Euroopa Liidu
Nõukogu

Brüssel, 17. oktoober 2022
(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

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	17. oktoober 2022
Saaja:	Delegatsioonid
Eelmise dok nr:	12930/22
Teema:	Nõukogu järeldused IKT tarneahela turvalisuse kohta – Nõukogu järeldused, mille nõukogu kiitis heaks 17. oktoobri 2022. aasta istungil

Delegatsioonidele edastatakse lisas 17. oktoobril 2022 toimunud nõukogu istungil heaks kiidetud nõukogu järeldused IKT tarneahela turvalisuse kohta

LISA

Nõukogu järeldused IKT tarneahela turvalisuse kohta

EUROOPA LIIDU NÕUKOGU,

TULETADES MEELDE

– oma järeldusi, mis käsitlevad Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ (20. november 2017);

– oma järeldusi küberturvalisuse alase võimsuse ja suutlikkuse suurendamise kohta ELis;

– oma järeldusi, milles käsitletakse 5G tähendust Euroopa majandusele ning vajadust maandada 5G-ga seotud turvariske;

– oma järeldusi Euroopa digituleviku kujundamise kohta;

– oma järeldusi „Dünaamilisemale, vastupanu- ja konkurentsivõimelisemale Euroopa tööstusele üleminekut edendav taastamine“;

– oma järeldusi ühendatud seadmete küberturvalisuse kohta;

– oma järeldusi, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks;

– oma järeldusi Euroopa Liidu kübervaldkonna positsiooni arendamise kohta;

– oma järeldusi, milles käsitletakse Euroopa Kontrollikoja eriaruannet 03/2022 „5G-võrkude kasutuselevõtt ELis hilineb ja turvaprobleemid on endiselt lahendamata“,

TULETADES MEELDE Euroopa Ülemkogu järeldusi, milles käsitletakse teemasid, nagu:

– COVID-19, ühtne turg, tööstuspoliitika ja digiaspektid ning välissuhted (1. ja 2. oktoober 2020);

– Venemaa sõjaline agressioon Ukraina vastu, julgeolek ja kaitse, energeetika, majandusküsimused, COVID-19 ning välissuhted (24. ja 25. märts 2022);

– Ukraina, toiduga kindlustatus, julgeolek ja kaitse ning energeetika (30. ja 31. mai 2022);

1. võttes arvesse geopoliitika kasvavat tähtsust küberturvalisuse jaoks, RÕHUTAB, et Euroopa Liit ja selle liikmesriigid peavad käsitlema küberturvalisust terviklikul ja strateegilisel viisil. Venemaa sõjaline agressioon Ukraina vastu on põhjustanud olulise muutuse Euroopa Liidu strateegilises ja julgeolekukeskkonnas ning on näidanud vajadust tugevama ja võimekama Euroopa Liidu järele julgeoleku ja kaitse valdkonnas. See on näidanud, kuivõrd üliolulineon võtta geopoliitilist keskkonda asjakohaselt arvesse mitte ainult pahatahtlikule kübertegevusele reageerimisel, vaid ka info- ja kommunikatsioonitehnoloogia (IKT) vastupidavuse loomisel ja säilitamisel. See on eriti oluline IKT-toodete ja -teenuste tarneahelate puhul (IKT tarneahelad), mida võib ohustada nii geopoliitiline rivaalitsemine, mida näitlikustab SolarWinds'i rünne, kui ka geopoliitilised pinged ja ebastabiilsus, mille näiteks on oht sõltuda Venemaa Ukraina-vastase sõjalise agressiooni ajal Venemaa IKT-tarnijatest;

2. MÄRGIB, et need riskid, mida seostatakse IKT tarneahelaga, mis koosneb ettevõtjate (nagu määratletud määruses (EL) 2019/1020) vahelistest seotud ressurssidest ja protsessidest ja algab tooraine hankimisega ning jätkub IKT-toodete ja -teenuste tootmise, töötlemise, käitlemise ja kättetoimetamisega, sealhulgas toe pakkumisega IKT-toodete ja -teenuste olelusringi jooksul, on sedalaadi, mis toovad kaasa ainulaadseid väljakutseid ja potentsiaalselt kaugeleulatuvaid tagajärgi. Lisaks IKT-toodete kättesaamatusega seotud riskidele, näiteks nende tootmiseks vajalike kriitilise tähtsusega toorainete ja pooljuhtide nappus, ähvardavad IKT-toodete ja -teenuste tarneahelaid ka muud ohud. Eelkõige võivad pahatahtlikud osalejad neid sihikule võtta või väärkasutada keerukal ja sageli varjatud viisil, mis mõjutab edastatud ja talletatud tundlike andmete konfidentsiaalsust, terviklust ja kättesaadavust;

3. tunnistades, et IKT varade kindlustamisel on vaja kasutada kõiki ohte hõlmavat lähenemisviisi, TUNNUSTAB kriitilise tähtsusega üksuste vastupidavusvõime direktiivi ettepaneku asjakohasust kriitilise tähtsusega üksuste füüsilise julgeoleku parandamisel ning RÕHUTAB, et tarneahelate küberrünnetele vastupidavuse suurendamise kõrval on sama oluline tugevdada IKT tarneahelate üldist vastupidavust ja kindlustatust mitmesuguste ohutegurite suhtes, nagu loodusnähtused, süsteemirikked, siseohud või inimlikud eksimused; sellega seoses TUNNISTAB, et IKT tarneahela turvalisus hõlmab IKT tarneahelates toodetavate, tarnitavate, hangitavate ja kasutatavate IKT-toodete ja -teenuste kaitsmise tagamist, sealhulgas üksikute komponentide ja edastatud andmete kaitsmise kaudu;

4. tuginedes sellele, mida oleme õppinud tagajärgedest, mida on toonud Euroopa Liidu strateegiline sõltuvus Venemaa fossiilkütustest, ning mõjust, mida avaldasid COVID-19 pandeemia aegsed tarneahelate häired, eelkõige seoses ravimite ja pooljuhtidega, ja mis paljastasid ELi strateegilise sõltuvuse, INNUSTAB liikmesriike tegema tööd selle nimel, et vältida sarnaseid soovimatuid strateegilisi sõltuvusi välistest tarnijatest IKT-toodete ja -teenuste puhul. Võttes arvesse ühiskonna üha ulatuslikumat digiüleminekut ja IKT üha laialdasemat kasutamist elutähtsas taristus, tuleks IKT-toodete ja -teenuste ning nende tarneahelatega seotud strateegilist välistest tarnijatest sõltumist pidevalt hinnata ja vajaduse korral selle probleemiga tegeleda;

5. TULETAB MEELDE, et strateegilise autonoomia saavutamine käsikäes avatud majanduse säilitamisega on üks liidu põhieesmärke, mis hõlmab strateegiliste sõltuvuste kindlakstegemist ja vähendamist ning vastupidavuse suurendamist kõige tundlikumates tööstusökosüsteemides ja konkreetsetes valdkondades, sealhulgas digivaldkonnas. See hõlmab strateegilise digivõimekuse ja -taristu arendamist ja kasutuselevõttu, samuti iseseisvate tehnoloogiliste valikute tegemise suutlikkuse suurendamist ning ühe peamise sambana vastupidavate ja turvaliste taristute, toodete ja teenuste tagamist, et suurendada usaldust digitaalse ühtse turu ja Euroopa ühiskonna vastu, ning seejuures avatuse säilitamist, ülemaailmse koostöö jätkamist sarnaselt meelestatud partneritega ja konkurentsivõime alahoidmist ning nendest tulenevate potentsiaalsete eeliste ärakasutamist. Euroopa Liidu põhiväärtused hõlmavad eelkõige privaatsuse, turvalisuse, võrdsuse, inimväärikuse, õigusriigi põhimõtet ning avatud internetti kui digitaalse inimkeskse ühiskonna, majanduse ja tööstuseni jõudmise eeldusi;

6. MÄRGIB, et küberohtude maastikul toimuvate sündmuste tõttu, mida ilmestavad viimastel aastatel aset leidnud väga mõjusad ja keerukad tarneahelaründed (näiteks ründed nimega SolarWinds, Mimecast ja Kaseya), mille esiletõusu aeg langeb kokku oluliste IKT-teenuste allhangete tegemisega ning mida süvendab üldine sõltuvus kolmandate isikute toodetavatest ja pakutavatest IKT-toodetest ja/või nende osutatavatest IKT-teenustest, on tulevikus väga tõenäoline, et esineb rohkem tarneahelaründeid, mis kahjustavad oluliselt majandust ja ühiskonda; RÕHUTAB seda arvesse võttes IKT tarneahelate turvalisuse ja vastupidavuse suurendamise tähtsust ühtse turu toimimise jaoks ning vajadust tagada IKT-toodete ja -teenuste kättesaadavus, turvalisus ja mitmekesisus ühtsel turul; seetõttu TUNNISTAB vajadust maksimeerida ja ühtlustada olemasolevate ELi vahendite ja lähenemisviiside kasutamist nende eesmärkide saavutamiseks, samuti vajadust pidevalt kohaneda muutuvate küberohtudega, võttes kasutusele täiendavad sobivad meetmed ja mehhanismid, sealhulgas seoses kujunemisjärgus ja lõhkuvate tehnoloogiate võimalike turvariskidega; JULGUSTAB liikmesriike järgima sellega seoses riskipõhist lähenemisviisi, et tulla toime uue tehnoloogia arenguga;

7. TUNNISTAB, et IKT tarneahelatega seotud riskide tõhusaks maandamiseks on oluline mõista pidevalt muutuvat küberohtude maastikku ja tarneahela rünnete keerukust; RÕHUTAB sellega seoses vajadust kohaneda uute ohtudega, jälgides, analüüsides ja hinnates aktiivselt ja pidevalt tarneahelat ähvardavate ohtude maastikku, et suurendada teadlikkust ohtudest ja nõrkadest kohtadest ning koguda nende kohta teadmisi ning hoiatada asjaomaseid üksusi ennetavalt ja kohandatud viisil, PEAB TERVITATAVAKS Euroopa Liidu Küberturvalisuse Ameti (ENISA) tööd IKT tarneahela turvalisuse valdkonnas, eelkõige ameti aruannet tarneahelarünnetega seotud ohuolukorra kohta,

VALDKONNAÜLESED VAHENDID JA LÄHENEMISVIISID

8. KINNITAB TAAS, kui oluline on, et liikmesriigid kaaluksid vajadust mitmekesistada kriitilise tähtsusega IKT tarnijaid, et vältida või piirata suure sõltuvuse tekkimist üksikutest tarnijatest, eelkõige suure riskiga tarnijatest, kuna see suurendab haavatavust seoses võimalike häirete tagajärgedega; TUNNISTAB, et müüjatest sõltuvuse vältimine ja IKT-teenuste osutajate mitmekesistamine on siseturu stabiilsuse ja turvalisuse tagamise üks olulisi komponente; TÕSTAB ESILE vajadust edendada ja rakendada asjakohaseid strateegiaid, mis hõlbustavad müüjate mitmekesistamist ja konkurentsivõime suurendamist tehnoloogianeutraalsel viisil; INNUSTAB ka lisama ELi õigusaktidesse aspekte, mis seonduvad müüjatest sõltuvuse vältimisega; VÕTAB sellega seoses TEADMISEKS ettepaneku võtta vastu määrus ühtlustatud õigusnormide kohta, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist (andmealane õigusakt), mille eesmärk on suurendada andmetöötlusteenuste koostalitlusvõimet ja kõrvaldada takistused andmetöötlusteenuste osutajate vahetamisel;

9. TUNNISTAB IKT tarneahela turvalisuse seost riigihangetega; RÕHUTAB vajadust, et riigihankemenetlustes võetaks piisavalt arvesse IKT tarneahela turvalisuse tähtsust, kehtestades vajaduse korral objektiivsed ja riskipõhised valikukriteeriumid, mis on seotud pakkujate suutlikkusega tagada osutatavate teenuste turvalisuse kõrge tase; ESITAB ÜLESKUTSE leida õige tasakaal ühelt poolt avaliku sektori vahendite kõige tõhusama ja õiglasema kasutamise avaliku huvi ning teiselt poolt infosüsteemide turvalisuse ja ühtse turu sujuva toimimise tagamise avaliku huvi vahel; selleks et hõlbustada asjakohaste riigihanke-eeskirjade rakendamist, pidades silmas küberturvalisuse suurenemist, KUTSUB komisjoni ÜLES töötama 2023. aasta kolmandaks kvartaliks välja metoodilised suunised, et julgustada avaliku sektori hankijaid pöörama asjakohast tähelepanu pakkujate ja nende alltöövõtjate küberturvalisuse tavadele ning hindama asjakohaseid riigihankealaseid õigusakte ja vajaduse korral esitama ettepanekuid nende läbivaatamiseks või täiendamiseks;

10. VÕTAB TEADMISEKS, et IKT-toodete ja -teenustega seotud välismaised otseinvesteeringud, mis annavad liikmesriikidele, ettevõtjatele ja kodanikele majanduslikku ja sotsiaalset kasu, võivad hõlmata julgeoleku ja avaliku korraga seotud riske, ning MÄRGIB, et ELi välismaiste otseinvesteeringute taustauuringumehhanismi koos vastavate riiklike taustauuringusüsteemidega, mis pakuvad vahendeid selliste riskidega tegelemiseks, võiks samuti rakendada kasuliku vahendina IKT tarneahela turvalisuse ja vastupidavuse tagamiseks, aidates kõrvaldada suure riskiga investeeringuid, mis võivad mõjutada sellist turvalisust ja vastupidavust; TUNNISTAB, et selle mehhanismi kaudu vahetatav ja jagatav teave võib aidata liikmesriikidel paremini hinnata võimalikke ohte IKT tarneahelate turvalisusele ja võtta vastavalt vajalikke meetmeid; KUTSUB asjaomaseid riiklikke osalejaid ÜLES võtma vajaduse korral arvesse ka taustauuringumehhanismi seda mõõdet;

11. KINNITAB sellega seoses TAAS enda poolt komisjonile esitatud üleskutset hinnata 2023. aastal koos liikmesriikidega ELi julgeoleku- ja kaitsehuvidega seotud riske, mis ohustavad elutähtsa taristu tarneahelaid eri valdkondades, sealhulgas digivaldkonnas, ning uurida võimalusi küberturvalisuse suurendamiseks kogu ELi kaitsesektori tehnoloogilise ja tööstusliku baasi tarneahelas; KUTSUB lisaks liikmesriike ja komisjoni ÜLES analüüsima IKT tarneahela turvalisust strateegilise kompassi kohustuste ja meetmete rakendamisel;

12. tunnistades kriitilise tähtsusega toorainete ja igat liiki pooljuhtide tähtsust IKT-toodete põhielementidena, INNUSTAB pidama konstruktiivseid läbirääkimisi määruse ettepaneku üle, millega kehtestatakse meetmete raamistik Euroopa pooljuhiökosüsteemi tugevdamiseks (kiibimäärus), ja ettepaneku üle võtta vastu nõukogu määrus, millega muudetakse määrust (EL) 2021/2085 (millega luuakse ühisettevõtted programmi „Euroopa horisont“ raames) seoses kiipide ühisettevõttega;

KÜBERVALDKONNA VAHENDID

13. pidades eelkõige silmas telekommunikatsioonitaristut, TUNNISTAB liidu tasandil tehtud edusamme 5G-võrkude tarneahela turvalisuse parandamisel, eelkõige 5G turvalisuse ELi meetmepaketi (ELi 5G meetmepakett) kaudu; KUTSUB liikmesriike ÜLES täiendavalt vahetama teavet ELi 5G meetmepaketis soovitatud meetmete rakendamise parimate tavade ja meetodite kohta ning eelkõige kohaldama vajaduse korral ELi koordineeritud riskihindamises kriitilise tähtsusega ja tundlikena määratletud põhivarade puhul asjakohaseid piiranguid suure riskiga tarnijate suhtes; TOONITAB, et ELi 5G meetmepakett on paindlik riskipõhine vahend tuvastatud turvaprobleemide lahendamiseks, mis võimaldab käsitleda 5G küberturvalisuse aspekte õigeaegselt ja tõhusalt, austades samal ajal liikmesriikide pädevusi, ning TUNNISTAB, et see on väärtuslik vahend telekommunikatsioonivõrkude tarneahela turvalisuse täiendavaks koordineeritud ja täielikult läbipaistvaks suurendamiseks viisil, mis võib olla inspiratsiooniks muude elutähtsate sektoritega seotud riskihindamis- ja leevendamisvahendite puhul; TULETAB MEELDE asjaomaste ametiasutuste üleskutset sõnastada riskihindamisel põhinevad soovitused liikmesriikidele ja komisjonile, et tugevdada vastupidavust suurendavaid sidevõrke ja -taristuid Euroopa Liidus, sealhulgas jätkata ELi 5G meetmepaketi rakendamist;

14. MÄRGIB, kui olulised on koostalitlusvõimelised lähenemisviisid, mis võivad käsitleda müüjatest sõltuvust ja vähendada kontsentratsiooniriski, parandades samal ajal tarneahela turvalisust kogu IKT-taristu ja -teenuste spektri ulatuses; TUNNISTAB eelkõige 5G-võrkudega seoses avatud raadio juurdepääsuvõrgu kontseptsiooni võimalikku kasu ning TULETAB samal ajal MEELDE võrgu- ja infoturbe koostöörühma avaldatud aruannet avatud raadio juurdepääsuvõrgu küberturvalisuse kohta, milles märgiti, et see kontseptsioon on alles väljatöötamisel ning selle turvalisus, läbipaistvus ja standardimine on varases küpsusjärgus, ning RÕHUTAB, kui oluline on hinnata riske enne mis tahes üleminekut uutele standarditele või struktuuridele;

15. TOONITAB, kui olulised on IKT tarneahela turvalisuse suurendamiseks kehtivad ja tulevased horisontaalsed küberturvalisuse õigusaktid, eelkõige määrus, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist (küberturvalisuse määrus), tulevane direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse 2. direktiiv), ettepanek võtta vastu määrus, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes, ning ettepanek võtta vastu määrus digielementidega toodete horisontaalsete küberturvalisuse nõuete kohta (küberkerksuse õigusakt); MÄRGIB lisaks olulisi arenguid valdkondlikes küberturvalisuse määrustes, eelkõige tulevases määruses, mis käsitleb finantssektori digitaalset tegevuskerksust (DORA), mis sisaldab järelevalveraamistikku finantssektori ettevõtjate jaoks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle; nende määrustega kehtestatakse tarneahela turvalisusega seotud üldised kohustused ning asjaomase sektori jaoks asjakohased üksikasjalikud ja konkreetsed nõuded; RÕHUTAB samas, et tarnijad pakuvad oma tooteid ja teenuseid sageli eri sektorites, mitte vaid ühele tööstusharule; seetõttu on väga oluline tagada, et tarneahela turvalisuse nõuded oleksid võimalikult suures ulatuses ühtlustatud kõigis asjaomastes sektorites, eelkõige tulevase küberturvalisuse 2. direktiiviga hõlmatud sektorites, et vältida lahknevusi tarnijatele kehtestatud kohustuste vahel ja vähendada kriitilise tähtsusega sektorite operaatorite koormust hinnata tarnijate vastavust nendele kohustustele, võttes samal ajal arvesse sektorite eripära;

16. TERVITAB küberkerksuse õigusakti ettepanekut, mis on oluline õigusakt digielementidega toodete turvalise arendamise edendamiseks ja selle tagamiseks, et küberturvalisust võetakse arvesse digielementidega toodete kogu olelusringis; MÄRGIB, et küberkerksuse õigusakti ettepanek võib märkimisväärselt kaasa aidata IKT tarneahela turvalisuse tugevdamisele; INNUSTAB pidama konstruktiivseid läbirääkimisi ja võtma akt õigeaegselt vastu;

17. TUNNISTAB sellega seoses, et ENISA juhtimisel toimub koos liikmesriikide ja muude sidusrühmadega töö selle nimel, et kooskõlas küberturvalisuse määrusega koostada ELi jaoks IKT-toodete, -teenuste ja -protsesside sertifitseerimiskavad, mis peaksid aitama kaasa üldise küberturvalisuse taseme tõstmisele digitaalsel ühtsel turul; INNUSTAB kõiki sidusrühmi osalema konkreetsete Euroopa sertifitseerimiskavadega seotud ettevalmistavas töös, et suurendada usaldust turvaliste IKT-toodete, -protsesside ja -teenuste vastu ning tugevdada nende vastupanuvõimet, ning KUTSUB komisjoni ÜLES pärast ettevalmistava töö lõpuleviimist kiiresti ette valmistama rakendusakte Euroopa sertifitseerimiskavade kohta, eelkõige ühistel kriteeriumidel põhineva Euroopa küberturvalisuse sertifitseerimiskava kohta; MÄRGIB, et Euroopa sertifitseerimiskavad peaksid vajaduse korral sisaldama tarneahela turvalisuse nõudeid, sealhulgas suhteid tarnijatega;

18. TOONITAB vajadust rakendada põhjalikult kõiki tulevasi küberturvalisuse 2. direktiivi sätteid, mis on seotud IKT tarneahela turvalisusega; RÕHUTAB sellega seoses kriitilise tähtsusega tarneahelate ELi koordineeritud riskihindamise (koordineeritud tarneahela riskihindamised), tarneahela turvalisust käsitleva riikliku poliitika ja tarneahelaga seotud turvameetmete asjakohasust; MÄRGIB, et seoses riskidega põhitarnija või lõpptarbija turvalisusele tuleks tähelepanu pöörata mitte ainult esmastele tarnijatele, vaid ka asjaomastele alltöövõtjatele; INNUSTAB tarneahela riskijuhtimismeetmete rakendamise hõlbustamise eesmärgil ENISAt tegema võrgu- ja infoturbe koostöörühma abiga kokkuvõtte tarneahela riskijuhtimiseks kättesaadavatest parimatest tavadest ja koondama need metoodilisteks suunisteks; INNUSTAB lisaks ENISAt jälgima investeeringuid IKT tarneahela turvalisusesse üksustes, mida reguleeritakse tulevase NIS2 direktiiviga;

19. TOONITAB ka kasu ja riske, mis kaasnevad hallatud teenuste osutajate ja hallatud turbetarnijate kasutamisega tarneahela turvalisuse kontekstis; kuigi nende kasutamine võib oluliselt parandada organisatsioonisisest turvalisust ja suurendada küberturvalisust, võib IKT-süsteemide ja -teenuste kaugjuhtimine koos privilegeeritud juurdepääsuga klientide IKT-keskkonnale, mida hallatud teenuste osutajad ja hallatud turbetarnijad võivad vajada, põhjustada nõudeid mittetäitvate hallatud teenuste osutajate ja hallatud turbetarnijate puhul ahelreaktsioonina avalduva suure mõju suurele hulgale klientidele; seetõttu on äärmiselt oluline, et hallatud teenuste osutajad ja hallatud turbetarnijad säilitaksid oma siseturvalisuse ja nende osutatavate teenuste turvalisuse kõrge taseme ning järgiksid oma klientide suhtes läbipaistvat lähenemisviisi seoses nende osutatavate teenuste turvalisusega; TERVITAB sellega seoses nende tulevast lisamist kavandatava küberturvalisuse 2. direktiivi kohaldamisalasse;

20. seoses tarneahela koordineeritud riskihindamise mehhanismi rakendamisega tulevase küberturvalisuse 2. direktiivi kohaselt MÄRGIB mittetehniliste riskitegurite asjakohasust, nagu kolmanda riigi lubamatu mõju tarnijatele ja teenuseosutajatele, ning TUNNISTAB sellega seoses tegureid, mida saab kasutada 5G-võrkude küberturvalisuse ELi koordineeritud riskihindamises nimetatud riskiprofiili hindamiseks; KUTSUB komisjoni ÜLES määrama 2023. aasta teiseks kvartaliks pärast võrgu- ja infoturbe koostöörühma ja ENISAga konsulteerimist kindlaks konkreetsed IKT-teenused, -süsteemid või -tooted, mille suhtes võidakse esmajärjekorras kohaldada tarneahela koordineeritud riskihindamisi;

21. MÄRGIB, et sõltuvus kriitilise tähtsusega võrkude ja süsteemide käitamiseks kasutatavate IKT-toodete ja -teenuste suure riskiga tarnijatest kujutab endast strateegilist ohtu, mida tuleb leevendada asjakohase poliitika abil nii riiklikul kui ka ELi tasandil ning liikmesriikide vahelise ja sarnaselt meelestatud rahvusvaheliste partneritega tehtava koostöö kaudu; hõlbustamaks selle strateegilise riski maandamist ja toetamaks tarneahela koordineeritud riskihindamist, KUTSUB võrgu- ja infoturbe koostöörühma ÜLES töötama koostöös komisjoni ja ENISAga välja meetmepaketi IKT tarneahela kriitilise tähtsusega riskide vähendamiseks (IKT tarneahela meetmepakett). IKT tarneahela meetmepakett peaks tuginema IKT tarneahelate puhul kindlaks tehtud strateegilise ohu stsenaariumidele ja pakkuma meetmeid nendele stsenaariumidele reageerimiseks, võimendades 5G meetmepaketist ja riiklikul tasandil saadud kogemusi. Meetmepakett peaks läbipaistval viisil täiendama konkreetsete IKT-teenuste, -süsteemide või -toodete tarneahela koordineeritud riskihindamist tulevase küberturvalisuse 2. direktiivi alusel, pakkudes üldisi meetmeid riskide vähendamiseks, mida saab konkreetsete IKT-teenuste, -süsteemide või -toodete puhul skaleeritaval viisil kohandada, lähtudes individuaalsete tarneahela koordineeritud riskihindamiste käigus kindlaks tehtud riskidest;

22. RÕHUTAB teadusuuringute, innovatsiooni, investeeringute ja ettevõtluse olulist rolli digi- ja küberturvalisuse valdkonnas, samuti sellise tegevuse rahastamise olulist rolli, pidades silmas võimalike tulevaste soovimatute strateegiliste sõltuvuste vältimist ja IKT tarneahelate üldise vastupidavuse tugevdamist; TOONITAB sellega seoses küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (ECCC) ning riiklike koordineerimiskeskuste võrgustiku täidetavate strateegiliste ja rakendusülesannete rolli ja asjakohasust investeeringute mõju maksimeerimisel, et tugevdada liidu juhtpositsiooni ja avatud strateegilist autonoomiat küberturvalisuse valdkonnas ning toetada liidu tehnoloogilist suutlikkust ja oskusi ning suurendada liidu ülemaailmset konkurentsivõimet; KUTSUB sellega seoses ÜLES ECCC-d kiiresti käivitama; KUTSUB ECCC-d ÜLES võtma oma strateegilises tegevuskavas arvesse IKT tarneahela turvalisuse aspekte, sealhulgas näiteks tarkvara turvalist arendamist, tagades samal ajal järjepidevuse ja vastastikuse täiendavuse ning vältides jõupingutuste dubleerimist; TOETAB küberturvalisuse valdkonnas Euroopa konkurentsivõime suurendamist selliste rahastamisprogrammide kaudu nagu teadusuuringute ja innovatsiooni raamprogramm „Euroopa horisont“ ning programm „Digitaalne Euroopa“, mille eesmärk on tugevdada, arendada ja omandada ELi digitaalmajanduse, ühiskonna ja demokraatia jaoks olulist suutlikkust;

TOETUSMEHHANISMID

23. JULGUSTAB suurendama rahalise toetuse stiimuleid, mis on seotud IKT tarneahela turvalisuse suurendamise meetmetega; KUTSUB ECCC-d, komisjoni ja asjaomaseid sidusrühmi üles prioriteetse küsimusena uurima, pidades silmas ka küberturvalisuse 2. direktiivi eelseisvat rakendamist, võimalusi IKT tarneahela turvalisuse aspektide lisamiseks tulevastesse projektikonkurssidesse programmi „Digitaalne Euroopa“ ja programmi „Euroopa horisont“ küberturvalisuse tööprogrammide raames või mis tahes muudesse asjakohastesse rahastamisvõimalustesse. Nende rahastamisvõimaluste eesmärk peaks muu hulgas olema võimaldada organisatsioonidel toetada küberturvalisuse kõrge taseme säilitamist IKT-toodete ja -teenuste hankimisel kogu tarneahelas, eelkõige seoses konkreetsete kriitilise tähtsusega IKT-teenuste, -süsteemide või -toodete asendamisega, mille puhul peetakse riski suureks vastavalt tulevastele tarneahela koordineeritud riskihindamistele;

24. TUNNISTAB, et üleilmastumisega ja IKT-teenuste spetsialiseerumisega ning suurema sõltuvusega kolmandate isikute toodetest ja teenustest kaasneb vajadus teha ELis ja rahvusvahelisel tasandil tihedat koostööd teadmiste ja eksperditeadmiste jagamiseks asjaomaste sidusrühmade vahel, ning INNUSTAB neid leidma tugevat ja koordineeritud positsiooni, millega tagatakse IKT tarneahela turvalisus terviklikul viisil; TUNNISTAB samuti vajadust täiendavalt uurida asjakohaseid tipptasemel lähenemisviise ja meetodeid seoses nii asjakohase elementaarse küberhügieeniga kui ka pikaajaliste lahendustega turvaliste ja vastupidavate IKT tarneahelate kujundamiseks, samuti kõige sobivamaid viise nende edendamiseks ja võimalikuks kaasamiseks poliitikameetmetesse või muudesse algatustesse; TÕDEB sellega seoses, et eriti hoolikalt tuleks uurida eeliseid ja puudusi, mis on seotud selliste süstemaatiliste lahendustega nagu usaldamatuse põhimõtted, tarkvaramaterjalide loetelu ja sarnased pikaajalised lahendused; SOOVITAB sel eesmärgil kasutada võrgu- ja infoturbe koostöörühma;

25. MÄRGIB, et küberintsidente ja -ohte käsitleva teabe seirest ja tõhusast jagamisest on kasu tarneahela rünnete ennetamisel, avastamisel ja leevendamisel; RÕHUTAB vajadust jätkata liikmesriikide vahelise usalduse ja kindlustunde suurendamist seoses sellise teabe tõhusa jagamisega; MEENUTAB sellega seoses komisjoni ettepanekut toetada liikmesriike infoturbekeskuste loomisel ja tugevdamisel, et luua kogu ELis infoturbekeskuste võrgustik, et täiendavalt jälgida ja prognoosida signaale võrgustike vastu suunatud rünnete kohta; TULETAB MEELDE vajadust vastastikuse täiendavuse ja koordineerimise järele olemasolevate võrgustike ja mehhanismide puhul ning RÕHUTAB sellega seoses eelkõige küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustiku rolli ja vajadust uurida täiendavalt nende võrgustike potentsiaali tõhusa, turvalise ja usaldusväärse teabejagamiskultuuri edendamiseks; MEENUTAB ELi toetusel tehtud liikmesriikide jõupingutusi valdkondlike, riiklike ja piirkondlike CSIRTide ning teabe jagamise ja analüüsimise riiklike või Euroopa keskuste loomiseks liidu küberturvalisuse partnerluste tõhusa võrgustiku osana;

26. kuna IKT tarneahelaga seotud ohud on omavahel seotud ja üleilmsed, TOONITAB IKT tarneahela turvalisuse ülemaailmsel tasandil käsitlemise ja selle tugevdamise tähtsust; SOOVITAB seda silmas pidades kasutada digipartnerlusi, küberdialooge ja muid asjakohaseid ELi algatusi, sealhulgas vajaduse korral vabakaubanduslepinguid, et edendada IKT-toodete tarnijate ja IKT-teenuste osutajate riskipõhist hindamist, usaldusväärsete tarnijate kasutamist ning avatud, koostalitlusvõimelistel ja läbipaistvatel standarditel põhineva turvalise ja uuendusliku digitaalse ökosüsteemi kasutuselevõttu; KORDAB lisaks visiooni Global Gateway partnerlustest ning ELi-USA kaubandus- ja tehnoloogianõukogust ning selle töörühmade raames toimuvast tegevusest, mille eesmärk on edendada usaldusväärsete ja muude kui suure riskiga tarnijate kasutamist ning töötada välja rahastamismehhanism, et võimaldada projekte, mis muudavad kolmandate riikide IKT taristu ja -teenused turvalisemaks, vastupidavamaks ja usaldusväärsemaks, sealhulgas hoidudes tehnoloogianeutraalsel viisil rahastamast oste ebausaldusväärsetelt ja suure riskiga tarnijatelt;

27. KINNITAB TAAS oma pühendumust avatud, vaba, ülemaailmse, stabiilse ja turvalise küberruumi toetamisele ja edendamisele ning ÜRO raamistikus sätestatud riikide vastutustundlikku küberruumis käitumist käsitlevate normide, reeglite ja põhimõtete järgimisele; TULETAB eelkõige seoses IKT tarneahela turvalisusega MEELDE ÜRO valitsusekspertide rühma ja tähtajata töörühma poolt heaks kiidetud normi, milles julgustatakse riike võtma mõistlikke meetmeid, et tagada tarneahela terviklikkus, sealhulgas töötades välja objektiivsed koostöömeetmed, et lõppkasutajad saaksid olla kindlad IKT-toodete turvalisuses, ning püüda ära hoida IKT-kahjurvahendite ja -kahjurtehnoloogia levikut ning kahjulike varjatud funktsioonide kasutamist, ning POOLDAB selle normi laialdast rakendamist.