**­­**

****

**Luonnos versio 1.0**

**4.3.2019**

**Suomen kyberturvallisuusstrategia 2019**

Sisällys

[Johdanto 2](#_Toc2584596)

[Strategiset linjaukset 3](#_Toc2584597)

[1. Kansainvälisen yhteistyön kehittäminen – kybertoimintaympäristön rajatonta turvaamista 3](#_Toc2584598)

[2. Kyberturvallisuuden johtamisen kehittäminen – kehittämisohjelma ja parempi koordinaatio 3](#_Toc2584599)

[3. Kyberturvallisuuden osaamisen kehittäminen – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina 5](#_Toc2584600)

# Johdanto

Suomen kyberturvallisuusstrategiassa 2019 asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi[[1]](#footnote-1). Kansallisen kyberturvallisuuden toteutus kytkeytyy Yhteiskunnan turvallisuusstrategiaan (2017) ja siinä kuvattuun yleisiin varautumisen ja turvallisuuden yhteensovittamisen sekä toimivaltaisen viranomaisen periaatteisiin. Strategia nojautuu Suomen kyberturvallisuusstrategian 2013 yleisiin periaatteisiin, Suomen tavoite on olla kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa. Tämän uuden strategian tarkoituksena on lisäksi vahvistaa yhteiskunnan ja kansalaisten luotettavia digitaalisia palveluita sekä lisätä mahdollisuuksia kehittää Suomessa korkealaatuista ja luotettavaa digitaalista liiketoimintaa.

Uusi kyberturvallisuusstrategia käynnistää kansallisen kyberturvallisuuden kehittämisohjelman valmistelun. Kehittämisohjelman valmistelua tukee uusi johtamisen koordinaatiomalli. Suomen kyberturvallisuusstrategia 2019:n keskeisin tavoite on kytkeä kyberturvallisuuden yhteiskunnallinen, julkisen hallinnon ja elinkeinoelämän suunnittelu ja yhteistyö kiinteämmin toisiinsa. Tämä toteutuu yhteistyössä laadittavalla kehittämisohjelmalla, joka parantaa tilannekuvaa ja liittää suunnittelun selkeämmin muuhun toimintaan. Kehittämisohjelma on osa EU:n kyberturvallisuusstrategian toimeenpanoa.

Suomen kyberturvallisuusstrategian päivittämistarpeeseen ovat vaikuttaneet toimintaympäristössä tapahtuneet merkittävät muutokset ja kansallisessa toiminnassa havaitut kehittämiskohteet. Digitaalisen toimintaympäristön kehitys tarjoaa uusia merkittäviä mahdollisuuksia, kuten alustatalous, ekosysteemit, uudet palveluiden tuotantomallit ja päätelaitteiden sekä tietoliikenteen kehittäminen. Toisaalta toimintaympäristöön kohdistuu paitsi vanhoja riskejä, kuten ihmisen tekevät virheet, myös kehittyviä ja muuttuvia uhkia, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja, erityisesti kyberrikollisuuden, valtiollisen tiedustelun ja erilaisin hybridivaikuttamisen keinoin. Suomen kansallisen kyberturvallisuuden tilasta on tehty useita selvityksiä[[2]](#footnote-2). Niissä tehtyjä ehdotuksia on huomioitu tässä strategiassa ja ne otetaan huomioon myös valmisteltavassa kehittämisohjelmassa.

# Strategiset linjaukset

# Kansainvälisen yhteistyön kehittäminen – kybertoimintaympäristön rajatonta turvaamista

Kansainvälinen yhteistyö on Suomen kyberturvallisuudelle elintärkeää. Suomen etu on tehdä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Tämä koskee niin teknistä yhteistyötä kuin poliittisenkin tason yhteistyötä ja vuoropuhelua.

Kansainvälinen yhteistyö nojaa voimassaolevaan kansainväliseen oikeuteen, kansainvälisiin sopimuksiin ja ihmisoikeuksien kunnioittamiseen myös kybertoimintaympäristössä. Suomi haluaa säilyttää universaalin, vapaan ja vakaan internetin. Suomi ei hyväksy pyrkimystä rajoittaa internetin vapautta ja avoimuutta ja sitä kautta yksilön perusoikeuksia ja –vapauksia. Suomi korostaa kaikessa kyberyhteistyössä oikeusvaltionäkökohtia, demokratiaa, läpinäkyvyyttä sekä monitoimijamalliin (valtio, yritykset, tutkimustoiminta, kansalaisjärjestöt) pohjautuvaa toimintaa.

Suomi vaikuttaa kansainvälisen kyberagendan kysymysten kehittämiseen aktiivisesti Euroopan Unionissa ja keskeisissä kansainvälisissä järjestöissä (mm. YK, ETYJ, EN, Nato, OECD). Tämä työ on osa kansainvälisen sääntöpohjaisen järjestelmän vahvistamista, mikä on Suomen ulkopolitiikan keskeinen tavoite.

Euroopan Unionin päätökset sekä EU:ssa tehtävä yhteistyö luovat selkärangan Suomen kansalliselle kyberpolitiikalle ja sen kehittämiselle. EU:n uudistettu kyberstrategia[[3]](#footnote-3) sekä keskeiset lainsäädäntöhankkeet, esim. EU:n verkko- ja tietoturvadirektiivi (NIS), vaikuttavat vahvasti kyberturvallisuuden kehittämiseen myös kansallisella tasolla. Suomi on lisäksi aktiivisesti mukana kehittämässä EU:n kyberiin liittyvää yhteistä ulko- ja turvallisuuspolitiikkaa. EU:n kyberturvallisuuden laaja tutkimus- ja kehittämistoiminta edellyttää kansallisten painopisteiden määrittämistä ja aktiivista osallistumista.

# Kyberturvallisuuden johtamisen kehittäminen – kehittämisohjelma ja parempi koordinaatio

Kyberturvallisuusstrategian toimeenpano-ohjelmat ovat tähän mennessä perustuneet vain kehittämiseen sitoutuneiden toimijoiden esityksiin ja toimivaltaisten viranomaisten osittain siilomaiseen työskentelyyn. Tuloksekas kyberturvallisuuden suunnittelu edellyttää vahvempaa sidosta muuhun toimintaan, talouden suunnitteluun ja yhteistoimintafoorumeihin. Tätä parantaa hallituskausien yli ulottuva kyberturvallisuuden kehittämisohjelma. Ohjelma konkretisoi linjauksia, selkeyttää kyberturvallisuuden hankkeiden, tutkimuksen ja kehittämisohjelmien kokonaiskuvaa, seuraa strategian toimeenpanoa sekä parantaa rahoituksen yhteensovittamista.

Kyberturvallisuuden koordinaation parantamiseksi perustetaan Suomen kyberturvallisuusjohtajan tehtävä. Hänen johdollaan laaditaan ministeriöiden, Turvallisuuskomitean ja kyberturvallisuustoimijoiden asiantuntemusta hyödyntäen kyberturvallisuuden kokonaisvaltainen tilannekuva ja kehittämisohjelma sekä seurataan kyberturvallisuuden kehittymistä. Kyberturvallisuusjohtaja toimii myös kyberturvallisuusasioissa neuvonantajana valtion johdolle. Uusi tehtävä perustetaan valtioneuvoston kansliaan. Suomen kyberturvallisuusjohtajan tehtävänkuva on yhteensovittava, joten se ei muuta ministeriöiden ja toimivaltaisten viranomaisten kyberturvallisuustehtäviä ja toimivaltuuksia.

Kybertoimintaympäristöön kohdistuvien häiriötilanteiden johtamista ja yhteistyötä operatiivisella tasolla kehitetään kyberturvallisuustoimijoiden kesken. Häiriötilanteiden hallinnassa tukeudutaan yleiseen häiriötilanteiden hallintamalliin ja hyödynnetään tarvittaessa valmiuspäällikkö­kokousta. Kyberturvallisuuskeskuksen kykyä kansallisen kyberturvallisuuden tilannekuvan kokoamisessa ja strategisessa johtamisessa tarvittavan tiedon tuottamisessa vahvistetaan.

Viranomaisten kyberturvallisuusyhteistyötä kehitetään uuden tiedustelu- ja muun toimialaan kytkeytyvän lainsäädännön myötä kehittämisohjelmassa. Keskeisiä kehittämisen osa-alueita ovat kyberpuolustus ja kyberrikollisuuden torjunta.

Digitaalisessa toimintaympäristössä toisiinsa liittyviä ja toisistaan riippuvaisia toimintoja ei voida kehittää toimintavarmoiksi ja yhteensopiviksi ottamatta huomioon kokonaisarkkitehtuuria. Toiminnan jatkuvuus ja häiriötilanteisiin varautuminen edellyttää hankinta- ja kilpailuttamisosaamista, sopimusvelvoitteiden toteutumisen arviointia sekä kokonaisvaltaista toimittajaverkoston ja toimitusketjujen hallintaa. Digitaalisessa toimintaympäristössä kyberturvallisuuteen varautuminen edellyttää yhteiskunnan eri toimijoiden, valtionhallinnon ja elinkeinoelämän välistä yhteistyötä ja osaamisen vahvistamista eri sektoreilla.

Yhteiskunnan tietovarallisuuden turvaamiseen tulee kiinnittää jatkossa huomiota entistä enemmän. Tämä koskee erityisesti turvaluokitellun tiedon hallintaa. Tiedon hallinnan oikeuksien tulee toisaalta taata tiedon pysyminen vain siihen oikeutettujen käytettävissä ja toisaalta mahdollistaa sen tehokas hyödyntäminen esimerkiksi tarvittavan tilannekuvan muodostamisessa. Tämä korostaa myös kokonaisarkkitehtuurin luomisen tarvetta luokitellun tiedon osalta tieto- ja palveluintegraation mahdollistamiseksi.

Muita strategisia toimenpiteitä osa-alueen kehittämiseksi:

* Tunnistetaan yhteiskunnan elintärkeille toiminnoille välttämättömät tietovarannot, digitaaliset palvelut ja infrastruktuuri. Tämä on edellytys sille, että jatkuvuuden ja turvallisuuden kehittämiseen käytettävät resurssit voidaan kohdentaa oikein. Erityisesti tulee kehittää elintärkeille toiminnoille välttämättömien verkostojen riskienhallintaa, häiriönhallintaa sekä toimintojen varamenettelyjä tilanteisiin, joissa tietotekniset ratkaisut ovat vakavasti häiriintyneet. Tämän mahdollistamiseksi luodaan malli, jolla kriittisiä palveluita luokitellaan ja priorisoidaan sekä tunnistetaan niihin liittyvät kyberturvallisuuden velvoitteet.
* Linjataan perusteet toiminnan jatkuvuuden kehittämiselle sekä yhteistyölle digitaalisessa yhteiskunnassa. Linjauksissa määritetään kyberturvallisuuteen liittyvä palveluiden tuottamisen, hankkimisen ja toiminnan kansallinen tavoitetaso. Lisäksi määritetään, mitkä ovat sellaisia olemassa olevia kriittisiä digitaalisia palveluita, joita kansalliset jatkuvuuden, turvaamisen ja hallinnan vaatimukset koskevat ja mitä on tarpeen kehittää.
* Kaupallisissa ympäristöissä on kyettävä toimimaan kriittisten toimintojen asettamien turvallisuusvaatimusten mukaisesti. Kansallisen turvallisuuden ja standardien mukaista vaatimustenhallintaa parannetaan ja yhtenäistetään turvallisuuskriittisissä palveluissa. Tuotteiden ja kokonaisten ratkaisuympäristöjen toteutuksen todentamista, testausta, arviointia ja käyttösuosituksia kehitetään vaatimusten toteutumisen varmistamiseksi.
* Turvataan turvallisuusviranomaisten ja elinkeinoelämän kriittisten toimijoiden digitaalisten palvelujen käyttö ja kehittäminen kaupallisia palveluja hyödyntävillä ja niitä täydentävillä erityissuojatuilla ratkaisuilla. Ratkaisuihin liitetään luotettava paikannus ja ajan jakaminen sekä varmistetaan sähkönsaanti pitkäkestoisessa sähköhäiriössä.
* Tuetaan yhteiskunnan elintärkeisiin toimintoihin liittyvien yritysten kriittisten palvelujen tuottamista ja jatkuvuudenhallintaa. Tehtävien tavoitetason kuvaaminen ja viranomaisten tarjoamien tukimekanismien kehittäminen selkiyttävät yritysten asemaa. Vastuuviranomaisille asetetaan selkeät tavoitteet kyberturvallisuuden kehittämiseksi. Viranomaiset voivat edistää kyberturvallisuustavoitteiden toteutumista muun muassa sisällyttämällä niitä kaupallisiin sopimuksiin ja tärkeimmiltä osin myös lainsäädäntöön.

# Kyberturvallisuuden osaamisen kehittäminen – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina

Suomalainen yhteiskunta tarvitsee kyberturvallisuuden osaamista sekä julkisessa hallinnossa että elinkeinoelämässä. Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, jossa jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme. Jokainen kansalainen on siten tärkeä kyberturvallisuustoimija, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen. Kansallisesti on varmistettava, että jokaisella kansalaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä.

Hallitakseen kyberturvallisuutta koskevia riskejä, viranomaiset ja yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin alihankkijoidensa piirissä. Kansallisella tasolla on varmistettava, että yrityksillä on sekä huippuosaajia että muuta osaavaa henkilöstöä riittävästi saatavilla. Osaamisen kehittäminen korostuu myös elinkeinoelämän ja tutkimuksen välisessä yhteistyössä. Tiiviillä yhteistyöllä, vaihtamalla tietoja asiakastarpeista ja kehittämällä palvelunkehitystä voidaan luoda merkittävää uutta osaamista jo pelkästään kansallisilla sisämarkkinoilla. Osaamiskysymyksen ja kilpailukyvyn kannalta on tärkeää löytää uusia keinoja, joilla kansalliset yritykset saisivat pidettyä huippuosaajansa kansainvälisen kilpailun kasvaessa. Suomen kilpailukyvyn kannalta olisi myös olennaista, että kansainväliset standardit tukevat tuotteita, joiden valmistuksessa suomalaisilla yrityksillä on vahvuuksia. Vahvalla osallistumisella standardointityöhön voitaisiin parantaa kansallisten yritystemme mahdollisuuksia menestyä kansainvälisessä kilpailussa.

Yhteiskunnan kyberturvallisuuden ja elinkeinoelämän näkökulmasta on keskeistä, kuinka kyberturvallisuus saadaan keskeiseksi osaksi myös muiden kuin kyberturvallisuustuotteita, -palveluita ja ratkaisuja tuottavien yritysten toimintaa. Yhä merkittävämmässä roolissa ovat tulevaisuudessa ne yritykset, joiden varsinainen liiketoiminta on kyberturvallisuusalan ulkopuolella, mutta joiden toimintaan kyberturvallisuus ja siihen liittyvät häiriöt vaikuttavat merkittävästi. Tällaisia aloja on hahmotettu erityisesti verkko- ja tietoturvaa koskevissa lainsäädäntöhankkeissa, joissa tällaisiksi aloiksi katsottiin mm. tietoliikenne, energian tuotanto/jakelu, finanssi- ja vakuutusala ja terveydenhuolto.

Kyberturvallisuuden kehittäminen asettaa julkiselle vallalle osaamisvaatimuksia ja yhteistyövelvoitteita. Kriittisistä toiminnoista vastaavien viranomaisten kyberturvallisuuden ohjaus-, tuki- ja valvontavastuita sekä näiden edellyttämiä resursseja ja keinovalikoimaa parannetaan kaikilla hallinnonaloilla ja hallinnon tasoilla. Yhteistyötä tietoturvallisuuden yritysten kanssa tiivistetään.

Kyberosaamista parannetaan:

* Vahvistamalla ammattikorkeakoulujen ja yliopistojen kyber- ja tietoturvallisuuteen, ohjelmisto- ja sovelluskehitykseen sekä tietoverkkoihin ja tietoliikenteeseen liittyviä koulutusohjelmia
* Vahvistamalla kansallista kyberturvallisuuden tutkimus-, kehitys- ja testaustoimintaa
* Kehittämällä valtakunnallista digiturvallisuuden koulutus- ja harjoitusjärjestelmää osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Sillä kehitetään julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista
* Varmistamalla kansallisesti kriittisten kyberosaamisalueiden edellyttämä korkeatasoinen koulutus. Tätä tuetaan sekä kansallisella että kansainvälisellä koulutuksella ja harjoitustoiminnalla
* Kehittämällä edelleen Kyberturvallisuuskeskuksen yhteistyötä viranomaisten ja elinkeinoelämän välillä. Tämä edistää Suomen kykyä tunnistaa tietoturvauhkia ja varoittaa niistä sekä parantaa edelleen elinkeinoelämän mahdollisuuksia varautua tietoturvauhkiin
* Lisäämällä julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta uusien palveluiden ja tuotteiden tietoturvasta. Kyberturvallisuus on datatalouden ja tekoälyyn perustuvien sovellusten ehdoton edellytys. Tämä edellyttää valmistajien ja palveluntarjoajien luottamusta toisiinsa sekä kansalaisten luottamusta heille tarjottuihin palveluihin ja tuotteisiin.
1. ***Kyberturvallisuudella*** *ymmärretään tilaa, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta on turvattu (TSK 51).* **Kybertoimintaympäristö** puolestaan voidaan käsittää samana, kuin digitaalinen toimintaympäristö, joka kehittyy yhteiskunnan osana ja palveluina nopeasti. [↑](#footnote-ref-1)
2. Tärkeimpinä VTT:n selvitys kyberosaamisesta Suomessa (2016), jossa on 12 toimenpidettä Suomen kyberturvallisuusosaamisen edelleen kehittämiseksi ja vahvistamiseksi. Jyväskylän ja Aalto-yliopistojen selvitys Suomen kyberturvallisuuden nykytilasta (2017), jossa on nostettu esille Suomen kyberturvallisuuden nykytilassa tunnistettuja puutteita ja kehityskohteita luokiteltuna 12 osa-alueeseen. Näiden lisäksi Valtiontalouden tarkastusvirasto on julkaissut tarkastuskertomuksen kybersuojauksen järjestämisestä Suomessa (2017), jossa on viisi kannanottoa sekä neljä suositusta kokonaisuuden kehittämiseksi. Oikeusministeriön raportissa Nettiäänestyksen edellytykset Suomessa (2017) selvitettiin nettiäänestyksen toteuttamisesta. Työryhmä ei suositellut nettiäänestyksen käyttöönottoa, koska tällä hetkellä riskit ovat suuremmat kuin hyödyt. Jyväskylä ja Aalto-yliopistot laativat selvityksen kyberturvallisuuden strategisesta johtamisesta Suomessa (2018), jossa laadittiin toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, kybertoimintaympäristön laajojen häiriötilanteiden hallintaan sekä kyberturvallisuuden tilan mittaamiseen. [↑](#footnote-ref-2)
3. Vuonna 2013 annettua EU:n kyberturvallisuusstrategiaa on päivitetty komission tiedonannoin, viimeisimpänä 2017 syksyllä annetussa tiedonannossa Resilienssi, pelote ja puolustus, vahvan kyberturvallisuuden rakentaminen EU:lle. [↑](#footnote-ref-3)