Mikko Soikkeli

LAINSÄÄDÄNTÖ TIETO- JA KYBERTURVALLISUUDEN PERUSTANA – VALTIONHALLINNON VIRANOMAISEN NÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Soikkeli, Mikko
Lainsäädäntö tieto- ja kyberturvallisuuden perustana – valtionhallinnon viranomaisen näkökulma
Jyväskylä: Jyväskylän yliopisto, 2021, 74 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Työn tavoitteena oli selvittää, miten kansallinen lainsäädäntö velvoittaa ja ohjaa valtionhallinnon viranomaisia tieto- ja kyberturvallisuuden osalta. Alaongelmana vastattiin kysymykseen "Mitä eroa tieto- ja kyberturvallisuudella on lainsäädännössä? Tutkimuksen erityisenä mielenkiinnon kohteena oli viranomaisten toimivaltaa ja yhteistoimintaa koskeva sääntely.

Tutkimus toteutettiin grounded teoria -menetelmällä ja tutkimusaineiston muodostivat tieto- ja kyberturvallisuuteen liittyvät lait, asetukset, hallituksen esitykset sekä relevantit valtioneuvoston periaatepäätökset.

Tulosten perusteella lainsäädäntö on kaiken viranomaisen toiminnan perusta. Viranomaisen tieto- ja kyberturvallisuus muodostuu strategisesta ohjauksesta, operatiivisesta kyberturvallisuustoiminnasta ja päivittäisistä tietoturvallisuustoimenpiteistä. Kyberturvallisuus eroaa tietoturvallisuudesta siten, että sitä ei käsitteenä esiinny lainsäädännössä, mutta turvallisuusviranomaiset toteuttavat kuitenkin toimenpiteitä, joilla pyritään varmistamaan yhteiskunnan elintärkeiden toimintojen turvaaminen. Kyberturvallisuus edustaa uusiin teknologioihin liittyvää poikkihallinnollista haastetta, joka ilmenee mm. hallinnonaloille jakautuneina vastuina eikä viranomaisten yhteistyölle ole selkeää lakipohjaa.

Hallinnon julkisuusperiaate asettaa viranomaisen tietoturvallisuudelle vaatimuksen julkisuusnäkökulmasta käytettävyydelle ja salassa pidon osalta luottamuksellisuudelle ja eheydelle. Tutkimuksen perusteella tietoturvallisuuden perustan muodostavia yhtenäisiä vaatimuksia ei ole säädetty ja viranomaisten tietoteknisten ratkaisujen arvioinnin säätely ei edellytä viranomaiselta kansallisen tiedon osalta tietojärjestelmien arviointia. Valtion yhteisten tieto- ja viestintäteknisten palvelujenkaan osalta ei ole asetettu selkeitä vaatimuksia, mikä osaltaan jättää palveluntuottajille merkittävän vastuun.

Asiasanat: tietoturvallisuus, kyberturvallisuus, tietoturvallisuuden hallinta, kyberturvallisuuden hallinta, kokonaisturvallisuus, lainsäädäntö

ABSTRACT

Soikkeli, Mikko
Legal basis for information and cyber security – government authority's viewpoint
Jyväskylä: University of Jyväskylä, 2021, 74 pp.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

The goal of this thesis was to find out, how national legislation obligates and guides government authorities in information and cyber security. A sub question was "What is the difference between information and cyber security by legislation?" Special attention was given to legislation of jurisdiction and cooperation between different authorities.

The study was executed according to grounded theory. The research material comprised acts on information and cyber security, government decrees, government proposals and relevant government resolutions.

All activities of the public authorities are based on legislation. Authorities' information and cyber security comprises strategic guidance, operational cyber security activities and daily information security measures. Cyber security is not included in legislation as a concept, but still, security authorities execute actions to maintain the vital functions of the society. Cyber security represents emerging technology, which creates a cross governmental challenge by dived responsibilities. Furthermore, legislation gives not enough clear jurisdiction for the cooperation between different authorities.

Principle of public access sets requirements for the information security of the authorities. Public access is related to the availability of the information and on the other hand, secrecy is related to confidentiality and integrity of the information. Based on the results, there are no common criteria for information security requirements by the legislation. No act obligates audit of the information systems containing only national information. There are also no clear information security requirements for government's common ICT-services, which gives the service provider a remarkable responsibility.

Keywords: information security, cyber security, information security management, cyber security management, comprehensive security, legislation

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Lokakuussa 2020 Suomessa levisi julkisuuteen tieto psykoterapiapalvelun laajasta tietovuodosta, tai ehkä oikeammin tietomurrosta – niin sanotusta Vastaamo-tapauksesta. Yli neljänkymmenentuhannen yrityksen potilaana olleen henkilön tiedot joutuivat rikollisen käsiin. Asian selvittelyn yhteydessä paljastui, että tiedot olivat päätyneet vääriin käsiin jo toista vuotta aikaisemmin. Esiin nousi myös se, että yrityksen tietojärjestelmä vastasi muodollisesti lain vaatimuksia, mutta lain vaatimukset tietoturvallisuuden osalta olivat varsin kevyet. Tapahtuma käynnisti nopeasti pääministerin toimeksiannosta poikkihallinnollisen työskentelyn, jolla tavoiteltiin konkreettisia korjaavia toimenpiteitä (Liikenne- ja viestintäministeriö, 2020).

Keskusrikospoliisi kertoi joulukuussa 2020 (Yle-uutiset, 2020) eduskuntaan aikaisemmin samana vuonna kohdistuneen tietomurron liittyvän todennäköisesti vakoiluun. Yle-uutisten (2021) mukaan Suojelupoliisi kertoi maaliskuussa 2021 tietomurron olleen kybervakoilua, joka oli peräisin Kiinasta. Suojelupoliisin mukaan kyseessä oli APT31-ryhmittymän suorittama kybervakoilu.

Helsingin Sanomat (2020) uutisoi samoin joulukuussa Solarwinds-yritykseen kohdistuneesta hyökkäyksestä, jossa yrityksen toimittaman ohjelmiston kautta vakoiltiin USA:n viranomaisia ja tuhansia isoja yrityksiä. Vakoilun takana epäiltiin olevan Venäjä.

Ilta-Sanomat uutisoi puolestaan huhtikuussa 2021 (Iltasanomat, 2021) viranomaisen olevan vaitelias valtion virastoihin kohdistuneesta tietomurrosta, jossa hyödynnettiin laajasti käytössä olleen etäyhteysohjelman haavoittuvuutta. Haavoittuvuutta oli muualla hyväksikäytetty Kiinasta. Uutisen perusteella Valtori kertoi kyseessä olevan epäilyn, mutta asiaa selvitettävän yhdessä Kyberturvallisuuskeskuksen ja Keskusrikospoliisin kanssa. Asiasta oli ilmoitettu myös Suojelupoliisille ja tietosuojavaltuutetulle.

Ajallisesti työ kiinnittyy Suomessa poikkeuksellisen ajankohtaan, jolloin maailmanlaajuinen pandemia johti ensimmäistä kertaa toisen maailmansodan jälkeen valmiuslain käyttöönottoasetuksella poikkeusolojen julistamiseen Suomeen – kahteen kertaan. Pandemia lisäsi maailmanlaajuisesti kyberrikollisuutta ja -vakoilua. Sähköisten järjestelmien käyttö lisääntyi ennenkokemattoman rajusti ihmisten siirtyessä massamaisesti etätyöskentelyyn.

1.1 Tutkimuksen tausta ja tavoitteet

Suomessa on käyty viimeisen kahdenkymmenen vuoden aikana keskustelua tieto- ja kyberturvallisuuden tilasta sekä niihin liittyvästä johtamisesta valtiotasolla. Toistuvasti esiin on noussut kysymys siitä, kuka johtaa kyberturvallisuutta niin strategisesti, kuin operatiivisestikin. Vastaus on aina sama. Kyberturvallisuuden hallinta perustuu kokonaisturvallisuuden malliin ja viranomaisten yhteistyöhön kulloisessakin tilanteessa toimivaltaisen viranomaisen johdolla. Kukin hallinnonala vastaa oman toimintansa johtamisesta ja ohjeista.

Myös tietoturvallisuus ja eri toimijoiden kyvykkyys sen hallinnassa on aika ajoin noussut julkisuuteen. Valtion keskeinen palveluntuottaja Valtori on joutunut selittämään julkisuudessa epäonnistumisiaan useamman kerran. Molempia aiheita on selvitetty useampaan kertaan ja erilaisia raportteja ja suosituksia ovat kirjoittaneet niin tutkijat kuin tuloksellisuuden tarkastajatkin. Kaikissa selvityksissä on ollut yhtenäisenä huomiona se, että toiminta perustuu lainsäädäntöön, joka on periaatteessa kunnossa, mutta jokin ei toimi.

Vuoden 2020 aikana käynnistettiin valtiovarainministeriön johtamana digitaalisen turvallisuuden toimeenpano-ohjelma (Valtiovarainministeriö, 2021) ja samaan aikaan liikenne- ja viestintäministeriön johdolla käynnistettiin kyberturvallisuuden kehittämisohjelman laatiminen (Liikenne- ja viestintäministeriö, 2021). Alussa mainitun Vastaamo-tapauksen perusteella käynnistettiin niin ikään liikenne- ja viestintäministeriön johdolla selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Liikenne- ja viestintäministeriö, 2020). Kaikissa näissä yhtenä tarkasteltavana osa-alueena on lainsäädännön kehittämistarve.

Lainsäädännön merkitystä tieto- ja kyberturvallisuudelle on tutkittu eri näkökulmista. Johnson, Lincke, Imhof ja Lim (2014) päätyivät kansainvälisessä vertailussaan siihen, että osa maista painottaa tietoa ja osa turvallisuutta. Kehittyvien teknologioiden sääntelyyn liittyviä haasteita on tarkasteltu lainsäätäjän ja eri hallinnonalojen näkökulmasta (Lewallen, 2020). Taloustutkimuksessa mm. Moore (2010) on tutkinut ennakoivaa ja toisaalta sanktioivaa lainsäädäntöä. Hiller ja Russel (2013) toteavat myös yksityisten yritysten kyberturvallisuudella olevan vaikutusta kansalliselle turvallisuudelle. Von Solm ja van Russow (2013) ovat määritelleet kyberturvallisuuden käsitettä ja sen eroja tietoturvallisuuteen.

Voutilainen (2006) tutki työssään hyvää tietohallintoa ja sen sääntelyä viranomaistoiminnassa. Voutilaisen (2006 s. 19) mukaan viranomaisen huolehtimisvelvollisuutta tietoturvallisuudesta voidaan pitää sähköisen viranomaistoiminnan keskeisenä vaatimuksena ja perusedellytyksenä.

Valtioneuvosto julkaisi vuonna 2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä, millä korvattiin edellinen vastaava, jo vuonna 1999 julkaistu periaatepäätös (Valtiovarainministeriö, 2009). Periaatepäätöksen mukaisesti jokaisen viranomaisen tulee huolehtia siitä, että riittävän hyvä tietoturvallisuus toteutuu omassa organisaatiossa ja yhteistyössä sidosryhmien kanssa sekä hankittaessa ulkopuolisia palveluita. Riittävä

tietoturvallisuuden ja varautumisen taso tulee määritellä ottaen huomioon säädökset ja organisaation oman toiminnan sekä tietosisältöjen erityispiirteet (Valtiovarainministeriö, 2009).

Valtiontalouden tarkastusvirasto on toteuttanut useita tarkastuksia ja julkaisi mm. syksyllä 2017 tarkastuskertomuksensa ”Kybersuojauksen järjestäminen” (Valtiontalouden tarkastusvirasto, 2017). Kertomuksen perusteella valtionhallinnon kybersuojauskykyä oli pyritty kehittämään suunnitelmallisesti, mutta toteutuksessa oli silti puutteita. Yhtenä tekijänä oli Valtorin perustaminen ja palveluiden keskittäminen.

Osana valtioneuvoston selvitys- ja tutkimustoimintaa laadittiin kaksi selvitystä. Ensimmäisen selvityksen (Lehto, Limnéll, Innola, Pöyhönen, Rusi, ja Salmela, 2017) mukaan tietoturvallisuutta on säädelty jo pitkään, joten perusasiat ja toimintatavat ovat kunnossa, lainsäädännössä ei koeta olevan puutteita eikä lainsäädäntöä pidetä esteenä viranomaisten yhteistoiminnalle. Lainsäädännön kehittäminen pelkästään kyberturvallisuuden näkökulmasta koetaan hankalana ilmiön poikkileikkaavuuden takia (Lehto ym., 2017). Toisen selvityksen laativat lähes samat tutkijat (Lehto, M., Limnéll, J., Kokkomäki, Pöyhönen ja Salminen, 2018). Tutkimuksen perusteella kyberturvallisuuden strategisessa johtamisessa on perusongelmana valtioneuvoston tasalla ministeriöiden itsenäiseen toimintaan omilla sektoreillaan, jolloin kokonaisvaltainen strateginen johtajuus puuttuu (Lehto ym., 2018).

Oikeusministeriön selvityksen (Luoma, 2019) perusteella viranomaisten mahdollisuudet puuttua tietoliikenteen tai tietojärjestelmien häiriötilanteisiin vaihtelevat sektorikohtaisesti. Säännökset ovat osin epäselviä tai niitä ei ole lainkaan. Liikenne- ja viestintävirastolla on kyberuhkien osalta laajimmat, mutta silti sektorikohtaiset toimivaltuudet (Luoma, 2019).

Valtioneuvoston kanslian toimeksiantamassa selvityksessä ”Kansallisen turvallisuuden vaikutusten arviointi” (Lonka, Laitinen, Keinänen, Wähä, Huhtinen ja Paasonen, 2020) todettiin kansallisen turvallisuuden määritelmän olevan haastavan ja sitä tulkitaan kovin eri tavoin. Laajasti sisältöön kuuluvaksi koettiin tietoverkkoihin liittyvät uhat. Vaikka selkeää vastuunjakoa ministeriöiden välillä pidetään tärkeänä, lisää se samalla siiloutumista. Tätä lisäävät omalta osaltaan erilaiset hallinnonalakohtaiset selonteot. Poikkihallinnollista yhteistyötä arvostetaan, mutta sitä pidetään haastavana koska kellään ei tunnu olevan kokonaisymmärrystä (Lonka ym., 2020, s. 35).

Tämän tutkimuksen tavoitteena on selvittää, miten kansallinen lainsäädäntö velvoittaa ja ohjaa valtionhallinnon viranomaisia tieto- ja kyberturvallisuuden osalta. Alaongelmana vastataan kysymykseen "Mitä eroa tieto- ja kyberturvallisuudella on lainsäädännössä? Erityinen mielenkiinto liittyy viranomaisten toimivaltaa ja yhteistoimintaa koskevaan sääntelyyn. Tutkimuksessa ei käsitellä EU-lainsäädäntöä, koska se ei ensisijaisuudestaan huolimatta säätele tarkasteltavaa toimintaa kuin pieneltä osin, mutta siihen viitataan. Aiheen laajuudesta johtuen myöskään tietosuojaa ei tarkastella.

1.2 Tärkeimmät käsitteet

Tutkielman käsitteet määritellään aiheen takia lainsäädännön mukaisesti niiltä osin, kuin se on mahdollista. Mikäli käsitteen osalta on lainsäädännössä horjuvuutta, määrittelyä on voitu tarkentaa tutkimusten tai muiden lähteiden avulla.

Tietoturvallisuutta ei ole sananmukaisesti lainsäädännössä määritelty. Laki sähköisen viestinnän palveluista (917/2014) määrittelee tietoturvan, joka Kielitoimiston sanakirjan (2020) mukaisesti tarkoittaa tietoturvallisuutta. Sähköisen viestinnän palveluista annetun lain (2014/917) 3 §:n mukaisesti tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla (luottamuksellisuus), että tietoja eivät voi muuttaa muut kuin siihen oikeutetut (eheys) sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (saatavuus). Vastaavasti julkisen hallinnon tiedonhallinnasta annettu laki (2019/906) määrittelee tietoturvallisuustoimenpiteet tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamiseksi hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Edellä esitetyn perusteella keskeiset tekijät ovat saatavuus, eheys ja luottamuksellisuus.

Kyberturvallisuus tarkoittaa Kyberturvallisuuden sanaston (2018, s. 22) mukaisesti tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa. Kyberturvallisuuden saavuttamisessa tietoturva on keskeisessä asemassa, mutta siihen liittyy laajempana näkemyksenä digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuus sekä tämän vaikutus toimintaan (Kyberturvallisuuden sanasto, s. 22). Kyberpuolustus on kyberturvallisuuden osa-alue, josta vastaa Puolustusvoimat. Se muodostuu tiedustelun, suojaamisen ja vaikuttamisen suorituskyvyistä (Kyberturvallisuuden sanasto, s. 22).

Valtioneuvoston periaatepäätöksen ”Julkisen hallinnon digitaalinen turvallisuus” (Valtiovarainministeriö, 2020) mukaisesti digitaalinen turvallisuus voidaan nähdä kyberturvallisuuden synonyyminä. Tässä työssä digitaalisella turvallisuudella tarkoitetaan kansalaisten, yhteisöjen ja yhteiskunnan suojaamista riskeiltä ja uhkilta, jotka kohdistuvat henkilötietoihin, yhteiskunnan ja viranomaisten toimintaan, prosesseihin, palveluihin ja tietoaineistoihin digitaalisessa toimintaympäristössä (Valtiovarainministeriö, 2020).

Kokonaisturvallisuudella tarkoitetaan tavoitetilaa, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhat ovat hallittavissa. Yhteiskunnan elintärkeitä toimintoja ylläpidetään varautumalla uhkiin, hallinnoimalla häiriötilanteita ja poikkeusoloja sekä toipumalla niistä (Kokonaisturvallisuuden sanasto, 2017.) Kokonaisturvallisuuteen liittyy olennaisesti käsite toimivaltaisesta viranomaisesta. Vaikka varautuminen ja muu toiminta tapahtuu yhdessä, operatiivisista toimenpiteistä vastaa ja toimintaa johtaa kulloinkin kyseessä oleva toimivaltainen viranomainen valtioneuvoston ohjesäännön toimialajaon mukaisesti (HE 261/2016 vp).

Kansallinen turvallisuus määritellään tässä tutkimuksessa perustuslain yksityisyyden suojaa koskevan 10 §:n muuttamisesta annetun hallituksen esityksen

(HE 198/2017 vp) pohjalta. Kansallisella turvallisuudella tarkoitetaan ihmisten kollektiivista turvallisuutta välittömästi tai välillisesti väkivaltaista ulkoista uhkaa vastaan. Uhkaava toiminta ei kohdistu keneenkään yksilönä vaan yleisemmin yhteiskuntaan. Keskeisiä ovat yhteiskunnan perustoiminnot, joiden häirintä tai lamauttaminen saattaisi johtaa ihmisten hengen tai terveyden vakavaan vaarantumiseen. Kyseessä olevat perustoiminnot voivat olla mm. sähkö-, viestintä- ja liikenneverkot tai kansallista huoltovarmuutta ylläpitävät toiminnot. Uhka voi ilmetä avoimen väkivallan lisäksi tietoverkkoihin kohdistuvina hyökkäyksinä tai erilaisten keinojen yhdistelminä (HE 198/2017 vp.)

1.3 Tutkimusmenetelmä ja keskeiset tulokset

Tutkimus toteutettiin laadullisena tutkimuksena, jossa analyysimenetelmänä käytettiin grounded teoriaa. Tutkimuksessa pyrittiin tunnistamaan lainsäädännössä olevat säännönmukaisuudet ja edelleen elementit, joista ne muodostuivat. Tutkimusaineisto muodostui suomalaisesta lainsäädännöstä, joka liittyy valtionhallinnon viranomaisten tieto- ja kyberturvallisuuden hallintaan. Aineisto käsitti lakitekstien lisäksi asetukset sekä molempien osalta pääosin myös lakiesitykset perusteluineen. Tämän lisäksi aineistossa oli mukana myös valtioneuvoston periaatepäätöksiä.

Työn toisessa luvussa perehdytään lainsäädännön yleiseen velvoittavuuteen viranomaisen osalta, tarkastellaan kyberturvallisuuteen liittyviä näkökulmia sekä luodaan katsaus poikkihallinnollisen työskentelyn problematiikkaan. Kolmas luku käsittelee tieto- ja kyberturvallisuuden hallintaa aikaisempiin tutkimuksiin perustuen, tarkastelee tieto- ja kyberturvallisuuden hallintajärjestelmiä valikoitujen standardien pohjalta sekä luo katsauksen palvelukeskuksen vaikutuksiin käyttäjäorganisaatioiden tietoturvalle. Neljäs luku sisältää kuvauksen tutkimuksen toteutuksesta ja viidennessä luvussa esitetään tutkimuksen tulokset, jotka perustuvat mm. 29 eri lain analysointiin. Kuudennessa luvussa tulkitaan tulokset ja arvioidaan niiden merkitystä. Seitsemännessä luvussa esitetään työn yhteenveto.

Työn keskeisinä tuloksina todettiin, että valtionhallinnon osalta tieto- ja kyberturvallisuus muodostuu strategisesta ohjauksesta ja operatiivisesta kyberturvallisuustoiminnasta sekä päivittäisistä tietoturvallisuustoimenpiteistä. Kyberturvallisuuden osalta lainsäädäntö ei ole kehittynyt sillä tavoin, kuin vuoden 2013 kyberturvallisuusstrategiassa linjattiin. Erityisesti viranomaisten yhteistyön edellytyksiä tulisi parantaa lainsäädäntöä kehittämällä. Tietoturvallisuuden osalta valtiovarainministeriö on keskeisessä roolissa ja lainsäädäntöä tulisi kehittää yhteisten tietoturvallisuusvaatimusten, riskienhallinnan sekä tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnin osalta.

2 HALLINTO PERUSTUU LAINSÄÄDÄNTÖÖN

Lainsäädännön perusteella keskeisiä periaatteita viranomaisen toiminnassa ovat julkisuus- ja avoimuus, hyvä hallintotapa, hyvä tiedonhallintatapa sekä toisaalta lainalaisuus ja lakisidonnaisuus. Luvussa tarkastellaan hallinnon perusteita sekä kyberturvallisuuden erityispiirteitä ja poikkihallinnollisuuteen liittyviä haasteita.

2.1 Erityyppiset lait ohjaavat eri tavoin

Johnson ym. (2014) toteavat analyysinsä perusteella, että eri maissa tietoturvallisuuden sääntely painottuu eri tavoin. Jotkut maat (esim. Saksa) painottavat tietoa, kun taas Yhdysvallat painottaa turvallisuutta. Tietoa painottavat maat kuvaavat suojattavan tiedon tyypit ja vaatimuksen suojaamisesta muodollisen standardin mukaisesti. Turvallisuuden painotuksessa tärkeimmiksi sääntelykohteiksi muodostuvat hallinnolliset, tekniset ja fyysiset turvallisuusvaatimukset (Johnson ym., 2014.)

Tutkijat erottelevat myös strategisen ja taktisen tason eri maiden lainsäädännön perusteella (Johnson ym., 2014). Heidän mukaansa Yhdysvaltojen lähestymistapa on taktinen, koska toimivalta sääntelystä on hallinnonaloilla. Vastaavasti saksalaista mallia pidetään strategisena, koska täsmällisiä turvallisuusvaatimuksia ei ole vaan niiden oletetaan tulevan standardeista. Esitetty havainto ei kaikilta osin pidä paikkaansa, koska esim. Yhdysvaltojen presidentin antama ”Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (Whitehouse, 2017) toteaa virastojen tehtäviksi ottaa käyttöön NIST:n kyberturvallisuudenhallintamalli 90 päivän kuluessa määräyksestä.

Suomessa säädöksellä tarkoitetaan tekstikokonaisuutta, joka sisältää oikeusohjeen (Eduskunnan kirjasto, 2020). Säädöksiin kuuluvat mm. lait, tasavallan presidentin ja valtioneuvoston asetukset sekä viranomaisten määräykset. Säädöshierarkia määrittää säädösten keskinäisen suhteen ja periaatteena on, että alemman tasoinen säädös ei voi olla ristiriidassa ylemmän kanssa. Lait voidaan sisällön perusteella jaotella mm. yleis- ja erityislaeiksi (Tieteen termipankki, 2021). Yleislaki antaa tiettyä toimintaa koskevat yleiset säännökset ja lailla on tarkoitus säädellä toimintaa kattavasti (Emt., 2021). Erityislaki puolestaan säätelee erityistä toimintaa ja sillä annetaan yleislakia täsmentäviä, täydentäviä ja siitä poikkeavia säännöksiä (Emt., 2021). Lainkirjoittajan oppaan (Oikeusministeriö, 2021, 12.1) mukaan keskeiset lainalat on säännelty perustuslain mukaisin yleislaein ja lähtökohtaisesti muut lait laaditaan yleislakien mukaisiksi.

Tietoturvallisuutta ja kyberturvallisuutta on eri aikoina pyritty kehittämään myös valtioneuvoston periaatepäätöksillä. Valtioneuvoston periaatepäätöksellä ei ole säädöksen asemaa, vaan kyse on lähinnä poliittisesta tahdonilmauksesta tai kannanotosta (Valtioneuvosto, 2020). Lopulliset päätökset tekee asiaa

käsittelevä toimivaltainen viranomainen, mikä näkyy esimerkiksi siinä, että kyberturvallisuusstrategian suosituksia on noudatettu vain niiltä osin, kuin sitä on pidetty tarkoituksenmukaisena (Valtiontalouden tarkastusvirasto, 2017). Jokainen hallitus päättää toimikautensa alussa, mitkä aikaisempien hallitusten tekemistä periaatepäätöksistä on voimassa kuluvalla hallituskaudella.

Turvallisuussääntely voidaan Mooren (2010) mukaan jakaa ex ante- ja ex post-periaatteisiin. Ex ante -periaate tarkoittaa ennakoivaa sääntelyä, jonka tarkoituksena on ehkäistä turvallisuuspoikkeamia sääntelyä noudattamalla. Periaatteiden liityntä talouteen näkyy siinä, että ex post -sääntelyssä pyritään ehkäisemään turvallisuuspoikkeamia määrittämällä vastuutaholle taloudellinen sanktio mahdollisen poikkeaman tapahtuessa. Mooren (2010) mukaan viranomaista koskeva sääntely on valtaosin ex ante -perusteista, mitä voidaan pitää luontevana, koska taloudelliset sanktiot eivät välttämättä toimi järkevästi. Moore (2010) viittaa toisten tutkijoiden (Shavel, 1984 ja Kolstad, Ulen & Johnsson, 1990) tekemään havaintoon siitä, että toisaalta ex ante -periaate ei toimi tilanteissa, joissa lainsäätäjä on epävarma aiheutuvasta haitasta tai siitä, mikä pitäisi olla minimivaatimus. Myös tiedonantovelvollisuus voi toimia sääntelynä (Moore, 2010, s. 108). Tutkija toteaa asioiden saattamisen julkiseksi aina hyväksi ja toisaalta yhteisöllä voi olla oikeus saada tieto myös kiusallisista asioista (Emt., 2010, s. 108).

2.2 Tietoturvallisuus osana hyvää tiedonhallintatapaa

Perustuslain (Perustuslaki 739/1999) 2§:n mukaisesti ”Julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisen vallan käytössä on tarkoin noudatettava lakia.” Mäenpään (2020., s. 6) mukaan oikeusvaltion vaatimuksiin kuuluu lisäksi mm. oikeus hyvään hallintoon sekä hallinnon julkisuus ja valvottavuus.

Lainalaisuusperiaatteella tarkoitetaan sitä, että hallinnon toimintaa rajoitetaan julkisen vallan käytön osalta sitomalla se laissa määriteltyihin perusteisiin (Mäenpää, 2020, s. 19). Samalla mainittu periaate tuo ennustettavuutta viranomaistoimintaan sitomalla sen ennalta julkisesti ja demokraattisesti määriteltyihin perusteisiin. Mäenpään (2020, s.21) mukaan lakisidonnaisuus asettaa vaatimuksen sitä, että viranomaisen on tarkoin noudatettava lakia. Viranomainen toteuttaa sille laissa määritellyt tehtävät, noudattaa itseään koskevaa lainsäädäntöä ja toimii lain määrittelemissä rajoissa.

Hallintolakia ja siten myös hyvää hallintotapaa sovelletaan Mäenpään (2020, s. 55) mukaan myös viranomaisen ja hallintokoneiston sisäiseen toimintaan, kuten hallinnon ylläpitoon ja johtamiseen sekä julkisten palvelujen tuottamiseen ja järjestämiseen.

Hyvä hallintotapa perustuu hallintolakiin (Hallintolaki, 434/2003). Hyvällä hallintotavalla tarkoitetaan sitä, että viranomainen käyttää toimivaltaansa yksinomaan lain mukaan hyväksyttäviin tarkoituksiin ja toimet ovat oikeassa suhteessa tavoiteltuun päämäärään nähden. Viranomainen avustaa toista viranomaista toimivaltansa rajoissa ja asian vaatimassa laajuudessa sekä pyrkii edistämään viranomaisten yhteistyötä.

Hyvä tiedonhallintatapa on määritelty asetuksessa viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (Julkisuuslaki 1030/1999), josko asetus viittaa julkisuuslain (621/1999) kumottuun 18 §:ään, mikä puolestaan liittyy vuoden 2020 alusta voimaan tulleeseen tiedonhallintalakiin (Tiedonhallintalaki 906/2019). Mäenpään (2020, s. 87) mukaan hyvän tiedonhallintatavan keskeinen tavoite on tiedon laadun säilyttäminen, mihin vaikuttavat asiakirjojen ja tiedon saatavuus, käytettävyys, eheys ja suojaaminen. Jokaisella on oltava mahdollisuus saada tieto julkisista asiakirjoista ja tietojärjestelmistä. Tiedonhallintalaissa (906/2019) sama asia on todettu tavoitteeksi varmistaa tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi.

Voutilaisen (2006, s. 3) mukaan hyvän hallinnon perusteisiin kuuluu myös palvelujen laatuvaatimus ja toiminnan tuloksellisuusvaatimus osana tehokkuusvaatimusta. Voutilainen (2006) kytkee hyvään hallintoon myös tietoturvallisuuden sekä viranomaisten tietovarantojen hyvän julkisuus- ja salassapitorakenteen.

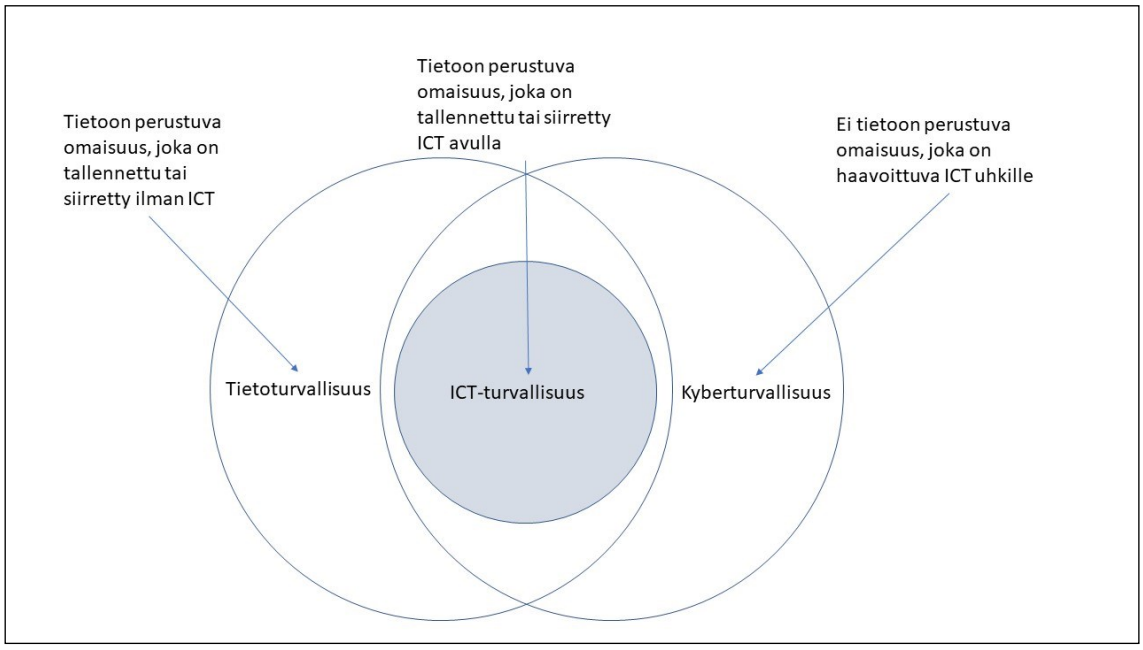
Voutilainen (2006, s. 18) toteaa tietoturvallisuuden yleensä kuuluvan vain tietohallinnolle, vaikka sillä on vaikutusta laajasti organisaation toimintaan. Tämän takia tietoturvallisuuden vastuut on määriteltävä hajautetusti eri organisaatioyksiköille. Mikäli tietoturvallisuus lyödään laimin ja tietojen eheydestä ei voida varmistua tai tiedot joutuvat vääriin käsiin, voi asiankäsittely hidastua ja tuottaa vääriä ratkaisuja. Tietoturvallisuudella onkin merkitys hyvän hallinnon edellyttämälle asian käsittelyn joutuisuudelle ja asianmukaisuudelle (Emt., 2006, s. 19).

Vaikka tietoturvallisuus on keskeisessä asemassa sähköisessä asioiden käsittelyssä, viranomaisen on noudatettava toimenpiteiden suunnittelussa suhteellisuusperiaatetta (Voutilainen, 2006, s. 20). Tietoturvallisuustoimenpiteet tulee mitoittaa suojattavan tiedon perusteella niin, että ylimitoitetut järjestelyt eivät hidasta perusteettomasti viranomaisen toimintaa.

2.3 Vaikeasti ymmärrettävä kyberturvallisuus

Von Solmsin ja van Niekerkin (2013) mukaan tietoturvallisuus, tieto- ja tietoliikenneturvallisuus (ICT-turvallisuus) sekä kyberturvallisuus kytkeytyvät toisiinsa. ICT-turvallisuus liittyy teknisen infrastruktuurin ja siihen tallennetun tiedon turvallisuuteen, kun taas tietoturvallisuus sisältää digitaalisen tiedon lisäksi myös muodossa olevan tiedon. Tästä johdettuna von Solms ja van Niekerk (2013) toteavat ICT-turvallisuudessa keskeisesti suojattavan kohteen olevan teknologia ja vastaavasti tietoturvallisuudessa suojataan tietoa. Tutkijoiden mukaan (von Solms & van Niekerk, 2013) kaikessa turvallisuudessa on kyse omaisuuden suojaamisesta erilaisilta uhkilta, jotka liittyvät luontaisiin haavoittuvuuksiin. Haavoittuvuuksista aiheutuvia riskejä pyritään vähentämään turvallisuuskontrolleilla.

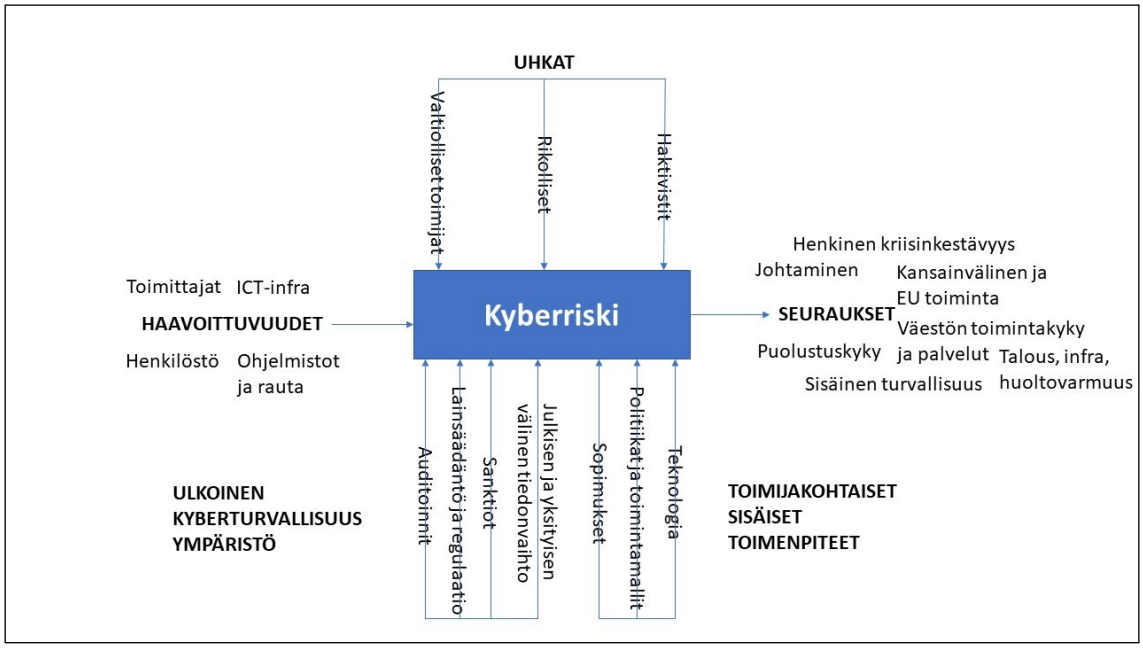
Von Solms ja van Niekerk (2013) toteavat kyberturvallisuuden poikkeavan aikaisemmin esitetystä, koska suojattavan omaisuuden kirjo on paljon laajempi kattaen kaikenlaiset verkkoon liitetyt laitteet, ihmiset, yhteiskunnan kannalta tärkeät toiminnot sekä kansallisesti kriittisen infrastruktuurin. Keskeistä kuitenkin on se, että kaikkeen suojattavaan omaisuuteen liittyy haavoittuvuuksia, jotka johtuvat tieto- ja tietoliikennetekniikan käytöstä. Tutkijoiden mukaan (von Solms & van Niekerk, 2013) kyberturvallisuuden tavoitteena ei ole suojata kybertoimintaympäristöä, vaan siellä toimivat yksilöt, organisaatiot ja valtiot. Turvallisuuden osa-alueiden välinen suhde on kuvattu kuviossa 1.



KUVIO 1: Tietoturvallisuuden, ICT-turvallisuuden ja kyberturvallisuuden välinen suhde (Mukailtu von Solms & van Niekerk, 2013)

Hillerin ja Russelin (2013) tutkimuksessa tekijät tutkivat lainsäädännön vaikutuksia yksityisen yrityksen kyberturvallisuuteen toisaalta arvioiden yritysten kyberturvallisuuden edistävän myös kansallista turvallisuutta. Tutkijat esittävät riskin muodostuvan uhkista, haavoittuvuuksista, kyberturvallisuusympäristöstä sekä vahingon pienentämiseen tähtäävistä toimista. Hiller ja Russel (2013) toteavat haavoittuvuuksien olevan sisäisiä riskejä, jotka liittyvät työntekijöiden toimintaan, heikkoon infrastruktuuriin ja toimittajiin. Vastaavasti uhka on ulkoinen riski, joka muodostuu mm. valtiollisista toimijoista, rikollisista ja hakkereista. Uhkataso nousee, mikäli mainitut toimijat havaitsevat haavoittuvuuksia. Vahingon pienentämiseen tähtäävien toimenpiteiden avulla pyritään sisäisesti vähentämään hyökkäysten todennäköisyyttä tai niiden aiheuttamia vahinkoja. Toimenpiteitä ovat mm. turvallisuuteen liittyvät politiikat ja toimintamallit, tekniset ratkaisut sekä eri tahojen kanssa laadittavat sopimukset. Sisäisiä toimenpiteitä tukee ja niihin vaikuttaa ulkoinen kyberturvallisuusympäristö, joka käsittää mm. standardit ja parhaat käytänteet, lainsäädännön ja regulaation sekä mahdollisiin

turvallisuuspoikkeamiin liittyvät velvoitteet. Turvallisuuspoikkeamilla on negatiivisia seurauksia, jotka tutkijoiden (Hiller & Russel, 2013) mallia soveltaen Suomen kansallisella tasolla tarkasteltuna vaikuttavat tai voivat vaikuttaa yhteiskunnan elintärkeisiin toimintoihin kuvion 2 mukaisesti.



KUVIO 2: Kyberriskin muodostuminen ja vaikutukset (Mukailtu Hiller & Russel, 2013)

Yhteiskunnan elintärkeät toiminnot liittyvät Suomessa käytössä olevaan kokonaisturvallisuuden malliin (Turvallisuuskomitea, 2017). Malli perustuu viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyöhön, jolla varaudutaan erilaisiin häiriötilanteisiin ja huolehditaan yhteiskunnan elintärkeistä toiminnoista. Käytännön toteutus perustuu hallinnonalakohtaisiin tai poikkihallinnollisiin strategioihin ja niiden toimenpano-ohjelmiin, kuten esimerkiksi kyberturvallisuusstrategia (Turvallisuuskomitea, 2017). Kokonaisturvallisuus voidaan nähdä mallina ja periaatteena, jonka pohjalta asioita tarkastellaan valtioneuvoston tasolla (Kokonaisturvallisuuden sanasto, 2017).

Mikäli tarkastelunäkökulma lasketaan yksittäisen viranomaisen tasolle, vaikutukset kohdentuvat ko. viranomaisen sisäiseen operatiiviseen toimintaan tai palvelutuotantoon. Operatiiviseen toimintaan kohdistuvat vaikutukset riippuvat viranomaisen toimialasta ja tehtävästä. Käytännön vaikutukset yhteiskunnan elintärkeiden toimintojen osalta kohdentuvat niihin liittyvään kriittiseen infrastruktuuriin, josko osin kriittinen infrastruktuuri voi sisältää itsessään haavoittuvuuksia. Kriittisen infrastruktuurin käsitteen alla on laaja kirjo nimensä mukaisesti infrastruktuuria, mutta myös erilaisia toimintoja ja palveluita (Valtioneuvosto, 2018). Kriittiseen infrastruktuurin kuuluvia elementtejä on kuvattu taulukossa 1.

TAULUKKO 1: Yhteiskunnan kriittinen infrastruktuuri (Valtioneuvosto, 2018).

Digitaalinen yhteiskunta	Tietojärjestelmät, viestintäverkot ja -palvelut, tieto-omaisuus
Media	Sisällöntutotanto, julkaisu, jakelu
Finanssialan palvelut ja järjestelmät	Rahoitus- ja vakuutuspalvelut, maksuliikenne, arvopaperit, korttimaksaminen
Logistiset verkostot ja palvelut	Ohjausjärjestelmät, liikenne- ja kuljetuspalvelut
Energia-ala	Sähkö, lämpö, polttoaineet
Kriittinen tuotanto	Vesihuolto, teollisuus, infran rakentaminen ja kunnossapito, elintarvikehuolto, sosiaali- ja terveydenhuolto, jätehuolto

Suomen ensimmäisessä kyberturvallisuusstrategiassa (Turvallisuuskomitean sihteeristö, 2013, s. 2) todettiin, että kyberturvallisuutta ei ole tarkoitettu oikeudelliseksi käsitteeksi, joka antaisi uusia toimivaltuuksia viranomaisille. Strategian mukaan kyberturvallisuuden asiat kuuluvat ensisijaisesti valtioneuvoston toimivaltaan ja tehtävät on säädetty eri hallinnonaloille. Tuolla perusteella kunkin ministeriön vastuulla on toimialansa kyberturvallisuuden asioiden valmistelu ja hallinnon järjestely (Turvallisuuskomitean sihteeristö, 2013, s. 5). Kuitenkin strategiassa määritettiin strateginen linjaus nro 8, jonka perusteella liittyvä lainsäädäntö kartoitetaan. Tarkoituksena oli, että lainsäädäntö antaisi riittävät keinot ja toimivaltuudet viranomaisille yhteiskunnan elintärkeiden toimintojen ja valtion turvallisuuden suojaamiseksi kyberuhkia vastaan. Strategiassa määritetyt linjaukset on esitetty oheisessa luettelossa:

1. *Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli*
2. *Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä*
3. *Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa*
4. *Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia*
5. *Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään*
6. *Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaa*
7. *Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä*

8. *Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset*
9. *Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle*
10. *Strategian toimeenpanoa valvotaan ja toteumaa seurataan*

Strategian pohjalta on syytä nostaa esiin muutamia tarkennuksia edelliseen luetteloon. Tehokkaaseen yhteistoimintamalliin kuuluu mm. harjoitustoiminnan ja sääntelyn kehittäminen. Harjoitustoiminnalla parannetaan organisaatioiden kyvykkyyttä ja sääntelyllä viranomaisten ja elinkeinoelämän välistä tiedonvaihtoa. Tilannetietoisuuden ja tilanneymmärryksen kehittämisen keskeiset toimenpiteet ovat Kyberturvallisuuskeskuksen perustaminen, ja valtioneuvoston tilannekeskuksen kyky jakaa tilannekuvaa. Kyberpuolustuksen osalta perustelumuistio tarkentaa linjausta jonkin verran laajemmaksi. Perustelumuistion mukaan kyberpuolustus toteutetaan yhteistyössä Puolustusvoimien, muiden viranomaisten ja muun yhteiskunnan kanssa. Tilannekuva muodostetaan yhdessä Kyberturvallisuuskeskuksen kanssa ja myös muut viranomaiset tukevat Puolustusvoimia kyberpuolustustehtävissä. Toisaalta Puolustusvoimien kykyä kehitetään muiden viranomaisten tukemiseen. Lainsäädännön osalta perustelumuistio toteaa mm. sen, että kansallisessa lainsäädännössä ei ole kyberuhkia koskevaa yhtenäistä sääntelyä. (Turvallisuuskomitean sihteeristö, 2013)

Valtioneuvoston periaatepäätös ”Suomen kyberturvallisuusstrategia 2019” (Turvallisuuskomitean sihteeristö, 2019) nojaa edellisen strategian yleisiin periaatteisiin ja kytkeytyy osaltaan Yhteiskunnan turvallisuusstrategiaan (Turvallisuuskomitea, 2017) sekä siinä kuvattuun toimivaltaisen viranomaisen periaatteeseen.

Kansallisen kehittämisen koordinointia varten perustettiin liikenne- ja viestintäministeriöön kyberturvallisuusjohtajan tehtävä. Tehtävän perustaminen ei muuttanut ministeriöiden ja toimivaltaisten viranomaisten vastuita tai toimivaltuuksia. Viranomaisten yhteistyötä todettiin kehitettäväksi strategian perusteella valmisteltavassa kehittämisohjelmassa keskeisinä osa-alueina kyberpuolustus ja kansallista turvallisuutta vaarantavien uhkien torjunta (Turvallisuuskomitean sihteeristö, 2019, s. 7). Strategiassa määritetään kolme linjausta:

1. *Suomi huolehtii kybertoimintaympäristöstään aktiivisen kansainvälisen ja EU-yhteistyön tukemana*
2. *Kansallisen kyberturvallisuuden kokonaistilaa parannetaan kehittämisohjelmalla sekä sen suunnittelua ja seurantaa edistävällä yhteistyöllä*
3. *Kansallinen kyberturvallisuuden osaaminen varmistetaan tunnistamalla osaamistarve sekä vahvistamalla koulutusta ja tutkimusta*

Todettakoon turvallisuuteen liittyvän valtionhallinnon strategioiden perusteella useita turvallisuuslähtöisiä käsitteitä, jotka eivät välttämättä helposti erotu toisistaan. Kyberturvallisuutta on eri tavoin kytketty mm. kansalliseen turvallisuuteen. Valtioneuvoston kanslian toimeksiantamassa

selvityksessä ”Kansallisen turvallisuuden vaikutusten arviointi” (Lonka ym., 2020) todettiin kansallisen turvallisuuden määritelmän olevan haastavan ja sitä tulkitaan kovin eri tavoin. Laajasti sisältöön kuuluvaksi koettiin kuitenkin tietoverkkoihin liittyvät uhat.

2.4 Toimivaltainen viranomainen poikkihallinnollisessa asiassa

Lewallenin (2020) mukaan kehittyvien teknologioiden sääntelyyn liittyy neljä haastetta. Ensimmäinen koskee epävarmuutta, joka liittyy olemassa oleviin ongelmiin ja sääntelyyn suhteessa uusiin teknologioihin sekä toisaalta siihen, kenellä on toimivalta sääntelyyn. Kehittyvät teknologiat haastavat olemassa olevan toimivallan rakenteita ja lainsäätäjät kilpailevat toimivallasta yrittäen omia sen itselleen joko yksittäisessä organisaatiossa tai koko hallinnossa. Hallinnon sisäinen toimivaltakamppailu saattaa johtaa myös siihen, että säädeltävän elinkeinon toimijat pyrkivät hyödyntämään epäselvää tilannetta.

Toinen haaste liittyy siihen, että hajautettu toimivalta johtaa samalla pilkottuun sääntelyyn, joka vaatii hallinnon sisäistä koordinaatiota (Lewallen, 2020). Teknologia-ohjattu sääntely, kuten kyberturvallisuudessa, hajautuu useille vastuutahoille poikkihallinnollisesti. Hajautettu sääntely ei välttämättä ole huono asia, erityisesti jos säätelijät ovat epävarmoja päätöstensä vaikutuksista, mutta kokonaisuudenhallinta vaatii koordinaatiota. Eri hallinnonalojen ohjaus voi olla erilaista. Toinen toimii hyvin ja proaktiivisesti, kun taas toinen ei pysy kehityksen mukana.

Kolmanneksi haasteeksi Lewallen (2020) nimeää koordinaatiopyrkimysten vastustuksen, mikä johtuu koordinoitavan asian tavoitteesta tai päämäärästä. Hallinnon sisäinen koordinointi edellyttää järjestelyjä, jotka edistävät eri osatekijöiden keskinäistä integrointia toimivaksi kokonaisuudeksi. Disruptiivisiin teknologioihin voi liittyä tekijöitä, jotka estävät integroinnin onnistumisen. Esimerkiksi puolustuksen tai ulkoasianhallinnon näkemys kyberturvallisuudesta ei ole välttämättä helposti kytkettävissä potilastietojen suojaamiseen. Puuttuva koordinaatio voi johtaa sääntelyyn, joka perustuu aikaisempaan sääntelyyn ottamatta huomioon teknologian erityispiirteitä. Kyberturvallisuuden osalta lainsäätäjien keskustelu on yleensä keskittynyt siihen, miten olemassa olevaa sääntelyä voidaan soveltaa, sen sijaan että olisi haettu uusia ratkaisuja. Tämä voi säästää aikaa, mutta johtaa sääntelyyn, joka ei sovellu sellaisenaan mihinkään yksittäiseen tilanteeseen.

Neljäs haaste koskee lainsäätäjien kokemaa epävarmuutta. Epävarmuuden kasvaessa byrokraattisuus lisääntyy, mikä näkyy vetoamisena olemassa olevaan sääntelyyn (Lewallen, 2020). Teknologiat ja niihin liittyvät ongelmat voivat kehittyä eri hallinnonaloilla ennen kuin yhteinen näkemys on kyetty muodostamaan ja päätös mukaan otettavista näkökulmista tekemään. Sen sijaan lainsäätäjät keskittyvät soveltamaan olemassa olevaa sääntelyä uusiin ongelmiin välttääkseen lisäongelmia sidosryhmien kanssa. Sääntelyn kohteena oleva

elinkeinoelämä voi hyötyä sirpaleisesta sääntelystä ja toimivallasta, kun kaikkia sääntelyn riskejä ja kustannuksia ei kyetä määrittämään.

Perustuslain (731/1999) 68 §:n mukaisesti kukin ministeriö vastaa toimialallaan valtioneuvostolle kuuluvien asioiden valmistelusta ja hallinnon asianmukaisesta toiminnasta. Laki valtioneuvostosta (175/2003) määrittää ministeriöt ja mm. valtioneuvoston kanslian vastuita tietoturvallisuudesta tiedonhallintalain (906/2019) perusteella. Valtioneuvoston ohjesääntö (262/2003) antaa yhteiset säännökset ministeriön toimivallasta. Yleisenä periaatteena todetaan toimivaltaisen ministeriön olevan se, jonka toimialaan asia pääosaltaan kuuluu (262/2003 10 §). Kukin ministeriö käsittelee mm. omaan toimialaansa kuuluvat lainvalmisteluasiat, tietoyhteiskunta-asiat, hallintoasiat sekä tietohallintoasiat. Valtioneuvoston kanslian tehtäviin kuuluu mm. valtioneuvoston ja ministeriöiden yhteinen tietohallinto ja asiakirjahallinto sekä niihin liittyvä hyvän tiedonhallintatavan ja yhteentoimivuuden ohjaus.

Osana valtioneuvoston selvitys- ja tutkimustoimintaa julkaistiin ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (Lehto ym., 2017). Selvityksen mukaan tietoturvallisuutta on säädelty jo pitkään, joten perusasiat ja toimintatavat ovat kunnossa, lainsäädännössä ei koeta olevan puutteita eikä lainsäädäntöä pidetä esteenä viranomaisten yhteistoiminnalle, mitä voidaan pitää osin ristiriitaisena toteamuksena oikeusministeriön selvityksen tai tietoturvallisuuden ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla selvittäneen työn perusteella.

Oikeusministeriön selvityksessä (Luoma, 2019) tarkasteltiin viranomaisten toimivaltuuksia häiriötilanteissa. Selvityksen perusteella viranomaisten mahdollisuudet puuttua tietoliikenteen tai tietojärjestelmien häiriötilanteisiin vaihtelevat sektorikohtaisesti. Säännökset ovat osin epäselviä tai niitä ei ole lainkaan. Liikenne- ja viestintävirastolla on kyberuhkien osalta laajimmat, mutta silti sektorikohtaisesti rajatut toimivaltuudet (Luoma, 2019).

Tietoturvallisuuden ja tietosuojan kehittäminen yhteiskunnan kriittisillä toimialoilla (TITUKRI) -selvityksen (Lehtilä, Nyström, Ronikonmäki & Sirviö, 2021) perusteella kehittämistarpeita tietoturvallisuuden- ja tietosuojan osalta on lainsäädännössä, viranomaisten yhteistoiminnassa, velvoittavissa tietoturvallisuusvaatimuksissa sekä vaatimusten säännöllisessä arvioinnissa ja valvonnassa.

Lainsäädännön kehittäminen pelkästään kyberturvallisuuden näkökulmasta koetaan hankalana ilmiön poikkileikkaavuuden takia (Lehto ym., 2017). Kyberturvallisuuden strategisessa johtamisessa on puolestaan kaksi perusongelmaa (Lehto ym., 2018). Ensimmäinen liittyy valtioneuvoston tasalla ministeriöiden itsenäiseen toimintaan omilla sektoreillaan, jolloin kokonaisvaltainen strateginen johtajuus puuttuu. Toinen ongelma juontuu suoraan edellisestä. Hajautunut hallinnonalakohtainen johtaminen ei ota huomioon laajempaa yhteiskunnallista näkökulmaa (Lehto ym., 2018). Samaan ongelmaan kiinnittivät huomiota myös Lonka ym. (2020). Heidän mukaansa selkeää vastuunjakoa ministeriöiden välillä pidetään tärkeänä, mutta se lisää samalla siiloutumista. Tätä lisäävät omalta osaltaan myös erilaiset hallinnonalakohtaiset selonteot.

Poikkihallinnollista yhteistyötä arvostetaan, mutta sitä pidetään haastavana koska kellään ei tunnu olevan kokonaisymmärrystä (Lonka ym., 2020, s. 35).

3 TIETO- JA KYBERTURVALLISUUDEN HALLINTA

Tässä luvussa tarkastellaan riskienhallintaa osana tietoturvallisuuden hallintaa sekä standardien vaikutusta ja merkitystä. Toisena osana käsitellään palvelukeskusmallin vaikutusta viranomaisen tietoturvallisuuden hallintaan.

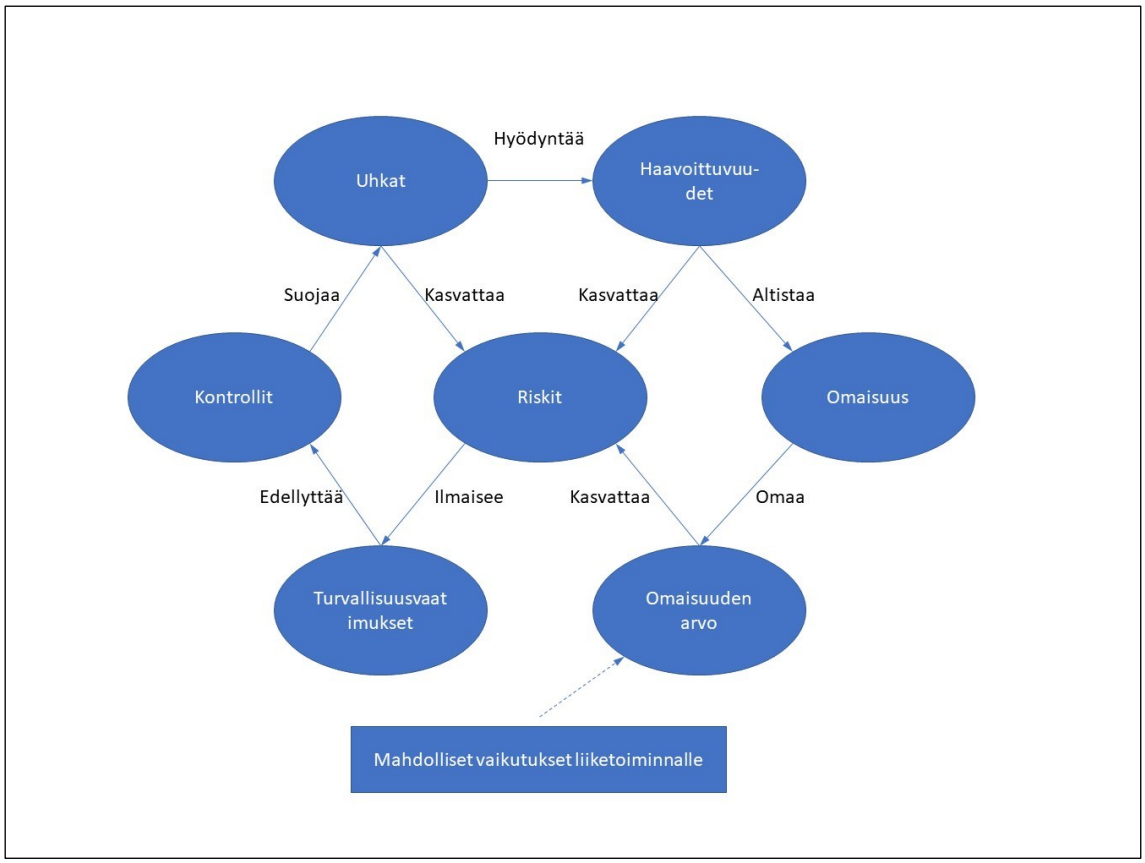
3.1 Riskiperustainen lähestyminen ja riskien arviointi

Kyberturvallisuutta koskevassa luvussa käsiteltiin jo hieman riskien muodostumista ja ei toivottuja vaikutuksia, joita riskit voivat aiheuttaa ilman asianmukaisia toimenpiteitä. Riskien arviointi muodostaa keskeisen perustan tietoturvallisuudenhallintajärjestelmälle (Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). Shameli-Sendin ym. (2016) mukaan tietoturvallisuusriskien hallinta on jatkuva prosessi, joka tuottaa liiketoiminnalle ymmärryksen organisaation tieto-omaisuuteen kohdistuvista potentiaalisista riskeistä. Reaalimaailmassa riskienhallinta on haastava prosessi, koska riskitekijät ovat jatkuvassa muutoksessa. Shameli-Sendi ym. (2016) kritisoivat erilaisten riskienhallintamallien yleistä luonnetta ja käytäntöön viemisen edellyttämien yksityiskohtien puuttumista.

Kuviossa 3 on esitetty Tupan ja Steinerin (2006) yksinkertaistus riskienhallinnan osa-alueiden välisistä suhteista. Uhkat kasvattavat osaltaan riskejä ja hyödyntävät haavoittuvuuksia, jotka myös kasvattavat riskejä ja altistavat tieto-omaisuuden riskeille. Tieto-omaisuudella on tietty arvo, joka kasvattaa riskejä ja toisaalta saa vaikutuksia riskien mahdollisista vaikutuksista tieto-omaisuudelle. Riskit osoittavat ja ilmaisevat turvallisuusvaatimuksia, jotka edellyttävät turvallisuuskontrolleja, jotka tuovat suojaa uhkilta.

Riskianalyysi edellyttää Tupan ja Steinerin (2006) mukaan uhkien tunnistamista, uhkien todennäköisyyden arviointia, omaisuuden tunnistamista ja arvottamista, haavoittuvuuksien määrittämistä, uhkan toteutumiseen liittyvien odotettujen menetysten laskemista ja riskianalyysin evaluointia, mikä vastaa myös Shameli-Sendin ym. (2016) näkemystä.

Riskien evaluoinnissa arvioidaan riskien merkittävyys ja määritetään tarvittavat toimenpiteet riskien todennäköisyyden ja vaikutusten perusteella (Shameli-Sendi ym., 2016). Toimenpiteet voidaan jakaa neljään luokkaan. Tietyt riskit voidaan tietoisesti hyväksyä, jotkut riskeille altistavat toiminnot jätetään toteuttamatta, osa riskeistä siirretään jonkun toisen vastuulle ja osa riskeistä käsitellään eri tavoin pienentäen vaikutuksia niin, että se voidaan hyväksyä. Jäljelle jäävien riskien osalta on tärkeää seurata niitä säännöllisesti ja dokumentoidusti (Shameli-Sendi ym. 2016).



KUVIO 3: Riskienhallinnan osa-alueiden väliset suhteet (Mukailtu Tupa & Steiner, 2006)

Valtiontalouden tarkastusviraston mukaan (2017, s. 43) Suomessa ei ole julkisen hallinnon kattavaa riskienhallintaprosessia. Yhteisen prosessin kautta voitaisiin tuottaa tarvittavat tiedot kyberloukkaustilanteen operatiiviselle johtamiselle suojattavien kohteiden kustannusvaikutusten, riskianalyysin ja priorisoinnin perusteella.

3.2 Hallinnan osa-alueet

Tieto- tai kyberturvallisuuden hallinnan avulla pyritään varmistamaan organisaation tiedon ja sen käsittelyjärjestelmien turvallisuus estämällä tai minimoimalla uhkiin liittyvien riskien toteutuminen (Szczepaniuk, E., Szczepaniuk, H., Rokicki, & Klepacki, 2019). Tutkijoiden mukaan tietoturvallisuuden hallintajärjestelmä on osa organisaation johtamisjärjestelmää perustuen organisaation rakenteeseen, tietoturvallisuuspolitiikkaan, prosesseihin ja resursseihin (Szczepaniuk ym., 2019). Susanto, Amunawar ja Tuan (2006) puolestaan toteavat tietoturvallisuuden hallintajärjestelmän olevan välttämätön tieto-omaisuuden suojaamiseksi tehokkaasti. Puolassa toteutetun tutkimuksensa perusteella Szczepaniuk ym. (2019) totesivat julkisten organisaatioiden lisänneen tietoturvallisuuden hallintamallien käyttöönottoa sen jälkeen, kun kansalliseen lainsäädäntöön

otettiin EU:n velvoitteet kuten tietosuoja-asetus sekä verkko- ja tietoturvadirektiivi.

Siponen ja Willison (2009) toteavat artikkelissaan organisaatioiden pyrkivän noudattamaan tietoturvallisuuden hallinnassaan yleisesti tunnettuja parhaita käytänteitä pyrkien näin myös osoittamaan sitoutumistaan liiketoimintansa turvaamiseen. Todisteellinen sitoutuminen ja standardoitu toiminta on merkki ulospäin siitä, että organisaatio pyrkii määrätietoisesti suojaamaan oman toimintansa. Siponen ja Willison (2009) pitävät tärkeänä sitä, että hallintamenetelmät on sovitettu organisaation toimintaympäristöön ja toimintaan organisaatiokohtaisesti, mikä todettiin myös valtioneuvoston tietoturvallisuutta koskevassa periaatepäätöksessä (Valtiovarainministeriö, 2009). Tutkijoiden mukaan yleiset ja yhdenmukaiset, turvallisuustoimenpiteet voivat jättää huomiotta organisaatiokohtaisia erityispiirteitä, mikä voi johtaa turhiin kustannuksiin väärin perustein ja toisaalta turvattomiin ratkaisuihin (Siponen & Willison, 2009). Saman johtopäätöksen tekevät myös Shameli-Sendi ym. (2016) todetessaan, että jopa standardit jättävät johdon vaille selkeää visualisointia turvallisuusriskien arvioinnista.

Toteuttamassaan kirjallisuuskatsauksessa Soomro ym. (Soomro, Hussain & Ahmed, 2015) toteavat tietoturvallisuuden osalta vastuun siirtyneen tietohallinnolta johdolle, koska tietoturvallisuudella on vaikutus organisaation julkisuuskuvaan. Tutkijat toteavat, että tehokkaan tietoturvallisuuspolitiikan kehittämisellä ja jalkauttamisella on keskeinen rooli tietoturvallisuuden hallinnassa. Muita merkityksellisiä tekijöitä ovat mm. inhimillinen tekijä (Human factor), tietoturvakoulutus, työntekijöiden osuus tietomurroissa, ylimmän johdon tuki sekä teknisten ja hallinnollisten toimenpiteiden integrointi. Näkemys vastaa Susanton ym. (2006) toteuttamaa vertailua viiden tunnetun hallintajärjestelmän kesken. Susanton ym. (2006) näkemys hallintajärjestelmän osa-alueista on kuvattu taulukossa 2.

TAULUKKO 2: Tietoturvallisuuden hallinnan osa-alueet. Mukailtu Susanto ym., 2006.

Osa-alue	**Sisältö**
Tietoturvallisuuspolitiikka	Miten organisaatio kuvaa tietoturvallisuuden tavoitteet, johdon aikomukset tiedon turvaamiseksi, ohjeet henkilöstölle ja viestintä sidosryhmille
Käyttö- ja viestintäturvallisuus (Palvelutuotannon ja tietoliikenteen turvallisuus)	Määritetty politiikka, jonka avulla pyritään pienentämään tietojärjestelmiin ja niiden ylläpitoon sekä tietoliikenteeseen liittyviä riskejä
Pääsynhallinta	Järjestelmä, jolla hallitaan pääsyoikeuksia tietojärjestelmiin ja fyysisiin tiloihin
Tietojärjestelmien hankinta, kehittäminen ja ylläpito	Yhteinen prosessi, joka määrittää välirajat ja tekniset tietojärjestelmät

Osa-alue	Sisältö
Tietoturvallisuusorganisaatio	Organisointi, jolla tietoturvallisuus viedään käytäntöön; johdon rooli, koordinointi, tiedon käsittelyn auktorisointi. Jakautuu sisäiseen ja ulkoiseen
Omaisuuden hallinta	Määritellyn omaisuuden tunnistaminen, jäljittäminen, luokittelu ja omistajuuden määrittäminen
Tietoturvallisuustapahtumien ja poikkeaminen hallinta	Varautuminen tietoturvallisuustapahtumiin ja poikkeamiin sekä tarvittavien resurssien määrittely
Liiketoiminnan jatkuvuuden hallinta	Toiminnan jatkumisen varmistaminen erilaisissa poikkeamatilanteissa
Henkilöstöturvallisuus	Varmistetaan kaikkien tiedon käsittelijöiden osaaminen ja ymmärrys omista rooleistaan ja vastuistaan sekä se, että oikeudet tietoon poistetaan työsuhteen päättyessä
Fyysinen ja ympäristöturvallisuus	Järjestelmien, tukevan infrastruktuurin, rakennusten ja tilojen suojaaminen vahingoilta tai oikeudettomalta pääsyltä
Vaatimustenmukaisuus	Ulkoisen sääntelyn (lainsäädäntö ym noudattaminen ja toisaalta sisäisten politiikkojen, määräysten ja ohjeiden noudattaminen

Roy (2020) vertailee konferenssipaperissaan ISO 27001 -standardia ja yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) kyberturvallisuuden viitekehystä. ISO 207001 (Suomen standardisoimisliitto ry., 2017)) on eurooppalainen standardi ja hyväksytty myös kansalliseksi standardiksi Suomessa. Standardi kuvaa vaatimukset tietoturvallisuuden hallintajärjestelmälle, joka pyrkii suojaamaan riskienhallinnan avulla tiedon luottamuksellisuutta, eheyttä ja saatavuutta. NIST:n kyberturvallisuuuden viitekehys (NIST, 2018) on vapaaehtoinen, erityisesti kriittisen infrastruktuurin kyberturvallisuuden riskien hallintaan kehitetty työkalu, jota voidaan käyttää kuitenkin erilaisten organisaatioiden tarpeisiin. Roy (2020) päätyy vertailussaan johtopääkseen, että standardi ja vapaaehtoinen viitekehys eivät ole keskenään kilpailevia, vaan paras lopputulos syntyy käyttämällä niitä täydentämään toisiaan. Standardin vaatimuksiin perustuva hallintamalli luo pohjan enemmän teknisiä kontrolleja sisältävän viitekehyksen hyödyntämiselle.

Molemmissa hallintamalleissa lainsäädäntö on selkeästi osa tietoturvallisuudenhallintaa. ISO 27001 osalta liitteessä A (Suomen standardisoimisliitto ry., 2017) kuvataan hallintatavoitteiden ja keinojen viiteluettelo. Lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattamisen osalta tavoitteena on kaikkien tietoturvallisuutta koskevien lakien, asetusten, säännösten ja sopimusten velvoitteiden ja turvallisuusvaatimusten noudattaminen. Standardi edellyttää,

että vaatimukset ja organisaation toimintamalli vaatimusten täyttämiseksi on yksilöitävä ja dokumentoitava. Vastaavasti NIST:n kyberturvallisuuden viitekehyksessä (NIST, 2018, s.26) tunnista-toiminnossa on hallinto -kategoria, joka määrittelee lainsäädännölliset vaatimukset osaksi kyberturvallisuudenhallintaa. Viitekehys edellyttää, että vaatimusten hallintaan ja valvontaan määritetyt politiikat, toimintatavat ja prosessit on ymmärretty ja johto pidetään tietoisena riskeistä. Alakategoria määrittää edelleen huomioon otettavaksi lainsäädännölliset vaatimukset, joihin kuuluvat kyberturvallisuuden osa-alueina myös tietosuoja ja kansalaisten perusoikeudet.

3.3 Palvelukeskusmalli valtionhallinnossa

3.3.1 Valtion yhteiset tieto- ja viestintätekniset palvelut

Palvelukeskukset ovat viimeisten vuosikymmenten aikana olleet poliitikkojen suosiossa tehokkuuden tavoittelun takia. Palvelukeskusmalli on osin ulkoistuksen kaltainen, mutta erityisesti valtionhallinnon kokonaisuudessa sisäinen toimenpide. Bergeronin (2003, s. 3) mukaan palvelukeskus on yhdessä tekemisen strategia, jossa liiketoiminnan toimintoja keskitetään uuteen puoli-itsenäiseen yksikköön. Tavoitteena on tehokkuutta lisäävä rakenne, arvonluonti, kustannussäästöt ja parantuneet palvelut isäntäorganisaation sisäisille asiakkaille.

Tietoturvallisuuden osalta ulkoistamiseen liittyy huolia, joiden oletetaan tässä tutkimuksessa esiintyvän myös palvelukeskustoiminnan yhteydessä. Dhillon, Syed ja de Sá-Soares (2016) tutkivat ulkoistamiseen liittyviä huolia, joita ulkoistavat organisaatiot ja toisaalta toimittajat kokivat. Tutkimuksessa kehitetyn mallin perusteella ulkoistamiseen liittyvä tietoturvallisuus voidaan varmistaa kolmen osa-alueen kautta (Dhillon ym., s. 461). Nämä osa-alueet ovat toimittajan kyvykkyys, politiikkojen ja sääntelyn noudattaminen sekä luottamus kontrolleihin ja tiedon suojaamiseen. Toimittajien kyvykkyys muodostuu tietoturvallisuuden kyvykkyydestä ja teknologisesta kypsyydestä. Politiikkojen ja sääntelyn mukaisuus perustuu puolestaan lainsäädännön ja asiakkaiden politiikkojen noudattamiseen. Luottamus tiedon suojaamiseen perustuu luottamukseen siitä, että tarvittavat kontrollit ovat olemassa ja toisaalta asiakkaan tieto on suojattu.

Suomessa perustettiin vuonna 2014 valtion tieto- ja viestintätekniikkakeskus Valtori keskittämällä noin 80 viraston toimialariippumattomat palvelut uuteen palvelukeskukseen (Valtori, 2021). Valtiontalouden tarkastusviraston (VTV) noin viisi vuotta myöhemmin julkaisemassa tarkastuskertomuksessa (Valtiontalouden tarkastusvirasto, 2019a) todetaan monien asetettujen tavoitteiden jääneen ainakin toistaiseksi saavuttamatta. Tarkastusvirasto toteaa kertomuksessaan, että palvelukeskuksen perustaminen ja palveluiden keskittäminen ei perustunut riittävän tarkkaan suunnitteluun tai säästöpotentiaalin arviointiin, mikä on aiheuttanut myöhemmin erilaisia ongelmia (VTV, 2019, s.). Keskeinen tavoite palvelukeskuksen perustamisella oli kustannussäästöjen saavuttaminen ja laadun

parantuminen, mitkä vastaavat edellä esitettyjä yleisiä tavoitteita palvelukeskuksen perustamisella. Joiltain osin kustannukset jopa kasvoivat keskittämisen myötä ja tarjottavien palveluiden ei koeta vastaavan asiakastarpeita.

Valtiontalouden tarkastusvirasto toteutti tuloksellisuustarkastuksen vuonna 2017 selvittäen valtionhallinnon kybersuojauksen tilaa (Valtiontalouden tarkastusvirasto, 2017). Tarkastuksessaan virasto arvioi myös Valtorin perustamisen vaikutuksia kybersuojaukseen. VTV:n mukaan virastot ja laitokset menettivät kybersuojaukseen liittyvää toimivaltaa ja resursseja keskittämisen seurauksena. Keskittämisestä huolimatta toimivaltaa koskevia säädöksiä ei päivitetty, vaan vastuu jäi edelleen toimialoille. Valtioneuvostotasolla asiaa mutkistaa kaksinkertainen palvelukeskusmalli, jossa valtioneuvoston hallintoyksikkö hankkii ministeriöille palvelut Valtorilta, joka tuottaa palveluita itse tai hankkii niitä edelleen markkinoilta. Keskittäminen yhteen palvelukeskukseen lisää tarkastusviraston mukaan laajavaikutteisen häiriön riskiä, mikäli jatkuvuudenhallintaa ei ole hoidettu asianmukaisesti. Valtorin toiminta rahoitetaan asiakasmaksuilla, jolloin myös tieto- ja kyberturvallisuuden kehittämiseen tarvittava rahoitus tulee asiakkailta. Maksukyvykkyys ja halukkuus voi vaihdella asiakkaittain. Valtorin kaikki palvelut eivät ole kyberloukkausten havainnointijärjestelmän piirissä ja Valtorin teknisissä menettelyissä on puutteita, jotka heikentävät kykyä havaita haitallisia muutoksia. Valtori ei myöskään tarkastusviraston kertomuksen (VTV, 2017) perusteella kykene raportoimaan kattavasti palveluidensa tietoturvatilanteesta.

Edellä kuvatun VTV:n tarkastuksen tulokset peilautuvat suoraan myös Lehtilän ym. (2021) suosituksiin. Suositusten perusteella Valtorin tulee keskeisesti kehittää palvelujen laatua ja tietojärjestelmien arviointia. Toisaalta Valtorin ja muiden valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietosuojaa ja tietoturvaa koskevia vastuita tulee arvioida. Edelleen yhteisille palveluille määritetään palvelukohtaisesti tietosuoja-, tietoturvallisuus- ja toimintavarmuusvaatimukset, jotka arvioidaan hyväksytyn kriteeristön mukaisesti. Valtorin osalta arvioidaan myös tietosuojan ja tietoturvan vaatimat resurssit. (Lehtilä ym., 2021)

3.3.2 Turvallisuusverkkotoiminta rinnakkaisena ratkaisuna

Julkisen hallinnon turvallisuusverkkotoiminta käynnistyi vuonna 2015 (Laki julkisen hallinnon turvallisuusverkkotoiminnasta [TUVE-laki], 2015/10). Valtiontalouden tarkastusvirasto toteutti välittömästi toiminnan alkamisen jälkeen toiminnan ohjaukseen liittyvän tuloksellisuustarkastuksen, jonka havainnoissa mitä ilmeisimmin näkyy osaltaan toiminnan alkuvaihe (VTV, 2016). Tarkastukseen liittyvä seurantatarkastus julkaistiin 2019 (VTV, 2019b), mikä puolestaan osoittaa tarkastusviraston mukaan toiminnan kehittyneen kuluneiden noin kahden vuoden aikana.

Hallinnon turvallisuusverkko on rakennettu täyttämään korkean turvallisuuden ja varautumisen vaatimukset (VTV, 2016). Tavoitteena on varmistaa kaikissa tilanteissa valtion ylimmän johdon ja turvallisuusviranomaisten viestintä sekä päätöksenteossa tarvittavan tiedon käytettävyys, eheys ja

luottamuksellisuus (TUVE-laki, 2015/10). Verkon käyttöön liittyy käyttövelvoite, joka koskee mm. valtioneuvostoa, Puolustusvoimia, poliisia, rajavartiolaitosta sekä joitakin muita viranomaisia (2015/10).

VTV:n tarkastuksen (2016) perusteella TUVE-hankkeen aikana asetettuja vaatimuksia ei kaikilta osin ollut kyetty todentamaan ja tämän osalta dokumentaatiossa oli puutteita vaatimustenhallinnan prosessissa. Tarkastusraportti toteaa, että tietoturvallisuuden osalta toimintaan liittyy jatkossa riski siitä, että tietoturvallisuudesta tingitään kustannuspaineiden takia (VTV, 2016, s. 41). Osaltaan tähän liittyy ns. toimialasidonnaisten (TOSI) järjestelmien saattaminen vastaamaan turvallisuusverkon vaatimuksia, mitä käyttäjäorganisaatiot pitivät liian kalliina.

Valtiovarainministeriön mukaan (VTV, 2016) TUVE-palvelut ja TUVE-verkossa käytettävät TOSI-palvelut tulee auditoida. Auditoinnille on verkko- ja infrastruktuuripalvelujen osalta määritetty laissa (10/2015) takarajaksi kolme vuotta lain voimaantulosta, mutta tieto- ja viestintäteknisille palveluille ei ollut annettu takarajaa. VTV:n tarkastuksen aikana käynnissä oli 12 auditointia ja VTV piti riskinä, että auditoinnissa paljastuu seikkoja, jotka osoittavat, että toteutettu arkkitehtuuri ei vastaa vaatimuksia (VTV, 2016, s. 42).

Osaltaan auditointeja vaikeuttaa koko valtionhallinnolta puuttuvat yhteiset tietoturvavaatimukset (VTV, 2017, s. 41). Turvallisuusverkon osalta tieto- ja viestintäteknisille palveluille on määritelty korkean varautumisen, valmiuden ja turvallisuuden kriteeristö (VaVaTu), jota on käytetty luonnoksena. Toisaalta on käytetty myös Katakri-kriteeristöä (VTV, 2016, s. 42), joka on ulkoministeriön (2021) mukaan viranomaisten auditointityökalu, jota viranomainen voi käyttää arvioidessaan salassa pidettävän tiedon suojaamisen kykyä.

VTV toteaa jälkiseurantaraportissaan (2019b) valtiovarainministeriön pyrkineen kehittämään turvallisuusverkkotoiminnan ohjausta varsinaisen tarkastuskertomuksen jälkeen. Käyttäjien tarpeita pyritään ymmärtämään paremmin ja turvallisuusverkkotoiminnan ohjauksen kytkeytymisestä julkisen hallinnon ICT-ohjauksen kokonaisuuteen huolehditaan. Ohjaukseen liittyviä malleja ja prosesseja on kuvattu paremmin ja rahoitusmalli perustuu palvelumaksuihin.

4 TUTKIMUKSEN TOTEUTUS

4.1 Menetelmälliset valinnat

Tieto- ja kyberturvallisuuteen sekä valtionhallinnon ICT-palvelujen järjestämiseen liittyvä lainsäädäntö on tullut varsin tutuksi ja näkyy omassa työssäni lähes päivittäin. Tämä on samalla herättänyt oman kiinnostuksen selvittää tarkemmin lainsäädännön ohjaavaa vaikutusta. Lainsäädännössä on merkityksellistä, mitä lakiin on kirjoitettu, mutta myös perustelut, joiden mukaisesti laki on hyväksytty. Toisaalta lainsäädäntö muodostuu eri hallinnonalojen vastuulla olevista yleis- ja erityislaeista, jotka muodostavat moniulotteisen ja maallikolle usein vaikeaselkoisenkin kokonaisuuden.

Koska tutkittava aihe on itselleni käytännön kautta varsin tuttu, liittyy siihen tästä syystä ennakkokäsityksiä. Tutkimuksen läpinäkyyden takia ohessa on kuvattu omaa aihetta sivuavaa työhistoriaani melko tarkasti, sillä oma työni on viimeisen noin kuuden vuoden aikana liittynyt monin tavoin viranomaisten tieto- ja viestitäteknisten palveluiden järjestämiseen tai tieto- ja kyberturvallisuuteen sekä niiden kehittämiseen. Olen ollut mukana palvelujen siirrossa Valtorille sen toiminnan käynnistämisen yhteydessä, turvallisuusverkkotoiminnan käynnistämisessä ja toimintaan kuuluvissa ohjauselimissä sekä myös vähäisissä rooleissa lainvalmistelun yhteydessä mm. kun lakia sähköisen viestinnän palveluista muutettiin. Kuulun työni puolesta edelleen mm. Valtorin asiakasneuvottelukuntaan ja valtionhallinnon tiedonhallinnan yhteistyöryhmään.

Hirsijärven ym. (Hirsijärvi, Remes, & Sajavaara, 2005) mukaan laadullisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen ja kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti. Kirjoittajien mukaan kvalitatiivisessa tutkimuksessa on pyrkimyksenä löytää tai paljastaa tosiasioita. Metsämuuronen (2008, s. 208) toteaa puolestaan kvalitatiivisen tutkimusotteen soveltuvan erityisen hyvin käytettäväksi, kun ollaan kiinnostuneita yksityiskohtaisista rakenteista, halutaan tutkia luonnollisia tilanteita tai halutaan saada tietoa tiettyihin tapauksiin liittyvistä syy-seuraussuhteista.

Hirsijärvi ym. (2005, s. 156) jakavat kvalitatiivisen tutkimuksen kiinnostuksen kohteet neljään ryhmään aikaisemman tutkimuksen perusteella. Säännönmukaisuuksien etsiminen voidaan edelleen ulottaa elementtien tunnistamiseen ja niiden suhteiden kartoittamiseen, mihin liittyvä yksi tutkimustyyppi on grounded teoria. Metsämuuronen (2008, s. 217) selittää grounded teorian aineistopohjaiseksi teoriaksi, jossa tutkimuksen teoria muotoillaan tutkittavan aineiston pohjalta. Aikaisempaan tutkimukseen perustaen Metsämuuronen (2008, s. 218) toteaa grounded teorian käytön vaihtelevan mm. tutkimuskohteen, tarkoituksen, ilmenneiden sattumien ja tutkijan kyvykkyyden perusteella. Grounded teoriassa aineisto kertoo, mitä se pitää sisällään ja teoria muodostetaan sen perusteella (Metsämuuronen, 2008, s. 218). Corbin ja Straus (1990) toteavat

artikkelissaan, että grounded teorian yhteydessä data voi olla useista eri lähteistä, kuten valtiollisista dokumenteista tai mistä tahansa, kunhan se tuo lisävalaistusta käsillä olevaan ongelmaan. Martti J. Kari (2019) käytti omassa kyberturvallisuuden väitöskirjassaan lähteinä mm. Venäjän lakeja ja presidentin asetuksia, kun tässä työssä kiinnostuksen kohteina ovat Suomen kansalliset lait ja asetukset.

4.2 Tutkimusaineisto

Kirjallisuuskatsaus perustuu valikoituun akateemiseen tutkimukseen, jota täydentää käytännön ongelmien ratkaisuun tähdänneet valtioneuvoston selvitykset ja tehtyjen päätösten hyötyjä ja vaikuttavuutta selvittäneet valtiontalouden tarkastusviraston raportit. Tällä on pyritty osoittamaan teorian ja käytännön yhteys.

Tutkimusaineistoksi valikoitui keskeinen tietoturvallisuutta koskeva ja kyberturvallisuuteen liittyvä lainsäädäntö perusteluineen sekä kyberturvallisuuden kehittämiseen tähdänneet valtioneuvoston periaatepäätökset, minkä avulla pyrittiin tarkastelemaan mahdollisia eroja näiden välillä. Aineiston valinnoilla pyrittiin varmistamaan sisällöllistä validiteettia varmistamalla keskeisten käsitteiden ottaminen huomioon (Metsämuuronen, 2008, s. 116). Sisällöllisen validiteetin avulla varmistetaan se, tutkitaan sitä, mitä halutaan tutkia.

Tietoturvallisuuden perusteet tulevat julkisuusperiaatteen mukaisesti julkisuuslaista (Laki viranomaisen toiminnan julkisuudesta, 1999/621), missä kuvataan viranomaisen asiakirjojen lähtökohtainen julkisuus sekä periaatteet salassapidolle. Julkisuuslakia sovelletaan edelleen viranomaistoiminnassa tiedonhallintalain kautta, mitä täydentää lain perusteella annettu asetus. Tiedonhallintalain pyrkimyksenä on varmistaa tietoaineistojen hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi (Tiedonhallintalaki, 2019/906). Lain perusteella annetussa valtioneuvoston asetuksessa säädetään tarkemmin asiakirjojen turvallisuusluokittelusta ja tarvittavista tietoturvallisuustoimenpisteistä (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 2019/1101). Laki sähköisestä asioinnista viranomaistoiminnassa (2003/13) pyrkii lisäämään sujuvuutta asioinnissa sekä tietoturvallisuutta erilaisissa hallintotehtävissä ja laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista[1] (2016/571) pyrkii parantamaan mm. julkisten palvelujen saatavuutta, laatua ja tietoturvallisuutta. Viranomaisten tietoteknisten ratkaisujen turvallisuus pyritään varmistamaan lailla viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuudesta (2011/1406). Laki kansainvälisistä tietoturvallisuusvelvoitteista (2004/588) säätelee toimenpiteitä kansainvälisten velvoitteiden toteuttamiseksi. Viranomaisten velvollisuudesta käyttää nimenomaisesti tiettyjä palveluita ja tehdä hankintoja määrätyin periaattein säädetään kahdessa eri laissa. Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä[2] (2013/1226) pyrkii tehostamaan toimintoja, parantamaan laatua ja kustannustehokkuutta

[1] Ns. KaPA-laki
[2] Ns. TORI-laki

sekä ohjausta. Laki julkisen hallinnon turvallisuusverkkotoiminnasta[3] (2015/10) pyrkii puolestaan varmistamaan valtion ylimmän johdon ja tärkeiden turvallisuusviranomaisten sekä muiden toimijoiden viestinnän häiriöttömyyden ja jatkuvuuden. Laki sähköisen viestinnän palveluista (2014/917) säätelee nimensä mukaisesti sähköistä viestintää laajasti, ja pyrkii myös turvaamaan sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan. Vastaavasti laki digitaalisten palvelujen tarjoamisesta (2019/306) pyrkii edistämään digitaalisten palveluiden saatavuutta, laatua ja tietoturvallisuutta. Valmiuslaki (2011/1552) on tarkoitettu poikkeusoloissa turvaamaan yhteiskunnan toiminnot.

4.3 Grounded teoria ja aineiston analysointi

Corbinin ja Straussin (1990, s. 6) mukaan aineiston kerääminen ja analysointi liittyvät toisiinsa. Analysointi alkaa välittömästi, kun ensimmäinen pala aineistoa on kerätty. Tässä työssä kirjallisuuskatsauksen laatiminen jäsensi analyysiä ennalta. Analysointi alkoi tutkimusaineiston muodostamisen käynnistyessä, josko pohjaa tälle loi kirjallisuuskatsauksen lisäksi oma esiymmärrykseni aiheesta. Lainsäädännön tarkastelu alkoi perustuslaista ja lähti sitä kautta etenemään yleislakien kautta kohti erityislakeja. Lain viittaus johti toiseen lakiin tai asetukseen, mikä johto edelleen kolmanteen lakiin ja niin edelleen. Useissa kohdin lain pykäläkirjaus ei sellaisenaan tuntunut kertovan koko totuutta, jolloin oli tarpeen perehtyä lain perusteluihin hallituksen esityksessä, mikä edellytti puolestaan alkuperäisen säädöksen kautta etenemistä.

Kaikki esiin nousevat käsitteet ovat aluksi ehdokkaita. Käsitteiden tulee tukea orastavaa teoriaa ja alustavat käsitteet aineiston todellisuudessa mahdollistavat teorian havainnoinnin (Corbin & Strauss, 1990, s. 7). Aineiston muodostamisen ja analyysin alkaessa käsitteet valikoituivat käytännössä kirjallisuuskatsauksen kautta. Tätä kautta kytkettiin toisiinsa tiettyä kokonaisuutta käsittelevä lainsäädäntö, joka jakautuu kirjallisuuskatsauksen perusteella useille eri osa-alueille. Käsitteistä tulisi edelleen kehittää kategorioita sen perusteella, miten käsitteet liittyvät toisiinsa. Kaikki käsitteet eivät kuitenkaan Corbinin ja Straussin (1990, s. 7) mukaan muodosta kategorioita. Kategoriat ovat korkeamman tason ilmentymiä ja abstraktimpia kuin käsitteet, joita ne edustavat. Näin on myös tässä tutkimuksessa.

Tutkimuksen tulokset on jäsennelty kirjallisuuskatsauksen ja oman esiymmärrykseni perusteella kyberturvallisuuteen ja tietoturvallisuuteen, joissa molemmissa tarkempi jäsentely perustuu toiminnan eri osa-alueisiin luvun viisi mukaisesti. Nämä kaksi kokonaisuutta on edelleen pyritty yhdistämään uudeksi teoriaksi grounded teorian mukaisesti. Jäsentely ilmentää samalla avointa-, aksiaalista ja selektiivistä koodausta (Airaksinen, J., 2021), jossa eri vaiheissa löydetään käsitteitä, vertaillaan niitä, yhdistetään niitä kategorioihin ja edelleen

[3] Ns. TUVE-laki,

valikoiden teoriaksi ydinkategorian ympärille. Tässä työssä ydinkategoriaksi osoittautui lainsäädännön perusta kaikelle viranomaistoiminnalle.

Hirsijärven ym. (2005, s. 217) mukaan kaiken tutkimuksen luotettavuutta ja pätevyyttä tulee arvioida, vaikka tutkija ei haluaisikaan käyttää termejä validiteetti ja reliabiliteetti. Laadullisessa tutkimuksessa validius merkitsee Hirsijärven ym. (2005, s.217) mukaan kuvauksen ja siihen liitettyjen selitysten ja tulkintojen yhteensopivuutta. Luotettavuutta voidaan lisätä tarkalla selostuksella tutkimuksen toteuttamisesta, mitä tässä tutkimuksessa on pyritty edellä tekemään. Tutkimuksen kannalta keskeinen merkitys on aineiston analyysissä käytetyllä luokittelulla, jonka perusteet on kuvattu edellä ja sisältö esitetty tuloksissa. Tulosten tulkinnan osalta validiteetti pyrittiin varmistamaan kytkemällä tulokset aikaisempaan tutkimukseen.

5 LAINSÄÄDÄNTÖ OHJAA VIRANOMAISTA HAJANAISESTI

Tässä luvussa esitetään tutkimuksen tulokset. Tulokset on ryhmitelty kolmeen alalukuun.

5.1 Strategisella tasolla vastuut ja toimivalta jakautuvat

Valtioneuvostossa ratkaistavat asiat ratkaistaan joko valtioneuvoston yleisistunnossa tai ministeriössä riippuen aiheesta (Laki valtioneuvostosta, 2003/175, 12 §). Valtioneuvoston ohjesääntö (2003/262) määrittää ministeriöt ja niiden toimialat. Perussääntönä asioiden käsittelyssä on, että asian käsittelee ministeriö, jonka toimialaan se pääosin kuuluu. Tieto- tai kyberturvallisuutta ei valtioneuvoston ohjesäännössä mainita, mutta kukin ministeriö käsittelee mm. oman toimialansa lainvalmisteluasiat, tietoyhteiskunta-asiat, tietohallintoasiat sekä muut sellaiset asiat, jotka liittyvät toimialan tehtävien hoitamiseen (Valtioneuvoston ohjesääntö, 2003/262, 11 §). Kukin ministeriö käsittelee toimialansa virastoja koskevat asiat.

Valtioneuvoston tasolla vastuut tieto- ja kyberturvallisuudesta jakautuvat useille ministeriöille. Valtioneuvoston kanslian tehtäviin kuuluu mm. yhteinen tilannekuva, varautuminen, häiriötilanteiden hallinnan yleinen yhteensovittaminen, valtioneuvoston yhteinen tietohallinto ja hyvän tiedonhallintotavan ohjaus (Valtioneuvoston ohjesääntö, 2003/262, 12 §). Tilannekuvan kokoamis- ja jakeluvastuu[4] on valtioneuvoston tilannekeskuksella (Laki valtioneuvoston tilannekeskuksesta, 2017/300). Tilannekeskuksen toimintaa säätelevän lain perusteluissa (HE 261/2016 vp) todetaan uusien laaja-alaisten uhkien, kuten hybridivaikuttamisen ja kyberhyökkäysten torjuntakyvyn merkitys. Toisaalta perusteluissa kytketään keskeiseksi tilannekuvan perustaksi tuolloin valmistelussa olleiden tiedustelulakien mahdollistama tiedonhankinta.

Valtioneuvostossa toimii pysyvinä yhteistyöeliminä kansliapäällikkö- ja valmiuspäällikkökokoukset (Valtioneuvoston ohjesääntö, 2003/262, 10 §). Valmiuspäällikkökokouksen tehtävänä on toimia häiriötilanteiden johtamisessa tukena kansliapäälliköille ja toimivaltaiselle viranomaiselle sekä ministeriöille mm. esityksillä toiminnan yhteen sovittamisesta. Valmiuspäälliköille asioita valmistelee valmiussihteerikokous (HE 261/2016 vp.)

Valtioneuvostoa ja ministeriöitä avustaa myös Turvallisuuskomitea, joka toimii puolustusministeriön yhteydessä (Valtioneuvoston asetus Turvallisuuskomiteasta, 2013/77). Turvallisuuskomitea on kokonaisturvallisuuden ja varautumisen pysyvä yhteistoiminta- ja häiriötilanteissa asiantuntijaelin. Komitea avustaa varautumisessa ja sen yhteen sovittamisessa, seuraa ja arvioi

[4] Laki määrittää erikseen velvoitteen jakaa tilannekuvaa, toisin kuin Kyberturvallisuuskeskusta koskeva laki (Laki valtioneuvoston tilannekeskuksesta, 2017/300; Laki liikenne- ja viestintävirastosta, 2018/935)

yhteiskunnan muutosten vaikutuksia, seuraa eri hallinnonalojen ja -tasojen toimia varautumisjärjestelyjen ylläpidossa ja sovittaa tarvittaessa yhteen laajoja varautumisen asiakokonaisuuksia. Turvallisuuskomitean jäseninä ovat tasavallan presidentin kanslian kansliapäällikkö, pääministerin valtiosihteeri, ministeriöiden kansliapäälliköt, Rajavartiolaitoksen päällikkö, pääesikunnan päällikkö, poliisiylijohtaja, pelastusylijohtaja, Tullin pääjohtaja, suojelupoliisin päällikkö ja Huoltovarmuuskeskuksen toimitusjohtaja (Asetus 2013/77.)

Ulkoministeriön vastuulla on yleisesti kansainväliset suhteet (Valtioneuvoston ohjesääntö, 2003, 262, 14 §), mutta se toimii myös kansainvälisten tietoturvallisuustoimenpiteiden osalta kansallisena turvallisuusviranomaisen[5] (Laki kansainvälisistä tietoturvallisuusvelvoitteista, 2004/588, 4 §). Kansallisen turvallisuusviranomaisen tukena toimivat henkilöstö-, yritys- ja toimitilaturvallisuuden osalta nimetyt turvallisuusviranomaiset[6], joita ovat puolustusministeriö, pääesikunta, suojelupoliisi sekä liikenne- ja viestintäministeriö (Laki 2004/588).

Oikeusministeriön toimialaan liittyy tietoverkko- ja kyberrikollisuuteen kuuluva sääntely rikosoikeuden alalla (Valtioneuvoston ohjesääntö, 2003/262, 14 §), mikä tarkoittaa käytännössä rikoslakia (1889/39). Sisäministeriön vastuulle kuuluu yleinen turvallisuus ja järjestys sekä poliisihallinto (Valtioneuvoston ohjesääntö, 2003/262, 15 §), mihin liittyy toisaalta kyberrikosten torjunta[7] (Sisäministeriö, 2021a), mutta myös Suojelupoliisin toteuttama siviilitiedustelu ja tietoliikennetiedustelu osana sitä (Sisäministeriö, 2021b; Poliisilaki, 2011/872; Laki tietoliikennetiedustelusta siviilitiedustelussa, 2019/582). Sotilaallinen maanpuolustus kuuluu puolustusministeriön toimialalle (Valtioneuvoston ohjesääntö, 2003/262, 16 §), mihin liittyy kyberpuolustus ja sitä kautta sotilastiedustelu (Laki sotilastiedustelusta, 2019/590).

Valtiovarainministeriö huolehtii julkishallinnon yleisestä kehittämisestä ja julkisen hallinnon tietopolitiikan, tiedonhallinnan ja sähköisen asioinnin kehittämisestä (Valtioneuvoston ohjesääntö, 2003/262, 17 §). Tuolla perusteella valtiovarainministeriö on säätänyt julkisen hallinnon tiedonhallinnasta (Tiedonhallintalaki, 2019/906), millä pyritään varmistamaan viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely. Valtiovarainministeriö myös toisaalta ohjaa tietoteknisiä hankintoja ja velvoittaa käyttämään Valtorin toimialariippumattomia, valtion yhteisiä tieto- ja viestintäteknisiä palveluja (Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä [TORI-laki], 2013/1226) tai julkisen hallinnon turvallisuusverkon palveluja (Laki julkisen hallinnon turvallisuusverkkotoiminnasta [TUVE-laki], 2015/10). Valtiovarainministeriö ohjaa viranomaisia mahdollistamaan sähköisen asioinnin ja pyrkii lisäämän sujuvuutta sekä tietoturvallisuutta tällä tavoin (Laki sähköisestä asioinnista viranomaistoiminnassa, 2003/13), pyrkii edistämään digitaalisten palvelujen saatavuutta ja tietoturvallisuutta (Laki digitaalisten palvelujen tarjoamisesta, 2019/306) ja edellyttää mm. Digi- ja väestötietoviraston tuottamien

[5] National Security Authority (NSA)

[6] Designated Security Authority (DSA)

[7] Sisäministeriö käyttää termiä kyberrikollisuus sekä sen synonyymeinä tietoverkkorikollisuus ja tietotekniikkarikollisuus (Sisäministeriö, 2021a)

tukipalvelujen käyttöä sähköisessä asioinnissa mm. tietoturvallisuuden ja yhteentoimivuuden nimissä (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista [KaPA-laki], 2016/571). Valtiovarainministeriön alaan kuuluu myös yhteistoimintamenettely (Laki yhteistoiminnasta valtion virastoissa ja laitoksissa, 2013/1233). Siinä edellytetään käsiteltäväksi teknisen valvonnan käyttö ja sen menetelmät sekä sähköpostin ja tietoverkon käytön periaatteet ja virkamiehen sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely.

Liikenne- ja viestintäministeriölle kuuluu sähköinen viestintä ja viestintäpalvelujen tietoturvallisuus (Valtioneuvoston ohjesääntö, 2003/262, 20 §). Laki sähköisen viestinnän palveluista (2014/917) pyrkii tavoitteillaan mm. edistämään sähköisen viestinnän palvelujen käyttöä, varmistamaan viestintäverkkojen ja -palvelujen toimintavarmuuden ja turvallisuuden sekä turvaamaan sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan. Laki sääntelee viranomaisten toimintaa monin tavoin. Sääntelyä liittyy mm. siihen, kun viranomainen tarjoaa itse palvelut ja käsittelee välitystietoja, tietoliikennelaitteiden sijoittamiseen viranomaisen hallussa oleviin tiloihin, viranomaisliittymiin, viranomaisten väliseen yhteistyöhön tietyiltä osin ja moniin muihin asioihin. Erityisenä huomiona voidaan todeta uutta teknologiaa koskeva erityinen sääntely (244a ja 244b §) kansallisen turvallisuuden näkökulmasta. Laki sähköisen viestinnän palveluista (2014/917 325 §) antaa liikenne- ja viestintävirastolle laajan tarkastusoikeuden teleyrityksiin, viranomaisviestintään liittyvän palveluntarjoajan toimintaan sekä satelliittipaikannusteknologiaa tuottaviin tai käyttäviin yrityksiin. Laki antaa myös yleiset perusteet yritykselle, viranomaiselle tai muulle yhteisölle huolehtia tietoturvastaan sekä siihen liittyen mm. analysoida verkkoonsa tulevien viestien sisältöä haittaohjelmien tai vastaavien osalta sekä ryhtyä tarvittaviin välttämättömiin toimenpiteisiin tietoturvan varmistamiseksi (Laki 2014/917, 272 §; HE 221/2013 vp, s. 196).

Työ- ja elinkeinoministeriön osalta suoraan tieto- tai kyberturvallisuuteen liittyvää erityistä toimivaltaa ei valtioneuvoston ohjesäännön perusteella pysty tunnistamaan (Valtioneuvoston ohjesääntö, 2003/262, 21 §). Ministeriön vastuulle kuuluva laki huoltovarmuuden turvaamisesta (1992/1390) määrittää Huoltovarmuuskeskuksen kehittämän ja ylläpitämään huoltovarmuutta ja kunkin ministeriön kehittämään sitä omalla toimialallaan. Huoltovarmuuskeskuksen tehtävänä on mm. kehittää julkishallinnon ja elinkeinoelämän yhteistoimintaa, varmistaa elintärkeiden teknisten järjestelmien (kriittisien infrastruktuurin) toimivuus ja turvata tavara- ja palvelutuotanto. Huoltovarmuuskeskuksen mukaan (2021) tietoyhteiskuntatoimialan tehtävänä on varmistaa yhteiskunnan kannalta välttämättömien palveluiden toimivuus kaikissa olosuhteissa. Sähköiset tieto- ja viestintäjärjestelmät pyritään suojaamaan ja varmentamaan jo normaalioloissa osana yhteiskunnan kriittisen infrastruktuurin toiminnan varmistamista. Varautuminen tapahtuu yritysten omaehtoisena toimintana, mutta Huoltovarmuuskeskus myös rahoittaa varautumista erilaisten ohjelmien kautta.

Viranomaisten toimivaltuuksista poikkeusoloissa säädetään valmiuslaissa (2011/1552). Lain tarkoituksena on mahdollistaa yhteiskunnan toiminta myös poikkeusoloissa, joita ovat mm. Suomeen kohdistuva aseellinen hyökkäys tai

vakavuudeltaan siihen rinnastettava muu hyökkäys ja sen jälkitila tai em. hyökkäyksen uhka, jonka vaikutuksen torjuminen edellyttää valmiuslain toimivaltuuksia. Lain perusteluissa (HE 3/2008 vp) todetaan aseelliseen hyökkäykseen rinnastettavaksi myös tietojärjestelmiin kohdistunut isku. Hyökkäys voi tarkoittaa myös ei-valtiollisen toimijan toteuttamaa hyökkäystä, mikäli se on laajuudeltaan ja vaikuttavuudeltaan verrattavissa valtion toteuttamaan hyökkäykseen.

Sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi laki antaa liikenne- ja viestintäministeriölle toimivaltuuden mm. antaa velvoitteita teleyrityksille (Valmiuslaki 2011/1552, 60 §). Edelleen lain 62 § antaa liikenne- ja viestintäministeriölle toimivallan tietoturvallisuuden sääntelyyn myös viranomaisten osalta. Liikenne- ja viestintäministeriö voisi lain 63 §:n perusteella määrätä yksityisen henkilön tai yhteisön luovuttamaan käyttöoikeuden esim. päätelaitteisiin, tietojärjestelmiin tai varavoimalaitteisiin. Vastaavasti laki sähköisen viestinnän palveluista (2014/917, 283 §) velvoittaa teleyrityksiä varautumaan normaalioloissa siihen, että kriittinen viestintäverkon järjestelmä ja sen ohjaus sekä hallinta voidaan valmiuslain toimivaltuuksin palauttaa Suomeen.

Valtiovarainministeriö voi poikkeusoloissa määrätä valtion tietohallinnon ja tietoturvallisuuden järjestämisestä (Valmiuslaki, 2011/1552, 105 §). Tämä ei kuitenkaan koske mm. puolustusvoimien ja poliisin toiminnallisia tietojärjestelmiä.

5.2 Operatiivinen kyberturvallisuustoiminta kaipaa tiiviimpää yhteistoimintaa

5.2.1 Yleiset huomiot

Kyberturvallisuus sellaisena käsitteenä, kuin se on esitetty kansallisissa kyberturvallisuusstrategioissa 2013 ja 2019 (Turvallisuuskomitean sihteeristö, 2013 ja 2019) ei sellaisenaan kuulu lainsäädäntöön. Hakusanalla kyberturva* löytyy Finlexistä (Oikeusministeriö, 2021b) kolme säädöstä, jotka koskevat oikeusministeriön työjärjestystä, liikenne- ja viestintäviraston tehtäviä ja virkamieslain vaatimuksia niistä tehtävistä, jotka edellyttävät Suomen kansalaisuutta. Tämä ei tarkoita sitä, etteikö lainsäädäntö sisältäisi muutoinkin kyberturvallisuutta tai siihen läheisesti liittyviä osa-alueita. Vaikuttaisi kuitenkin siltä, että kyberturvallisuus pirstaloituu toisin käsittein useisiin erityislakeihin ja eri hallinnonaloille

Kun lähtökohtana käytetään kyberturvallisuusstrategiaa vuodelta 2013, voidaan tarkastelu kohdentaa linjauksiin 1, 2, 4, 5 ja 8 eli viranomaisten yhteistyöhön, kyberturvallisuuskeskuksen perustamiseen ja tilannekuvan muodostamiseen, poliisin ja puolustusvoimien toimintaedellytyksiin sekä lainsäädäntöön. Viranomaisten yhteistyön osalta ei löytynyt yksiselitteisesti sellaista lakia, joka edellyttäisi nimenomaisesti kyberturvallisuuden osalta yhteistyöhön. Liikenne-

ja viestintäministeriön (2020) mukaan viranomaisten välinen yhteistyö perustuu merkittävissä määrin virka-apuun ja tiedonvaihtoon, joita säädellään eri laeissa. Hallintolaki (2003/434, 10§) velvoittaa viranomaista avustamaan toista viranomaista toimivaltansa rajoissa ja asian vaatimassa laajuudessa, mutta virka-avusta muille viranomaisille säädetään hallinnonalakohtaisesti. Laki sähköisen viestinnän palveluista (2014/917, 244 b §) määrittää erityisen verkkoturvallisuuden neuvottelukunnan, jonka tehtävänä on arvioida kansallisen turvallisuuden toteutumista viestintäverkoissa sekä seurata toimivaltaisen viranomaisen tukena viestintäverkkojen ja teknologian kehittymistä sekä verkkoturvallisuutta koskevan lainsäädännön soveltamiskäytäntöä sekä esittää suosituksia. Toimivaltainen viranomainen johtaa toimintaa, joten johtava viranomainen määräytyy tilanteen perusteella, mikä osaltaan ei edistä vakiomuotoista toimintaa.

5.2.2 Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen perustaminen oli yksi vuoden 2013 Kyberturvallisuusstrategian tavoitteista (Turvallisuuskomitean sihteeristö, 2013). Kyberturvallisuuskeskus kuuluu liikenne- ja viestintävirastoon (Laki liikenne- ja viestivirastosta, 2018/935), jossa sen tehtävinä on mm. tukea, ohjata ja valvoa tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Kyberturvallisuuskeskus ylläpitää kansallisen kyberturvallisuuden tilannekuvaa, mutta laki ei määritä sitä jakamaan tilannekuvaa. Lain perusteluissa (HE 61/2018 vp, s. 83) tilannekuvan tuottaminen ja ylläpito liittyy viraston Computer Emergency Response Team -toimintoon (CERT) yhdessä koti- ja ulkomaisten luotettavien kumppanien ja vastintahojen kanssa. Ilmaisu luotettavista kotimaisista kumppaneista tuntuu poikkeavalta verrattuna esimerkiksi valtioneuvoston tilannekeskuksen tehtäviin tilannekuvan jakajana tai ylipäätään yhteistoimintaan viranomaisten kanssa. Jonkinlaisena erityispiirteenä voidaan pitää sitäkin, että liikenne- ja viestintäministeriön alaisen viraston osan toimintaa rahoitetaan erikseen valtiovarainministeriöstä ja Huoltovarmuuskeskuksesta, mikä osaltaan liittynee nettobudjetoinnin periaatteeseen (HE 61/2018 vp, s. 84).

CERT-toiminnon lisäksi Kyberturvallisuuskeskus toimii EU:n verkko- ja tietoturvadirektiivin (Euroopan unioni, 2016/1148) mukaisena Computer Security Incident Response Teamina (CSIRT) osallistuen kansainvälisen verkoston toimintaan välittämällä tietoja koti- ja ulkomaisille toimijoille (HE 61/2018 vp, s. 84). Verkko- ja tietoturvadirektiivi (NIS-direktiivi) määrittää seitsemän huoltovarmuuskriittistä sektoria tai toimialaa[8], jotka kuuluvat sen sääntelyn piiriin ja kuuluvat kansallisesti kriittiseen infrastruktuuriin (Valtioneuvosto, 2018). Direktiivin velvoitteet on sisällytetty sektorikohtaiseen lainsäädäntöön ja valvonta kuuluu kyseiselle hallinnonalalle. Kyberturvallisuuskeskus toimii kansallisena

[8] Energia, terveydenhuolto, finanssiala, finanssialan infrastruktuuri, liikenne, vesihuolto, digi-infrastruktuuri ja digitaaliset palvelut

koordinaattorina NIS-toimijoiden yhteistyöryhmässä ja raportoi vuosittain Euroopan komission NIS-direktiivi tiimille (Kyberturvallisuuskeskus, 2021).

Keskuksen toimintaan liittyy taajuuksien ja salausteknisen aineiston saatavuuden varmistaminen muiden viranomaisten tarpeisiin. Keskus toimii kansallisena tietoliikenneturvallisuusvirastona[9], joka vastaa salassa pidettävän aineiston sähköiseen tiedonsiirtoon ja käsittelyyn liittyvistä asioista osana kansainvälisiä turvallisuusvelvoitteita. Yhtenä Kyberturvallisuuskeskuksen tehtävänä on toimia kansallisena ohjaus- ja valvontaviranomaisena[10] teleyritysten, vahvojen sähköisten tunnistuspalveluidentarjoajien, luottamuspalveluntarjoajien ja verkkotunnusvälittäjien osalta.

5.2.3 Kyberrikostorjunta ja siviilitiedustelu

Poliisilain (2011/872) mukaan poliisin tehtävinä ovat oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen ja selvittäminen. Tietoverkkorikoksista pääosan tutkii paikallispoliisi, jossa toimii digitaalisen todistusaineiston käsittelyyn ja analysointiin erikoistuneita yksiköitä (Sisäministeriö, 2021a). Laajemmat tietoverkkorikokset ja kansainväliset rikoskokonaisuudet tutkii keskusrikospoliisin Kyberrikostorjuntakeskus (Sisäministeriö, 2021a).

Kun tarkastellaan rikoslain (1889/39) mukaisia tieto- ja viestintärikoksia, ei niiden osalta näyttäisi poliisilaissa olevan erityisiä toimivaltuuksia perusmuotoisille rikoksille[11]. Sen sijaan, mikäli kyse on maanpetos[12]- tai terrorismirikoksista[13], voidaan niiden estämiseksi, paljastamiseksi tai vaaran torjumiseksi käyttää salaisia tiedonhankintakeinoja (Poliisilaki, 2011/872), joita on lukuisia. Kybertoimintaympäristöön käytettävistä keinoista voidaan mainita tekninen laitetarkkailu, jolla tarkoitetaan tietokoneen tai sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen tallentamista tai muuta käsittelyä (Poliisilaki, 2011/872, 23 §). Mainittu tallentaminen tai käsittely ei koske viestin sisältöä tai tunnistamistietoa. Teknistä laitetarkkailua voidaan käyttää epäiltäessä törkeää tietoliikenteen häirintää tai törkeää tietomurtoa (Poliisilaki, 2011/872, 8 §.)

Poliisilain (2011/872) 5a luku käsittelee suojelupoliisin suorittamaa siviilitiedustelua ja siinä käytettäviä tiedustelumenetelmiä, jotka ovat käytännössä samat kuin poliisin salaiset tiedonhankintakeinot. Yleistäen voidaan todeta siviilitiedustelun kohteena olevan kansallista turvallisuutta uhkaava toiminta, kuten ulkomainen tiedustelutoiminta, joka voi tapahtua myös

[9] National Communications Security Authority (NCSA)

[10] National Regulatory Authority (NRA)

[11] Salassapitorikos, viestintäsalaisuuden loukkaus, tietoliikenteen häirintä, tietojärjestelmän häirintä, tietomurto, suojauksen purkujärjestelmärikos, tietosuojarikos tai identiteettivarkaus

[12] Maanpetos, törkeä maanpetos, vakoilu, törkeä vakoilu, turvallisuussalaisuuden paljastaminen tai luvaton tiedustelutoiminta

[13] Eri tavoin terrorismiin liittyviä rikoksia

kybertoimintaympäristössä. Yhtenä kohteena on erikseen mainittu yhteiskunnan elintärkeitä toimintoja uhkaava toiminta (Poliisilaki, 2011/872, 5a, 3 §).

Tietoliikennetiedustelusta siviilitiedustelussa säädetään erikseen siitä annetussa laissa (2019/582). Lain perusteella tietoliikennetiedustelun kohteet ovat samat, kuin siviilitiedustelun muutoinkin, mutta tietoliikennetiedustelu voidaan käyttää, mikäli se on välttämätöntä tiedon saamiseksi kansallista turvallisuutta uhkaavasta toiminnasta, eikä tietoa voida hankkia jollain toisella menetelmällä (Laki 2019/582, 4 §).

Tietoliikennetiedustelu herätti runsasta yhteiskunnallista keskustelua ennen tiedustelulakien säätämistä. Tietoliikennetiedustelua pidettiin massavalvontana, joka loukkaa yksityisyydensuojaa ja on sen takia jopa perustuslain vastaista. Asiaa selvittänyt työryhmä (Puolustusministeriö, 2015) jäi erimieliseksi niin, että liikenne- ja viestintäministeriön edustajat jättivät raporttiin eriävän mielipiteensä juuri yksityisyyden suojan ja tietoliikennetiedustelun osalta. Edustajat perustelivat eriävää näkemystään yksityisyyden suojan lisäksi mm. mahdollisilla kielteisillä vaikutuksilla elinkeinoelämään ja investointihalukkuuden vähenemisellä. Kun tiedustelulait aikanaan hyväksyttiin, oli sen edellytyksenä perustuslain yksityisyyden suojaa koskevan muotoilun muuttaminen (HE 198/2017 vp).

Poliisilain 5a luvun 54 §:n perusteella suojelupoliisin tulee toimia yhteistyössä sotilastiedusteluviranomaisen kanssa molempien tiedustelutehtävien tarkoituksenmukaiseksi hoitamiseksi. Edelleen suojelupoliisin tulee antaa tarkoituksenmukaisen yhteistyön kannalta tarvittavat tiedot. Tietoliikennetiedustelun osalta Puolustusvoimien tiedustelulaitos toimii sen teknisenä toteuttajana suojelupoliisin toimeksiannosta (Laki 2019/582, 10 §).

5.2.4 Kyberpuolustus

Kyberpuolustus on määritelty Kyberturvallisuuden sanastossa (2018) kyberturvallisuuden maanpuolustukselliseksi osa-alueeksi, joka muodostuu tiedustelun, vaikuttamisen ja suojan suorituskyvyistä, mutta lainsäädäntö ei sitä terminä tunne. Kyberturvallisuusstrategiassa (Turvallisuuskomitean sihteeristö, 2013) kyberpuolustuksen todetaan liittyvän Puolustusvoimien omien järjestelmien suojaamiseen, jotta se kykenee suoriutumaan lakisääteisistä tehtävistään huolimatta kybertoimintaympäristössä esiintyvistä uhkista. Maanpuolustuskorkeakoulun julkaisussa asiaa on muotoiltu niin, että kyberpuolustuksella suojataan sotilaallisen maanpuolustuksen kannalta kriittinen tieto, tietojärjestelmät, tietoliikennejärjestelyt ja mahdollistetaan Puolustusvoimien operaatiot sekä tuetaan tilannekuvan muodostamista (Laari (toim), Flyktman, Härmä, Timonen, & Tuovinen, 2019). Tälle tarkennukselle ei näyttäisi suoraan löytyvän toimivaltaa lainsäädännöstä, mikäli sotilaallisen maanpuolustuksen kannalta kriittisiä elementtejä on jonkun muun, kuin Puolustusvoimien hallinnassa.

Mukaillen Laarin ym. (2019, s. 58) kuvausta puolustuksellisista kyberoperaatioista suojan suorituskyky voisi muodostua päivittäisistä jatkuvan palvelun hallintaan liittyvistä tietoturvallisuustoimenpiteistä sekä kyvykkyydestä puolustuksellisiin operaatioihin. Puolustuksellissakin operaatioissa tarkoitus voi olla

esim. seurata omiin järjestelmiin tunkeutunutta toimijaa, vaikka toisessa valtiossa sijaitsevaan tietoverkkoon. Vastaavasti hyökkäyksellisissä kyberoperaatioissa on selkeä pyrkimys tunkeutua vastapuolen tietoverkkoihin ja järjestelmiin sekä vaikuttaa niiden toimintaan tai sen kautta johonkin fyysisen maailman toimintoon.

Laki puolustusvoimista (2007/551) määrittelee 2 luvun 4 §:ssä toimivallan liittyen kansan elinmahdollisuuksien ja valtionjohdon toimintavapauden turvaamiseen sekä laillisen yhteiskuntajärjestyksen puolustamiseen. Kyseisessä pykälässä todetaan:

> *Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen. Sotilaallisten voimakeinojen tulee olla sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa. Sotilaallisilla voimakeinoilla tarkoitetaan sotilaan henkilökohtaisen aseen ja sitä voimakkaampaa asevoiman käyttöä.*

Hallituksen esityksessä (HE 264/2006 vp) otetaan kantaa sotilaallisiin voima- ja vaikuttamiskeinoihin, joihin todetaan kuuluvaksi myös elektronisen ja tietosodankäynnin. Tällä perusteella sotilaallisten kybersuorituskykyjen käytön oikeutus syntyisi osaltaan esim. YK:n peruskirjan mukaisesta itsepuolustusoikeudesta ja muista kansainvälisen oikeuden piiriin kuuluvista säännöksistä. Kyse olisi tällöin maanpuolustustehtävään liittyvästä sotilaallisen voiman käytöstä, jota säädellään sotilaskäskyasiana, mikä kuuluu tasavallan presidentin toimivaltaan. Mikäli voimankäyttöä voitaisiin tarkastella aluevalvontakysymyksenä, olisi siihen liittyvä voimankäyttö puolestaan puolustusministerin toimivaltaan kuuluva (HE 264/2006 vp).

Puolustusvoimien toisena tehtävänä on muiden viranomaisten tukeminen, johon kuuluu mm. virka-apu terrorismirikosten estämiseksi ja keskeyttämiseksi sekä muuksi yhteiskunnan turvaamiseksi (2007/551). Virka-avusta poliisille säädetään omassa laissaan (Laki puolustusvoimien virka-avusta poliisille, 1989/781). Virka-apu muuksi yhteiskunnan turvaamiseksi voi lain perustelujen mukaisesti (HE 264/2006 vp) käsittää sellaisia tehtäviä, jotka eivät kuulu Puolustusvoimien muihin tehtäviin, mutta joihin sillä on osaamista, henkilöstöä ja materiaalia. Huomattavaa kuitenkin on, että virka-avun antaminen edellyttää, että sen vastaanottamisesta on myös säädetty. Näin ei ole esimerkiksi Kyberturvallisuuskeskuksen ja Puolustusvoimien välillä. Kyberturvallisuuskeskus (Liikenne- ja viestintävirasto) voi antaa virka-apua asiantuntija-apuna Puolustusvoimille, mutta voi ottaa sitä vastaan ainoastaan radioviestinnän häiriöiden selvittämiseksi (Laki 2014/917). Tätä voi selittää osaltaan halu pitää Kyberturvallisuuskeskus riippumattomana sotilas- ja tiedusteluorganisaatioista (Liikenne- ja viestintäministeriö, 2020). Myös tiedonvaihdon osalta tilanne vaikuttaa samanlaiselta. Puolustusvoimilla on oikeus lakisääteisten tehtäviensä toteuttamiseksi saada välttämättömät tiedot viranomaisilta tai julkista tehtävää hoitavalta yhteisöltä (Laki 2007/551). Kun asiaa tarkastellaan sähköisen viestinnän palveluista

annetun lain (2014/917) näkökulmasta, Kyberturvallisuuskeskus ei voi luovuttaa Puolustusvoimille tietoja, paitsi sellaisia tietoja, jotka se on saanut selvittäessään tietoturvaloukkausta, jonka kohteeksi Puolustusvoimat on joutunut tai voinut joutua. Erikseen on säädetty, että Puolustusvoimilla on oikeus saada taajuuksien käyttöä koskevia valmiussuunnittelun ja poikkeusoloihin varautumisen kannalta merkityksellisiä tietoja (Laki 2014/917, 320 §).

Sotilastiedustelulaki (2019/590) annetiin samaan aikaan siviilitiedustelua koskevien lakien kanssa, mikä näkyy melko samanlaisena sisällöllisenä muotoiluna ja tämän tutkimuksen puitteissa poikkeuksellisena lainsäädännöllisenä vaatimuksena viranomaisten välisestä yhteistyötä. Sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa mm. Suomeen kohdistuvasta sotilaallisesta toiminnasta tai sellaisesta toiminnasta, jonka osalta ylin valtionjohto tarvitsee tietoa päätöksenteon tueksi Puolustusvoimien tehtävien toteuttamiseksi. Näitä toimintoja ovat esimerkiksi asevoimien ja niihin rinnastettavien joukkojen toiminta tai sen valmistelu sekä maanpuolustukseen kohdistuva tiedustelu (Laki 2019/590, 3–4 §). Tiedustelun kohteena on myös muu toiminta, joka uhkaa vakavasti maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. Muuksi maanpuolustusta vaarantavaksi toiminnaksi voidaan katsoa esimerkiksi laajamittainen ja pitkäkestoinen tietoverkoissa tapahtuva hyökkäys (HE 203/2017 vp, s. 191). Yhteiskunnan elintärkeitä toimintoja vaarantavan toiminnan voidaan katsoa liittyvän Puolustusvoimien lakisääteisiin tehtäviin Puolustusvoimista annetun lain 4 §:n mukaisesti. Tietoa voidaan hankkia toiminnasta, joka pyrkii keskeyttämään tai tuhoamaan esim. sähköntuotantoa tai tietoliikenne- ja tietojärjestelmiä. Tietoa voidaan hankkia myös haittaohjelmista ja niiden mahdollisesta leviämisestä viranomaisten käyttämiin tietojärjestelmiin sekä niitä levittävistä toimijoista (HE 203/2017 vp, s.192).

Laki velvoittaa sotilastiedustelun toimimaan yhteistyössä siviilitiedustelun kanssa, mikä vastaa siviilitiedustelulle tehtyä kirjausta (Laki 2019/590, 17–19 §). Sotilastiedustelun osalta säädetään kuitenkin tarkemmin ja erikseen salaisen tiedonhankinnan yhteensovittamisesta tarvittaessa suojelupoliisin ja keskusrikospoliisin kanssa. Sotilastiedustelun edellytetään toimivan tarpeen mukaan yhteistyössä muiden viranomaisten kanssa ja se voi luovuttaa tietoja muille viranomaiselle, mikäli se on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Yrityksille tai yhteisöille voidaan luovuttaa tietoja esim. haittaohjelmasta, mikäli se on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi. Tietoliikennetiedustelun kautta hankittua tietoa haittaohjelmasta voidaan kuitenkin luovuttaa yrityksen tai yhteisön etujen turvaamiseksi (Laki 2019/590, 74 §). Sotilastiedustelu voi vaihtaa tiedustelutietoja ulkomaisten tiedustelupalvelujen kanssa ja osallistua tiedustelutietojen hankkimiseen liittyvään kansainväliseen yhteistyöhön (Laki2019/590, 17–20 §).

Siviilitiedustelusta poiketen, sotilastiedustelu voi toteuttaa tietojärjestelmätiedustelua, joka kohdistuu Suomen ulkopuolella sijaitsevaan tietojärjestelmään (Laki 2019/590, 62 §). Edellytyksenä on, että sillä oletetaan olevan erittäin tärkeä merkitys tiedustelutehtävän kannalta. Muutoin käytettävät

tiedustelumenetelmät vastaavat poliisin tai Suojelupoliisin käyttämiä salaisia tiedonhankintakeinoja. Tietoliikennetiedustelun osalta sotilastiedustelulaissa on säädetty aiheesta monipuolisemmin osin ainakin johtuen siitä, että tekninen toteutus on aina Puolustusvoimien tiedustelulaitoksella. Laissa on erikseen säädetty (65–66 §) siitä, että tietoliikennetiedustelu ei saa olla yleistä ja kohdentamatonta. Tiedustelulaitos voi tiedustelun kohdentamiseksi kerätä ja tallentaa hetkellisesti sekä automaattisesti käsitellä tietoliikenteen teknisiä tietoja. Tietoliikennetiedustelu voi kohdentua valtiolliseen toimijaan (68 §) tai muuhun kuin valtiolliseen toimijaan (70 §). Jälkimmäinen on rajatumpaa ja edellyttää, että tiedot eivät ole hankittavissa muilla tiedustelumenetelmillä. Suojelupoliisin puolesta toteutetulla teknisellä tietoliikennetiedustelulla tarkoitetaan sitä, että Puolustusvoimien tiedustelulaitos toteuttaa teknisten tietojen analyysin suojelupoliisin toimeksiannosta ja että tiedustelulaitos toteuttaa tietojen keräämisen selvittämättä sisältöä (73 §).

Kyberpuolustuksen kannalta mielenkiintoinen kysymys liittyy aluevalvontaan ja täysivaltaisuuteen. Aluevalvontalaki (2000/755) määrittää maa- ja merialueen sekä ilmatilan valvonnasta. Lain keskeiset käsitteet ovat alueellisen koskemattomuuden valvonta ja turvaaminen. Valvonnalla tarkoitetaan rajoilla tapahtuvaa valvontaa aluerikkomusten ja -loukkausten ehkäisemiseksi ja selvittämiseksi. Turvaamisella puolestaan tarkoitetaan Puolustusvoimien tai muiden aluevalvontaviranomaisten voimankäyttöä tai muita toimenpiteitä aluelouk-kausten estämiseksi tai torjumiseksi. Laki mm. rajoittaa valtionalusten ja -ilmaalusten tai sotilasosastojen tuloa Suomen alueelle. Puolustusministeriö johtaa toimintaa, ellei toimivalta ole tasavallan presidentillä. Puolustusvoimat huolehtii aluevalvonnan toimeenpanosta ja viranomaisten yhteistoiminnasta sekä kokoaa tilannekuvaa.

Kansainvälisen oikeuden pätevyydestä kybertoimintaympäristössä vallitsee melko yksimielinen näkemys. Kuitenkin eri valtioilla on eriäviä näkemyksiä siitä, voiko kybertoimintaympäristössä tehtävä loukkaus yksin rikkoa valtion itsemääräämisoikeutta vastaan. Suomi on yksi niistä valtioista, joiden mukaan voi, mutta esimerkiksi Iso-Britannian kanta on toinen. Sen mukaan kyberoperaatio ei voi yksin loukata itsemääräämisoikeutta, vaikka se voikin olla voimankäyttöä tai muu kansainvälisesti tuomittava teko. (Cyber Law Toolkit, 2021)

Vaikka ulkoministeriö onkin em. Suomen kannan esittänyt (Ulkoministeriö, 2021c), ei se näy kansallisessa lainsäädännössä. Tämä myös tarkoittaa sitä, että millään viranomaisella ei ole velvoitetta tai toimivaltaa valvoa kansallista kybertoimintaympäristöä niiltä osin, kuin kyse on jostain muusta kuin viranomaisen omista tietoliikennejärjestelyistä tai tietojärjestelmistä.

5.3 Tietoturvallisuustoimenpiteet arjen turvana

5.3.1 Julkisuusperiaate ja salassapito

Julkisuuslain (1999/621) mukaan kolme keskeistä käsitettä ovat asiakirja, julkisuusperiaate ja salassapito. Asiakirja voi olla kirjallinen tai kuvallinen esitys, mutta myös yhteenkuuluvista merkeistä muodostuva tietty kohde tai asiaa koskeva viesti, joka saadaan selville vain automaattisen tietojenkäsittelyn tai muun apuvälineen avulla. Viranomaisen asiakirja puolestaan on asiakirja, joka on viranomaisen hallussa ja jonka on laatinut viranomainen tai sen palveluksessa oleva tai joka on toimitettu viranomaiselle. Lähtökohtaisest viranomaisen asiakirja on julkinen ja kellä tahansa on oikeus saada siitä tieto. Vastaavasti salassa pidettävästä asiakirjasta saa antaa tiedon vain, mikäli laissa niin säädetään. Joissain tilanteissa asiakirja voi olla harkinnanvaraisesti annettava, mikäli luovuttaminen on viranomaisen harkittavissa lain perusteella tai asiakirjaan sisältyviä tietoja saa käyttää vain tiettyyn tarkoitukseen (1999/621, 16 a §).

Asiakirjasalaisuudella tarkoitetaan sitä, että salassa pidettävää asiakirjaa ei saa näyttää, eikä antaa sivulliselle. Asiakirja on pidettävä salassa, mikäli se on säädetty pidettäväksi salassa tai viranomainen on määrännyt asiakirjan salassa pidettäväksi (Laki 1999/621, 22 §). Viranomainen voi antaa tiedon salassa pidettävästä asiakirjastaan mm., mikäli tiedon antamisesta on laissa säädetty, kyse on virka-avun antamisesta tai viranomaisen toimeksiannosta tehtävästä työstä. Huomattavaa on, että viranomainen ei voi antaa salassa pidettävää asiakirjaa toiselle viranomaisellekaan ilman hyväksyttävää perustetta (Laki 1999/621, 29 §).

Julkisuuslaki määrittelee (1999/621, 24 §) yhteensä 33 kohtaa perusteina sille, missä tapauksissa asiakirja on salassa pidettävä. Perusteet liittyvät ulkosuhteisiin, sisäiseen turvallisuuteen, maanpuolustukseen, turvallisuusjärjestelyihin, esitutkintaan, yksityiseen liikesalisuuteen ja moneen muuhun asiaan. Tiedonhallintalaki (2019/906, 18 §) määrää edelleen, että valtion viranomaisen ja tiettyjen muiden toimijoiden on turvallisuusluokiteltava asiakirjansa ja tehtävä asiakirjoihin vastaava merkintä osoittaakseen, minkälaisia tietoturvallisuustoimenpiteitä asiakirjan käsittelyssä on noudatettava. Turvallisuusluokituksesta säädetään edelleen valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (2019/1101). Asetuksen perusteella turvallisuusluokkia on neljä sen perusteella, minkälaista vahinkoa asiakirjaan sisältyvän tiedon oikeudeton paljastaminen tai käyttö aiheuttaisi. Asetusta sovelletaan myös kansainvälisten tietoturvallisuusvelvoitteiden perusteella turvaluokiteltuihin asiakirjoihin, ellei kansainvälisistä tietoturvallisuusvelvoitteista annettu laki (2004/588) muuta määrää. Taulukossa 3 on esitetty turvallisuusluokat ja niiden perusteella tehtävät merkinnät. Merkinnät tehdään ruotsiksi ruotsinkielisinä laadittuihin tai ruotsiksi käännettyihin. Englanninkielinen merkintä osoittaa vastaavuuden, ellei asiasta ole säädetty jotain muuta, kuten on Naton osalta sen kanssa laaditun valtiosopimuksen (Valtioneuvoston asetus, 2013/8) perusteella. Euroopan unionin kanssa

tehdyn valtiosopimuksen (Valtioneuvoston asetus, 2015/77) perusteella turvallisuusluokittelu poikkeaa jonkin verran kansallisesta ja Naton luokittelusta. Tämä on kuvattu taulukossa 4.

TAULUKKO 3: Kansalliset ja Naton turvallisuusluokat (Valtioneuvoston asetukset 2019/1101 ja 2013/8)

Turvallisuusluokka	**Kuvaus**	**Merkintä**
TL I	tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa	ERITTÄIN SALAINEN YTTERST HEMLIG TOP SECRET
TL II	tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa	SALAINEN HEMLIG SECRET NATO SECRET
TLIII	tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa	LUOTTAMUKSELLINEN KONFIDENTIELL CONFIDENTIAL NATO CONFIDENTIAL
TLIV	tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG RESTRICTED NATO RESTRICTED

TAULUKKO 4: EU turvallisuusluokitukset (Valtioneuvoston asetus 2015/77)

Kuvaus	Merkintä
Tieto tai aineisto, jonka luvaton ilmitulo saattaisi vahingoittaa poikkeuksellisen vakavasti Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja	TRES SECRET UE / EU TOP SECRET
Tieto tai aineisto, jonka luvaton ilmitulo saattaisi vahingoittaa vakavasti Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja	SECRET UE / EU SECRET
Tieto tai aineisto, jonka luvaton ilmitulo saattaisi vahingoittaa Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja	CONFIDENTIEL UE / EU CONFIDENTIAL

Tieto tai aineisto, jonka luvattomasta ilmitulosta saattaisi olla haittaa Euroopan unionin tai yhden tai useamman jäsenvaltion eduille	RESTREINT UE / EU RESTRICTED

Naton ja EU:n kanssa solmitut valtiosopimukset eivät määritä yksityiskohtaisia tietoturvallisuusvaatimuksia, vaan vaatimukset on esitetty erillisissä asiakirjoissa. Kansallinen turvallisuusviranomainen on edelleen antanut ohjeen nimenomaisesti EU:n ja Naton turvallisuusluokiteltujen asiakirjojen käsittelyvaatimuksista (Ulkoministeriö, 2021b).

5.3.2 Tietoturvallisuuden hallinta

Tiedonhallintalaki (2019/906) määrittelee vastuulliseksi toimijaksi tiedonhallintayksikön, joka on esimerkiksi virasto tai laitos. Tiedonhallintayksikön johdon tulee huolehtia vastuiden määrittelystä, ajantasaisista ohjeista, koulutuksesta ja riittävästä osaamisesta, tarkoituksenmukaisista työkaluista sekä riittävän valvonnan järjestämisestä.

Tiedonhallintalaki (2019/906, 4-5 §) määrittää erityisen tiedonhallintamallin, jota tiedonhallintayksikön tulee ylläpitää. Mallin tulee sisältää tiedot toimintaprosesseista, tietovarannoista sekä niihin kuuluvista henkilötiedoista, arkistoinnista ja tuhoamisesta, tietojärjestelmistä ja niistä vastaavista viranomaisista sekä liitynnöistä muihin tietojärjestelmiin. Mikäli tiedonhallintayksikkö toteuttaa sellaisia muutoksia toimintaan tai ottaa käyttöön uusia tietojärjestelmiä, jotka vaikuttavat vastuisiin tai mallin sisältöihin oleellisesti, tulee muutokset vaikutuksineen arvioida. Muutosten vaikutukset tulee arvioida myös uusien säädösten valmistelussa ministeriötasolla.

Tietoturvallisuuden osalta tiedonhallintalaki asettaa vaatimuksia mm. erityistä luotettavuutta edellyttävien tehtävien tunnistamiseksi (Laki 2019/906, 12 §). Näissä tehtävissä toimivista laaditaan henkilöturvallisuusselvitys turvallisuusselvityslain (2014/726) tai kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (2004/588) mukaisesti. Huomattavaa on, että viranomaisen tulee henkilöturvallisuusselvitystä hakiessaan huolehtia siitä, että se rajoittaa pääsyä suojattaviin tietoihin ja huolehtii tilojensa ja tietojärjestelmiensä suojaamisesta sekä toteuttaa muita asianmukaisia turvallisuustoimenpiteitä (Laki 2014/726, 18 §). Turvallisuusselvitys laaditaan suppeana, perusmuotoisena tai laajana riippuen tehtävästä, jossa selvityksen kohde toimii. Turvallisuusselvitys toimii perustana käsittelyoikeuksien myöntämiselle, mistä on säädetty turvallisuusluokitusasetuksessa (Asetus 2019/1101). Sen perusteella käsittelyoikeudet tulee myöntää työtehtävien ja niihin liittyvän tarpeen perusteella. Turvallisuusluokkien III, II ja I käsittelyoikeuksista tulee pitää ajantasaista luetteloa.

Lähtökohtaisesti tiedonhallintayksikön tulee mitoittaa tietoturvallisuustoimenpiteet tietojenkäsittelyyn kohdistuvien arvioitujen riskien perusteella (Tiedonhallintalaki, 2019/906, 13 §), mikä tulee suhteuttaa

omaan toimintaympäristöön ja sen tietoturvallisuuden tilaan. Toiminnan kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on testattava säännöllisesti. Julkisuusperiaatteen mukaisesti tietojärjestelmät tulee suunnitella niin, että asiakirjojen julkisuus voidaan toteuttaa ja toisaalta hankinnoissa tulee varmistaa riittävät tietoturvallisuustoimenpiteet, jotka vaihtelevat käsiteltävän aineiston turvallisuusluokkien mukaisesti. Turvallisuusluokitusasetuksen (2019/1101) mukaisesti tiedonhallintayksikön tulee toteuttaa tietojärjestelmän, tietoliikennejärjestelyn sekä turvallisuusalueen osalta ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä sekä toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi ja edelleen tilanteen palauttamiseksi ennalleen.

Turvallisuusalueilla tarkoitetaan hallinnollisia- ja turva-alueita, joille pääsyä säädellään (Asetus 2019/1101). Turvallisuusalueilla myöskin suojellaan asiakirjojen käsittelyä ja tietojärjestelmiä niin, että korkeampien turvallisuusluokkien asiakirjoja saa käsitellä ja tietojärjestelmät sijoittaa vain turva-alueille, joille on pääsy vain erityisellä luvalla. Tästä voidaan poiketa, mikäli hajasäteilyä vähennetään.

Tietoaineistojen turvallisuudesta tulee huolehtia niiden koko elinkaaren ajan huolehtimalla mm. muuttumattomuuden riittävältä suojaamisesta, teknisiltä ja fyysisiltä vahingoilta suojaamisesta, saatavuuden ja käyttökelpoisuuden varmistamisesta sekä alkuperäisyyden, ajantasaisuuden virheettömyyden varmistamisesta (Tiedonhallintalaki, 2019/906). Tiedonhallintalaki edellyttää, että tietojen siirtäminen tapahtuu salattuna, mikäli salassa pidettäviä tietoja siirretään yleisessä tietoliikenneverkossa. Turvallisuusluokiteltuja tietoja saa siirtää vastaavalla tavalla, mutta asetus (2019/1101) määrittelee niiden siirtämisestä tarkemmin ottaen huomioon turvallisuusalueet [14] ja alempien turvallisuusluokkien ratkaisut. Mikäli tietoaineistoja kuljetetaan turvallisuusalueiden ulkopuolella, tulee ne suojata riittävällä salauksella. Tiedonhallintalaki (2019/906, 17 §) edellyttää, että tietojärjestelmien käytöstä ja tietojen luovutuksesta on kerättävä tarpeelliset lokitiedot tietojen käytön ja luovutuksen seurantaa varten. Turvallisuusluokitusasetus puolestaan edellyttää, että turvallisuusluokitellun tiedon osalta tulee noudattaa turvallisuusluokasta riippuen seurantaa eri tavoin asiakirjojen käsittelystä. Turvallisuusluokkien III-I asiakirjojen osalta käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään tai itse asiakirjaan ja asiakirjan lähettäminen sekä vastaanottaminen on rekisteröitävä. Korkeimpien turvallisuusluokkien II-I asiakirjoja ei saa kopioida ilman laatijan lupaa ja kopiot käsittelijöineen on luetteloitava.

Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset ovat yleisellä tasolla (Asetus 2019/1101). Vaatimukset kohdentuvat eri turvallisuusluokkien mukaisten tietojärjestelmien ja tietoliikenneratkaisujen erotteluun, haittaohjelmilta suojautumiseen, käyttäjille annettaviin oikeuksiin, tiedon eheyden varmistamiseen, tietojärjestelmien ja niiden käyttäjien

[14] Turvallisuusasetuksen kyseinen kohta on epäselvä, koska turvallisuusalueet käsittävät sekä hallinnolliset-, että turva-alueet

tunnistamiseen, toiminnallisuuksien rajaamiseen ja salausratkaisujen riittävään turvallisuuteen turvallisuusluokittain. Edelleen edellytetään turvallisuusluokkien III-I osalta riskien vähentämistä hajasäteilyn ja elektronisen tiedustelun osalta.

Viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista säädetään lailla (2011/1406), minkä lisäksi kansainvälisistä tietoturvallisuusvelvoitteista säädetään erikseen (2004/588). Kansallisesti säädetään edelleen omalla lailla tietoturvallisuuden arviointilaitoksista (Laki tietoturvallisuuden arviointilaitoksista, 2011/1405). Missään näistä laeista ei säädetä täsmällisiä vaatimuksia, vaan todetaan yleisesti, mistä vaatimukset voivat muodostua. Lain tasolla ei myöskään velvoiteta viranomaista arvioituttamaan ratkaisujaan, vaan lait määrittävät käytännössä sen, kuka arvioinnin voi tehdä. Arviointi voi perustua (Laki 2011/1406) lailla tai asetuksella säädettyyn vaatimukseen ja valtiovarainministeriön ohjeeseen, kansallisen turvallisuusviranomaisen ohjeeseen, EU :n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, yleisesti tai alueellisesti sovellettuihin säännöksiin, määräyksiin tai ohjeisiin sekä vahvistettuun standardiin. Liikenne- ja viestintävirastolla (Kyberturvallisuuskeskus) on keskeinen rooli arviointien toteuttajana tai vastaavasti arviointilaitosten hyväksyjänä. Kyberturvallisuuskeskus voi myös pyydettäessä antaa todistuksen vaatimuksenmukaisuudesta. Näihin verrattuna laissa (2011/1406) oleva maininta siitä, että Viestintävirasto (nykyisin liikenne- ja viestintävirasto) toteuttaa tehtävät käytössään olevien voimavarojen ja resurssien (HE 45/2011 vp) mukaisesti, tuntuu erikoiselta. Laki (2011/1406, 4 § 3 mom) viittaa tarkastusten osalta kansainvälisten tietoturvallisuusvelvoitteiden ensisijaisuuteen sekä toisaalta siihen, että viranomaisten tietojärjestelmiä tarkastettaessa tulisi tarkastamisella olla yleistä tietoturvallisuutta edistävää vaikutusta.

Laki sähköisen viestinnän palveluista (2014/917, 17-18 luku) velvoittaa myös viranomaisia viestinnän luottamuksellisuuden ja yksityisyydensuojan osalta. Tämä liittyy oikeuteen käsitellä viestejä tai niihin liittyviä välitystietoja mm. väärinkäytösten selvittämiseksi. Tieto- ja kyberturvallisuuden osalta lain 272 § määrittää viranomaiselle tai palveluntuottajalle toimivallan huolehtia tietoturvallisuudesta mm. viestien sisällön selvittämällä, viestien välittämistä tai vastaanottamista rajoittamalla tai sen estämällä ja haittaohjlemien automaattisella poistamisella. Myös muut vastaavat teknisluonteiset toimenpiteet ovat mahdollisia, mikä tarkoittaa sitä, että toimivalta on käytännössä se, jota normaali viranomainen voi käyttää. Toimivalta ei ole suoraan viranomaisella, vaan viestinnän välittäjällä. Jos viranomainen ei itse toimi viestinnän välittäjänä, toimivalta on sen lukuun toimivalla palveluntuottajalla.

5.3.3 Yhteisten palvelujen käyttövelvoite

Valtionhallinnon viranomaisen on käytettävä Valtorin palveluja. Tähän velvoittaa valtiovarainministeriön hallinnonalaan kuuluvat lait valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (2013/1226), julkisen hallinnon turvallisuusverkkotoiminnasta annettu laki (2015/10), talousarviolaki (1988/423) sekä laki Valtion talous- ja henkilöstöhallinnon palvelukeskuksesta (2019/179).

TORI-lain (2013/1226) perusteella yhteisiä tieto- ja viestintäteknisiä palveluita ovat yhteiset perustietotekniikkapalvelut ja yhteiset tietojärjestelmäpalvelut (2013/1226, 2 §). Perustietotekniikkapalveluilla tarkoitetaan laitteita, ohjelmistoja, tietoliikenne- ja viestintäpalveluja sekä tarvittavia infrastruktuuri- ja tukipalveluja, jotka on yksityiskohtauisesti määritelty valtioneuvoston asetuksessa valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (2014/132). Asetuksen perusteella konesali- ja kapasiteettipalvelut kuuluvat yhteisiin palveluihin, mikä edelleen luo perusteet sille, että viranomaisen toimialasidonnaiset (TOSI) tietojärjestelmät on ilman erillistä poikkeusta sijoitettava palvelua tarjoavan palvelukeskuksen ylläpitoon.

Yhteiset tietojärjestelmäpalvelut puolestaan ovat tietojärjestelmiä ja niillä tuotettavia palveluita, joilla tuetaan julkisen hallintotehtävän tai samankaltaisen toiminnan toteuttamista. Tietojärjestelmäpalvelut on eritelty asetuksessa (2014/132). Näistä voidaan mainita talous- ja henkilöstöhallinnon tietojärjestelmäpalvelut, joiden keskittämisestä talous- ja henkilöstöhallinnon palvelukeskukseen säädetään talousarviolaissa (1988/423) ja toisaalta palvelukeskuksesta annetussa laissa (2019/179). Jälkimmäisen perusteella palvelukeskuksella on yhteisrekisterinpitäjyys asiakasvirastojen kanssa niistä tiedoista, joita se käsittelee tietojärjestelmissään. Samalla palvelukeskukselle on määritetty selkeä vastuu tietojärjestelmien käytettävyydestä ja tietojen eheydestä, suojaamisesta ja säilyttämisestä, vaikka järjestelmissä olevat tallenteet ovatkin asiakkaiden asiakirjoja.

TORI-laki puolestaan ottaa kantaa tietoturvallisuuteen hyvin yleisellä tasolla. Lain 2 § 3 momentin perusteella yhteisten palvelujen on täytettävä tarpeen mukaiset tietoturvallisuus- ja varautumisvaatimukset. Laki tarkentaa asiaa varautumisen ja häiriötilanteiden osalta hieman 15 § :ssä, jonka perusteella palveluntuottajien on huolehdittava siitä, että toiminta ja palvelujen tuotanto jatkuvat mahdollisimman häiriöttömästi myös poikkeusoloissa. Asiaa ei tarkenneta myöskään asetuksessa (2014/132), joka velvoittaa kuitenkin palveluntuottajia käyttämään laadunhallintaa palvelujen laadun, palvelutasojen ja kustannustehokkuuden jatkuvaan kehittämiseen. TORI-lakia koskevassa hallituksen esityksessä (HE 150/2013 vp, s. 29) todetaan, että valtiovarainministeriön johdolla ohjataan palvelutuotantoa siten, että palvelujen laatu on varmistettu ja todennettu. Edelleen samaisessa perustelussa todetaan, että ohjaamisessa kiinnitetään erityinen huomio mm. siihen, että palvelut ovat tietoturvallisia ja varautumisvaatimusten mukaisia.

Julkisen hallinnon turvallisuusverkkotoiminnasta annettu laki on hallituksen esityksen perusteella erillislaki TORI-lain rinnalla ja molemmat erityislakeja, joita yleislakina ohjaa laki julkisen hallinnon tiedonhallinnasta (HE 54/2013 vp). TUVE-laki on erityisesti säädetty varmistamaan valtion ylimmän johdon ja turvallisuusviranomaisten ja muiden toimijoiden viestinnän häiriöttömyys ja jatkuvuus (2015/10, 1 §). Turvallisuusverkko on viranomaisverkko, joka täyttää korkean varautumisen ja turvallisuuden vaatimukset. Kun tarkastellaan hallituksen esityksestä (HE 54/2013 vp, s.35) tarkempaa määrittelyä, korkean turvallisuuden ja varautumisen vaatimuksilla tarkoitetaan toimintavarmuuden varmistamista ja jatkuvuuden turvaamista hallinnollisin, toiminnallisin ja teknisin ratkaisuin. Tätä tarkennetaan kuitenkin valtion omistuksella keskeisistä osista, fyysisellä murtosuojauksella ja suojalla asevaikutusta vastaan, varavoimalla, sähkömagneettisella suojauksella, verkkoliikenteen valvonnalla ja automaattisella reitityksellä, tietoliikenteen salauksella ja tietoturvavalvonnalla sekä henkilöstö- ja tilaturvajärjestelyillä.

Hallituksen esityksen (HE 54/2013 vp, s. 36) ja turvallisuusverkkotoiminnasta annetun valtioneuvoston asetuksen muutoksen (2020/442, 10 §) perusteella turvallisuusverkkotoiminnan tietoturvallisuusvaatimusten perusteella palvelut tulee toteuttaa niin, että ne täyttävät turvallisuusluokkien IV-II vaatimukset. Lisäksi palveluiden tulee tulee täyttää kansainväliselle erityissuojattavalle aineistolle asetetut tietoturvallisuusvaatimukset. Valtiovarainministeriö hyväksyy palvelut käyttöön varmistuttuaan niiden täyttävän vaatimukset riittäviltä osin ja kaikilta osin määräajan puitteissa (2020/442, 11). Kun kyse on käyttäjäorganisaation TOSI-palvelusta, tulee käyttäjän antaa selvitys palveluntuottajalle (Valtori) vaatimustenmukaisuudesta ennen kuin palvelu tai tietojärjestelmä voidaan liittää turvallisuusverkkoon.

Turvallisuusverkon käyttövelvoite koskee korkean turvallisuuden ja varautumisen vaatimuksia edellyttävää viranomaisten sisäistä ja välistä yhteistoimintaa ja viestintää (TUVE-laki, 2015/10, 2 §). Viranomaisten toimintoina tämä tarkoittaa valtion johtamista ja turvallisuutta, maanpuolustusta, yleistä järjestystä ja turvallisuutta, rajaturvallisuutta, pelastustoimintaa, meripelastustoimintaa, hätäkeskustoimintaa, maahanmuuttoa ja ensihoitopalvelua. Edellä olevan perusteella käyttöön velvoitetut viranomaiset on varsin helppo nimetä Tullia lukuun ottamatta. Laki mahdollistaa turvallisuusverkon käytön myös muille toimijoille, mikäli heidän toimintansa liittyy edellä kuvattuihin toimintoihin.

5.3.4 Viranomaisten tarjoamat palvelut

Laki sähköisestä asioinnista viranomaistoiminnassa (2003/13) säätää viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. Tietoturvallisuuden osalta vaatimukset viranomaiselle koskevat päätösasiakirjan sähköistä allekirjoittamista ja sähköistä tiedonantoa,

mutta toisaalta vaatimuksena voidaan pitää sitäkin, että asiakkaan ei tarvitse allekirjoittaa sähköistä asiakirjaa, jos asiakirjasta ilmenevät tiedot lähettäjästä, eikä asiakirjan alkuperäisyyttä tai eheyttä tarvitse epäillä. Päätösasiakirja voidaan allekirjoittaa sähköisesti EU asetuksen vaatimukset täyttävällä kehittyneellä allekirjoituksella tai muulla tavalla, joka mahdollistaa varmistumisen asiakirjan alkuperästä ja eheydestä (Laki 2003/13, 16 §). Todisteellista luovutusta edellyttävä asiakirja voidaan asianosaisen susotumuksella antaa tiedoksi sähköisesti ilmoittamalla, että asiakirja on noudettavissa palvelimelta, tietokannasta tai muulla tavoin. Asiakirjan noutajan on tunnistauduttava todisteellisesti.

Viranomaisen tulee suunnitella ja ylläpitää digitaaliset palvelunsa niin, että tietoturvallisuudesta, tietosuojasta, löydettävyydestä ja helppokäyttöisyydestä on varmistuttu (Laki digitaalisten palvelujen tarjoamisesta, 2019/309). Lakia koskevan hallituksen esityksen (HE 60/2018 vp) perusteella tietoturvallisuudesta varmistuminen tarkoittaa jo suunnitteluvaiheessa arviointia siitä, miten tietoturvallisuus aiotaan järjestää. Tietoturvallisuus tulee kyetä osoittamaan suunniteludokumentaatiolla ja testausraporteilla. Laki määrittää edelleen, että viranomaisen tulee huolehtia palvelun saatavuudesta muutoinkin kuin virka-aikana. Muille palveluja tarjoavan viranomaisen tulee huolehtia sähköisten tiedonsiirtomenetelmien saatavuudesta vastaavalla tavalla.

Viranomaisen tulee digitaalista palvelua tarjotessaan antaa jokaiselle mahdollisuus asioida digitaalisen palvelun tai sähköisen tiedonsiirtomenetelmän avulla (Laki 2019/309, 5 §). Jokaisella on oltava mahdollisuus käyttää valtion yhteistä viestinvälityspalvelua tai muuta riittävän tietoturvallista tiedonsiirtomenetelmää. Sähköistä tunnistautumista saa vaatia vain, mikäli se on tarpeen tietosisältöön liittyvän käyttöoikeuden varmistamiseksi tai palvelun käyttöön liittyvien oikeusvaikutusten takia. Mikäli palveluun liittyy salassa pidettävää tietoa, tulee käyttäjä tunnistaa vahvasti.

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (2016/571) velvoittaa viranomaista yhteisten tukipalvelujen käyttöön. Tukipalvelut muodostuvat yhdeksästä palvelusta, joista pääosaa tuotta Digi- ja väestötietovirasto. Valtiokonttori ja Maanmittauslaitos tuottavat kumpikin yhtä palvelua. Palveluihin kuuluu :

1. Tiedonvälityskanava käyttäjäorganisaatioille (kansallinen palveluväylä), DVV
2. Käyttäjäorganisaatioiden palvelukuvaukset (palvelutietovaranto), DVV
3. Käyttäjän rekisteritietojen palvelunäkymä, DVV
4. Luonnollisen henkilön tunnistuspalvelu, DVV
5. Muut kuin vahvaan tunnistamiseen perustuvat tunnistamispalvelut, DVV
6. Asiointivaltuutuspalvelu, DVV
7. Viestinvälityspalvelu, DVV
8. Verkkomaksamisen kokoamis- ja hallinnointipalvelu, VK
9. Hallinnon karttapalvelu, MML.

Tukipalvelujen osalta palveluntuottaja vastaa tuottamiensa palveluiden laadusta, toimintavarmuudesta, käyttäjäystävällisyydestä ja tarvittavien tietojen yhdistämisen oikeellisuudesta sekä niiden käsittelyn tietoturvallisuudesta (Laki 2016/571). Palveluntuottajalta edellytetään lisäksi palvelujensa osalta hyvää teknistä laatua ja tietoturvallisuutta, kestävyyttä ulkoisilta häiriöiltä ja tietoturvauhkilta, laadun ja toimintavarmuuden seurantaa sekä sitä, että siihen kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat voidaan havaita. Vaatimuksia voidaan pitää jossain määrin erikoisina, koska esimerkiksi uhkan havaitseminen ennalta on vaikeaa, ellei jopa mahdotonta. Hallituksen esityksen (HE 59/2016 vp) perusteella esimerkiksi haittaohjelmatartunnat ja palvelunestohyökkäykset, jotka ovat asiantuntemuksella ja ammattitaidolla ennakoitavissa, eivät saisi vaikuttaa palvelun toimivuuteen. Tietoturvaloukkausten ja uhkien havaitsemisella halutaan asettaa vaatimuksia palveluntuottajalle. Merkittävinä tietoturvaloukkauksina mainitaan käyttäjätietojen päätyminen vääriin käsiin tai palvelun eheyden menettäminen. Uhkien osalta esimerkkinä käytetään teknistä haavoittuvuutta.

Laki (2016/571, 17 §) asettaa vaatimuksia palvelujen tuottamisessa käytettäville tietojärjestelmille. Perusvaatimuksen tietojärjestelmän tulee mm. toimia tietoturvallisuutta ja tietosuojaa koskevien lakien ja niiden perusteella annettujen muiden säännösten ja määräysten mukaisesti. Tukipalvelun tulee toteuttaa niin, että sitä voidaan käyttää perustason tai korotetun tason vaatimukset täyttävässä tietojenkäsittely-ympäristössä[15]. Lain perusteluissa (HE 59/2016 vp, s.59) todetaan, että palveluntuottajan tulee tarkoituksenmukaisella tavalla varmistua tietojärjestelmän tietoturvallisuudesta. Se voisi tehdä tämän itse tai pyytää ulkoista arviointia ja valtiovarainministeriö voisi ohjata palveluntuottajaa pyytämään ulkoisen arvioinnin. Tukipalvelun tuottaja voi puolestaan edellyttää käyttäjäorganisaatiolta sen tietojärjestelmän testaamista ja todentamista tietoturvallisuuden ja laadun osalta ennen liittämistä tukipalveluun.

[15] Perustaso ja korotettu taso viittaavat kumottuihin säädöksiin, jotka määrittivät suojaustasot. Perustasolla tarkoitetaan suojaustasoa IV ja korotetulla tasolla suojaustasoa III (Vahti-ohje 3/2012, Teknisen ICT-ympäristön tietoturvataso-ohje)

6 VALTIONHALLINNON TIETO- JA KYBERTURVALLISUUDEN HALLINTA

Luvussa selitetään tutkimustulokset sekä vastataan tutkimusongelmiin ja kytketään tulokset aikaisempaan tutkimukseen. Luvussa esitetään tulosten perusteella muodostettu uusi teoria aiheeseen. Tulosten luotettavuutta, merkittävyyttä, teoreettisia ja käytännöllisiä hyötyjä sekä tulosten yleistettävyyden rajoitteita pohditaan. Tämän pohjalta esitetään jatkotutkimusaiheita.

6.1 Laki sallii, oikeuttaa tai velvoittaa

Strategisella tasolla valtioneuvostossa kukin ministeriö vastaa oman hallinnonalansa kyber- ja tietoturvallisuudesta. Pääministeri johtaa valtioneuvoston toimintaa, joten varsin luontevasti valtioneuvoston kanslian tehtävänä on häiriötilanteiden koordinointi myös tieto- ja kyberturvallisuuden osalta. Valtioneuvoston tilannekeskuksen tehtävä on muodostaa ja jakaa tilannekuvaa ja Turvallisuuskomitea tukee poikkihallinnollisesti valtioneuvostoa normaalioloissa varautumisessa yhteistoimintaelimenä ja valmistautuu häiriötilanteissa toimimaan asiantuntijaelimenä. Huomattavaa on kuitenkin se, että normaalitilanteessa selkeää johtovastuuta ei ministeriöiden välillä ole. Toimintaa yhteensovitetaan kansliapäällikkökokouksessa, jota tukee häiriötilanteissa valmiuspäällikkökokous. Valmiuslain toimivaltuudet antavat liikenne- ja viestintäministeriölle sekä valtiovarainministeriölle selkeän mahdollisuuden säädellä toimintaa erityisillä toimivaltuuksilla, mikä edellyttää kuitenkin poikkeusolojen toteamista. Normaalioloissa viranomaisia koskeva sääntely on pääosin valtiovarainministeriön ja osin liikenne- ja viestintäministeriön toimivallassa. Jälkimmäisen sääntely suuntautuu kuitenkin yleistä regulaatiota lukuun ottamatta merkittävissä määrin muihin toimijoihin kuin viranomaisiin. Laki sähköisen viestinnän palveluista määrittää kuitenkin viranomaistenkin osalta toimivallan tieto- ja kyberturvallisuuden tekniseen valvontaan.

Vajaassa kymmenessä vuodessa lainsäädäntö ei näytä kehittyneen siten, kuin kyberturvallisuusstrategiassa vuonna 2013 esitettiin, eikä kyberturvallisuuden osalta ole säädetty eheää lainsäädännöllistä kokonaisuutta, joka sovittaisi eri viranomaisten toiminnan selkeästi yhteen strategisesti tai operatiivisesti. Kansallisessa lainsäädännössä kyberturvallisuuden ongelmana on sen puuttuminen käsitteenä lainsäädännöstä. Vaikka kyberturvallisuus perustuu tietoturvallisuuteen, on sillä oma erityinen merkityksensä mahdollisten fyysisen maailman vaikutusten kannalta. Terminologisesti olisi selkeämpää, mikäli käsite esiintyisi myös lainsäädännössä, eikä vain poliittisina tahdonilmauksina valtioneuvoston periaatepäätöksissä, jotka ovat aina kulloinkin istuvan hallituksen tuotteita, vaikka myöhemmätkin hallitukset voivat edelleen pitää periaatepäätökset

voimassa. Kokemus tosin on osoittanut, että periaatepäätösten varassa turvallisuudesta huolehtiminen voi olla valikoivaa.

Kyberturvallisuuteen liittyy Suomessa olennaisesti yhteiskunnan elintärkeät toiminnot, joihin käsitteellisesti liittyy kansallinen turvallisuus. Nämä on otettu huomioon uusimmassa lainsäädännössä, jota edustavat tiedustelulait. Lait edustavat selkeästi yhtenäistä valmistelua ja sitä kautta myös poikkihallinnollisuutta. Tämä osaltaan osoittaa sen, että lainsäädäntö kehittyy ajassa ja uudet uhkakuvat muokkaavat lainsäädäntöä. Toisaalta voidaan myös todeta, että siviili- ja sotilastiedustelu ovat luonteeltaan samaa toimintaa, jota toteuttavat eri kohteisiin eri viranomaiset. Tästä näkökulmasta lakien ja toiminnan yhteensovittaminen on varsin luontevaa. Tutkimuksen perusteella ei pysty varmasti selittämään sitä, miksi muuta lainsäädäntöä ei ole kehitetty kyberturvallisuusstrategian mukaisesti. Huomionarvoista on kuitenkin se, että tiedustelulakienkin osalta selvitysvaiheessa liikenne- ja viestintäministeriö esitti eriävän mielipiteensä tietoliikennetiedustelusta ja sen mahdollisesta loukkaavuudesta yksityisyyden suojaa kohtaan, mikä sittemmin johtikin perustuslain muuttamiseen. Alustavasti voidaan kuitenkin pohtia, mikä merkitys on sillä, että yksityisyyden suojasta viestinnässä säädetään liikenne- ja viestintäministeriön toimivaltaan kuuluvassa lainsäädännössä.

Poikkihallinnollisuuden puute näkyy yhdessä terminologian vajavaisuuden kanssa erityisesti viranomaisten välisessä tiedonvaihdossa ja virka-avussa. Salassa pidettävän tiedon luovuttaminen edellyttää aina laissa todettua erityistä perustetta ja virka-apu edellyttää myös oman määrittelynsä sen osalta, mitä ja kenelle voidaan tarjota. Näiden osalta eri hallinnonalojen osalta on eroja tarkkuudessa, jolla perusteet on kirjattu. Joiltain osin tiedonluovutusvelvoitteet tai oikeudet vastaanottaa tietoa on kirjattu varsin yleisesti kuten ”lakisääteisiin tehtäviinsä liittyen”. Toisessa tapauksessa taas kirjaus saattaa olla hyvin yksityiskohtainen, mikä saattaa olla tarkkarajainen ja täsmällinen, mutta samalla sulkee pois mahdollisuuksia. Tältä osin kyse lienee tarkoituksellisuudesta, koska lait tulee kirjoittaa tarkkarajaisesti ja täsmällisesti.

Nykyisen lainsäädännön puitteissa tietoturvallisuuden tai kyberturvallisuuden valvontaan liittyvät toimet on rajattu palveluntuottajille (viestinnän välittäjälle) olkoon kyseessä viranomainen tai sen lukuun toimiva muu taho. Tämä korostaa Valtorin, sen alihankkijoiden ja turvallisuusverkon osalta Erillisverkkojen keskeistä merkitystä tietoturvallisuuden valvonnassa.

Tietoturvallisuuden taso on viime kädessä poliittinen päätös, mikä näkyy myös viranomaisen tietoturvallisuutta käsittelevässä lainsäädännössä. Toisaalta julkisen hallinnon keskeinen periaate Suomessa on julkisuusperiaate. Julkisuuslain mukaisesti viranomaista velvoittaa vaatimus avoimuudesta ja asiakirjajulkisuudesta, mutta yhtä lailla velvoite salassa pidosta silloin, kun laki sitä edellyttää. Julkisuuslain näkökulmasta vaatimukset kohdistuvat nimenomaan yksittäiseen viranomaiseen ja sen asiakirjoihin toimien vaatimuksina tiedon käytettävyyden ja luottamuksellisuuden osalta.

Valtiovarainministeriö on keskeisessä roolissa viranomaisen tietoturvallisuuden osalta. Toimivaltansa mukaisesti se määrittää tiedonhallintalailla yleiset

velvoitteet tiedonhallinnalle ja edelleen useilla erillislaeilla velvoitteet tiettyjen valtion omien palvelukeskusten tuottamien palveluiden käyttöön. Tällä tavoin valtiovarainministeriö ottaa vastuun osaltaan viranomaisen tietoturvallisuudesta, koska viranomaisella ei ole mahdollisuuksia vaikuttaa erityisesti yhteisten palveluiden osalta niiden tietoturvallisuuteen tai riskienhallintaan kuin käyttäjien hallinnan osalta. Periaatteessa TOSI-palveluiden osalta voidaan sopimuksella sopia tietoturvallisuuden tasosta, mutta käytännössä tietojärjestelmäpalveluita käytetään kuitenkin palveluntuottaja ratkaisujen kautta. Näin ollen vaatimus riskiperusteisista tietoturvallisuustoimenpiteistä on jossain määrin teoreettinen. Palveluntuottajien osalta riskit tulisi olla yhteisten palvelujen osalta kaikilla käyttäjäorganisaatioilla yhteiset, mikä puolestaan edellyttää, että riskiarviot laaditaan yhdessä tai kaikki käyttävät palveluntuottajien antamia perusteita.

Turvallisuusverkon palveluiden osalta asetus säätää ja lain perustelut kuvaavat varsin tarkasti tietoturvallisuus- ja varautumisvaatimukset. Yhteisten tieto- ja viestintäteknisten palveluiden (TORI-palveluiden) osalta laki puolestaan toteaa vain tarpeen mukaisen tietoturvallisuuden tason, vaikka lain perusteluissa kuvataankin sitä, miten valtiovarainministeriö ohjaa palvelukeskusta tältä osin. Lain ja asetuksen tasolla ei kuitenkaan ole tietoturvallisuuden osalta kuvattuna vaatimustasoa. Laki asettaa eksplisiittisesti tarkoitukseksi parantaa palvelujen laatua ja yhteentoimivuutta sekä toisaalta kustannustehokkuutta ja ohjausta, mutta ei tietoturvallisuutta.

Tietoturvallisuuden vaatimuksenmukaisuus vaikuttaa analyysin perusteella veteen piirretyltä viivalta kansallisen tietoturvallisuuden osalta. Tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettu laki jättää varsin paljon vapausasteita sen osalta, mitä kriteerejä vasten arviointi toteutetaan. Arvioinnin toteutus puolestaan riippuu siitä, haluaako viranomainen teettää arvioinnin. Tämä voi johtaa siihen, että kaksi eri viranomaista pyytää arvioinnin toteuttamista eri kriteerien perusteella, jolloin kahden eri viranomaisen tietojärjestelmät voivat olla esimerkiksi turvallisuusluokan III vaatimusten mukaisia, mutta vaatimukset eivät ole samoja.

Kansainvälisten tietoturvallisuusvelvoitteiden osalta valtiosopimukset yksilöivät vaatimukset ja EU:n sekä Naton osalta on erikseen Kansallisen turvallisuusviranomaisen laatima soveltamisohje. Muiden maiden ja kansainvälisten järjestöjen kanssa tehtävä yhteistyö on tällä perusteella tärkeämpää, kun kansallinen tietoturvallisuus. Tämä voidaan nähdä luontevaksi yhteistyön edellyttämän luottamuksen takia. Mikäli tietojärjestelmiä ei arvioida yhteisten vaatimusten perusteella, johtaa se myös siihen, että vaatimuksia noudatettaessa eri vaatimukset edellyttävät myös eri tietojärjestelmiä. Vaatimuksia harmonisoimalla voitaisiin kenties saavuttaa hyötyjä ja vähentää käytettävien järjestelmien määrää.

6.2 Tulosten asemointi

Tutkimuksen pääongelmana oli "Miten kansallinen lainsäädäntö velvoittaa ja ohjaa valtionhallinnon viranomaisia tieto- ja kyberturvallisuuden osalta?"

Alaongelmana vastataan kysymykseen "Mitä eroa tieto- ja kyberturvallisuudella on lainsäädännössä?" Pelkistetysti voidaan todeta, että viranomaisen toiminta perustuu aina lainsäädäntöön. Kyberturvallisuus ero tietoturvallisuudesta siinä, että se ei käsitteenä esiinny lainsäädännössä, mutta eri viranomaiset lakisääteisiä tehtäviään valtakunnan tasolla toteuttaessaan samalla suojaavat yhteiskunnan elintärkeitä toimintoja ja toteuttavat kyberturvallisuustoimenpiteitä. Tietoturvallisuutta säädellään useilla eri laeilla julkisuusperiaatteen, tietoturvallisuudenhallinnan, palvelutuotannon sekä viranomaisten tarjoamien palvelujen osalta. Tutkimuksen perusteella valtionhallinnon viranomaisen näkökulmasta tieto- ja kyberturvallisuuden hallinta muodostuu strategisen tason ohjauksesta, joka kohdistuu operatiiviseen kyberturvallisuustoimintaan ja pävittäisen tietoturvallisuuden varmistamiseen tähtäävistä tietoturvallisuustoimenpiteistä. Näiden osalta vaatimustenmukaisuuden hallinta asettaa merkittävän määrällisen haasteen. Eritasoista sääntelyä on erittäin paljon ja toisaalta se jakautuu monelta osin kyseessä olevalle viranomaiselle sekä lain velvoittamana palveluja tuottavalle Valtorille.

6.2.1 Julkisen vallan käyttö on säänneltyä

Kaiken viranomaisen toiminnan perustana on lainsäädäntö, koska perustuslain mukaisesti julkisen vallan käytön tulee perustua lakiin ja siinä tulee tarkoin noudattaa lakia. Mäenpään (2020) mukaan tämä tarkoittaa viranomaiselle lainalaisuusperiaatteen noudattamista. Lainalaisuusperiaate rajoittaa vallan käyttöä ja antaa sille ennakoitavuutta sitomalla sen lainsäädäntöön. Vastaavasti lakisidonnaisuus tarkoittaa viranomaiselle sille laissa määrättyjen tehtävien toteuttamista, itseään koskevan sääntelyn noudattamista sekä toimimista muutoinkin lain määrittelemissä rajoissa.

Julkisen hallinnon keskeisiä periaatteita ovat avoimuus ja julkisuus. Tältä osin julkisuuslain lähtökohtana on julkisuus, mutta laki säätää yhtä lailla salassapidosta. Julkisuusperiaatteen mukaisesti kuka tahansa voi saada tiedon viranomaisen julkisesta asiakirjasta, mikä edellyttää tiedon käytettävyyttä. Vastaavasti salassapito edellyttää asiakirjalta luottamuksellisuutta ja eheyttä. Nämä havainnot liittyvät Voutilaisen (2006) mukaan hyvän hallinnon vaatimuksiin.

Suomalainen lainsäädäntö tieto- ja kyberturvallisuuden osalta on tämän tutkimuksen perusteella turvallisuutta painottava ja taktinen, kun sitä verrataan Johnsonin ym. (2014) tuloksiin. Lainsäädäntö painottaa hallinnollisiä, teknisiä ja fyysisiä turvallisuusvaatimuksia standardinmukaisuuden sijaan ja toimivalta on hallinnonaloilla. Suomalaisen lainsäädännön osalta on kuitenkin tarpeen ottaa huomioon se, että vaikka lainsäädännössäkin selkeitä vaatimuksia asetetaan, joiltain osin täsmällisten vaatimusten puute viranomaisten tietoturvallisuuden osalta on silmiin pistävää.

Vaatimusten puuttuminen linkittää tutkimuksen tulokset Mooren (2010) havaintoihin ex ante -periaatteen toimivuudesta. Mooren mukaan ennakoiva sääntely ei toimi tilanteissa, joissa viranomainen on epävarma sääntelyn

vaikutuksista. Sama voidaan todeta myös tilanteesta, jossa vaatimuksia ei ole, koska tällöin ennakoivaa sääntelyäkään ei ole.

Tutkimuksen perusteella perustuslakiin pohjautuva lainsäädäntö johtaa tieto- ja kyberturvallisuuden osalta valtioneuvoston strategisen tason toimijaksi vastaavalla tavalla, kuin millä tahansa muulla hallinnon osa-alueella. Normaalitilanteissa toimivaltuudet eivät osoita suoraa johtovastuuta millekään ministeriölle, vaan jokainen ministeriö säätelee tieto- ja kyberturvallisuutta omalla toimialallaan. Häiriötilanteissa koordinointivastuu on valtioneuvoston kanslialla ja poikkeusoloissa erityisiä toimivaltuuksia saavat liikenne- ja viestintäministeriö sekä valtiovarainministeriö. Strategisen johtajuuden osalta havainnot vastaavat Lehdon ym. (2018) tuloksia siitä, että selkeä strateginen johtajuus puuttuu ja hallinnonalat toimivat omina siiloinaan.

6.2.2 Kyberturvallisuutta koskeva sääntely kaipaa kehittämistä

Kyberturvallisuuden osalta lainsäädäntö ei ole tulosten perusteella kehittynyt vuoden 2013 kyberturvallisuusstrategiassa viitoitetulla tavalla, mikä vastaa Valtiontalouden tarkastusviraston havaintoa siitä, että strategian suosituksia on noudatettu vain siltä osin, kuin niitä on pidetty tarkoituksenmukaisina (VTV, 2017). Tätä tukee Lehdon ym. (2017) toteamus siitä, että lainsäädäntöä ei haluta kehittää pelkästään kyberturvallisuuden osalta, koska kyseessä on poikkihallinnollinen ilmiö. Koska lainsäädäntöä ei ole kehitetty, on tutkimuksen havainto johtamisen haasteesta normaalioloissa strategisella tasolla yhtenevä Lehdon ym. (2018) tuloksen kanssa strategisen johtajuuden puuttumisesta. Hallinnonalakohtainen siiloutuminen on edelleen säilynyt, koska poikkihallinnollista lainsäädäntöä ei ole tiedustelulakeja lukuun ottamatta laadittu. Tätä tukevat myös Lonkan ym. (2020) tulokset siitä, että poikkihallinnollisuutta arvostetaan, mutta se koetaan hyvin vaikeaksi.

Huolimatta lainsäädännön kehittymättömyydestä, on tietyillä turvallisuusviranomaisilla selkeitä lakiin perustuvia kyberturvallisuustehtäviä, jotka tässä tutkimuksessa nimettiin operatiiviseksi kyberturvallisuustoiminnaksi. Tälle toiminnalle on on yhteistä yhteiskunnan elintärkeät toiminnot ja niiden turvaaminen. Tutkimuksen perusteella vaikuttaa siltä, että viranomaisten yhteistoiminta ja tiedonvaihto eivät ole tarkoituksenmukaisella tasolla.

Edellä esitetyt havainnot ovat myös linjassa Lewallenin (2017) tulosten kanssa. Lewallen päätyi uusien teknologioiden osalta neljään keskeiseen haasteeseen. Näistä ensimmäinen liittyy epävarmuuteen toimivallan jaosta viranomaisten välillä ja sitä koskevaan mahdolliseen kilvoitteluun. Jonkinlainen kilvoitteluasetelma voidaan tulkita johdannossa ja kirjallisuuskatsauksessa esitettyjen kehittämistoimenpiteiden osalta. Liikenne- ja viestintäministeriö rakentaa kyberturvallisuuden kehittämisohjelmaa ja selvittää tietoturvan ja tietosuojan parantamista, kun samaan aikaan valtiovarainministeriössä kehitetään digitaalista turvallisuutta. Molemmat ohjelmat ovat toki keskenään koordinoituja, mutta yksittäisen viranomaisen kannalta samaan aiheeseen liittyen huomio hajautuu eri suuntiin.

Toinen haaste koskee toimivallan jakautumista eri hallinnonaloille, mikä edellyttää yhteensovittamista. Tämä puolestaan on jo osoitettu haastavaksi normaalioloissa, jossa ei lainsäädännön perusteella voida osoittaa selkeää johtovastuuta, vaan vastuu vaihtelee toimivaltaisen viranomaisen perusteella. Vastuun jakautuminen voi edelleen tarkoittaa eri hallinnonalojen erilaisia tulkintoja, mikä vastaa Lehtilän ym. (2021) havaintoja tietoturvallisuuden ja tietosuojan osalta yhteiskunnan kriittisillä toimialoilla.

Tulosten perusteella on arvioitavissa, että myös Lewellenin (2020) nimeämä kolmas haaste toteutuu. Tuo haaste liittyy eri hallinnonalojen koordinaatiopyrkimysten vastustamiseen, mikä johtaa siihen, että uutta teknologiaakin säädellään vanhoin periaattein sen sijaan, että pyrittäisiin rakentamaan uutta. Kyberturvallisuudenkin osalta vastuita on haluttu tulkita perustuslaista johdetuin, valtioneuvoston ohjesäännön mukaisin vastuin, vaikka käsitettä ei eksplisiittisesti kyseisessä säädöksessä mainita. Kyberturvallisuuden kannalta selkeyttä lisäisi yleislaki, joka määrittäisi eri osa-alueet ja niihin liittyvät vastuut. Ongelmana on kuitenkin se, että millään hallinnonalalalla ei ole selkeää toimivaltaa säätää kyseistä lakia ja osaltaan kokonaisuuteen liittyy myös kansainvälisen oikeuden osalta vastakkaisia näkemyksiä. Osaltaan vastuun epäselvyys liittyy suoraan Lewallenin (2020) mainitsemaan neljänteen haasteeseen, joka koskee viranomaisen kokemaa epävarmuutta uuden teknologian sääntelystä. Tällöin vedotaan olemassa olevaan sääntelyyn ja lisätään byrokratiaa sitä kautta.

6.2.3 Tietoturvallisuuden hallinta edellyttää riskienhallintaa

Tiedonhallintalain mukaisesti viranomaisen tietoturvallisuustoimenpiteet tulee mitoittaa arvioitujen riskien perusteella, mikä on aikaisempien tutkimusten (esim. Shameli-Sendi ym., 2016) keskeinen periaate tietoturvallisuuden hallinnassa. Tietoturvallisuuden hallinnan osalta tärkeimmät havainnot liittyvät viranomaisten tietojärjestelmien ja tietoliikenneratkaisujen arviointiin ja sitä koskeviin vaatimuksiin. Arviointi on kiinni viranomaisesta itsestään ja viranomainen pyytää itse arviointia niin halutessaan velvoittavuuden sijaan, mikä aiheuttaa todennäköisesti epäselvyyksiä vaatimustenmukaisuuden todentamisessa. Tätä näkemystä tukee VTV:n (2017) tarkastuskertomuksen havainnot yhteisten vaatimusten puuttumisesta. Kansainvälisten tietoturvavelvoitteiden osalta Naton ja EU:n osalta on selkeät vaatimukset eri turvallisuusluokkien tietojen käsittelylle, mutta kansallisen tiedon osalta yksiselitteisiä vaatimuksia ei ole. Arviointiin liittyen Kyberturvallisuuskeskus on tärkeä toimija arvioitsijana ja arviointilaitosten hyväksyjän. Omassa arviointitoiminnassaan se toimii resurssiensa sallimissa rajoissa ja painottaa kansainvälisiä tietoturvallisuusvelvoitteista ja niihin liittyviä arviointeja.

Yhteisten palvelujen käyttövelvoitteen osalta TORI- ja TUVE-palvelut eroavat toisistaan siinä, että TORI-palveluiden osalta ei ole asetettu käytännössä tietoturvallisuusvaatimuksia. Vastaavasti TUVE-palveluille on asetettu tietoturvallisuus- ja arviointivaatimuksia merkittävässä määrin. VTV:n toteuttamien

tuloksellisuustarkastusten perusteella molempien osalta on ollut vaikeuksia toteuttaa arviointeja ja siten osoittaa vaatimustenmukaisuus. Dhillonin ym. (2016) tulosten perusteella palvelujen ulkoistamisessa on tietoturvallisuuden osalta tärkeää mm. varmistua luottamuksesta palveluntuottajan kyvykkyyteen suojata tiedot asettamalla tarvittavat kontrollit. Mikäli tietoturvallisuudelle ei ole asetettu selkeitä yhteisiä vaatimuksia, ei näin ollen myöskään voi syntyä luottamusta palveluntuottajan kyvykkyyteen.

6.3 Teoria tieto- ja kyberturvallisuudesta viranomaistoiminnassa

Tieto- ja kyberturvallisuus muodostuvat strategisesta ohjauksesta, operatiivisesta kyberturvallisuustoiminnasta ja tietoturvallisuustoimenpiteistä. Strateginen ohjaus muodostuu valtioneuvoston toiminnasta ja operatiivinen kyberturvallisuustoiminta rikostorjunnasta, siviilitiedustelusta, kyberpuolustuksesta ja Kyberturvallisuuskeskuksen toiminnasta. Tietoturvallisuustoimenpiteet toteutuvat viranomaisen ja palveluntuottajien yhteistyönä julkisuusperiaatteen ja salassapitovelvoitteiden mukaisesti.

Lainsäädännön ohjaus toteutuu taktisena, koska toimivalta on hallinnonaloilla ja lainsäädännön velvoittavuus perustuu yksityiskohtaisiin vaatimuksiin. Strateginen ote edellyttää poikkihallinnollista valmistelua, jota kuitenkin pidetään vaikeana. Tämä on johtanut tilanteeseen, jossa lainsäädäntö ei ole kehittynyt poliittisina tahdonilmauksina hallituskausittain laadittujen valtioneuvoston periaatepäätösten mukaisesti. Huolimatta siitä, että kyberturvallisuus käsitteenä ei ole lainsäädännössä, viranomaiset toteuttavat lainsäädännön mukaisesti kyberturvallisuutta edistäviä toimia. Yhtenäisen kyberturvallisuuslainsäädännön puute jättää kuitenkin viranomaisten yhteistyölle rajoitteita.
Tietoturvallisuuden osalta lainsäädäntö asettaa valtionhallinnon viranomaisille selkeät velvoitteet yhteisten palvelujen käyttämisestä, mutta yhteisille palveluille ei ole turvallisuusverkkoa lukuun ottamatta säädetty yksiselitteisiä tietoturvallisuusvaatimuksia. Lainsäädäntö määrittelee salassapitovelvoitteiden perusteet ja turvallisuusluokat, mutta turvallisuusluokille ei ole asetettu yksiselitteisiä yhteisiä vaatimuksia eikä viranomaisella ole velvoitetta pyytää käyttämiensä ratkaisujen arviointia ulkopuoliselta arviointilaitokselta. Yhdistettynä siihen, että valtionhallinnosta puuttuu yhteinen riskienhallintaprosessi, voidaan päätyä tilanteeseen, jossa viranomainen ei pysty varmistumaan lainsäädännön velvoitteiden ja tietoturvallisuusvaatimusten noudattamisesta kansallisen tiedon osalta.

6.4 Tulosten merkitys ja luotettavuus

Tutkimuksessa luotiin katsaus valtionhallinnon viranomaisen tieto- ja kyberturvallisuuden hallintaan vaikuttavaan lainsäädäntöön uudesta näkökulmasta. Tutkimuksen perusteella esitettiin tieto- ja kyberturvallisuuden

osalta kolmiosainen rakenne, jossa strateginen ohjaus, operatiiviset kyberturvallisuustoimet ja päivittäiset tietoturvallisuustoimenpiteet muodostavat valtionhallinnon kokonaisuuden. Tutkimuksen tulokset yhtyvät monelta osin aikaisempiin tutkimuksiin ja selvityksiin. Työssä esitettiin tulosten perusteella alustava teoria tieto- ja kyberturvallisuuden lainsäädännöstä viranomaistoiminnan kannalta. Tutkimuksen tulokset tukevat aikaisempia tuloksia mm. poikkihallinnollisen valmistelun vaikeudesta ja uusien teknologioiden sääntelyyn liittyvistä haasteista tai ulkoistamiseen liittyvään haasteeseen tietoturvallisuuden osalta. Teoreettisina löytöinä voidaan pitää havaintoa poikkihallinnollisen valmistelun hyödyistä ja onnistumisesta silloin, kun eri hallinnonalat valmistelevat saman tyyppistä lainsäädäntöä tai lainsäädännön taktista luonnetta. Tutkimuksen käytännön tulokset osoittavat tarpeen kyberturvallisuutta koskevalle yhteiselle sääntelylle sekä viranomaisten tietojärjestelmien ja tietoliikenneratkaisujen arviointia koskevan sääntelyn kehittämiselle. Käytännön hyötynä voidaan pitää itsessään lainsäädännön kokonaisvaltaista tarkastelua yhdessä tutkimuksessa yhdistämällä tieto- ja kyberturvallisuutta koskevan sääntelyn perusteluineen samaan analyysiin. Työn keskeisimpiä rajoitteita on se, että työssä tarkasteltiin sitä, mitä lainsäätäjä on kirjoittanut ja tarkoittanut. Miten lain kirjain ja tavoitteet toteutuvat, ei selviä tässä tutkimuksessa, mutta sitä voidaan jossain määrin arvioida aikaisemman tutkimuksen perusteella.

Analyysin osalta tutkijan oma koulutus ei ole lainsäädännön alalta, mikä voi näkyä lakitekstien tulkinnassa. Lainkirjoittajan oppaan (Oikeusministeriö, 2021a) mukaisesti jokainen säädös on osa oikeusjärjestyksen kokonaisuutta ja ymmärrettävissä vain kokonaisuuden tuntemisen kautta. Säädöksen koko merkitys ei ilmene pelkästä säädöstekstistä, vaan osaltaan muusta lainsäädännöstä. Joissain tilanteissa jopa yleisistä oikeusperiaatteista. Tässä työssä on tehty lainsäädännöstä tutkimuksen kannalta tarkoituksenmukainen otanta, joka voi kuitenkin em. perustein rajoittaa tulkinnan luotettavuutta.

Tutkimuksessa pyrittiin välttämään virheitä, mutta niitä ei voitu varmuudella välttää. Tutkijan oma objektiivisuus pyrittiin varmistamaan sillä, että analyysiin ja sen tuloksiin otetaan mukaan vain ne asiat, jotka perustuvat käytettyyn aineistoon. On kuitenkin mahdollista, että tutkijan aihepiiriin varsin läheisesti liittyvä arkityö ja sitä kautta syntyneet omat kokemukset ovat välittyneet tutkimustuloksiin. On mahdollista, että samaa aineistoa käyttävä toinen tutkija päätyisi erilaisiin tulkintoihin toisenlaisella aineiston koodauksella ja luokittelulla, mutta tulokset saavat tukea aikaisemmasta tutkimuksesta ja selvityksistä. Validiteetin osalta tutkimuksen toteutus on pyritty kuvaamaan mahdollisimman tarkasti, mutta on selvää, että käyttämällä tutkimuksen yhteydessä toisena menetelmänä esimerkiksi haastatteluja, olisi tulosten luotettavuutta voitu parantaa.

Tutkimuksen perusteella jatkotutkimusaiheiksi nousee keskeisesti operatiivisen kyberturvallisuustoiminnan osalta viranomaisten yhteistoiminnan tarkempi selvittäminen sekä toisaalta tieto- ja kyberturvallisuusvalvontaan liittyvä sääntely. Vastaavasti tietoturvallisuustoimenpiteiden osalta kiinnostavia

ja lisäselvyyttää kaipaavia osa-alueita ovat valtionhallinnon yhteinen riskienhallinta ja tietojärjestelmien arviointiin liittyvän sääntelyn kehittäminen.

7 YHTEENVETO

Työn alkuperäisenä motivaationa toimi merkittävältä osin oman työn yhteydessä tehdyt havainnot. Työn ajankohtaisuus on kuitenkin korostunut noin puoli vuotta kestäneen prosessin aikana, kun Suomessa ja maailmalla on jouduttu todistamaan erilaisia kyberhyökkäyksiä. Työn tulokset osoittavat edelleen sen, että tämän tyyppiselle tutkimukselle oli tarve.

Työn tavoitteena oli selvittää, miten kansallinen lainsäädäntö velvoittaa ja ohjaa valtionhallinnon viranomaisia tieto- ja kyberturvallisuuden osalta. Alaongelmana vastattiin kysymykseen "Mitä eroa tieto- ja kyberturvallisuudella on lainsäädännössä? Tutkimuksen erityisenä mielenkiinnon kohteena oli viranomaisten toimivaltaan ja yhteistoimintaa koskeva sääntely. Tutkimuksessa ei käsitelty EU-lainsäädäntöä, vaikka siihen viitattiinkin. Aiheen laajuudesta johtuen myöskään tietosuojaa ei tarkasteltu.

Tutkimuksen perusteella strategisen tason ohjaus valtioneuvostossa on sidottu kokonaisturvallisuuden mallin mukaisesti toimivaltaisen viranomaisen rooliin, mikä on perustuslaista peräisin olevaa sääntelyä. Tämä yhdistettynä operatiiviseen kyberturvallisuustoimintaan luo tilanteen, jossa kyberturvallisuusstrategiassa vuonna 2013 esitetyt tavoitteet eivät ole toteutuneet lainsäädännön osalta, eikä kyberturvallisuutta ole käsitteenä sisällytetty lainsäädäntöön. Viranomaisten tiedonvaihtoa rajoittavat hallinnonalakohtaiset lait ja se, että sääntelyä ei ole kehitetty yhteistoiminnan edistämiseksi kuin tiedustelulakien osalta. Toisaalta tiedustelulait osoittavat poikkihallinnollisen säädösvalmistelun olevan mahdollista ainakin rajatusti ja tilanteissa, joissa eri viranomaisten toiminta on samantyyppistä. Tämän perusteella olisi luontevaa kehittää sääntelyä niin, että tietoturvallisuuteen liittyvää teknistä valvontaa tai havainnointia voisi tehdä myös lakisääteistä tehtävää toteuttava viranomainen, eikä pelkästään viestinnän välittäjä. Tähän voi toki liittyä vastaava perustuslaillinen haaste, joka johti perustuslain muuttamiseen tiedustelulakien yhteydessä yksityisyydensuojan osalta.

Kyberturvallisuuden osalta tulokset ovat kytkettävissä ja selitettävissä Lewallenin (2020) aikaisempien tulosten perusteella. Lewallenin mukaan uuden teknologian sääntely voi olla vaikeaa, koska vastuutahoa ei kyetä osoittamaan. Toisaalta tilanne voi johtaa hallinnonalojen väliseen kilvoitteluun omistajuudesta. Kaikki tämä hidastaa tarkoituksenmukaisen sääntelyn aikaan saamista. Hallinnonalakohtainen sääntely on Johnssonin ym. (2014) mukaan osoitus yhdessä suoraan lainsäädäntöön kirjoitettujen hallinnollisten, teknisten ja fyysisten turvallisuusvaatimusten kanssa taktisesta sääntelystä strategisen sijaan.

Tietoturvallisuuden osalta tutkimuksen tulokset osoittavat lainsäädännön johtavan viranomaisen osin ristitiitaiseen tilanteeseen riskienhallinnan osalta. Laki edellyttää riskiperusteista arviointia tarvittavista tietoturvallisuustoimenpisteistä, mutta käytännössä erittäin merkittävä osa teknisistä haavoittuvuuksista kuuluu palveluntuottajalle, jota viranomaisen on lain perusteella käytettävä. Toisaalta lainsäädännöstä puuttuvat yksiselitteiset

vaatimukset tietoturvallisuudesta eri turvallisuusluokissa, eikä viranomaisilla ole velvoitetta kansallisen tiedon osalta tietojärjestelmiensä tai tietoliikennejärjestelyjensä arviointiin. Myöskään valtion yhteisille toimialariippumattomille tieto- ja viestintäteknisille palveluille tai tietojärjestelmäpalveluille ei ole asetettu selkeitä tietoturvallisuusvaatimuksia. Valtiontalouden tarkastusvirasto on päätynyt omissa tarkastuksissaan (2016 ja 2017) siihen, että valtionhallinnosta puuttuu yhteinen riskienhallintaprosessi ja yhteiset tietoturvallisuusvaatimukset eikä Valtori ei ole kyennyt osoittamaan omien ratkaisujensa vaatimustenmukaisuutta. Kun tätä verrataan Dhillonin ym. (2017) tuloksiin ulkoistamiseen liittyvästä luottamuksen tarpeesta palveluntuottajaan, voisi tilanne olla parempikin.

Tutkimuksessa käytettiin analyysimenetelmänä grounded teoriaa, jonka osalta tutukimuksen mahdolliset rajoitteet voivat liittyä koodaukseen ja aineiston luokitteluun. Tutkimuksessa koodaus ja luokittelu tapahtuivat kirjallisuuskatsauksen perusteella muodostettuun rakenteeseen, mikä osaltaan asetti analyysille ennalta tietyt rajoitteet. Tutkimusaineiston rajoittuminen vain kirjalliseen materiaaliin rajoittaa myös osaltaan tehtäviä johtopäätöksiä. Tutkimuksessa voidaan arvioida ja analysoida sisältöjä, mutta miten lakeja ja asetuksia viranomaisessa noudatetaan, ei ole tutkimuksen puitteissa selvitettävissä. Toisaalta säädöstekstien tulkinta otoksena lainsäädännön kokonaisuudesta voi myös jättää jotain asiaoita huomioimatta. Tutkijan omat ennakkokäsitykset ja aiheen tuntemus voivat myös vaikuttaa tulkintoihin, vaikka pyrkimyksenä oli objektiivinen aineiston analyysi.

Tutkimuksen perusteella olisi hyvin luontevaa tutkia edelleen kyberturvallisuuden osalta viranomaisten yhteistoiminnan edellytyksiä ja yhteistoimintatarpeita. Toisaalta sekä kyber-, että tietoturvallisuuden osalta riskienhallinnan kokonaisuus valtionhallinnossa kaipaisi selkeästi tarkempaa selvittämistä yhdessä tietojärjestelmien ja tietoliikenneratkaisujen arviointiin liittyvien näkökulmien kanssa.

LÄHTEET

a) Artikkeli tieteellisessä aikakauslehdessä:

Corbin, J. & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology, 13, 1, 3-21.*

Dhillon, G., Syed, R. & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, *54, 452-464*.

Hiller, J. S. & Russel, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29, 3, 236-245.*

Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management*, 9, 89-116.

Kolstad, C., Ulen, T., & Johnson, G. (1990). Ex post liability for harm vs. ex ante safety regulation: substitutes or complements? *American Economic Review 80, 4, 888–901.*

Lewallen, J. (2020). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance.*

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *Internatiomnal journal of critical infrastructure protection 3, 103-117.*

Siponen, M. & Willison, R. (2009). Information management standards: Problems and solutions. *Information & Management, 46, 5, 267-270.*

Shameli-Sendi, A., Aghababaei, R. & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57, 14-30.*

Shavell, S. (1984). A model of the optimal use of liability and safety regulation. *RAND Journal of Economics 15 (2) 271–280.*

Soomro, Z. A., Hussain, M. & Ahmed, J. (2015). Information security management needs more holistic approach: A literature review. *International Journal of Information Management 36, 215–225*.

Susanto, H., Amunawar, M. N. & Tuan, Y.C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS, 11, 5, 23-29*.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T. & Klepacki, B. (2019). Information security assessment in public administration. *Computers & Security 90, 101709.*

Tupa, J. & Steiner, F. (2006). Implementation of information security management system in the small healthcare organization. *Journal of Telecommunications and Information Technology, 2, 52-58.*

Von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38, 97-102.*

b) Artikkeli kokoomateoksessa:

Airaksinen, J. (2021). Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. *Tampere: Yhteiskuntatieteellinen tietoarkisto*. Haettu osoitteesta https://www.fsd.tuni.fi/palvelut/menetelmaopetus/

Voutilainen, T. (2006). Hyvä tietohallinto ja sen sääntely viranomaistoiminnassa. *EDILEX Edita Publishing Oy 2006.* Haettu osoitteesta https://www.ulapland.fi/loader.aspx?id=404ab602-8b00-44a1-875d-2fda14fe709a

c) Artikkeli konferenssijulkaisussa:

Roy, P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 1-3.

d) Kirja:

Bergeron, B. (2003). *Essentials of Shared Services*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita.* (15. uud. painos). Helsinki: Tammi.

Metsämuuronen, J. (2008). *Tutkimuksen tekemisen perusteet ihmistieteissä*. (4. painos). Vaajakoski: Gummerrus Kirjapaino Oy.

e) Raportti:

Lehtilä, O., Nyyström, P., Ronikonmäki, N-M. & Sirviö, T-H. (2021). *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti.* Helsinki: Liikenne- ja viestintäministeriö. Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/162783

Lehto, M., Limnéll, J., Innola, Pöyhönen, J., Rusi, T., & Salmela, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. *Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisu 30/2017*. Haettu osoitteesta https://tietokayttoon.fi/julkaisu?pubid=17805

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. *Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018.* Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/160717

Liikenne- ja viestintäministeriö. (2020). *Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimilaloilla; työryhmän väliraportti.* Haettu osoitteesta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=9bc97079-06ac-4fef-ab9c-bc1929790ddf.

Lonka, H., Laitinen, K., Keinänen, A., Wähä, S., Huhtinen, A-M. & Paasonen, J. (2020). Kansallisen turvallisuuden vaikutusten arviointi. *Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2020:28.* Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/162212

Luoma, R. (2019). Viranomaisten toimivaltuudet häiriötilanteissa. *Oikeusministeriön julkaisuja, Selvityksiä ja ohjeita 2019:18.* Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/161604

Puolustusministeriö. (2015). Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. Haettu osoitteesta https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Valtiontalouden tarkastusvirasto. (2016). Hallinon turvalisuusverkkotoiminnan ohjaus. *Valtiontalouden tarkastusviraston tarkastuskertomukset 14/2016*. Dnro 172/54/2015. Haettu osoitteesta https://www.vtv.fi/app/uploads/2018/06/15082229/hallinnon-turvallisuusverkkotoiminnan-ohjaus-14-2016.pdf

Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. *Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017*. Dnro 185/54/2016. Haettu osoitteesta

https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf

Valtiontalouden tarkastusvirasto. (2019a). Keskitetyt ICT-palvelut ja hankinnat. *Valtiontalouden tarkastusviraston tarkastuskertomukset 4/2019.* Dnro 303/54/2017. Haettu osoitteesta https://www.vtv.fi/app/uploads/2019/02/VTV-Tarkastuskertomus-4-2019-Keskitetyt-ICT-palvelut-ja-hankinnat.pdf

Valtiontalouden tarkastusvirasto. (2019b). *Jälkiseurantaraportti*. Dnro 172/54/2015. Haettu osoitteesta https://www.vtv.fi/app/uploads/2019/03/VTV-Jalkiseuranta-Hallinnon-turvallisuusverkkotoiminnan-ohjaus-14-2016.pdf

f) Manuaali:

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2012). *Teknisen ICT-ympäristön tietoturvataso-ohje*. Haettu osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-32012-teknisen-ymparistön-tietoturvataso-ohje

g) Opinnäyte:

Kari, M. J. (2019). *Russian Strategic Culture in CyberspaceTheory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats.* JYU Dissertations. Haettu osoitteesta https://jyx.jyu.fi/handle/123456789/65402

h) Elektroninen kirja:

Kielitoimiston sanakirja. (2020). Tietoturva. Kotimaisten kielten keskus ja Kielikone Oy. Haettu osoitteesta https://www.kielitoimistonsanakirja.fi/#/tietoturva?searchMode=all

Laari, T. (toim), Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). *#kyberpuolustus. Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita no. 12. Haettu osoitteesta https://www.doria.fi/handle/10024/173254

Kokonaisturvallisuuden sanasto. (2017). *TSK 50*. Sanastokeskus TSK ry. Haettu osoitteesta https://www.tsk.fi/tsk/fi/kokonaisturvallisuuden_sanasto_tsk_50-1089.html

Kyberturvallisuuden sanasto. (2018). *TSK 52*. Sanastokeskus TSK ry ja Huoltovarmuuskeskus. Haettu osoitteesta https://www.tsk.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html

Mäenpää, O. (2020). *Julkinen valta ja oikeusvaltio*. Helsingin yliopiston oikeustieteellinen tiedekunta. Haettu osoitteesta https://unicontent.unigrafia.fi/#/reader/469b0a20-8848-11ea-bfb9-00155d64030a.

Oikeusministeriö. (2021a). *Lainkirjoittajan opas*. Kansallisten säädösten valmistelua koskevat ohjeet. Finlex-julkaisut. Haettu osoitteesta http://lainkirjoittaja.finlex.fi/

i) Virallislähteet:

Aluevalvontalaki 2000/755. Annettu Helsingissä 18.8.2000. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2000/20000755#L6

Arkistolaki 1994/831. Annettu Helsingissä 23.9.1994. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1994/19940831

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (pääosin kumoutunut, 2 a luku jätetty voimaan) 1999/1030. Annettu Helsingissä 12.11.1999. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Euroopan unioni. (2016/1148). *Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa*. Annettu Strasbourgissa 6.7.2016. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FIN

Hallintolaki 2003/434. Annettu Helsingissä 6.6.2003. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2003/20030434

HE 264/2006 vp. *Hallituksen esitys Eduskunnalle puolustusvoimalaiksi ja eräiksi siihen liittyviksi laeiksi*. Haettu osoitteesta https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+264/2006

HE 3/2008 vp. *Hallituksen esitys Eduskunnalle valmiuslaiksi ja eräiksi siihen liittyviksi laeiksi.* Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+3/2008

HE 45/2011 vp. *Hallituksen esitys eduskunnalle laeiksi tietoturvallisuuden arviointilaitoksista, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista sekä viestintähallinnosta annetun lain 2 §:n muuttamisesta.* Haettu osoitteesta https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+45/2011

HE 150/2013 vp. *Hallituksen esitys eduskunnalle laeiksi valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä, julkisen hallinnon tietohallinnon ohjauksesta annetun lain 11 §:n ja 13 §:n 2 momentin kumoamisesta sekä valtiokonttorista annetun lain 2 §:n 4 momentin kumoamisesta.* Haettu osoitteesta https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+150/2013

HE 54/2013 vp. *Hallituksen esitys eduskunnalle laeiksi julkisen hallinnon turvallisuusverkkotoiminnasta ja viestintämarkkinalain 2 §:n muuttamisesta.* Haettu osoitteesta https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+54/2013

HE 221/2013 vp. *Hallituksen esitys eduskunnalle tietoyhteiskunta-kaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta*. Haettu osoitteesta https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+221/2013

HE 59/2016 vp. *Hallituksen esitys eduskunnalle laeiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain muuttamisesta*. Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_59+2016.aspx

HE 261/2016 vp. *Hallituksen esitys eduskunnalle laiksi valtioneuvoston tilannekeskuksesta.* Haettu osoitteesta https://finlex.fi/sv/esitykset/he/2016/20160261

HE 198/2017 vp. *Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.* Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_198+2017.aspx

HE 203/2017 vp. *Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi.* Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_203+2017.aspx

HE 61/2018 vp. *Hallituksen esitys eduskunnalle laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ja eräiksi niihin liittyviksi laeiksi.* Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_61+2018.aspx

HE 60/2018 vp. *Hallituksen esitys eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta.* Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_60+2018.aspx

Laki digitaalisten palvelujen tarjoamisesta 2019/306. Annettu Helsingissä 15.3.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190306

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 2016/571. Annettu Helsingissä 29.6.2016. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2016/20160571

Laki huoltovarmuuden turvaamisesta 1992/1390. Annettu Helsingissä 18.12.1992. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1992/19921390

Laki julkisen hallinnon tiedonhallinnasta 2019/906. Annettu Naantalissa 9.8.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190906

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 2015/10. Annettu Helsingissä 13.1.2015. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Laki kansainvälisistä tietoturvallisuusvelvoitteista 2004/588. Annettu Naantalissa 24.6.2004. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki liikenne- ja viestintävirastosta 2018/935. Annettu Helsingissä 23.11.2018. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2018/20180935

Laki puolustusvoimien virka-avusta poliisille 1989/781. Annettu Helsingissä 5.12.1980. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/1980/19800781

Laki puolustusvoimista 2007/551. Annettu Helsingissä 11.5.2007. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2007/20070551

Laki sotilastiedustelusta 2019/590. Annettu Helsingissä 26.4.2019. Haettu osoitteesta https://finlex.fi/fi/laki/alkup/2019/20190590#Pidp447692528

Laki sähköisen viestinnän palveluista 2014/917. Annettu Helsingissä 7.11.2014. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Laki sähköisestä asioinnista viranomaistoiminnassa 2003/13. Annettu Helsingissä 23.1.2003. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2003/20030013

Laki tietoliikennetiedustelusta siviilitiedustelussa 2019/582. Annettu Helsingissä 26.4.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190582

Laki tietoturvallisuuden arviointilaitoksista 2011/1405. Annettu Helsingissä 22.12.2011. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/2011/20111405

Laki valtioneuvostosta 2003/175. Annettu Helsingissä 28.2.2003. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2003/20030175#L2P12

Laki valtion talousarviosta 1988/423. Annettu Helsingissä 13.5.1988. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1988/19880423

Laki Valtion talous- ja henkilöstöhallinnon palvelukeskuksesta 2019/179. Annettu Helsingissä 8.2.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2019/20190179

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä. 2013/1226. Annettu Helsingissä 30.12.2013. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2013/20131226

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 2011/1406. Annettu Helsingissä 22.12.2011. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20111406

Laki viranomaisten toiminnan julkisuudesta 1999/621. Annettu Helsingissä 21.5.1999. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/1999/19990621

Laki yhteistoiminnasta valtion virastoissa ja laitoksissa 2013/1233. Annettu Helsingissä 30.12.2013. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2013/20131233

Poliisilaki 2011/872. Annettu Naantalissa 22.7.2011. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110872

Rikoslaki 1889/39. Annettu Helsingissä 19.12.1889. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Suomen perustuslaki 1991/731. Annettu Helsingissä 1.3.2000. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

The White House. (2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Haettu osoitteesta https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Turvallisuuskomitea. (2017). *Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepää*tös. Helsinki: Lönnberg Print. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Turvallisuuskomitean sihteeristö. (2013). *Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös*. Forssa: Forssa print. Haettu osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

Turvallisuuskomitean sihteeristö. (2019). *Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös*. Haettu osoitteesta https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80655af5

Turvallisuusselvityslaki 2014/726. Annettu Helsingissä 19.9.2014. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/2014/20140726

Valmiuslaki 2011/1552. Annettu Helsingissä 29.12.2011. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

Valtioneuvosto. (2018). *Valtioneuvoston päätös huoltovarmuuden tavoitteista, 1048/2018.* Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2018/20181048

Valtioneuvoston asetus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä tehdyn sopimuksen voimaansaattamisesta sekä sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaantulosta 2015/77. Annettu Helsingissä 19.11.2015. Haettu osoitteesta https://www.finlex.fi/fi/sopimukset/sopsteksti/2015/20150077

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 2015/1109. Annettu Helsingissä 27.8.2015. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2015/20151109

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta annetun valtioneuvoston asetuksen muuttamisesta. (2020/442). Annettu Helsingissä 11.6.2020. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2020/20200442

Valtioneuvoston asetus Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen voimaansaattamisesta sekä hallinnollisen järjestelyn ja tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaantulosta 2013/8. Annettu Helsingissä 24.1.2013. Haettu osoitteesta https://www.finlex.fi/fi/sopimukset/sopsteksti/2013/20130008

Valtioneuvoston asetus Turvallisuuskomiteasta 2013/77. Annettu Helsingissä 24.2.2013. Haettu osoitteesta https://edilex.fi/lainsaadanto/20130077

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 2014/132. Annettu Helsingissä 20.2.2014. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2014/20140132

Valtioneuvoston ohjesääntö 2003/262. Annettu Helsingissä 3.4.2003. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/2003/20030262

Valtiovarainministeriö. (2009). *Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä. Vahti 7/2009*. Helsinki: Edita Prima Oy. Haettu osoitteesta https://vm.fi/documents/10623/307681/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009/24355a33-4042-42fb-9dba-981e6398ee7a

Valtiovarainministeriö. (2020). *Julkisen hallinnon digitaalinen turvallisuus. Valtioneuvoston periaatepäätös*. Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/162169

j) Verkkosivu:

Cyber Law Toolkit. (2021). *International Cyber Law in Practise: Interactive Toolkit.* Soverignity. Haettu osoitteesta https://cyberlaw.ccdcoe.org/w/index.php?title=Sovereignty&mobileaction=toggle_view_desktop#cite_note-9

Eduskunnan kirjasto. (2020). *Lainsäädäntö.* Haettu osoitteesta https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx

Helsingin Sanomat. (2020). *Tietoliikenneyritys hakkeroitiin, ja uhreiksi joutuivat Yhdysvaltain ministeriöt ja suuryhtiöt: Venäjän uskotaan olevan tietomurron takana*. Haettu ositteesta https://www.hs.fi/ulkomaat/art-2000007687185.html

Huoltovarmuuskeskus. (2021). *Tietoyhteiskunta*. Haettu osoittesta https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta

Ilta-Sanomat. (2021). *Valtion virastoihin tietomurto – Kiina vastaavien iskujen takana, viranomainen vaitelias. Ohjelmistoaukon kautta tehty hyökkäys herättää paljon kysymyksiä, mutta vastaukset ovat niukkoja.* Haettu osoitteesta https://www.is.fi/digitoday/tietoturva/art-2000007942369.html

Kyberturvallisuuskeskus. (2021). *NIS-koordinointi ja viranomaisyhteistyö*. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo

Liikenne- ja viestintäministeriö. (2021). *Kehittämisohjelma kyberturvallisuuden kokonaistilan parantamiseksi.* Haettu osoitteesta https://www.lvm.fi/-/kehittamisohjelma-kyberturvallisuuden-kokonaistilan-parantamiseksi-1250784

Oikeusministeriö. (2021b). *Finlex-oikeudellisen aineiston internet-palvelu*. Haettu osoitteesta https://www.finlex.fi/fi/

Sisäministeriö. (2021a). *Kyberrikollisuus ylittää rajat tietoverkoissa*. Haettu osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö. (2021b). *Siviilitiedustelulla suojataan Suomen kansallista turvallisuutta*. Haettu osoitteesta https://intermin.fi/poliisiasiat/siviilitiedustelu

Tieteen termipankki (2021). *Oikeustiede:säädöstyypit*. Haettu osoitteesta https://tieteentermipankki.fi/wiki/Oikeustiede:säädöstyypit.)

Ulkoministeriö. (2021a). *Katakri – tietoturvallisuuden auditointityökalu viranomaisille*. Haettu osoitteesta https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Ulkoministeriö. (2021b). *Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje.* Haettu osoitteesta https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje

Ulkoministeriö. (2021c). *International law and cyberspace. Finland's national positions.* Haettu osoitteesta https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

Valtioneuvosto. (2020). *Periaatepäätökset*. Haettu osoitteesta https://valtioneuvosto.fi/paatokset/periaatepaatokset.

Valtiovarainministeriö. (2019). *TUVE tietoturvavalvonnan edellyttämän lainsäädännön valmisteluryhmän asettaminen (VM/1644/03.01.00/2019).* Haettu osoitteesta https://vm.fi/hanke?tunnus=VM012:00/2020

Valtiovarainministeriö. (2021). *Digitaalisen turvallisuuden kehittäminen*. Haettu osoitteesta https://vm.fi/kehittaminen

Valtori. (2021). *Lukuja ja historiaa.* Haettu osoitteesta https://valtori.fi/lukuja-ja-historiaa

Yle-uutiset. (28.12.2020). *KRP tutkii äärimmäisen harvinaista rikosta: Eduskuntaan kohdistunut tietomurto voi olla vakoilua ja kansanedustajien sähköposteja vaarantunut.* Haettu osoitteesta https://yle.fi/uutiset/3-11715912

Yle-uutiset. (18.3.2021). *Supo: Eduskuntaan kohdistunut vakoilu viittaa Kiinaan – poliisin mukaan verkkovakoilulla on yritetty kalastella tietoja vieraalle valtiolle.* Haettu osoitteesta https://yle.fi/uutiset/3-11843261

k) Standardit:

Suomen standardisoimisliitto ry. (2017). *SFS-EN ISO/IEC 27001:2017*. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*. Haettu osoitteesta https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf