Euroopan unionin
neuvosto

Bryssel, 17. lokakuuta 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

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	17. lokakuuta 2022
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	12930/22
Asia:	Neuvoston päätelmät tieto- ja viestintäteknisen toimitusketjun turvallisuudesta – Neuvoston istunnossaan 17. lokakuuta 2022 hyväksymät neuvoston päätelmät

Valtuuskunnille toimitetaan liitteessä neuvoston istunnossaan 17. lokakuuta 2022 hyväksymät neuvoston päätelmät tieto- ja viestintäteknisen toimitusketjun turvallisuudesta.

LIITE

Neuvoston päätelmät tieto- ja viestintäteknisen toimitusketjun turvallisuudesta

EUROOPAN UNIONIN NEUVOSTO, joka

PALAUTTAA MIELEEN päätelmänsä

– yhteisestä tiedonannosta Euroopan parlamentille ja neuvostolle "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle", 20. marraskuuta 2017,

– kyberturvallisuusvalmiuksista ja suorituskykyjen kehittämisestä EU:ssa,

– 5G:n merkityksestä Euroopan taloudelle ja tarpeesta lieventää 5G:hen liittyviä turvallisuusriskejä,

– Euroopan digitaalisen tulevaisuuden rakentamisesta,

– Euroopan teollisuuden dynaamisuuden, kestokyvyn ja kilpailukyvyn paranemista edistävästä elpymisestä,

– internetiin yhdistettyjen laitteiden kyberturvallisuudesta,

– EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle,

– Euroopan unionin kybertoimien kehittämisestä,

– Euroopan tilintarkastustuomioistuimen erityiskertomuksesta nro 03/2022: ”5G-verkot EU:ssa: viiveitä käyttöönotossa ja ratkaisemattomia turvallisuusongelmia”;

PALAUTTAA MIELEEN Eurooppa-neuvoston päätelmät

– covid-19:stä, sisämarkkinoista, teollisuuspolitiikasta, digitaaliasioista ja ulkosuhteista (1.–2. lokakuuta 2020),

– Venäjän sotilaallisesta hyökkäyksestä Ukrainaan, turvallisuudesta ja puolustuksesta, energiasta, talouskysymyksistä, covid-19:stä ja ulkosuhteista (24.–25. maaliskuuta 2022),

– Ukrainasta, ruokaturvasta, turvallisuudesta ja puolustuksesta sekä energiasta (30.–31. toukokuuta 2022);

1. Ottaen huomioon geopolitiikan kasvavan merkityksen kyberturvallisuuden kannalta KOROSTAA, että Euroopan unionin ja sen jäsenvaltioiden on lähestyttävä kyberturvallisuutta kokonaisvaltaisella ja strategisella tavalla. Venäjän sotilaallinen hyökkäys Ukrainaa vastaan on aiheuttanut merkittävän muutoksen Euroopan unionin strategisessa ja turvallisuusympäristössä ja osoittanut, että turvallisuuden ja puolustuksen alalla tarvitaan vahvempi ja toimintakykyisempi Euroopan unioni. Se on tuonut esiin, että on äärimmäisen tärkeää ottaa asianmukaisesti huomioon geopoliittinen ympäristö paitsi vastattaessa haitallisiin kybertoimiin myös kehitettäessä ja ylläpidettäessä tieto- ja viestintätekniikan häiriönsietokykyä. Tämä on erityisen tärkeää tieto- ja viestintätekniikan tuotteiden ja palvelujen toimitusketjuissa, jäljempänä ’tieto- ja viestintätekniikan toimitusketjut’, jotka saattavat sekä vaarantua geopoliittisen kilpailun vuoksi, kuten SolarWinds-isku osoitti, että olla alttiina geopoliittisille jännitteille ja epävakaudelle, mistä osoituksena on uhka, joka liittyy riippuvuuteen venäläisistä tieto- ja viestintätekniikan myyjistä Venäjän Ukrainaan kohdistaman sotilaallisen hyökkäyksen aikana.

2. TOTEAA, että tieto- ja viestintätekniikan toimitusketjuun, joka koostuu (asetuksessa (EU) 2019/1020 määriteltyjen) talouden toimijoiden välisistä resursseista ja prosesseista ja joka alkaa raaka-aineiden hankinnasta ja kattaa tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistuksen, jalostuksen, käsittelyn ja toimittamisen, mukaan lukien tuen tarjoaminen tieto- ja viestintätekniikan tuotteiden ja palvelujen elinkaaren aikana, liittyvien riskien luonne aiheuttaa ainutlaatuisia haasteita ja mahdollisesti kauaskantoisia seurauksia. Niiden riskien lisäksi, jotka liittyvät siihen, että tieto- ja viestintätekniikan tuotteita ei ole saatavilla esimerkiksi siksi, että niiden tuotannossa tarvittavista kriittisistä raaka-aineista ja puolijohteista on pulaa, tieto- ja viestintätekniikan tuotteiden ja palvelujen toimitusketjut ovat myös alttiina muille uhkille. Pahantahtoiset toimijat voivat erityisesti kohdistaa niihin hyökkäyksiä tai käyttää niitä väärin kehittyneillä ja usein vaivihkaisilla tavoilla, jotka vaikuttavat lähetettyjen ja tallennettujen arkaluonteisten tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen.

3. Tunnustaen, että tieto- ja viestintäteknisen omaisuuden turvaamisessa tarvitaan kaikki vaarat kattavaa lähestymistapaa, TOTEAA, että ehdotus kriittisten yksiköiden häiriönsietokykyä koskevaksi direktiiviksi on merkityksellinen kriittisten toimijoiden fyysisen turvallisuuden parantamiseksi, ja KOROSTAA, että sen lisäksi, että on parannettava kykyä selviytyä toimitusketjuihin kohdistuvista kyberhyökkäyksistä, on myös yhtä tärkeää vahvistaa tieto- ja viestintätekniikan toimitusketjujen yleistä häiriönsietokykyä ja turvallisuutta kaikkien uhkatekijöiden, kuten luonnonilmiöiden, järjestelmähäiriöiden, sisäpiiriuhkien tai inhimillisten virheiden, osalta. TOTEAA tässä yhteydessä, että tieto- ja viestintätekniikan toimitusketjun turvallisuuteen kuuluu tieto- ja viestintätekniikan toimitusketjuissa tuotettujen, toimitettujen, hankittujen ja käytettyjen tieto- ja viestintätekniikan tuotteiden ja palvelujen suojaamisen varmistaminen, myös suojaamalla yksittäisiä komponentteja ja siirrettyä dataa.

4. Ottaen huomioon kokemukset seurauksista, joita EU:n strategiset riippuvuudet Venäjän fossiilisista polttoaineista ovat aiheuttaneet, sekä vaikutuksista, joita covid-19-pandemian aikasilla, EU:n strategiset riippuvuudet paljastaneilla toimitusketjujen häiriöillä on ollut erityisesti lääkkeiden ja puolijohteiden osalta, KANNUSTAA jäsenvaltioita pyrkimään välttämään vastaavia tilanteita, joissa tieto- ja viestintätekniikan tuotteisiin ja palveluihin liittyy ei-toivottuja strategisia ulkoisia riippuvuuksia. Koska yhteiskunta digitalisoituu entisestään ja tieto- ja viestintätekniikan tuotteita hyödynnetään jatkuvasti enemmän kriittisissä infrastruktuureissa, tieto- ja viestintätekniikan tuotteisiin ja palveluihin ja niiden toimitusketjuihin liittyviä strategisia ulkoisia riippuvuuksia olisi arvioitava jatkuvasti ja niihin olisi tarvittaessa puututtava.

5. MUISTUTTAA, että strategisen riippumattomuuden saavuttaminen siten, että samalla säilytetään avoin talous, on unionin keskeinen tavoite, johon sisältyy strategisten riippuvuuksien tunnistaminen ja vähentäminen sekä häiriönsietokyvyn parantaminen herkimmissä teollisissa ekosysteemeissä ja tietyillä aloilla, myös digitaalialalla. Tämä edellyttää, että kehitetään ja otetaan käyttöön strategisia digitaalisia valmiuksia ja infrastruktuuria ja vahvistetaan kykyä tehdä autonomisia teknologisia valintoja sekä yhtenä keskeisistä tekijöistä varmistetaan häiriönsietokykyiset ja turvalliset infrastruktuurit, tuotteet ja palvelut, jotta voidaan rakentaa luottamusta digitaalisilla sisämarkkinoilla ja eurooppalaisessa yhteiskunnassa, samalla kun säilytetään avoimuus, maailmanlaajuinen yhteistyö samanmielisten kumppanien kanssa ja kilpailukyky sekä hyödynnetään niiden mahdollisesti tarjoamat hyödyt. Euroopan unionin perusarvoissa vaalitaan erityisesti yksityisyyttä, turvallisuutta, tasa-arvoa, ihmisarvoa, oikeusvaltiota ja avointa internetiä edellytyksinä digitaalivetoiselle ja ihmiskeskeiselle yhteiskunnalle, taloudelle ja teollisuudelle.

6. PANEE MERKILLE, että koska kyberuhkaympäristö on kehittynyt viime vuosina, mistä osoituksena ovat erittäin tehokkaat ja kehittyneet toimitusketjuun kohdistuvat hyökkäykset, kuten SolarWinds-, Mimecast- tai Kaseya-hyökkäykset, jotka liittyvät keskeisten tieto- ja viestintäteknisten palvelujen ulkoistamiseen ja joita voimistaa yleinen riippuvuus kolmansien osapuolten valmistamista, tarjoamista tai ylläpitämistä tieto- ja viestintätekniikan tuotteista ja palveluista, on erittäin todennäköistä, että toimitusketjuihin kohdistuu tulevaisuudessa enemmän hyökkäyksiä, jotka aiheuttavat huomattavaa vahinkoa taloudelle ja yhteiskunnalle. Tämän vuoksi KOROSTAA, että on tärkeää parantaa tieto- ja viestintätekniikan toimitusketjujen turvallisuutta ja häiriönsietokykyä sisämarkkinoiden toiminnan takaamiseksi ja varmistaa tieto- ja viestintätekniikan tuotteiden ja palvelujen saatavuus, turvallisuus ja monipuolisuus sisämarkkinoilla. TOTEAA siksi, että EU:n nykyisten välineiden ja lähestymistapojen käyttö on maksimoitava ja sitä on virtaviivaistettava näiden tavoitteiden saavuttamiseksi, minkä lisäksi on mukauduttava jatkuvasti muuttuvaan kyberuhkaympäristöön ottamalla käyttöön soveltuvia lisätoimia ja -mekanismeja, myös nousevien ja murroksellisten teknologioiden mahdollisiin turvallisuusriskeihin liittyen. KANNUSTAA jäsenvaltioita noudattamaan tässä yhteydessä riskiperusteista lähestymistapaa uuden teknologian kehitykseen vastaamiseksi.

7. TOTEAA, että jatkuvasti kehittyvän kyberuhkaympäristön ja toimitusketjuihin kohdistuvien hyökkäysten monimutkaisuuden ymmärtäminen on olennaisen tärkeää, jotta voidaan tehokkaasti lieventää tieto- ja viestintätekniikan toimitusketjuihin liittyviä riskejä. PAINOTTAA tässä yhteydessä, että on mukauduttava uusiin uhkiin toimitusketjun uhkaympäristön aktiivisella ja jatkuvalla seurannalla, analysoinnilla ja arvioinnilla, lisättävä tietoisuutta ja tietämystä uhkista ja haavoittuvuuksista sekä varoitettava ennakoivasti asianomaisia tahoja räätälöidyllä tavalla. ON TYYTYVÄINEN Euroopan unionin kyberturvallisuusviraston (ENISA) tieto- ja viestintätekniikan toimitusketjun turvallisuuteen liittyvään työhön ja erityisesti sen raporttiin toimitusketjuihin kohdistuvien hyökkäysten uhkaympäristöstä (Threat Landscape for Supply Chain Attacks).

MONIALAISET VÄLINEET JA LÄHESTYMISTAVAT

8. VAHVISTAA, että jäsenvaltioiden on tärkeää harkita kriittisen tieto- ja viestintätekniikan toimittajien monipuolistamista, jotta vältetään suuren riippuvuuden muodostuminen tai rajoitetaan sellaisen muodostumista yksittäisistä toimittajista ja erityisesti suuririskisistä toimittajista, sillä se lisäisi altistumista mahdollisten häiriöiden seurauksille. TOTEAA, että toimittajariippuvuuden välttäminen ja tieto- ja viestintätekniikan toimittajien monipuolistaminen ovat tärkeitä tekijöitä sisämarkkinoiden vakauden ja turvallisuuden varmistamisessa. TÄHDENTÄÄ, että on edistettävä ja toteutettava asianmukaisia strategioita, joilla helpotetaan toimittajien monipuolistamista ja parannetaan kilpailukykyä teknologianeutraalilla tavalla. KANNUSTAA lisäksi sisällyttämään toimittajariippuvuuden ehkäisemiseen liittyvät näkökohdat EU:n lainsäädäntöön. PANEE tässä yhteydessä MERKILLE ehdotuksen asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös), jolla pyritään lisäämään datankäsittelypalvelujen yhteentoimivuutta ja poistamaan esteitä datankäsittelypalvelujen tarjoajan vaihtamiselta.

9. TUNNUSTAA tieto- ja viestintätekniikan toimitusketjun turvallisuuden ja julkisten hankintojen välisen yhteyden. KOROSTAA, että julkisissa hankintamenettelyissä on otettava asianmukaisesti huomioon tieto- ja viestintätekniikan toimitusketjun turvallisuuden merkitys asettamalla tarvittaessa objektiivisia ja riskiperusteisia valintaperusteita, jotka liittyvät tarjoajien kykyyn varmistaa tarjottujen palvelujen korkea turvallisuustaso. KEHOTTAA löytämään oikean tasapainon toisaalta julkisten varojen mahdollisimman tehokasta ja oikeudenmukaista käyttöä koskevan yleisen edun ja toisaalta tietojärjestelmien turvaamista ja sisämarkkinoiden moitteettoman toiminnan varmistamista koskevan yleisen edun välillä. Jotta voidaan helpottaa asiaankuuluvien julkisia hankintoja koskevien sääntöjen täytäntöönpanoa paremman kyberturvallisuuden edistämiseksi, PYYTÄÄ komissiota laatimaan vuoden 2023 kolmanteen neljännekseen mennessä menettelyohjeet, joilla kannustetaan hankintaviranomaisia keskittymään asianmukaisesti tarjoajien ja niiden alihankkijoiden kyberturvallisuuskäytäntöihin, ja arvioimaan asiaankuuluvaa julkisia hankintoja koskevaa lainsäädäntöä ja tarvittaessa tekemään ehdotuksia sen tarkistamiseksi tai täydentämiseksi.

10. TOTEAA, että tieto- ja viestintätekniikan tuotteisiin ja palveluihin liittyvät ulkomaiset suorat sijoitukset, jotka tarjoavat taloudellisia ja sosiaalisia etuja jäsenvaltioille, yrityksille ja kansalaisille, voivat kuitenkin sisältää turvallisuuteen ja yleiseen järjestykseen kohdistuvia riskejä, ja PANEE MERKILLE, että EU:n ulkomaisten suorien sijoitusten seurantamekanismia ja vastaavia kansallisia seurantajärjestelmiä, jotka tarjoavat keinoja puuttua tällaisiin riskeihin, voitaisiin myös hyödyntää välineenä tieto- ja viestintätekniikan toimitusketjun turvallisuuden ja häiriönsietokyvyn turvaamisessa, sillä ne auttavat ehkäisemään sellaisia suuririskisiä investointeja, jotka voivat vaikuttaa kyseiseen turvallisuuteen ja häiriönsietokykyyn. TOTEAA, että tämän mekanismin kautta vaihdetut ja jaetut tiedot voivat auttaa jäsenvaltioita arvioimaan paremmin tieto- ja viestintätekniikan toimitusketjujen turvallisuuteen mahdollisesti kohdistuvia uhkia ja toteuttamaan tarvittavia toimia sen mukaisesti. KEHOTTAA asianomaisia kansallisia toimijoita ottamaan tarvittaessa huomioon myös seurantamekanismin tämän ulottuvuuden.

11. Puolustuksen osalta TOISTAA komissiolle esittämänsä pyyntönsä arvioida yhdessä jäsenvaltioiden kanssa vuonna 2023 EU:n turvallisuus- ja puolustusetuihin liittyviä kriittisen infrastruktuurin toimitusketjuihin kohdistuvia riskejä eri aloilla, myös digitaalialalla, sekä tutkia vaihtoehtoja kyberturvallisuuden lisäämiseksi Euroopan puolustuksen teollisen ja teknologisen perustan koko toimitusketjussa. KEHOTTAA lisäksi jäsenvaltioita ja komissiota pohtimaan tieto- ja viestintätekniikan toimitusketjun turvallisuutta strategisen kompassin sitoumusten ja toimien täytäntöönpanon yhteydessä.

12. Tunnustaen kriittisten raaka-aineiden ja kaikenlaisten puolijohteiden merkityksen tieto- ja viestintätekniikan tuotteiden perusrakenneosina KANNUSTAA rakentaviin neuvotteluihin ehdotuksesta asetukseksi Euroopan puolijohde-ekosysteemiä vahvistavasta toimenpidekehyksestä (sirusäädös) ja ehdotuksesta neuvoston asetukseksi Horisontti Eurooppa -ohjelman yhteisyritysten perustamisesta annetun asetuksen (EU) 2021/2085 muuttamisesta siruyhteisyrityksen osalta.

KYBERALAN VÄLINEET

13. Erityisesti televiestintäinfrastruktuurin osalta TUNNUSTAA unionin tason saavutukset 5G-verkkojen toimitusketjun turvallisuuden parantamisessa, etenkin 5G-kyberturvallisuutta koskevan EU:n välineistön (EU:n 5G-välineistö) avulla. KEHOTTAA jäsenvaltioita jatkamaan tietojen vaihtamista parhaista käytännöistä ja menetelmistä EU:n 5G-välineistössä suositeltujen toimien toteuttamiseksi sekä erityisesti soveltamaan asiaankuuluvia rajoituksia EU:n koordinoidussa riskinarvioinnissa kriittisiksi ja arkaluonteisiksi määriteltyjen keskeisten kohteiden suuririskisiksi katsottuihin toimittajiin. KOROSTAA, että EU:n 5G-kyberturvallisuusvälineistö on joustava riskiperusteinen väline tunnistettuihin turvallisuushaasteisiin vastaamiseksi, mikä mahdollistaa 5G:n kyberturvallisuusnäkökohtien oikea-aikaisen ja tehokkaan käsittelyn kunnioittaen samalla jäsenvaltioiden toimivaltaa, ja TOTEAA, että se on arvokas väline, jolla voidaan täysin avoimesti parantaa televerkkojen toimitusketjun turvallisuutta koordinoidulla tavalla ja joka voisi toimia inspiraationa muille keskeisiin aloihin liittyville riskinarviointi- ja riskien vähentämisvälineille. PALAUTTAA MIELEEN asianomaisten viranomaisten kehotuksen laatia riskinarviointiin perustuvia suosituksia jäsenvaltioille ja komissiolle viestintäverkkojen ja -infrastruktuurien häiriönsietokyvyn vahvistamiseksi Euroopan unionissa, mukaan lukien EU:n 5G-välineistön täytäntöönpanon jatkaminen.

14. TOTEAA, että on tärkeää soveltaa yhteentoimivia lähestymistapoja, joilla voidaan puuttua toimittajariippuvuuteen ja lieventää keskittymäriskiä ja samalla parantaa toimitusketjun turvallisuutta koko tieto- ja viestintätekniikan infrastruktuurin ja palvelujen alalla. Erityisesti 5G-verkkojen yhteydessä TUNNUSTAA Open RAN -tekniikan mahdolliset hyödyt tältä osin ja samalla PALAUTTAA MIELEEN verkko- ja tietoturva-alan yhteistyöryhmän Open RAN -tekniikan kyberturvallisuudesta julkaiseman raportin, jossa todetaan, että kyseistä tekniikkaa vasta kehitetään ja että sen turvallisuus, avoimuus ja standardointi ovat alkuvaiheessa, ja KOROSTAA, että riskejä on tärkeää arvioida ennen siirtymistä uusiin standardeihin tai arkkitehtuureihin.

15. PAINOTTAA nykyisten ja tulevien kyberturvallisuutta koskevien horisontaalisten säädösten merkitystä tieto- ja viestintätekniikan toimitusketjun turvallisuuden lisäämisessä; näitä ovat erityisesti asetus Euroopan unionin kyberturvallisuusvirastosta ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus), tuleva direktiivi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa (NIS 2), ehdotus asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa sekä ehdotus asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista (kyberresilienssisäädös). PANEE lisäksi MERKILLE merkittävän kehityksen alakohtaisten kyberturvallisuusasetusten osalta, erityisesti tulevan finanssialan digitaalista häiriönsietokykyä koskevan asetuksen (DORA), johon sisältyy valvontakehys sellaisia tieto- ja viestintätekniikan palveluntarjoajana olevia kolmansia osapuolia varten, jotka ovat finanssialan yhteisöjen kannalta kriittisiä. Näissä asetuksissa säädetään toimitusketjun turvallisuuteen liittyvistä yleisistä velvoitteista sekä kyseisen alan kannalta merkityksellisistä yksityiskohtaisista ja erityisistä vaatimuksista. TÄHDENTÄÄ samalla, että toimittajat toimittavat tuotteitaan ja palvelujaan usein eri aloille eivätkä vain yhdelle toimialalle. Sen vuoksi on erittäin tärkeää varmistaa, että toimitusketjun turvallisuusvaatimukset ovat mahdollisuuksien mukaan yhdenmukaiset kaikilla asiaankuuluvilla aloilla, erityisesti niillä, jotka kuuluvat tulevan NIS 2 -direktiivin soveltamisalaan, jotta vältetään erot toimittajille asetettujen velvoitteiden välillä ja kevennetään kriittisten alojen toimijoille aiheutuvaa rasitetta sen arvioimisessa, noudattavatko toimittajat näitä velvoitteita, ottaen samalla huomioon alan erityispiirteet.

16. PANEE TYYTYVÄISENÄ MERKILLE kyberresilienssisäädöstä koskevan ehdotuksen tärkeänä lainsäädäntövälineenä, jolla edistetään digitaalisia elementtejä sisältävien tuotteiden turvallista kehittämistä ja varmistetaan, että kyberturvallisuus otetaan huomioon digitaalisia elementtejä sisältävien tuotteiden koko elinkaaren ajan. TOTEAA, että kyberresilienssisäädöstä koskevalla ehdotuksella voidaan merkittävästi vahvistaa tieto- ja viestintätekniikan toimitusketjun turvallisuutta. KANNUSTAA rakentaviin neuvotteluihin ja säädöksen ripeään hyväksymiseen.

17. Tässä yhteydessä ANTAA TUNNUSTUSTA ENISAn johtamalle työlle, jota tehdään parhaillaan yhdessä jäsenvaltioiden ja muiden sidosryhmien kanssa sellaisten kyberturvallisuusasetuksen mukaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointijärjestelmien perustamiseksi EU:lle, joiden on määrä osaltaan parantaa kyberturvallisuuden yleistä tasoa digitaalisilla sisämarkkinoilla. KANNUSTAA kaikkia sidosryhmiä osallistumaan yksittäisiä eurooppalaisia sertifiointijärjestelmiä koskevaan valmistelutyöhön, jotta voidaan rakentaa luottamusta turvallisiin tieto- ja viestintätekniikan tuotteisiin, prosesseihin ja palveluihin ja vahvistaa niiden häiriönsietokykyä, ja PYYTÄÄ komissiota valmistelutyön päätyttyä valmistelemaan pikaisesti eurooppalaisia sertifiointijärjestelmiä, erityisesti yhteisiin kriteereihin perustuvaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää, koskevia täytäntöönpanosäädöksiä. TOTEAA, että eurooppalaisiin sertifiointijärjestelmiin olisi tarvittaessa sisällytettävä toimitusketjun turvallisuutta koskevia vaatimuksia, mukaan lukien suhteet toimittajiin.

18. KOROSTAA, että kaikki tieto- ja viestintätekniikan toimitusketjun turvallisuuteen liittyvät tulevat NIS 2 -säännökset on pantava perusteellisesti täytäntöön. PAINOTTAA tässä yhteydessä kriittisiä toimitusketjuja koskevien EU:n koordinoitujen riskinarviointien (koordinoidut toimitusketjun riskinarvioinnit), toimitusketjun turvallisuutta koskevien kansallisten politiikkojen ja toimitusketjuun liittyvien turvallisuustoimenpiteiden merkitystä. TOTEAA, että tarkasteltaessa pääasiallisen toimittajan tai loppukäyttäjän turvallisuuteen kohdistuvia riskejä, huomiota olisi kiinnitettävä pääasiallisten toimittajien lisäksi myös asianomaisiin alihankkijoihin. Toimitusketjun riskinhallintatoimenpiteiden toteuttamisen helpottamiseksi KANNUSTAA ENISAa tekemään verkko- ja tietoturva-alan yhteistyöryhmän avustuksella selvityksen parhaista käytännöistä toimitusketjun riskinhallinnan alalla ja laatimaan niiden pohjalta menettelyohjeet. Lisäksi KANNUSTAA ENISAa valvomaan tulevan NIS 2 -direktiivin nojalla säänneltyjen toimijoiden investointeja tieto- ja viestintätekniikan toimitusketjun turvallisuuteen.

19. PAINOTTAA myös toimitusketjun turvallisuuden yhteydessä niitä etuja ja riskejä, jotka liittyvät hallintapalvelujen tarjoajien ja tietoturvapalveluntarjoajien käyttöön. Vaikka tällaisten palveluntarjoajien käyttö voi parantaa merkittävästi turvallisuutta organisaatioiden sisällä ja nostaa kyberturvallisuuden tasoa, tieto- ja viestintätekniikan järjestelmien ja palvelujen etähallinta yhdistettynä kyseisten palveluntarjoajien mahdollisesti tarvitsemaan etuoikeutettuun pääsyyn asiakkaiden tieto- ja viestintätekniseen ympäristöön voi aiheuttaa huomattavia kerrannaisvaikutuksia suurelle määrälle asiakkaita, mikäli kyseisten palveluntarjoajien turvallisuus on vaarantunut. Sen vuoksi on äärimmäisen tärkeää, että kyseiset palveluntarjoajat pitävät yllä korkeaa sisäisen turvallisuuden ja tarjoamiensa palvelujen turvallisuuden tasoa ja toimivat asiakkaitaan kohtaan läpinäkyvästi tarjoamiensa palvelujen turvallisuuden suhteen. PANEE tässä yhteydessä TYYTYVÄISENÄ MERKILLE niiden sisällyttämisen tulevan NIS 2 -direktiivin soveltamisalaan.

20. Mitä tulee toimitusketjun koordinoitua riskinarviointia koskevan mekanismin täytäntöönpanoon tulevan NIS 2 -direktiivin mukaisesti, TOTEAA, että muilla kuin teknisillä riskitekijöillä, kuten kolmannen valtion sopimattomalla vaikuttamisella toimittajiin ja palveluntarjoajiin, on tässä yhteydessä merkitystä ja PANEE tältä osin MERKILLE 5G-verkkojen kyberturvallisuutta koskevassa EU:n koordinoidussa riskinarvioinnissa mainitut tekijät, joita voidaan käyttää riskiprofiilin arviointiin. PYYTÄÄ komissiota määrittämään vuoden 2023 toiseen neljännekseen mennessä verkko- ja tietoturva-alan yhteistyöryhmää ja ENISAa kuultuaan ne erityiset tieto- ja viestintätekniikan palvelut, järjestelmät tai tuotteet, joihin voitaisiin ensisijaisesti soveltaa koordinoituja toimitusketjun riskinarviointeja.

21. TOTEAA, että riippuvuus kriittisten verkkojen ja järjestelmien toiminnassa käytettävien tieto- ja viestintätekniikan tuotteiden ja palvelujen suuririskisistä toimittajista on strateginen uhka, jota on lievennettävä asianmukaisilla toimintapolitiikoilla niin kansallisella kuin EU:n tasolla ja tekemällä yhteistyötä jäsenvaltioiden kesken sekä samanmielisten kansainvälisten kumppaneiden kanssa. Tämän strategisen riskin lieventämisen helpottamiseksi ja toimitusketjun koordinoitujen riskinarviointien tukemiseksi KEHOTTAA verkko- ja tietoturva-alan yhteistyöryhmää kehittämään yhteistyössä komission ja ENISAn kanssa välineistön tieto- ja viestintätekniikan kriittisen toimitusketjun riskien vähentämiseksi (tieto- ja viestintätekniikan toimitusketjun välineistö). Tieto- ja viestintätekniikan toimitusketjun välineistön olisi perustuttava tieto- ja viestintätekniikan toimitusketjuille määritettyihin strategisiin uhkaskenaarioihin ja tarjottava toimenpiteitä näihin skenaarioihin vastaamiseksi hyödyntämällä 5G-välineistöstä ja kansallisella tasolla saatuja kokemuksia. Sen olisi täydennettävä avoimella tavalla tulevan NIS 2 -direktiivin mukaisia tiettyjen tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden toimitusketjun koordinoituja riskinarviointeja tarjoamalla yleisiä toimenpiteitä riskien vähentämiseksi. Näitä toimenpiteitä voidaan mukauttaa tiettyjen tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden osalta skaalautuvasti yksittäisissä toimitusketjun koordinoiduissa riskinarvioinneissa yksilöityjen riskien perusteella.

22. KOROSTAA tutkimuksen, innovoinnin, investointien ja yritystoiminnan keskeistä roolia digitaali- ja kyberturvallisuuden alalla sekä niiden rahoittamisen merkitystä, kun on kyse mahdollisten tulevien ei-toivottujen strategisten riippuvuuksien välttämisestä ja tieto- ja viestintätekniikan toimitusketjujen yleisen häiriönsietokyvyn vahvistamisesta. KOROSTAA tässä yhteydessä Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen (ECCC) ja kansallisten koordinointikeskusten verkoston strategisten tehtävien ja täytäntöönpanotehtävien merkitystä niiden investointien vaikutusten maksimoimisessa, jotka tehdään unionin johtajuuden ja avoimen strategisen riippumattomuuden vahvistamiseksi kyberturvallisuuden alalla, unionin teknologisten valmiuksien ja taitojen tukemiseksi ja unionin maailmanlaajuisen kilpailukyvyn lisäämiseksi. Tässä yhteydessä KEHOTTAA saattamaan ECCC:n nopeasti toimintavalmiuteen. KEHOTTAA ECCC:tä ottamaan strategisessa ohjelmassaan huomioon tieto- ja viestintätekniikan toimitusketjun turvallisuusnäkökohdat, mukaan lukien esimerkiksi turvallinen ohjelmistokehitys, varmistaen samalla johdonmukaisuuden ja täydentävyyden ja välttäen toimien päällekkäisyyttä. KANNATTAA Euroopan kilpailukyvyn parantamista kyberturvallisuuden alalla rahoitusohjelmien, kuten tutkimuksen ja innovoinnin Horisontti Eurooppa -puiteohjelman sekä Digitaalinen Eurooppa -ohjelman, avulla EU:n digitaalitalouden, yhteiskunnan ja demokratian keskeisten valmiuksien vahvistamiseksi, kehittämiseksi ja hankkimiseksi.

TUKIMEKANISMIT

23. KANNUSTAA lisäämään taloudellisen tuen kannustimia, jotka liittyvät tieto- ja viestintätekniikan toimitusketjun turvallisuuden vahvistamiseen tähtääviin toimiin. KEHOTTAA ensisijaisesti, myös NIS 2 -direktiivin tulevaa täytäntöönpanoa silmällä pitäen, ECCC:tä, komissiota ja asiaankuuluvia sidosryhmiä tutkimaan vaihtoehtoja tieto- ja viestintätekniikan toimitusketjun turvallisuusnäkökohtien sisällyttämiseksi tuleviin ehdotuspyyntöihin Digitaalinen Eurooppa -ohjelman ja Horisontti Eurooppa -ohjelman kyberturvallisuutta koskevien työohjelmien tai muiden asiaankuuluvien rahoitusmahdollisuuksien yhteydessä. Näillä rahoitusmahdollisuuksilla olisi muun muassa pyrittävä siihen, että organisaatiot voivat tukea korkean kyberturvallisuuden tason ylläpitämistä tieto- ja viestintätekniikan tuotteiden ja palvelujen hankinnassa koko toimitusketjussa, erityisesti kun on kyse sellaisten kriittisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden korvaamisesta, jotka katsotaan suuririskisiksi tulevien toimitusketjun koordinoitujen riskinarviointien perusteella.

24. TOTEAA, että globalisaatio ja tieto- ja viestintätekniikan palvelujen erikoistuminen sekä lisääntynyt riippuvuus kolmansien osapuolten tuotteista ja palveluista edellyttävät tiivistä yhteistyötä EU:ssa ja kansainvälisesti tietämyksen ja asiantuntemuksen jakamiseksi asiaankuuluvien sidosryhmien kesken, ja KANNUSTAA niitä löytämään vahvan ja koordinoidun kannan, jolla varmistetaan tieto- ja viestintätekniikan toimitusketjun turvallisuus kattavasti. TOTEAA myös, että on tutkittava edelleen asiaankuuluvia uusimpia lähestymistapoja ja huipputekniikoita, jotka koskevat sekä asianmukaista perustason kyberhygieniaa että pitkän aikavälin ratkaisuja turvallisten ja häiriönsietokykyisten tieto- ja viestintätekniikan toimitusketjujen luomiseksi, sekä sopivimpia keinoja edistää niitä ja sisällyttää ne mahdollisesti politiikkaan tai muihin aloitteisiin. TOTEAA tässä yhteydessä, että olisi kiinnitettävä erityistä huomiota systeemisten ratkaisujen, kuten luottamattomuuden periaatteiden, ohjelmistojen materiaaliluettelon ja vastaavien pitkän aikavälin ratkaisujen, etujen ja haittojen tutkimiseen. SUOSITTAA, että tähän tarkoitukseen käytetään verkko- ja tietoturva-alan yhteistyöryhmää.

25. PANEE MERKILLE kyberturvallisuuspoikkeamia ja -uhkia koskevan seurannan ja tehokkaan tietojenvaihdon hyödyt toimitusketjuihin kohdistuvien hyökkäysten ehkäisemisessä, havaitsemisessä ja niiden vaikutusten lieventämisessä. PAINOTTAA, että jäsenvaltioiden välistä luottamusta on rakennettava edelleen, jotta tällaisia tietoja voidaan jakaa tehokkaasti. PALAUTTAA tässä yhteydessä MIELEEN komission ehdotuksen jäsenvaltioiden tukemisesta turvaoperaatiokeskusten perustamisessa ja vahvistamisessa, jotta koko EU:hun luotaisiin turvaoperaatiokeskusten verkosto seuraamaan ja ennakoimaan verkkohyökkäyksiin viittaavia signaaleja. MUISTUTTAA, että olemassa olevissa verkostoissa ja mekanismeissa tarvitaan täydentävyyttä ja koordinointia, ja ennen kaikkea KOROSTAA tässä yhteydessä tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (CSIRT-toimijoiden) verkoston roolia ja tarvetta selvittää edelleen näiden verkostojen tarjoamia mahdollisuuksia tehokkaan, turvallisen ja luotettavan tiedonjaon kulttuurin edistämiseksi. PALAUTTAA MIELEEN jäsenvaltioiden EU:n tukemana toteuttamat toimet alakohtaisten, kansallisten ja alueellisten CSIRT-toimijoiden perustamiseksi sekä kansallisten tai eurooppalaisten tietojen jakamisen ja analysoinnin keskusten perustamiseksi osana tehokasta kyberturvallisuuskumppanuuksien verkostoa unionissa.

26. Tieto- ja viestintätekniikan toimitusketjuun liittyvien uhkien toisiinsa kytkeytyvän ja maailmanlaajuisen luonteen vuoksi KOROSTAA, että on tärkeää lähestyä ja parantaa tieto- ja viestintätekniikan toimitusketjun turvallisuutta maailmanlaajuisesti. Tämän vuoksi SUOSITTELEE hyödyntämään digitaalisia kumppanuuksia, kybervuoropuheluja ja muita asiaankuuluvia EU:n aloitteita, tarvittaessa myös vapaakauppasopimuksia, tieto- ja viestintätekniikan tuotteiden ja palvelujen tarjoajien riskiperusteisten arviointien edistämiseksi, luotettavien toimittajien käyttämiseksi ja avoimiin, yhteentoimiviin ja läpinäkyviin standardeihin perustuvan turvallisen ja innovatiivisen digitaalisen ekosysteemin luomiseksi. Lisäksi PALAUTTAA MIELEEN Global Gateway -kumppanuuksien sekä EU:n ja Yhdysvaltojen kauppa- ja teknologianeuvoston ja sen työryhmien toiminnan vision edistää luotettavien / muiden kuin suuririskisten toimittajien käyttöä ja kehittää rahoitusmekanismi, jolla mahdollistetaan hankkeet, joilla parannetaan kolmansien valtioiden tieto- ja viestintätekniikan infrastruktuurin ja palvelujen turvallisuutta, häiriönsietokykyä ja luotettavuutta, muun muassa pidättäytymällä rahoittamasta hankintoja epäluotettavilta/suuririskisiltä toimittajilta teknologianeutraalilla tavalla.

27. VAHVISTAA olevansa sitoutunut edistämään avointa, vapaata, maailmanlaajuista, vakaata ja turvallista kybertoimintaympäristöä ja noudattamaan YK:n kehyksessä vahvistettuja valtion vastuullista toimintaa kybertoimintaympäristössä koskevia normeja, sääntöjä ja periaatteita. Erityisesti tieto- ja viestintätekniikan toimitusketjun turvallisuuden osalta PALAUTTAA MIELEEN YK:n hallitustenvälisen asiantuntijaryhmän ja avoimen työryhmän hyväksymän normin, jolla valtioita kannustetaan toteuttamaan kohtuullisia toimia toimitusketjun eheyden varmistamiseksi, muun muassa kehittämällä objektiivisia yhteistyötoimenpiteitä, jotta loppukäyttäjät voivat luottaa tieto- ja viestintätekniikan tuotteiden turvallisuuteen, ja pyrkimään estämään haitallisten tieto- ja viestintätekniikan välineiden ja tekniikoiden leviäminen ja haitallisten piilotoimintojen käyttö, ja KANNATTAA sen laajaa täytäntöönpanoa.