EUROOPAN
KOMISSIO

UNIONIN ULKOASIOIDEN
JA TURVALLISUUSPOLITIIKAN
KORKEA EDUSTAJA

Bryssel 13.9.2017
JOIN(2017) 450 final

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

1. JOHDANTO

Kyberturvallisuus on erittäin tärkeää hyvinvointimme ja turvallisuutemme kannalta. Arkemme ja taloutemme ovat koko ajan yhä riippuvaisempia digitaaliteknologiasta, jolloin olemme yhä alttiimpia uhille. Kyberturvallisuuspoikkeamat muuttuvat erilaisemmiksi sen osalta, kuka on vastuussa, ja myös sen osalta, mikä on heidän tavoitteenaan. Haitalliset kybertoimet ovat uhka talouksillemme ja digitaalisten sisämarkkinoiden vetokyvylle, mutta myös demokratioidemme, vapauksiemme ja arvojemme toiminnalle. Turvallisuutemme tulevaisuudessa riippuu siitä, miten kykenemme muokkaamaan taitojamme suojella EU:ta kyberuhkia vastaan. Siviili-infrastruktuuri ja sotilaalliset valmiudet ovat riippuvaisia turvallisista digitaalisista järjestelmistä. Tämä on tunnustettu kesäkuun 2017 Eurooppa-neuvostossa[1] ja EU:n ulko- ja turvallisuuspoliittisessa globaalistrategiassa[2].

Riskit kasvavat eksponentiaalisesti. Tutkimusten mukaan kyberrikollisuuden vaikutus talouteen viisinkertaistui vuosien 2013 ja 2017 välillä, ja se voi edelleen nelinkertaistua vuoteen 2019 mennessä[3]. Erityisesti kiristyshaittaohjelmat[4] ovat lisääntyneet, ja viimeaikaiset hyökkäykset[5] osoittavat, miten dramaattisesti kyberrikollisten toiminta on kasvanut. Kiristyshaittaohjelmat eivät kuitenkaan ole läheskään ainoa uhka.

Kyberuhat ovat lähtöisin valtiosta riippumattomilta ja valtiollisilta toimijoilta. Uhkien motiivi on usein rikollinen voiton tavoittelu, mutta ne voivat olla luonteeltaan myös poliittisia tai strategisia. Rikollisuuden uhka kasvaa kyberrikollisuuden ja perinteisen rikollisuuden välisen rajan hämärtyessä, kun rikolliset käyttävät internetiä laajentamaan toimintaansa ja lähteenä uusien rikoksentekomenetelmien ja -välineiden löytämiseksi[6]. Silti valtaosassa tapauksista mahdollisuus jäljittää rikollinen on vain hyvin pieni, ja syytteen nostamisen mahdollisuus on sitäkin pienempi.

Samaan aikaan valtiolliset toimijat toteuttavat geopoliittisia tavoitteitaan käyttämällä paitsi perinteisiä välineitä, kuten sotilaallista voimaa, myös vähemmän huomiota herättäviä kybervälineitä, joihin kuuluu sisäisiin demokraattisiin prosesseihin vaikuttaminen. Nykyisin tunnustetaan laajasti, että kyberympäristöä käytetään sodan taistelukenttänä joko sellaisenaan tai osana hybridimallia. Elintärkeään infrastruktuuriin kohdistuvat disinformaatiokampanjat, valeuutiset ja kyberoperaatiot ovat yleistymässä, ja niihin on reagoitava. Tästä syystä komissio korosti yhteistyön merkitystä kyberpuolustuksen alalla Euroopan puolustuksen tulevaisuutta[7] käsittelevässä pohdinta-asiakirjassaan.

Jollemme merkittävästi paranna kyberturvallisuuttamme, riski kasvaa digitalisaatiokehityksen myötä. Internetiin oletetaan olevan vuoteen 2020 mennessä kytkettynä kymmeniä miljardeja ”esineiden internetin” laitteita, mutta kyberturvallisuutta ei ole vielä asetettu ensisijaiseksi niiden suunnittelussa[8]. Sähköverkkoja, autoja ja liikenneverkkoja, tehtaita, rahoitusalaa,

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Katso esimerkiksi McAfee ja Centre for Strategic and International Studies ”Net losses: Estimating the Global Cost of Cybercrime” 2014.

4 Kiristyshaittaohjelma on haittaohjelma, joka estää tai rajoittaa käyttäjän pääsyä järjestelmään joko lukitsemalla järjestelmän näytön tai käyttäjän tiedostot, jos lunnaita ei makseta.

5 WannaCry-kiristyshaittaohjelmalla toukokuussa 2017 tehdyn hyökkäyksen vaikutus ulottui yli 400 000 tietokoneeseen yli 150 maassa. Kuukautta myöhemmin Petya-kiristyshaittaohjelmalla tehty hyökkäys iski Ukrainaan ja useisiin yrityksiin kaikkialla maailmassa.

6 Europolin vuonna 2017 laatima vakavaa ja järjestäytynyttä rikollisuutta koskeva uhkakuva-arvio (Serious and Organised Crime Threat Assessment).

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_fi.pdf.

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, komissiolle tehty tutkimus.

sairaaloita ja koteja valvovien laitteiden suojaamatta jättämisellä voisi olla tuhoisat vaikutukset ja se voisi vahingoittaa vakavasti kuluttajien luottamusta uusiin teknologioihin. Siviilikohteisiin kohdistuvien poliittisiin vaikuttimiin perustuvien hyökkäysten riski ja sotilaallisen kyberpuolustuksen puutteiden riski syventävät uhkaa entisestään.

Tässä yhteisessä tiedonannossa esitetty lähestymistapa antaa EU:lle paremmat valmiudet kohdata nämä uhat. Sen avulla voidaan lisätä resilienssiä ja strategista riippumattomuutta, lisätä teknologian ja taitojen valmiuksia sekä auttaa luomaan vahvat sisämarkkinat. Tämä edellyttää oikeanlaisia rakenteita vahvan kyberturvallisuuden rakentamiseksi ja tarvittaessa reagoimiseksi niin, että kaikki avaintoimijat osallistuvat täysimääräisesti. Tämä lähestymistapa auttaisi myös ehkäisemään kyberhyökkäyksiä tehostamalla tekijöiden havaitsemista, jäljittämistä ja vastuuseen saattamista. Siinä otettaisiin huomioon myös globaali ulottuvuus kehittämällä kansainvälistä yhteistyötä foorumiksi EU:n johtajuudelle kyberturvallisuuden alalla. Nämä toimet perustuvat digitaalisten sisämarkkinoiden, globaalistrategian, Euroopan turvallisuusagendan[9], hybridiuhkien torjumista koskevan yhteisen kehyksen[10] ja EU:n puolustusrahaston käyttöönotosta annetun tiedonannon lähestymistapaan[11][12].

EU tekee jo töitä usealla eri alalla ongelmiin reagoimiseksi. On tullut aika vetää langat yhteen. Vuonna 2013 EU esitti kyberturvallisuusstrategian, jolla käynnistettiin useita keskeisiä toimintalinjoja kyberresilienssin vahvistamiseksi[13]. Sen keskeiset tavoitteet ja periaatteet luotettavan, turvallisen ja avoimen kybertoimintaympäristön edistämiseksi ovat edelleen voimassa. Jatkuvasti muuttuvat ja syventyvät uhkakuvat edellyttävät kuitenkin lisätoimia hyökkäysten torjumiseksi ja ehkäisemiseksi tulevaisuudessa[14].

EU on hyvissä asemissa kyberturvallisuuden puolustamiseksi, kun otetaan huomioon sen politiikkojen soveltamisala ja käytettävissä olevat välineet, rakenteet ja valmiudet. Vaikka jäsenvaltiot ovat edelleen vastuussa kansallisesta turvallisuudesta, uhan laajuus ja rajatylittävä luonne edellyttävät, että EU ryhtyy toimimaan tarjotakseen jäsenvaltioille aloitteita ja tukea, joilla ne voivat kehittää ja ylläpitää laajempia ja parempia kyberturvallisuuden valmiuksia, kehittäen samalla EU:n tason valmiuksia. Tämän lähestymistavan avulla voidaan saada kaikki toimijat – EU, jäsenvaltiot, teollisuus ja yksityishenkilöt – antamaan kyberturvallisuudelle etusija. Se on tarpeen resilienssin kasvattamiseksi ja kyberhyökkäyksiin reagoimisen parantamiseksi EU-tasolla. Se sisältää konkreettisia toimia, joiden avulla voidaan havaita ja tutkia kaikki EU:hun ja sen jäsenvaltioihin kohdistuvat kyberturvallisuuspoikkeamat ja vastata niihin asianmukaisesti esimerkiksi saattamalla rikolliset syytteeseen. EU:n ulkoinen toiminta voi sen avulla tehokkaasti edistää kyberturvallisuutta maailmanlaajuisesti. Tuloksena EU vaihtaa lähestymistavan jälkikäteen reagoimisesta ennakolta varautumiseen suojellakseen eurooppalaista hyvinvointia, yhteiskuntaa, arvoja sekä perusoikeuksia ja -vapauksia vastaamalla nykyisiin ja tuleviin uhkiin.

---

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Tämä lähestymistapa perustuu myös Euroopan komission tieteellisen neuvonannon mekanismin tieteellisten neuvonantajien korkean tason ryhmän antamaan tieteelliseen neuvonantoon (katso viite jäljempänä).

13 JOIN(2013) 1 final. Strategian arviointi on saatavilla asiakirjassa SWD (2017) 295.

14 Jollei toisin ilmoiteta, tässä tiedonannossa esitetyillä ehdotuksilla ei ole vaikutusta talousarvioon. Sellaisen aloitteen, jolla on vaikutus talousarvioon, on tarkoin noudatettava vuotuisia talousarviomenettelyjä, eikä se voi vaikuttaa ennalta vuoden 2020 jälkeiseen seuraavaan monivuotiseen rahoituskehykseen.

2. EU:N RESILIENSSIN KASVATTAMINEN KYBERHYÖKKÄYSTEN VARALTA

Vahva kyberresilienssi edellyttää kollektiivista ja laaja-alaista lähestymistapaa. Sitä varten rakenteiden on oltava kestävämpiä ja tehokkaampia kyberturvallisuuden edistämiseksi ja kyberhyökkäyksiin reagoimiseksi jäsenvaltioissa ja myös EU:n omissa toimielimissä, virastoissa ja elimissä. Se edellyttää myös kattavampaa ja monialaista lähestymistapaa kyberresilienssiä ja strategista riippumattomuutta rakennettaessa, vahvoja sisämarkkinoita, EU:n teknologisen valmiuden mittavia parannuksia ja osaavien asiantuntijoiden paljon suurempaa määrää. Keskeistä on hyväksyä yleisesti, että kyberturvallisuus on yhteinen yhteiskunnallinen haaste, jotta hallinnon, talouden ja yhteiskunnan eri kerrokset saadaan osallistumaan.

2.1 Euroopan unionin verkko- ja tietoturvaviraston vahvistaminen

Euroopan unionin verkko- ja tietoturvavirasto, (ENISA) on avainasemassa vahvistettaessa EU:n kyberresilienssiä ja reagoimista, mutta sen nykyinen toimeksianto rajoittaa sitä. Komissio esittää sen vuoksi kunnianhimoisen uudistusehdotuksen, joka sisältää **pysyvän toimeksiannon virastolle**[15]. Sen avulla ENISA voi tarjota tukea jäsenvaltioille, EU:n toimielimille ja keskeisten alojen yrityksille esimerkiksi verkko- ja tietojärjestelmien turvallisuudesta annetun direktiivin[16] (verkko- ja tietoturvadirektiivi) ja kyberturvallisuuden sertifiointijärjestelmien kehystä koskevan ehdotuksen täytäntöönpanemiseksi.

Uudistetulla ENISAlla on vahva neuvoa-antava rooli politiikan kehittämisessä ja täytäntöönpanossa, mukaan lukien alakohtaisten aloitteiden sekä verkko- ja tietoturvadirektiivin välisen johdonmukaisuuden edistäminen sekä tietojen jakamisen ja analysoinnin alakohtaisten keskusten perustamisessa auttaminen kriittisillä sektoreilla. ENISA nostaa vaatimustasoa ja tehostaa eurooppalaista valmiutta järjestämällä vuosittain yleiseurooppalaisia kyberturvallisuusharjoituksia, joissa yhdistetään reagointitapoja eri tasoilla. Se tukee myös EU:n politiikan kehittämistä tieto- ja viestintäteknologian kyberturvallisuuden sertifioinnin alalla, ja sillä on merkittävä tehtävä toiminnallisen yhteistyön ja kriisinhallinnan tehostamisessa eri puolilla EU:ta. Viraston tehtävänä on myös toimia kyberturvallisuusyhteisön tiedotuksen ja tietämyksen yhteyspisteenä.

Nopeasti muodostettu yhteinen näkemys uhista ja vaaratilanteista on edellytys päätöksenteolle siitä, tarvitaanko yhteistä EU:n tukemaa lieventävää tai reagoivaa tointa. Sellainen tietojenvaihto edellyttää, että kaikki toimijat – EU:n elimet ja virastot sekä jäsenvaltiot – osallistuvat teknisellä, toiminnallisella ja strategisella tasolla. Myös ENISA osallistuu EU:n tasoisen tilannetietoisuuden rakentamiseen toimien yhteistyössä jäsenvaltioiden ja EU:n asianomaisten elinten kanssa. Osallisina ovat erityisesti tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt[17], CERT-EU, Europol ja EU:n tiedusteluanalyysikeskus (EU INTCEN). Tätä voidaan hyödyntää uhkia koskevassa tiedustelussa ja politiikanteossa uhkakuvien säännöllisen seurannan ja tehokkaan toiminnallisen yhteistyön yhteydessä sekä vastauksissa laajamittaisiin rajatylittäviin poikkeamiin.

---

15 COM(2017) 477.

16 Euroopan parlamentin ja neuvoston direktiivi 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

17 Kuten säädetään verkko- ja tietoturvadirektiivin 9 artiklassa.

2.2 Kohti kyberturvallisuuden sisämarkkinoita

Lukuisat tekijät hillitsevät kyberturvallisuusmarkkinoiden tuotteiden, palvelujen ja prosessien kasvua EU:ssa. Keskeinen näkökohta on EU:n jäsenvaltioissa tunnustettujen kyberturvallisuuden sertifiointijärjestelmien puuttuminen. Niiden avulla voitaisiin vaatia tuotteilta parempaa resilienssiä ja vahvistaa EU:n laajuista markkinaluottamusta. Komissio ehdottaa sen vuoksi **EU:n kyberturvallisuuden sertifiointipuitteiden** perustamista[18]. Niissä säädettäisiin menettelystä sellaisten EU:n laajuisten tuotteita, palveluja ja/tai järjestelmiä koskevien kyberturvallisuuden sertifiointijärjestelmien perustamiseksi, joilla mukautetaan varmuustaso kyseiseen käyttöön (oli sitten kyseessä elintärkeät infrastruktuurit tai kuluttajille tarkoitetut laitteet)[19]. Se toisi selkeitä hyötyjä yrityksille, koska niiden ei tarvitsisi käydä läpi useita sertifiointiprosesseja rajatylittävässä kaupankäynnissä, joten ne säästäisivät hallinnollisia ja rahoituskustannuksia. Kyseisissä puitteissa kehitetyt järjestelmät voisivat myös auttaa rakentamaan kuluttajien luottamusta käyttämällä vaatimustenmukaisuutta koskevaa todistusta, jolla voidaan informoida ja vakuuttaa ostajia ja käyttäjiä tuotteiden ja palvelujen turvallisuusominaisuuksista. Näin voitaisiin luoda kilpailuetuna toimiva laadukas kyberturvallisuus. Tuloksena olisi resilienssin kasvu, koska tieto- ja viestintätekniikan tuotteet ja -palvelut olisi muodollisesti arvioitava noudattaen määritettyjä kyberturvallisuusstandardeja, jotka voitaisiin kehittää tiiviissä yhteydessä laajemman tieto- ja viestintätekniikan standardien kehitystyön kanssa[20].

Puitteiden järjestelmät olisivat vapaaehtoisia eivätkä ne aiheuttaisi välittömiä lainsäädännöllisiä velvollisuuksia myyjille tai palvelun tuottajille. Järjestelmät eivät olisi ristiriidassa sovellettavien lakisääteisten vaatimusten kuten EU:n tietosuojalainsäädännön kanssa.

Kun puitteet on vahvistettu, komissio pyytää asianomaisia sidosryhmiä pohtimaan kolmea painopistealaa:

- Elintärkeiden tai korkean riskin sovellusten turvallisuus[21]. Järjestelmät, joista olemme riippuvaisia jokapäiväisissä toimissamme kuten autot ja tehtaiden koneet, suurimmat järjestelmät kuten lentokoneet tai voimalat taikka pienet järjestelmät kuten lääkinnälliset laitteet muuttuvat jatkuvasti digitaalisemmiksi ja yhteenliitetymmäksi. Sen vuoksi sellaisten tuotteiden ja järjestelmien keskeisten tieto- ja viestintätekniikan komponenttien turvallisuutta olisi arvioitava perusteellisesti.

- Kyberturvallisuus yksityisen ja julkisen sektorin laajasti käyttämissä digitaalisissa tuotteissa, järjestelmissä ja palveluissa hyökkäyksiltä puolustautumiseksi ja lainsäädännöllisten velvollisuuksien[22] soveltamiseksi, kuten sähköpostin salaus, palomuurit ja virtuaaliset erillisverkot. On hyvin tärkeää, että tällaisten välineiden käytön lisääntyminen ei johda uusien riskien tai haavoittuvuuksien ilmaantumiseen.

---

18 COM(2017) 477.

19 Varmuustaso osoittaa turvallisuusarvioinnin kurinalaisuutta ja se on usein suhteessa riskitasoon, joka liittyy kyseisiin soveltamisalueisiin tai toimintoihin (eli korkeampaa varmuustasoa edellytetään niiltä tieto- ja viestintätekniikan tuotteilta tai -palveluilta, joita käytetään korkean riskin aloilla tai toiminnoissa).

20 COM(2016) 176.

21 Poikkeuksena olisi tilanne, jossa muut unionin säädökset sääntelevät pakollista tai vapaaehtoista sertifiointia.

22 Esimerkiksi direktiivissä (EU) 2016/1148, asetuksessa (EU) 2016/679, direktiivissä (EU) 2015/2366 ja muissa ehdotetuissa säädöksissä, kuten eurooppalaisessa sähköisen viestinnän säännöstössä, edellytetään kussakin, että organisaatiot ottavat käyttöön asianmukaiset turvatoimet olennaisten kyberturvallisuuteen liittyvien riskien käsittelemiseksi.

- Sisäänrakennetun turvallisuuden menetelmien käyttäminen edullisissa, digitaalisissa ja yhteenliitetyissä suurille kuluttajajoukoille tarkoitetuissa laitteissa, jotka muodostavat esineiden internetin. Puitteiden mukaisia järjestelmiä voitaisiin käyttää ilmoittamaan, että tuotteet on rakennettu käyttämällä uusimpia turvallisuutta kehittäviä menetelmiä, niiden turvallisuus on riittävästi testattu ja myyjät ovat sitoutuneet päivittämään ohjelmistot, jos ilmenee uusia haavoittuvuuksia tai uhkia.

Näillä painopistealoilla olisi otettava erityisesti huomioon kyberturvallisuuden uhkakuvat sekä sellaisten olennaisten palvelujen merkitys kuten liikenne, energia-ala, terveydenhuolto, pankkitoiminta, rahoitusalan infrastruktuurit, juomavesi tai digitaalinen infrastruktuuri[23].

Minkään tieto- ja viestintätekniikan tuotteen, järjestelmän tai palvelun ei voida taata olevan 100-prosenttisen turvallinen, ja tieto- ja viestintätekniikan tuotteiden suunnittelussa on hyvin tunnettuja ja hyvin dokumentoituja puutteita, joita voidaan käyttää hyökkäyksissä hyväksi. Jos verkkoon liitettyjen laitteiden sekä tietoteknisten ohjelmistojen ja laitteiden valmistajat ottaisivat käyttöön sisäänrakennettua turvallisuutta korostavan lähestymistavan, voitaisiin varmistaa, että kyberturvallisuuskysymykset käsitellään ennen uusien tuotteiden saattamista markkinoille. Tämä voisi olla osa toimialan kanssa edelleen kehitettävää varmistamisvelvollisuuden periaatetta, jonka avulla voitaisiin vähentää tuotteiden ja ohjelmistojen haavoittuvuuksia soveltamalla monenlaisia menetelmiä suunnittelussa, testaamisessa ja tarkistuksia tehtäessä. Esimerkkeinä menetelmistä voisivat olla viralliset tarkastukset tarvittaessa, pitkän aikavälin ylläpito, turvallisten elinkaaren kehittämistä koskevien prosessien käyttäminen, ohjelmisto- ja korjauspäivityksien kehittäminen aiemmin havaitsematta jääneiden haavoittuvuuksien käsittelemistä varten sekä nopeat päivitykset ja korjaukset[24]. Tämä lisäisi myös kuluttajien luottamusta digitaalisiin tuotteisiin.

Lisäksi on tunnustettava kolmannen osapuolen turvallisuusalan tutkijoiden tärkeä rooli, kun havaitaan haavoittuvuuksia nykyisissä tuotteissa ja palveluissa, ja jäsenvaltioissa olisi luotava olosuhteet koordinoidun haavoittuvuuden havaitsemisohjelman[25] käyttöönottoa varten perustuen parhaisiin käytäntöihin[26] ja asianomaisiin standardeihin[27].

Samaan aikaan **tietyillä aloilla** on erityisiä ongelmia, ja niitä olisi kannustettava kehittämään omaa lähestymistapaansa. Näin toimien yleistä kyberturvallisuusstrategiaa täydennettäisiin alakohtaisilla kyberturvallisuusstrategioilla sellaisilla aloilla kuin rahoituspalvelut[28], energia, liikenne ja terveys[29].

---

[23] Toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa 6. heinäkuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin 2016/1148 soveltamisalaan kuuluvat alat.

[24] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017

[25] Koordinoitu haavoittuvuuden havaitsemisohjelma on yhteistyömuoto, joka auttaa ja mahdollistaa turvallisuusalan tutkijoita ilmoittamaan haavoittuvuuksista tietojärjestelmän omistajalle tai myyjälle. Sen avulla organisaatiolla on mahdollisuus diagnosoida ja korjata haavoittuvuus asianmukaisesti ja oikea-aikaisesti, ennen kuin haavoittuvuutta koskevat yksityiskohtaiset tiedot paljastetaan kolmansille osapuolille tai suurelle yleisölle.

[26] Esimerkiksi Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, ENISA, 2016.

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure.

[28] Komission tuleva työ rahoitusteknologian alalla kattaa kyberturvallisuuden rahoitusalalla.

[29] Esimerkiksi energia-alalla yhdistämällä hyvin vanhaa ja uusinta tietotekniikkaa erityisesti sähköverkkojen reaaliaikaisten vaatimusten yhteydessä.

Komissio on jo esittänyt kysymyksiä, jotka koskevat **vastuuta** uusien digitaalitekniikoiden[30] yhteydessä, ja vaikutuksia ollaan analysoimassa. Seuraavat vaiheet saatetaan päätökseen kesäkuuhun 2018 mennessä. Kyberturvallisuus herättää vastuukysymyksiä vahinkotapauksissa yrityksille ja toimitusketjuille, ja jos näitä kysymyksiä ei voida käsitellä, se estää kyberturvallisuuden tuotteiden ja palvelujen vahvojen sisämarkkinoiden kehittymisen.

EU:n sisämarkkinoiden kehittäminen riippuu myös siitä, miten kyberturvallisuus otetaan huomioon kauppaa ja investointeja koskevissa politiikoissa. Tärkeä esimerkki kyberturvallisuudesta on ulkomaisten hankintojen vaikutus elintärkeisiin teknologioihin. Se on keskeinen näkökohta **Euroopan unionissa tehtyjen ulkomaisten suorien sijoitusten seuraamista**[31] koskevissa puitteissa, joiden tavoitteena on mahdollistaa kolmansista maista tulevien investointien seuraaminen turvallisuuden ja yleisen järjestyksen perusteella. Samasta syystä kyberturvallisuutta koskevat vaatimukset ovat jo luoneet kaupan esteitä EU:n tavaroille ja palveluille tärkeillä aloilla lukuisissa kolmansien maiden talouksissa. EU:n kyberturvallisuutta koskevan sertifioinnin puitteet vahvistavat Euroopan kansainvälistä asemaa entisestään, ja niitä olisi täydennettävä jatkuvilla pyrkimyksillä kehittää korkean turvallisuustason maailmanlaajuisia standardeja ja keskinäisiä tunnustamista koskevia sopimuksia.

2.3 Verkko- ja tietojärjestelmien turvallisuudesta annetun direktiivin täysimääräinen täytäntöönpano

Koska keskeiset välineet kyberturvallisuuden edistämiseksi ovat tällä hetkellä kansallisia, EU on havainnut tarpeen käyttää isompaa työkalua. Laaja-alaiset kyberturvallisuuspoikkeamat vaikuttavat harvoin vain yhteen jäsenvaltioon, koska keskeisten alojen, kuten pankkitoiminta, energia tai liikenne, luonne muuttuu jatkuvasti globaalimmaksi, digitaaliriippuvaisemmaksi ja yhteenliittyneemmäksi.

Verkko- ja tietojärjestelmien turvallisuudesta annettu direktiivi (verkko- ja tietoturvadirektiivi) on ensimmäinen EU:n laajuinen kyberturvallisuutta koskeva säädös[32]. Se on suunniteltu kehittämään resilienssiä parantamalla kansallisia kyberturvallisuuden valmiuksia, edistämään parempaa yhteistyötä jäsenvaltioiden välillä ja edellyttämään, että keskeisten talouden alojen yritykset ottavat käyttöön tehokkaita riskinhallintakäytäntöjä ja ilmoittavat vakavista turvapoikkeamista kansallisille viranomaisille. Kyseisiä velvoitteita sovelletaan myös kolmentyyppisiin keskeisten internet-palvelujen tarjoajiin. Ne tarjoavat pilvipalveluja, hakukoneita ja verkossa toimivia markkinapaikkoja. Tavoitteena on vahvempi ja järjestelmällisempi lähestymistapa ja parempi tiedonkulku.

EU:n kyberresilienssin kannalta on keskeistä, että kaikki jäsenvaltiot panevat direktiivin täysimääräisesti täytäntöön toukokuuhun 2018 mennessä. Tätä prosessia tuetaan jäsenvaltioiden kollektiivisilla toimilla, joiden tuloksena saadaan syksyyn 2017 mennessä suuntaviivat yhdenmukaisemman täytäntöönpanon tukemiseksi erityisesti suhteessa keskeisten palvelujen tarjoajiin. Komissio antaa myös tiedonannon[33] osana tätä kyberturvallisuuspakettia tukeakseen niiden pyrkimyksiä tarjoamalla parhaita käytänteitä

[30] COM(2017) 228.
[31] COM(2017) 478.
[32] Euroopan parlamentin ja neuvoston direktiivi 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.
[33] COM(2017) 476.

direktiivin täytäntöönpanon kannalta olennaisilta jäsenvaltioilta ja opastamalla, miten direktiivi toimii käytännössä.

Direktiiviä on tarpeen täydentää tiedonkulun alalla. Nyt se esimerkiksi kattaa vain keskeiset strategiset alat, mutta loogisesti olisi tarpeen soveltaa samanlaista lähestymistapaa kaikkiin verkkohyökkäyksistä kärsineisiin sidosryhmiin, jotta haavoittuvuuksia voidaan arvioida järjestelmällisesti ja tutkia mitä kautta kyberhyökkääjät tulevat. Lisäksi julkisen ja yksityisen sektorin välisen yhteistyön ja tietojen jakamisen tiellä on lukuisia esteitä. Hallitukset ja viranomaiset ovat haluttomia jakamaan kyberturvallisuuteen liittyviä tietoja, koska ne pelkäävät vaarantavansa kansallisen turvallisuuden tai kilpailukyvyn. Yksityiset yritykset ovat haluttomia jakamaan tietoja kyberhaavoittuvuuksistaan ja niistä seuraavista tappioistaan, koska ne pelkäävät paljastavansa arkaluonteisia liiketoimintatietoja, vaarantavansa maineensa tai rikkovansa tietosuojasääntöjä[34]. On vahvistettava luottamusta julkisen ja yksityisen sektorin kumppanuuksiin laajemman yhteistyön tukemiseksi ja tietojen jakamiseksi useammalle alalle. Tietojen jakamisen ja analysoinnin alakohtaisten keskusten rooli on erityisen tärkeä, kun luodaan tarvittavaa luottamusta tietojen jakamiseksi yksityisen ja julkisen sektorin välillä. Joihinkin ensimmäisiin toimiin on ryhdytty tietyillä kriittisillä sektoreilla kuten ilmailualalla, perustamalla ilmailualan kyberturvallisuuden eurooppalainen keskus[35], ja energia-alalla kehittämällä tietojen jakamisen ja analysoinnin alakohtaisia keskuksia[36]. Komissio tukee kaikilta osin tätä lähestymistapaa ENISAn tuella. Erityisesti on kiihdytettävä vauhtia niiden alojen osalta, jotka tarjoavat verkko- ja tietoturvadirektiivissä määriteltyjä keskeisiä palveluja.

2.4 Resilienssi nopean hätäavun avulla

Kyberhyökkäyksen aikana nopea ja tehokas reagointi voi lieventää sen vaikutuksia. Näin voidaan myös osoittaa, että viranomaiset eivät vain seuraa voimattomana sivusta kyberhyökkäysten aikana, ja rakentaa luottamusta. EU:n toimielinten oman reagoinnin osalta kybernäkökulma olisi sisällytettävä olemassa oleviin EU:n kriisinhallintamekanismeihin. Näitä ovat neuvoston puheenjohtajan koordinoimat EU:n poliittisen kriisitoiminnan integroidut järjestelyt[37] ja nopea yleishälytysjärjestelmä[38]. Tarve reagoida erityisen vakavaan kyberturvallisuuspoikkeamaan tai hyökkäykseen voisi olla riittävä peruste, jotta EU:n jäsenvaltio voi vedota EU:n yhteisvastuulausekkeeseen[39].

Nopea ja tehokas toiminta riippuu myös kaikkien keskeisten toimijoiden välisestä nopeasta tietojenvaihdon järjestelmästä kansallisella tasolla ja EU:ssa, mikä puolestaan edellyttää, että niiden roolit ja vastuualueet ovat selkeät. Komissio on kuullut toimielimiä ja jäsenvaltioita suunnitelmasta, joka koskee sitä, kuinka EU ja jäsenvaltiot voivat reagoida tehokkaasti laajamittaisen kyberhyökkäyksen tapahtuessa. **Suunnitelmassa**, joka esitetään tähän pakettiin

---

[34] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017. Erityinen kysymys koskee liikesalaisuuksia, josta heinäkuussa 2016 annetussa tiedonannossa ”Euroopan kyberresilienssijärjestelmän vahvistaminen” mainitaan pidättyväisyys ilmoittaa liikesalaisuuksien kybervarkauksista ja luottamuksellisuuden varmistavien ilmoituskanavien merkitys.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Nämä ovat yksityisten ja julkisten toimijoiden muodostamia voittoa tavoittelemattomia organisaatioita kyberuhkia ja riskejä, niiden ehkäisemistä ja lieventämistä sekä niihin vastaamista varten. Katso esim. European Energy Information Sharing and Analysis Centres (http://www.ee-isac.eu).

[37] Sen avulla on mahdollista koordinoida reagointia korkeimmalla poliittisella tasolla nopeasti merkittäviin eri alojen kriiseihin.

[38] Niiden avulla voidaan jakaa sisäisesti tietoja ja koordinoida ilmeneviä monialaisia kriisejä taikka ennakoitavissa olevia tai välittömiä uhkia, jotka edellyttävät toimia EU:n tasolla.

[39] Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklan nojalla.

kuuluvassa suosituksessa[40], selitetään miten kyberturvallisuus on sisällytetty olemassa oleviin EU:n kriisinhallintamekanismeihin ja määritellään jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten[41] välisen yhteistyön tavoitteet ja muodot vastattaessa laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin. Suosituksessa jäsenvaltioita ja EU:n toimielimiä pyydetään myös perustamaan EU:n kyberturvallisuuden kriisinhallintakehys, jotta suunnitelma voitaisiin toteuttaa käytännössä. Suunnitelmaa testataan säännöllisesti kyberturvallisuusriskien ja muiden kriisien hallintaa koskevissa harjoituksissa[42], ja sitä päivitetään tarvittaessa.

Koska kyberturvallisuuspoikkeamat voisivat olennaisesti vaikuttaa talouteen ja ihmisten jokapäiväiseen elämään, yhtenä vaihtoehtona voisi olla tutkia **kyberturvallisuuden hätäapurahaston** perustamisen mahdollisuutta muilla EU:n politiikan aloilla olevien muiden vastaavien kriisinhallintamekanismien esimerkkiä seuraten. Se voisi auttaa jäsenvaltioita hakemaan apua EU:n tasolla merkittävän poikkeaman sattuessa edellyttäen, että jäsenvaltio oli ennen poikkeamaa ottanut käyttöön vakaan kyberturvallisuusjärjestelmän, johon kuuluu verkko- ja tietoturvadirektiivin täysimääräinen täytäntöönpano ja kehittyneet riskienhallinta- ja valvontapuitteet kansallisella tasolla. Sellainen rahasto, joka täydentäisi olemassa olevia kriisinhallintamekanismeja EU:n tasolla, voisi käyttää nopean reagoinnin valmiutta yhteisvastuulle ja rahoitukselle ominaisiin hätäaputoimiin. Näitä toimia ovat esimerkiksi sellaisten laitteiden, joiden turvallisuus on vaarantunut, korvaaminen taikka lieventävien tai reagoivien välineiden käyttöönotto. Tässä voitaisiin hyödyntää kansallista asiantuntemusta EU:n pelastuspalvelumekanismin pohjalta.

2.5 Kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus

Kyberturvallisuuden teknologiset välineet ovat strateginen voimavara sen lisäksi, että ne ovat keskeisiä kasvuteknologioita tulevaisuutta varten. On EU:n strategisen edun mukaista varmistaa, että EU säilyttää ja kehittää keskeisiä valmiuksia digitaalisen taloutensa, yhteiskuntansa ja demokratiansa turvaamiseksi, suojatakseen kriittiset laitteistot ja ohjelmistot sekä tarjotakseen keskeisiä kyberturvallisuuspalveluja.

Vuonna 2016 perustettu julkisen ja yksityisen sektorin kyberturvallisuuskumppanuus[43] oli merkittävä ensimmäinen toimi, jonka perusteella tehdään jopa 1,8 miljardin euron investointeja vuoteen 2020 mennessä. Muualla maailmassa tehtävien investointien laajuus[44] osoittaa kuitenkin, että EU:n on investoitava enemmän ja käsiteltävä jotenkin valmiuksien sirpaloituminen ympäri EU:ta.

EU voi tarjota lisäarvoa, kun otetaan huomioon kyberturvallisuusteknologian kehittyneisyys, tarvittavat mittavat investoinnit ja EU:n laajuisesti toimivien ratkaisujen tarve. Jäsenvaltioiden sekä julkisen ja yksityisen sektorin kumppanuuden suorittamaan työhön perustuvana jatkotoimena voitaisiin vahvistaa EU:n kyberturvallisuusvalmiuksia **kyberturvallisuuden**

---

40 C(2017) 6100.

41 Mukaan lukien Europol, ENISA, EU:n toimielinten, elinten ja virastojen EU-tietoturvayksikkö (Computer Emergency Response Team, CERT-EU) ja EU:n tiedusteluanalyysikeskus (EU INTCEN).

42 Esimerkiksi ENISAn järjestämissä: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

43 C(2016) 4400 final.

44 Yhdysvallat investoi 19 miljardia dollaria kyberturvallisuuteen pelkästään vuonna 2017, mikä merkitsee 35 prosentin kasvua verrattuna vuoteen 2016. Valkoisen talon tiedottaja: 'Fact Sheet: Cybersecurity National Action Plan', 9. helmikuuta 2016.

osaamiskeskusten verkoston[45] avulla. Sen keskiössä olisi **eurooppalaisen kyberturvallisuuden tutkimus- ja osaamiskeskus**. Tämä verkosto ja osaamiskeskus innostaisivat teknologian kehittämistä ja käyttöönottoa kyberturvallisuuden alalla, ja ne täydentäisivät tämän alan valmiuksien kehittämistä EU:ssa ja kansallisesti. Komissio käynnistää vaikutustenarvioinnin saatavilla olevien vaihtoehtojen tarkastelemiseksi – mukaan lukien mahdollisen yhteisyrityksen perustaminen – jotta tämä rakenne voidaan perustaa vuonna 2018.

Ensimmäisenä toimena ja tulevaan suunnitteluun varautumiseksi komissio ehdottaa pilottivaiheen käynnistämistä Horisontti 2020 -ohjelman puitteissa. Sen avulla voidaan verkottaa kansalliset keskukset kyberturvallisuuden osaamisen kasvattamiseksi ja teknologian kehittämiseksi. Komissio aikoo ehdottaa 50 miljoonan euron lyhyen aikavälin rahoitusta tähän tarkoitukseen. Tämä toimi täydentää nykyistä julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden toteutusta.

Tutkimustointen keskittäminen ja muokkaaminen olisivat verkoston keskiössä ja keskuksen alkuperäinen painopiste. Teollisten valmiuksien kehittämisen tukemiseksi keskus voisi toimia valmiuksia käsittelevän hankkeen johtajana, joka kykenee käsittelemään monikansallisia hankkeita. Se antaisi myös pontta EU:n teollisuuden innovoinnille ja kilpailukyvylle maailmanlaajuisesti kehitettäessä seuraavan sukupolven digitaalisia teknologioita, kuten tekoälyä, kvanttilaskentaa, lohkoketjujärjestelmiä ja turvallisia digitaalisia identiteettejä, sekä varmistettaessa, että EU:hun sijoittautuneilla yrityksillä on pääsy massadataan. Nämä kaikki ovat keskeisiä tekijöitä tulevaisuuden kyberturvallisuuden kannalta. Keskus hyödyntäisi myös EU:n toimia laajentaakseen suurteholaskentainfrastruktuuria. Se on keskeistä suurten tietomäärien analysoimiseksi, tiedon nopeaa salausta ja salauksen purkua varten, henkilöllisyyden tarkastamiseksi, kyberhyökkäysten simuloimiseksi ja videoaineiston analysoimiseksi[46].

Osaamiskeskusten verkostolla voisi olla myös valmiuksia tukea teollisuutta testaamisen ja simuloinnin kautta 2.2 kohdassa kuvaillun kyberturvallisuuden sertifioinnin tukemiseksi. Sen osallistuminen kaikkeen EU:n kyberturvallisuustoimintaan varmistaisi, että sen kohdistamista päivitetään jatkuvasti tarpeiden mukaan. Keskuksen tavoitteena olisi edistää korkeatasoista kyberturvallisuutta teknologian ja kyberturvallisuuden järjestelmissä ja myös ammattilaisten korkeatasoisten taitojen kehittämistä tarjoamalla ratkaisuja ja malleja kansallisen tason toimille digitaalisten taitojen saamiseksi käyttöön. Tältä osin se lisäisi myös kyberturvallisuuden valmiuksia EU:n tasolla ja kehittäisi yhteisvaikutuksia erityisesti ENISAn, CERT-EU:n, Europolin, mahdollisen tulevan kyberturvallisuuden hätäapurahaston ja kansallisten CSIRT-toimijoiden kanssa.

Osaamisverkoston työskentelyssä on keskityttävä erityisesti siihen, että Euroopasta puuttuu valmius arvioida kansalaisten, yritysten ja julkishallintojen käyttämien tuotteiden ja palvelujen **salaus** digitaalisilla sisämarkkinoilla. Tehokkaassa kyberturvallisuudessa keskeisessä asemassa olevat turvalliset digitaaliset tunnistusjärjestelmät perustuvat vahvaan salaukseen[47]. Sillä myös suojataan ihmisten henkinen omaisuus ja mahdollistetaan

[45] Verkostoon kuuluisivat nykyiset ja tulevat jäsenvaltioihin perustetut kyberturvallisuuskeskukset, joiden jäsenet olisivat tyypillisesti julkisia tutkimusorganisaatioita ja laboratorioita.

[46] COM(2012) 45 final ja COM(2016) 178 final.

[47] Komissio aikoo jo Horisontti 2020 -ohjelman puitteissa käynnistää uuden neljän miljoonan euron Horisontti-palkintohaasteen parhaalle innovatiiviselle saumattomien sähköisen todentamisen menetelmien ratkaisulle.

perusoikeuksien, kuten sanavapauden ja henkilötietojen suoja, turvaaminen ja varmistetaan turvallinen sähköinen kaupankäynti[48].

Koska EU:n siviili- ja puolustusalan kyberturvallisuusmarkkinat jakavat samat haasteet[49] ja kaksikäyttöteknologian, joka edellyttää läheistä yhteistyötä kriittisillä aloilla, verkoston ja sen keskuksen toista vaihetta voitaisiin edelleen kehittää kyberpuolustukseen liittyvän ulottuvuuden osalta. Samalla olisi täysin noudatettava yhteistä turvallisuus- ja puolustuspolitiikkaa koskevia perustamissopimuksen määräyksiä. Teknologisen keskittymisen lisäksi puolustusulottuvuus voisi auttaa jäsenvaltioiden välistä yhteistyötä kyberpuolustuksen alalla. Se sisältää esimerkiksi tietojen jakamisen, tilannetietoisuuden, asiantuntemuksen ja koordinoidun reagoinnin sekä jäsenvaltioiden yhteisten valmiuksien kehittämisen tukemisen. Se voisi toimia myös foorumina, jonka avulla jäsenvaltiot voivat määrittää EU:n kyberpuolustuksen painopisteet, tutkia yhteisiä ratkaisuja, osallistua yhteisten strategioiden kehittämiseen, edistää yhteistä kyberpuolustuskoulutusta, harjoituksia ja testaamista euroopan tasolla ja tukea kyberpuolustuksen luokitteluun ja standardeihin liittyvää työtä ja jossa keskuksella olisi tukeva ja neuvova rooli. Edellä mainittujen tehtävien suorittamiseksi keskuksen on toimittava tiiviissä yhteistyössä ja kokonaisvaltaisesti täydentäen Euroopan puolustusviraston kanssa kyberpuolustuksen alalla ja ENISAn kanssa kyberresilienssin alalla. Tässä puolustusulottuvuudessa otettaisiin huomioon Euroopan puolustuksen tulevaisuutta käsittelevässä pohdinta-asiakirjassa käynnistetty prosessi.

Kyberpuolustuksessa tarvittava korkeatasoinen resilienssi edellyttää tutkimus- ja teknologiatyön erityistä kohdentamista. Yritysten kehittämät kyberpuolustushankkeet tai -teknologiat voisivat saada rahoitusta Euroopan puolustusrahastosta tutkimus- ja kehittämisvaiheessa[50]. Tässä yhteydessä erityisen merkityksellistä voisivat olla eritysalat kuten kvanttiteknologiaan perustuvat salausjärjestelmät, kybertilannetietoisuus, biometriset kulunvalvontajärjestelmät, edistyneiden pitkäkestoisten uhkien havaitseminen tai tiedonlouhinta. Korkea edustaja, Euroopan puolustusvirasto, ja komissio tukevat jäsenvaltioita sellaisten alojen yksilöimiseksi, joilla voisi harkita yhteisiä kyberturvallisuuhankkeita EU:n puolustusrahaston tuella.

2.6 Vahvan kyberosaamispohjan rakentaminen EU:ssa

Kyberturvallisuudella on vahva koulutusulottuvuus. Tehokas kyberturvallisuus on paljolti asianomaisten henkilöiden taitojen varassa. Kyberturvallisuuden ammattilaisia ennustetaan kuitenkin puuttuvan Euroopan yksityiseltä sektorilta 350 000 kappaletta vuoteen 2022 mennessä[51]. Kyberturvallisuuden koulutusta tulisi kehittää kaikilla tasoilla alkaen kyberalan työvoiman säännöllisestä koulutuksesta. Olisi tarjottava myös kyberturvallisuuden lisäkoulutusta kaikille tieto- ja viestintätekniikan asiantuntijoille ja uusia erityisiä kyberturvallisuuteen keskittyviä opetusohjelmia. Olisi perustettava vahvoja tieteellisiä osaamiskeskuksia nopeutetun koulutuksen tarpeita varten. Eurooppalaisen kyberturvallisuuden tutkimus- ja osaamiskeskus ja ENISA voisivat ohjata niitä. Tavoitteena olisi oltava, että tietoturvan periaatteiden sisällyttäminen heti alusta lähtien tulee luonnolliseksi osaksi tieto- ja viestintätekniikan tuotteiden ja järjestelmien suunnittelua. Kyberturvallisuuskoulutusta ei pitäisi rajata vain tieto- ja viestintätekniikan ammattilaisiin,

[48] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017.

[49] ”Study on synergies between the civilian and the defence cybersecurity markets” (Optimity; SMART 2014-0059).

[50] Kyberpuolustushankkeet asetetaan nyt jo etusijalle Euroopan puolustusteollisuuden kehitysohjelmassa, ja kyberpuolustus on yksi vuonna 2018 käynnistettävän ehdotuspyynnön teemoista.

[51] Global Information Security Workforce Study 2017. Maailmanlaajuinen vaje on 1,8 miljoonaa.

vaan se olisi sisällytettävä muiden alojen, kuten tekniikan, yritysjohdon tai oikeustieteen koulutukseen sekä alakohtaisiin koulutusmalleihin. Ala- ja yläkoulun opettajat ja oppilaat olisi myös tehtävä tietoisiksi kyberrikollisuudesta ja -turvallisuudesta, kun he hankkivat digitaalisia taitoja kouluissa.

EU:n olisi yhdessä jäsenvaltioiden kanssa osallistuttava tähän tehtävään digitaalitaitoja ja työpaikkoja edistävän koalition[52] työn pohjalta, ottamalla käyttöön esimerkiksi pk-yritysten kyberturvallisuutta koskevia oppisopimusjärjestelmiä.

2.7 Kyberhygienian ja kyberturvallisuustietoisuuden edistäminen

Noin 95 prosentin kyberturvallisuuspoikkeamista väitetään olevan sellaisia, jotka on mahdollistanut jonkinlainen – tarkoituksellinen tai tahaton – inhimillinen virhe[53]. Inhimillisillä tekijöillä on siis hyvin suuri merkitys, minkä vuoksi kyberturvallisuus onkin kaikkien vastuulla. Se tarkoittaa, että henkilökohtaisia, yritystason ja julkisen hallinnon toimintatapoja on muutettava, jotta voidaan varmistaa, että jokainen ymmärtää uhan ja kykenee käytössään olevien välineiden ja taitojensa puolesta tunnistamaan hyökkäykset nopeasti ja suojautumaan niiltä aktiivisesti. Ihmisten on omaksuttava tarvittavat kyberhygieniatottumukset ja yritysten ja organisaatioiden on laadittava asianmukaiset riskiperusteiset kyberturvallisuusohjelmat sekä päivitettävä niitä säännöllisesti riskiympäristön muuttuessa.

Verkko- ja tietoturvadirektiivissä säädetään, että jäsenvaltioiden on paitsi vaihdettava tietoja kyberhyökkäyksistä EU:n tasolla myös perustettava kehittyneet kansalliset kyberturvallisuusstrategiat ja verkko- ja tietojärjestelmien turvallisuuskehykset. EU:n ja kansallisen tason julkishallintojen olisi otettava johtoasema näiden pyrkimysten edistämisessä.

Jäsenvaltioiden olisi ensiksikin turvattava kyberturvallisuuden välineiden mahdollisimman laaja saatavuus yrityksille ja yksityishenkilöille. Erityisesti olisi lisättävä toimia, joilla voidaan ehkäistä ja lieventää kyberrikollisuuden vaikutuksia loppukäyttäjiin. Tällainen esimerkki on jo olemassa Europolin työstä NoMoreRansom-kampanjassa[54], joka perustuu lainvalvojien ja kyberturvallisuusyritysten tiiviiseen yhteistyöhön. Sen tarkoituksena on antaa käyttäjille keinoja, jotka auttavat välttämään kiristysohjelmien uhriksi joutumista sekä purkamaan kiristysohjelman asettaman salauksen. Samanlaisia järjestelyjä olisi otettava käyttöön muiden haittaohjelmien suhteen muilla aloilla, ja EU:n olisi kehitettävä **portaali, johon kootaan keskitetysti yhteen kaikki tällaiset välineet** ja joka tarjoaa käyttäjille opastusta haittaohjelmien ehkäisemiseen ja havaitsemiseen sekä linkkejä ilmoitusmekanismeihin.

Toiseksi jäsenvaltioiden olisi nopeutettava **kyberturvallisempien välineiden käyttöä sähköisen hallinnon kehittämisen yhteydessä** sekä hyödynnettävä kaikin tavoin osaamisverkostoa. Olisi edistettävä sellaisten turvallisten tunnistautumiskeinojen käyttöönottoa, jotka perustuvat sähköistä tunnistamista ja sähköisiin transaktioihin liittyviä luottamuspalveluja sisämarkkinoilla koskeviin puitteisiin. Nämä puitteet ovat olleet voimassa vuodesta 2016 lähtien, ja ne tarjoavat ennakoitavan sääntely-ympäristön turvalliselle ja

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM:n "The Cybersecurity Intelligence Index" 2014, johon viitataan julkaisussa Securitymagazine.com, 19.6.2014.

[54] https://www.nomoreransom.org/.

saumattomalle sähköiselle asioinnille yritysten, yksityishenkilöiden ja viranomaisten välillä[55]. Lisäksi julkisten elinten – erityisesti välttämättömiä palveluja tarjoavien – olisi varmistettava, että niiden henkilöstö on koulutettu kyberturvallisuuteen liittyvissä asioissa.

Kolmanneksi jäsenvaltioiden olisi korostettava kyberturvallisuustietoisuutta muun muassa kouluille, yliopistoille, yrityksille ja tutkimuslaitoksille suunnatuissa **valistuskampanjoissa**. ENISAn koordinoimaa kyberturvallisuuskuukautta, jonka aika on vuosittain lokakuussa, tehostetaan laajemman kohderyhmän saavuttamiseksi yhteisille tiedotustoimille EU:n ja kansallisella tasolla. Yhtä tärkeää on lisätä tietoisuutta sosiaalisen median sähköisistä **disinformaatiokampanjoista ja valeuutisista**, joiden tarkoituksena on heikentää demokraattisia prosesseja ja eurooppalaisia arvoja. Päävastuu on edelleen kansallisella tasolla – myös Euroopan parlamentin vaalien osalta – mutta asiantuntemuksen keskittämisellä ja kokemusten vaihdolla Euroopan tasolla on osoittautunut olevan lisäarvoa toiminnan suuntaamisessa[56].

Merkittävässä roolissa on myös **toimiala** yleisesti, mutta erityishuomio kiinnittyy digitaalisten palvelujen tarjoajiin ja valmistusteollisuuteen. Toimialan pitää tukea käyttäjiä (yksityishenkilöitä, yrityksiä ja julkishallintoja) välineillä, jotka antavat käyttäjille mahdollisuuden ottaa vastuuta omasta toiminnastaan verkossa, sekä tehdä selväksi, että kyberhygienia on erottamaton osa kuluttajille tarjottavia tuotteita[57]. Haavoittuvuuksien tunnistamiseksi ja poistamiseksi toimialan olisi pyrittävä toteuttamaan sisäiset prosessit, joilla käsitellään haavoittuvuuksien tutkintaa, luokittelua ja korjaamista, riippumatta siitä, onko mahdollisen haavoittuvuuden lähde ulkoinen vai kyseessä olevan yrityksen sisäinen.

Avaintoimet

- Verkko- ja tietojärjestelmien turvallisuudesta annetun direktiivin paneminen kaikilta osin täytäntöön;
- ENISAn uutta toimeksiantoa ja sertifioinnin eurooppalaisia puitteita koskevan asetuksen[58] hyväksyminen nopeasti Euroopan parlamentissa ja neuvostossa;
- Komission ja toimialan yhteinen aloite varmistamisvelvollisuuden periaatteen määrittelemiseksi, jotta voidaan vähentää tuotteiden ja ohjelmistojen haavoittuvuutta ja edistää sisäänrakennettua turvallisuutta;
- Laajamittaisiin rajat ylittäviin poikkeamiin reagoimista koskevan suunnitelman nopea täytäntöönpano;
- Vaikutustenarviointi mahdollisuudesta esittää vuonna 2018 komission ehdotus kyberturvallisuuden osaamiskeskusten verkoston ja eurooppalaisen kyberturvallisuuden tutkimus- ja osaamiskeskuksen perustamiseksi viipymättä aloitettavan pilottivaiheen pohjalta;
- Jäsenvaltioiden tukeminen sellaisten alojen yksilöimiseksi, joiden yhteisiin kyberturvallisuushankkeisiin voisi ehkä saada tukea EU:n puolustusrahastosta;
- EU:n laajuinen keskitetty asiointipiste, joka auttaisi kyberhyökkäysten uhreja, jakaisi

[55] Asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla (eIDAS-asetus), annettu 23. heinäkuuta 2014. Euroopan komissio tarjoaa myös sähköisen tunnistuksen ja sähköisen allekirjoituksen yhteentoimivuuden rakenneosia ja välineitä (esim. luotettujen luetteloiden selausohjelmistoja) Verkkojen Eurooppa -välineen kautta.

[56] Yksi esimerkki on East StratCom Task Force, jonka jäsenvaltiot ja korkea edustaja perustivat vuonna 2015 Venäjän jatkuvien disinformaatiokampanjoiden käsittelemiseksi. Se kehittää viestintätuotteita ja -kampanjoita, joissa keskitytään selittämään EU:n politiikkaa itäisen kumppanuuden alueella.

[57] Jotkin valmistajat ovat jo tottuneet tähän ajattelutapaan, sillä osaan eurooppalaista tuotelainsäädäntöä (esimerkiksi konedirektiiviin 2006/42/EY) sisältyy sisäänrakennetun turvallisuuden periaatteita.

[58] COM(2017) 477.

tietoa uusimmista uhkista ja kokoaisi yhteen käytännön neuvoja ja kyberturvallisuusvälineitä;
- Jäsenvaltioiden toimet kyberturvallisuuden valtavirtaistamiseksi taitojen kehittämistä koskeviin ohjelmiin, sähköiseen hallintoon ja valistuskampanjoihin;
- Toimialan toimet henkilöstön kyberturvallisuuteen liittyvän koulutuksen lisäämiseksi ja sisäänrakennettuun turvallisuuteen perustuvan lähestymistavan omaksumiseksi suhteessa tuotteisiin, palveluihin ja prosesseihin.

3. TOIMIVAN KYBERPELOTTEEN LUOMINEN

Toimiva pelote tarkoittaa toimenpiteitä, jotka ovat sekä uskottavia että ennaltaehkäisevästi varoittavia mahdollisten kyberrikollisten ja -hyökkääjien kannalta. Niin kauan kuin kyberhyökkäysten tekijöillä – sekä valtiollisilla että muilla – ei ole muuta pelättävää kuin epäonnistuminen, juuri mikään ei estä niitä yrittämästä. Toimivan pelotteen aikaansaamisen kannalta keskeisessä asemassa ovat tehokkaammat lainvalvontatoimet, jotka keskittyvät kyberrikollisten löytämiseen, jäljittämiseen ja syytteeseenpanoon. Tämän lisäksi EU:n on tarpeen tukea jäsenvaltioitaan kyberturvallisuuden kaksikäyttövalmiuksien kehittämisessä. Kyberhyökkäyksiä voidaan vähentää vain lisäämällä kiinnijäämisen mahdollisuuksia ja hyökkäyksistä aiheutuvia seuraamuksia. Kyberhyökkäykset olisi tutkittava viipymättä ja saatettava tekijät oikeuteen tai toteutettava välittömästi asiaankuuluvia poliittisia tai diplomaattisia toimia. Jos ilmenee vakava kriisi, jolla on merkittävää kansainvälistä ja puolustuksellista ulottuvuutta, korkea edustaja voisi esittää neuvostolle vaihtoehtoja asiaan reagoimiseksi.

Yksi askel kohti kyberhyökkäysten tehokkaampaa torjuntaa rikoslain keinoin on jo otettu vuonna 2013, jolloin hyväksyttiin direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä[59]. Siinä vahvistettiin vähimmäissäännöt rikosten määrittelylle ja sovellettaville seuraamuksille tietojärjestelmiin kohdistuvien hyökkäysten alalla ja säädettiin toimenpiteistä viranomaisten välisen yhteistyön parantamiseksi. Direktiivi on edistänyt merkittävästi sitä, että kyberhyökkäysten kriminalisointi on kaikissa jäsenvaltioissa vertailukelpoisella tasolla, mikä helpottaa tämäntyyppisiä rikoksia tutkivien lainvalvontaviranomaisten yhteistyötä yli valtioiden rajojen. Direktiivin koko potentiaali voitaisiin kuitenkin saada paremmin käyttöön, jos kaikki jäsenvaltiot panisivat kaikki sen säännökset täytäntöön kaikilta osin[60]. Komissio jatkaa jäsenvaltioiden tukemista direktiivin täytäntöön panemiseksi eikä katso tällä hetkellä olevan tarvetta esittää siihen muutoksia.

3.1 Pahantekijöiden tunnistaminen

Jotta rikoksentekijöitä voitaisiin saattaa useammin oikeuteen, on kiireellisesti parannettava valmiuksia tunnistaa kyberhyökkäysten tekijöitä. Suuren haasteen lainvalvontaviranomaisille muodostaa se, miten löytää kyberrikollisuuden tutkintaan hyödyllistä tietoa, joka useimmiten tarkoittaa digitaalisia jälkiä. Siksi on tarpeen lisätä teknologisia valmiuksia tutkintojen tehostamiseksi. Tämä tarkoittaa myös Europolin kyberrikollisuusyksikön vahvistamista kyberasiantuntijoilla. Europolista on tullut avaintoimija tuettaessa useita lainkäyttöalueita koskevia jäsenvaltioiden tutkimuksia. Siitä olisi tehtävä asiantuntemuskeskus online-tutkintaan ja kyberrikostutkintaan liittyvälle jäsenvaltioiden lainvalvonnalle.

[59] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä.
[60] COM(2017) 474.

Laajalle levinnyt tapa sijoittaa useita – joskus jopa tuhansia – käyttäjiä saman IP-osoitteen taakse tekee haitallisen verkkokäyttäytymisen tutkimisesta teknisesti hyvin hankalaa. Lisäksi sen vuoksi on joskus – esimerkiksi vakavien rikosten kuten lasten seksuaalisen hyväksikäytön tapauksissa – tarpeen tutkia suuri määrä käyttäjiä yhden pahantekijän kiinni saamiseksi. Tämän vuoksi EU kannustaa uuden yhteyskäytännön (IPv6) laajempaan käyttöönottoon, sillä se mahdollistaa yhden IP-osoitteen osoittamisen kullekin käyttäjälle, mikä tietysti auttaa lainvalvonnassa ja kyberturvallisuustutkinnoissa. Ensimmäisenä askeleena yleistymisen edistämiseksi komissio ottaa IPv6-yhteyskäytäntöön siirtymisen osaksi kaikkea politiikkaansa asettamalla sen vaatimukseksi esimerkiksi hankintojen ja hankkeiden ja tutkimusten rahoittamisen yhteydessä, sekä tukee tarvittavan koulutusaineiston kehittämistä. Lisäksi jäsenvaltioiden olisi harkittava internetpalvelujen tarjoajien kanssa vapaaehtoisia sopimuksia, joilla edistetään IPv6:n yleistymistä.

Belgia on maailman ykkönen[61] IPv6:n käyttöönotossa julkisen ja yksityisen sektorin yhteistyön ansiosta: alan sidosryhmät ovat esittäneet vapaaehtoista itsesääntelytoimenpidettä, johon sisältyy yhden IP-osoitteen käytön rajoittaminen enintään 16 käyttäjälle, mikä on kannustanut siirtymään IPv6:n käyttöön[62].

Vastuullisuutta verkossa yleisesti olisi edistettävä entisestäänkin esimerkiksi toimenpiteillä, joilla ehkäistään verkkotunnusten väärinkäyttö ei-toivottuun viestintään tai verkkourkintahyökkäyksiin. Tämän tavoitteen saavuttamiseksi komissio pyrkii parantamaan verkkotunnuksia ja IP-osoitteita koskevien WHOIS-järjestelmien[63] toimintaa ja niissä olevien tietojen saatavuutta ja paikkansapitävyyttä yhdenmukaisesti sen työn kanssa, jota toteuttaa *Internet Corporation for Assigned Names and Numbers*[64].

3.2 Lainvalvontakeinojen tehostaminen

Kyberhyökkäysten torjunnassa tärkeän pelotteen muodostaa kyberrikosten tehokas **tutkinta** ja **syytteeseenpano**. Nykyisiä menettelyjä on kuitenkin muokattava paremmin internetaikakauteen sopiviksi[65]. Kyberhyökkäysten nopeus voi olla liikaa näille menettelyille. Lisäksi se tuo mukanaan erityistä tarvetta nopealle yhteistyölle yli rajojen. Tätä varten komissio aikoo, kuten Euroopan turvallisuusagendan yhteydessä ilmoitettiin, antaa vuoden 2018 alussa ehdotuksia **sähköisen todistusaineiston rajat ylittävän saatavuuden helpottamiseksi**. Samaan aikaan komissio toteuttaa käytännön toimenpiteitä, joiden tarkoituksena on parantaa sähköisen todistusaineiston rajatylittävää saatavuutta rikostutkintaa varten. Näihin sisältyy muun muassa rahoitusta rajatylittävää yhteistyötä koskevaan koulutukseen, sähköisen alustan kehittäminen tietojen vaihtamiseksi EU:ssa sekä jäsenvaltioiden välisten oikeudellisten yhteistyömuotojen standardointi.

Toinen tehokkaan syytteeseenpanon este johtuu siitä, että jäsenvaltioissa käytetään kyberrikosten tutkinnassa erilaisia rikosteknisen tutkinnan menettelyjä sähköisen

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Laajalti käytetty kysely- ja vastausprotokolla, jonka avulla tehdään kyselyjä tietokantoihin, joihin tallennetaan jonkin internetlähteen rekisteröidyt käyttäjät tai haltijat.

64 Internet Corporation for Assigned Names and Numbers (ICANN) on voittoa tavoittelematon organisaatio, joka vastaa useiden internetin nimiavaruuksiin liittyvien tietokantojen ylläpidon ja menettelyjen koordinoinnista.

65 Esimerkiksi Avalanche-bottiverkon (virtuaalinen) keskuskomentopalvelin vaihtoi fyysistä serveriä ja verkkoaluetta joka viides minuutti.

todistusaineiston keräämiseen. Tämän vaikutusta voisi lievittää kehittämällä yhteisiä rikostutkinnan standardeja. Lisäksi on tarpeen lisätä rikostutkinnan valmiuksia jäljitettävyyden ja syyllisyyden osoittamisen tukemiseksi. Ensimmäisessä vaiheessa voitaisiin jatkokehittää rikostutkinnan valmiuksia Europolissa mukauttamalla Europolin Euroopan kyberrikostorjuntakeskuksen budjetti- ja henkilöstöresursseja siten, että voidaan paremmin vastata kasvavaan tarpeeseen operatiiviselle tuelle valtioiden rajat ylittävässä kyberrikostutkinnassa. Toinen mahdollisuus olisi myötäillä edellä esitettyä salaukseen keskittyvää teknologista painopistettä tutkimalla, miten salauksen väärinkäyttö rikollisten käsissä muodostaa merkittäviä haasteita vakavien rikosten kuten terrorismin ja kyberrikollisuuden torjunnalle. Komissio esittää tulokset **salauksen roolia rikostutkinnassa**[66] koskevista pohdinnoista lokakuuhun 2017 mennessä[67].

Internetin rajaton luonne huomioon ottaen Euroopan neuvoston **tietoverkkorikollisuutta koskevaan Budapestin yleissopimukseen**[68] perustuvat kansainvälisen yhteistyön puitteet tarjoavat erilaisille maille mahdollisuuden käyttää eri kansallisten lainsäädäntöjen osalta soveltuvinta oikeusperiaatetta kyberrikollisuuden käsittelyyn. Mahdollisuutta lisätä yleissopimukseen pöytäkirja on tutkittu[69]. Sekin voisi tarjota hyvän mahdollisuuden käsitellä kysymystä, joka koskee sähköisen todistusaineiston rajatylittävää saatavuutta kansainvälisessä ympäristössä. EU ei kannata uuden kansainvälisen oikeuden välineen perustamista kyberrikollisuutta varten vaan kehottaa kaikkia maita laatimaan soveltuvaa kansallista lainsäädäntöä ja jatkamaan yhteistyötä olemassa olevissa kansainvälisissä puitteissa.

Koska välineitä tunnistetietojen poistamiseksi on laajalti saatavissa, rikollisten on helpompi välttää kiinni jääminen. **Pimeä verkko**[70] on avannut rikollisille uusia mahdollisuuksia saada käsiinsä lasten seksuaaliseen hyväksikäyttöön liittyvää aineistoa, huumeita tai aseita niin, että kiinni jäämisen riski on usein vähäinen[71]. Se on nykyisin myös kyberrikollisuuden välineiden, kuten haittaohjelmien ja hakkerointityökalujen, lähde. Komissio tutkii yhdessä sidosryhmien kanssa kansallisia lähestymistapoja uusien ratkaisujen löytämiseksi. Europolin olisi helpotettava ja tuettava pimeän verkon tutkintaa, arvioitava uhkia ja autettava lainkäyttöalueen määrittelyssä sekä priorisoitava korkean riskin tapaukset, ja EU:lla voi olla johtava asema kansainvälisten toimien koordinoinnissa[72].

Yksi kyberrikollisuuden kasvava ala on luottokorttitietojen tai muiden sähköisten maksuvälineiden laiton käyttö. Verkkokauppoihin tai muihin laillisen liiketoiminnan harjoittajiin kohdistetuilla kyberhyökkäyksillä saatuja maksutietoja myydään verkossa, ja

---

66 Neuvoston puheenjohtaja, ”Outcome of the Justice and Home Affairs Council meeting of 8 and 9 December 2016”, nro 15391/16.

67 Eighth progress report towards an effective and genuine Security Union, 29.6.2017, COM(2017) 354 final.

68 Yleissopimus on ensimmäinen kansainvälinen sopimus, joka koskee internetin ja muiden tietoverkkojen avulla tehtyjä rikoksia ja jossa käsitellään muun muassa tekijänoikeusrikoksia, tietokoneavusteisia petoksia, lapsipornografiaa ja verkkoturvallisuuden loukkauksia. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 Vuoteen 2017 mennessä Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen on ratifioinut tai siihen on liittynyt 55 maata.

69 Tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen toisen lisäpöytäkirjan luonnoksen laatimista koskeva toimeksianto T-CY (2017)3.

70 Pimeä verkko muodostuu sisällöstä rinnakkaisverkoissa, jotka käyttävät internetiä mutta joihin pääsy edellyttää erityistä ohjelmistoa, konfiguraatiota tai pääsyvaltuutusta. Pimeä verkko on osa syvää verkkoa eli tietoverkon osaa, jota ei löydy hakupalvelujen avulla.

71 Poikkeus on äskettäinen kahden suurimman pimeän verkon markkinapaikan AlphaBayn ja Hansan sulkeminen: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Europolilla on jo tärkeä rooli tällä alalla. Ks. esimerkiksi: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

rikolliset voivat käyttää niitä petosten tekemiseen[73]. Komissio ehdottaa pelotteen tehostamista **direktiivillä muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjumisesta**[74]. Sen tarkoituksena on päivittää alan säännöt ja tehostaa lainvalvonnan valmiuksia tällaisiin rikoksiin puuttumiseksi.

On myös tarpeen parantaa jäsenvaltioiden lainvalvontaviranomaisten kyberrikosten tutkintavalmiuksia sekä tietämystä kyberympäristöä hyväksi käyttäen tehtävistä rikoksista ja syyttäjien ja oikeuslaitoksen käytettävissä olevista tutkintakeinoista. Eurojust ja Europol edistävät osaltaan tämän tavoitteen saavuttamista ja koordinoinnin lisäämistä yhteistyössä Europolin kyberrikostorjuntakeskuksen erikoistuneiden neuvoa-antavien ryhmien, kyberrikollisuuden torjuntayksikköjen päällikköjen ja kyberrikollisuuteen erikoistuneiden syyttäjien verkoston kanssa. Komissio osoittaa kyberrikollisuuden torjuntaan 10,5 miljoonaa euroa pääasiassa **sisäisen turvallisuuden rahaston poliisiyhteistyön ohjelmasta**. Koulutus on tärkeä osatekijä, jota varten Euroopan kyberrikollisuuden tutkinnan koulutusryhmä on kehittänyt käyttökelpoisia aineistoja. Ne olisi saatava laajasti lainvalvonnan ammattilaisten käyttöön Euroopan unionin lainvalvontakoulutusviraston (CEPOL) tuella.

3.3 Julkisen ja yksityisen sektorin yhteistyö kyberrikollisuuden torjunnassa

Lainvalvonnan toimivuudelle asettaa haasteen digitaalinen maailma, joka koostuu pääasiassa yksityisessä omistuksessa olevasta infrastruktuurista ja monista eri toimijoista eri lainkäyttöalueilla. Sen vuoksi yhteistyö yksityisen sektorin kanssa, toimiala ja kansalaisyhteiskunta mukaan luettuina, on välttämätöntä viranomaisille, jotta ne voivat torjua rikoksia tehokkaasti. Tässä yhteydessä keskeisessä asemassa on myös finanssiala, ja yhteistyötä sen kanssa olisikin lisättävä. Esimerkiksi rahanpesun selvittelykeskusten[75] roolia kyberrikollisuuden yhteydessä olisi vahvistettava.

Jotkin jäsenvaltiot ovat jo ryhtyneet toimiin asiassa. Alankomaissa rahoituslaitokset ja lainvalvontaviranomaiset työskentelevät yhdessä verkkopetosten ja kyberrikollisuuden torjumiseksi sähköisen rikollisuuden erityistyöryhmässä. Saksassa on kyberrikollisuuden torjunnan osaamiskeskus, joka mahdollistaa jäsentensä välisen tietojen vaihtamisen tiiviissä yhteistyössä Saksan liittovaltion poliisin kanssa sekä kehittää toimenpiteitä kyberrikollisuudelta suojautumiseksi. Kuusitoista jäsenvaltiota[76] on perustanut kyberrikollisuuden torjunnan osaamiskeskuksia helpottaakseen yhteistyötä lainvalvontaviranomaisten, tiedemaailman ja yksityisen sektorin välillä parhaiden käytäntöjen, koulutuksen ja valmiuksien kehittämiseksi ja vaihtamiseksi.
Komissio tukee julkisen ja yksityisen sektorin kumppanuuksien ja yhteistyömekanismien perustamista kohdennetuilla hankkeilla, jollaisia ovat esimerkiksi verkkopetosten kyberkeskusten ja asiantuntijoiden verkosto[77], joka toteuttaa tiedonjakomallin ja -standardin sähköisten rikosten riskien ja verkkopetosten analysoimiseksi ja torjumiseksi.

---

[73] Petosten tuotto on järjestäytyneelle rikollisuudelle merkittävä tulonlähde, jonka avulla rahoitetaan myös muuta rikollista toimintaa, kuten terrorismia sekä huume- ja ihmiskauppaa.

[74] COM(2017) 489.

[75] Rahanpesun selvittelykeskukset ovat kansallisia keskuksia, jotka vastaanottavat ja analysoivat ilmoituksia epäilyttävistä liiketoimista ja muita tietoja rahanpesusta, siihen liittyvistä esirikoksista ja terrorismin rahoituksesta sekä jakavat tietoja analysointien tuloksista.

[76] Belgia, Bulgaria, Espanja, Irlanti, Itävalta, Kreikka, Kypros, Liettua, Puola, Ranska, Romania, Saksa, Slovenia, Tšekki, Viro ja Yhdistynyt kuningaskunta.

[77] EU-OF2CEN-aloitteen tavoitteena on mahdollistaa EU:n laajuinen järjestelmällinen tietojen jakaminen internet-petoksista pankkien ja lainvalvontaviranomaisten välillä, jotta voidaan ehkäistä maksujen suorittamista petoksentekijöille ja rahamuuleille sekä tutkia ja saattaa syytteeseen rikoksentekijät. Se saa osarahoitusta EU:lta (sisäisen turvallisuuden rahaston poliisiyhteistyön ohjelmasta).

Kun on kyse kyberrikollisuudesta, yksityisten yritysten on voitava jakaa lainvalvontaviranomaisten kanssa tietoja konkreettisista poikkeamista. Tämä voi koskea myös henkilötietoja, ja silloin on noudatettava tietosuojasääntöjä kaikilta osin. EU:n tietosuojauudistukseen, joka tulee voimaan toukokuussa 2018, sisältyy yhteinen joukko sääntöjä lainvalvontaviranomaisten ja yksityisten tahojen yhteistyön edellytyksistä. Euroopan komissio pyrkii yhdessä Euroopan tietosuojaneuvoston ja sidosryhmien kanssa yksilöimään alan parhaita käytäntöjä ja antamaan tarvittaessa ohjeistusta.

3.4 Politiikkatoimien tehostaminen

EU on äskettäin hyväksynyt **puitteet EU:n yhteiselle diplomaattiselle vastaukselle haitallisiin kybertoimiin**[78] (niin sanottu kyberdiplomatian välineistö). Niihin sisältyy yhteiseen ulko- ja turvallisuuspolitiikkaan kuuluvia, tarvittaessa myös rajoittavia toimenpiteitä, joiden avulla voidaan lujittaa EU:n vastausta toimintaan, joka vahingoittaa sen poliittisia, turvallisuuteen liittyviä ja taloudellisia etuja. Mainitut puitteet ovat tärkeä askel kehitettäessä ilmoittamis- ja reagointivalmiuksia EU:ssa ja jäsenvaltioissa. Ne auttavat parantamaan valmiuksia haitalliseen kybertoimintaan syyllistyvien löytämiseksi. Tavoitteena on vaikuttaa mahdollisten hyökkääjien käyttäytymiseen, ottaen huomioon tarve varmistaa vastatoimien oikeasuhteisuus. Valtiollisen tai valtiosta riippumattoman toimijan syyllisyyden osoittaminen on suvereeni poliittinen päätös, joka perustuu kaikista lähteistä saatavaan tiedustelutietoon. Puitteiden täytäntöönpano on parhaillaan käynnissä jäsenvaltioiden kanssa, ja sen edistämistä koordinoidaan läheisesti myös laajamittaisiin kyberhyökkäyksiin reagointia koskevan suunnitelman[79] kanssa. EU:n tiedusteluanalyysikeskuksen[80] olisi yhdistettävä, analysoitava ja jaettava puitteisiin sisältyvien toimenpiteiden käytön kannalta tarvittavaa tilannetietoisuutta läheisessä yhteistyössä jäsenvaltioiden ja EU:n toimielinten kanssa.

3.5 Kyberturvallisuuspelotteen kehittäminen jäsenvaltioiden puolustusvalmiuksien avulla

Jäsenvaltiot kehittävät jo nyt kyberpuolustusvalmiuksiaan. EU:lla on hyvät edellytykset auttaa sotilas- ja siviilipuolen välisen synergian edistämisessä, ottaen huomioon kyberpuolustuksen ja kyberturvallisuuden välisten rajojen hämärtyminen sekä kybervälineiden ja -teknologian kaksikäyttöluonne ja se, että eri jäsenvaltioiden lähestymistavoissa on suuria eroja.[81].

Jäsenvaltiot, joilla on edistyneimmät kyberturvallisuusvalmiudet ja jotka haluavat tehdä niiden suhteen yhteistyötä, voisivat harkita kyberpuolustuksen sisällyttämistä – korkean edustajan, komission ja Euroopan puolustusviraston tuella – pysyvän rakenteellisen yhteistyön puitteisiin. Tämä voisi rakentua niiden toimien varaan, joita edellä on esitetty EU:n teollisten valmiuksien ja strategisen riippumattomuuden edistämiseksi. EU voi myös edistää yhteentoimivuutta, myös helpottamalla valmiuksien kehittämistä, koulutuksen koordinointia ja kaksikäyttöstandardien kehittämistä.

Lisäksi olisi hyödynnettävä kaikin tavoin yhteinen kehys hybridiuhkien, joihin usein liittyy kyberhyökkäyksiä, torjumiseksi erityisesti EU:n hybridianalyysikeskuksen ja Helsinkiin hiljattain perustetun Euroopan hybridiuhkien torjunnan osaamiskeskuksen välityksellä.

---

78 http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

79 C(2017) 6100.

80 JOIN(2016) 018 final.

81 EU käsittää kyberavaruuden maahan, ilmaan ja mereen verrattavissa olevaksi toimintaympäristöksi. Kyberpuolustukseen sisältyy myös avaruusresurssien ja niihin liittyvän maainfrastruktuurin suojaaminen ja resilienssi.

Kyseisen hybridiosaamiskeskuksen tehtävänä on kannustaa strategiseen vuoropuheluun sekä tehdä tutkimusta ja analyysejä.

EU antaa vuonna 2014 hyväksytylle EU:n kyberpuolustuspolitiikan kehykselle[82] uutta painoarvoa välineenä, jonka avulla voidaan jatkaa kyberturvallisuuden ja -puolustuksen integroimista yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP). YTPP:n operaatioiden itsensä kyberresilienssi on olennaista, ja siksi kehitetään standardoituja menettelyjä ja teknisiä valmiuksia, joilla voidaan tukea sekä siviilialan että sotilaallisia operaatioita samoin kuin niiden suunnittelu- ja toteutusvoimavarojen rakenteita ja Euroopan ulkosuhdehallinnon tietoteknologian palveluntarjoajia. Jäsenvaltioiden yhteistyön edistämiseksi ja EU:n työn ohjaamiseksi tällä alalla Euroopan puolustusvirasto ja Euroopan ulkosuhdehallinto helpottavat yhteistyössä komission yksikköjen kanssa jäsenvaltioiden kyberpuolustuksen alan päätöksentekijöiden strategisen tason osallistumista. Lisäksi EU tukee eurooppalaisten kyberturvallisuusratkaisujen kehittämistä osana toimia, joita se toteuttaa Euroopan puolustuksen teollisen ja teknologisen perustan hyväksi. Tähän sisältyy myös kyberturvallisuuden ja -puolustuksen huippuosaamisen alueellisten klusterien edistäminen.

Komission yksiköt tekevät läheistä yhteistyötä EU:n ulkosuhdehallinnon, jäsenvaltioiden ja muiden asiaan liittyvien EU-elinten kanssa perustaakseen vuoteen 2018 mennessä **kyberpuolustuksen koulutusfoorumin** korjaamaan nykyistä osaamisvajetta kyberpuolustuksen alalla. Se täydentää Euroopan puolustusviraston työtä tällä alalla ja auttaa korjaamaan nykyistä osaamisvajetta kyberturvallisuuden ja kyberpuolustuksen alalla.

Avaintoimet

- Sähköisen todistusaineiston rajat ylittävää saatavuutta koskeva komission aloite (vuoden 2018 alussa);
- Muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjumiseksi ehdotetun direktiivin nopea hyväksyminen Euroopan parlamentissa ja neuvostossa;
- IPv6-vaatimusten sisällyttäminen EU:n hankintoihin, tutkimukseen ja hankkeiden rahoitukseen; jäsenvaltioiden ja Internet-palveluntarjoajien välisiä vapaaehtoisia sopimuksia IPv6:n käyttöönoton nopeuttamiseksi;
- Kyberrikostutkinnan ja pimeän verkon seurannan uusi laajennettu keskittäminen Europoliin;
- EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevien puitteiden täytäntöönpano;
- Taloudellisen tuen lisääminen kansallisille ja ylikansallisille hankkeille rikosoikeuden tehostamiseksi kybertoimintaympäristössä.
- Vuoteen 2018 mennessä kyberpuolustuksen koulutusfoorumi korjaamaan nykyistä osaamisvajetta kyberpuolustuksen alalla.

4. KYBERTURVALLISUUTTA KOSKEVAN KANSAINVÄLISEN YHTEISTYÖN LUJITTAMINEN

EU:n kansainvälinen kyberturvallisuuspolitiikka, jota ohjaavat EU:n perusarvot ja -oikeudet, kuten ilmaisunvapaus ja oikeus yksityisyyteen ja henkilötietojen suojaan, sekä avoimen, vapaan ja turvallisen kybertoimintaympäristön edistäminen, on suunniteltu vastaamaan maailmanlaajuisen kybervakauden edistämiseen liittyvään jatkuvasti muuttuvaan haasteeseen

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

sekä edistämään Euroopan strategista riippumattomuutta ja turvallisuutta kybertoimintaympäristössä.

4.1 Kyberturvallisuus ulkosuhteissa

On olemassa näyttöä siitä, että eri puolilla maailmaa ihmiset pitävät muista maista tulevia kyberhyökkäyksiä yhtenä suurimmista kansalliseen turvallisuuteen kohdistuvista uhkista[83]. Kun otetaan huomioon uhkan maailmanlaajuinen luonne, vahvojen liittolaisuus- ja kumppanuussuhteiden luominen ja ylläpitäminen kolmansien maiden kanssa on olennaisen tärkeää kyberhyökkäysten ehkäisemiseksi ja niitä koskevan pelotteen luomiseksi, mikä on entistäkin tärkeämpää kansainvälisen vakauden ja turvallisuuden kannalta. EU pitää kahdenvälisissä, alueellisissa, usean sidosryhmän välisissä ja monenvälisissä sitoumuksissaan ensisijaisena konfliktien estoa ja kyberympäristön vakautta edistävän strategisen kehyksen luomista.

EU kannattaa vahvasti kansainvälisen oikeuden ja erityisesti YK:n peruskirjan soveltamista kybertoimintaympäristössä. Sitovan kansainvälisen oikeuden täydennykseksi EU kannattaa valtion vastuullista käyttäytymistä koskevia vapaaehtoisia ei-sitovia normeja, sääntöjä ja periaatteita, joita on esittänyt YK:n hallitustenvälinen asiantuntijaryhmä[84]. Lisäksi se kannustaa kehittämään ja panemaan täytäntöön alueellisia luottamusta lisääviä toimenpiteitä sekä Euroopan turvallisuus- ja yhteistyöjärjestössä että muilla alueilla.

Kahdenvälisellä tasolla jatketaan kyberalan vuoropuheluja[85] ja niitä täydennetään toimilla yhteistyön helpottamiseksi kolmansien maiden kanssa, jotta voidaan lujittaa asianmukaisen huolellisuuden ja valtion vastuun periaatteita kybertoimintaympäristössä. EU painottaa kansainvälisessä toiminnassaan kansainvälisiä turvallisuuskysymyksiä kybertoimintaympäristössä, mutta varmistaa, että kyberturvallisuudesta ei tule tekosyytä markkinoiden suojelulle ja perusoikeuksien ja -vapauksien rajoittamiselle, mukaan lukien ilmaisunvapaus ja tiedonsaantioikeus. Kattava lähestymistapa kyberturvallisuuteen edellyttää ihmisoikeuksien noudattamista, ja EU jatkaa perusarvojensa puolustamista maailmanlaajuisesti ja noudattaen EU:n ihmisoikeussuuntaviivoja vapaudesta verkossa[86]. Tässä yhteydessä EU korostaa, että on tärkeää saada kaikki sidosryhmät osallistumaan internetin hallintoon.

Komissio on tehnyt myös ehdotuksen[87] EU:n vientivalvonnan uudistamiseksi. Siihen sisältyy säännöksiä sellaisen verkkovalvontateknologian vientivalvonnasta, josta voi aiheutua ihmisoikeuksien loukkauksia tai jota voitaisiin käyttää EU:n oman turvallisuuden vastaisesti. Komissio tehostaa vuoropuheluja kolmansien maiden kanssa edistääkseen maailmanlaajuista lähentymistä ja vastuullista käytöstä alalla.

4.2 Kyberturvallisuuteen liittyvien valmiuksien kehittäminen

Maailmanlaajuinen kybervakaus riippuu kaikkien maiden paikallisesta ja kansallisesta valmiudesta ehkäistä kyberturvallisuuspoikkeamia ja reagoida niihin sekä tutkia kyberrikostapauksia ja nostaa niistä syytteitä. Kansallisen resilienssin parantamiseen tähtäävien toimien tukeminen kolmansissa maissa parantaa kyberturvallisuuden tasoa

---

83 Spring 2017 Global Attitudes Survey, Pew Research Centre.
84 A/68/98 ja A/70/174.
85 Syyskuussa 2017 EU kävi kyberalan vuoropuheluja Yhdysvaltojen, Kiinan, Japanin, Korean tasavallan ja Intian kanssa.
86 EU Human Rights Guidelines on Freedom of Expression Online and Offline.
87 COM(2016) 616.

maailmanlaajuisesti, millä on myönteinen vaikutus myös EU:hun. Nopeasti kehittyvien kyberuhkien torjumiseksi tarvitaan toimia koulutuksen, politiikan ja lainsäädännön kehittämiseksi sekä tehokkaasti toimivia tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyviä ryhmiä ja kyberrikollisuuden torjuntayksikköjä kaikissa maailman maissa.

EU on johtanut kansainvälistä kyberturvallisuusvalmiuksien kehittämistä vuodesta 2013 ja liittänyt tähän liittyviä toimia järjestelmällisesti kehitysyhteistyöhönsä. EU jatkaa oikeusperustaisen valmiuksien kehittämismallin edistämistä Digital4Development-lähestymistavan[88] mukaisesti. Valmiuksien kehittämisen painopiste on EU:n naapuruuspolitiikan maissa ja kehitysmaissa, joissa verkkoyhteydet lisääntyvät ja uhkat kehittyvät nopeasti. EU:n toimet täydentävät EU:n kehitystavoitteita kestävän kehityksen toimintaohjelman Agenda 2030 valossa sekä yleisiä toimia institutionaalisten valmiuksien kehittämiseksi.

Jotta voidaan parantaa EU:n kykyä hyödyntää kollektiivista asiantuntemustaan valmiuksien kehittämisen tukemiseksi, olisi perustettava EU:n kybervalmiuksien kehittämisverkosto, joka saattaisi yhteen EU:n ulkosuhdehallinnon, jäsenvaltioiden kyberturvallisuusviranomaiset, EU:n virastot, komission yksiköt, tiedeyhteisön ja kansalaisyhteiskunnan. EU laatii kybervalmiuksien kehittämiselle suuntaviivat, jotka auttavat tarjoamaan parempaa poliittista ohjausta ja EU:n toimien priorisointia kolmansien maiden auttamiseksi.

Lisäksi EU työskentelee yhdessä muiden kehitysavun antajien kanssa tällä alalla, jotta voidaan välttää päällekkäisyyksiä ja helpottaa valmiuksien kehittämisen kohdentamista eri alueilla.

4.3 EU:n ja NATOn yhteistyö

EU syventää jo hyvin edennyttä kyberturvallisuuden, hybridiuhkien ja puolustuksen alan yhteistyötä NATOn kanssa 8. heinäkuuta 2016 annetun yhteisen julistuksen mukaisesti[89]. Painopisteitä ovat yhteentoimivuuden edistäminen johdonmukaisten kyberpuolustusvaatimusten ja -standardien avulla, yhteistyön lujittaminen koulutuksen ja harjoitusten aloilla sekä koulutusvaatimusten yhdenmukaistaminen.

EU ja NATO lisäävät myös kyberpuolustukseen liittyvää tutkimus- ja innovointiyhteistyötä sekä kehittävät nykyistä teknistä järjestelyä kyberturvallisuutta koskevien tietojen jakamiseksi kyberturvallisuusyksikköjensä välillä[90]. Viimeaikaisia yhteisiä toimia hybridiuhkiin vastaamiseksi, erityisesti EU:n hybridianalyysikeskuksen ja NATOn hybridianalyysiosaston välistä yhteistyötä, olisi tehostettava entisestään resilienssin ja reagointivalmiuksien parantamiseksi. EU:n ja NATOn yhteistyötä tiivistetään myös kyberpuolustusharjoituksilla, joihin osallistuu EU:n ulkosuhdehallinto ja muita EU:n yksikköjä sekä vastaavia yksikköjä NATOsta, mukaan lukien NATOn kyberpuolustuksen osaamiskeskus Tallinnassa. NATO ja EU toteuttavat ensimmäistä kertaa rinnakkaisia ja koordinoituja harjoituksia, joissa testataan vastausta hybridiuhkaskenaarioon. NATO johtaa harjoitusta vuonna 2017 ja EU samalla tavoin vuonna 2018. EU:n ja NATOn neuvostoille joulukuussa 2017 toimitettava seuraava raportti EU:n ja NATOn yhteistyöstä tarjoaa tilaisuuden tarkastella mahdollisuuksia laajentaa yhteistyötä entisestään, erityisesti varmistamalla turvalliset ja varmat viestintäkeinot kaikkien niiden instituutioiden ja elinten välillä, joita asia koskee, ENISA mukaan lukien.

Avaintoimet

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU ja NATOn NCIRC-yksikkö (Computer Incident Response Capability).

- Edistetään konfliktien estoa ja kyberympäristön vakautta koskevan strategisen kehyksen luomista;
- Perustetaan uusi kybervalmiuksien kehittämisverkosto, jotta voidaan tukea kolmansien maiden kykyä puuttua kyberuhkiin, ja laaditaan EU:n kyberturvallisuusvalmiuksien kehittämiselle suuntaviivat EU:n toimien priorisoimiseksi;
- Jatketaan EU:n ja NATOn yhteistyötä, mukaan lukien yhteinen osallistuminen rinnakkaisiin ja koordinoituihin harjoituksiin sekä kyberturvallisuusstandardien yhteentoimivuuden parantaminen.

5. PÄÄTELMÄT

EU:n varautuminen kyberuhkiin on keskeistä sekä digitaalisten sisämarkkinoiden että turvallisuus- ja puolustusunionin kannalta. Euroopan kyberturvallisuuden tehostaminen ja sekä siviili- että sotilaskohteisiin kohdistuviin uhkiin puuttuminen on välttämätöntä.

Tuleva digitaalihuippukokous, jonka järjestää puheenjohtajavaltio Viro 29. syyskuuta 2017, tarjoaa tilaisuuden osoittaa, miten yhdessä sitoudutaan asettamaan kyberturvallisuus keskiöön EU:ssa digitaalisena yhteiskuntana. Osana tätä yhteistä sitoutumista komissio kehottaa jäsenvaltioita vakuuttamaan, miten ne aikovat toimia aloilla, joista ne ovat ensi sijassa vastuussa. Tähän olisi sisällyttävä kyberturvallisuuden lujittamista seuraavin keinoin:

- Verkko- ja tietoturvadirektiivin tosiasiallinen täytäntöönpano kaikilta osin 9. toukokuuta 2018 mennessä sekä kyberturvallisuudesta vastaaville viranomaisille resurssit, jotka ne tarvitsevat tehtäviensä suorittamiseen;
- Samat säännöt julkishallinnoille, ottaen huomioon niiden merkitys koko yhteiskunnassa ja taloudessa;
- Kyberturvallisuuskoulutusta julkishallinnossa;
- Kyberturvallisuustietoisuuden priorisointi tiedotuskampanjoissa ja kyberturvallisuuden sisällyttäminen tieteellisiin ja ammatillisiin opetussuunnitelmiin;
- Kyberpuolustushankkeiden tukeminen pysyvän rakenteellisen yhteistyön ja Euroopan puolustusrahaston aloitteilla.

Yhteisessä tiedonannossa esitetään haasteen mittasuhteet sekä toimenpiteet, joita EU voi toteuttaa. Euroopalla on oltava sietokykyä uhkia vastaan, jotta se voi suojella tehokkaasti kansalaisiaan varautumalla mahdollisiin kyberturvallisuuspoikkeamiin, varmistaa vahvan suojauksen rakenteissaan ja käyttäytymisessään, palautua nopeasti mahdollisista kyberhyökkäyksistä ja ehkäistä pelotteella hyökkäyksiin syyllistymistä. Tiedonannossa esitetään kohdennettuja toimenpiteitä EU:n kyberturvallisuusrakenteiden ja -valmiuksien lujittamiseksi koordinoidusti jäsenvaltioiden ja niiden EU:n eri rakenteiden, joita asia koskee, täysimittaisella yhteistyöllä ja kunnioittaen näiden toimivaltuuksia ja vastuualueita. Tiedonanto osoittaa selkeästi, että EU ja sen jäsenvaltiot toimivat yhdessä toteuttaakseen kyberturvallisuusstandardin, joka on Euroopan nykyisten, koko ajan kasvavien haasteiden tasolla.