Eiropas Savienības
Padome

Briselē, 2022. gada 23. maijā
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2022. gada 23. maijs
Saņēmējs:	delegācijas
Temats:	Padomes secinājumi par Eiropas Savienības pozīcijas kiberjautājumos izstrādi – Padomes secinājumi, kurus Padome apstiprināja 2022. gada 23. maija sanāksmē

Pielikumā pievienoti Padomes secinājumi par Eiropas Savienības pozīcijas kiberjautājumos izstrādi, kurus Padome apstiprināja 2022. gada 23. maija sanāksmē.

PIELIKUMS

Padomes secinājumi par Eiropas Savienības pozīcijas kiberjautājumos izstrādi

EIROPAS SAVIENĪBAS PADOME,

ATGĀDINOT savus secinājumus:

– par 2013. gada 25. jūnija kopīgo paziņojumu Eiropas Parlamentam un Padomei "Eiropas Savienības kiberdrošības stratēģija – "atvērta un droša kibertelpa" [1],

– par ES kiberaizsardzības politikas satvaru [2],

– par interneta pārvaldību [3],

– par kiberdiplomātiju [4],

– "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" [5],

– par 2017. gada 20. novembra kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" [6],

– par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums") [7],

– par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm [8],

– par ES ārējo kiberspēju veidošanas pamatnostādnēm [9],

– Padomes Īstenošanas lēmumu (ES) 2018/1993 (2018. gada 11. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem [10],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– par kiberdrošības spēju un spēju veidošanu ES [11],

– par 5G nozīmi Eiropas ekonomikā un nepieciešamību mazināt ar 5G saistītos drošības riskus [12],

– par augsti digitalizētas Eiropas nākotni pēc 2020. gada: "Visas Savienības digitālās un ekonomiskās konkurētspējas un digitālās kohēzijas stiprināšana" [13],

– "Papildu centieni uzlabot noturību un novērst hibrīddraudus" [14],

– "Eiropas digitālās nākotnes veidošana" [15],

– par savienoto ierīču kiberdrošību [16],

– par ES kiberdrošības stratēģiju digitālajai desmitgadei [17],

– par drošību un aizsardzību [18],

– "Izpētīt kopējās kibervienības iniciatīvas potenciālu – papildināt koordinētu ES reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm" [19]

– Stratēģiskais kompass drošībai un aizsardzībai – Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību [20],

---

10 OV L 320, 17.12.2018., 28.–34. lpp.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. UZSVER, ka pēdējos gados ir pastiprinājusies gan valstisko, gan nevalstisko aktoru ļaunprātīga rīcība kibertelpā, tostarp strauji un pastāvīgi pieaug tādu ļaunprātīgu darbību skaits, kas vērstas pret ES un tās dalībvalstu kritisko infrastruktūru, piegādes ķēdēm un intelektuālo īpašumu, palielinās plašākas ietekmes risks, kā arī pieaug izspiedējprogrammatūru uzbrukumi mūsu uzņēmumiem, organizācijām un iedzīvotājiem. NORĀDA, ka, atgriežoties pie spēka politikas, dažas valstis arvien vairāk mēģina apstrīdēt un apdraudēt uz noteikumiem balstīto starptautisko kārtību kibertelpā, pārvēršot kibertelpu līdzās atklātai jūrai, gaisa telpai un kosmiskai telpai par arvien apstrīdētāku jomu. ATZĪST, ka liela mēroga kiberuzbrukumi vai mēģinājumi ielauzties tīklā un informācijas sistēmās, traucēt tiem vai iznīcināt tos, radot sistēmiskas sekas, ir kļuvuši izplatītāki, tie var apdraudēt mūsu ekonomisko drošību un ietekmēt mūsu demokrātiskās iestādes un procesus, kā arī liecina par dažu aktoru gatavību apdraudēt starptautisko drošību un stabilitāti. UZSVER, ka Krievijas militārā agresija pret Ukrainu ir parādījusi, ka ofensīvas kiberdarbības var tikt veiktas kā neatņemama daļa no hibrīdstratēģijām, kas apvieno iebiedēšanu, destabilizāciju un ekonomikas traucējumus.

2. ATKĀRTOTI NORĀDA, ka, saskaroties ar pašreizējām ģeopolitiskajām pārmaiņām, mūsu Savienības spēks ir vienotībā, solidaritātē un apņēmībā un ka Stratēģiskā kompasa īstenošana uzlabos ES stratēģisko autonomiju un tās spēju sadarboties ar partneriem, lai aizsargātu savas vērtības un intereses, tostarp kiberjomā. UZSVER, ka spēcīgāka un spējīgāka ES drošības un aizsardzības jomā dos pozitīvu ieguldījumu globālajā un transatlantiskajā drošībā un papildinās NATO, kas joprojām ir tās locekļu kolektīvās aizsardzības pamats. ATKĀRTOTI APSTIPRINA ES nodomu pastiprināt atbalstu starptautiskajai noteikumos balstītajai kārtībai, kuras centrā ir Apvienoto Nāciju Organizācija.

3. Saskaņā ar Padomes secinājumiem par ES kiberdrošības stratēģiju un Stratēģisko kompasu ATKĀRTOTI NORĀDA, ka ir jāizstrādā Savienības pozīcija kiberjautājumos, uzlabojot mūsu spēju novērst kiberuzbrukumus ar spēju veidošanas, spēju attīstības, apmācības, mācību, uzlabotas noturības starpniecību un ar stingru reakciju uz kiberuzbrukumiem ES un tās dalībvalstīm, izmantojot visus pieejamos ES instrumentus. Tas ietver arī turpmāku ES apņemšanos vērst tūlītēju un ilgtermiņa atbildes reakciju pret tiem apdraudējuma izraisītājiem, kuri mēģinās traucēt atvērtu un drošu pieeju kibertelpai un ietekmēt mūsu stratēģiskās intereses, tostarp mūsu partneru drošību. Šajā sakarā UZSVER, ka pozīcijas kiberjautājumos mērķis ir apvienot dažādas iniciatīvas, kas atbilst ES darbībām miera un stabilitātes konsolidācijai kibertelpā un atvērtas, brīvas, globālas, stabilas un drošas kibertelpas atbalstam, vienlaikus uzlabojot īstermiņa, vidēja termiņa un ilgtermiņa darbību koordināciju nolūkā novērst un nepieļaut kiberdraudus un kiberuzbrukumus, atturēt no tiem un reaģēt uz tiem, kā arī labāk izmantojot kiberspējas. UZSVER, ka šie elementi būtu jāiekļauj ES pozīcijā kiberjautājumos saskaņā ar piecām ES funkcijām kiberjomā: stiprināt mūsu kibernoturību un aizsardzības spējas; stiprināt solidāru un visaptverošu krīžu pārvarēšanu; popularizēt mūsu redzējumu par kibertelpu; uzlabot sadarbību ar partnervalstīm un starptautiskām organizācijām; novērst kiberuzbrukumus, aizstāvēties pret tiem un reaģēt uz tiem.

I. STIPRINĀT MŪSU KIBERNOTURĪBU UN AIZSARDZĪBAS SPĒJAS

4. ATKĀRTOTI UZSVER, ka ir jāpaaugstina ES kiberdrošības vispārējais līmenis, GAIDA, ka ātri tiks pieņemts projekts direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (TID), projekts regulai par finanšu sektora digitālās darbības noturību (*DORA*), projekts direktīvai par kritisko vienību noturību (*CER*) un PIEŅEM ZINĀŠANAI priekšlikumu regulai, ar ko nosaka augsta līmeņa kiberdrošības pasākumus Savienības iestādēs, struktūrās, birojos un aģentūrās, lai veicinātu tādu Eiropas Savienību, kas aizsargā savus iedzīvotājus, sabiedriskos pakalpojumus un uzņēmumus kibertelpā. MUDINA Komisiju pabeigt galveno priekšlikumu pieņemšanu ar mērķi nodrošināt digitālo infrastruktūru, tehnoloģiju, produktu un pakalpojumu drošību, lai raidītu skaidru signālu par ES vērienīgajiem mērķiem šajos jautājumos un varētu atbalstīt uzņēmumus šo izaicinājumu pārvarēšanā. AICINA Komisiju ierosināt kopīgas ES kiberdrošības prasības savienotām ierīcēm un ar tām saistītiem procesiem un pakalpojumiem, izmantojot Kibernoturības aktu, kas Komisijai būtu jāierosina līdz 2022. gada beigām, ņemot vērā nepieciešamību pēc horizontālas un holistiskas pieejas, kas aptver visu digitālo produktu aprites ciklu, kā arī spēkā esošo regulējumu, jo īpaši kiberdrošības jomā.

5. AICINA attiecīgās iestādes, piemēram, Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*), Eiropas Savienības Kiberdrošības aģentūru (*ENISA*) un Tīklu un informācijas drošības (TID) sadarbības grupu, kā arī Eiropas Komisiju, pamatojoties uz riska novērtējumu, formulēt ieteikumus dalībvalstīm un Eiropas Komisijai, lai stiprinātu sakaru tīklu un infrastruktūru noturību Eiropas Savienībā, tostarp turpinātu īstenot ES 5G rīkkopu.

6. AICINA ES un tās dalībvalstis pastiprināt centienus, lai paaugstinātu vispārējo kiberdrošības līmeni, piemēram, veicinot uzticamu kiberdrošības pakalpojumu sniedzēju darbības sākšanu, un UZSVER, ka šādu pakalpojumu sniedzēju darbības attīstības veicināšanai vajadzētu būt ES rūpniecības politikas prioritātei kiberdrošības jomā. Lai labāk pretotos kiberuzbrukumiem ar iespējamu sistēmisku ietekmi un tos novērstu un ņemot vērā pieredzi, kas gūta, risinot *Solarwinds*, *Microsoft Exchange* un *Apache Log4J* ievainojamības problēmas, AICINA Komisiju ierosināt iespējas, kā veicināt uzticamas kiberdrošības pakalpojumu nozares rašanos, stiprināt IKT piegādes ķēdes kiberdrošību, novērst programmatūras ievainojamības iespējamo ietekmi uz ES un tās dalībvalstīm, tostarp ņemot vērā gaidāmo Kibernoturības aktu, un uzlabot kiberdraudu atklāšanu un spēju kopīgošanu dalībvalstīs un starp tām.

7. ATKĀRTOTI APLIECINA, ka investīcijām inovācijā un civilo tehnoloģiju labākai izmantošanai ir būtiska nozīme, lai stiprinātu mūsu tehnoloģisko suverenitāti, tostarp kiberjomā, AICINA Komisiju ātri iedarbināt Eiropas Kiberdrošības kompetences centru nolūkā izveidot spēcīgu Eiropas pētniecības, rūpniecības un tehnoloģiju ekosistēmu kiberjomā, UZSVER, ka ir jāveicina pētniecība un inovācija, vairāk jāiegulda civilajā un aizsardzības jomā, lai stiprinātu ES aizsardzības tehnisko un rūpniecisko pamatu (*EDTIB*), un jāattīsta ES un tās dalībvalstu kiberspējas, tostarp stratēģiskā atbalsta spējas. UZSVER, ka ir svarīgi intensīvi izmantot jaunās tehnoloģijas, jo īpaši kvantisko datošanu, mākslīgo intelektu un lielos datus, lai gūtu salīdzinošas priekšrocības, tostarp attiecībā uz reaģēšanas operācijām uz kiberincidentiem.

8. ATZĪSTOT, ka mūsu kiberdrošības uzlabošana ir veids, kā palielināt mūsu centienu efektivitāti un drošību uz sauszemes, gaisā, jūrā un kosmosā, UZSVER, cik svarīgi ir kiberdrošības apsvērumus integrēt visās ES publiskās politikas jomās, tostarp nozaru tiesību aktos, kas papildina TID 2 direktīvu, un AICINA Komisiju izpētīt iespējas palielināt kiberdrošību visā ES aizsardzības tehniskā un rūpnieciskā pamata (*EDTIB*) piegādes ķēdē.

9. ATZĪST, ka pienācīgu finanšu resursu un cilvēkresursu nodrošināšana kiberdrošībai un pasākumi, kuru mērķis ir radīt labvēlīgu vidi privātā sektora konkurētspējai, ir būtiski, lai izstrādātu ES pozīciju kiberjautājumos, un ka jautājums par stabilu un ilgtermiņa finansējumu kiberdrošībai, tostarp augsti kvalificētu cilvēkresursu izmaksas, būtu jārisina arī ES līmenī, izstrādājot un īstenojot horizontālu mehānismu, kurā apvienoti vairāki finansējuma avoti. Tādēļ AICINA Komisiju līdz 2022. gada beigām izskatīt iespējas šādam mehānismam, kas jāapspriež attiecīgajās Padomes struktūrās.

10. UZSVER nepieciešamību stiprināt mūsu centienus un pastiprināt sadarbību cīņā pret starptautisko kibernoziedzību, jo īpaši izspiedējprogrammatūru, izmantojot *EMPACT* (Eiropas daudzdisciplīnu platformu pret noziedzības draudiem) mehānismu, apmainoties ar informāciju starp kiberdrošības, tiesībaizsardzības un diplomātiskajām nozarēm un stiprinot tiesībaizsardzības spējas kibernoziegumu izmeklēšanā un kriminālvajāšanā. ATKĀRTOTI pauž apņemšanos informēt sabiedrību par kiberdraudiem un valsts un ES līmenī veiktajiem pasākumiem pret šiem draudiem, iesaistot pilsonisko sabiedrību, privāto sektoru un akadēmiskās aprindas, lai palielinātu informētību un veicinātu pienācīgu kiberaizsardzības un kiberhigiēnas līmeni. UZSVER, ka galvenā uzmanība jāpievērš iedzīvotāju kiberdrošības prasmēm un spējām ES un dalībvalstu līmenī un ka lietotāji aktīvi jāiesaista viņu pašu aizsardzībā.

II. **STIPRINĀT SOLIDĀRU UN VISAPTVEROŠU KRĪŽU PĀRVARĒŠANU**

11. Pamatojoties uz ikgadējām kiberdrošības mācībām, citām mācībām, kas saistītas ar kiberdimensiju, un mācībām "*EU CyCLES* 2022", UZSVER, cik svarīgi ir izveidot regulāru starpkopienu un daudzlīmeņu kiberdrošības mācību programmu, lai pārbaudītu un pilnveidotu ES iekšējo un ārējo reakciju uz liela mēroga kiberdrošības incidentiem, piedaloties Padomei, EĀDD, Komisijai un attiecīgajām ieinteresētajām personām, piemēram, *ENISA* un privātajam sektoram, un kas atbildīs vispārējai ES mācību politikai un to veicinās. UZSVER, ka ir svarīgi turpināt attīstīt mācības "Kibereiropa" un "*BlueOLEx*", kas apvieno atbildes reakciju dažādos līmeņos. ATZĪST, ka ir jāizvērtē un jākonsolidē esošās mācības un jāizpēta turpmāku mācību iespējas konkrētos kiberjomas segmentos, jo īpaši *CERT* militāras mācības un mācības, kas vērstas uz ES iestāžu, struktūru un aģentūru sadarbību krīzes situācijās. ATZĪST, ka Savienības pozīcija kiberjautājumos stiprinās mūsu spēju novērst kiberuzbrukumus, izmantojot dažādas darbības, tostarp apmācību, un tāpēc AICINA dalībvalstis uzlabot civilmilitāro sadarbību kiberjomas apmācībā un kopīgās mācībās.

12. UZSVER, ka ir jāturpina pārbaudīt un stiprināt operatīvo sadarbību un kopīgu situācijas apzināšanos starp dalībvalstīm, tostarp izmantojot izveidotos tīklus, piemēram, *CSIRT* tīklu un Kiberkrīžu sadarbības organizāciju tīklu (*EU CyCLONe*), lai uzlabotu ES gatavību vērsties pret liela mēroga kiberdrošības incidentiem. UZSVER, cik svarīgi ir strādāt pie tā, lai starp dalībvalstīm un ES iestādēm, struktūrām, birojiem un aģentūrām izstrādātu kopīgu valodu, kas būtu pielāgota diskusijām politiskā līmenī, lai atbalstītu konsolidēta novērtējuma sagatavošanu par attiecīgo kiberincidentu smagumu un ietekmi, kā arī iespējamiem attīstības scenārijiem un attiecīgā gadījumā no tiem izrietošajām vajadzībām. UZSVER, ka šajā sakarā ir jāuzlabo kopīgo situācijas apzināšanās ziņojumu, tostarp Kiberkrīžu sadarbības organizāciju tīkla (*EU-CyCLONE*) ziņojumu par liela mēroga kiberdrošības incidentu ietekmi un smagumu ES dalībvalstīs un ES Izlūkošanas un situāciju centra (*EU INTCEN*) ES kiberdiplomātijas rīkkopas ietvaros sniegto draudu novērtējumu, papildināmība. Aicina Komisiju, Augsto pārstāvi un TID sadarbības grupu koordinācijā ar attiecīgajām civilajām un militārajām struktūrām un aģentūrām un izveidotajiem tīkliem, tostarp *ES CyCLONe*, līdz 2022. gada beigām veikt riska izvērtēšanu un izstrādāt riska scenārijus no kiberdrošības perspektīvas situācijā, kad pastāv apdraudējums vai iespējams uzbrukums dalībvalstīm vai partnervalstīm, un iesniegt tos attiecīgajām Padomes struktūrām. UZSVER, ka ir vajadzīga pienācīga un koordinēta sabiedrības informēšana par ES reakciju uz liela mēroga kiberdrošības incidentiem.

13. Liela mēroga kiberdrošības incidenta gadījumā – UZSVER, ka ir jāpastiprina koordinācija un attiecīgā gadījumā, balstoties uz panākto progresu un *PESCO* kiberdrošības ātrās reaģēšanas vienību paveikto darbu un izmantojot *CSIRT* tīkla un ES *CyCLONe* darbu, jāpastiprina mūsu reaģēšanas uz incidentiem spēju brīvprātīga apvienošana starp dalībvalstīm. ATZĪST, ka saikņu veidošana ar privāto sektoru varētu pastiprināt publiskās spējas, jo īpaši saistībā ar prasmju nepietiekamību visā ES, un ka šo privāto partneru apzināšanai un koordinēšanai varētu būt labvēlīga ietekme plaša mēroga incidentu gadījumā. Lai pilnībā sagatavotos plaša mēroga kiberdrošības incidentiem, AICINA Komisiju līdz 2022. gada 3. ceturkšņa beigām nākt klajā ar priekšlikumu par jaunu ārkārtas reaģēšanas fondu kiberdrošības jomā.

14. Saskaņā ar Stratēģisko kompasu ATKĀRTOTI UZSVER, ka ir jāiegulda mūsu savstarpējā palīdzībā saskaņā ar Līguma par Eiropas Savienību 42. panta 7. punktu, kā arī solidaritātē saskaņā ar Līguma par Eiropas Savienības darbību 222. pantu, jo īpaši ar biežām mācībām. Šajā sakarā UZSVER, ka ir jāturpina darbs pie divpusēja civila un/vai militāra atbalsta sniegšanas un koordinācijas, tostarp, izskatot iespējamu atbalstu, ko pēc dalībvalstu skaidra lūguma sniedz ES, un pie atbilstīgu reaģēšanas pasākumu apzināšanas, tostarp, izstrādājot koordinētu komunikācijas stratēģiju, saistībā ar 42. panta 7. punkta īstenošanu. ATZĪMĒ, ka tam būtu jāietver arī saikņu izpēte ar esošajiem ES krīžu pārvarēšanas mehānismiem un ES civilās aizsardzības mehānismu.

15. UZSVER, ka pastiprinātai ES pozīcijai kiberjautājumos būs vajadzīgi uzlaboti drošie sakari. Tālab ATKĀRTOTI UZSVER Stratēģiskajā kompasā šajā sakarā sniegtās ievirzes, un AICINA Komisiju un citas attiecīgās iestādes, struktūras un aģentūras līdz 2022. gada beigām veikt kartēšanu attiecībā uz esošajiem drošo sakaru rīkiem kiberjomā, kuri jāapspriež attiecīgajās Padomes struktūrās un ar attiecīgajām sadarbības grupām, piemēram, *CSIRT* tīklu un ES *CyCLONe*.

III. POPULARIZĒT MŪSU REDZĒJUMU PAR KIBERTELPU

16. ATGĀDINA, ka kopīgās un visaptverošās ES pieejas kiberdiplomātijai mērķis ir veicināt konfliktu novēršanu, kiberdraudu mazināšanu un lielāku stabilitāti starptautiskajās attiecībās. Šajā sakarā ATKĀRTOTI APSTIPRINA ES apņemšanos iestāties par starptautisku strīdu kibertelpā risināšanu miermīlīgā ceļā un starptautisko tiesību, tostarp starptautisko cilvēktiesību un starptautisko humanitāro tiesību, piemērošanu valstu darbībām kibertelpā. UZSVER ES un tās dalībvalstu apņemšanos rīkoties saskaņā ar brīvprātīgām, nesaistošām valstu atbildīgas rīcības kibertelpā normām, par kurām vienojušās visas ANO dalībvalstis. UZSVER, cik svarīga ir atvērta, brīva, globāla, stabila un droša kibertelpa, kurā pilnībā tiek piemērotas cilvēktiesības, pamatbrīvības un tiesiskums, lai atbalstītu mūsu brīvo un demokrātisko sabiedrību sociālo labklājību, ekonomisko izaugsmi, pārticību un integritāti, un ATKĀRTOTI APSTIPRINA ES un tās dalībvalstu apņemšanos turpināt popularizēt minētās vērtības un principus. Lai pilnveidotu kanālus konstruktīvam, vaļsirdīgam un atklātam dialogam ar svarīgākajām kibertelpā ieinteresētajām personām, UZSVER, cik svarīgi ir kiberjautājumus, tostarp ES kiberdiplomātijas rīkkopu, padarīt par neatņemamu daļu sarunās par pievienošanos Savienībai un ES stratēģiskajos un politiskajos dialogos gan ar starptautiskajiem partneriem, gan ar konkurentiem, un vienlaikus AICINA Augsto pārstāvi pārskatīt esošos divpusējos dialogus par kiberjautājumiem un vajadzības gadījumā ierosināt sākt līdzīgu sadarbību ar vēl citām valstīm vai attiecīgām starptautiskām organizācijām.

17. ATGĀDINA, cik svarīga ir daudzu ieinteresēto personu sadarbība, jo arī citas ieinteresētās personas ir atbildīgas par kiberdrošību, jo īpaši attiecībā uz starptautiskajos un reģionālajos forumos pieņemto ieteikumu un lēmumu īstenošanu. AICINA ES un tās dalībvalstis turpināt popularizēt mūsu kibertelpas un interneta modeli, kura pamatā ir daudzu ieinteresēto personu pieeja, un darīt to ar tādām iniciatīvām kā Parīzes aicinājums nodrošināt uzticēšanos un drošību kibertelpā un Deklarācija par interneta nākotni, uzsverot kopīgos ieguvumus, ko sniedz stabilitāte kibertelpā, un visā pasaulē palielinot informētību par briesmām, ko rada valsts centrisks un autoritārs interneta redzējums, un AICINA ES un tās dalībvalstis vēl vairāk stiprināt sadarbību ar daudzu ieinteresēto personu kopienu, tostarp, izmantojot attiecīgus projektus, piemēram, ES ārpolitikas instrumenta ES kiberdiplomātijas iniciatīvu.

18. APŅEMAS pastāvīgi iesaistīties attiecīgajās starptautiskajās organizācijās, jo īpaši ar ANO Pirmo un Trešo komiteju saistītajos procesos, vienlaikus uzsverot, ka kibertelpā un attiecībā uz to bez atrunām piemēro esošās starptautiskās tiesības. UZSVER, cik svarīgi ir turpināt centienus atbalstīt un veicināt ANO sistēmu attiecībā uz valstu atbildīgu rīcību, un UZSVER, ka ES un tās dalībvalstis aktīvi strādās pie tā, lai stiprinātu tā īstenošanu, tostarp, izveidojot Rīcības programmu valstu atbildīgas rīcības veicināšanai kibertelpā. UZSVER, ka ES un tās dalībvalstis aktīvi iesaistīsies sarunās par turpmāko ANO konvenciju, lai tā kalpotu par efektīvu tiesībaizsardzības un tiesu iestāžu instrumentu globālajā cīņā pret kibernoziedzību, pilnībā ņemot vērā šajā jomā esošo starptautisko un reģionālo instrumentu sistēmu, jo īpaši Budapeštas konvenciju par kibernoziegumiem. UZSVER, ka ir svarīgi turpināt atbalstīt uzticības veicināšanas pasākumu (UVP) izstrādi un ieviešanu reģionālā un starptautiskā līmenī un turpināt mudināt EDSO satvarā izmantot esošos UVP kiberjomā, tostarp starptautisku saspīlējumu laikā.

19. ATGĀDINA, ka proaktīvas, cilvēktiesībās balstītas pieejas īstenošana nolūkā nodrošināt starptautiskus standartus jauno tehnoloģiju un interneta pamata arhitektūras jomās saskaņā ar demokrātiskām vērtībām un principiem, ir būtiska, lai nodrošinātu, ka internets arvien ir globāls, nefragmentēts un atvērts, un ATBALSTA principu, saskaņā ar kuru tehnoloģiju izmantošanā un izstrādē tiek ievērotas cilvēktiesības, tās ir vērstas uz privātumu un to izmantošana ir likumīga, droša un ētiska. MUDINA Augsto pārstāvi un Komisiju izstrādāt stratēģisku redzējumu par tādiem tehniskiem jautājumiem digitālajā jomā, kas ietekmē ārpolitiku un varētu ietekmēt kibertelpas un jo īpaši interneta stabilitāti, tostarp attiecīgajās specializētajās starptautiskajās organizācijās (Starptautiskajā Telesakaru savienībā u. c.).

IV. UZLABOT SADARBĪBU AR PARTERVALSTĪM UN STARPTAUTISKĀM ORGANIZĀCIJĀM

20. UZSVER, ka ES kiberspēju veidošanas stratēģija ir labāk jāsasaista ar ANO normām par valstu atbildīgu rīcību kibertelpā, tostarp, izstrādājot pielāgotas sadarbības un spēju veidošanas programmas, lai atbalstītu trešās valstis to centienos tās īstenot, un tādējādi turpinot un paplašinot mūsu centienus veicināt ANO Rīcības programmu valstu atbildīgas rīcības veicināšanai kibertelpā. UZSVER, ka ir svarīgi kiberspēju veidošanu pilnībā integrēt kā daļu no piedāvājuma, ko sniedz ES kā drošības garants, pienācīgi koordinējot centienus starp dalībvalstīm un ES iestādēm, struktūrām un aģentūrām, un jo īpaši ATZINĪGI VĒRTĒ sadarbību starp dalībvalstīm, kā arī ar publiskā un privātā sektora partneriem, jo īpaši ar ES *CyberNet* (ES kiberspēju veidošanas tīkls) un Globālā kiberekspertīzes foruma (*GFCE*) starpniecību, lai nodrošinātu koordināciju un izvairītos no dublēšanās.

AICINA Augsto pārstāvi un Komisiju līdz 2022. gada 3. ceturksnim izveidot *Kiberspēju veidošanas valdi* un regulāri rīkot viedokļu apmaiņas Kiberjautājumu horizontālajā darba grupā. AICINA Komisiju un Augsto pārstāvi turpināt mobilizēt Kaimiņattiecību, attīstības sadarbības un starptautiskās sadarbības instrumentu (*NDICI*), Pirmspievienošanās palīdzības instrumentu (*IPA III*) un citus finanšu instrumentus, piemēram, Eiropas Miera mehānismu (*EPF*) un *Global Gateway* iniciatīvu, lai atbalstītu mūsu partneru noturības stiprināšanu, to spēju identificēt kiberdraudus un vērsties pret tiem un izmeklēt kibernoziegumus un saukt par tiem pie atbildības, un sadarbības projektu izstrādi, tostarp saistībā ar krīzi, jo īpaši MUDINA uz sadarbību ar partneriem Rietumbalkānos un ES austrumu un dienvidu kaimiņreģionā un ES un dalībvalstu ekspertu izvietošanu nolūkā sniegt atbalstu kiberkrīžu gadījumos, ņemot vērā esošās juridiskās pilnvaras.

21. UZSVER, ka ir jāpastiprina centieni izstrādāt strukturētu un atvērtu ES informēšanas pieeju attiecībā uz to, kā veicināt globālu vienotu izpratni par starptautisko tiesību piemērošanu kibertelpā, ANO sistēmu attiecībā uz valstu atbildīgu rīcību kibertelpā, tostarp iniciatīvu par Rīcības programmu valstu atbildīgas rīcības veicināšanai kibertelpā, kā arī attiecībā uz ES un tās dalībvalstu nostāju notiekošajās sarunās par ANO Konvenciju par kibernoziegumiem, un kā daļu no šiem centieniem LŪDZ Augsto pārstāvi līdz 2022. gada beigām iesniegt Padomei informēšanas plānu. MUDINA Augsto pārstāvi un Komisijas dienestus pilnībā un sistemātiski izmantot 145 delegācijas un izveidot regulāru, auglīgu sadarbību starp tām un dalībvalstu vēstniecībām trešās valstīs iecerētā ES Kiberdiplomātijas tīkla aizgādībā. AICINA Augsto pārstāvi līdz 2022. gada 3. ceturksnim izveidot ES Kiberdiplomātijas tīklu, veicinot informācijas apmaiņu, kopīgus apmācības pasākumus ES un dalībvalstu personālam, saskaņotus spēju veidošanas centienus un stiprinot ANO sistēmas attiecībā uz valstu atbildīgu rīcību kibertelpā īstenošanu, kā arī uzticības veicināšanas pasākumus starp valstīm.

22. UZSVER savu apņemšanos turpināt sadarboties ar starptautiskām organizācijām un partnervalstīm, lai veicinātu kopīgu izpratni par kiberapdraudējumu ainu, pilnveidotu sadarbības mehānismus un proaktīvi noteiktu uz sadarbību vērstu diplomātisko reakciju. ATGĀDINOT par galvenajiem sasniegumiem ES un NATO sadarbībā kiberdrošības jomā 2016. gada Varšavas un 2018. gada Briseles kopīgo deklarāciju īstenošanas satvarā, pilnībā ievērojot abu organizāciju lēmumu pieņemšanas autonomiju un procedūras un pamatojoties uz pārredzamības, savstarpīguma un iekļautības principiem, UZSVER, ka ir jāturpina attīstīt sadarbību kiberjomā ar NATO, izmantojot mācības, informācijas apmaiņu un viedokļu apmaiņas starp ekspertiem, tostarp par spēju attīstību, partneru spēju veidošanu un misijām un operācijām, kā arī par starptautisko tiesību un ANO normu par valstu atbildīgu rīcību kibertelpā piemērojamību un iespējamu koordinētu reaģēšanu uz ļaunprātīgām kiberdarbībām.

V. NOVĒRST KIBERUZBRUKUMUS, AIZSTĀVĒTIES PRET TIEM UN REAĢĒT UZ TIEM

23. ATZĪST, ka kibertelpa ir kļuvusi par ģeopolitiskas konkurences arēnu, un tādēļ ATKĀRTOTI UZSVER, ka ES ir jāspēj ātri un spēcīgi reaģēt uz kiberuzbrukumiem, piemēram, valsts atbalstītām ļaunprātīgām kiberdarbībām, kas mērķtiecīgi vērstas pret ES un tās dalībvalstīm, un tādēļ tai ir jāstiprina ES kiberdiplomātijas rīkkopa un pilnībā jāizmanto visi tās instrumenti, tostarp pieejamie politiskie, ekonomiskie, diplomātiskie, juridiskie un stratēģiskās komunikācijas rīki, lai novērstu un kavētu ļaunprātīgas kiberdarbības, atturētu no tām un reaģētu uz tām. UZSVER, ka naidīgiem aktoriem ir jāapzinās, ka kiberuzbrukumi dalībvalstīm un ES iestādēm tiks agrīni atklāti, nekavējoties identificēti un risināti ar visiem nepieciešamajiem rīkiem un politikām. Jo īpaši ņemot vērā pozīcijā kiberjautājumos ietvertos elementus un pieredzi, kas gūta no kiberdiplomātijas rīkkopas īstenošanas kopš tās darbības uzsākšanas un no ES *CyCLES* darbības, AICINA dalībvalstis un Augsto pārstāvi ar Komisijas atbalstu līdz 2023. gada 1. ceturkšņa beigām izstrādāt pārskatītu ES kiberdiplomātijas rīkkopas īstenošanas pamatnostādņu versiju, jo īpaši, izskatot papildu reaģēšanas pasākumus.

24. UZSVER, ka attiecīgajās Padomes struktūrās un komitejās ir regulāri jārīko viedokļu apmaiņas par kiberapdraudējumu ainu, vienlaikus arī regulāri iesaistot privāto sektoru un ņemot vērā neseno incidentu ietekmes un smaguma novērtējumu, lai palielinātu vispārējo informētību un gatavību ES kiberdiplomātijas rīkkopas turpmākiem lietojumiem un izstrādātu turpmākus rīkus tās īstenošanas atbalstam. Lai gan valsts drošība paliek vienīgi katras dalībvalsts atbildībā, ATZĪMĒ, ka ir jāstiprina izlūkdatu un informācijas apmaiņa un sadarbība starp dalībvalstīm, kā arī ar ES *INTCEN*, lai lēmumu pieņemšanas procesa sākumā varētu apmainīties ar izlūkdatiem, tostarp jautājumā par attiecināšanu, un tādējādi ļautu ātri un pamatoti reaģēt uz ļaunprātīgām kiberdarbībām, kas vērstas pret ES un tās partneriem. ATKĀRTOTI UZSVER, cik svarīgi ir stiprināt ES *INTCEN* spējas kiberjomā, balstoties uz dalībvalstu izlūkdienestu brīvprātīgu ieguldījumu un neskarot dalībvalstu kompetenci, un izskatīt priekšlikumu par dalībvalstu kiberizlūkošanas darba grupas iespējamo izveidi.

25. ATZĪSTOT, ka ES deklarācijas un ierobežojošie pasākumi, kas veikti ES kiberdiplomātijas rīkkopas ietvaros, ir devuši spēcīgu vēstījumu par to, ka ļaunprātīgas kiberdarbības, kas rada ārēju apdraudējumu ES, tās dalībvalstīm un partneriem, ir nepieņemamas, un tādējādi tie palīdz novērst un kavēt ļaunprātīgām kiberdarbības, atturēt no tām un reaģēt uz tām, ATKĀRTOTI APSTIPRINA savu apņemšanos izmantot šos pasākumus, lai atgādinātu par saistībām, kas ir attiecināmas uz kibertelpu saskaņā ar starptautiskajām tiesībām, tostarp ANO Statūtiem kopumā, un sekmēt ANO sistēmu attiecībā uz valstu atbildīgu rīcību kibertelpā, tostarp pienācīgas pārbaudes pienākumu visām valstīm, proti, apzināti neļaut savu teritoriju izmantot starptautiski nelikumīgām darbībām, kurās izmanto IKT, nolūkā turpināt pilnveidot un popularizēt ES kopīgo viedokli par starptautisko tiesību piemērošanu kibertelpā. Atzīmējot, ka atbilstīgi un ātri vēstījumi mazina eskalācijas riskus un var atturēt uzbrucējus, kas vēršas pret Eiropas interesēm, AICINA Augsto pārstāvi izstrādāt un iesniegt dalībvalstīm saskaņotu komunikācijas stratēģiju par ES kiberdiplomātijas rīkkopas izmantošanu.

26. MUDINA izstrādāt pakāpeniskas, mērķorientētas un ilgtspējīgas pieejas un reakcijas uz ļaunprātīgām kiberdarbībām, izmantojot plašo rīku klāstu, ko sniedz ES kiberdiplomātijas rīkkopa, tostarp ES kibersankciju režīms, un paredzot papildu pasākumus. UZSVER, ka ir jāpalielina iespēja, izskatot katru gadījumu atsevišķi, mobilizēt visus pieejamos iekšējos un ārējos rīkus, lai novērstu un kavētu kiberuzbrukumus, atturētu no tiem un reaģētu uz tiem, īstenojot tos ātrā, efektīvā, pakāpeniskā, mērķorientētā un ilgtspējīgā pieejā, kuras pamatā ir ilgtermiņa stratēģiska iesaiste. AICINA Augsto pārstāvi sadarbībā ar Komisiju visā spektrā apzināt iespējamas ES kopīgas reakcijas uz kiberuzbrukumiem, tostarp sankciju iespējas, lai vajadzības gadījumā tā būtu gatava ātri un efektīvi rīkoties, un līdz 2023. gada 1. ceturkšņa beigām tās iesniegt Padomei.

27. Atzīmējot, ka kiberaizsardzība galvenokārt ir valsts atbildība, MUDINA dalībvalstis turpināt attīstīt savas spējas veikt kiberaizsardzības operācijas, tostarp proaktīvus pasākumus, lai aizsargātu no kiberuzbrukumiem, atklātu tos, aizstāvētu pret tiem un atturētu no tiem un, iespējams, lai atbalstītu citas dalībvalstis un ES. Katra dalībvalsts tiek mudināta vajadzības gadījumā uzlabot savas spējas sniegt un saņemt palīdzību un atbalstu. UZSVER, ka šo spēju turpmākai attīstīšanai vajadzētu būt vienam no galvenajiem mērķiem gaidāmajā ES kiberaizsardzības politikā. ATZĪMĒ, ka ES kiberaizsardzības politikā būtu vairāk jāapsver, kāda var būt attiecīgo ES iestāžu un struktūru loma, lai saskaņā ar to attiecīgajām pilnvarām pastiprinātu sadarbību starp ES un dalībvalstu attiecīgajiem kiberaizsardzības aktoriem un attīstītu savas spējas. AICINA Augsto pārstāvi kopā ar Komisiju papildināt ES pozīcijas kiberjautājumos izstrādi, 2022. gadā nākot klajā ar vērienīgu priekšlikumu par ES kiberaizsardzības politiku, kas pavērs ceļu, lai Padome ES pozīciju kiberjautājumos turpmāk pilnveidotu.

28. UZSVER, ka ir jāpalielina sadarbspēja un informācijas apmaiņa, izmantojot sadarbību starp militārajām datorapdraudējumu reaģēšanas vienībām (*milCERT*). AICINA dalībvalstis, balstoties uz EAA darbu, izveidot *MilCERT* tīklu, lai pilnveidotu sadarbību un atvieglotu informācijas apmaiņu, kas arī palīdzētu sekmēt koordināciju ar citām kiberkopienām, kā arī militāro kiberkomandieru tīklu, lai stiprinātu stratēģisko sadarbību starp ES dalībvalstu kiberkomandām vai citām attiecīgām iestādēm. Šo tīklu izveide kopā ar *PESCO* kiberjomas projektiem veicinātu spēcīgāku kiberaizsardzību ES līmenī. Uzsver, cik svarīga ir ierosinātā *milCERT* tīkla sadarbība ar jau esošo civilo (*CSIRT*) tīklu, lai uzlabotu informācijas apmaiņu un situācijas apzināšanos.

29. Pamatojoties uz ES Militāro redzējumu un stratēģiju par kibertelpu kā operāciju jomu un ņemot vērā to, ka pašlaik tiek izstrādāta militārā Kiberaizsardzības koncepcija attiecībā uz ES vadītām militāram operācijām, ATKĀRTOTI UZSVER, ka kiberdimensija ir jāintegrē KDAP misiju un operāciju plānošanā un īstenošanā, tostarp, uzlabojot to kiberspējas, un UZSVER, ka tas palīdzēs uzlabot situācijas apzināšanos kiberjomā ES līmenī.

30. Noslēgumā ATZĪMĒ, ka pozīcija kiberjautājumos būs solis uz priekšu, lai izveidotu ES doktrīnu rīcībai kibertelpā, pamatojoties uz uzlabotu noturību, spējām un reaģēšanas iespējām, kā arī kopīgu nostāju attiecībā uz starptautisko tiesību piemērošanu kibertelpā. Padome 2023. gadā IZVĒRTĒS progresu, kas panākts šo secinājumu īstenošanā, lai nodrošinātu ES pozīcijas kiberjautājumos turpmāku attīstību.