EUROOPAN
KOMISSIO

UNIONIN ULKOASIOIDEN
JA TURVALLISUUSPOLITIIKAN
KORKEA EDUSTAJA

Bryssel 16.12.2020
JOIN(2020) 18 final

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle

I. JOHDANTO: KYBERTURVALLINEN DIGITAALINEN SIIRTYMÄ MONITAHOISESSA UHKAYMPÄRISTÖSSÄ

Kyberturvallisuus on olennainen osa eurooppalaisten turvallisuutta. Olipa kyse sitten verkkoon liitetyistä laitteista, sähköverkoista, pankkipalveluista, lentokoneista, julkishallinnosta tai sairaaloista, ihmisten on voitava luottaa siihen, että heitä suojellaan kyberuhkilta. EU:n talous, demokratia ja yhteiskunta ovat ennennäkemättömän riippuvaisia turvallisista ja luotettavista digitaalisista välineistä ja yhteyksistä. Kyberturvallisuuden varmistaminen onkin välttämätön osa selviytymiskykyisen, vihreän ja digitaalisen Euroopan rakentamista.

Liikenne, energia, terveydenhuolto, tietoliikenne, rahoitusala, turvallisuus, demokratian toteutuminen, avaruus ja puolustus ovat kaikki erittäin riippuvaisia verkko- ja tietojärjestelmistä, joilla on koko ajan enemmän yhteyksiä keskenään. Vastaavasti verkot ja tietojärjestelmät ovat erittäin riippuvaisia vakaasta sähköntoimituksesta, eli eri alojen välillä on erittäin vahvoja riippuvuussuhteita. Maailmassa on jo enemmän verkkoon liitettyjä laitteita kuin ihmisiä, ja niiden määrän odotetaan kasvavan 25 miljardiin vuoteen 2025 mennessä.[1] Silloin näistä laitteista neljännes tulee olemaan Euroopassa. Koronaviruspandemia on vauhdittanut työskentelymallien digitalisoitumista entisestään, sillä sen aikana EU:ssa 40 prosenttia työntekijöistä siirtyi etätyöhön. Tällä on todennäköisesti pysyviä vaikutuksia arkielämään.[2] Samalla alttius kyberhyökkäyksille lisääntyy.[3] Monilla kuluttajien käytössä olevilla verkkoon liitetyillä esineillä tiedetään olevan haavoittuvuuksia, jotka lisäävät entisestään haitallisen kybertoiminnan hyökkäyspinta-alaa.[4] EU:n teollinen toimintaympäristö on yhä digitalisoituneempi ja verkottuneempi. Tämä tarkoittaa, että myös kyberhyökkäykset voivat vaikuttaa teollisuuteen ja ekosysteemeihin laajemmin kuin koskaan aikaisemmin.

---

[1] Televiestintäalan toimialajärjestön GSMA:n arvio (https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). International Data Corporation ennustaa verkkoon liitettyjen koneiden, antureiden ja kameroiden määrän kasvavan 42,6 miljardiin (https://www.idc.com/getdoc.jsp?containerId=prUS45213219).

[2] Kesäkuussa 2020 tehdyssä kyselyssä 47 prosenttia yritysjohtajista ilmoitti aikovansa antaa työntekijöille mahdollisuuden tehdä etätyötä kokopäiväisesti, vaikka työpaikalle palaaminen olisi mahdollista, ja 82 prosenttia aikoi sallia ainakin satunnaisen etätyöskentelyn (https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time).

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Yksi tähän mennessä haitallisimmista haittaohjelmista tunnetaan nimellä Mirai. Se loi yli 600 000 laitteen bottiverkon, jonka kautta häirittiin useiden merkittävien verkkosivustojen toimintaa Euroopassa ja Yhdysvalloissa.

Uhkia pahentavat geopoliittiset jännitteet, joita liittyy maailmanlaajuiseen ja avoimeen internetiin ja teknologian hallintaan koko toimitusketjussa.[5] Nämä jännitteet näkyvät siinä, että yhä useammat valtiot rakentavat digitaalisia rajoja. Internetin ja sen käytön rajoitukset uhkaavat paitsi maailmanlaajuista ja avointa kybertoimintaympäristöä myös oikeusvaltioperiaatetta, perusoikeuksia, vapautta ja demokratiaa, jotka ovat EU:n keskeisiä arvoja. Kybertoimintaympäristöä käytetään yhä enemmän poliittisiin ja ideologisiin tarkoituksiin, ja lisääntyvä polarisoituminen kansainvälisellä tasolla haittaa tehokasta monenvälisyyttä. Hybridiuhkissa disinformaatiokampanjat yhdistyvät kyberhyökkäyksiin, jotka kohdistuvat infrastruktuuriin, taloudellisiin prosesseihin ja demokraattisiin instituutioihin. Näin voidaan aiheuttaa fyysistä vahinkoa, saada laittomasti haltuun henkilötietoja, varastaa teollisia tai valtionsalaisuuksia, lietsoa epäluottamusta ja heikentää sosiaalista yhteenkuuluvuutta. Tällainen toiminta heikentää kansainvälistä turvallisuutta ja vakautta sekä vaarantaa edut, joita kybertoimintaympäristöstä on taloudelliselle, sosiaaliselle ja poliittiselle kehitykselle.

Kriittiseen infrastruktuuriin kohdistuvat vihamieliset hyökkäykset ovat merkittävä maailmanlaajuinen riski[6]**.** Internetin rakenne on hajautettu, eikä sillä ole keskusrakennetta eikä eri sidosryhmien yhteistä hallintoa. Internet on selvinnyt verkkoliikenteen eksponentiaalisesta kasvusta siihen jatkuvasti kohdistuneista vihamielisistä häiriöyrityksistä huolimatta.[7] Samaan aikaan riippuvuus maailmanlaajuisen ja avoimen internetin keskeisistä toiminnoista, kuten DNS-nimijärjestelmästä (Domain Name System), ja viestintään ja verkkoisännöintiin, sovelluksiin ja dataan liittyvistä keskeisistä internetpalveluista on lisääntynyt. Nämä palvelut keskittyvät yhä enemmän muutamien yksityisten yritysten käsiin.[8] Tämä lisää Euroopan talouden ja yhteiskunnan haavoittuvuutta tilanteissa, joissa internetin ytimeen tai yhteen tai useampaan näistä yrityksistä kohdistuu haitallisia geopoliittisia tai teknisiä tapahtumia. Kun pandemian aikana internetin käyttö on lisääntynyt ja toimintamallit muuttuneet, on huomattu, miten haavoittuvaisia digitaalisesta infrastruktuurista riippuvaiset toimitusketjut ovat.

Huoli turvallisuudesta on yksi tavallisimmista syistä olla käyttämättä verkkopalveluja[9]**.** EU:ssa kaksi viidestä verkkopalveluiden käyttäjästä on kohdannut turvallisuusongelmia, ja

[5] Mukaan lukien elektroniset komponentit, data-analytiikka, pilvipalvelut, verkkojen muuttuminen nopeammiksi ja älykkäämmiksi 5G:n myötä ja sen jälkeen, salaus, tekoäly sekä uudenlaiset laskennan ja datan luotettavan käsittelyn menetelmät, kuten lohkoketjuteknologia, siirtymä pilvestä reunalaskentaan ja kvanttilaskenta.

[6] Maailman talousfoorumin vuoden 2020 raportti maailmanlaajuisista riskeistä (Global Risks Report 2020).

[7] Taloudellisen yhteistyön ja kehityksen järjestön (OECD) mukaan internetliikenne lisääntyi pandemian myötä 60 prosenttia (https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/). Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin ja komissio julkaisevat säännöllisesti raportteja internetkapasiteetin tilasta koronaviruspandemiasta johtuvien liikkumisrajoitusten aikana. ENISAn raportin mukaan hajautettuja palvelunestohyökkäyksiä tehtiin vuoden 2019 kolmannella neljänneksellä 241 prosenttia enemmän kuin samana ajanjaksona vuonna 2018. Hajautetut palvelunestohyökkäykset ovat entistä rajumpia. Helmikuussa 2020 tehtiin tähän asti suurin hyökkäys, jossa liikenne oli enimmillään 2,3 terabittiä sekunnissa. Elokuussa 2020 yhdysvaltalaisella internetpalveluntarjoajalla CenturyLinkillä oli reititysongelmasta johtuva palvelukatkos, jonka seurauksena maailmanlaajuinen verkkoliikenne väheni 3,5 prosenttia (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service).

[8] Internet Societyn raportti ”The Global Internet Report: Consolidation in the Internet Economy” (https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/).

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

kolme viidestä kokee, ettei kykene suojautumaan kyberrikollisuudelta.[10] Joka kolmas on saanut kolmen viime vuoden aikana vilpillisiä sähköpostiviestejä tai puheluja, joissa on kysytty henkilötietoja, mutta 83 prosenttia ei ole koskaan ilmoittanut verkkorikoksesta. Joka kahdeksas yritys on kärsinyt kyberhyökkäyksistä.[11] Yli puolet yritysten ja yksityishenkilöiden tietokoneista, joihin on tarttunut haittaohjelma, saa toisenkin haittaohjelman samana vuonna.[12] Joka vuosi menetetään satoja miljoonia tietueita tietoturvaloukkausten vuoksi. Yksittäiselle yritykselle tietoturvaloukkauksesta koituvat keskimääräiset kustannukset nousivat vuonna 2018 yli 3,5 miljoonaan euroon.[13] Kyberhyökkäyksen vaikutuksia ei useinkaan voida eristää, vaan niistä voi käynnistyä ketjureaktioita, jotka vaikuttavat koko talouteen ja yhteiskuntaan ja siten miljooniin ihmisiin.[14]

Digitaalisuus on läsnä lähes kaikenlaisten rikosten tutkinnassa. Vuonna 2019 poikkeamien määrän ilmoitettiin kolminkertaistuneen edellisvuodesta. Tavallisimmin kyberhyökkäys tapahtuu haittaohjelmien välityksellä. Tällaisista ohjelmista on saatu arviolta 700 miljoonaa uutta näytettä.[15] Vuonna 2020 kyberrikollisuudesta aiheutuu maailmantaloudelle arviolta 5,5 biljoonan euron kustannukset, mikä on kaksi kertaa enemmän kuin vuonna 2015.[16] Tämä on kaikkien aikojen suurin taloudellisen varallisuuden siirto, joka ylittää jopa maailmanlaajuisen huumekaupan. Vuonna 2017 tehtiin erityisen suuri yksittäinen kiristysohjelmahyökkäys (WannaCry), josta aiheutui maailmantaloudelle arviolta 6,5 miljardin euron kustannukset.[17]

Digitaaliset palvelut ja rahoitusala samoin kuin julkinen sektori ja valmistusteollisuus ovat kyberhyökkäysten tavallisimpia kohteita. Tästä huolimatta kyberturvallisuuteen liittyvät valmiudet ja kybertietoisuus ovat edelleen heikolla tasolla[18], ja työntekijöiden kyberturvallisuustaidoissa on vakavia puutteita.[19] Vuonna 2019 tapahtui lähes 450 kyberturvallisuuspoikkeamaa, jotka liittyivät rahoituksen ja energian kaltaisiin elintärkeisiin infrastruktuureihin Euroopassa.[20] Pandemian aikana on koeteltu etenkin

[10] Digitaalitalouden ja -yhteiskunnan indeksi 2020 (https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020). https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Eurostatin lehdistötiedote 6/2020 ”ICT security measures taken by vast majority of enterprises in the EU”, 13. tammikuuta 2020. Maailman talousfoorumin vuoden 2020 raportissa maailmanlaajuisista riskeistä (Global Risks Report 2020) todetaan, että kriittiseen infrastruktuuriin kohdistuvista kyberhyökkäyksistä on tullut arkipäivää esimerkiksi energia-alalla, terveydenhuollossa ja liikennealalla.

[12] Lähde: Comparitech.

[13] Ponemon Instituten vuotuinen raportti tietoturvaloukkausten kustannuksista (Cost of a Data Breach Report 2020), joka perustuu kvantitatiiviseen analyysiin 524 viimeaikaisesta tietoturvaloukkauksesta 17 maantieteellisellä alueella ja 17 toimialalla (https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf).

[14] Yhteisen tutkimuskeskuksen raportti ”Cybersecurity – Our Digital Anchor” (https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor).

[15] Lähde: AV-TEST (https://www.av-test.org/en/statistics/malware/).

[16] Yhteisen tutkimuskeskuksen raportti ”Cybersecurity – Our Digital Anchor”.

[17] Lähde: Cyence.

[18] Myös riski liikesalaisuuksien verkkovarkauksista tiedostetaan yhä heikosti varsinkin pk-yrityksissä. PwC:n laatima tutkimus ”Study on the scale and impact of industrial espionage and theft of trade secrets through cyber – Dissemination report on measures to tackle and prevent cyber-theft of trade secrets”, 2018.

[19] Katso ENISAn Threat Landscape 2020 -raportti. Katso myös Verizonin tutkimusraportti tietosuojaloukkauksesta (Data Breach Investigations Report 2020) (https://enterprise.verizon.com/resources/reports/dbir/).

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

terveydenhuollon organisaatioita ja työntekijöitä. Kun teknologia ja fyysinen maailma kytkeytyvät erottamattomasti toisiinsa, kyberhyökkäykset vaarantavat kaikkein heikoimmassa asemassa olevien ihmisten hengen ja hyvinvoinnin.[21] Yli kaksi kolmasosaa yrityksistä, erityisesti pk-yrityksistä, on kyberturvallisuusasioissa aloittelijoita, ja eurooppalaisissa yrityksissä valmiustason katsotaan olevan heikommalla tasolla kuin aasialaisissa ja amerikkalaisissa yrityksissä.[22] Euroopassa on edelleen täyttämättä arviolta 291 000 kyberturvallisuusammattilaisen paikkaa. Kyberturvallisuusasiantuntijoiden rekrytoinnin ja kouluttamisen hitaus lisää organisaatioiden kyberturvallisuusriskejä.[23]

EU:lla ei ole yhteisiä tilannetietoja kyberuhkista. Tämä johtuu siitä, että kansalliset viranomaiset eivät kerää ja jaa järjestelmällisesti tietoja, esimerkiksi yksityiseltä sektorilta saatavia tietoja, jotka voisivat auttaa arvioimaan kyberturvallisuuden tilaa EU:ssa. Jäsenvaltiot ilmoittavat vain murto-osasta poikkeamia, eikä tietojen jakaminen ole järjestelmällistä eikä kattavaa.[24] Kyberhyökkäykset saattavat olla vain yksi osa keskitettyjä vihamielisisiä hyökkäyksiä eurooppalaisia yhteiskuntia vastaan. Tällä hetkellä jäsenvaltiot antavat toisilleen vain vähän operatiivista apua, eikä jäsenvaltioilla ja EU:n toimielimillä, virastoilla ja elimillä ole yhteistä operatiivista mekanismia laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien tai -kriisien varalta.[25]

Kyberturvallisuuden parantaminen on olennaisen tärkeää, jotta ihmiset voivat luottaa siihen, että innovaatioiden, yhteenliitettävyyden ja automaation käyttö on turvallista ja jotta voidaan turvata perusoikeudet ja -vapaudet, mukaan lukien oikeus yksityisyyteen ja henkilötietojen suojaan, sekä sananvapaus ja tiedonvälityksen vapaus. Kyberturvallisuus on välttämätön edellytys verkkoyhteyksille sekä maailmanlaajuiselle ja avoimelle internetille, jotka muodostavat 2020-luvulla talouden ja yhteiskunnan muutoksen perustan. Se auttaa luomaan lisää ja parempia työpaikkoja, lisää työskentelyn joustavuutta, tehostaa ja kestävöittää liikennettä ja maataloutta sekä helpottaa ja parantaa terveyspalvelujen saatavuutta. Kyberturvallisuus liittyy läheisesti rajatylittäviin verkkoihin, älykkäisiin mittareihin ja päällekkäisten datavarastojen välttämiseen, ja on siten keskeisessä roolissa myös siirryttäessä Euroopan vihreän kehityksen ohjelman[26] mukaisesti puhtaampaan energiaan. Se on välttämätön myös kansainvälisen turvallisuuden ja vakauden sekä talouksien, demokratioiden ja yhteiskuntien kehityksen kannalta kaikkialla maailmassa. Siksi on tärkeää, että hallitukset, yritykset ja yksityishenkilöt käyttävät digitaalisia välineitä vastuullisella ja turvallisuustietoisella tavalla. Arkisia toimintoja koskevan digitaalisen siirtymän on rakennuttava kyberturvallisuustietoisuudelle ja kyberhygieniasta huolehtimiselle.

[21] Kiristysohjelmia on käytetty sairaaloihin ja terveystietoihin kohdistuvissa hyökkäyksissä, esimerkiksi Romaniassa (kesäkuu 2020), Düsseldorfissa (syyskuu 2020) ja terapiayritys Vastaamon tapauksessa (lokakuu 2020).

[22] PwC: ”The Global State of Information Security 2018”; ESI Thoughtlab: ”The Cybersecurity Imperative”, 2019.

[23] EU:n kyberturvallisuusviraston julkaisu ”Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA’s Higher Education Database”, joulukuu 2019.

[24] Verkko- ja tietojärjestelmien turvallisuudesta annetun direktiivin (direktiivi (EU) 2016/1148) 10 artiklan 3 kohdan mukaisesti jäsenvaltioiden on toimitettava yhteistyöryhmälle vuosittain tiivistelmäraportti saaduista ilmoituksista.

[25] CSIRT-verkostolla on menettelyohjeet jäsenten keskinäistä avunantoa varten.

[26] Euroopan vihreän kehityksen ohjelma, COM(2019) 640 final.

EU:n uusi kyberturvallisuusstrategia digitaaliselle vuosikymmenelle liittyy kiinteästi tiedonantoon ”*Euroopan digitaalista tulevaisuutta rakentamassa*”[27], komission laatimaan Euroopan elvytyssuunnitelmaan[28], vuosien 2020–2025 turvallisuusunionistrategiaan[29], EU:n ulko- ja turvallisuuspoliittisen globaalistrategiaan[30] ja Eurooppa-neuvoston strategiseen ohjelmaan 2019–2024[31]. Siinä esitetään, miten EU suojelee kansalaisiaan, yrityksiään ja instituutioitaan kyberuhkilta ja miten se edistää kansainvälistä yhteistyötä ja johtaa pyrkimyksiä turvata avoin ja maailmanlaajuinen internet.

II. GLOBAALI NÄKÖKULMA, EUROOPAN TASON TOIMINTA

Strategian tavoitteena on varmistaa maailmanlaajuinen ja avoin internet, jossa eurooppalaisten turvallisuutta ja perusoikeuksia ja -vapauksia voidaan tehokkaasti suojella niihin kohdistuvilta riskeiltä. Strategia jatkaa siitä, mihin aiempien strategioiden avulla on päästy, ja sisältää konkreettisia ehdotuksia ottaa käyttöön sääntelyä, investointeja ja politiikkaa koskevia välineitä **kolmella EU:n toiminta-alalla: 1) häiriönsietokyky, teknologinen riippumattomuus ja johtajuus, 2) operatiivisten valmiuksien kehittäminen uhkien ehkäisemiseksi ja torjumiseksi ja niihin vastaamiseksi ja 3) maailmanlaajuisen ja avoimen kybertoimintaympäristön edistäminen.** EU on sitoutunut tukemaan tätä strategiaa **ennennäkemättömän suurilla** – aiempiin verrattuna jopa nelinkertaisilla – **investoinneilla EU:n digitaaliseen siirtymään seuraavien seitsemän vuoden aikana** osana uutta teknologia- ja teollisuuspolitiikkaa ja elpymisohjelmaa.[32]

Kyberturvallisuusulottuvuus on sisällytettävä kaikkiin näihin digitaaliseen siirtymään liittyviin investointeihin ja erityisesti investointeihin, jotka koskevat tekoälyn, salauksen ja kvanttilaskennan kaltaisia keskeisiä teknologioita. Apuna käytetään kannustimia, velvoitteita ja vertailuarvoja. Tämä voi vauhdittaa Euroopan kyberturvallisuustoimialan kasvua ja rohkaista poistamaan vanhat järjestelmät asteittain käytöstä. Euroopan kyberpuolustusratkaisut ovat osa Euroopan puolustuksen teollista ja teknologista perustaa, ja niitä tuetaan Euroopan puolustusrahastosta. Kyberturvallisuusulottuvuus sisältyy kumppaneidemme tukemiseksi käytettävissä ulkoisen toiminnan rahoitusvälineisiin, erityisesti naapuruus-, kehitys- ja kansainvälisen yhteistyön välineeseen. Teknologioiden väärinkäytön estäminen, elintärkeiden infrastruktuurien suojeleminen ja toimitusketjujen eheyden varmistaminen auttavat EU:ta noudattamaan myös vastuullista valtion toimintaa koskevia YK:n normeja, sääntöjä ja periaatteita[33].

[27] Euroopan digitaalista tulevaisuutta rakentamassa, COM(2020) 67 final.
[28] Euroopan h-hetki: korjaamalla ja kehittämällä parempaa seuraavalle sukupolvelle, COM(2020) 98 final.
[29] EU:n turvallisuusunionistrategia 2020–2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#
[32] Digitaaliteknologian koko toimitusketjuun tehtävien investointien, joilla edistetään digitaalista siirtymää ja vastataan siihen liittyviin haasteisiin, odotetaan olevan yhteensä vähintään 20 prosenttia eli 134,5 miljardia euroa avustuksista ja lainoista koostuvan elpymis- ja palautumistukivälineen 672,5 miljardista eurosta. Vuosien 2021–2027 monivuotisessa rahoituskehyksessä on suunnitteilla EU:n rahoitusta kyberturvallisuutta varten Digitaalinen Eurooppa -ohjelman puitteissa ja kyberturvallisuutta koskevaa tutkimusta varten Horisontti Eurooppa -ohjelman puitteissa. Painopiste on erityisesti pienten ja keskisuurten yritysten tukemisessa, ja rahoituksen määrä voisi olla yhteensä 2 miljardia euroa jäsenvaltioiden ja teollisuuden investointien lisäksi.
[33] https://undocs.org/A/70/174

1. HÄIRIÖNSIETOKYKY, TEKNOLOGINEN RIIPPUMATTOMUUS JA JOHTAJUUS

EU:n elintärkeät infrastruktuurit ja keskeiset palvelut digitalisoituvat ja ovat yhä riippuvaisempia toisistaan. Kaikki internetiin yhteydessä olevat tuotteet, oli kyse sitten automatisoiduista autoista, teollisuuden valvontajärjestelmistä tai kodinkoneista, ja koko niiden markkinoille saattamiseen liittyvä toimitusketju on suunniteltava alusta asti turvallisuutta silmällä pitäen. Niillä on oltava hyvä kyberturvallisuuspoikkeamien sietokyky, ja niiden on oltava nopeasti korjattavissa, kun haavoittuvuuksia havaitaan. Tämä on olennaisen tärkeää, jotta EU:n yksityisellä ja julkisella sektorilla olisi käytössään mahdollisimman turvalliset infrastruktuurit ja palvelut. Tulevalla vuosikymmenellä EU:lla on mahdollisuus ottaa johtoasema turvallisten teknologioiden kehittämisessä koko toimitusketjua varten. Häiriönsietokyvyn ja kyberturvallisuuteen liittyvien teollisten ja teknologisten valmiuksien varmistamiseksi olisi otettava käyttöön kaikki tarvittavat sääntelyä, investointeja ja politiikkaa koskevat välineet. Riskejä voidaan lieventää suunnittelemalla teollisuusprosessit, toiminnot ja laitteet alusta asti kyberturvallisiksi. Tämä voi myös vähentää yrityksille ja yhteiskunnalle koituvia kustannuksia ja siten parantaa häiriönsietokykyä.

1.1 Infrastruktuurin ja kriittisten palveluiden hyvä häiriönsietokyky

Verkko- ja tietojärjestelmien turvallisuutta koskevat EU:n säännöt (NIS) ovat kyberturvallisuuden sisämarkkinoiden ytimessä. Komissio ehdottaa, että näitä sääntöjä uudistetaan tarkistetussa verkko- ja tietoturvadirektiivissä. Tarkoituksena on parantaa **kyberuhkien sietokykyä kaikilla talouden ja yhteiskunnan kannalta tärkeillä aloilla niin julkisella kuin yksityisellä sektorilla**.[34] Direktiivin tarkistaminen on tarpeen epäjohdonmukaisuuksien vähentämiseksi sisämarkkinoilla. Yhdenmukaistukset koskevat soveltamisalaa, turvallisuutta ja poikkeamista ilmoittamista koskevia vaatimuksia, kansallista valvontaa ja täytäntöönpanoa sekä toimivaltaisten viranomaisten valmiuksia.

Uudistettu verkko- ja tietoturvadirektiivi muodostaa perustan yksityiskohtaisemmille säännöille, joita tarvitaan myös strategisesti tärkeillä aloilla, kuten energia-alalla, liikenteessä ja terveydenhuollossa. Jotta voidaan varmistaa vuosia 2020–2025 koskevassa turvallisuusunionistrategiassa esitetty johdonmukainen lähestymistapa, uudistetun direktiivin ohella ehdotetaan myös kriittisen infrastruktuurin häiriönsietokykyä koskevan lainsäädännön tarkistamista.[35] Digitaalisia komponentteja sisältävät energiateknologiat ja niihin liittyvien toimitusketjujen turvallisuus ovat tärkeitä keskeisten palvelujen jatkuvuuden ja kriittisen energiainfrastruktuurin strategisen valvonnan kannalta. Sen vuoksi komissio ehdottaa toimenpiteitä, kuten verkkosääntöjen asettamista koskevia sääntöjä, joilla varmistetaan rajat ylittävien sähkövirtojen kyberturvallisuus. Komission ehdottamat toimenpiteet on määrä hyväksyä vuoden 2022 loppuun mennessä. Komissio on ehdottanut[36], että myös rahoitusala vahvistaa digitaalista häiriönsietokykyään ja varmistaa, että se kestää kaikenlaisia tieto- ja viestintätekniikkaan liittyviä häiriöitä ja uhkia. Komissio on puuttunut liikenteeseen kohdistuviin kyberuhkiin lisäämällä ilmailun turvaamista koskevaan EU:n lainsäädäntöön kyberturvallisuutta koskevia säännöksiä[37] ja jatkaa toimia kaikkien liikennemuotojen

[34] [*Lisätään viittaus NIS-ehdotukseen*]
[35] [Lisätään viittaus *ehdotukseen* direktiiviksi kriittisten yksiköiden häiriönsietokyvystä]
[36] Ehdotus asetukseksi finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014 ja (EU) N:o 909/2014 muuttamisesta, COM/2020/595 final.
[37] Komission täytäntöönpanoasetus (EU) 2019/1583.

kyberuhkien sietokyvyn parantamiseksi. **Demokraattisten prosessien ja instituutioiden** häiriönsietokyvyn vahvistaminen kyberuhkien varalta on keskeinen osa demokratiaa koskevaa eurooppalaista toimintasuunnitelmaa, jolla pyritään turvaamaan ja edistämään vapaita vaaleja, demokraattista keskustelua ja tiedotusvälineiden moniarvoisuutta.[38] Tulevan avaruusohjelman puitteissa komissio edistää infrastruktuurin ja palvelujen turvallisuutta laajentamalla Galileon kyberturvallisuusstrategiaa maailmanlaajuisen satelliittinavigointijärjestelmän seuraavan sukupolven palveluihin ja avaruusohjelman muihin uusiin osatekijöihin.[39]

1.2 EU:n kyberturvallisuusjärjestelyn kehittäminen

Kun yhteenliitettävyys yleistyy ja kyberhyökkäykset muuttuvat yhä monimutkaisemmiksi, tiedon jakamisen ja analysoinnin keskukset (ISAC) tekevät tärkeää työtä, myös toimialatasolla, mahdollistaessaan kyberuhkia koskevien tietojen vaihdon useiden sidosryhmien välillä.[40] Myös verkkoja ja tietojärjestelmiä on seurattava ja analysoitava jatkuvasti, jotta tunkeutumiset ja poikkeamat voidaan havaita reaaliajassa. Monet yksityiset yritykset, julkiset organisaatiot ja kansalliset viranomaiset ovatkin perustaneet tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä eli CSIRT-toimijoita ja tietoturvan valvomopalveluja (SOC).

Tietoturvan valvomopalvelut tekevät korvaamatonta työtä kerätessään lokitietoja[41] ja eristäessään epäilyttäviä tapahtumia, joita ne havaitsevat valvomissaan viestintäverkoissa. Tätä varten ne seuraavat signaaleja ja toimintamalleja ja keräävät uhkia koskevaa tietoa suurista määristä arvioitavaa dataa. Ne ovat auttaneet havaitsemaan vihamielisiä suoritustiedostoja ja siten osaltaan torjuneet kyberhyökkäyksiä. Tietoturvan valvomopalvelujen työ on erittäin vaativaa ja nopeatahtista, minkä vuoksi tekoäly ja erityisesti koneoppimistekniikat voivat olla korvaamaton apu alan toimijoille.[42]

Komissio ehdottaa, että **koko EU:n alueelle rakennetaan tietoturvan valvomopalveluiden verkosto**[43] ja tuetaan olemassa olevien tietoturvan valvomopalveluiden parantamista ja uusien perustamista. Se tukee myös tietoturvan valvomopalveluja hoitavan henkilöstön koulutusta ja taitojen kehittämistä. Se voisi sitoutua tukemaan yli 300 miljoonalla eurolla julkisen ja yksityisen sektorin yhteistyötä ja rajat ylittävää yhteistyötä sellaisten kansallisten ja alakohtaisten verkostojen luomiseksi, joihin osallistuu myös pk-yrityksiä ja jotka perustuvat asianmukaiseen hallintoon, tietojen jakamiseen ja turvallisuutta koskeviin

[38] Tiedonanto Euroopan demokratiatoimintasuunnitelmasta, COM(2020) 790. Suunnitelman mukaan Euroopan vaaliyhteistyöverkoston (European Cooperation Network on Elections) ja kansallisten vaaliverkostojen kautta tuetaan yhteisten asiantuntijaryhmien käyttöä vaaliprosesseihin kohdistuvien uhkien, myös kyberuhkien, torjumiseksi https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

[39] Tämä tarkoittaa muun muassa uutta valtiollista satelliittiviestintää (GOVSATCOM) koskevaa aloitetta ja avaruusesineiden valvontaa ja seurantaa (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[41] Siten, että lainvalvonta- ja oikeusviranomaiset voivat käyttää niitä todisteina.

[42] Lähde: Ponemon Instituten tutkimus ”Improving the Effectiveness of the SOC, 2019”. Lisätietoa tekoälyn käytöstä tietoturvan valvomopalveluissa esimerkiksi seuraavassa tutkimuksessa: Khraisat, A., Gondal, I., Vamplew, P. *et al.*: ”Survey of intrusion detection systems: techniques, datasets and challenges”, *Cybersecurity* 2**,** 20 (2019).

[43] Tarkoitus on kehittää yksityiskohtaisempia järjestelyjä näiden palvelujen hallintoa, toimintaperiaatteita ja rahoitusta varten sekä täsmentää sitä, miten ne täydentävät olemassa olevia rakenteita, kuten digitaali-innovointikeskittymiä.

säännöksiin. Tukitarpeet määritettiin asianomaisten sidosryhmien kanssa toteutetussa tarveanalyysissa, jota EU:n kyberturvallisuusvirasto (ENISA) tuki.

Jäsenvaltioita kannustetaan osallistumaan tämän hankkeen rahoitukseen. Näin keskukset voisivat tehokkaammin jakaa ja suhteuttaa havaittuja signaaleja ja koota uhkakuvista korkealaatuisia tiedustelutietoja, jotka voidaan jakaa tiedon jakamisen ja analysoinnin keskusten ja kansallisten viranomaisten kanssa tilannetietoisuuden parantamiseksi. Tavoitteena olisi yhdistää vaiheittain mahdollisimman monta tietoturvan valvomopalvelua eri puolilta EU:ta yhteisen tietämyksen luomiseksi ja parhaiden käytäntöjen jakamiseksi. Nämä palvelut saavat tukea parantaakseen poikkeamien havaitsemista, analysointia ja reagointinopeutta käyttämällä uusinta tekoäly- ja koneoppimisteknologiaa ja Euroopan suurteholaskennan yhteisyrityksen[44] EU:ssa kehittämää suurteholaskennan infrastruktuuria.

Tietoturvan valvomopalvelujen verkosto tekee jatkuvaa yhteistyötä antaakseen viranomaisille ja muille asiasta kiinnostuneille sidosryhmille (yhteinen kyberturvallisuusyksikkö mukaan luettuna) oikea-aikaisia varoituksia kyberturvallisuuspoikkeamista (ks. 2.1 kohta). **Se toimii EU:n todellisena ”kyberturvallisuuskilpenä”** ja on kuin vartiotornien verkosto, jonka avulla mahdolliset uhat voidaan havaita ennen kuin ne aiheuttavat laajamittaista vahinkoa.

1.3 Huipputurvallinen viestintäinfrastruktuuri

Euroopan avaruusohjelmaan kuuluva EU:n valtiollinen satelliittiviestintäohjelma[45] tarjoaa turvallisia ja kustannustehokkaita avaruusperusteisia viestintävalmiuksia, joilla turvataan EU:n ja sen jäsenvaltioiden, kansalliset turvallisuusalan toimijat ja EU:n toimielimet, elimet ja virastot mukaan lukien, hallinnoimat turvallisuuden kannalta kriittiset tehtävät ja operaatiot.

Jäsenvaltiot ovat sitoutuneet tekemään komission kanssa yhteistyötä turvallisen kvanttiviestintäinfrastruktuurin käyttöönottamiseksi Euroopassa.[46] Kvanttiviestintäinfrastruktuurin myötä viranomaiset saavat täysin uudenlaisen tavan toimittaa luottamuksellisia tietoja siten, että kyberhyökkäyksiltä suojaudutaan käyttäen eurooppalaiseen teknologiaan pohjautuvaa huipputurvallista salausta. Kvanttiviestintäinfrastruktuuri koostuu kahdesta osasta: olemassa olevat maanpäälliset kuituviestintäverkot, jotka yhdistävät strategisia kohteita maiden sisällä ja niiden välillä, ja niihin liitetyt avaruussatelliitit, jotka kattavat koko EU:n, sen merentakaiset alueet mukaan lukien.[47] Kyseisellä aloitteella kehitetään ja otetaan käyttöön uusia ja turvallisempia

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

[45] GOVSATCOM on osa unionin avaruusohjelmaa.

[46] Useimmat jäsenvaltiot ovat allekirjoittaneet EuroQCI-julistuksen. Infrastruktuurin kehittäminen ja käyttöönotto on tarkoitus toteuttaa vuosina 2021–2027 Horisontti Eurooppa -ohjelmasta ja Digitaalinen Eurooppa -ohjelmasta sekä Euroopan avaruusjärjestöltä saadun rahoituksen avulla ja asianmukaisten hallintojärjestelyjen mukaisesti (https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network).

[47] Avaruuskomponentin kehittäminen on tarpeen, jotta voidaan luoda pitkän matkan (> 1000 km) kaksipisteyhteyksiä, joihin maassa sijaitseva infrastruktuuri ei pysty. Kvanttiviestintäinfrastruktuurissa hyödynnetään kvanttimekaniikan ominaisuuksia, jotta osapuolet voivat ensi alkuun jakaa turvallisesti salaisia satunnaisavaimia, joita käytetään viestien salaamiseen ja salauksen purkamiseen. Kvanttiviestintäinfrastruktuurin osana tullaan ottamaan käyttöön myös testaus- ja vaatimustenmukaisuusinfrastruktuuri, jotta voidaan arvioida, ovatko eurooppalaiset kvanttiviestintälaitteet ja -järjestelmät sekä niiden sertifiointi ja validointi kvanttiviestintäinfrastruktuurin kannalta sopivia ennen niiden sisällyttämistä siihen. Infrastruktuuri suunnitellaan siten, että se tukee lisäsovelluksia, kunhan ne saavuttavat

salausmenetelmiä ja kehitetään uusia tapoja suojata kriittisiä viestintä- ja dataresursseja. Näin aloite auttaa turvaamaan arkaluonteiset tiedot ja kriittiset infrastruktuurit.

Tätä ja vielä kunnianhimoisempia tavoitteita silmällä pitäen komissio aikoo tutkia mahdollisuutta ottaa käyttöön monikiertoratainen turvallisten yhteyksien järjestelmä. Se olisi jatkoa GOVSATCOMin ja kvanttiviestintäinfrastruktuurin parissa tehdylle työlle, ja siinä huipputeknologiat (kvantti-, 5G-, tekoäly- ja reunalaskentateknologiat) yhdistettäisiin erittäin tiukkoihin kyberturvallisuusrajoituksiin, jotta edistettäisiin turvallisuuslähtöistä palvelusuunnittelua esimerkiksi luotettavien, turvallisten ja kustannustehokkaiden yhteyksien ja kriittisissä viranomaistoiminnoissa käytettävän salatun viestinnän suunnittelussa.

1.4 Seuraavan sukupolven mobiililaajakaistaverkkojen turvaaminen

EU:n kansalaisilla ja yrityksillä, jotka käyttävät **5G-verkkojen ja tulevien sukupolvien verkkojen** mahdollistamia kehittyneitä ja innovatiivisia sovelluksia, olisi oltava turvanaan tiukat turvallisuusvaatimukset. Jäsenvaltiot ovat komission ja ENISAn tuella vahvistaneet 5G-verkkojen kyberturvallisuutta koskevan kattavan ja objektiivisen riskiperusteisen lähestymistavan hyväksymällä tammikuussa 2020 EU:n 5G-kyberturvallisuusvälineistön[48]. Lähestymistapa perustuu mahdollisten riskinhallintasuunnitelmien arviointiin ja tehokkaimpien toimenpiteiden yksilöintiin. Lisäksi EU vahvistaa 5G:hen ja sitä seuraaviin teknologioihin liittyviä valmiuksiaan välttääkseen riippuvuudet ja edistääkseen toimitusketjun kestävyyttä ja monipuolisuutta.

Komissio julkaisi joulukuussa 2020 kertomuksen 5G-verkkojen kyberturvallisuudesta 26. maaliskuuta 2019 annetun suosituksen vaikutuksista.[49] Se osoitti, että asiassa on edistytty huomattavasti välineistöstä sopimisen jälkeen ja että useimmat jäsenvaltiot ovat hyvää vauhtia saattamassa välineistön toimenpiteet päätökseen lähitulevaisuudessa, vaikkakin joitakin eroavaisuuksia ja puutteita vielä on, kuten heinäkuussa 2020 julkaistussa edistymiskertomuksessa kerrottiin.[50]

Eurooppa-neuvosto kehotti lokakuussa 2020 EU:ta ja jäsenvaltioita ”hyödyntämään täysimääräisesti 5G-kyberturvallisuusvälineistöä” ja ”soveltamaan asiaankuuluvia rajoituksia EU:n laajuisessa koordinoidussa riskinarvioinnissa kriittisiksi ja arkaluonteisiksi katsottujen keskeisten kohteiden suuririskisiksi katsottuihin toimittajiin”, jotka on arvioitu ”yhteisten puolueettomien kriteerien perusteella”.[51]

Tulevaisuutta varten EU:n ja sen jäsenvaltioiden olisi varmistettava, että havaittuja riskejä on lievennetty asianmukaisesti ja koordinoidusti, jotta voidaan erityisesti minimoida suuririskisiksi katsotuille toimittajille altistuminen ja välttää riski tulla riippuvaiseksi näistä toimittajista kansallisella ja unionin tasolla, ja että kaikki uudet merkittävät muutokset tai riskit otetaan huomioon. Jäsenvaltioita kehotetaan hyödyntämään välineistöä täysimääräisesti digitaalisia valmiuksia ja yhteenliitettävyyttä koskevissa investoinneissaan.

---

tarvittavan teknologisen kehitysasteen. Tämänhetkinen OpenQKD-pilottihanke (https://openqkd.eu/) on tämän testaus- ja vaatimustenmukaisuusinfrastruktuurin edeltäjä.

[48] Tiedonanto ”*5G:n turvallinen käyttöönotto EU:ssa – EU:n välineistön täytäntöönpano*”, COM(2020) 50.

[49] Komission kertomus 5G-verkkojen kyberturvallisuudesta 26. maaliskuuta 2019 annetun komission suosituksen vaikutuksista, 15. joulukuuta 2020.

[50] Verkko- ja tietoturva-alan yhteistyöryhmän 24. heinäkuuta 2020 antama raportti välineistön täytäntöönpanosta.

[51] EUCO 13/20, Eurooppa-neuvoston ylimääräisen kokouksen (1. ja 2. lokakuuta 2020) päätelmät.

Vuonna 2019 annetun suosituksen vaikutuksia koskevan kertomuksen perusteella komissio kannustaa jäsenvaltioita nopeuttamaan välineistön keskeisten toimenpiteiden täytäntöönpanoa niin, että se saadaan päätökseen vuoden 2021 toisella neljänneksellä. Lisäksi se kehottaa jäsenvaltioita seuraamaan edelleen yhdessä sitä, miten täytäntöönpanossa edistytään, ja varmistamaan, että lähestymistapoja yhdenmukaistetaan entisestään. EU:n tasolla tätä prosessia tuetaan kolmen päätavoitteen kautta: varmistetaan, että riskinvähentämistä koskeva lähestymistapa on entistä yhdenmukaisempi koko EU:ssa, tuetaan jatkuvaa tiedonvaihtoa ja valmiuksien kehittämistä sekä edistetään toimitusketjun häiriönsietokykyä ja muita EU:n strategisia turvallisuustavoitteita. Näihin keskeisiin tavoitteisiin liittyvät konkreettiset toimet esitetään tämän tiedonannon asiaa koskevassa lisäyksessä.

Komissio jatkaa tiivistä yhteistyötä jäsenvaltioiden kanssa näiden tavoitteiden saavuttamiseksi ja toimien toteuttamiseksi ENISAn tuella (ks. liite).

EU:n 5G-välineistöön perustuva lähestymistapa on herättänyt kiinnostusta myös sellaisissa EU:n ulkopuolisissa maissa, jotka kehittävät parhaillaan omaa lähestymistapaansa viestintäverkkojen turvaamiseen. Komission yksiköt ovat yhdessä Euroopan ulkosuhdehallinnon ja EU:n edustustojen verkoston kanssa valmiita antamaan pyydettäessä lisätietoja kattavasta, objektiivisesta ja riskiperusteisesta EU:n lähestymistavasta viranomaisille eri puolilla maailmaa.

1.5 Tietoturvallisten esineiden internet

Jokaisessa verkkoon yhteydessä olevassa esineessä on heikkouksia, joita saatetaan käyttää hyväksi mahdollisesti laajoin seurauksin. Sisämarkkinasääntöihin sisältyy suojatoimia turvallisuuden vaarantavia tuotteita ja palveluja vastaan. Komissio työskentelee jo **kyberturvallisuusasetuksen puitteissa varmistaakseen avoimet turvallisuusratkaisut ja sertifioinnin** sekä kannustaakseen turvallisten tuotteiden ja palvelujen kehittämiseen suorituskyvyn kärsimättä.[52] Se hyväksyy ensimmäisen unionin jatkuvan työohjelman[53] vuoden 2021 ensimmäisellä neljänneksellä (minkä jälkeen se päivitetään vähintään kolmen vuoden välein), jotta teollisuuden toimijat, kansalliset viranomaiset ja standardointielimet voivat valmistautua etukäteen tuleviin eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin. Esineiden internetin laajentuessa tarvitaan entistä vahvempia täytäntöönpanokelpoisia sääntöjä yleisen häiriönsietokyvyn varmistamiseksi ja kyberturvallisuuden edistämiseksi.

Komissio harkitsee kokonaisvaltaista lähestymistapaa, johon voisi sisältyä **uusia horisontaalisia sääntöjä kaikkien sisämarkkinoille saatettujen verkkoon liitettyjen tuotteiden ja niihin liittyvien palvelujen kyberturvallisuuden parantamiseksi**.[54]

[52] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus). Kyberturvallisuusasetuksella edistetään tieto- ja viestintätekniikan sertifiointia EU:n tasolla ottamalla käyttöön eurooppalainen kyberturvallisuuden sertifiointikehys vapaaehtoisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamista varten. Tarkoituksena on varmistaa, että tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuuden taso on unionissa riittävä, ja vähentää sisämarkkinoiden hajanaisuutta unionin kyberturvallisuuden sertifiointijärjestelmien osalta. Toisaalta kyberturvallisuusluokituksia tekevät yritykset ovat yleensä sijoittautuneet EU:n ulkopuolelle, ja niiden avoimuus ja valvonta on vähäistä (https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings).

[53] Vaaditaan kyberturvallisuusasetuksen 47 artiklan 5 kohdassa.

[54] Neuvoston päätelmissä (13629/20, 2. joulukuuta 2020) kehotetaan toteuttamaan internetiin yhdistettyjen laitteiden kyberturvallisuutta koskevia horisontaalisia toimenpiteitä.

Tällaisiin sääntöihin voisi sisältyä **verkkoon liitettyjen laitteiden valmistajia koskeva uusi huolellisuusvelvoite**, jonka mukaan niiden olisi ratkaistava ohjelmistojen haavoittuvuuksia esimerkiksi jatkamalla ohjelmisto- ja tietoturvapäivityksiä sekä varmistamalla, että henkilötiedot ja muut arkaluonteiset tiedot poistetaan laitteen käyttöiän lopussa. Nämä säännöt tukisivat kiertotalouden toimintasuunnitelmassa esitettyä aloitetta, joka koskee oikeutta päivittää vanhentuneita ohjelmistoja, ja täydentäisivät käynnissä olevia tietyntyyppisiä tuotteita koskevia toimenpiteitä, joihin kuuluu muun muassa ehdotus tiettyjen langattomien tuotteiden markkinoille pääsyä koskevista pakollisista vaatimuksista (radiolaitedirektiivin[55] mukainen delegoitu säädös), sekä tukisivat tavoitetta panna moottoriajoneuvoja koskevat kyberturvallisuussäännöt täytäntöön kaikissa uusissa ajoneuvotyypeissä heinäkuusta 2022 alkaen.[56] Ne perustuisivat yleisten tuoteturvallisuussääntöjen ehdotettuun tarkistukseen. Nykyisellään tuoteturvallisuussäännöissä ei oteta suoraan kantaa kyberturvallisuusnäkökohtiin[57].

1.6 Internetin turvallisuuden maailmanlaajuinen parantaminen

Keskeisimmillä protokollilla ja niitä tukevalla infrastruktuurilla varmistetaan internetin toimivuus ja eheys kaikkialla maailmassa.[58] Yksi kyseisistä protokollista on DNS-järjestelmä ja sen alaiset hierarkkiset ja delegoidut tasot, joiden hierarkian huipulla on juurialue ja kolmetoista DNS-juuripalvelinta[59], joista World Wide Web on riippuvainen. Komissio aikoo laatia **maailmanlaajuisen DNS-järjestelmän eheyteen ja saatavuuteen vaikuttavien äärimmäisten skenaarioiden varalta valmiussuunnitelman, jota tuetaan EU:n rahoituksella**. Yhteistyössä ENISAn, jäsenvaltioiden, EU:n kahden DNS-juuripalvelinoperaattorin[60] ja monisidosryhmäisen yhteisön kanssa komissio arvioi näiden toimijoiden roolia sen takaamisessa, että internet on jatkossakin käytettävissä kaikkialla maailmassa ja kaikissa olosuhteissa.

Jotta käyttäjä pääsee käsiksi tietyllä verkkotunnuksella internetissä olevaan resurssiin, DNS-nimipalvelimen on selvitettävä sen osoitteeseen (tyypillisimmin URL-osoite eli ”Uniform Resource Locator”) liitetty IP-osoite. EU:n kansalaiset ja organisaatiot ovat kuitenkin koko ajan riippuvaisempia muutamista EU:n ulkopuolisten tahojen hallinnoimista julkisista DNS-nimipalveluista. DNS-nimipalvelun keskittyminen tällä tavalla muutaman yrityksen[61] käsiin vaarantaa nimipalvelun onnistumisen silloin, kun tapahtuu jotain, mikä häiritsee merkittävästi

[55] Direktiivi 2014/53/EU.
[56] Kesäkuussa 2020 hyväksytyn E-säännön mukaisesti (http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf).
[57] Nykyisten yleistä tuoteturvallisuutta koskevien sääntöjen (direktiivi 2001/95/EY) tarkistus. Ehdotetut mukautetut säännöt koskevat myös tuottajien vastuuta digitaalisessa ympäristössä vastuuta koskevan EU:n sääntelykehyksen puitteissa.
[58] Avoimen internetin julkinen ydin – eli sen tärkeimmät protokollat ja infrastruktuuri, jotka ovat globaali julkishyödyke – huolehtii koko internetin keskeisistä toiminnoista ja tukee sen normaalia toimintaa. ENISAn olisi tuettava muun muassa mutta ei pelkästään avoimen internetin julkisen ytimen keskeisten protokollien (erityisesti DNS:n, BGP:n ja iPv6:n) toiminnan turvallisuutta ja vakautta, verkkotunnusjärjestelmän toimintaa (mukaan lukien kaikkien aluetunnusten toiminta) sekä juurialueen toimintaa.” (Kyberturvallisuusasetuksen johdanto-osan 23 kappale.)
[59] https://www.iana.org/domains/root/servers
[60] Netnodin Ruotsissa ylläpitämät i.root-palvelimet ja RIPE NCC:n Alankomaissa ylläpitämät k.root-palvelimet.
[61] Tieteellinen julkaisu ”Consolidation in the DNS resolver market – how much, how fast, how dangerous?” (). Tieteellinen julkaisu ”Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services” ( ).

jonkin tärkeän palvelutarjoajan toimintaa. Lisäksi se vaikeuttaa EU:n viranomaisten työtä, kun ne pyrkivät torjumaan mahdollisia vihamielisiä kyberhyökkäyksiä ja merkittäviä geopoliittisia tapahtumia tai teknisiä poikkeamia.[62]

Markkinoiden keskittymiseen liittyvien turvallisuusongelmien vähentämiseksi komissio kannustaa asianomaisia sidosryhmiä, kuten eurooppalaisia yrityksiä, internetpalveluntarjoajia ja selaimia myyviä yrityksiä, hyväksymään DNS-nimipalvelujen monipuolistamisstrategian. Komissio aikoo myös edistää internetyhteyksien turvaamista tukemalla julkisen **eurooppalaisen DNS-nimipalvelun** kehittämistä. Tämä DNS4EU-aloite tarjoaa vaihtoehdon käyttää maailmanlaajuista internetiä eurooppalaisen palvelun avulla. DNS4EU:n on määrä olla avoin ja viimeisimpien tietoturvaa, tietosuojaa ja yksityisyyden suojaa koskevien standardien ja sääntöjen mukainen, ja siitä tulee osa teollisuuden datan ja pilvipalveluiden eurooppalaista allianssia (European Industrial Alliance for Data and Cloud).[63]

Lisäksi komissio aikoo yhdessä jäsenvaltioiden ja alan toimijoiden kanssa **nopeuttaa keskeisten internetstandardien, kuten IPv6:n[64], sekä vakiintuneiden internetin turvallisuusstandardien ja DNS-järjestelmää, reititystä ja sähköpostin turvallisuutta koskevien hyvien käytäntöjen[65]** käyttöönottoa, mutta myös sääntelytoimenpiteet, kuten IPv4:ää koskeva eurooppalainen raukeamislauseke, ovat mahdollisia markkinoiden ohjaamiseksi, jos edellä mainittujen standardien ja käytäntöjen käyttöönotossa edistytään liian hitaasti. EU:n olisi edistettävä (esimerkiksi EU–Afrikka-strategian[66] mukaisesti) kyseisten standardien täytäntöönpanoa kumppanimaissa keinona tukea maailmanlaajuisen ja avoimen internetin kehittämistä ja torjua internetin suljettuja ja valvottuja malleja. Komissio harkitsee, onko sellaiselle mekanismille tarvetta, jonka avulla pystyttäisiin seuraamaan järjestelmällisesti internetliikennettä ja koostamaan sitä koskevia tietoja sekä neuvomaan mahdollisissa häiriötilanteissa.[67]

1.7 Vahvistettu läsnäolo teknologian toimitusketjussa

EU aikoo antaa vuosien 2021–2027 monivuotisen rahoituskehyksen aikana rahoitustukea kyberturvalliselle digitaaliselle siirtymälle, ja samalla sillä on ainutlaatuinen tilaisuus yhdistää voimavaransa edistääkseen teollisuusstrategiaansa[68] ja johtajuuttaan digitaaliteknologian ja kyberturvallisuuden alalla koko digitaalisessa toimitusketjussa (mukaan lukien data ja pilvipalvelut, seuraavan sukupolven prosessoriteknologiat, huipputurvalliset yhteydet ja 6G-verkot) omien arvojensa ja prioriteettiensa mukaisesti. Julkisen sektorin toimien olisi perustuttava EU:n julkisia hankintoja koskevan

[62] On näyttöä siitä, että DNS-dataa voidaan käyttää profilointitarkoituksiin eli sillä on merkitystä myös yksityisyyden suojan ja tietosuojan kannalta.
[63] Yhteinen julistus seuraavan sukupolven pilvipalvelujen luomisesta EU:n yrityksille ja julkiselle sektorille (https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe).
[64] IPv6:n käyttöönotossa on edetty pidemmälle nyt, kun IPv4-osoitteiden tarjonta on tuntuvasti heikentynyt ja kustannukset nousseet. IPv6:n käyttöönotto on kuitenkin eri vaiheessa eri puolilla EU:ta.
[65] Tällaisia standardeja ovat muun muassa DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE sekä reititykseen liittyvät normit ja hyvät käytännöt, kuten yhteisesti sovitut reitityksen turvallisuusstandardit (MANRS).
[66] Yhteinen tiedonanto ”*Tavoitteena kokonaisvaltainen EU–Afrikka-strategia*”, 9.3.2020, JOIN(2020) 4 final.
[67] Tällainen ”internetin seurantakeskus” voisi kuulua Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen toimialaan. Ehdotus asetukseksi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta, COM(2018) 630 final.
[68] Tiedonanto ”*Euroopan uusi teollisuusstrategia*”, COM(2020) 102 final.

sääntelykehyksen ja Euroopan yhteistä etua koskevien tärkeiden hankkeiden tarjoamiin välineisiin. Tämän lisäksi voidaan houkutella yksityisiä investointeja julkisen ja yksityisen sektorin kumppanuuksien kautta (muun muassa hyödyntämällä kokemuksia, joita on saatu julkisen ja yksityisen sektorin kyberturvallisuuskumppanuutta koskevasta sopimuksesta ja sen täytäntöönpanosta Euroopan kyberturvallisuusjärjestön kautta), riskipääomaa pk-yritysten tueksi ja muodostaa teknologisia valmiuksia koskevia toimiala-alliansseja ja strategioita.

Erityistä huomiota kiinnitetään myös teknisen tuen välineeseen[69] ja uusimpien kyberturvallisuusvälineiden parhaaseen mahdolliseen käyttöön pk-yrityksissä – erityisesti niissä, jotka eivät kuulu tarkistetun verkko- ja tietoturvadirektiivin soveltamisalaan. Tässä hyödynnetään muun muassa digitaali-innovointikeskittymien Digitaalinen Eurooppa -ohjelman puitteissa toteuttamia kohdennettuja toimia. Tavoitteena on saada jäsenvaltiot tekemään yhtäläinen määrä investointeja, ja toimialalta odotetaan vastaavaa panostusta ehdotetussa **kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkostossa (CCCN)** toteutettavan ja jäsenvaltioiden kanssa yhteistyössä johdetun kumppanuuden puitteissa. CCCN:llä olisi oltava toimialan ja akateemisten yhteisöjen myötävaikutuksella keskeinen rooli kehitettäessä EU:n teknologista itsemääräämisoikeutta kyberturvallisuuden alalla, luotaessa valmiuksia 5G:n kaltaisten arkaluonteisten infrastruktuurien turvaamiseksi ja vähennettäessä ratkaisevan tärkeisiin teknologioihin liittyvää riippuvuutta maailman muista osista.

Komissio aikoo tukea, mahdollisesti CCCN:n avulla, kyberturvallisuuden maisteriohjelman kehittämistä ja edistää Euroopan kyberturvallisuusalan tutkimusta ja innovointia koskevan etenemissuunnitelman laatimista vuoden 2020 jälkeistä aikaa varten. CCCN:n kautta tehtävät investoinnit perustuisivat osaltaan kyberturvallisuuden osaamiskeskusten verkostoissa tehtyyn tutkimus- ja kehitysyhteistyöhön. Ne toisivat Euroopan parhaat tutkimusryhmät ja alan toimijat yhteen suunnittelemaan ja toteuttamaan yhteisiä tutkimusohjelmia Euroopan kyberturvallisuusjärjestön etenemissuunnitelman[70] mukaisesti. Komissio tukeutuu edelleen ENISAn ja Europolin tutkimustyöhön ja tukee jatkossakin Horisontti Eurooppa -ohjelman puitteissa myös internet-asioihin keskittyviä yksittäisiä innovoijia, jotka kehittävät yksityisyyden suojaa ja tietoturvaa parantavia viestintäteknologioita, jotka perustuvat avoimen lähdekoodin ohjelmistoihin ja laitteistoihin, kuten tällä hetkellä tehdään seuraavan sukupolven internetiä koskevan aloitteen puitteissa.

1.8 Kyberturvallisuusasiat osaava EU:n työvoima

EU:n toimet työvoiman kehittämiseksi, parhaiden kyberturvallisuusosaajien kouluttamiseksi, houkuttelemiseksi ja sitouttamiseksi sekä maailmanluokan tutkimukseen ja innovointiin investoimiseksi ovat tärkeä osa yleistä suojautumista kyberuhkia vastaan. Tällä alalla on paljon mahdollisuuksia. Siksi on kiinnitettävä erityistä huomiota siihen, että saadaan koulutettua, houkuteltua ja sitoutettua monenlaisia huippuosaajia. Tarkistettu digitaalisen koulutuksen toimintasuunnitelma lisää yksilöiden, erityisesti lasten ja nuorten, ja organisaatioiden, erityisesti pk-yritysten, kyberturvallisuustietoisuutta.[71] Lisäksi se kannustaa naisia opiskelemaan luonnontieteitä, teknologiaa, insinööritieteitä ja matematiikkaa (STEM-tieteet) sekä kehittämään ja uudistamaan digitaalista osaamista tieto- ja viestintätekniikan alan työpaikoissa. Lisäksi komissio kehittää yhdessä Europoliin kuuluvan EU:n

[69] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=COM:2020:0409:FIN
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_fi

teollisoikeuksien viraston, ENISAn, jäsenvaltioiden ja yksityisen sektorin kanssa välineitä tietoisuuden lisäämiseen sekä ohjeistusta, joka parantaa EU:n yritysten kykyä **torjua teollis- ja tekijänoikeuksien kybervarkauksia**[72].

Koulutuksella – mukaan lukien ammatillinen koulutus, tiedotus ja harjoitukset – voidaan kehittää kyberturvallisuutta ja kyberpuolustusta koskevia taitoja EU:n tasolla. Tätä varten asiaankuuluvien EU:n toimijoiden, kuten ENISAn, Euroopan puolustusviraston (EDA) ja Euroopan turvallisuus- ja puolustusakatemian (ETPA)[73], olisi pyrittävä synergiaan toimiensa välillä.

Strategiset aloitteet

EU:n olisi varmistettava

- tarkistetun verkko- ja tietoturvadirektiivin hyväksyminen
- tietoturvallisten esineiden internetiä koskevat sääntelytoimenpiteet
- investoinnit kyberturvallisuuteen CCCN:n kautta (erityisesti Digitaalinen Eurooppa -ohjelman, Horisontti Eurooppa -ohjelman ja elpymisvälineen kautta) siten, että julkiset ja yksityiset investoinnit saadaan nostettua vuosina 2021–2027 jopa 4,5 miljardiin euroon
- tekoälyn avulla toimivien tietoturvan valvomopalvelujen verkosto EU:ssa ja huipputurvallinen ja kvanttiteknologiaa hyödyntävä viestintäinfrastruktuuri
- kyberturvallisuusteknologioiden laajamittainen käyttöönotto tukemalla erityisesti pk-yrityksiä digitaali-innovointikeskittymien puitteissa
- EU:n DNS-nimipalvelun kehittäminen, jotta EU:n kansalaisilla, yrityksillä ja julkishallinnolla on turvallinen ja avoin vaihtoehto internetin käyttöön ja
- 5G-välineistön täytäntöönpano niin, että se saadaan päätökseen vuoden 2021 toisella neljänneksellä (ks. liite).

2. OPERATIIVISTEN VALMIUKSIEN KEHITTÄMINEN UHKIEN EHKÄISEMISEKSI JA TORJUMISEKSI JA NIIHIN VASTAAMISEKSI

Kyberturvallisuuspoikkeamat, olivatpa ne tahattomia taikka rikollisten, valtiollisten toimijoiden tai valtiosta riippumattomien toimijoiden tahallaan aikaansaamia, voivat aiheuttaa valtavaa vahinkoa. Ne ovat laajoja ja monimutkaisia, ja niissä hyödynnetään usein kolmansien osapuolten palveluja, laitteistoja ja ohjelmistoja lopullisen tavoitteen saavuttamiseksi. EU:n yhteisen uhkaympäristön hallinta onkin haastavaa ilman järjestelmällistä ja kattavaa tietojenvaihtoa ja vastatoimia koskevaa yhteistyötä. EU pyrkii **sääntelyvälineiden täysimääräisen täytäntöönpanon, mobilisoinnin ja yhteistyön avulla** auttamaan jäsenvaltioita puolustamaan kansalaisiaan sekä taloudellista ja kansallista turvallisuuttaan kunnioittaen kaikilta osin perusoikeuksia ja -vapauksia sekä oikeusvaltioperiaatetta. Useat eri yhteisöt, esimerkiksi EU:n toimielimet, elimet ja virastot sekä jäsenvaltioiden viranomaiset, ovat vastuussa kyberuhkien ehkäisemisestä ja torjumisesta

[72] https://ec.europa.eu/commission/presscorner/detail/fi/IP_20_2187
[73] Kyberpuolustusalan koulutus-, harjoitus- ja arviointifoorumin kautta (ETEE).

ja niihin vastaamisesta, ja ne käyttävät tässä apuna omia välineitään ja aloitteitaan.[74] Tällaisia yhteisöjä ovat muun muassa seuraavat: i) verkko- ja tietoturvaviranomaiset, kuten CSIRT-toimijat, ja katastrofiapu; ii) lainvalvonta- ja oikeusviranomaiset; iii) kyberdiplomatia; ja iv) kyberpuolustus.

2.1 Yhteinen kyberturvallisuusyksikkö

Yhteinen kyberturvallisuusyksikkö toimisi virtuaalisena ja fyysisenä yhteistyöfoorumina EU:n eri kyberturvallisuusyhteisöille ja keskittyisi operatiiviseen ja tekniseen koordinointiin merkittävien rajat ylittävien kyberturvallisuuspoikkeamien ja kyberuhkien torjumiseksi.

Yhteinen kyberturvallisuusyksikkö olisi merkittävä askel kohti **Euroopan kyberturvallisuuden kriisinhallintakehyksen** valmiiksi saattamista. Kuten komission puheenjohtajan poliittisissa suuntaviivoissa[75] todetaan, yksikön avulla jäsenvaltiot ja EU:n toimielimet, elimet ja virastot saisivat suurimman hyödyn olemassa olevista rakenteista, resursseista ja valmiuksista. Se myös edistäisi ”**jaetaan tarvittaessa**” -lähestymistapaa. Se tarjoaisi keinon vahvistaa edistystä, jota tähän mennessä on saavutettu koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin vuonna 2017 annetun suosituksen (”EU:n suunnitelma”)[76] täytäntöönpanossa. Se tarjoaisi myös tilaisuuden vahvistaa edelleen EU:n suunnitelman arkkitehtuuriin liittyvää yhteistyötä ja hyödyntää erityisesti verkko- ja tietoturva-alan yhteistyöryhmässä ja CyCLONe-verkostossa saavutettua edistystä.

Näin voitaisiin korjata **kaksi keskeistä puutetta**, jotka tällä hetkellä lisäävät haavoittuvuutta ja aiheuttavat tehottomuutta, kun reagoidaan unioniin vaikuttaviin rajat ylittäviin uhkiin ja poikkeamiin. Ensinnäkin siviili-, diplomaatti-, lainvalvonta- ja puolustusalan **kyberturvallisuusyhteisöillä** ei ole vielä yhteisiä puitteita, joissa ne voisivat edistää jäsenneltyä yhteistyötä ja helpottaa operatiivista ja teknistä yhteistyötä. Toiseksi kyberturvallisuusalan sidosryhmät eivät ole vielä pystyneet hyödyntämään kaikkia operatiivisen yhteistyön ja keskinäisen avunannon tarjoamia **mahdollisuuksia** nykyisissä verkostoissa ja yhteisöissä. Tämä johtuu osin siitä, ettei ole olemassa foorumia, joka mahdollistaisi operatiivisen yhteistyön yksityisen sektorin kanssa. Yhteisen kyberturvallisuusyksikön tehtävä olisi parantaa ja nopeuttaa koordinointia, jolloin EU:lla olisi paremmat valmiudet torjua laajamittaisia kyberturvallisuuspoikkeamia ja -kriisejä.

Yhteinen kyberturvallisuusyksikkö ei olisi uusi itsenäinen elin, eikä se vaikuttaisi kansallisten kyberturvallisuusviranomaisten tai EU:n osallistujien toimivaltuuksiin. Yksikkö toimisi pikemminkin varautumisjärjestelynä, jossa osallistujat voisivat tukeutua toistensa asiantuntemukseen erityisesti tilanteissa, joissa eri kyberyhteisöjen on tehtävä tiivistä yhteistyötä. Samaan aikaan viimeaikaiset tapahtumat osoittavat, että EU:n on nostettava

[74]Näihin lukeutuvat muun muassa Euroopan unionin kyberturvallisuusviraston (ENISA) tuki operatiiviselle yhteistyölle ja kriisinhallinnalle; CSIRT-verkosto; kyberkriisien yhteysorganisaatioiden verkosto (CyCLONe, josta tulee verkko- ja tietoturvadirektiivin tarkistuksen myötä EU-CyCLONe); verkko- ja tietoturva-alan yhteistyöryhmä; rescEU; Euroopan kyberrikostorjuntakeskus ja kyberrikollisuutta torjuva yhteisen toiminnan työryhmä Europolissa sekä lainvalvonnan hätäaputoimien protokolla; EU:n tiedusteluanalyysikeskus (EU INTCEN) ja kyberdiplomatian välineistö; yhtenäisen tiedustelun analysointikyky (SIAC); kyberturvallisuuteen liittyvät pysyvän rakenteellisen yhteistyön (PRY) hankkeet, erityisesti kyberalan nopean toiminnan ryhmät ja kyberturvallisuuteen liittyvä keskinäinen avunanto.

[75]Euroopan komission puheenjohtajaehdokas Ursula von der Leyenin poliittiset suuntaviivat seuraavalle Euroopan komissiolle (2019–2024) – ”Kunnianhimoisempi unioni: Ohjelma Euroopalle”.

[76]Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annettu komission suositus (suunnitelma) C(2017) 6100 final.

tavoitetasoaan ja valmiuttaan selviytyä kyberuhkaympäristöstä ja sen realiteeteista. Osana yksikölle antamaansa tukea EU:n toimijat (komissio ja EU:n virastot ja elimet) ovat näin ollen valmiita lisäämään merkittävästi voimavarojaan valmiuksiensa ja häiriönsietokykynsä parantamiseksi.

Yhteisellä kyberturvallisuusyksiköllä olisi kolme päätavoitetta. Ensinnäkin se varmistaisi kyberturvallisuusyhteisöiden **varautumisen**. Toiseksi se tarjoaisi jatkuvan yhteisen **tilannetietoisuuden** jakamalla tietoja. Kolmanneksi se vahvistaisi koordinoitua **reagoimista** ja elpymistä. Jotta nämä tavoitteet saavutetaan, yksikön toiminnalla on oltava selvästi määritellyt **osa-alueet ja tavoitteet**, kuten **turvallisen ja nopean tietojen vaihdon varmistaminen**, yhteistyön **parantaminen** osallistujien välillä, mukaan luettuna jäsenvaltioiden ja asianomaisten EU:n yksiköiden välinen vuorovaikutus, järjestelmällisten **kumppanuuksien perustaminen luotettavien toimialan edustajien kanssa** sekä koordinoidun lähestymistavan edistäminen **ulkoisten kumppaneiden kanssa tehtävään yhteistyöhön**. Onnistuakseen tässä yksikkö voisi kartoittaa kansallisella ja EU:n tasolla käytettävissä olevia voimavaroja ja edistää siten yhteistyöpuitteiden kehittämistä.

Jotta yhteisestä kyberturvallisuusyksiköstä saataisiin tehtyä EU:n operatiivisen kyberturvallisuusyhteistyön ydin, komissio tekee yhteistyötä jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen, kuten ENISAn, CERT-EU:n ja Europolin, kanssa edistääkseen **vaiheittaista ja osallistavaa lähestymistapaa** kunnioittaen kaikilta osin kaikkien asianosaisten toimivaltuuksia ja toimeksiantoja. Tämän lähestymistavan mukaisesti yksikkö voisi edistää tietyn kyberyhteisön toimijoiden välistä yhteistyötä, jos ne pitävät sitä tarpeellisena.

Yhteisen kyberturvallisuusyksikön perustamiseksi ehdotetaan neljää päävaihetta:

- *määrittely* kartoittamalla kansallisella ja EU:n tasolla käytettävissä olevat voimavarat
- *valmistelu* laatimalla puitteet jäsennellylle yhteistyölle ja avunannolle
- *käyttöönotto* panemalla puitteet täytäntöön osallistujien tarjoamien resurssien avulla, jotta yhteinen kyberturvallisuusyksikkö saadaan toimintavalmiiksi
- *laajentaminen* vahvistamalla koordinoituja reagointivalmiuksia toimialan ja kumppaneiden myötävaikutuksella.

Jäsenvaltioiden, EU:n toimielinten, elinten ja virastojen kuulemisen tulosten[77] pohjalta komissio esittää korkean edustajan avustuksella ja hänen toimivaltansa mukaisesti helmikuuhun 2021 mennessä menettelyn, välitavoitteet ja aikataulun **yhteisen kyberturvallisuusyksikön määrittelyä, valmistelua, käyttöönottoa ja laajentamista** varten.

2.2 Kyberrikollisuuden torjunta

Riippuvuutemme verkkovälineistä on lisännyt eksponentiaalisesti kyberrikollisten hyökkäyspinta-alaa ja johtanut tilanteeseen, jossa lähes kaikentyyppisten rikosten tutkinnassa on digitaalinen osatekijä. Lisäksi kybertoimijat ja ne, jotka käyttävät kybervälineitä laittoman

[77]Jäsenvaltioiden kuuleminen (mukaan lukien Blue OLEx20-harjoitus, johon osallistui kansallisten kyberturvallisuusviranomaisten johtajia), EU:n toimielinten, elinten ja virastojen kuuleminen heinä-marraskuussa 2020.

toimintansa suunnitteluun ja toteuttamiseen, uhkaavat yhteiskunnan keskeisiä osia. Nämä kysymykset liittyvät läheisesti EU:n yleiseen turvallisuuspolitiikkaan, kuten vuoden 2020 turvallisuusunionistrategiassa ja EU:n terrorisminvastaisessa ohjelmassa[78] esitetään.

Kyberrikollisuuden tehokas torjunta on keskeinen tekijä kyberturvallisuuden varmistamisessa, koska hyvä häiriönsietokyky ei yksin riitä pelotteeksi, vaan rikoksentekijät on myös tunnistettava ja pantava syytteeseen. Sen vuoksi on olennaisen tärkeää edistää yhteistyötä ja tiedonvaihtoa kyberturvallisuusalan toimijoiden ja lainvalvontaviranomaisten välillä. Europol ja ENISA ovatkin jo tehneet tiivistä yhteistyötä EU:n tasolla järjestämällä yhteisiä konferensseja ja työpajoja ja toimittamalla komissiolle, jäsenvaltioille ja muille sidosryhmille yhteisiä raportteja kyberturvallisuusuhkista ja teknologisista haasteista. Komissio tukee edelleen tätä yhdennettyä lähestymistapaa varmistaakseen, että reagointi on johdonmukaista ja tehokasta ja että se perustuu kattavaan tietämykseen.

Yhtenä tärkeänä osana tätä toimintaa EU:n ja kansallisten viranomaisten on laajennettava ja parannettava lainvalvontaviranomaisten valmiuksia tutkia kyberrikollisuutta siten, että perusoikeuksia kunnioitetaan kaikilta osin ja eri oikeuksien ja etujen välillä pyritään tarvittavaan tasapainoon. EU:n olisi voitava torjua kyberrikollisuutta panemalla täytäntöön tarkoituksenmukainen lainsäädäntö, jossa keskitytään erityisesti verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjuntaan ja digitaaliseen tutkintaan, mukaan lukien rikollisuus pimeässä verkossa. Lainvalvontaviranomaisilla on oltava täydet valmiudet digitaaliseen tutkintaan. Sen vuoksi komissio aikoo esittää toimintasuunnitelman, jolla parannetaan lainvalvontaviranomaisten digitaalisia valmiuksia, jotta niillä olisi käytössään tarvittava osaaminen ja välineet. Sen lisäksi erityisesti Europol kehittää edelleen rooliaan asiantuntijakeskuksena, joka tukee kansallisia lainvalvontaviranomaisia kyberympäristöä hyväksi käyttävän tai siitä riippuvaisen rikollisuuden torjunnassa ja osallistuu yhteisten rikosteknisten standardien määrittelyyn (Europolin innovointilaboratorion ja -keskuksen kautta). Kaikki nämä toimet edellyttävät jäsenvaltioiden asianmukaista osallistumista. Jäsenvaltioita kannustetaan hyödyntämään sisäisen turvallisuuden rahaston kansallisia ohjelmia ja ehdottamaan hankkeita vastauksena ehdotuspyyntöihin osana temaattista rahoitusvälinettä.

Komissio käyttää kaikkia asianmukaisia keinoja, myös rikkomusmenettelyjä, varmistaakseen, että tietojärjestelmiin kohdistuvista hyökkäyksistä vuonna 2013 annettu direktiivi[79] saatetaan kokonaan osaksi kansallista lainsäädäntöä ja pannaan täytäntöön, mukaan lukien sen säännökset jäsenvaltioiden toimittamista tilastoista. Direktiivin avulla voidaan ehkäistä paremmin verkkotunnusten väärinkäyttöä, tarvittaessa myös laittoman sisällön jakelua, ja pyrkiä varmistamaan täsmällisten rekisteröintitietojen saatavuus jatkamalla yhteistyötä ICANNin (Internet Corporation for Assigned Names and Numbers) ja muiden internetin hallintojärjestelmän sidosryhmien kanssa, erityisesti ICANNin hallitusten neuvoa-antavan komitean yleisen turvallisuuden työryhmän kautta. Ehdotuksessa tarkistetuksi verkko- ja tietoturvadirektiiviksi säädetään näin ollen verkkotunnusten ja rekisteröintitietojen eli WHOIS-tietojen tarkkojen ja täydellisten tietokantojen ylläpitämisestä ja nimetyn verkkotunnuksen turvallisuuden, vakauden ja häiriönsietokyvyn varmistamisen kannalta tärkeän laillisen pääsyn tarjoamisesta näihin tietoihin.

[78]Tiedonanto terrorisminvastaisesta EU:n ohjelmasta: Ennakointi, ennaltaehkäisy, suojelu ja reagoiminen, 9.12.2020, COM(2020) 795 final.
[79]Direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä.

Komissio pyrkii myös edelleen tarjoamaan asianmukaisia kanavia ja selkeyttämään sääntöjä, jotka koskevat rikostutkintaa varten tarvittavan sähköisen todistusaineiston rajat ylittävää saatavuutta (sitä tarvitaan 85 prosentissa tutkinnoista, ja 65 prosenttia kaikista pyynnöistä osoitetaan toiselle lainkäyttöalueelle sijoittautuneille palveluntarjoajille), helpottamalla sähköistä todistusaineistoa koskevan paketin ja käytännön toimenpiteiden hyväksymistä ja täytäntöönpanoa.[80] Euroopan parlamentin ja neuvoston on hyväksyttävä nopeasti sähköistä todistusaineistoa koskevat ehdotukset, jotta rikostutkijat saisivat käyttöönsä tehokkaan välineen. Sähköisen todistusaineiston on oltava luettavissa, joten komissio jatkaa työtä lainvalvontaviranomaisten digitaalisen tutkinnan valmiuksien tukemiseksi, mukaan lukien rikostutkinnassa esiintyvän salauksen käsittely, samalla kuitenkin toteuttaen täysin tehtäväänsä suojella perusoikeuksia ja kyberturvallisuutta.

2.3 EU:n kyberdiplomatian välineistö

EU on käyttänyt **kyberdiplomatian välineistöään**[81] estääkseen, hillitäkseen, ehkäistäkseen ja torjuakseen haitallista kybertoimintaa ja vastatakseen siihen. Sen jälkeen kun toukokuussa 2019 otettiin käyttöön oikeudellinen kehys kyberhyökkäysten vastaisille kohdennetuille rajoittaville toimenpiteille[82], EU merkitsi heinäkuussa 2020[83] luetteloon kuusi henkilöä ja kolme yhteisöä, jotka ovat vastuussa EU:hun ja sen jäsenvaltioihin kohdistuvista kyberhyökkäyksistä tai sekaantuneet niihin. Lokakuussa 2020[84] luetteloon merkittiin vielä kaksi henkilöä ja yksi elin. Haitallisiin kybertoimiin, myös hitaasti eteneviin, olisi puututtava tehokkailla ja kattavilla EU:n yhteisillä diplomaattisilla toimilla, joissa käytetään kaikkia EU:n tason toimenpiteitä.

Nopea ja tehokas EU:n yhteinen diplomaattinen toiminta edellyttää vahvaa yhteistä tilannetietoisuutta ja kykyä valmistella nopeasti EU:n yhteinen kanta. Unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja kannustaa ja helpottaa EU:n tiedusteluanalyysikeskukseen (INTCEN) sijoitetun **jäsenvaltioiden EU-kybertiedustelua käsittelevän työryhmän** perustamista. Työryhmän on tarkoitus edistää kyberuhkia ja -toimia koskevaa strategista tiedusteluyhteistyötä. Tämä työ tukee edelleen EU:n tilannetietoisuutta ja

[80] COM(2018) 225 ja COM(2018) 226, C(2020) 2779 lopullinen. Erityisesti SIRIUS-hanke sai äskettäin lisärahoitusta kumppanuusvälineestä, jotta voidaan parantaa rikostutkintaa varten tarvittavan sähköisen todistusaineiston rajat ylittävää saatavuutta (sitä tarvitaan 85 prosentissa vakavien rikosten tutkinnoista, ja 65 prosenttia kaikista pyynnöistä osoitetaan toiselle lainkäyttöalueelle sijoittautuneille palveluntarjoajille) ja vahvistaa yhteensopivat säännöt kansainvälisellä tasolla.

[81] https://www.consilium.europa.eu/fi/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] Neuvoston päätös (YUTP) 2019/797, annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129 I, 17.5.2019, s. 13) ja neuvoston asetus (EU) 2019/796,
annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129 I, 17.5.2019, s. 1).

[83] Neuvoston päätös (YUTP) 2020/1127, annettu 30 päivänä heinäkuuta 2020, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta (ST/9564/2020/INIT) (EUVL L 246, 30.7.2020, s. 12–17) ja neuvoston täytäntöönpanoasetus (EU) 2020/1125, annettu 30 päivänä heinäkuuta 2020, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun asetuksen (EU) 2019/796 täytäntöönpanosta (ST/9568/2020/INIT)(EUVL L 246, 30.7.2020, s. 4–9).

[84] Neuvoston päätös (YUTP) 2020/1537, annettu 22 päivänä lokakuuta 2020, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta (EUVL L 351 I, 22.10.2020, s. 5–7) ja neuvoston täytäntöönpanoasetus (EU) 2020/1536, annettu 22 päivänä lokakuuta 2020, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun asetuksen (EU) 2019/796 täytäntöönpanosta (EUVL L 351 I, 22.10.2020, s. 1–4).

yhteistä diplomaattista vastausta koskevaa päätöksentekoa. Työryhmän on tarkoitus olla yhteydessä nykyisiin välineisiin[85], tarvittaessa myös niihin, jotka kattavat hybridiuhkien ja ulkomaisen sekaantumisen muodostaman laajemman uhan, ja kerätä tilannetietoja ja arvioida niitä.

Jotta EU voisi paremmin estää, hillitä, ehkäistä ja torjua haitallista kybertoimintaa ja vastata siihen, korkea edustaja antaa yhdessä komission kanssa toimivaltansa mukaisesti ehdotuksen EU:lle sen **kyberpelotetta koskevan kannan** määrittelemiseksi tarkemmin. Kyberpelotetta koskevalla kannalla olisi edistettävä valtion vastuullista käyttäytymistä ja yhteistyötä kybertoimintaympäristössä kyberdiplomatian välineistön puitteissa tähän mennessä tehdyn työn pohjalta. Sillä olisi ohjattava erityisesti sellaisten kyberhyökkäysten torjuntaa, joilla on suurin vaikutus, erityisesti niiden, jotka vaikuttavat kriittiseen infrastruktuuriin, demokraattisiin instituutioihin ja prosesseihin[86], sekä toimitusketjuihin kohdistuvien hyökkäysten ja teollis- ja tekijänoikeuksien kybervarkauksien torjuntaa. Kannanotossa olisi hahmoteltava, miten EU ja jäsenvaltiot voisivat hyödyntää poliittisia, taloudellisia, diplomaattisia, oikeudellisia ja strategisia viestintävälineitään haitallisen kybertoiminnan torjunnassa, sekä pohdittava, miten EU ja jäsenvaltiot voisivat edistää valmiuksiaan haitalliseen kybertoimintaan syyllistyvien löytämiseksi. Lisäksi korkea edustaja pyrkii yhdessä neuvoston ja komission kanssa tarkastelemaan **kyberdiplomatian välineistön lisätoimenpiteitä**, mukaan lukien mahdollisuutta uusiin rajoittaviin toimenpiteisiin sekä tarkastelemaan **määräenemmistöpäätöksiä kyberhyökkäysten vastaisten horisontaalisten pakotteiden yhteydessä**. Lisäksi EU:n olisi toteutettava lisätoimia **vahvistaakseen yhteistyötä kansainvälisten kumppaneiden kanssa**, Nato mukaan luettuna, edistääkseen uhkaympäristöä koskevaa yhteistä ymmärrystä, kehittääkseen yhteistyömekanismeja ja määrittääkseen yhteistyöhön perustuvia diplomaattisia toimia.

Korkea edustaja aikoo myös ehdottaa yhdessä komission kanssa **kyberdiplomatian välineistön täytäntöönpanoa koskevien suuntaviivojen päivittämistä**[87], myös päätöksentekoprosessin tehostamiseksi. Hän järjestää myös edelleen säännöllisesti kyberdiplomatian välineistöä koskevia harjoituksia ja arviointeja. Lisäksi EU:n olisi **integroitava kyberdiplomatian välineistö tiiviimmin EU:n kriisimekanismeihin** ja pyrittävä synergiaan sellaisten toimien kanssa, joita toteutetaan hybridiuhkien torjumista koskevan yhteisen kehyksen[88] ja demokratiaa koskevan eurooppalaisen toimintasuunnitelman puitteissa hybridiuhkien, disinformaation ja ulkomaisen sekaantumisen torjumiseksi. Tässä yhteydessä EU:n olisi pohdittava, miten kyberdiplomatian välineistö ja SEU-sopimuksen 42 artiklan 7 kohdan ja SEUT-sopimuksen 222 artiklan[89] mahdollinen käyttö vaikuttavat toisiinsa.

[85] Esimerkiksi EU:n yhtenäisen tiedustelun analysointikyky (SIAC) ja tarvittaessa PRY-yhteistyön puitteissa perustetut asiaankuuluvat hankkeet sekä vuoden 2018 nopea hälytysjärjestelmä (RAS), joka perustettiin tukemaan EU:n yleistä lähestymistapaa disinformaation torjuntaan.

[86] Erityisesti pyrkimällä synergiaan eurooppalaisen demokratian toimintasuunnitelman mukaisten aloitteiden kanssa.

[87] 13007/17.

[88] https://eur-lex.europa.eu/legal-content/fi/TXT/PDF/?uri=CELEX:52016JC0018&from=fi

[89] Keskinäistä puolustusta koskeva lauseke, yhteisvastuulauseke.

2.4 Kyberpuolustusvalmiuksien tehostaminen

EU:n ja jäsenvaltioiden on parannettava valmiuksiaan ehkäistä kyberuhkia ja reagoida niihin vuonna 2016 annettuun EU:n globaalistrategiaan[90] perustuvan EU:n tavoitetason mukaisesti. Tätä varten korkea edustaja aikoo yhteistyössä komission kanssa **tarkastella uudelleen kyberpuolustuspolitiikan kehystä** tehostaakseen koordinointia ja yhteistyötä EU:n toimijoiden[91] välillä sekä jäsenvaltioiden kanssa ja niiden välillä, myös yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) operaatioiden osalta. Kyberpuolustuspolitiikan kehyksessä olisi annettava tietoja tulevaa strategista kompassia[92] varten ja varmistettava, että kyberturvallisuus ja kyberpuolustus sisällytetään laajempaan turvallisuus- ja puolustusohjelmaan.

Vuonna 2018 EU määritteli kybertoimintaympäristön toiminnan alueeksi (domain of operations)[93]. EU:n sotilaskomitean tulevassa asiakirjassa, joka käsittelee **sotilaallista visiota ja strategiaa kyberavaruudesta toiminnan alueena** (”Military Vision and Strategy on Cyberspace as a Domain of Operations”) olisi määriteltävä tarkemmin, miten kyberavaruus toiminnan alueena mahdollistaa EU:n YTPP-sotilasoperaatiot. Euroopan puolustusviraston (EDA) perustama **sotilaallinen CERT-verkosto**[94] lisää merkittävästi jäsenvaltioiden välistä yhteistyötä. Lisäksi avaruusohjelman vastuulle kuuluvien kriittisten avaruusinfrastruktuurien kyberturvallisuuden varmistamiseksi vahvistetaan Euroopan avaruusohjelmavirastoa ja erityisesti Galileon turvallisuuden valvontakeskusta. Viraston toimivaltaa laajennetaan muihin avaruusohjelman kriittisiin resursseihin.

EU:n ja jäsenvaltioiden olisi annettava lisäpontta **huipputason kyberpuolustusvoimavarojen kehittämiselle** EU:n eri politiikkojen ja välineiden, erityisesti kyberpuolustuspolitiikan kehyksen, avulla ja tarvittaessa Euroopan puolustusviraston työn pohjalta. Tämä edellyttää, että painotetaan voimakkaasti tekoälyn, salauksen ja kvanttilaskennan kaltaisten keskeisten teknologioiden kehittämistä ja käyttöä. EU:n vuoden 2018 voimavarojen kehittämisen painopisteiden[95] mukaisesti ja ensimmäisen täysimääräisen puolustuksen koordinoidun vuosittaisen tarkastelun (CARD)[96] tulosten perusteella EU:n olisi edelleen edistettävä jäsenvaltioiden välistä yhteistyötä **kyberpuolustuksen tutkimuksessa, innovoinnissa ja voimavarojen kehittämisessä**. Sen olisi samalla kannustettava

[90] Neuvoston päätelmät (14149/16) EU:n globaalistrategian täytäntöönpanosta turvallisuus- ja puolustuspolitiikan alalla.
[91] Erityisesti Euroopan ulkosuhdehallinto, mukaan lukien EU:n sotilasesikunta (EUSE), Euroopan turvallisuus- ja puolustusakatemia (ETPA), komissio ja EU:n virastot, erityisesti Euroopan puolustusvirasto (EDA).
[92] Neuvoston päätelmät turvallisuus- ja puolustuspolitiikasta, 17. kesäkuuta 2020 (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/fi/pdf
[94] EU:n sotilaallisen CERT-verkoston perustaminen vastaa vuoden 2018 kyberpuolustuspolitiikan kehyksessä määritettyä tavoitetta, ja sen tavoitteena on edistää aktiivista vuorovaikutusta ja tietojenvaihtoa EU:n jäsenvaltioiden sotilaallisten CERT-ryhmien välillä.
[95] Jäsenvaltiot sopivat kesäkuussa 2018 Euroopan puolustusviraston johtokunnassa EU:n tason puolustusyhteistyön ohjaamisesta.
[96] Puolustusministerit hyväksyivät sen Euroopan puolustusviraston johtokunnassa marraskuussa 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

jäsenvaltioita hyödyntämään kaikkia **pysyvän rakenteellisen yhteistyön (PRY)**[97] ja **Euroopan puolustusrahaston**[98] tarjoamia mahdollisuuksia.

Siviili-, puolustus- ja avaruusteollisuuden välisiä synergioita koskevaan komission toimintasuunnitelmaan, joka on määrä esittää vuoden 2021 ensimmäisellä neljänneksellä, sisältyy toimia synergian tukemiseksi ohjelmien, teknologian, innovoinnin ja aloittelevien yritysten tasolla asianomaisten ohjelmien[99] hallinnoinnin mukaisesti.

Lisäksi olisi kehitettävä asiaankuuluvia synergioita ja rajapintoja sellaisten kyberpuolustusaloitteiden välillä, joita edistetään muissa yhteyksissä, mukaan lukien jäsenvaltioiden PRY-yhteistyön[100] puitteissa sekä EU:n kyberturvallisuusrakenteiden kanssa toteutetut kyberalan yhteistyöhankkeet, jotta voidaan tukea tietojen jakamista ja keskinäistä tukea.

Strategiset aloitteet

EU:n pitäisi

- saattaa valmiiksi Euroopan kyberturvallisuuden kriisinhallintakehys ja määrittää yhteisen kyberturvallisuusyksikön perustamisprosessi, välitavoitteet ja aikataulu
- jatkaa kyberrikollisuutta koskevan ohjelman täytäntöönpanoa turvallisuusunionistrategian mukaisesti
- kannustaa ja helpottaa EU:n tiedusteluanalyysikeskukseen sijoitettavan jäsenvaltioiden kybertiedustelua käsittelevän työryhmän perustamista
- edistää kyberpelotetta koskevan kannan soveltamista estääkseen, hillitäkseen, ehkäistäkseen ja torjuakseen haitallista kybertoimintaa ja vastatakseen siihen
- tarkistaa kyberpuolustuspolitiikan kehystä
- helpottaa EU:n sotilaallista visiota ja strategiaa kyberavaruudesta toiminnan alueena koskevan asiakirjan kehittämistä YTPP:n sotilasoperaatioita varten
- tukea siviili-, puolustus- ja avaruusteollisuuden välisiä synergioita ja
- vahvistaa kriittisten avaruusinfrastruktuurien kyberturvallisuutta avaruusohjelman puitteissa.

[97] Tällä hetkellä on käynnissä useita kyberturvallisuuteen liittyviä PRY-hankkeita, erityisesti kyberuhkia ja kybertapahtumiin reagoimista käsittelevä tiedonvaihtoalusta, kyberalan nopean toiminnan ryhmät ja kyberturvallisuuteen liittyvä keskinäinen avunanto, EU:n kyberakatemia ja innovaatiokeskittymä sekä kyber- ja tietoalan koordinointikeskus (CIDCC).

[98] Komissio on jo yksilöinyt Euroopan puolustusrahaston puitteissa mahdollisuuksia yhteistyöhön perustuviin kyberpuolustuksen tutkimus- ja kehittämistoimiin, joilla pyritään vahvistamaan yhteistyötä, innovointivalmiuksia ja puolustusteollisuuden kilpailukykyä.

[99] Kuten Horisontti Eurooppa, Digitaalinen Eurooppa ja Euroopan puolustusrahasto.

[100] https://pesco.europa.eu/

3. MAAILMANLAAJUISEN JA AVOIMEN KYBERTOIMINTAYMPÄRISTÖN EDISTÄMINEN

EU:n olisi jatkettava yhteistyötä kansainvälisten kumppaneiden kanssa edistääkseen poliittista mallia ja visiota kybertoimintaympäristöstä, joka perustuu oikeusvaltioperiaatteeseen, ihmisoikeuksiin, perusvapauksiin ja demokraattisiin arvoihin, tukeakseen maailmanlaajuista sosiaalista, taloudellista ja poliittista kehitystä ja edistääkseen turvallisuusunionia. Kansainvälinen yhteistyö on olennaisen tärkeää, jotta kybertoimintaympäristö voidaan pitää maailmanlaajuisena, avoimena, vakaana ja turvallisena. Tätä varten EU:n olisi jatkettava yhteistyötä kolmansien maiden, kansainvälisten järjestöjen sekä monisidosryhmäisen yhteisön kanssa johdonmukaisen ja kokonaisvaltaisen kansainvälisen kyberpolitiikan kehittämiseksi ja toteuttamiseksi ottaen huomioon, että uusien teknologioiden, sisäisen turvallisuuden sekä ulko-, turvallisuus- ja puolustuspolitiikan taloudellisten näkökohtien välillä on yhä enemmän yhteyksiä. EU on keskeisiin demokraattisiin arvoihin, oikeusvaltioperiaatteeseen ja perusoikeuksien kunnioittamiseen perustuva vahva talous- ja kaupparyhmittymä, ja sillä on myös ainutlaatuinen asema, josta se voi johtaa kansainvälisten normien ja standardien määrittelyä ja edistämisestä.

3.1 EU:n johtoasema kybertoimintaympäristön standardeissa, normeissa ja kehyksissä

Kansainvälisen standardoinnin tehostaminen

Edistääkseen ja puolustaakseen kybertoimintaympäristöä koskevaa visiotaan kansainvälisellä tasolla EU:n on **tehostettava osallistumistaan kansainvälisiin standardointiprosesseihin ja johtajuuttaan niissä sekä lisättävä edustustaan kansainvälisissä ja eurooppalaisissa standardointielimissä sekä muissa standardointiorganisaatioissa**[101]. Koska digitaaliteknologia kehittyy nopeasti, kansainväliset standardit ovat yhä tärkeämpiä perinteisten sääntelytoimien täydentämiseksi tekoälyn, pilvipalvelujen, kvanttilaskennan ja kvanttiviestinnän kaltaisilla aloilla. Kolmannet maat käyttävät yhä enemmän kansainvälistä standardointia edistääkseen poliittista ja ideologista ohjelmaansa, joka ei useinkaan vastaa EU:n arvoja. Lisäksi on yhä suurempi riski, että kansainvälistä standardointia varten syntyy kilpailevia järjestelmiä, mikä johtaa pirstaloitumiseen.

Uusien teknologioiden ja keskeisten internet-arkkitehtuurien kansainvälisten standardien muokkaaminen EU:n arvojen mukaisiksi on olennaisen tärkeää, jotta voidaan varmistaa, että internet pysyy maailmanlaajuisena ja avoimena, että teknologiat ovat ihmiskeskeisiä ja tietoturvallisia ja että niiden käyttö on laillista, turvallista ja eettistä. Osana tulevaa standardointistrategiaansa EU:n olisi määriteltävä **kansainvälistä standardointia koskevat tavoitteensa** ja toteutettava ennakoivia ja koordinoituja toimia niiden edistämiseksi kansainvälisellä tasolla. Samanmielisten kumppanien ja eurooppalaisten sidosryhmien kanssa olisi pyrittävä tiiviimpään yhteistyöhön ja taakanjakoon.

Valtion vastuullisen toiminnan edistäminen kybertoimintaympäristössä

EU tekee edelleen yhteistyötä kansainvälisten kumppaneiden kanssa edistääkseen maailmanlaajuista, avointa, vakaata ja turvallista kybertoimintaympäristöä, jossa

[101] Esim. kansainvälinen standardisoimisjärjestö (ISO), kansainvälinen sähkötekniikan toimikunta (IEC), kansainvälinen televiestintäliitto (ITU), Euroopan standardointikomitea (CEN), Euroopan sähkötekniikan standardointikomitea (CENELEC), Euroopan telealan standardointilaitos (ETSI), Internet Engineering Task Force (IETF), 3rd Generation Partnership Project -yhteistyöorganisaatio (3GPP) ja kansainvälinen sähkö- ja elektroniikkainsinöörien järjestö (IEEE).

noudatetaan kansainvälistä oikeutta, erityisesti Yhdistyneiden kansakuntien (YK) peruskirjaa[102], ja jossa noudatetaan **valtion vastuullista toimintaa koskevia vapaaehtoisia ei-sitovia normeja, sääntöjä ja periaatteita.**[103] Koska kansainvälistä turvallisuutta kybertoimintaympäristössä koskevan monenvälisen keskustelun vaikuttavuus on heikentynyt, EU:n ja jäsenvaltioiden on selvästi omaksuttava ennakoivampi kanta YK:ssa ja muilla asiaankuuluvilla kansainvälisillä foorumeilla käytävissä keskusteluissa. EU:lla on parhaat edellytykset **edistää, koordinoida ja vahvistaa jäsenvaltioiden kantoja kansainvälisillä foorumeilla, ja sen** olisi **muodostettava EU:n yhteinen kanta kansainvälisen oikeuden soveltamiseen kybertoimintaympäristössä**. Korkea edustaja pyrkii yhdessä jäsenvaltioiden kanssa edistämään YK:ssa osallistavaa ja yhteisymmärrykseen perustuvaa ehdotustaan poliittisesta sitoutumisesta **toimintaohjelmaan**[104]**, joka koskee valtion vastuullisen toiminnan edistämistä kybertoimintaympäristössä**. Kyseinen toimintaohjelma tarjoaa YK:n yleiskokouksen[105] hyväksymän voimassa olevan säännöstön pohjalta foorumin yhteistyölle ja parhaiden käytäntöjen vaihdolle YK:ssa ja ehdottaa sellaisen mekanismin perustamista, jolla pannaan täytäntöön valtion vastuullisen toiminnan normit ja edistetään valmiuksien kehittämistä. Lisäksi korkea edustaja pyrkii vahvistamaan ja kannustamaan **luottamusta lisäävien toimenpiteiden** toteuttamista valtioiden välillä jakamalla parhaita käytäntöjä alueellisella ja monenvälisellä tasolla ja edistämällä alueiden välistä yhteistyötä.

Maailmanlaajuisten yhteyksien parantaminen ei saisi johtaa sensuuriin, laajamittaiseen valvontaan, tietoturvaloukkauksiin eikä tukahduttamistoimiin, jotka kohdistuvat kansalaisyhteiskuntaan, tiedemaailmaan tai kansalaisiin. EU:n olisi jatkossakin johdettava **ihmisoikeuksien ja perusvapauksien** suojelua ja edistämistä verkossa. Tätä varten EU:n olisi edistettävä kansainvälisen ihmisoikeuslainsäädännön ja -normien[106] noudattamista ja pantava täytäntöön ihmisoikeuksia ja demokratiaa koskeva toimintasuunnitelmansa (2020–2024)[107] sekä edistettävä sananvapautta verkossa ja verkon ulkopuolella koskevia ihmisoikeussuuntaviivojaan[108] ja **annettava näin uutta pontta EU:n välineiden käytännön soveltamiseen**. EU:n olisi pyrittävä jatkuvasti **suojelemaan ihmisoikeuksien puolustajia, kansalaisyhteiskuntaa ja tiedeyhteisöä, jotka työskentelevät muun muassa kyberturvallisuuden, tietosuojan, valvonnan ja verkossa tapahtuvan sensuurin parissa.** Tätä varten EU:n olisi annettava lisää käytännön ohjeita, edistettävä parhaita käytäntöjä ja tehostettava toimiaan uusien teknologioiden väärinkäytön estämiseksi erityisesti käyttämällä tarvittaessa diplomaattisia toimenpiteitä sekä tällaisten teknologioiden vientivalvontaa. EU:n olisi myös jatkettava toimia yhteiskunnan haavoittuvimpien jäsenten suojelemiseksi verkossa esittämällä lainsäädäntöä, jolla lapsia suojellaan paremmin seksuaaliselta hyväksikäytöltä ja riistolta, ja lasten oikeuksia koskeva strategia.

---

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Tämä käy ilmi valtion vastuullisen käyttäytymisen edistämistä kybertoimintaympäristössä kansainvälisen turvallisuuden kannalta käsittelevien hallitusten asiantuntijaryhmien (UNGGE) asiaa koskevista raporteista, jotka YK:n yleiskokous on hyväksynyt, ja erityisesti vuosien 2015, 2013 ja 2010 raporteista.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Tämä käy ilmi valtion vastuullisen käyttäytymisen edistämistä kybertoimintaympäristössä kansainvälisen turvallisuuden kannalta käsittelevien hallitusten asiantuntijaryhmien (UNGGE) asiaa koskevista raporteista, jotka YK:n yleiskokous on hyväksynyt, ja erityisesti vuosien 2015, 2013 ja 2010 raporteista.

[106] Erityisesti YK:n peruskirja ja ihmisoikeuksien yleismaailmallinen julistus.

[107] https://www.consilium.europa.eu/fi/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

Kyberrikollisuutta koskeva Budapestin yleissopimus

EU tukee edelleen kolmansia maita, jotka haluavat liittyä **Euroopan neuvoston kyberrikollisuutta koskevaan Budapestin yleissopimukseen**, ja pyrkii viimeistelemään **Budapestin yleissopimuksen toisen lisäpöytäkirjan**, joka sisältää toimenpiteitä ja suojatoimia kansainvälisen yhteistyön parantamiseksi lainvalvonta- ja oikeusviranomaisten välillä sekä muiden maiden viranomaisten ja palveluntarjoajien välillä ja jonka neuvotteluihin komissio osallistuu EU:n puolesta[109]. Nykyinen YK:n tasolla esitetty aloite kyberrikollisuutta koskevaksi uudeksi oikeudelliseksi välineeksi uhkaa voimistaa jakolinjoja ja hidastaa kipeästi kaivattuja kansallisia uudistuksia ja niihin liittyviä valmiuksien kehittämistoimia, mikä saattaa haitata tehokasta kansainvälistä yhteistyötä kyberrikollisuuden torjumiseksi. EU ei pidä tarpeellisena kyberrikollisuutta koskevaa uutta oikeudellista välinettä YK:n tasolla. EU jatkaa **kyberrikollisuutta koskevaa monenvälistä tietojenvaihtoa** varmistaakseen ihmisoikeuksien ja perusvapauksien kunnioittamisen osallistamalla sekä käyttämällä avoimuutta ja käytettävissä olevaa asiantuntemusta. Tavoitteena on tuottaa lisäarvoa kaikille.

3.2 Yhteistyö kumppanien ja monisidosryhmäisen yhteisön kanssa

EU:n olisi **vahvistettava ja laajennettava kybervuoropuhelujaan kolmansien maiden kanssa** edistääkseen kybertoimintaympäristöä koskevia arvojaan ja visioitaan, jakaakseen parhaita käytäntöjä ja pyrkiäkseen tehokkaampaan yhteistyöhön. EU:n olisi myös käynnistettävä **jäsennelty tietojenvaihto alueellisten järjestöjen** kanssa, kuten Afrikan unioni, ASEANin alueellinen foorumi, Amerikan valtioiden järjestö ja Euroopan turvallisuusyhteistyöjärjestö. Samalla EU:n olisi pyrittävä mahdollisuuksien mukaan löytämään muiden kumppaneiden kanssa yhteinen lähestymistapa yhteistä etua koskeviin kysymyksiin. Toimimalla yhteistyössä EU:n edustustojen ja tarvittaessa eri puolilla maailmaa sijaitsevien jäsenvaltioiden suurlähetystöjen kanssa EU:n olisi muodostettava epävirallinen **EU:n kyberdiplomatian verkosto**, jolla edistetään EU:n visiota kybertoimintaympäristöstä, vaihdetaan tietoja ja koordinoidaan säännöllisesti kybertoimintaympäristön kehitystä.[110]

EU:n olisi jatkettava 8. heinäkuuta 2016[111] ja 10. heinäkuuta 2018[112] annettujen yhteisten julkilausumien pohjalta **EU:n ja Naton yhteistyön** edistämistä erityisesti kyberpuolustuksen yhteentoimivuusvaatimusten osalta. Tässä yhteydessä EU:n olisi jatkettava asiaankuuluvien YTPP-rakenteiden liittämistä Naton operaatioiden verkostoon (Federated Mission Networking), mikä mahdollistaisi tarvittaessa verkostojen yhteentoimivuuden Naton ja kumppanien kanssa. Lisäksi olisi tutkittava edelleen mahdollisuuksia EU:n ja Naton koulutus- ja harjoitusyhteistyöhön muun muassa pyrkimällä synergiaan Euroopan turvallisuus- ja puolustusakatemian ja Naton kyberpuolustuksen osaamiskeskuksen välillä.

Arvojensa mukaisesti EU tukee ja edistää voimakkaasti **internetin monisidosryhmäistä hallintomallia**. Yksikään yksittäinen taho, hallitus tai kansainvälinen järjestö ei saisi pyrkiä valvomaan internetiä. EU:n olisi jatkettava toimintaansa foorumeilla[113] tehostaakseen yhteistyötä ja varmistaakseen perusoikeuksien ja -vapauksien suojelun, erityisesti oikeuden

[109] Neuvoston päätös, tehty kesäkuussa 2019 (viite 9116/19).
[110] Se voisi tarvittaessa hyödyntää myös jäsenvaltioiden ulkoministeriöitä yhdistävän epävirallisen EU:n digitaalisen diplomatian verkoston toimintaa.
[111] http://www.consilium.europa.eu/fi/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/fi/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Esimerkiksi Internet Cooperation for Assigned Names and Numbers (ICANN) ja internetin hallintofoorumi (Internet Governance Forum, IGF).

ihmisarvoon, yksityisyydensuojan sekä sananvapauden ja tiedonvälityksen vapauden. Edistääkseen monisidosryhmäistä yhteistyötä kyberturvallisuuskysymyksissä komissio ja korkea edustaja pyrkivät toimivaltojensa rajoissa vahvistamaan **säännöllistä ja jäsenneltyä tietojenvaihtoa** sidosryhmien kanssa, yksityinen sektori, tiedemaailma ja kansalaisyhteiskunta mukaan luettuina, ja korostavat, että kybertoimintaympäristö on luonteeltaan yhteenliitetty, mikä edellyttää, että kaikki sidosryhmät vaihtavat tietoja ja kantavat erityisvastuunsa maailmanlaajuisen, avoimen, vakaan ja turvallisen kybertoimintaympäristön ylläpitämiseksi. Nämä toimet antavat vahvan panoksen mahdollisiin keskeisiin EU:n tason toimiin.

3.3 Maailmanlaajuisten valmiuksien vahvistaminen maailmanlaajuisen häiriönsietokyvyn parantamiseksi

Sen varmistamiseksi, että kaikki maat voivat hyötyä internetin ja teknologian käytön sosiaalisista, taloudellisista ja poliittisista eduista, EU tukee edelleen kumppaneitaan, jotta ne voivat parantaa kyberuhkien sietokykyään, valmiuksiaan tutkia kyberrikollisuutta ja nostaa syytteitä kyberrikoksista sekä puuttua kyberuhkiin. Yleisen johdonmukaisuuden varmistamiseksi EU:n olisi laadittava **EU:n ulkoisten kybervalmiuksien kehittämisohjelma**, jolla ohjataan näitä toimia ulkoisten kybervalmiuksien kehittämistä koskevien suuntaviivojen[114] ja kestävän kehityksen Agenda 2030 -toimintaohjelman[115] mukaisesti. Ohjelmassa olisi hyödynnettävä jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen asiantuntemusta ja aloitteita (mukaan lukien kybervalmiuksien kehittämistä koskeva EU:n verkosto[116]) niiden toimeksiantojen mukaisesti. On perustettava **EU:n toimielinten välinen kybervalmiuksien kehittämiskomitea**, joka kattaa asiaankuuluvat EU:n institutionaaliset sidosryhmät ja seuraa edistymistä sekä uusien synergioiden ja mahdollisten puutteiden määrittämistä. Lisäksi se voi tukea tiiviimpää yhteistyötä jäsenvaltioiden sekä julkisen ja yksityisen sektorin kumppaneiden ja muiden asiaankuuluvien kansainvälisten elinten kanssa toimien koordinoinnin varmistamiseksi ja päällekkäisyyksien välttämiseksi.

EU:n kybervalmiuksien kehittämisessä olisi edelleen keskityttävä Länsi-Balkaniin ja EU:n naapurimaihin sekä kumppanimaihin, joissa digitaalinen kehitys on nopeaa. EU:n toimilla olisi tuettava kumppanimaiden lainsäädännön ja politiikkojen kehittämistä kyberdiplomatiaa koskevien EU:n politiikkojen ja normien mukaisesti. Tässä yhteydessä kyberturvallisuuden olisi aina sisällyttävä EU:n valmiuksien kehittämispyrkimyksiin digitalisoinnin alalla. Tätä varten EU:n olisi kehitettävä koulutusohjelma EU:n henkilöstölle, joka vastaa EU:n digitaalisten ja ulkoisten kybervalmiuksien kehittämistoimien täytäntöönpanosta. EU:n olisi myös demokratiaa koskevan eurooppalaisen toimintasuunnitelman mukaisesti autettava näitä maita selviytymään vihamielisistä kybertoimista, jotka ovat koko ajan suurempi ongelma ja jotka vahingoittavat niiden yhteiskuntien kehitystä ja **demokraattisten järjestelmien koskemattomuutta ja turvallisuutta**. EU:n jäsenvaltioiden sekä asiaankuuluvien EU:n virastojen ja kolmansien maiden välinen vertaisoppiminen voisi olla erityisen hyödyllistä tässä suhteessa.

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

Vuoden 2018 YTPP-siviilialan sopimuksen[117] puitteissa YTPP-siviilioperaatiot voivat myös edistää EU:n laajempaa reagointia kyberturvallisuushaasteisiin erityisesti vahvistamalla kumppanimaiden oikeusvaltioperiaatetta sekä lainvalvonta- ja siviilihallintojen valmiuksia.

Strategiset aloitteet

EU:n pitäisi

- määritellä tavoitteet kansainvälisissä standardointiprosesseissa ja edistää niitä kansainvälisellä tasolla
- edistää kansainvälistä turvallisuutta ja vakautta kybertoimintaympäristössä, erityisesti antamalla EU:n ja sen jäsenvaltioiden ehdotuksen valtion vastuullisen toiminnan edistämistä kybertoimintaympäristössä koskevaksi toimintaohjelmaksi YK:ssa
- antaa käytännön ohjeita ihmisoikeuksien ja perusvapauksien soveltamisesta kybertoimintaympäristössä
- suojella lapsia paremmin seksuaaliselta hyväksikäytöltä ja riistolta sekä laatia lapsen oikeuksia koskeva strategia
- vahvistaa ja edistää kyberrikollisuutta koskevaa Budapestin yleissopimusta keskittyen muun muassa Budapestin yleissopimuksen toiseen lisäpöytäkirjaan
- laajentaa EU:n kybervuoropuhelua kolmansien maiden sekä alueellisten ja kansainvälisten järjestöjen kanssa, myös epävirallisen EU:n kyberdiplomatian verkoston kautta
- vahvistaa yhteistyötä monisidosryhmäisen yhteisön kanssa erityisesti säännöllisellä ja jäsennellyllä tietojenvaihdolla yksityisen sektorin, tiedemaailman ja kansalaisyhteiskunnan kanssa ja
- ehdottaa EU:n ulkoisten kybervalmiuksien kehittämisohjelmaa ja EU:n toimielinten välistä kybervalmiuksien kehittämiskomiteaa.

III. KYBERTURVALLISUUS EU:N TOIMIELIMISSÄ, ELIMISSÄ JA VIRASTOISSA

EU:n toimielimet, elimet ja virastot ovat säännöllisesti kyberhyökkäysten, erityisesti kybervakoilun, kohteina, mikä johtuu niiden korkeasta poliittisesta profiilista, niiden kriittisistä tehtävistä erittäin arkaluonteisten kysymysten koordinoinnissa ja niiden roolista suurten julkisten varojen hallinnoinnissa. Näillä toimijoilla on niille kertyneen kokemuksen vuoksi kuitenkin keskenään hyvin erilaiset valmiudet sietää kyberuhkia, havaita haitallisia kybertoimia ja reagoida niihin. Sen vuoksi on tarpeen parantaa kyberturvallisuuden yleistä tasoa johdonmukaisten ja yhtenäisten sääntöjen avulla.

Tietoturvan alalla on edistytty **EU:n turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen** suojaamista koskevien sääntöjen yhdenmukaistamisessa. Turvaluokiteltujen tietojärjestelmien yhteentoimivuus on kuitenkin edelleen vähäistä, mikä estää saumattoman tiedonsiirron eri toimijoiden välillä. On pyrittävä

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/fi/pdf

siihen, että EU:n turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen käsittelyyn voitaisiin soveltaa toimielinten välistä lähestymistapaa, joka voisi myös toimia mallina jäsenvaltioiden väliselle yhteentoimivuudelle. Olisi myös vahvistettava perustaso menettelyjen yksinkertaistamiseksi jäsenvaltioiden kanssa. EU:n olisi myös kehitettävä edelleen kykyään turvalliseen viestintään kumppaneidensa kanssa ja hyödynnettävä tässä mahdollisuuksien mukaan nykyisiä järjestelyjä ja menettelyjä.

Kuten turvallisuusunionistrategiassa ilmoitettiin, komissio tekee vuonna **2021 ehdotuksia tietoturvaa koskeviksi yhteisiksi sitoviksi säännöiksi ja kyberturvallisuutta koskeviksi yhteisiksi sitoviksi säännöiksi kaikille EU:n toimielimille, elimille ja virastoille** kyberturvallisuudesta parhaillaan käytävien EU:n toimielinten välisten keskustelujen[118] pohjalta.

Etätyön nykyiset ja tulevat suuntaukset edellyttävät myös lisäinvestointeja turvallisiin laitteisiin, infrastruktuureihin ja välineisiin, jotka mahdollistavat etätyöskentelyn arkaluonteisten ja turvallisuusluokiteltujen tiedostojen kanssa.

Lisäksi yhä vihamielisemmäksi muuttuva kyberuhkaympäristö ja EU:n toimielimiin, elimiin ja virastoihin kohdistuvien kehittyneempien kyberhyökkäysten määrän lisääntyminen lisäävät tarvetta lisätä investointeja kyberturvallisuuden korkean tason saavuttamiseksi. Kaikille EU:n toimielimille, elimille ja virastoille ollaan perustamassa kyberturvallisuustietoisuutta lisäävä ohjelma, jonka tarkoituksena on lisätä henkilöstön tietoisuutta sekä kyberhygieniaa ja tukea yhteistä kyberturvallisuuskulttuuria.

CERT-EU:n vahvistaminen paremmalla rahoitusmekanismilla on tarpeen, jotta se voi paremmin auttaa EU:n toimielimiä, elimiä ja virastoja soveltamaan uusia kyberturvallisuussääntöjä ja parantaa niiden kyberuhkien sietokykyä. CERT-EU:n toimeksiantoa on myös vahvistettava, jotta sille voidaan tarjota vankat keinot näiden tavoitteiden saavuttamiseksi.

Strategiset aloitteet

1. asetus tietoturvasta EU:n toimielimissä, elimissä ja virastoissa
2. asetus yhteisistä kyberturvallisuussäännöistä EU:n toimielimiä, elimiä ja virastoja varten
3. uusi oikeusperusta CERT-EU:lle sen toimeksiannon ja rahoituksen vahvistamiseksi.

IV. PÄÄTELMÄT

EU:n kyberturvallinen digitaalinen vuosikymmen, turvallisuusunionin toteuttaminen ja EU:n maailmanlaajuisen aseman vahvistaminen hyötyvät tämän strategian koordinoidusta täytäntöönpanosta.

EU:n olisi edistettävä standardeja ja normeja, jotka koskevat maailmanluokan ratkaisuja ja kyberturvallisuusstandardeja keskeisiä palveluja ja kriittisiä infrastruktuureja varten sekä

[118] Säännölliset EU:n toimielinten väliset keskustelut kyberturvallisuudesta ovat osa laajempaa keskustelua digitaalisen siirtymän EU:n toimielimiin kohdistamista mahdollisuuksista ja haasteista.

uusien teknologioiden kehittämistä ja soveltamista. Jokainen internetiä käyttävä organisaatio ja yksityishenkilö on osa ratkaisua, jolla varmistetaan kyberturvallinen digitaalinen siirtymä.

Komissio ja korkea edustaja seuraavat toimivaltuuksiensa mukaisesti tämän strategian edistymistä ja laativat arviointiperusteita. Seurannan olisi perustuttava ENISAn raportteihin ja komission turvallisuusunionia koskeviin säännöllisiin raportteihin. Tulokset edistävät digitaalisen vuosikymmenen tavoitteita[119]. Komissio ja korkea edustaja jatkavat toimivaltuuksiensa mukaisesti yhteydenpitoa jäsenvaltioiden kanssa määritelläkseen tarvittaessa käytännön toimenpiteitä kriittisen infrastruktuurin ja sisämarkkinoiden häiriönsietokyvyn, oikeuden ja lainvalvonnan, kyberdiplomatian ja kyberpuolustuksen muodostaman EU:n neljän kyberturvallisuusyhteisön yhdistämiseksi. Lisäksi komissio ja korkea edustaja jatkavat yhteistyötä monisidosryhmäisen yhteisön kanssa ja korostavat, että kaikkien internetiä käyttävien on tehtävä osansa sellaisen maailmanlaajuisen, avoimen, vakaan ja turvallisen kybertoimintaympäristön ylläpitämiseksi, jossa kaikki voivat elää turvallista digitaalista elämää.

[119] Kuten komission vuoden 2021 työohjelmassa ilmoitettiin.

Lisäys: seuraavat toimet 5G-verkkojen kyberturvallisuuden alalla

5G-verkkojen kyberturvallisuudesta annetun komission suosituksen[120] uudelleentarkastelun tulosten perusteella EU:n tasolla tehtävän koordinoidun työn seuraavissa vaiheissa olisi keskityttävä kolmeen keskeiseen tavoitteeseen ja seuraavassa taulukossa esitettyihin lyhyen ja keskipitkän aikavälin keskeisiin toimiin, jotka jäsenvaltioiden viranomaisten, komission ja ENISAn on toteutettava.

Seuraavan vaiheen ensisijaisena tavoitteena on **saattaa päätökseen välineistön täytäntöönpano kansallisella tasolla ja puuttua ongelmiin, jotka nousivat esiin heinäkuussa 2020 annetussa edistymiskertomuksessa**. Tässä yhteydessä **koordinointityön tai tiedonvaihdon tehostamisesta** voisi olla hyötyä joillekin välineistön strategisista toimenpiteistä verkko- ja tietoturva-alan yhteistyöryhmän puitteissa, kuten edistymiskertomuksessa jo todettiin, mikä voisi mahdollisesti johtaa **parhaiden käytäntöjen tai ohjeiden** kehittämiseen. Teknisten toimenpiteiden osalta ENISA voisi antaa lisätukea jo tekemänsä työn pohjalta, tutkia tiettyjä aiheita perusteellisemmin ja **laatia kattavan katsauksen kaikista asiaankuuluvista 5G-kyberturvallisuusvaatimuksia koskevista ohjeista matkaviestinoperaattoreille**.

Toiseksi jäsenvaltiot korostivat, että on tärkeää pysyä kehityksen vauhdissa mukana **seuraamalla jatkuvasti teknologian, 5G-arkkitehtuurin, uhkien ja 5G-käyttökohteiden ja sovellusten sekä ulkoisten tekijöiden kehitystä**, jotta voidaan **tunnistaa uusia tai kehittymässä olevia riskejä ja puuttua niihin**. Lisäksi alustavassa riskianalyysissä olisi tarkasteltava lähemmin useita näkökohtia, erityisesti sen varmistamiseksi, että siinä otetaan huomioon koko 5G-ekosysteemi, mukaan lukien kaikki asiaankuuluvat verkkoinfrastruktuurin osat ja 5G-toimitusketjun osat. Välineistö on suunniteltu joustavaksi ja mukautettavissa olevaksi, mutta keskipitkällä aikavälillä sitä voitaisiin tarvittaessa täydentää tai muuttaa, jotta se pysyisi kattavana ja ajantasaisena.

Kolmanneksi **EU:n tason toimia** olisi jatkettava välineistön tavoitteiden tukemiseksi ja täydentämiseksi ja niiden sisällyttämiseksi kokonaisuudessaan asiaankuuluviin unionin ja komission politiikkoihin, erityisesti niiden eri alojen toimien jatkotoimena, jotka komissio ilmoitti välineistöstä 29. tammikuuta 2020 antamassaan tiedonannossa[121] (esim. EU:n rahoitus turvallisille 5G-verkoille, investoinnit 5G-verkkoihin ja niiden jälkeisiin teknologioihin, kaupan suojatoimet ja kilpailu alalla, jotta vältetään 5G:n toimitusmarkkinoiden vääristyminen, jne.).

Keskeisten toimijoiden olisi tarvittaessa sovittava jäljempänä esitettyjä keskeisiä toimia koskevista yksityiskohtaisista järjestelyistä ja välitavoitteista vuoden 2021 alussa.

Päätavoite 1: yhtenäisten kansallisten lähestymistapojen varmistaminen tehokasta riskinhallintaa varten kaikkialla EU:ssa		
Alat	**Tärkeimmät lyhyen ja keskipitkän aikavälin toimet**	**Keskeiset toimijat**

[120] Komission raportti 5G-verkkojen kyberturvallisuudesta 26. maaliskuuta 2019 annetun komission suosituksen 2019/534 vaikutuksista.

[121] Komission tiedonanto COM(2020) 50, 5G:n turvallinen käyttöönotto EU:ssa – EU:n välineistön täytäntöönpano, 29. tammikuuta 2020.

Välineistön täytäntöönpano jäsenvaltioissa	Saatetaan välineistön päätelmissä suositeltujen toimenpiteiden täytäntöönpano päätökseen vuoden 2021 toiseen neljännekseen mennessä ja suoritetaan säännöllinen arviointi verkko- ja tietoturva-alan yhteistyöryhmässä.	Jäsenvaltioiden viranomaiset
Vaihdetaan toimittajiin liittyviä strategisia toimenpiteitä koskevia tietoja ja parhaita käytäntöjä	Tehostetaan tiedonvaihtoa ja tutkitaan mahdollisia parhaita käytäntöjä, jotka koskevat erityisesti seuraavia: - suuririskisiä toimittajia koskevat rajoitukset (SM03) ja järjestelmänhallintapalvelujen tarjoamiseen liittyvät toimenpiteet (SM04) - toimitusketjun turvallisuus ja häiriönsietokyky, erityisesti BEREC:n toteuttaman toimenpiteitä SM05–SM06 koskevan tutkimuksen seuranta.	Jäsenvaltioiden viranomaiset, komissio
Kehitetään valmiuksia ja annetaan teknisiä toimenpiteitä koskevia ohjeita	Perusteellisten teknisten tutkimusten toteuttaminen ja yhteisten ohjeiden ja välineiden kehittäminen, mukaan lukien seuraavat: - kattava ja dynaaminen matriisi turvavalvontatoimista ja parhaista käytännöistä 5G-turvallisuutta varten Ohjeet, joilla tuetaan välineistöstä valikoitujen teknisten toimenpiteiden toteuttamista.	ENISA, Jäsenvaltioiden viranomaiset
Päätavoite 2: Tuetaan jatkuvaa tiedonvaihtoa ja valmiuksien kehittämistä		
Alat	**Tärkeimmät lyhyen ja keskipitkän aikavälin toimet**	**Keskeiset toimijat**
Lisätään jatkuvasti tietämystä	Järjestetään tietämystä lisääviä toimia, jotka koskevat teknologiaa ja siihen liittyviä haasteita (avoimet arkkitehtuurit, 5G-ominaisuudet – esim. virtualisointi, kontittaminen, viipalointi jne.), uhkaympäristön kehitystä, tapahtuneita poikkeamia jne.	ENISA, jäsenvaltioiden viranomaiset, muut sidosryhmät
Riskinarvioinnit	Päivitetään ja vaihdetaan tietoja, jotka koskevat ajan tasalle saatettuja kansallisia riskinarviointeja.	Jäsenvaltioiden viranomaiset, komissio, ENISA
Yhteiset EU:n rahoittamat hankkeet välineistön täytäntöönpanon tukemiseksi	Tarjotaan taloudellista tukea välineistön täytäntöönpanoa tukeville hankkeille käyttämällä EU:n rahoitusta, erityisesti Digitaalinen Eurooppa -ohjelmasta (esim. kansallisten viranomaisten valmiuksien kehittämishankkeet, testausalustat tai muut kehittyneet valmiudet).	Jäsenvaltioiden viranomaiset, komissio
Sidosryhmien välinen yhteistyö	Edistetään yhteistyötä 5G-kyberturvallisuuden alalla toimivien kansallisten viranomaisten (esim. verkko- ja tietoturva-alan yhteistyöryhmä, kyberturvallisuusviranomaiset, televiestinnän sääntelyviranomaiset) ja yksityisten sidosryhmien kanssa.	Jäsenvaltioiden viranomaiset, komissio, ENISA
Päätavoite 3: Edistetään toimitusketjun häiriönsietokykyä ja muita EU:n strategisia turvallisuustavoitteita		
Alat	**Tärkeimmät lyhyen ja keskipitkän aikavälin toimet**	**Keskeiset toimijat**
Standardointi	Määritellään ja pannaan täytäntöön konkreettinen toimintasuunnitelma, jolla voidaan lisätä EU:n edustusta standardointielimissä, osana verkko- ja tietoturva-alan standardointia käsittelevän alaryhmän työn seuraavia	Jäsenvaltioiden viranomaiset

	vaiheita, jotta voidaan saavuttaa erityiset turvallisuustavoitteet, mukaan lukien yhteentoimivien rajapintojen edistäminen toimittajien monipuolisuuden lisäämiseksi.	
Toimitusketjun häiriönsietokyky	- Tehdään perusteellinen analyysi 5G-ekosysteemistä ja toimitusketjusta, jotta voidaan paremmin tunnistaa ja seurata keskeisiä kohteita ja mahdollisia kriittisiä riippuvuuksia. - Varmistetaan, että 5G-markkinoiden ja toimitusketjun toiminta on EU:n kauppaa ja kilpailua koskevien sääntöjen ja tavoitteiden mukaista, sellaisina kuin ne on määritelty komission 29. tammikuuta antamassa tiedonannossa, ja että suorien ulkomaisten sijoitusten seurantaa sovelletaan investointikehitykseen, joka saattaa vaikuttaa 5G-arvoketjuun, ottaen huomioon välineistön tavoitteet. - Seurataan nykyisiä ja odotettavissa olevia markkinasuuntauksia ja arvioidaan Open RAN -järjestelmän riskejä ja mahdollisuuksia erityisesti riippumattoman tutkimuksen avulla.	Jäsenvaltioiden viranomaiset, komissio
Sertifiointi	Aloitetaan keskeisten 5G-komponenttien ja -toimittajien ehdolla olevien prosessien sertifiointijärjestelmien valmistelu, jotta voidaan puuttua tiettyihin teknisiin haavoittuvuuksiin liittyviin riskeihin, sellaisina kuin ne on määritelty välineistön riskinhallintasuunnitelmissa.	Komissio, ENISA, kansalliset viranomaiset, muut sidosryhmät
EU:n valmiudet ja verkon turvallinen käyttöönotto	- Investoidaan tutkimukseen ja innovointiin sekä valmiuksiin erityisesti hyväksymällä älykkäitä verkkoja ja palveluja koskeva kumppanuus. - Pannaan täytäntöön EU:n rahoitusohjelmien ja -välineiden (sisäiset ja ulkoiset) turvallisuusehdot komission 29. tammikuuta antaman tiedonannon mukaisesti.	Jäsenvaltiot, komissio, 5G-alan sidosryhmät
Ulkoiset näkökohdat	Vastataan myönteisesti kolmansien maiden pyyntöihin, jotka haluavat ymmärtää ja mahdollisesti käyttää EU:n kehittämää välineistöä.	Jäsenvaltiot, komissio, EUH, EU:n edustustot