Eiropas Savienības
Padome

Briselē, 2022. gada 17. oktobrī
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2022. gada 17. oktobris
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	12930/22
Temats:	Padomes secinājumi par IKT piegādes ķēdes drošību – Padomes secinājumi, ko Padome apstiprināja 2022. gada 17. oktobra sanāksmē

Pielikumā pievienoti Padomes secinājumi par IKT piegādes ķēdes drošību, kurus Padome apstiprināja 2022. gada 17. oktobra sanāksmē.

PIELIKUMS

Padomes secinājumi par IKT piegādes ķēdes drošību

EIROPAS SAVIENĪBAS PADOME,

ATGĀDINOT savus secinājumus:

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

– par kiberdrošības spēju un spēju veidošanu ES,

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

– par Eiropas digitālās nākotnes veidošanu,

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

– par savienoto ierīču kiberdrošību,

– par ES kiberdrošības stratēģiju digitālajai desmitgadei,

– par Eiropas Savienības pozīcijas kiberjautājumos izstrādi,

– par Eiropas Revīzijas Palātas Īpašo ziņojumu Nr. 03/2022 "5G ierīkošana Eiropas Savienībā: tīklu ieviešana kavējas, turklāt drošības jautājumi joprojām nav atrisināti",

ATGĀDINOT Eiropadomes secinājumus:

– par Covid-19, vienoto tirgu, rūpniecības politiku, digitālo dimensiju un ārējām attiecībām (2020. gada 1. un 2. oktobris),

– par Krievijas militāro agresiju pret Ukrainu, drošību un aizsardzību, enerģētiku, ekonomikas jautājumiem, Covid-19 un ārējām attiecībām (2022. gada 24. un 25. marts),

– par Ukrainu, pārtikas nodrošinājumu, drošību un aizsardzību un enerģētiku (2022. gada 30. un 31. maijs).

1. Ņemot vērā ģeopolitikas pieaugošo nozīmi kiberdrošības jomā, UZSVER, ka Eiropas Savienībai un tās dalībvalstīm ir visaptveroši un stratēģiski jāpievēršas kiberdrošībai. Krievijas militārā agresija pret Ukrainu ir izraisījusi būtisku pārbīdi Eiropas Savienības stratēģiskajā un drošības vidē un apliecinājusi vajadzību pēc spēcīgākas un spējīgākas Eiropas Savienības drošības un aizsardzības jomā. Šī agresija akcentēja to, ka ir ārkārtīgi svarīgi pienācīgi ņemt vērā ģeopolitisko vidi, ne tikai reaģējot uz ļaunprātīgām kiberdarbībām, bet arī veidojot un uzturot informācijas un komunikācijas tehnoloģiju (IKT) noturību. Tas ir īpaši svarīgi attiecībā uz IKT produktu un pakalpojumu piegādes ķēdēm (IKT piegādes ķēdes), kam var pastāvēt apdraudējums ģeopolitiskās sāncensības dēļ, ko parādīja *SolarWinds* uzbrukums, un ko var ietekmēt ģeopolitiskā spriedze un nestabilitāte, par ko liecina draudi, kas saistīti ar atkarību no Krievijas IKT pārdevējiem laikā, kad Krievija īsteno militāro agresiju pret Ukrainu.

2. NORĀDA, ka to risku raksturs, kas saistīti ar IKT piegādes ķēdi, kuru veido saistīts resursu un procesu kopums starp ekonomikas dalībniekiem (kā definēts Regulā (ES) 2019/1020), kas sākas ar izejvielu ieguvi un aptver IKT produktu un pakalpojumu ražošanu, pārstrādi, apstrādi un piegādi, tostarp atbalsta sniegšanu IKT produktu un pakalpojumu aprites ciklā, rada unikālas problēmas un, iespējams, tālejošas sekas. Papildus riskiem, kas saistīti ar IKT produktu nepieejamību, piemēram, to ražošanai nepieciešamo kritiski svarīgo izejvielu un pusvadītāju trūkuma dēļ, IKT produktu un pakalpojumu piegādes ķēdes ir pakļautas arī citiem apdraudējumiem. Proti, ļaunprātīgi spēki var tiem uzbrukt vai ļaunprātīgi izmantot sarežģītos, bieži vien slēptos veidos, kas ietekmē nosūtīto un uzglabāto sensitīvo datu konfidencialitāti, integritāti un pieejamību.

3. Piekrītot, ka, lai nodrošinātu IKT aktīvu drošību, ir vajadzīga pieeja, kas aptver visus apdraudējumus, ATZĪST, cik svarīgs ir Kritisko vienību noturības direktīvas priekšlikums, lai uzlabotu kritisko vienību fizisko drošību, un UZSVER, ka papildus noturības uzlabošanai pret uzbrukumiem piegādes ķēdei, kurus veic, izmantojot kiberlīdzekļus, tikpat svarīgi ir stiprināt IKT piegādes ķēžu vispārējo noturību un drošību pret visdažādākajiem apdraudējuma faktoriem, piemēram, dabas parādībām, sistēmas kļūmēm, iekšnieku draudiem vai cilvēka kļūdām. Šajā sakarā ATZĪST, ka IKT piegādes ķēdes drošība ietver tādu IKT produktu un pakalpojumu aizsardzības nodrošināšanu, ko izstrādā, piegādā, iepērk un izmanto IKT piegādes ķēdēs, tostarp, aizsargājot atsevišķus komponentus un nosūtītos datus.

4. Mācoties no sekām, ko radījusi Eiropas Savienības stratēģiskā atkarība no Krievijas fosilā kurināmā, kā arī no piegādes ķēžu traucējumu ietekmes Covid-19 pandēmijas laikā, jo īpaši attiecībā uz zālēm un pusvadītājiem, kas atklāja ES stratēģiskās atkarības, MUDINA dalībvalstis strādāt pie tā, lai izvairītos no līdzīgām situācijām saistībā ar nevēlamām stratēģiskām ārējām atkarībām IKT produktu un pakalpojumu jomā. Ņemot vērā pieaugošo sabiedrības digitalizāciju un arvien pieaugošo IKT izmantošanu kritiskajā infrastruktūrā, būtu pastāvīgi jāizvērtē un attiecīgā gadījumā jārisina stratēģiskās ārējās atkarības, kas saistītas ar IKT produktiem un pakalpojumiem un to piegādes ķēdēm.

5. ATGĀDINA, ka stratēģiskas autonomijas panākšana, vienlaikus saglabājot atvērtu ekonomiku, ir svarīgs Savienības mērķis, kas ietver stratēģisko atkarību apzināšanu un samazināšanu un noturības palielināšanu visjutīgākajās rūpniecības ekosistēmās un konkrētās jomās, tostarp digitālajā jomā. Tas ietver stratēģisku digitālo jaudu un infrastruktūras izveidi un izvēršanu, kā arī spēju izdarīt autonomas tehnoloģiskas izvēles stiprināšanu un – kā vienu no galvenajiem pīlāriem – noturīgu un drošu infrastruktūru, produktu un pakalpojumu nodrošināšanu, lai veidotu uzticēšanos digitālajam vienotajam tirgum un Eiropas sabiedrības uzticēšanos, vienlaikus saglabājot atvērtību, globālo sadarbību ar līdzīgi domājošiem partneriem un konkurētspēju un izmantojot tās potenciālos ieguvumus. Eiropas Savienības pamatvērtības jo īpaši aizsargā privātumu, drošību, līdztiesību, cilvēka cieņu, tiesiskumu un atvērtu internetu kā priekšnoteikumus, lai izveidotu digitāli orientētu, uz cilvēku vērstu sabiedrību, ekonomiku un rūpniecību.

6. ATZĪMĒ, ka, ņemot vērā norises kiberdraudu vidē, ko raksturo vairāki pēdējos gados notikušie sarežģītie uzbrukumi piegādes ķēdēm ar ļoti būtiskām sekām, piemēram, uzbrukumi *SolarWinds*, *Mimecast* vai *Kaseya*, kuri rodas līdz ar būtisko IKT pakalpojumu nodošanu ārpakalpojumā un kuri pastiprinās sakarā ar vispārēju paļaušanos uz trešo personu ražotiem, nodrošinātiem vai apkalpotiem IKT produktiem un pakalpojumiem, nākotnē ir ļoti iespējams, ka notiks vairāk uzbrukumu piegādes ķēdēm, nodarot būtisku kaitējumu ekonomikai un sabiedrībai. Ņemot to vērā, UZSVER, cik svarīgi vienotā tirgus darbībai ir uzlabot IKT piegādes ķēžu drošību un noturību un nodrošināt IKT produktu un pakalpojumu pieejamību, drošību un daudzveidību vienotajā tirgū. Tādēļ ATZĪST, ka, lai sasniegtu šos mērķus, ir maksimāli jāpalielina un jāracionalizē esošo ES instrumentu un pieeju izmantošana, kā arī ir pastāvīgi jāpielāgojas mainīgajai kiberdraudu videi, ieviešot piemērotus papildu pasākumus un mehānismus, tostarp saistībā ar iespējamiem jaunu un revolucionāru tehnoloģiju radītiem drošības riskiem. Šajā sakarībā MUDINA dalībvalstis izmantot uz risku balstītu pieeju, lai risinātu ar jauno tehnoloģiju attīstību saistītus jautājumus.

7. ATZĪST, ka, lai efektīvi mazinātu riskus, kas saistīti ar IKT piegādes ķēdēm, ir būtiski izprast pastāvīgi mainīgo situāciju kiberdraudu vidē, kā arī uzbrukumu piegādes ķēdēm sarežģītību. Šajā sakarā UZSVER, ka ir jāpielāgojas jauniem apdraudējumiem, aktīvi un pastāvīgi uzraugot, analizējot un novērtējot situāciju saistībā ar apdraudējumiem piegādes ķēdēm, jāpalielina informētība un jāvairo zināšanas par apdraudējumiem un neaizsargātību, kā arī pielāgotā veidā ir proaktīvi jābrīdina attiecīgās vienības. ATZINĪGI VĒRTĒ Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) darbu IKT piegādes ķēdes drošības jomā, jo īpaši tās ziņojumu par drošības apdraudējuma ainu saistībā ar uzbrukumiem piegādes ķēdēm ("*Report on the Threat Landscape for Supply Chain Attacks*").

STARPNOZARU INSTRUMENTI UN PIEEJAS

8. ATKĀRTOTI APSTIPRINA, ka ir svarīgi, lai dalībvalstis apsvērtu nepieciešamību dažādot kritisko IKT piegādātājus, lai novērstu vai ierobežotu to, ka tiek radīta būtiska atkarība no viena piegādātāja un jo īpaši no augsta riska piegādātājiem, jo tas palielina iespējamo traucējumu izraisīto seku ietekmi. ATZĪST, ka izvairīšanās no piesaistes vienam pārdēvējam un IKT piegādātāju dažādošana ir viens no svarīgajiem elementiem, lai nodrošinātu iekšējā tirgus stabilitāti un drošību. UZSVER, ka ir jāveicina un jāīsteno piemērotas stratēģijas, kas veicina pārdevēju dažādošanu un konkurētspēju tehnoloģiski neitrālā veidā. Turklāt MUDINA ES tiesību aktos integrēt aspektus, kas saistīti ar to, lai novērstu atkarību no viena pārdevēja. Šajā sakarā ATZINĪGI VĒRTĒ priekšlikumu Regulai par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to izmantošanu (Datu akts), kuras mērķis ir palielināt datu apstrādes pakalpojumu sadarbspēju un novērst šķēršļus datu apstrādes pakalpojumu sniedzēju maiņai.

9. ATZĪST IKT piegādes ķēdes drošības saikni ar publisko iepirkumu. UZSVER, ka publiskā iepirkuma procedūrās ir pienācīgi jāņem vērā IKT piegādes ķēdes drošības nozīme, attiecīgā gadījumā nosakot objektīvus un uz risku balstītus atlases kritērijus attiecībā uz pretendentu spēju nodrošināt augstu sniegto pakalpojumu drošības līmeni. AICINA rast pareizo līdzsvaru starp sabiedrības interesēm visefektīvākajā un godīgākajā publisko līdzekļu izmantošanā, no vienas puses, un sabiedrības interesēm nodrošināt informācijas sistēmu drošību un vienotā tirgus netraucētu darbību, no otras puses. Lai kiberdrošības palielināšanas kontekstā atvieglotu attiecīgo publiskā iepirkuma noteikumu īstenošanu, AICINA Komisiju līdz 2023. gada trešajam ceturksnim izstrādāt metodiskās pamatnostādnes, lai mudinātu līgumslēdzējas iestādes pievērst pienācīgu uzmanību pretendentu un to apakšuzņēmēju kiberdrošības praksei un izvērtēt attiecīgos publiskā iepirkuma tiesību aktus un vajadzības gadījumā nākt klajā ar priekšlikumiem to pārskatīšanai vai papildināšanai.

10. ATZĪST, ka ārvalstu tiešie ieguldījumi, kas saistīti ar IKT produktiem un pakalpojumiem, kaut arī sniedz ekonomiskus un sociālus ieguvumus dalībvalstīm, uzņēmumiem un iedzīvotājiem, varētu ietvert riskus drošībai un sabiedriskajai kārtībai, un ATZĪMĒ, ka ES ārvalstu tiešo ieguldījumu izvērtēšanas mehānismu kopā ar attiecīgajām valstu izvērtēšanas sistēmām, kas nodrošina līdzekļus šādu risku novēršanai, arī varētu izmantot kā noderīgu instrumentu, lai aizsargātu IKT piegādes ķēdes drošību un noturību, palīdzot novērst augsta riska ieguldījumus, kas var ietekmēt šādu drošību un noturību. ATZĪST, ka informācija, ar ko apmainās vai dalās, izmantojot šo mehānismu, var palīdzēt dalībvalstīm labāk novērtēt iespējamos draudus IKT piegādes ķēžu drošībai un attiecīgi veikt nepieciešamos pasākumus. AICINA attiecīgos valstu dalībniekus attiecīgā gadījumā ņemt vērā arī šo izvērtēšanas mehānisma dimensiju.

11. Attiecībā uz aizsardzību ATKĀRTOTI APSTIPRINA savu aicinājumu Komisijai 2023. gadā kopā ar dalībvalstīm novērtēt riskus kritiskās infrastruktūras piegādes ķēdēm dažādās jomās, tostarp digitālajā jomā, kas saistīti ar ES drošības un aizsardzības interesēm, kā arī izpētīt iespējas paaugstināt kiberdrošību visā ES aizsardzības tehniskā un rūpnieciskā pamata piegādes ķēdē. Turklāt AICINA dalībvalstis un Komisiju, īstenojot Stratēģiskā kompasa saistības un darbības, apsvērt IKT piegādes ķēdes drošību.

12. Atzīstot, cik nozīmīgas ir kritiski svarīgas izejvielas, kā arī visu veidu pusvadītāji kā IKT produktu pamatelementi, MUDINA risināt konstruktīvas sarunas par priekšlikumu Regulai, ar ko izveido pasākumu satvaru Eiropas pusvadītāju ekosistēmas stiprināšanai (Mikroshēmu akts), un priekšlikumu Padomes Regulai, ar kuru Regulu (ES) 2021/2085, ar ko izveido kopuzņēmumus pamatprogrammā "Apvārsnis Eiropa", groza attiecībā uz kopuzņēmumu "Mikroshēmas".

AR KIBERDROŠĪBU SAISTĪTI INSTRUMENTI

13. Konkrēti attiecībā uz telekomunikāciju infrastruktūru ATZĪST sasniegumus Savienības līmenī, lai uzlabotu 5G tīklu piegādes ķēdes drošību, jo īpaši, izmantojot ES rīkkopu 5G drošībai (ES 5G rīkkopa). AICINA dalībvalstis turpināt apmainīties ar informāciju par paraugpraksi un metodēm par to, kā īstenot pasākumus, kas ieteikti ES 5G rīkkopā, un jo īpaši piemērot attiecīgos ierobežojumus augsta riska piegādātājiem saistībā ar tiem galvenajiem aktīviem, kas ES koordinētajā riska novērtējumā definēti kā kritiski un sensitīvi. UZSVER, ka ES 5G rīkkopa ir ātrs, uz risku balstīts instruments apzināto drošības problēmu risināšanai, kas ļauj laikus un efektīvi risināt 5G kiberdrošības aspektus, vienlaikus ievērojot dalībvalstu kompetences, un ATZĪST, ka tas ir vērtīgs instruments, ar ko, ievērojot pilnīgu pārredzamību, koordinētā veidā vēl vairāk uzlabot telekomunikāciju tīklu piegādes ķēdes drošību, kas varētu kalpot par iedvesmas avotu riska novērtēšanas un mazināšanas rīkiem, kuri saistīti ar citām svarīgām nozarēm. ATGĀDINA par attiecīgo iestāžu aicinājumu, pamatojoties uz riska novērtējumiem, formulēt ieteikumus dalībvalstīm un Komisijai, lai stiprinātu sakaru tīklu un infrastruktūras noturību Eiropas Savienībā, tostarp turpināt īstenot ES 5G rīkkopu.

14. NORĀDA, cik svarīgas ir sadarbspējīgas pieejas, ar kurām var novērst atkarību no viena pārdevēja un mazināt koncentrācijas risku, vienlaikus uzlabojot piegādes ķēdes drošību visā IKT infrastruktūras un pakalpojumu spektrā. Jo īpaši attiecībā uz 5G tīkliem ATZĪST iespējamos ieguvumus, ko šajā sakarā var sniegt atvērta radiopiekļuves tīkla (*RAN*) koncepcija, vienlaikus ATGĀDINA TID sadarbības grupas publicēto ziņojumu par atvērtā *RAN* kiberdrošību, norādot, ka šī koncepcija joprojām tiek izstrādāta un ka *RAN* drošība, pārredzamība un standartizācija ir agrīnā gatavības stadijā, un UZSVER, cik svarīgi ir novērtēt riskus pirms jebkādas pārejas uz jauniem standartiem vai arhitektūrām.

15. UZSVER, cik svarīgi IKT piegādes ķēdes drošības paaugstināšanai ir esošie un gaidāmie horizontālie tiesību akti kiberdrošības jomā, jo īpaši Regula par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (Kiberdrošības akts), gaidāmā direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (TID 2), priekšlikums regulai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās, kā arī priekšlikums regulai par horizontālām kiberdrošības prasībām produktiem ar digitāliem elementiem (Kibernoturības akts). Turklāt ATZĪMĒ svarīgās norises nozaru kiberdrošības noteikumos, jo īpaši gaidāmo regulu par finanšu sektora digitālās darbības noturību (*DORA*), kurā ir ietverts trešo personu, kas sniedz IKT pakalpojumus, pārraudzības satvars, kas ir kritiski svarīgi finanšu vienībām. Šajās regulās ir paredzēti vispārīgi pienākumi saistībā ar piegādes ķēdes drošību, kā arī sīki izstrādātas un konkrētas prasības, kas attiecas uz attiecīgo nozari. Vienlaikus UZSVER, ka piegādātāji savus produktus un pakalpojumus bieži vien nodrošina dažādās nozarēs, nevis vienai nozarei. Tāpēc ir ļoti svarīgi nodrošināt, ka piegādes ķēdes drošības prasības, cik vien iespējams, tiek saskaņotas visās attiecīgajās nozarēs, jo īpaši tajās, uz kurām attiecas gaidāmā TID 2 direktīva, lai izvairītos no atšķirībām starp piegādātājiem noteiktajiem pienākumiem, kā arī lai atvieglotu kritiski svarīgu nozaru operatoriem radīto slogu novērtēt piegādātāju atbilstību minētajiem pienākumiem, vienlaikus ņemot vērā nozaru īpatnības.

16. ATZINĪGI VĒRTĒ Kibernoturības akta priekšlikumu kā svarīgu likumdošanas instrumentu, lai veicinātu tādu produktu drošu izstrādi, kuriem ir digitāli elementi, un lai nodrošinātu, ka kiberdrošība tiek ņemta vērā visā produktu ar digitālajiem elementiem aprites ciklā. ATZĪMĒ, ka Kibernoturības akta priekšlikumam ir potenciāls būtiski sekmēt IKT piegādes ķēdes drošības stiprināšanu. MUDINA risināt konstruktīvas sarunas par aktu un to savlaicīgi pieņemt.

17. Šajā sakarā ATZINĪGI VĒRTĒ *ENISA* vadībā un kopā ar dalībvalstīm un citām ieinteresētajām personām veikto darbu, kura mērķis ir nodrošināt ES ar IKT produktu, pakalpojumu un procesu sertifikācijas shēmām atbilstoši Kiberdrošības aktam, kam būtu jāpalīdz paaugstināt vispārējo kiberdrošības līmeni digitālajā vienotajā tirgū. MUDINA visas ieinteresētās personas piedalīties atsevišķo Eiropas sertifikācijas shēmu sagatavošanas darbā, lai vairotu uzticēšanos drošiem IKT produktiem, procesiem un pakalpojumiem un stiprinātu to noturību, un AICINA Komisiju pēc sagatavošanas darba pabeigšanas ātri sagatavot īstenošanas aktus par Eiropas sertifikācijas shēmām, jo īpaši par kopējos kritērijos balstītu Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*). ATZĪMĒ, ka Eiropas sertifikācijas shēmās vajadzības gadījumā būtu jāiekļauj prasības par piegādes ķēdes drošību, ietverot attiecības ar piegādātājiem.

18. UZSVER, ka ir rūpīgi jāīsteno visi gaidāmie TID 2 noteikumi, kas saistīti ar IKT piegādes ķēdes drošību. Šajā sakarā UZSVER, cik svarīgi ir koordinēti ES riska novērtējumi attiecībā uz kritiski svarīgām piegādes ķēdēm (koordinēti piegādes ķēdes riska novērtējumi), valstu politika attiecībā uz piegādes ķēdes drošību un ar piegādes ķēdi saistīti drošības pasākumi. NORĀDA, ka uzmanība būtu jāpievērš ne tikai primārajiem piegādātājiem, bet arī attiecīgajiem apakšuzņēmējiem attiecībā uz riskiem primārā piegādātāja vai galalietotāja drošībai. Lai atvieglotu piegādes ķēdes riska pārvaldības pasākumu īstenošanu, MUDINA *ENISA* ar TID sadarbības grupas palīdzību izvērtēt labāko praksi, kas pieejama piegādes ķēdes riska pārvaldībai, un apkopot to metodiskajās pamatnostādnēs. Turklāt MUDINA *ENISA* uzraudzīt ieguldījumus to vienību IKT piegādes ķēdes drošībā, kuras reglamentē gaidāmā TID 2 direktīva.

19. UZSVER arī ieguvumus un riskus, ko piegādes ķēdes drošības kontekstā rada pārvaldīto pakalpojumu sniedzēju un pārvaldīto drošības pakalpojumu sniedzēju izmantošana. Lai gan šo pakalpojumu sniedzēju izmantošana var būtiski uzlabot drošību organizācijās un panākt augstāku kiberdrošības līmeni, IKT sistēmu un pakalpojumu attālināta pārvaldība apvienojumā ar priviliģētu piekļuvi klientu IKT videi, kas varētu būt nepieciešama pārvaldīto pakalpojumu sniedzējiem un pārvaldīto drošības pakalpojumu sniedzējiem, var pārvaldīto pakalpojumu sniedzēju vai pārvaldīto drošības pakalpojumu sniedzēju apdraudējuma gadījumā pēc tam ietekmēt lielu skaitu klientu. Tāpēc ir ārkārtīgi svarīgi, lai pārvaldīto pakalpojumu sniedzēji un pārvaldīto drošības pakalpojumu sniedzēji uzturētu augstu savas iekšējās drošības līmeni un to sniegto pakalpojumu drošību un lai tie pret saviem klientiem īstenotu pārredzamu pieeju saistībā ar to sniegto pakalpojumu drošību. Šajā sakarā ATZINĪGI VĒRTĒ to turpmāko iekļaušanu gaidāmās TID 2 direktīvas darbības jomā.

20. Attiecībā uz mehānisma īstenošanu koordinētiem piegādes ķēdes riska novērtējumiem saskaņā ar gaidāmo TID 2 direktīvu ŅEM VĒRĀ netehnisku riska faktoru nozīmi šajā kontekstā, piemēram, trešās valsts nepamatotu ietekmi uz piegādātājiem un pakalpojumu sniedzējiem, un šajā sakarā ATZĪST faktorus, ko var izmantot, lai novērtētu riska profilu, kā minēts ES koordinētajā 5G tīklu kiberdrošības riska novērtējumā. AICINA Komisiju pēc apspriešanās ar TID sadarbības grupu un *ENISA* līdz 2023. gada otrajam ceturksnim apzināt konkrētus IKT pakalpojumus, sistēmas vai produktus, attiecībā uz kuriem prioritārā kārtā varētu veikt koordinētus piegādes ķēdes riska novērtējumus.

21. ATZĪMĒ, ka atkarība no augsta riska tādu IKT produktu un pakalpojumu piegādātājiem, ko izmanto kritisko tīklu un sistēmu ekspluatācijai, rada stratēģisku apdraudējumu, kurš jāmazina, izmantojot piemērotus politikas pasākumus gan valstu, gan ES līmenī, gan arī dalībvalstīm sadarbojoties savā starpā un ar līdzīgi domājošiem starptautiskajiem partneriem. Lai atvieglotu šā stratēģiskā riska mazināšanu un atbalstītu koordinētos piegādes ķēdes riska novērtējumus, AICINA TID sadarbības grupu sadarbībā ar Komisiju un *ENISA* izstrādāt pasākumu kopumu kritisko IKT piegādes ķēžu risku mazināšanai (IKT piegādes ķēžu rīkkopu). IKT piegādes ķēžu rīkkopā par pamatu būtu jāņem stratēģiskā apdraudējuma scenāriji, kas apzināti attiecībā uz IKT piegādes ķēdēm, un jāparedz pasākumi, ar ko uz šiem scenārijiem reaģē, produktīvi izmantojot atziņas, kas gūtas saistībā ar 5G rīkkopu un valstu līmenī. Tai pārredzamā veidā būtu jāpapildina koordinētie piegādes ķēdes riska novērtējumi konkrētiem IKT pakalpojumiem, sistēmām vai produktiem saskaņā ar gaidāmo TID 2 direktīvu, paredzot vispārējus riska mazināšanas pasākumus, ko mērogojami var pielāgot konkrētiem IKT pakalpojumiem, sistēmām vai produktiem, pamatojoties uz riskiem, kas identificēti atsevišķajos koordinētajos piegādes ķēdes riska novērtējumos.

22. UZSVER svarīgo lomu, kāda ir pētniecībai, inovācijai, investīcijām un uzņēmējdarbībai digitālajā un kiberdrošības jomā, kā arī šādu darbību finansēšanai attiecībā uz to, lai nākotnē izvairītos no iespējamas nevēlamas stratēģiskās atkarības un stiprinātu IKT piegādes ķēžu vispārējo noturību. Šajā kontekstā UZSVER lomu un nozīmi, kāda ir Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra un Nacionālo koordinācijas centru tīkla (*ECCC*) stratēģiskajiem un īstenošanas uzdevumiem, sekmējot investīciju maksimālu produktivitāti nolūkā stiprināt Savienības līderību un atvērtu stratēģisko autonomiju kiberdrošības un Savienības atbalsta tehnoloģisko spēju un prasmju jomā un palielināt Savienības globālo konkurētspēju. Šajā sakarā AICINA ātri sākt *ECCC* darbību. AICINA *ECCC* savā stratēģiskajā programmā ņemt vērā IKT piegādes ķēžu drošības aspektus, tostarp, piemēram, drošu programmatūru izstrādi, vienlaikus nodrošinot konsekvenci un papildināmību un izvairoties no jebkādas centienu dublēšanās. ATBALSTA Eiropas konkurētspējas uzlabošanu kiberdrošības jomā, izmantojot finansēšanas programmas, piemēram, pētniecības un inovācijas pamatprogrammu "Apvārsnis Eiropa", kā arī programmu "Digitālā Eiropa" ES digitālās ekonomikas, sabiedrības un demokrātijas būtisko spēju stiprināšanai, veidošanai un nodrošināšanai.

ATBALSTA MEHĀNISMI

23. MUDINA palielināt finansiālā atbalsta stimulus saistībā ar pasākumiem, kuri vērsti uz IKT piegādes ķēžu drošības pastiprināšanu. Prioritārā kārtā un ņemot vērā gaidāmo TID 2 direktīvas īstenošanu, AICINA *ECCC*, Komisiju un attiecīgās ieinteresētās personas izskatīt iespējas, kā iekļaut IKT piegādes ķēžu drošības aspektus paredzamajos uzaicinājumos kiberdrošības darba programmu ietvaros saskaņā ar programmām "Digitālā Eiropa" un "Apvārsnis Eiropa" vai jebkādās citās attiecīgās finansēšanas iespējās. Šīs finansēšanas iespējas cita starpā būtu jāvērš uz to, lai dotu organizācijām iespēju atbalstīt augsta līmeņa kiberdrošības uzturēšanu attiecībā uz IKT produktu un pakalpojumu iepirkšanu visā piegādes ķēdē, jo īpaši saistībā ar tādu konkrētu kritisko IKT pakalpojumu, sistēmu vai produktu aizstāšanu, kas atzīti par augsta riska pakalpojumiem, sistēmām vai produktiem saskaņā ar koordinētajiem piegādes ķēdes riska novērtējumiem nākotnē.

24. ATZĪST, ka IKT pakalpojumu globalizācija un specializācija un arvien pieaugošā atkarība no trešo personu produktiem un pakalpojumiem nozīmē, ka ES iekšienē un starptautiskā mērogā ir jānotiek ciešai sadarbībai zināšanu un zinātības apmaiņas jomā starp attiecīgajām ieinteresētajām personām, un MUDINA tās rast spēcīgu un koordinētu nostāju attiecībā uz IKT piegādes ķēdes drošības panākšanu visaptverošā veidā. ATZĪST arī to, ka ir vēl vairāk jāpēta attiecīgās mūsdienīgās pieejas un paņēmieni – gan attiecībā uz pienācīgu elementāru kiberhigiēnu, gan uz ilgtermiņa risinājumiem, ar ko panākt drošas un noturīgas IKT piegādes ķēdes, kā arī vispiemērotākie veidi to veicināšanai un iespējamai iestrādāšanai politikā vai citās iniciatīvās. Šajā sakarā ATZĪST, ka īpaša uzmanība būtu jāpievērš tam, lai pētītu priekšrocības un trūkumus tādiem sistemātiskiem risinājumiem kā "nulles uzticības" principi, programmatūras "materiālu komplekts" un līdzīgiem ilgtermiņa risinājumiem. IESAKA šajā nolūkā izmantot TID sadarbības grupu.

25. ATZĪMĒ priekšrocības, ko sniedz informācijas par kiberincidentiem un draudiem monitorings un efektīva apmaiņa nolūkā novērst, konstatēt un mazināt uzbrukumu piegādes ķēdēm sekas. UZSVER, ka šādas informācijas efektīvas apmaiņas nolūkos ir jāturpina vairot uzticību un paļāvību starp dalībvalstīm. šajā sakarā ATGĀDINA Komisijas priekšlikumu atbalstīt dalībvalstis drošības operāciju centru izveidē un stiprināšanā, lai visā ES varētu izveidot drošības operāciju centru tīklu, turpināt pārraudzīt signālus par uzbrukumiem tīkliem un tos prognozēt. ATGĀDINA, ka esošajos tīklos un mehānismos ir vajadzīga papildināmība un koordinācija, šajā sakarā jo īpaši UZSVER *CSIRT* tīkla nozīmi un to, ka šo tīklu potenciāls ir jāpēta vēl vairāk, lai veicinātu efektīvu, drošu un uzticamu informācijas apmaiņas kultūru. 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.

26. Tā kā IKT piegādes ķēžu apdraudējumi pēc sava rakstura ir savstarpēji saistīti un globāli, UZSVER, cik svarīgi ir pievērsties IKT piegādes ķēžu drošībai un to uzlabot globālā līmenī. Ņemot to vērā, nolūkā veicināt uz risku balstītus IKT produktu piegādātāju un IKT pakalpojumu sniedzēju izvērtējumus, uzticamu piegādātāju izmantošanu un drošas un tādas inovatīvas digitālās ekosistēmas lietošanu, kas balstīta atvērtos, sadarbspējīgos un pārredzamos standartos, IESAKA izmantot digitālās partnerības, kiberdialogus un citas attiecīgās ES iniciatīvas, tostarp attiecīgā gadījumā brīvās tirdzniecības nolīgumus. Papildus tam ATKĀRTOTI UZSVER redzējumu par *Global Gateway* partnerībām, kā arī ES un ASV Tirdzniecības un tehnoloģiju padomi un darbībām tās darba grupu paspārnē nolūkā veicināt uzticamu piegādātāju / piegādātāju, kas nav augsta riska piegādātāji, izmantošanu un izstrādāt finansēšanas mehānismu, kura rezultātā būtu iespējami projekti, ar kuriem trešo valstu IKT infrastruktūra un pakalpojumi tiek padarīti drošāki, noturīgāki un uzticamāki, tostarp, atturoties no iepirkumu finansēšanas no neuzticamiem / augsta riska piegādātājiem tehnoloģiski neitrālā veidā.

27. ATKĀRTOTI APSTIPRINA savu apņemšanos sniegt ieguldījumu atvērtā, brīvā, globālā, stabilā un drošā kibertelpā un to veicināt, un ievērot normas, noteikumus un principus attiecībā uz atbildīgu valsts rīcību kibertelpā, kā izklāstīts ANO satvarā. Jo īpaši attiecībā uz IKT piegādes ķēžu drošību ATGĀDINA *UNGGE* un atklātā sastāva darba grupas apstiprināto normu, ar kuru valstis tiek mudinātas veikt saprātīgus pasākumus, lai nodrošinātu piegādes ķēdes integritāti, tostarp, izstrādājot objektīvus sadarbības pasākumus, lai galalietotāji varētu uzticēties IKT produktu drošībai, un censties novērst ļaundabīgu IKT rīku un paņēmienu izplatīšanos un kaitīgu slēptu funkciju izmantošanu, un IESTĀJAS par tās plašu īstenošanu.