Kyberpuolustuksen kehittämisen strategiset linjaukset

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

SISÄLLYS

Julkaisija: Puolustusministeriö, 2019

Lisätietoja: Harri Mäntylä, harri.mantyla@defmin.fi

ISBN: 978-951-663-068-0 nid.
ISBN: 978-951-663-069-7 pdf.

Graafinen suunnittelu: Sanna Pyykkö, Sopiva Design
Kuvat: iStock

KYBERPUOLUSTUKSEN KEHITTÄMISEN STRATEGISET LINJAUKSET

1. Johdanto

Kybertoimintaympäristön merkitys turvallisuus- ja puolustuspolitiikassa kasvaa. Kyberkeinojen käyttöä poliittisten päämäärien saavuttamiseksi ei voida sulkea pois. Yhteiskunnan digitalisaatio, teknisten järjestelmien riippuvaisuus rajat ylittävistä tietoverkoista sekä järjestelmien keskinäiset riippuvuussuhteet ja haavoittuvuudet altistavat yhteiskunnan elintärkeät toiminnot kybervaikuttamiselle. Kyber- ja informaatiovaikuttamista on kohdistettu lähialueillemme ja myös Suomeen muun muassa kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan.

Kybertoimintaympäristön aiheuttamiin uhkiin vastaamiseksi ja kybertoimintaympäristön tarjoamien mahdollisuuksien hyödyntämiseksi on merkityksellistä, että puolustushallinnossa on määritetty strateginen tavoitetila. Tämän tilan saavuttamiseksi asetetaan selkeät strategiset linjaukset kyberpuolustuksen kehittämiselle sekä kyberpuolustuksen kannalta kriittisen kansallisen osaamisen, teknologian ja tutkimuksen kehittämiselle.

Puolustusministeriön asettama työryhmä on laatinut kyberpuolustuksen strategiset linjaukset suorituskyvyn rakentamisen tueksi. Linjaukset käsittävät seuraavat osa-alueet: osaaminen, teknologia, yritystoiminta, tutkimus, kansainvälinen yhteistoiminta ja kyberpuolustus osana kansallista kyberturvallisuutta.

2. Kyberpuolustuksen strateginen ohjaus

Kyberpuolustuksen strategista kehittämistä puolustushallinnossa ohjaa Suomen kyberturvallisuusstrategia (2013) ja sen toimeenpano-ohjelma (2017 – 2020) sekä Valtioneuvoston puolustusselonteko (2017). Suomen kyberturvallisuusstrategian päivitystyö on käynnistetty Turvallisuuskomitean päätöksellä keväällä 2018. Kyberpuolustuksen kehittämisen strategiset linjaukset huomioidaan soveltuvin osin strategian päivitystyössä.

Kyberpuolustus on yksi kansallisen kyberturvallisuuden määritetyistä osa-alueista. Suomen kyberturvallisuusstrategia edellyttää, että Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä.

Puolustusselonteossa kyberpuolustus määritetään yhdeksi puolustusjärjestelmän kehittämisen ja ylläpidon painopistealueeksi. Selonteon mukaan Puolustusvoimat rakentaa kyvyn kybertilannekuvan muodostamiseen, kyberoperaatioiden suunnitteluun ja toimeenpanoon sekä omien järjestelmien suojaamiseen ja valvontaan kybertoimintaympäristössä. Puolustusvoimien kybersuorituskyvyn kehittäminen edellyttää saumatonta yhteistyötä kansallisten ja kansainvälisten yhteistyötahojen kanssa.

Tietoverkkotiedustelun suorituskykyä rakennetaan ja käytetään 1.6.2019 voimaan tulleessa tiedustelulainsäädännössä säädetyllä tavalla. Uusi tiedustelulainsäädäntö mahdollistaa kyberpuolustuksen kokonaisuutta vahvistavien tiedustelusuorituskykyjen kehittämisen.

3. Strategiset linjaukset

3.1 Osaaminen

Kyberpuolustuksen suorituskyvyn merkittävä tekijä on riittävän korkeatasoinen kansallinen osaaminen. Keskeisimmiksi kyberpuolustuksen osaamisalueiksi on tällä hetkellä tunnistettu mm. tietoturvallisuus, havainnointi, kyberforensiikka ja haittaohjelma-analyysi, tiedonsiirtotekniikka, ohjelmistokehitys, suurten tietomäärien käsittely, kryptologia, tekoäly ja kvanttilaskenta. Osaamisalueiden kehittymistä, uusien osaamisalueiden merkityksen kasvamista ja mahdollisten osaamisvajeiden kehittymistä seurataan jatkuvasti.

Puolustusvoimien henkilökunnan, varusmiesten ja reserviläisten kyberpuolustukseen liittyvää osaamista kehitetään ja hyödynnetään suunnitelmallisesti. Kyberosaamista kehitetään sekä kansallisilla että kansainvälisillä koulutuksilla ja harjoituksilla. Näitä järjestetään yhteistyössä muiden viranomaisten, oppilaitosten ja yritysten kanssa.

Puolustusvoimien kyberhenkilöstön osalta selvitetään ja kehitetään keinoja korkeatasoisten kyberasiantuntijoiden saatavuuden ja pysyvyyden varmistamiseksi.

Kyberuhkiin varautuminen ja niiden torjuminen edellyttävät yhteiskunnan kaikilta osapuolilta entistä nopeampaa, läpinäkyvämpää ja paremmin koordinoitua toimintaa, sekä erikseen että yhdessä. Yhteistoimintaa kehitetään muiden viranomaisten ja yritysten osaamisen hyödyntämiseksi myös kyberpuolustuksessa kyberturvallisuusstrategian osoittamalla tavalla.

Yhteistyötä oppilaitosten kanssa kehitetään edelleen. Oppilaitosten koulutusohjelmien ja kurssien kehittämistä pyritään tukemaan siten, että ne palvelevat kyberpuolustuksen täydennyskoulutuksen tarpeita, parantavat kyberpuolustuksen rekrytointipohjaa ja edistävät kyberpuolustuksen osaamisalueiden kehityksen seuraamista. Alueellisten osaamiskeskittymien muodostumista edistetään.

TIETOTURVALLISUUS HAVAINNOINTI
KYBERFORENSIIKKA JA HAITTAOHJELMA-ANALYYSI
TIEDONSIIRTOTEKNIIKKA OHJELMISTOKEHITYS
SUURTEN TIETOMÄÄRIEN KÄSITTELY KRYPTOLOGIA
TEKOÄLY KVANTTILASKENTA

3.2 Teknologia

Teknologiaan liittyvien linjausten tavoitteena on varmistaa, että puolustusvoimat saa käyttöönsä mahdollisimman edistynyttä kyberpuolustuksen teknologiaa. Hankinnat pyritään suuntaamaan suomalaisille yrityksille ja muille toimijoille huoltovarmuuden ja operaatioturvallisuuden varmistamiseksi. Mikäli teknologiaa ei ole saatavissa suomalaisilta toimijoilta, se hankitaan ulkomailta. Rahoitus- ja hankintaprosesseja kehitetään ketteryyden varmistamiseksi kyberpuolustuksen alalla.

Puolustusvoimilla tulee olla kyky kehittää ja ylläpitää puolustusvoimien toiminnan kannalta keskeisimmillä osa-alueilla kriittisimpiä ja korkeinta salattavuutta edellyttäviä teknologisia ratkaisuja itsenäisesti.

Keskeisimmiksi teknologia-alueiksi on tunnistettu mm. haavoittuvuustutkimus, tunkeutumisen havaitsemis- ja estojärjestelmät, salausteknologia, suuren ja strukturoimattoman tietomäärän käsittely ja tekoälyteknologiat. Tällä hetkellä tunnistettujen alueiden lisäksi uuden teknologian kehityksen vaikutuksia kyberpuolustussuorituskyvylle arvioidaan jatkuvasti. Teknologista kehitystä seurataan suorituskyvyn kehittämisen ja ylläpidon kannalta ketterästi ja ennakoivasti.

Kyberpuolustuksen teknologiat sisältyvät valtioneuvoston periaatepäätöksessä (VnP 7.4.2016)[1] tunnistettuihin kriittisiin teknologia-alueisiin. Epäsuora teollinen yhteistyö pyritään kohdistamaan näille alueille, joita on edelleen tarkennettu strategisten hankkeiden epäsuoran teollisen yhteistyön painopistemäärittelyssä. Epäsuoran teollisen yhteistyön avulla voidaan hankkia kyberpuolustuksen kehittämisessä tarvittavaa teknologiaa ja osaamista ulkomaisilta toimijoilta.

Kansallinen kyky toteuttaa riittävän korkeatasoisia salausratkaisuja on tunnistettu keskeisimmäksi puutteeksi nykytilassa. Puutteen korjaamiseksi puolustushallinto edistää kansallisen kryptologiastrategian laatimista ja kansallisen salausratkaisun kehittämistä.

Keskeisimmiksi teknologia-alueiksi on tunnistettu mm.
HAAVOITTUVUUSTUTKIMUS, TUNKEUTUMISEN HAVAITSEMIS- JA ESTOJÄRJESTELMÄT, SALAUSTEKNOLOGIA, SUUREN JA STRUKTUROIMATTOMAN TIETOMÄÄRÄN KÄSITTELY JA TEKOÄLYTEKNOLOGIAT.

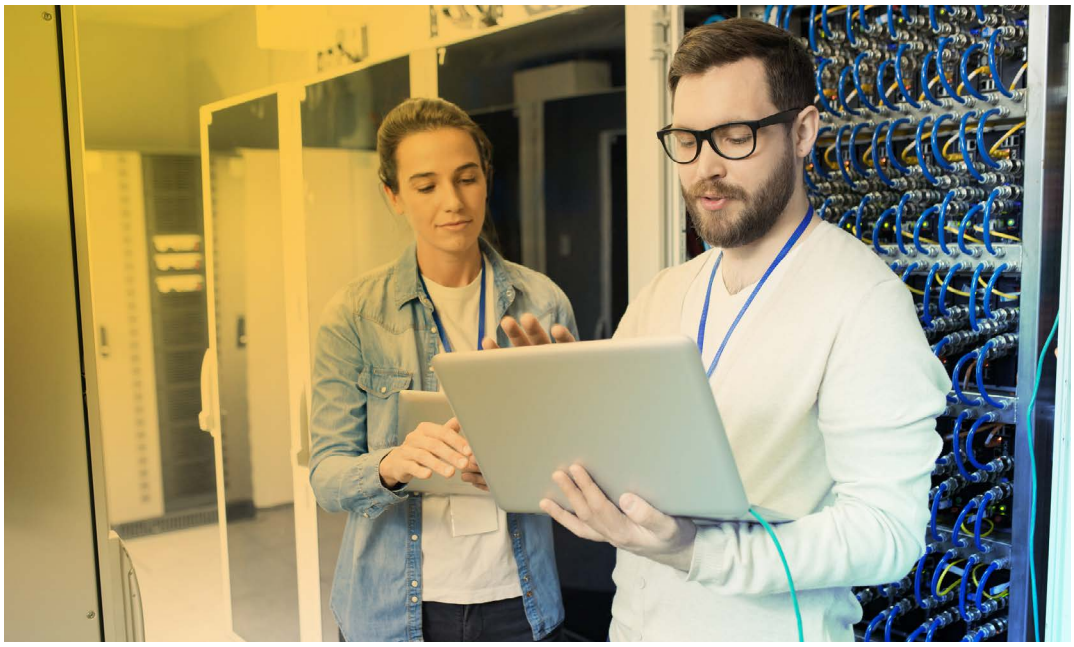
1 Valtioneuvoston periaatepäätös Suomen puolustuksen teknologisen ja teollisen perustan turvaamisesta (v. 2016)

3.3 Yritystoiminta

Suomessa on suhteellisesti katsottuna melko laaja kyberturvallisuuteen liittyvä yrityskenttä, ja alalla on vahvoja ja innovatiivisia yrityksiä. Yritykset ovat suurelta osin kooltaan pieniä ja merkittävä osa niistä on palveluyrityksiä. Alan yritykset panostavat tuotekehitykseen, mutta pitkäjänteiseen tutkimustoimintaan panostaminen on vähäistä. Yritysten absoluuttiset T&K-panostukset eivät ole kovin suuria johtuen yritysten pienestä koosta. Suomalaisten yritysten kapeiden erityisosaamisalueiden, jotka ovat keskeisiä kyberpuolustussuorituskyvyn kannalta, säilymistä Suomessa pyritään edistämään pitkäjänteisellä yhteistyöllä. Yritysten omistuspohjan muutoksiin, pysyvyyteen sekä jatkuvuuden hallintaan liittyvät riskit huomioidaan sopimuksissa ja yhteistyön syvyydessä.

Yritysten tarjoaman potentiaalin hyödyntämiseksi laajennetaan ja syvennetään yhteistyötä yritysten kanssa ja muodostetaan kumppanuuksia. Kumppanuudet edistävät toimintaympäristön muutoksen seuraamisessa tarvittavaa hankintojen ketteryyttä. Yrityksille ulkoistetaan kyberpuolustuksen tukipalveluiden tuottaminen silloin kun se on tarkoituksenmukaista. Lisäksi tarkastellaan tarvetta ja mahdollisuutta muodostaa strateginen kumppanuus kyberpuolustuksen alalle.

Kehittyvä ja syvenevä yhteistyö yritysten kanssa voi johtaa tilanteeseen, jossa yrityksellä on merkittävä vastuu Puolustusvoimien ydintoiminnoista kyberpuolustuksessa tai jossa yrityksellä on merkittävä asema poikkeusolojen tilanteissa. Tästä syystä yhteistoiminnassa yritysten kanssa huomioidaan jatkuvuus-, varautumis-, valmius- ja salassapitovaatimukset sopimuksissa ja toimintamallien suunnittelussa.



3.4 Tutkimus

Kyberpuolustuksen suorituskykyjen kehittäminen ja ylläpito edellyttävät puolustusvoimien omaa tutkimus- ja kehittämiskykyä sekä yhteistoimintaa tutkimus- ja tiedeyhteisön kanssa. Tutkimuksella tulee tunnistaa ja ennakoida kybertoimintaympäristön kehityskulkuja, jotta kyberpuolustuksen suorituskykyjä voidaan kehittää ennakoivasti kehittyvää teknologiaa ja toimintaympäristöä vastaaviksi. Tutkimuksella edistetään myös kotimaisen kyberosaamisen pitkäjänteistä kehittämistä ja osaamisen huoltovarmuutta.

Kyberpuolustuksen tutkimustiedon tarpeet huomioidaan Puolustusvoimien omassa sotatieteellisessä sekä teknologisessa tutkimustoiminnassa. Puolustushallinto osallistuu kansallisten ja kansainvälisten tutkimusverkostojen toimintaan. Puolustushallinto edistää suomalaisten tutkimuslaitosten ja yritysten osallistumista puolustusalan kybertutkimushankkeisiin.

Puolustusvoimien ulkopuolista kybertutkimusta rahoitetaan olemassa olevien rahoitusmekanismien, esimerkiksi MATINE:n ja Puolustusvoimien tutkimusohjelmien kautta. Tarvittaessa rahoitetaan erillisiä tutkimushankkeita kybertutkimuksen ketteryyden varmistamiseksi. Puolustushallinto pyrkii vaikuttamaan kansalliseen tiede-, teknologia- ja innovaatiopolitiikkaan kyberpuolustuksen kannalta tärkeän tutkimuksen edistämiseksi.

3.5 Kansainvälinen yhteistoiminta

Kybertoimintaympäristö ja kyberuhkat ovat luonteeltaan valtioiden rajat ylittäviä. Tästä syystä kansainvälinen yhteistoiminta on keskeistä kyberpuolustuksen suorituskyvyn kehittämisessä ja käyttämisessä. Osa kyberpuolustuksen suorituskyvyistä on saatavilla vain kansainvälisen yhteistyön kautta. Kahden- ja monenvälistä kansainvälistä yhteistoimintaa kehitetään erityisesti alueilla, jotka edistävät Suomen kyberpuolustuksen suorituskyvyn kehittämistä. Ensisijaisesti syvennetään olemassa olevia ja parhaiten kyberpuolustuksen suorituskyvyn kehittämistä tukevia yhteistoimintasuhteita.

Suomi jatkaa osallistumista kansainväliseen koulutus- ja harjoitustoimintaan sekä muuhun kansainväliseen toimintaan puolustusselonteon linjausten mukaisesti. Koulutus- ja harjoitustoimintaan osallistumisen painopisteenä ovat vaativat kansainväliset, kyberpuolustustoimintoja kehittävät, harjoitukset. Kansainvälisten kumppaneiden kutsumista kansallisiin harjoituksiin jatketaan, ja niitä voidaan yhdistää osaksi kumppaneiden harjoituksia.

Kahdenvälinen puolustusyhteistyö on Suomen kyberpuolustuskyvyn kehittämisessä keskeinen yhteistyömuoto. Yhteistyötä tehdään valikoitujen valtioiden kanssa resurssien mahdollistamalla tavalla. Puolustusyhteistyöhön voi kuulua mm. tiedonvaihto, suorituskykyjen ja valmiuden sekä yhteistoimintakyvyn vahvistaminen, harjoitustoiminta sekä materiaali- ja tutkimusyhteistyö mukaan lukien yhteiset hankinnat. Kahdenvälistä yhteistyötä tukemaan laaditaan kahdenvälisiä puitejärjestelyjä, jotka helpottavat puolustusyhteistyön ohjausta ja tekevät siitä suunnitelmallisempaa.

Myös monenvälisessä kyberpuolustusyhteistyössä esimerkiksi EU:n puitteissa ja Naton kanssa pyritään löytämään suorituskyvyn rakentamista tukevia yhteistyömuotoja. Monenväliseen yhteistyöhön osallistuminen priorisoidaan samaan tapaan kuin kahdenvälinen yhteistyö saatavan hyödyn perusteella.

3.6 Kyberpuolustus osana kansallista kyberturvallisuutta

Kyberpuolustuksen strategiset linjaukset antavat perusteita puolustushallinnon kyberpuolustuksen tavoitetilan saavuttamiseksi ja puolustusvoimien kyberpuolustuskyvyn kehittämiseksi. Strategiset linjaukset korostavat yhteistyötä eri tahojen kanssa kyberpuolustuksessa ja kyberturvallisuudessa. Kehittyvästä yhteistyöstä saadaan hyötyä kyberturvallisuuden kokonaisuudelle sekä kaikille osapuolille erikseen.

Puolustusvoimiin rakennettava kyberpuolustuskyky tukee Suomen kyberturvallisuutta. Puolustusvoimiin muodostuu kykyjä kuten edistyneen kyberuhkan havainnointikyky, kyky hyökkäyksellisen kyberoperaation toteuttajan tunnistamiseen ja vastatoimiin, joihin liittyy myös vaikuttaminen. Osa kyvyistä on sellaisia, joita ei ole mahdollista eikä tarkoituksenmukaista rakentaa muualle valtionhallintoon. Puolustusvoimat on keskeinen toimija kyberturvallisuuden viranomaisverkostossa.

Puolustushallinto tukee Suomen kyberturvallisuuden kehitystyötä, kuten kansallisen kyberstrategian päivitystyötä tai kyberturvallisuuden strategisen johtamisen ratkaisujen määrittämistä. Kansallisissa ratkaisuissa tulee hyödyntää Puolustusvoimien osaaminen, suorituskyvyt ja tilannekuva kyberturvallisuuden johtamisessa.

4. Strategiset linjaukset

Linjaus 1: Kyberpuolustuksen kriittiseksi tunnistettu osaaminen puolustushallinnossa turvataan rekrytoinneilla ja henkilöstön koulutuksella. Kansallista kyberpuolustuksessa tarvittavaa osaamispohjaa kehitetään yhteistyössä oppilaitosten, yritysten ja muiden viranomaisten kanssa. Kyberpuolustuksen kriittisten osaamisvaatimusten kehitystä seurataan ennakoivasti.

Linjaus 2: Kybersuorituskykyjä ja niihin liittyviä kriittisiä teknologia-alueita koskeva osaaminen ja kehittämiskyky turvataan Suomessa valtioneuvoston periaatepäätöksen (VnP 7.4.2016) linjausten mukaisesti.

Linjaus 3: Yhteistyötä ja kumppanuuksia yritysten kanssa syvennetään osaamisen ja teknologian saamiseksi kyberpuolustuksen rakentamisen tueksi. Sopimuksilla ja yhteistyön syvyydellä mahdollistetaan nopean teknologisen kehityksen mukaiset hankinnat ja hallitaan yritysyhteistyön riskejä.

Linjaus 4: Puolustushallinnon, yhteistyökumppaneiden ja tutkimusverkostojen tutkimustoimintaa suunnataan kyberpuolustuksen teknologiaennakoinnin kehittämiseksi. Tutkimuksella edistetään kotimaisen kyberosaamisen pitkäjänteistä kehittämistä ja osaamisen huoltovarmuutta.

Linjaus 5: Kansainvälistä yhteistoimintaa kehitetään ja priorisoidaan Suomen kyberpuolustuksen suorituskyvyn kehittämiselle saatavan hyödyn perusteella.

Linjaus 6: Puolustushallinto tukee kansallista kyberturvallisuustyötä puolustushallinnon kyberpuolustuksen suorituskyvyn hyödyntämiseksi osana kansallista kyberturvallisuutta sekä kansallisten ratkaisumallien selkeyttämiseksi.

Puolustusministeriö
Eteläinen Makasiinikatu 8
PL 31, 00131 Helsinki

Puhelin: vaihde (09) 16001