jo īpaši veselības nozarē. Tā ir arī palielinājusi savienotības nozīmi un sabiedrības atkarību no uzticamām un drošām tīklu un informācijas sistēmām, uz kurām var paļauties. Visbeidzot, tā ir uzsvērusi, ka ir vajadzīgs globāls, atvērts, brīvs, stabils un drošs internets, kā arī uzticēšanās informācijas un komunikācijas tehnoloģiju (IKT) produktiem, procesiem un pakalpojumiem un to drošībai, tostarp, ka ir jānodrošina noturīga piegādes ķēde.

---

8 14435/17 + COR 1.

9 7737/19.

10 *ENISA Threat Landscape 2020* (*ENISA* 2020. gada ziņojums par drošības apdraudējuma ainu).

3. ATKĀRTOTI UZSVER kibernoturības nozīmi un to, ka ir svarīgi turpināt izstrādāt ES kiberdrošības krīžu pārvarēšanas satvaru [11], kura mērķis ir efektīvi un laikus ES līmenī reaģēt uz liela mēroga kiberdrošības incidentiem un krīzēm, un to vēl vairāk integrēt esošajos horizontālajos un nozaru ES mehānismos reaģēšanai krīzes situācijās. UZSVER nozīmi, kāda ir Padomei un integrētajiem krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismiem, lai nodrošinātu savlaicīgu koordināciju un reaģēšanu Savienības politiskā līmenī krīzes situācijās, kuras rodas Savienībā vai ārpus tās un kurām ir plaša ietekme vai politiska nozīme. UZSVER, ka ir svarīgi šādus satvarus un mehānismus testēt regulārās mācībās.

4. ATGĀDINA, ka darbības ES līmenī attiecībā uz liela mēroga kiberincidentiem un krīzēm notiek saskaņā ar subsidiaritātes, proporcionalitātes, papildināmības, nedublēšanās un konfidencialitātes principiem. ATKĀRTOTI UZSVER, ka dalībvalstīm ir galvenā atbildība par reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm, kas tās ietekmē. ATGĀDINA, ka svarīgi ir respektēt dalībvalstu kompetenci un ka valsts drošība ir vienīgi to atbildībā – saskaņā ar Līguma par Eiropas Savienību 4. panta 2. punktu –, tostarp kiberdrošības jomā.

5. Vienlaikus ATGĀDINA, ka svarīgi ir ievērot ES iestāžu, struktūru un aģentūru kompetenci un pilnvaras. Arī Augstajam pārstāvim, Komisijai un citām ES iestādēm, struktūrām un aģentūrām ir būtiska loma, kas izriet no Savienības tiesībām, tostarp, ņemot vērā liela mēroga kiberdrošības incidentu un krīžu iespējamo ietekmi uz vienoto tirgu, kā arī uz pašu ES iestāžu, struktūru un aģentūru darbību.

---

[11] 10086/18.

6. UZSVER, ka ES kiberdrošības krīžu pārvarēšanas satvara turpmākajā izstrādē ir jāizvairās no nevajadzīgas dublēšanās un jācenšas panākt papildināmību un pievienoto vērtību un ka ir jānodrošina saskaņotība ar esošajiem mehānismiem, iniciatīvām, tīkliem, procesiem un procedūrām valstu un Eiropas līmenī. UZSVER, ka svarīgi ir racionalizēt esošos procesus un struktūras, lai mazinātu sarežģītību, un Savienības kohēzijas interesēs uzlabot piekļūstamību un reaģētspēju tiem, kas meklē palīdzību un solidaritāti.

7. ATZĪST starptautisko tiesību, tostarp Apvienoto Nāciju Organizācijas Statūtu kopumā, starptautisko humanitāro tiesību un cilvēktiesību, piemērojamību kibertelpā un VEICINA to, ka tiek ievērotas visu ANO dalībvalstu apstiprinātās brīvprātīgas, nesaistošas normas, noteikumi un principi par valstu atbildīgu rīcību kibertelpā.

8. ATZINĪGI VĒRTĒ progresu, kas pēdējos gados gūts Padomē, jo īpaši Kiberjautājumu horizontālajā darba grupā (*HWPCI*) un citās attiecīgās Padomes darba grupās, kā arī izveidojot citas sadarbības un informācijas apmaiņas iniciatīvas, tīklus un mehānismus starp dalībvalstīm, jo īpaši Tīklu un informācijas drošības (TID) sadarbības grupu un datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu, kas izveidots ar Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu (ES) 2016/1148, Kiberkrīžu sadarbības organizāciju tīklu (*CyCLONe*), kā arī attiecīgus ar kiberaizsardzību saistītus projektus, kas sākti pastāvīgās strukturētās sadarbības (*PESCO*) [12] ietvaros, Kopīgās kibernoziedzības rīcības uzdevumgrupu (*J-CAT*), Eiropas Tiesu iestāžu tīklu kibernoziedzības jautājumos (*EJCN*), dalībvalstu brīvprātīgos ieguldījumus ES *INTCEN* un koordināciju un sadarbību saistībā ar kiberdiplomātijas instrumentu kopumu.

[12] Jo īpaši "Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā", ko koordinē Lietuva, "Kibertelpas un informācijas telpas koordinācijas centrs", ko koordinē Vācija, "Kiberdraudu un kiberincidentu reaģēšanas informācijas apmaiņas platforma", ko koordinē Grieķija.

9. ATGĀDINA esošos ES iestāžu, struktūru un aģentūru sadarbības satvarus, piemēram, strukturēto sadarbību starp *ENISA* un *CERT-EU* un saprašanās memorandu starp *ENISA*, Eiropas Aizsardzības aģentūru (EAA), Eiropola Eiropas Kibernoziedzības apkarošanas centru (*EC3*) un *CERT-EU*. UZSVER, ka ir svarīgi turpināt regulāru informācijas apmaiņu ar Padomi par turpmāko attīstību šajos sadarbības satvaros.

10. UZSVER, ka ir svarīgi uzlabot sadarbību un informācijas apmaiņu starp dažādām kiberkopienām ES un tās dalībvalstīs visos nepieciešamajos līmeņos – tehniskajā, operatīvajā un stratēģiskajā/politiskajā – un savienot esošos krīžu pārvarēšanas mehānismus, tīklus, struktūras, procesus un procedūras, ja tādējādi atbalsta un uzlabo liela mēroga kiberincidentu un krīžu pārvarēšanu.

11. ATZĪST progresu, ko panākusi dalībvalstu grupa, *PESCO* satvarā izveidojot kopīgas operatīvas kiberspējas "Kiberdrošības ātrās reaģēšanas vienības", kuru mērķis ir, sniedzot savstarpēju palīdzību, padziļināt brīvprātīgu sadarbību kiberjomā, tostarp, reaģējot uz liela mēroga kiberincidentiem un krīzēm.

12. ATZĪST tiesībaizsardzības kopienas pieredzi un reaģēšanas spējas 24/7 režīmā operatīvās sadarbības un drošas informācijas apmaiņas jomā attiecībā uz lieliem pārrobežu kiberuzbrukumiem, kas tiek nodrošinātas, izmantojot ES tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokolu.

13. ATZĪST, ka tiek turpināts īstenot satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums"). ATGĀDINA, ka katra dalībvalsts katrā gadījumā atsevišķi var pieņemt pati savu suverēnu lēmumu par ļaunprātīgas kiberdarbības attiecināšanu. ATGĀDINA, ka pasākumiem, kas veikti satvara vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ietvaros, būtu jābalstās uz kopīgu situācijas apzināšanos, par ko vienojušās dalībvalstis. Būtiska nozīme ir ES *INTCEN* kā centram, kas Eiropas Savienībai nodrošina situācijas apzināšanos un draudu novērtējumu attiecībā uz kiberjautājumiem, balstoties uz dalībvalstu izlūkdienestu brīvprātīgiem ieguldījumiem un neskarot dalībvalstu kompetenci.

14. ATKĀRTOTI UZSVER savstarpējas palīdzības un solidaritātes nozīmi saskaņā ar Līguma par Eiropas Savienību 42. panta 7. punktu un Līguma par Eiropas Savienības darbību 222. pantu un AICINA rīkot turpmākas mācības, kuras ietver kiberdimensiju. ATGĀDINA, ka ir jāapsver saikne starp ES kiberdrošības krīžu pārvarēšanas satvaru, kiberdiplomātijas instrumentu kopumu un minēto pantu noteikumiem liela mēroga kiberincidenta vai krīzes gadījumā. Turklāt ATGĀDINA, ka dalībvalstu pienākumi, kas izriet no Līguma par Eiropas Savienību 42. panta 7. punkta, neskar dažu dalībvalstu drošības un aizsardzības politikas īpašās iezīmes. Tāpat ATGĀDINA, ka NATO joprojām ir to valstu, kuras ir NATO locekles, kolektīvās aizsardzības pamats.

15. ATZĪST ES un NATO sadarbību kiberdrošības un kiberaizsardzības jomā, tostarp informācijas apmaiņu starp *CERT-EU* un NATO Datorincidentu reaģēšanas spējām (*NCIRC*), pilnībā ievērojot pārredzamības, savstarpības un iekļautības principus, kā arī abu organizāciju lēmumu pieņemšanas autonomiju.

16. ATZĪST, ka attiecīgā gadījumā svarīga ir sadarbība ar privāto sektoru attiecībā uz informācijas apmaiņas mācībām un attiecīgu speciālo zināšanu sniegšanu, kā arī uzticamiem risinājumiem un pakalpojumiem, tostarp, piemēram, atbalstot reaģēšanu uz incidentiem un uzlabojot situācijas apzināšanos starp dažādām kiberkopienām.

17. UZSVER drošu sakaru kanālu nozīmi klasificētas un sensitīvas informācijas apmaiņā. UZSVER, ka ir vajadzīgs turpmāks progress.

Šajā sakarā un ņemot vērā iepriekš minēto,

18. ATZĪST Komisijas Ieteikumu par Kopējās kibervienības izveidošanu kā iniciatīvu, kas jāapsver, turpinot izstrādāt ES kiberdrošības krīžu pārvarēšanas satvaru [13].

19. AICINA ES un tās dalībvalstis turpināt centienus virzībā uz visaptverošāku un efektīvāku ES kiberdrošības krīžu pārvarēšanas satvaru, pamatojoties uz esošajiem mehānismiem un jau gūto progresu, un ņemt vērā kopējās kibervienības iniciatīvas potenciālu papildināt šos mehānismus, izmantojot pakāpenisku pieeju. UZSVER, ka pakāpenisks, pārredzams un iekļaujošs process ir būtisks, lai vairotu uzticēšanos, un tāpēc tam ir izšķiroša nozīme ES kiberdrošības krīžu pārvarēšanas satvara turpmākajā izstrādē. Šajā procesā būtu jāņem vērā dalībvalstu un ES iestāžu, struktūru un aģentūru esošās funkcijas, kompetences un pilnvaras, kā arī šajos secinājumos noteiktie principi, tostarp proporcionalitāte, subsidiaritāte, iekļautība, papildināmība, nedublēšanās un informācijas konfidencialitāte. Vienlaikus UZSVER, ka jebkāda iespējama dalībvalstu dalība vai ieguldījumi iespējamā kopējā kibervienībā ir brīvprātīgi.

[13] C(2021) 4520 final (11155/21 un 11155/21 ADD1).

20. UZSVER, ka ir jāizveido piemērotas darba metodes un pārvaldība, lai visas dalībvalstis varētu iesaistīties apspriedēs, izstrādē un efektīvā lēmumu pieņemšanas procesā par ES kiberdrošības krīžu pārvarēšanas satvaru, tostarp par iespējamās kopējās kibervienības iniciatīvu. AICINA ievērot Līgumos noteiktās Padomes prerogatīvas un lojālas sadarbības principu.

21. UZSVER, ka ir svarīgi apzināt un iesaistīt visas attiecīgās kiberkopienas ES un tās dalībvalstīs, vienlaikus ņemot vērā to atšķirīgās lomas un atbildību dažādu veidu liela mēroga kiberincidentos un krīzēs. UZSVER Padomes būtisko lomu, jo īpaši ar *HWPCI* starpniecību, politikas veidošanā un koordinācijas funkciju attiecībā uz ES kiberdrošības krīžu pārvarēšanas satvara turpmāku izstrādi. Tāpēc AICINA dalībvalstis, Komisiju, Eiropas Ārējās darbības dienestu (EĀDD), ES *INTCEN*, *CERT-EU*, *ENISA*, Eiropolu (*EC3*), *Eurojust* (*EJCN*), Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru (*ECCC*), kā arī *CSIRT* tīkla, *CyCLONe*, TID sadarbības grupas, EAA un attiecīgo *PESCO* projektu pārstāvjus, kā arī citas iespējamās ieinteresētās personas iesaistīties šajā procesā. Iespējamo darba grupu, kā ierosināts Komisijas ieteikumā, varētu izstrādāt sīkāk, nodrošinot visu dalībvalstu pienācīgu pārstāvību un rīkojoties saskaņā ar Padomes politiskajām norādēm, lai tā darbotos kā pagaidu forums, kurā kopā tiktu pulcēti pārstāvji no visām attiecīgajām kiberkopienām dalībvalstīs un ES. Šādai darba grupai būtu regulāri jāziņo par savām darbībām un iespējamie ierosinājumi jāiesniedz Padomei apspriešanai, apstiprināšanai un turpmākiem norādījumiem. Turklāt varētu izveidot citus dialoga veidus kopienās un starp tām, tostarp, izmantojot darbseminārus, seminārus, kopīgu apmācību un mācības.

22. UZSVER Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra (*ECCC*) un Nacionālo koordinācijas centru tīkla lomu saistībā ar iespējamo kopējo kiberdrošības vienību, jo īpaši, ņemot vērā, kāda tam ir loma, lai būtiski palielinātu Savienības tehnoloģiskās spējas, tehnoloģiskos risinājumus, spējas un prasmes kiberdrošības jomā.

23. AICINA ES un tās dalībvalstis iesaistīties ES kiberdrošības krīžu pārvarēšanas satvara turpmākā izstrādē, tostarp, izpētot kopējās kibervienības iniciatīvas potenciālu, nosakot un definējot procesu, tostarp starpposma mērķrādītājus un grafiku, kā arī precizējot mērķus un iespējamās funkcijas un pienākumus. UZSVER, ka prioritārā kārtā ir jākonsolidē esošie tīkli un mijiedarbība katrā kopienā, kā arī rūpīgi jāapzina iespējamie informācijas apmaiņas trūkumi un vajadzības kiberkopienās un starp tām, kā arī Eiropas iestādēs, struktūrās un aģentūrās un starp tām, un pēc tam jāvienojas par iespējamās kopējās kibervienības iespējamiem galvenajiem mērķiem un prioritātēm. Pāragri nespriežot par iznākumu, UZSVER, ka ir jākoncentrējas uz informācijas apmaiņas vajadzību apzināšanu, lai veidotu kopīgu situācijas apzināšanos starp visām attiecīgajām kopienām. Apzinot informācijas apmaiņas trūkumus un vajadzības, tostarp iespējamo virtuālo platformu izmantošanu, pienācīga uzmanība arvien būtu jāpievērš drošiem saziņas kanāliem klasificētas un sensitīvas informācijas apmaiņai, un vienlaikus UZSVER, ka svarīgi ir izmantot jau esošo infrastruktūru. Pakāpeniskas pieejas ieviešana ir paredzēta, lai veidotu uzticēšanos un pamatu iespējamiem turpmākiem pasākumiem, kas saistīti ar sagatavotības un operatīvās sadarbības uzlabošanu. ATZĪST, ka dažādiem mērķiem varētu būt vajadzīgi dažādi risinājumi un dažādu ES un tās dalībvalstu attiecīgo kiberkopienu pārstāvju iesaiste.

24. AICINA visā procesā turpināt apsvērt iespējamās kopējās kibervienības juridisko pamatu, tostarp novērtēt uzdevumus un funkcijas attiecībā pret tiem uzdevumiem un funkcijām, kas ieteikumā uzticēti *ENISA*, ņemot vērā Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa Regulas (ES) 2019/881 7. pantu. AICINA sīkāk apsvērt Ieteikuma par Kopējo kiberdrošības vienību atsevišķus elementus, tostarp attiecībā uz ideju par ES kiberdrošības ātrās reaģēšanas komandām un ES plānu reaģēšanai uz kiberdrošības incidentiem un krīzēm. UZSVER, ka iespējamai kopējai kibervienībai ir jāievēro tās iespējamo turpmāko dalībnieku kompetence, pilnvarojums un juridiskās pilnvaras.

25. AICINA ES un tās dalībvalstis apsvērt kopējās kibervienības iniciatīvas potenciālu arī no ES iestāžu, struktūru un aģentūru skatupunkta, lai papildinātu pašreizējos centienus dalībvalstu līmenī. ATZINĪGI VĒRTĒ Komisijas nodomu stiprināt attiecīgo ES iestāžu, struktūru un aģentūru noturību, proti, ar gaidāmo priekšlikumu regulai par kopīgiem saistošiem kiberdrošības noteikumiem ES iestādēm, struktūrām un aģentūrām.

26. Visbeidzot, ATKĀRTOTI APLIECINA savu apņemšanos uzlabot kibernoturību un turpināt izstrādāt ES kiberdrošības krīžu pārvarēšanas satvaru un REGULĀRI PĀRRAUDZĪS progresu, un sniegs turpmākus norādījumus ES kiberdrošības krīžu pārvarēšanas satvara papildināšanai.