Eiropas Savienības
Padome

Briselē, 2021. gada 9. martā
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

"I/A" PUNKTA PIEZĪME

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	Pastāvīgo pārstāvju komiteja / Padome
Temats:	Projekts – Padomes secinājumi par ES kiberdrošības stratēģiju digitālajai desmitgadei

1. Komisija un Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos 2020. gada 16. decembrī publicēja kopīgu paziņojumu Eiropas Parlamentam un Padomei "ES kiberdrošības stratēģija digitālajai desmitgadei" [1]. Jaunās kiberdrošības stratēģijas mērķis ir uzlabot Eiropas kolektīvo noturību pret kiberdraudiem un nodrošināt, ka visi iedzīvotāji un uzņēmumi var pilnībā izmantot priekšrocības, ko dod uzticami pakalpojumi un digitālie rīki, uz kuriem var paļauties.

[1] 14133/20.

2. Komisija un EĀDD ar kopīgu paziņojumu nāca klajā Kiberjautājumu horizontālās darba grupas (*HWPCI*) neformālajā videokonferencē 2020. gada 17. decembrī un 2021. gada 12. janvārī. *HWPCI* neformālajā videokonferencē 2020. gada 17. decembrī nākamā prezidentvalsts Portugāle paziņoja par nodomu sagatavot projektu Padomes secinājumiem par ES kiberdrošības stratēģiju digitālajai desmitgadei.

3. Padomes secinājumu pirmo projektu prezidentvalsts iesniedza *HWPCI* neformālajā videokonferencē 2021. gada 2. februārī. Šos secinājumus pēc tam apsprieda *HWPCI* neformālajās sanāksmēs, kas videokonferences veidā notika 2021. gada 9. februārī, 19. februārī, kā arī 1. un 9. martā.

4. Tā kā secinājumu projektā ir ietverta arī atsauce uz ES aizsardzības politiku (30. punkts), attiecīgo punktu 2021. gada 10. februāra sanāksmē apsprieda Politisku un militāru jautājumu grupa (*PMG*).

5. Vairāki punkti attiecas uz kopējo ārpolitiku un drošības politiku (1., 4., 7., 8., 9., 20., 23., 24., 26., 27., 28., 29., 30., 31., 32. un 33. punkts), un tāpēc tie tika iesniegti Politikas un drošības komitejai, kura šos punktus apstiprināja 2021. gada 4. marta sanāksmē.

6. Neformālajā videokonferencē 2021. gada 9. martā *HWPCI* panāca vienošanos par Padomes secinājumu projektu, kas izklāstīts dokumentā 6722/21.

7. Ņemot vērā minēto, Pastāvīgo pārstāvju komiteja tiek aicināta iesniegt Padomei pielikumā izklāstīto Padomes secinājumu projektu un ierosināt Padomei secinājumu projektu pieņemt kā darba kārtības "A" punktu.

PIELIKUMS

Projekts – Padomes secinājumi par ES kiberdrošības stratēģiju digitālajai desmitgadei

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" [2],

– par interneta pārvaldību [3],

– par 2017. gada 20. novembra kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" [4],

– par kiberdrošības spēju un spēju veidošanu ES [5],

– par 5G nozīmi Eiropas ekonomikā un nepieciešamību mazināt ar 5G saistītos drošības riskus [6],

– par augsti digitalizētas Eiropas nākotni pēc 2020. gada: "Visas Savienības digitālās un ekonomiskās konkurētspējas un digitālās kohēzijas stiprināšana" [7],

– "Papildu centieni uzlabot noturību un novērst hibrīddraudus" [8],

– "Eiropas digitālās nākotnes veidošana" [9],

---

2 12109/13.
3 16200/14.
4 14435/17 + COR 1.
5 7737/19.
6 14517/19.
7 9596/19.
8 14972/19.
9 8711/20.

– par digitālo diplomātiju [10],

– par noturības stiprināšanu un hibrīddraudu, tostarp dezinformācijas, apkarošanu saistībā ar Covid-19 pandēmiju [11],

– par kiberdiplomātiju [12],

– par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm [13],

– par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums") [14],

– par ES ārējo kiberspēju veidošanas pamatnostādnēm [15],

– "Atveseļošana, kas sekmē pārkārtošanos uz dinamiskāku, noturīgāku un konkurētspējīgāku Eiropas rūpniecību" [16],

– par savienoto ierīču kiberdrošību [17],

– "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" [18],

– un Padomes rezolūcija par šifrēšanu – Drošība, izmantojot šifrēšanu, un drošība, neraugoties uz šifrēšanu [19],

---

10 12804/20.
11 14064/20.
12 6122/15 + COR 1.
13 10086/18.
14 10474/17.
15 10496/18.
16 13004/20.
17 13629/20.
18 14540/16.
19 13084/1/20 REV 1.

– un dalībvalstu 2020. gada 15. oktobra deklarāciju "Veidojot nākamās paaudzes mākoni uzņēmumiem un publiskajam sektoram Eiropas Savienībā",

ATGĀDINOT Eiropadomes 2020. gada 1. un 2. oktobra secinājumus par Covid-19, vienoto tirgu, rūpniecības politiku, digitālo dimensiju un ārējām attiecībām [20] un 2019. gada 20. jūnija secinājumus par dezinformāciju un hibrīddraudiem un jaunu stratēģisko programmu 2019.–2024. gadam [21],

ATGĀDINOT 2016. gada 28. jūnija Globālo Eiropas Savienības ārpolitikas un drošības politikas stratēģiju "Kopīgs redzējums, kopīga rīcība – stiprāka Eiropa",

ATGĀDINOT Eiropas Komisijas 2020. gada 19. decembra paziņojumu par Eiropas digitālās nākotnes veidošanu [22] un 2020. gada 24. jūlija paziņojumu par ES Drošības savienības stratēģiju [23],

ATGĀDINOT Eiropas Komisijas un Augstā pārstāvja 2020. gada 2. decembra kopīgo paziņojumu "Jauna ES un ASV programma globālām pārmaiņām" [24],

1. UZSVER, ka kiberdrošība ir būtiska, lai veidotu noturīgu, zaļu un digitālu Eiropu, un ATZINĪGI VĒRTĒ kopīgo paziņojumu Eiropas Parlamentam un Padomei "ES kiberdrošības stratēģija digitālajai desmitgadei", kurā izklāstīts jaunais satvars ES rīcībai "noturības, tehnoloģiskās suverenitātes un līderības" jomā, kā arī tas, kā aizsargāt savus iedzīvotājus, uzņēmumus un iestādes pret kiberincidentiem un apdraudējumiem, vienlaikus uzlabojot personu un organizāciju uzticēšanos ES spējai veicināt drošu un uzticamu tīklu un informācijas sistēmas, infrastruktūru un savienojamību un sekmēt un aizsargāt globālu, atvērtu, brīvu, stabilu un drošu kibertelpu, kuras pamatā ir cilvēktiesības, pamatbrīvības, demokrātija un tiesiskums;

---

20 EUCO 13/20.
21 EUCO 9/19.
22 19.2.2020., COM(2020) 67 final.
23 24.7.2020., COM(2020) 605 final.
24 2.12.2020., JOIN(2020) 22 final.

2. ATZĪST, ka līdz ar Covid-19 pandēmiju mūsu ikdienas dzīves priekšplānā aizvien vairāk ir izvirzījusies nepieciešamība panākt uzticēšanos informācijas un komunikācijas tehnoloģiju (IKT) rīkiem un sistēmām un to drošību; UZSVER, ka kiberdrošība un globāls un atvērts internets ir ļoti svarīgi valsts pārvaldes un iestāžu darbībai gan valstu, gan ES līmenī, kā arī mūsu sabiedrībai un ekonomikai kopumā;

3. UZSVER, ka politisku un stratēģisku lēmumu pieņemšanas līmenī ir jāpalielina informētība par kiberjautājumiem, nodrošinot lēmumu pieņēmējiem attiecīgas zināšanas un informāciju, un AKCENTĒ to, ka ir jāuzlabo plašas sabiedrības informētība un jāveicina kiberhigiēna;

4. AICINA veicināt un aizsargāt tādas ES pamatvērtības kā demokrātija, tiesiskums, cilvēktiesības un pamatbrīvības, tostarp tiesības uz vārda un informācijas brīvību, tiesības uz pulcēšanās un biedrošanās brīvību un tiesības uz privātumu kibertelpā; šajā sakarībā ATZINĪGI VĒRTĒ turpmākus pastāvīgus centienus aizsargāt cilvēktiesību aizstāvjus, pilsonisko sabiedrību un akadēmiskās aprindas, kas strādā pie tādiem jautājumiem kā kiberdrošība, datu privātums, novērošana un cenzūra tiešsaistē; tas jāpanāk, sniedzot turpmākus praktiskus norādījumus, veicinot paraugpraksi un pastiprinot ES centienus novērst cilvēktiesību pārkāpumus un aizskārumus un jauno tehnoloģiju ļaunprātīgu izmantošanu, jo īpaši vajadzības gadījumā izmantojot diplomātiskus pasākumus, kā arī šādu tehnoloģiju eksporta kontroli; šajā kontekstā UZSVER, cik svarīgs ir ES Rīcības plāns cilvēktiesību un demokrātijas jomā 2020.–2024. gadam un ES cilvēktiesību pamatnostādnes par vārda brīvību tiešsaistē un bezsaistē;

5. ĪPAŠI NORĀDA, ka viens no Savienības galvenajiem mērķiem ir panākt stratēģisku autonomiju un vienlaikus saglabāt atvērtu ekonomiku, lai tā pati varētu noteikt savas ekonomikas virzību un intereses. Tas nozīmē, ka nolūkā nostiprināt ES digitālo līderību un stratēģiskās spējas jāstiprina arī spēja izdarīt autonomas izvēles kiberdrošības jomā; ATGĀDINA, ka tas ietver stratēģisko atkarību apzināšanu un mazināšanu un noturības palielināšanu vissensitīvākajās rūpnieciskajās ekosistēmās un konkrētās teritorijās; UZSVER, ka tas var ietvert ražošanas un piegādes ķēžu dažādošanu, ražošanas un investīciju sekmēšanu un piesaisti Eiropā, alternatīvu risinājumu un aprites modeļu izpēti un plašas rūpnieciskās sadarbības veicināšanu visās dalībvalstīs;

6. paturot prātā to, ka darbaspēkam trūkst digitālo un kiberdrošības prasmju, UZSVER, cik svarīgi – nolūkā spēt digitalizēt mūsu sabiedrību kiberdrošā veidā – ir apmierināt pieprasījumu pēc apmācīta darbaspēka digitālās drošības un kiberdrošības jomā, jo īpaši attīstot, noturot un piesaistot labākos talantus, piemēram, izmantojot izglītību un apmācību; MUDINA panākt sieviešu un meiteņu plašāku dalību zinātnes, tehnoloģijas, inženierzinātņu un matemātikas (*STEM*) izglītībā, kā arī IKT darbvietu prasmju pilnveidē un pārkvalifikācijā digitālo prasmju kontekstā, kas ir viens no veidiem, kā pārvarēt digitālo plaisu starp dzimumiem;

7. ATGĀDINA, ka kopīgās un visaptverošās ES pieejas kiberdiplomātijai mērķis ir veicināt konfliktu novēršanu, kiberdraudu mazināšanu un lielāku stabilitāti starptautiskajās attiecībās; šajā kontekstā ATKĀRTOTI APSTIPRINA savu apņemšanos starptautiskus strīdus kibertelpā risināt miermīlīgā ceļā un to, ka visiem ES diplomātiskajiem centieniem prioritārā kārtā vajadzētu būt vērstiem uz drošības un stabilitātes veicināšanu kibertelpā, pastiprinot starptautisko sadarbību, un uz to, lai samazinātu nepareizu priekšstatu, eskalācijas un konfliktu risku, ko var izraisīt IKT incidenti, un ATBALSTA uzticības veicināšanas pasākumu (UVP) turpmāku izstrādi un ieviešanu reģionālā un starptautiskā līmenī; ATKĀRTOTI NORĀDA uz Apvienoto Nāciju Organizācijas Ģenerālās asamblejas vienprātīgi apstiprināto aicinājumu ANO dalībvalstīm IKT izmantošanā ņemt vērā *UNGGE* ziņojumos paustos ieteikumus, un ATKĀRTOTI APSTIPRINA nepieciešamību kibertelpā piemērot starptautiskās tiesības, jo īpaši ANO Statūtus kopumā;

8. ATKĀRTOTI APSTIPRINA: lai visaptveroši veidotu starptautiskās normas un standartus jauno tehnoloģiju un tehniskās un loģiskās infrastruktūras jomā, kas ir būtiska interneta publiskā kodola vispārējai pieejamībai un integritātei, un lai tie atbilstu vispārējām un ES vērtībām un tiktu izmantota daudzu ieinteresēto personu pieeja, ir ļoti svarīgi Savienībā pilnveidot normu un standartu izstrādi. Tādējādi tiks nodrošināts, ka internets arī turpmāk būs globāls, atvērts, brīvs, stabils un drošs un ka digitālo tehnoloģiju izmantošanā un izstrādē tiek ievērotas cilvēktiesības, un ka to izmantošana ir likumīga, droša un ētiska; PIEŅEM ZINĀŠANAI gaidāmo standartizācijas stratēģiju un APŅEMAS īstenot proaktīvus un koordinētus informēšanas pasākumus nolūkā veicināt ES līderību un ES mērķus starptautiskā līmenī, tostarp dažādās starptautiskās standartizācijas struktūrās un sadarbojoties ar līdzīgi domājošiem partneriem, pilsonisko sabiedrību, akadēmiskajām aprindām un privāto sektoru;

9. STINGRI ATBALSTA daudzu ieinteresēto personu modeli interneta pārvaldības un kiberdrošības jomā un apņemas starptautiskos forumos stiprināt regulāru un strukturētu informācijas apmaiņu ar ieinteresētajām personām, tostarp privāto sektoru, akadēmiskajām aprindām un pilsonisko sabiedrību, arī Parīzes aicinājuma nodrošināt uzticēšanos un drošību kibertelpā kontekstā; SEKMĒ vispārēju, cenas ziņā pieejamu un vienlīdzīgu piekļuvi internetam, kas novērstu digitālās plaisas, un jo īpaši iespēju veicināšanu sievietēm un meitenēm un personām, kas ir neaizsargātas vai atrodas nelabvēlīgos apstākļos, gan attiecībā uz politikas izstrādi, gan interneta izmantošanu;

10. UZSVER, ka turpmākajos gados kiberdrošība ir jāiekļauj digitālās jomas investīcijās un iniciatīvās un ka ir pakāpeniski jāveicina vienlīdzīgi konkurences apstākļi kiberdrošības kontekstā, un NORĀDA uz Komisijas plānu kiberdrošības jomā palielināt publiskos izdevumus un piesaistīt privātās investīcijas; UZSVER mazo un vidējo uzņēmumu (MVU) nozīmi kiberdrošības ekosistēmā un ATZĪST attiecīgos finanšu instrumentus, kas pieejami, lai atbalstītu spēcīgu uzsvaru uz kiberdrošību digitālajā pārveidē 2021.–2027. gada daudzgadu finanšu shēmas (DFS) darbības laikā, kā arī Atveseļošanas un noturības mehānismā (ANM);

11. SAGAIDA Regulas par Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (*CCCN*) drīzu īstenošanu, tostarp Eiropas Kiberdrošības kompetenču centra ātru izveidi un darbības uzsākšanu Bukarestē. Tā darba kārtības ātra pieņemšana palīdzēs maksimāli palielināt investīciju ietekmi, lai stiprinātu Savienības līderību un stratēģisko autonomiju kiberdrošības jomā un atbalstītu tehnoloģiskās spējas un prasmes, un palielinātu Savienības globālo konkurētspēju, izmantojot rūpniecības un akadēmisko kopienu ieguldījumu kiberdrošībā, tostarp MVU un pētniecības centru ieguldījumu, kuri gūs labumu no sistemātiskākas, iekļaujošākas un stratēģiskākas sadarbības, ņemot vērā Savienības un visu tās dalībvalstu kohēziju;

12. ATZINĪGI VĒRTĒ *ENISA* kopā ar dalībvalstīm un ieinteresētajām personām vadīto darbu, kura mērķis ir nodrošināt ES ar IKT produktu, pakalpojumu un procesu sertifikācijas shēmām, kam būtu jāpalīdz paaugstināt vispārējo kiberdrošības līmeni digitālajā vienotajā tirgū; šajā kontekstā AR NEPACIETĪBU GAIDA Savienības mainīgo darba programmu (SMDP), lai varētu izstrādāt ES kiberdrošības sertifikācijas shēmas Kiberdrošības akta (KDA) satvarā. Šajā kontekstā ATZĪST, ka ES ir būtiska nozīme tādu standartu izstrādē, kas var veidot kiberdrošības apdraudējuma ainu un kas palīdz nodrošināt godīgu konkurenci ES un pasaules mērogā, veicinot piekļuvi tirgum, kā arī pievēršoties drošības riskiem un vienlaikus nodrošinot ES tiesiskā regulējuma piemērojamību;

13. ATKĀRTOTI NORĀDA, ka ir svarīgi izvērtēt vajadzību pēc horizontāla tiesību akta, kurā arī precizē nepieciešamos nosacījumus laišanai tirgū, ilgtermiņā, lai pievērstos visiem attiecīgajiem savienoto ierīču kiberdrošības aspektiem, piemēram, pieejamībai, integritātei un konfidencialitātei; šajā sakarā ATZINĪGI VĒRTĒ diskusiju, kuras mērķis ir izpētīt šāda tiesību akta darbības jomu un tā saiknes ar kiberdrošības sertifikācijas satvaru, kā noteikts KDA, ar mērķi paaugstināt drošības līmeni digitālajā vienotajā tirgū; UZSVER – lai izvairītos no neskaidrības un tiesību aktu sadrumstalotības, kiberdrošības prasības būtu jādefinē saskaņā ar attiecīgajiem Savienības tiesību aktiem, tostarp KDA, jauno tiesisko regulējumu (JTR), Regulu par Eiropas standartizāciju un iespējamu turpmāko horizontālo tiesību aktu;

14. ATZĪST, ka svarīga ir visaptveroša un horizontāla pieeja kiberdrošībai Savienībā un ka vienlaikus ir svarīgi pilnībā ievērot dalībvalstu kompetenci un vajadzības, kā arī pastāvīgi atbalstīt tehnisko palīdzību un sadarbību nolūkā veidot dalībvalstu spējas; ņemot vērā kiberapdraudējuma ainas attīstību, PIEŅEM ZINĀŠANAI jauno priekšlikumu Direktīvai, ar ko paredz pasākumus nolūkā visā Savienībā panākt vienādi augsta līmeņa kiberdrošību, kuras pamatā uz TID direktīva, un atkārtoti pauž atbalstu valstu kiberdrošības satvaru stiprināšanai un saskaņošanai un noturīgai sadarbībai starp dalībvalstīm; turklāt UZSVER, ka šajā jomā ir jāsaskaņo un skaidri jāformulē nozaru tiesību akti;

15. PIEŅEM ZINĀŠANAI Komisijas priekšlikumu atbalstīt dalībvalstis drošības operāciju centru izveidē un stiprināšanā, lai visā ES varētu izveidot drošības operāciju centru tīklu, turpināt pārraudzību un prognozēt signālus par uzbrukumiem tīkliem; šajā kontekstā GAIDA Komisijas sīki izstrādātos plānus attiecībā uz drošības operāciju centru tīklu un vienlaikus sagaida, ka tiks ievērota dalībvalstu kompetence; ATGĀDINA par dalībvalstu centieniem ar ES atbalstu izveidot nozaru, valstu un reģionu datordrošības incidentu reaģēšanas vienības un valstu vai Eiropas informācijas apmaiņas un analīzes centrus, kas būtu daļa no efektīva kiberdrošības partnerību tīkla Savienībā; AR NEPACIETĪBU GAIDA iespēju noskaidrot šā tīkla potenciālu stiprināt drošības operāciju centrus, kā arī to papildināmību un koordināciju ar esošajiem tīkliem un dalībniekiem (jo īpaši datordrošības incidentu reaģēšanas vienību tīklu), lai veicinātu efektīvu, drošu un uzticamu informācijas apmaiņas kultūru; UZSVER, ka šā procesa pamatā būs darbs, kas veikts saistībā ar mākslīgā intelekta un augstas veiktspējas datošanas iniciatīvām un ko veic Eiropas digitālās inovācijas centri;

16. ŅEM VĒRĀ tādas drošas savienojamības sistēmas iespējamo izstrādi, kuras pamatā būtu Eiropas kvantu sakaru infrastruktūra (*EuroQCI*) un Eiropas Savienības valdības satelītsakari (*GOVSATCOM*), un ATZĪST, ka jebkādai iespējamai turpmākai attīstībai vajadzētu būt balstītai uz stabilu kiberdrošības satvaru un tajā būtu jāņem vērā visa elektronisko sakaru infrastruktūra, piemēram, kosmosa, zemes un zemūdens tīklu sistēmas;

17. AR NEPACIETĪBU GAIDA diskusijas ar Komisiju, *ENISA*, diviem ES DNS saknes serveru operatoriem un daudzu ieinteresēto personu kopienu, lai novērtētu abu ES DNS saknes serveru operatoru lomu attiecībā uz to, ka tiek garantēts, ka arī turpmāk ir pieejams internets, kas nav fragmentēts; ATZINĪGI VĒRTĒ turpmākas diskusijas par Komisijas nodomu izstrādāt tādu alternatīvu Eiropas pakalpojumu piekļuvei globālajam internetam (iniciatīva *"DNS4EU"*), kura pamatā būtu pārredzams modelis, kas atbilstu jaunākajiem standartiem un noteikumiem attiecībā uz drošību, datu aizsardzību un privātumu (integrētu aizsardzību un aizsardzību pēc noklusējuma), lai veicinātu lielāku noturību, vienlaikus saglabājot un uzlabojot starptautisko savienojamību visās dalībvalstīs;

18. ATZĪST, ka Komisijai un dalībvalstīm jāīsteno kopīgi centieni, lai paātrinātu svarīgu interneta standartu, tostarp IPv6, un plaši atzītu interneta drošības standartu apgūšanu, jo tie ir būtiski, lai palielinātu globālā interneta vispārējo drošības, noturības, atvērtības un sadarbspējas līmeni, vienlaikus palielinot ES rūpniecības un jo īpaši interneta infrastruktūras operatoru konkurētspēju;

19. UZSVER, cik svarīga ir koordinēta pieeja, kā arī efektīvu pasākumu izstrāde un īstenošana valsts līmenī, lai stiprinātu 5G tīklu kiberdrošību; ATBALSTA nākamos soļus, kas jāveic 5G tīklu kiberdrošības jomā, kā izklāstīts ES kiberdrošības stratēģijas pielikumā un kā pamatā ir rezultāti, kas izriet no ziņojuma par Komisijas ieteikuma ietekmi uz 5G tīklu drošību, piemēram, saistībā ar ilgtermiņa un visaptverošas pieejas noteikšanu attiecībā uz visu 5G vērtības ķēdi un ekosistēmu; lai vēl vairāk stiprinātu koordinēto pieeju 5G tīklu drošībai, MUDINA dalībvalstis, ES iestādes un citas attiecīgās ieinteresētās personas turpināt periodisko novērtēšanu, kā arī informācijas un paraugprakses apmaiņu īpašajā TID sadarbības grupas darbplūsmā par 5G kiberdrošību un regulāri ziņot Padomei par gūtajiem panākumiem; UZSVER – vienlaikus akcentējot dalībvalstu atbildību par nacionālās drošības aizsardzību – savu stingro apņemšanos piemērot un ātri pabeigt ES 5G rīkkopas pasākumu īstenošanu un turpināt centienus garantēt 5G tīklu drošību un nākamo paaudžu tīklu attīstību. Ciešā sadarbība starp dalībvalstīm, Komisiju un *ENISA* 5G tīklu drošības jomā varētu kalpot par piemēru sadarbībai citos jautājumos kiberdrošības jomā, vienlaikus ievērojot dalībvalstu kompetences un subsidiaritātes un proporcionalitātes principus;

20. ATZĪST, ka ir svarīgi turpināt kiberdrošību integrēt ES mehānismos reaģēšanai krīzes situācijās un testēt tos attiecīgās mācībās, un UZSVER, cik svarīgi ir uzlabot sadarbību un informācijas apmaiņu starp dažādajām kiberkopienām ES un sasaistīt jau esošās iniciatīvas, struktūras un procedūras (piemēram, *IPCR*, *CSIRT* tīklu, TID sadarbības grupu, *CyCLONe*, Eiropas Kibernoziedzības apkarošanas centru, ES *INTCEN* un citas attiecīgas ES struktūras) liela mēroga un pārrobežu kiberincidentu un apdraudējumu gadījumā; ŅEMOT VĒRĀ šajā jomā jau panākto progresu, GAIDA Komisijas priekšlikumu par procesu, starpposma mērķrādītājiem un grafiku kopējās kibervienības (KKV) definēšanai nolūkā nodrošināt pievienoto vērtību, skaidras prioritātes un racionalizēt ES kiberdrošības krīžu pārvarēšanas satvaru, tostarp, nodrošinot sagatavotību, kopīgu situācijas apzināšanos, pastiprinātu koordinētu reakciju un mācības, ko paveic pārredzami un pakāpeniski, vienlaikus izvairoties no dublēšanās un pārklāšanās un ievērojot dalībvalstu kompetenci;

21. UZSVER gan to, cik svarīgi ir veicināt sadarbību un informācijas apmaiņu starp attiecīgajiem kiberdrošības dalībniekiem un kompetentajām iestādēm drošības un krimināljustīcijas jomā, piemēram, tiesībaizsardzības un tiesu iestādēm, gan to, ka ir nepieciešams paplašināt un uzlabot šo iestāžu spējas izmeklēt kibernoziegumus un saukt pie atbildības par tiem un veicināt starptautiskas sarunas un ES noteikumus par pārrobežu piekļuvi elektroniskiem pierādījumiem. Neatkarīgi no mūsdienu tehnoloģiskās vides ir būtiski drošības un krimināljustīcijas jomā saglabāt kompetento iestāžu pilnvaras, lai tās, izmantojot likumīgu piekļuvi, varētu veikt savus uzdevumus, kā noteikts un atļauts tiesību aktos. Šādos tiesību aktos, kuros paredzētas izpildes pilnvaras, vienmēr ir pilnībā jāievēro pienācīgs process un citi aizsardzības pasākumi, kā arī pamattiesības, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību un tiesības uz personas datu aizsardzību;

22. ATKĀRTOTI APSTIPRINA atbalstu spēcīgas šifrēšanas izstrādei, īstenošanai un izmantošanai, kas ir nepieciešams līdzeklis, lai aizsargātu pamattiesības un personu, valdību, industrijas un sabiedrības digitālo drošību, un vienlaikus ATZĪST, ka ir jānodrošina drošības un krimināljustīcijas jomā kompetento iestāžu, piemēram, tiesībaizsardzības un tiesu iestāžu, spējas īstenot savas likumīgās pilnvaras gan tiešsaistē, gan bezsaistē, lai tās varētu aizsargātu mūsu sabiedrību un iedzīvotājus. Kompetentajām iestādēm ir jāspēj likumīgi un mērķtiecīgi piekļūt datiem, pilnībā ievērojot pamattiesības un attiecīgos datu aizsardzības tiesību aktus un vienlaikus atbalstot kiberdrošību; UZSVER, ka visās veiktajās darbībās šīm interesēm jābūt rūpīgi līdzsvarotām ar nepieciešamības, proporcionalitātes un subsidiaritātes principiem;

23. ATBALSTA un SEKMĒ Budapeštas Konvenciju par kibernoziegumiem un darbu, kas turpinās pie minētās konvencijas otrā papildprotokola; turklāt turpina iesaistīties daudzpusējā viedokļu apmaiņā par kibernoziedzību, tostarp procesos, kas saistīti ar Eiropas Padomi, Apvienoto Nāciju Organizācijas Narkotiku un noziedzības novēršanas biroju (*UNODC*) un Noziedzības novēršanas un krimināl̄ās tiesvedības komisiju (*CCPCJ*), lai nodrošinātu pastiprinātu starptautisko sadarbību cīņā pret kibernoziedzību, tostarp nodrošinātu paraugprakses un tehnisko zināšanu apmaiņu, un atbalstītu spēju veidošanu, vienlaikus ievērojot, veicinot un aizsargājot cilvēktiesības un pamatbrīvības;

24. lai arī par nacionālo drošību joprojām atbildīga ir tikai attiecīgā dalībvalsts, ATZĪST, cik svarīga ir izlūkdienestu stratēģiska sadarbība attiecībā uz kiberdraudiem un kiberdarbībām, un AICINA dalībvalstis ar savu kompetento iestāžu starpniecību turpināt sniegt ieguldījumu ES *INTCEN* darbā, kas ir centrs situācijas apzināšanai un draudu izvērtēšanai kiberjautājumu kontekstā ES, un izskatīt priekšlikumu par dalībvalstu kiberizlūkošanas darba grupas iespējamo izveidi, ar ko varētu stiprināt *INTCEN* īpašās spējas šajā jomā, balstoties uz dalībvalstu izlūkdienestu brīvprātīgu ieguldījumu un neskarot dalībvalstu kompetenci;

25. UZSVER, cik svarīgs ir stabils un konsekvents drošības satvars, lai aizsargātu visu ES personālu, datus, sakaru tīklus un informācijas sistēmas, kā arī lēmumu pieņemšanas procesus, kuru pamatā ir visaptveroši, konsekventi un viendabīgi noteikumi. Tas jo īpaši būtu jādara, paaugstinot ES noturību un uzlabojot drošības kultūru cīņā pret kiberdraudiem un stiprinot klasificētu un neklasificētu ES tīklu drošību, vienlaikus nodrošinot pienācīgu pārvaldību un to, ka tiek darīti pieejami pietiekami resursi un spējas, tostarp *CERT-EU* pilnvaru pastiprināšanas kontekstā; šajā kontekstā ATZINĪGI VĒRTĒ notiekošās diskusijas par kopīgu informācijas drošības noteikumu izstrādi, pienācīgi ņemot vērā Padomes drošības noteikumus ES klasificētas informācijas aizsardzībai, kā arī visām ES iestādēm, struktūrām un aģentūrām paredzētu kopīgu saistošu noteikumu definēšanu kiberdrošības jomā;

26. BALSTOTIES UZ ES kiberdiplomātijas centieniem, APŅEMAS palielināt kiberdiplomātijas instrumentu kopuma efektivitāti un iedarbīgumu un CER padziļināt diskusijas par tā darbības jomu un pielietojumu, izmantojot pieredzi, kas gūta šā instrumentu līdzšinējā piemērošanā. Šīm diskusijām būtu jāpalīdz veicināt drošību starptautiskā līmenī, rosinot dialogu un sekmējot kopīgu redzējumu par kiberdrošības jautājumiem, stiprinot novēršanu, stabilitāti, sadarbību un veicinot uzticēšanos un spēju veidošanu, un vajadzības gadījumā piemērojot ierobežojošus pasākumus, lai novērstu un kavētu ļaunprātīgas kiberdarbības, kas vērstas pret ES un tās dalībvalstu integritāti un drošību, kā arī atturētu no šādām darbībām un reaģētu uz tām, tādējādi veicinot starptautisko drošību un stabilitāti un saliedējot ES nostāju kiberjautājumos, kā arī pilnībā ievērojot valstu kompetenci un prerogatīvas. Konkrēti, īpaša uzmanība būtu jāpievērš tam, lai novērstu un apkarotu kiberuzbrukumus ar sistēmisku iedarbību, kuri varētu ietekmēt mūsu piegādes ķēdes, kritisko infrastruktūru un pamatpakalpojumus, demokrātijas institūtus un procesus un apdraudēt mūsu ekonomisko drošību, tostarp ar kiberiespējotām intelektuālā īpašuma zādzībām. Dalībvalstīm un ES iestādēm būtu arī sīkāk jāapsver saikne starp ES kiberdrošības krīžu pārvarēšanas satvaru, kiberdiplomātijas instrumentu kopumu un LES 42. panta 7. punkta un LESD 222. panta noteikumiem, jo īpaši uz scenārijiem balstītā darbā veidojot kopīgu izpratni par LES 42. panta 7. punkta īstenošanas praktisko kārtību;

27. ATZĪST, ka ir svarīgi stiprināt sadarbību ar starptautiskām organizācijām un partnervalstīm nolūkā veicināt kopīgu izpratni par kiberapdraudējuma ainu, attīstīt dialogus un sadarbības mehānismus, attiecīgā gadījumā identificēt uz sadarbību vērstu diplomātisko reakciju, kā arī uzlabot informācijas apmaiņu, tostarp ar izglītības, apmācības un mācību palīdzību; jo īpaši UZSVER, ka spēcīga transatlantiskā partnerība kiberdrošības jomā veicina mūsu kopējo drošību, stabilitāti un labklājību, un NORĀDA uz ES un Apvienotās Karalistes Tirdzniecības un sadarbības nolīguma noteikumiem par sadarbību kiberdrošības jomā; ATGĀDINOT par galvenajiem sasniegumiem ES un NATO sadarbībā kiberdrošības jomā 2016. gada Varšavas un 2018. gada Briseles kopīgo deklarāciju īstenošanas satvarā, atkārtoti uzsver, cik svarīga ir ciešāka, savstarpēji pastiprinoša un izdevīga sadarbība, ko īsteno ar izglītību, apmācību, mācībām un koordinētu reakciju uz ļaunprātīgām kiberdarbībām, pilnībā ievērojot abu organizāciju lēmumu pieņemšanas autonomiju un procedūras un pamatojoties uz pārredzamības, savstarpīguma un iekļautības principiem;

28. lai veicinātu globālu, atvērtu, brīvu, stabilu un drošu kibertelpu, kura ir aizvien nozīmīgāka mūsu sabiedrības pastāvīgai labklājībai, izaugsmei, drošībai, labbūtībai, savienojamībai un integritātei, APŅEMAS pastāvīgi iesaistīties normu izstrādes procesos starptautiskās organizācijās, jo īpaši ar ANO pirmo komiteju saistītajos procesos, veicinot un sekmējot starptautisko tiesību piemērošanas kibertelpā atzīšanu un to, ka tiek ievēroti noteikumi, normas un principi, kas vērsti uz valstu atbildīgu uzvedību kibertelpā, tostarp, veicinot to, ka tiek ātri izveidota rīcības programma valstu atbildīgas uzvedības kibertelpā sekmēšanai, kas būtu konstruktīva, iekļaujoša un uz vienprātību balstīta turpmākā rīcība gan ANO valdības ekspertu grupas (*UNGGE*), gan atklātā sastāva darba grupas (*OEWG*) virzīto pašreizējo procesu satvarā;

29. ATGĀDINA savu stingro apņemšanos nodrošināt efektīvu multilaterālismu un uz noteikumiem balstītu globālo kārtību, kuras centrā ir Apvienoto Nāciju Organizācija, un apņēmību stiprināt sadarbību un koordināciju ar starptautiskām un reģionālām organizācijām, īpaši ANO sistēmu, NATO, Eiropas Padomi, EDSO, ESAO, ĀS, *OAS*, *ASEAN*, *ASEAN* Reģionālo forumu, Persijas līča sadarbības padomi (*GCC*) un Arābu valstu līgu (AVL), attiecībā uz diskusijām saistībā ar kiberjautājumiem, kā arī strukturētu ES kiberdialogu un konsultāciju ar trešām valstīm turpināšanu un paplašināšanu; UZSVER savu aktīvo atbalstu ANO, jo īpaši saistībā ar tās Programmu 2030. gadam, tostarp ilgtspējīgas attīstības mērķiem, un ATZINĪGI VĒRTĒ ANO ģenerālsekretāra Digitālās sadarbības ceļvedi un Atbruņošanās programmu, ar ko iecerēts veicināt pārskatatbildību un normu ievērošanu kibertelpā un palīdzēt novērst un miermīlīgi atrisināt konfliktus, kas izriet no ļaunprātīgām darbībām kibertelpā; ATZINĪGI VĒRTĒ Augstā pārstāvja ārlietās un drošības politikas jautājumos priekšlikumu izveidot neformālu ES kiberdiplomātijas tīklu nolūkā pilnveidot gan ES, gan dalībvalstu iesaisti starptautiskos kiberjautājumos un zinātību par tiem, lai tādējādi stiprinātu koordinētus informēšanas pasākumus;

30. AR CERĪBĀM RAUGĀS uz gaidāmo priekšlikumu par kiberaizsardzības politikas satvara (*CDPF*) pārskatīšanu un APŅEMAS turpināt centienus stiprināt kiberdrošības un kiberaizsardzības dimensijas, lai nodrošinātu, ka tās ir pilnībā integrētas plašākā drošības un aizsardzības jomā, jo īpaši darba pie Stratēģiskā kompasa kontekstā; UZSKATA, ka gaidāmais "Militārais redzējums un stratēģija par kibertelpu kā operāciju jomu" palīdzēs veicināt šīs diskusijas; ATZINĪGI VĒRTĒ Eiropas Aizsardzības aģentūras (EAA) iniciatīvu veicināt sadarbību starp militārām datorapdraudējumu reaģēšanas vienībām un ATBALSTA centienus uzlabot civilā un militārā sektora sinerģiju un koordināciju kiberaizsardzības un kiberdrošības jomā, tostarp ar kosmosu saistītu aspektu kontekstā, šajā nolūkā izmantojot arī īpašus *PESCO* projektus;

31. ATZINĪGI VĒRTĒ priekšlikumu izstrādāt ES ārējo kiberspēju veidošanas darba programmu, priekšlikumu izveidot ES kiberspēju veidošanas padomi un izveidot un īstenot ES *CyberNet* (ES kiberspēju veidošanas tīklu), lai visā pasaulē palielinātu kibernoturību un spējas; šajā kontekstā PAUŽ GANDARĪJUMU par sadarbību ar dalībvalstīm, kā arī ar publiskā un privātā sektora partneriem, jo īpaši Globālo kiberekspertīzes forumu (*GFCE*) un citām attiecīgām starptautiskām struktūrām, nolūkā nodrošināt koordināciju un izvairīties no dublēšanās; jo īpaši MUDINA sadarboties ar partneriem Rietumbalkānos un ES austrumu un dienvidu kaimiņreģionā;

32. lai nodrošinātu, ka visas valstis spēj izmantot interneta un tehnoloģiju izmantošanas sniegots sociālos, ekonomiskos un politiskos ieguvumus, APŅEMAS partnervalstīm palīdzēt – tostarp saskaņā ar Eiropas Demokrātijas rīcības plāna centieniem – pārvarēt pieaugošās grūtības, ko rada ļaunprātīgas kiberdarbības, jo īpaši tādas, kas kaitē to ekonomikas attīstībai, sabiedrībai un demokrātisko sistēmu integritātei un drošībai;

33. lai nodrošinātu ES kiberdrošības stratēģijā izklāstīto priekšlikumu izstrādi, īstenošanu un uzraudzību un ņemot vērā dažu iniciatīvu daudzgadu raksturu, MUDINA Komisiju un Augsto pārstāvi ārlietās un drošības politikas jautājumos izstrādāt detalizētu īstenošanas plānu, kurā būtu noteiktas prioritātes un plānoto darbību grafiks; PĀRRAUDZĪS šo secinājumu īstenošanā gūtos panākumus, izmantojot rīcības plānu, kuru Padome, cieši sadarbojoties ar Eiropas Komisiju un Augsto pārstāvi, regulāri pārskatīs un atjauninās.