Olli-Pekka Palonen

KYBERTURVALLISUUDEN JOHTAMINEN VIROSSA, ISRAELISSA JA ALANKOMAISSA – MITÄ VOIMME OPPIA?

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2019

TIIVISTELMÄ

Palonen Olli-Pekka
Kyberturvallisuuden johtaminen Virossa, Israelissa ja Alankomaissa – mitä voimme oppia?
Jyväskylä: Jyväskylän yliopisto, 2019, 80 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tässä tutkimuksessa tarkastellaan kyberturvallisuutta ja sen strategista johtamista valtion näkökulmasta. Tutkimuksen teoriaosuuden tarkoituksena oli selvittää mitä strateginen johtaminen on erityisesti kyberturvallisuuden kontekstissa. Tutkimuksen empiirisessä osuudessa tutkittiin kansallisen tason kyberturvallisuuden johtamista kolmessa kyberturvallisuuden näkökulmasta tarkasteltuna kärkivaltiossa. Tutkimuksessa pyrittiin myös selvittämään, voidaanko tutkimustulosten perusteella löytää tekijöitä, joita voidaan jalostaa kansallisen kyberturvallisuuden kehittämisajatuksiksi. Tutkimuksen aihe on tärkeä, koska sen avulla voidaan määrittää kyberturvallisuuden strategista johtamista valtion tasolla sekä sillä voidaan löytää tutkittavien valtioiden johtamisesta tekijöitä, joita voidaan edelleen jalostaa kansallisen kyberturvallisuuden kehittämiseksi. Tutkimuksen teoriaosuus sekä empiirinen osuus toteutettiin aineistolähtöistä sisällönanalyysiä käyttäen. Tutkimusmateriaali kerättiin julkisesti saatavissa olevista lähteistä. Tutkimuksen teoriaosuudessa havaittiin, että kyberturvallisuuden johtamisessa korostuu ajantasainen tilannetieto, toimijoiden välinen yhteistyö, uhkien tunnistaminen ja niihin vastaaminen sekä yhteiskunnan toimintojen jatkuvuuden varmistaminen ja niihin kohdistuvien häiriöiden vaikutuksista palautuminen mahdollisimman nopeasti. Tutkimuksen empiirisessä osiossa havaittiin, että tarkastelluissa valtioissa kyberturvallisuutta tuotetaan kokonaisvaltaisesti kansainvälisistä yhteistyökumppanuuksista yksityisiin kansalaisiin. Kokonaisvaltainen toiminnan koordinointi edellyttää riittäviä toimivaltuuksia ja kehittäminen riittäviä resursseja ja investointeja. Lisäksi organisaatiorakenteita pyritään yksinkertaistamaan keskittämällä tärkeitä toimintoja ja karsimalla sellaisia organisaatioita, joiden toimintaa voidaan yhdistää (Lehto 2018, 64).

Asiasanat: kyberturvallisuus, strateginen johtaminen, kansallinen kyberturvallisuus

ABSTRACT

Palonen, Olli-Pekka
Managing Cyber Security in Estonia, Israel and Netherlands – What can we learn?
Jyväskylä: University of Jyväskylä, 2019, 80 p.
Information system science, Master´s Thesis
Supervisor: Lehto, Martti

This study examines cyber security and its strategic management from a state perspective. The purpose of the theoretical part of the study was to find out what strategic management is especially in the context of cyber security. The empirical part of the research explored cyber security at national level in three cyber security perspectives in the top state. The study also sought to find out whether, on the basis of research results, there are factors that can be refined into national cyber security development ideas. The subject of the study is important because it can be used to determine the strategic management of cyber security at the state level, and it can find factors that can be further refined in order to develop national cyber security. The theoretical part of the research and the empirical part were carried out using data-based content analysis. The research material was collected from publicly available sources. In the theoretical part of the research, it was found that cyber security management emphasizes up-to-date situational information, co-operation between actors, identifying and responding to threats, and ensuring the continuity of social activities and restoring the impact of disruptions to them as quickly as possible. In the empirical part of the research, cyber security in the countries under review was comprehensively produced from international partnerships with private citizens. Comprehensive coordination of activities requires adequate powers and development of adequate resources and investments. In addition, efforts are made to simplify organizational structures by centralizing important activities and cutting down organizations that can be combined (Lehto 2018, 64).

Keywords: Cyber Security, strategic management, national cyber security

KUVIOT

SISÄLLYS

1 JOHDANTO

Kyberturvallisuudesta on tullut ilmiö, joka on keskeinen ja erottamaton osa yhteiskunnan kokonaisturvallisuutta. Digitaalinen vallankumous on synnyttänyt uudenlaisia uhkia. Uhkia, jotka vaikuttavat sähköisessä toimintaympäristössä, jota myös kutsutaan kybertoimintaympäristöksi. Tälle toimintaympäristölle on ominaista valtioiden rajat ylittävä liikkuvuus, suuri muutosnopeus sekä kompleksisuus. Tällä tarkoitetaan, että ympäristössä tapahtuvia häiriöitä on vaikea ennakoida ja usein ne ovat niin vaikeasti havaittavissa, että ne ovat jo tapahtuneet ennen niiden havaitsemista. Laaja-alaisen kyberhyökkäyksen seuraukset yhteiskunnalle voivat olla hyvin merkittäviä, jopa merkittävämpiä kuin fyysinen sotatoimi, mikäli ne kohdistuvat yhteiskunnan kriittisiin järjestelmiin, kuten esimerkiksi sähkönjakeluun tai vesihuoltoon. Yhteiskunnan toiminnan varmistamiseksi digitaalisessa toimintaympäristössä on kansallisen kyberturvallisuuden johtamisella suuri merkitys. Tämän tutkimuksen tarkoituksena on tarkastella strategista johtamista kyberturvallisuuden toimintaympäristössä sekä selvittää miten kyberturvallisuuden johtaminen on toteutettu valituissa kohdemaissa (Viro, Israel ja Alankomaat). Tutkimus toteutettiin kirjallisuuskatsauksena ja sitä tarkasteltiin aineistolähtöisen sisällönanalyysin avulla. Aineistosta analyysin perusteella löydetyistä tuloksista ja niistä tehdyistä päätelmistä pyrittiin jalostamaan kehittämisajatuksia kansallisen kyberturvallisuuden johtamiseen. Tutkimuksen tarkoitus ja tavoitteet, tutkimuskysymykset, aiheen rajaus, tutkimusasetelma ja –menetelmä, tutkimuksen validiteetti ja reliabiliteetti sekä odotetut tulokset ja niiden merkitys esitetään luvussa kaksi (2). Yhteiskunnan turvallisuuden ja toiminnan kannalta on merkityksellistä tutkia strategisen tason kyberturvallisuuden johtamista, kun ajatellaan yhteiskunnan sähköisiin toimintoihin kohdistuvien kyberuhkien ja häiriöiden aikaista havaitsemista ja estämistä, joka edellyttää nopeaa toimintaan, analysoitua ajantasaista tilannekuvaa sekä yhteiskunnan toimijoiden välistä yhteistyötä. Yhteiskunnan häiriöttömän toiminnan turvaamisen kannalta on tärkeää, että strategisen kyberturvallisuuden johtamisen keinoin voidaan vaikuttaa sekä normaaliolojen että häiriötilanteiden toimintaan.

2 TUTKIMUKSEN TARKOITUS JA TAVOITTEET

Tässä osiossa käsitellään tutkimuksen tausta ja aiheen rajaus, tutkimuskysymykset, tutkimusasetelma sekä –menetelmä, validiteetti ja reliabiliteetti ja lopuksi odotetut tulokset ja niiden merkitys. Tutkimus on tarkoitus toteuttaa kvalitatiivisena eli laadullisena tutkimuksena, jonka tavoite on erityisesti tarkastella strategista johtamista kyberturvallisuuden toimintaympäristössä sekä selvittää miten kyberturvallisuuden johtaminen on toteutettu valituissa kohdemaissa (Viro, Israel ja Alankomaat). Tutkimuksen materiaalia analysoimalla aineistolähtöisellä sisällönanalyysilla, pyritään löytämään aineistosta yhtäläisyyksiä ja eroavaisuuksia strategisessa johtamisessa. Analyysin perusteella saatuja tuloksia ja niistä tehtyjä päätelmiä edelleen jalostetaan kansallisen strategian kehittämisajatuksiksi perusteluineen. Tutkimuksen eräs osatavoite on määritellä mitä tarkoitetaan kyberturvallisuuden johtamisella. Tätä asiaa on käsitelty tarkemmin luvussa neljä (4).

2.1 Tutkimuksen tausta ja rajaus

Kyberturvallisuudesta on tullut keskeinen ja erottamaton osa yhteiskunnan turvallisuutta. Se on läsnä kaikkialla ja koskettaa meitä jokaista. Lehto, Limnell, Innola, Pöyhönen, Rusi ja Salminen (2017, 72–73) kuvaavat raportissaan ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” fyysisen- ja digitaalisen turvallisuuden asiaksi, jota on tänä päivänä yhä hankalampi erottaa toisistaan. Ne kytkeytyvät toisiinsa hyvin voimakkaasti. Digitaalisessa toimintaympäristössä tapahtuvilla muutoksilla on vaikutusta fyysiseen toimintaympäristöön ja fyysisessä toimintaympäristössä tapahtuvilla muutoksilla on vaikutusta digitaaliseen toimintaympäristöön. Kybertoimintaympäristöön. Tätä toimintaympäristöä on tarkasteltava kokonaisuutena.

VTT:n raportti (2016, 7-8) ”Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen” vahvistaa näkemystä siitä, että kyberturvallisuudesta on tullut merkittävä yhteiskunnan kannalta. Kyberturvallisuuden merkityksen kasvuun ovat vaikuttaneet muun muassa valtioiden keskeinen asema kyberturvallisuudessa sekä valtioiden väliset kybertoimet niin hyökkäyksiä tekevänä kuin puolustavana osapuolena. Kyberturvallisuuden merkityksen kasvu aiheuttaa myös merkittävästi erilaisten kyberuhkien kasvua. Raportissa julkaistun tutkimuksen mukaan Suomessa 84 prosenttia suuryrityksistä koki vuonna 2015 kyberturvallisuusriskit merkittävinä.

Kybertoimintaympäristössä tapahtuvat muutokset (kyberuhat) ovat hyvin nopeita, vaikeasti ennakoitavia ja usein niin hankalasti havaittavia, että ne ovat jo tapahtuneet ennen niiden havaitsemista. Muutosten seuraukset kybervaikutuksista voivat olla hyvinkin merkittäviä, mikäli ne kohdistuvat esimerkiksi kriittiseen infrastruktuuriin, jolloin tarkoitetaan yhteiskunnan elintärkeitä toimintoja, kuten kansalaisten turvallisuutta, vesihuoltoa, sähkönjakelua tai ruokahuoltoa. Yhteiskunnan näkökulmasta digitalisaation voimakas kehittyminen merkittäväksi osaksi yhteiskunnan eri toimintoja, on entisestään lisännyt kyberturvallisuusajattelun tärkeyttä.

Kuten aikaisemmin todettiin, kyberuhat aiheuttavat yhteiskunnalle merkittäviä ja kauaskantoisia seurauksia. Nämä uhat on pystyttävä nopealla toiminnalla tunnistamaan, analysoimaan ja reagoimaan ja lopuksi estämään, jotta voidaan taata yhteiskunnan infrastruktuurin häiriötön toiminta kaikissa tilanteissa. Jotta tämä onnistuisi, se edellyttää ajantasaista ja luotettavaa tilannekuvaa kybertoimintaympäristöstä sekä kaikkien toimijoiden saumatonta yhteistyötä. Suomessa kyberturvallisuuden toimijoita on paljon erilaisine vastuineen ja tehtäväalueineen ja siksi onkin erityisen tärkeää, että kokonaisuutta johdetaan riittävän järjestelmällisesti ja johdonmukaisesti, jotta asetetut tavoitteet voidaan saavuttaa ja toteuttaa. Tällä hetkellä kyberturvallisuutta ei johdeta riittävän voimallisesti ja tehokkaasti, jotta Suomen kyberturvallisuusstrategiassa määritellyt tavoitteet saavutettaisiin. Lehto ym. (2017, 67) raportti ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” tukee tätä havaintoa. Raportin mukaan tutkimuksessa nousi esiin voimakkaasti puutteet kyberturvallisuuden kokonaisvaltaisessa, kaikki yhteiskunnan kybertoiminnot yhdistävässä strategisessa johtamisessa. Raportin mukaan johtaminen pitäisi määrittää koko kansallisen kyberturvallisuuden kontekstissa, jossa huomioitaisiin myös koordinoinnin ja yhteistyön merkitys. Tässä tutkimuksessa tarkastellaan kyberturvallisuutta ja sen strategista johtamista valtion näkökulmasta. Tutkimuksessa käsitellään osaltaan johtamista myös organisaation näkökulmasta, koska kansallisella tasolla tehtävät strategiset päätökset ”valuvat” hierarkkisesti alaspäin organisaatiotasolle, jossa strategiset päätökset toteutetaan sovittujen tavoitteiden mukaisesti. Tutkimuksen pääpaino on kuitenkin valtiontasolla tapahtuvassa johtamisessa. Tutkimuksesta rajattiin pois yritykset ja yksityiset kansalaiset. Tutkimus perustuu julkisesti saatavilla oleviin lähteisiin, kuten raportteihin ja asiakirjoihin sekä Internet – lähteisiin.

Valtioneuvoston selvityksestä: Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen (2016, 46–47) löydetään myös tutkimusaiheeseen soveltuvaa tutkimusaineistoa. Raportissa otetaan varsin voimakkaasti kantaa strategisen johtamisen heikkouteen, yhteistyön puuttumiseen sekä kyberturvallisuus – kentän hajanaisuuteen erityisesti tiedonkulun suhteen. Keskeinen osa turvallisuusjohtamista on toimivan kyberturvallisuustoimijan muodostaminen, jonka tehtävänä olisi erityisesti kokonaisuuden strateginen johtaminen sekä toiminnan keskeinen hallinta kyberuhkatilanteissa, raportti tähdentää. Valtioneuvoston raportissa koetaan tärkeäksi kokonaisuuden kannalta myös yhteisen, kaikkien toimijoiden kesken kerätyn aineiston muodostaminen kokonaiskuvaksi ja edelleen jakaminen toimijoille koottuina arvioina ja toimintasuosituksina. Yhteistyön tärkeyttä sekä strategista päätöksen tärkeyttä korostetaan myös Nato Cyber Coalition 2014 harjoituksen yhteenvedossa. Ilman näitä ei pystytä varmistamaan ajantasaista tilannekuvaa, eikä luomaan toimijoiden välille sellaista luottamusta, jota tarvitaan kansallisen kyberturvallisuuden johtamiseen. Valtioneuvoston raportissa mainitaan myös, ettei kyberturvallisuusstrategia ole pystynyt luomaan yhteistyötä kannustavaa visiota ja yhteishenkeä sekä julkisen sektorin ja muiden toimijoiden välinen tiedonsiirto ja yhteistyö ovat paikoin hyvinkin vähäistä, puhutaan yhteistyön toimintamallin puuttumisesta. (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen 2015, 46–47)

Tutkimusten perusteella voidaan sanoa, että kyberturvallisuuden johtaminen vaatii kokonaisvaltaista, kyberturvallisuuden toimijoita yhdistävää, järjestelmällistä ja johdonmukaista strategista johtamista sekä ajantasaista ja luotettavaa tilannekuvaa. Tutkimukset osoittavat myös, että kyberturvallisuuden johtamisessa on havaittavissa johtamisongelma, joka haluttiin ratkaista tutkimalla ulkomaista kyberturvallisuuden johtamista. Tutkimuksen tuloksista voidaan saada ideoita, joilla kansallista strategista johtamista voidaan kehittää. Kehitys taas saattaa vaikuttaa yhteiskunnallisella tasolla edellä kuvattujen tunnistettujen ongelmien ainakin osittaiseen muutokseen, joka osaltaan mahdollistaa kansallisen kyberturvallisuustoimintaympäristön mahdollisuuksia vastata paremmin tämän päivän ja tulevaisuuden haasteisiin.

2.2 Tutkimuskysymykset

Tässä tutkimuksessa tarkastellaan kyberturvallisuuden johtamista Virossa, Israelissa sekä Alankomaissa. Tutkimus pyrkii myös selvittämään, voidaanko tutkimustulosten perusteella löytää sellaisia tekijöitä, joita voidaan edelleen jalostaa kansallisen strategisen kyberturvallisuuden kehittämisajatuksiksi.

Tutkimusongelmaa on selvitetty tutkimuskysymyksellä:

- Miten kyberturvallisuuden johtaminen on toteutettu tutkimuksen kohteena olevissa valtioissa ja miten tutkimustulosten perusteella Suomen kansallista kyberturvallisuuden strategista johtamista voisi kehittää?

Tutkimuskysymyksen ensimmäisessä osassa tarkastellaan kyberturvallisuuden johtamista valituissa kohdemaissa. Tutkimuksen tutkimusongelman selvittämiseksi tarkasteltaviksi valtioiksi valittiin Viro, Israel ja Alankomaat. Valtioiden valinnassa viitekehyksenä käytettiin kansainvälisen televiestintäliiton (ITU) kyberturvallisuusindeksiä vuodelta 2014 sekä Lehto ym. (2017) raporttia ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”. Aihetta käsitellään tarkemmin luvussa seitsemän (7), joka käsittelee aineistotutkimusta kohdemaiden kyberturvallisuuden johtamisesta.

Tutkimuskysymyksen toisessa osassa tarkoitus on selvittää tutkimustulosten perusteella, voidaanko tuloksista löytää sellaisia tekijöitä tarkasteltavien valtioiden kyberturvallisuuden johtamisessa, joita voitaisiin kehittää ja hyödyntää kansallisessa kyberturvallisuuden johtamisessa. Toiseen osaan liittyy vahvasti myös kansallinen kyberturvallisuus, joten sen käsittely pääpiirteittäin on tarpeellista, jotta lukijalle tulee käsitys, miten Suomessa on toteutettu kyberturvallisuuden johtaminen kansallisella eli valtion tasolla. Luvussa viisi (5) käsitellään kyberturvallisuuden johtamista Suomessa.

2.3 Tutkimusasetelma ja menetelmä

Metsämuuronen (2000, 8-11) mukaan tutkimusmenetelmän valinta on keskeisin valinta laadullisessa empiirisessä tutkimuksessa. Tutkimusmenetelmän on oltava oikeassa suhteessa ja yhtenevä tutkimuksen teorian, metodologian sekä hypoteesin osalta. Olennaista tutkimusmenetelmän valinnassa on myös se, mistä ja millaista tietoa haetaan.

Tässä tutkimuksessa tutkimusmenetelmänä käytetään kuvailevaa kvalitatiivista aineistolähtöistä sisällönanalyysia. Tutkimuksessa kuvailevan kvalitatiivisen tutkimuksen katsotaan olevan soveltuva metodologia tutkimukseen, jonka aihepiiristä ei ole juurikaan aikaisempaa tutkimustietoa, muutamaa raporttia lukuun ottamatta (Metsämuuronen 2003, 24). Aikaisemmat tutkimukset aiheesta ovat vähäisiä eikä varsinaista viitekehystä tutkimusalueeseen ollut saatavilla. Aikaisempi tutkimustieto koskee lähinnä kyberturvallisuutta tai strategista johtamista erikseen mutta ei kyberturvallisuuden strategista johtamista, mistä tässä tutkimuksessa oli kysymys. Kvalitatiivista tutkimusmenetelmän valintaa voidaan perustella tutkimuksen kohteena olevilla asiakirjoilla, joita on tarkasteltu hyvinkin yksityiskohtaisesti kyberturvallisuuden johtamiseen soveltuvasta lähtökohdasta (Metsämuuronen 2003, 166–167). Tutkimuksen aineiston kerääminen on luonteeltaan kokonaisvaltaista tiedonhankintaa, koska tutkimusta tehdessä pyritään keräämään kaikki julkisesti saatavilla oleva keskeinen tutkimusaihetta käsittelevä aineisto soveltuvista lähteistä.

Aineiston keräämistä mietittäessä kiinnitettiin huomiota seuraaviin kysymyksiin; Millaista tietoa etsitään? Millainen aineisto tarjoaa näkökulmia ja ratkaisuehdotuksia suhteessa tutkimustehtävään ja määriteltyihin tutkimuskysymyksiin? Tutkimuksessa päädyttiin käyttämään valmista aineistoa, joka koos-

tuu pääsääntöisesti erilaisista organisaatioiden raporteista ja Internet – julkaisuista sekä strategisen johtamisen osalta myös kirjallisuudesta. Tutkimuksessa on tarkoitus kerätä ja tarkastella aineistoa, joka koostuu valtiollisten organisaatioiden julkisista materiaaleista. Tämän tyyppinen aineisto vastaa tutkimusongelmaan ja antaa perusteltuja vastauksia tutkimuskysymyksen siihen osaan, joka käsittelee valtiollisten organisaatioiden kyberturvallisuuden johtamista.

Aineistoon kuuluvia lähteitä kartoitettiin apuna käyttäen useita toisiaan täydentäviä hakupalveluita. Aineisto koostuu pääasiassa Internetin julkisista lähteistä kerätyistä asiakirjoista, jotka sisältävät julkisen hallinnon tuottamia raportteja ja tutkimusmateriaalia sekä aineistoa, joka on muodostunut erilaisista asiakirjojen liitteistä ja hallinnon kokous- ja työryhmien julkisista materiaaleista. Aineistoa on kerätty lisäksi painetuista lähteistä, kuten kirjallisuudesta, jota ei ollut sähköisesti saatavissa. Kirjallisuudesta koostuva aineisto kattaa lähinnä strategiseen johtamiseen liittyvän materiaalin. Jokaisen lähteen kohdalla arvioitiin sen soveltuvuus ja luotettavuus kriittisesti tutkimuksen aiheeseen (Metsämuuronen 2003, 191–192). Tutkimusaineisto on kerätty ensin tarkastelemalla tutkimusaihetta, sen jälkeen sen soveltuvuutta tutkimusongelmaan ja tutkimuskysymyksiin ja lopuksi aineisto on kasattu yhteen ja saatu kokonaisaineisto on pohdinnan avulla työstetty johtopäätöksiksi ja kehittämisajatuksiksi (Metsämuuronen 2003, 198).

Tutkimusaineisto kerättiin ja analysoitiin käyttämällä aineistolähtöistä sisällönanalyysia. Menetelmän avulla tarkoitus on tarkastella tutkittavaa aineistoa systemaattisesti, yhtäläisyyksiä ja eroja etsien. Analyysin avulla pyritään muodostamaan tutkittavasta ilmiöstä tiivistetty kuvaus, joka kytkee ilmiön tulokset laajempaan kontekstiin. (Tuomi & Sarajärvi 2002, 105.) Sisällönanalyysin aikana aineisto jaetaan erilaisiin teemoihin, jotta pystyttäisiin paremmin hahmottamaan aineiston eri kokonaisuudet.

Sisällönanalyysin mahdollisti tutkimustiedon saamisen sellaiseen muotoon, että sitä voidaan teoreettisesti pohtia. Teoreettinen pohdinta kuuluu tutkimuksen tekijälle, tutkijalle, jonka on pohdittava analyysin tuloksia järjellisesti ja suhteutettava ne tutkimuksen taustalla oleviin teorioihin ja viitekehykseen ja vasta sen perusteella voidaan muodostaa tutkittavasta aiheesta johtopäätöksiä tai kehitysideoita.

2.4 Tutkimuksen validiteetti ja reliabiliteetti

Tutkimuksen prosessin aikana arvioitiin tutkimuksen tekijän omia tekoja, kerrottiin lukijalle prosessin eri vaiheista, tutkimuksen taustoista sekä tutkimuksen aikana tehdyistä valinnoista, jotka vaikuttavat kokonaisuuteen, kun arvioidaan tutkimuksen luotettavuutta ja pätevyyttä.

Varto kertoo tutkimuksessaan, että tutkimuksen voi sanoa olevan pätevä, kun se tulokset nousevat kokonaisuudesta niin, että ne vastaavat tutkimukselle asetettuja päämääriä ja ovat linjassa tutkimuskohteen kanssa. (Varto 1992, 103–104)

Tutkimuksen voidaan sanoa olevan luotettava, kun sen tutkimuksen kohde ja sen perusteella tulkittu aineisto ovat keskenään yhteensopivia eikä tulosten muodostumiseen ole vaikuttaneet epäolennaiset tai satunnaiset tekijät (Varto 1992, 102–104).

Lopuksi todettakoon, että tutkimuskirjallisuudessa kerrotaan myös, että viimekädessä tutkimuksen luottavuuden määrittelee tutkija itse ja hänen rehellisyytensä. Tutkijan tekemät valinnat, ratkaisut ja teot ovat tutkimuksen arvioinnin kohteena.

2.5 Odotetut tulokset ja niiden merkitys

Tutkimuksen tuloksena selvitetään mitä strateginen johtaminen tarkoittaa kyberturvallisuuden johtamisen kontekstissa sekä määritellään kyberturvallisuuden johtamisen käsitettä. Tutkimuksen pääasiallisena tuotoksena esitellään kehittämisajatuksia kansallisen strategisen kyberturvallisuuden johtamisen osalta.

Tulosten avulla voidaan löytää sellaisia keinoja, joita johtamalla Suomen kansalliseen strategiaan, kyberturvallisuuden johtaminen kokonaisvaltaisesti ja poikkihallinnollisesti tehostuu ja siinä tulisi huomioiduksi myös yhteistyön ja koordinoinnin merkitys sekä ajantasaisen tilannekuvan tärkeys koko kyberympäristöä ohjaavana tekijänä.

3 TEOREETTINEN VIITEKEHYS

Tässä osiossa käsitellään tutkimukseen liittyvät keskeiset käsitteet. Koska tutkimus sijoittuu johtamisen aihealueelle, tarkemmin sanottuna strategisen johtamisen alueelle, on olennnaista selvittää mitä strategisella johtamisella tarkoitetaan. Tutkimukseen liittyvät myös kaksi muuta tärkeää termiä, kuten kyberturvallisuus sekä tietoturvallisuuden johtaminen. Termiä kyberturvallisuuden johtaminen ei määritellä tässä kohdassa käsitteenä, koska aikaisemmista tutkimuksista ei ole löytynyt käsitteelle vakiintuneita malleja ja näin ollen termin määritteleminen vaatii hieman enemmän avaamista ja pohdintaa. Kyberturvallisuuden johtamista tarkastellaan luvussa neljä (4).

3.1 Keskeiset käsitteet

3.1.1 Strateginen johtaminen

Ennen kuin voidaan määritellä mitä tarkoitetaan strategisella johtamisella, tarkastellaan hieman historiaa. Strategia sanalle on tutkimuskirjallisuudessa esitetty lukuisia erilaisia määritelmiä. Strategia sana (engl. strategy) tulee alunperin Kreikasta, jossa stratos merkitsi armeijaa ja –ag johtamista. Kreikkalaiset tarkoittivat strategia sanalla kenraalin taitoja (engl. art of the general). Sana voi merkitä myös yleistä taitamista tai se voidaan mieltää myös taiteeksi, mikä sisältää viittauksen siitä, että sillä oli tarkoitettu kokonaisuuksien hallintaa. (Juuti & Luoma 2009, 15.)

Juuti ym. (2009) määrittelevät kirjassaan « Strateginen johtaminen » mitä strategia on :

- Pitkän linjan suunta, joka kuljettaa toimintaa eteenpäin. Hyvä strategia vie kohti tavoitteita vaikka sen asetelma olisi huonompi kuin kilpailijoiden.
- Tapa, jolla hyödynnetään resursseja toimintaympäristössään.

- Eräänlainen ainutlaatuinen kilpailuetu, jolla pyritään saavuttamaan asetetut tavoitteet.
- Strategia voi myös olla muodostunut sidosryhmien tarpeista, jolla organisaatio pyrkii toimimaan siltä odotettujen tarpeiden mukaisesti.
- Johdonmukaisuuden luoja toiminnassa, jonka merkitys korostuu silloin kun toimintaympäristössä olevat asiat muuttuvat nopeasti

Kaplanin ja Nortonin (2002, 1-2) tutkimuksessa todetaan, että toimintaympäristöllä ja sen jatkuvalla muutoksella on suuri merkitys strategian kannalta. Strategian voidaan ajatella vastaavan kysymykseen, kuinka voidaan saavuttaa ne tavoitteet ja päämäärät, jotka sille on asetettu ? tai miksei olemassaolevia strategioita pystytä hyödyntämään riittävän tehokkaasti ? Yksi syy siihen voi olla se, että edelleen asioita johdetaan perinteisen hallinnollisen hierarkian mallin mukaisesti ylhäältä alaspäin kiinnittäen liikaa huomiota ainoastaan taloudellisiin resursseihin. Ehkä tämä hierarkinen johtamismalli on yksi syy siihen miksei esimerkiksi kyberturvallisuutta johdeta riittävän järjestelmällisesti. Valtion tasolla strategiat laaditaan yleensä useammalle vuodelle kerrallaan, mikä saattaa olla haaste strategian kannalta (Kaplan ym. 2002, 1-2), koska ainakin kyberturvallisuuden toimintaympäristössä tullaan siihen tilanteeseen, ettei riittävän hyvin kyetä reagoimaan toimintaympäristön vaatimiin muutoksiin. Tämä taas saattaa tulkintani mukaan johtaa siihen, että toteutetaan sellaisia strategioita, joita ei pitäisi enää toteuttaa ollenkaan, koska se ei enää palvele muuttunutta kybertoimintaympäristöä sen vaatimalla tavalla.

Näiden määritelmien saattelemana päästään kohti strategisen johtamisen määritelmää. Juuti ym. (2009, 279) johtavat strategian määritelmän kolmen eri maailmankuvan (rationaalisen, kompleksisen sekä postmodernin) määritelmistä seuraavanlaiseksi : Strategia on sitä, mitä tahdotaan, tehdään ja puhutaan . Näin ollen *strateginen johtaminen tarkoittaa edellä mainittujen tahtomisen, tekemisen ja puhumisen aikaansaamista.* Koska kirjoittajat ovat pelkistäneet strategisen johtamisen käsitteen näin lyhyeen muotoon, on tarvetta hieman selventää sen tarkoitusta. *Tahtominen* viittaa jonkun idean muodostamiseen ja sen toteuttamispyrkimykseen. *Tekeminen* käsittää taas hyvää tarkoittavan vuorovaikutuksen. *Puhuminen* tarkoittaa merkityksiä, joilla pyritään tuottamaan ja vaihtamaan ja rakentamaan identiteettiä.

Kroll ym. (1998, 2-3) luonnehtii strategisen johtamisen tarkoittavan kokonaisuutta, joka käsittää tavoitteiden asettamisen sen määrittelemässä toimintaympäristössä. Strategiseen johtamiseen liittyy myös strateginen prosessi, jonka tarkoitus on aikaansaada päätöksiä asetettujen tavoitteiden osalta. Strategiaprosessi huomioi myös keskeisten sidosryhmien vaatimukset, tavoitteet sekä rajoitteet (Kyrölä 2010, 16). Samaisessa tutkimuksessa myös todetaan, että strateginen johtaminen tarkoittaa kaikkia niitä toimia, joilla pyritään vastaamaan paremmin ympäristönsä vaatimuksiin ja näin saavuttaa tehokkaammin ne tavoitteet, jotka toiminnalle on asetettu.

Strateginen johtaminen voidaan nähdä pyrkimyksenä ennustaa tulevaisuutta sekä ohjata strategista toimintaa tavoitteiden ja päämäärien

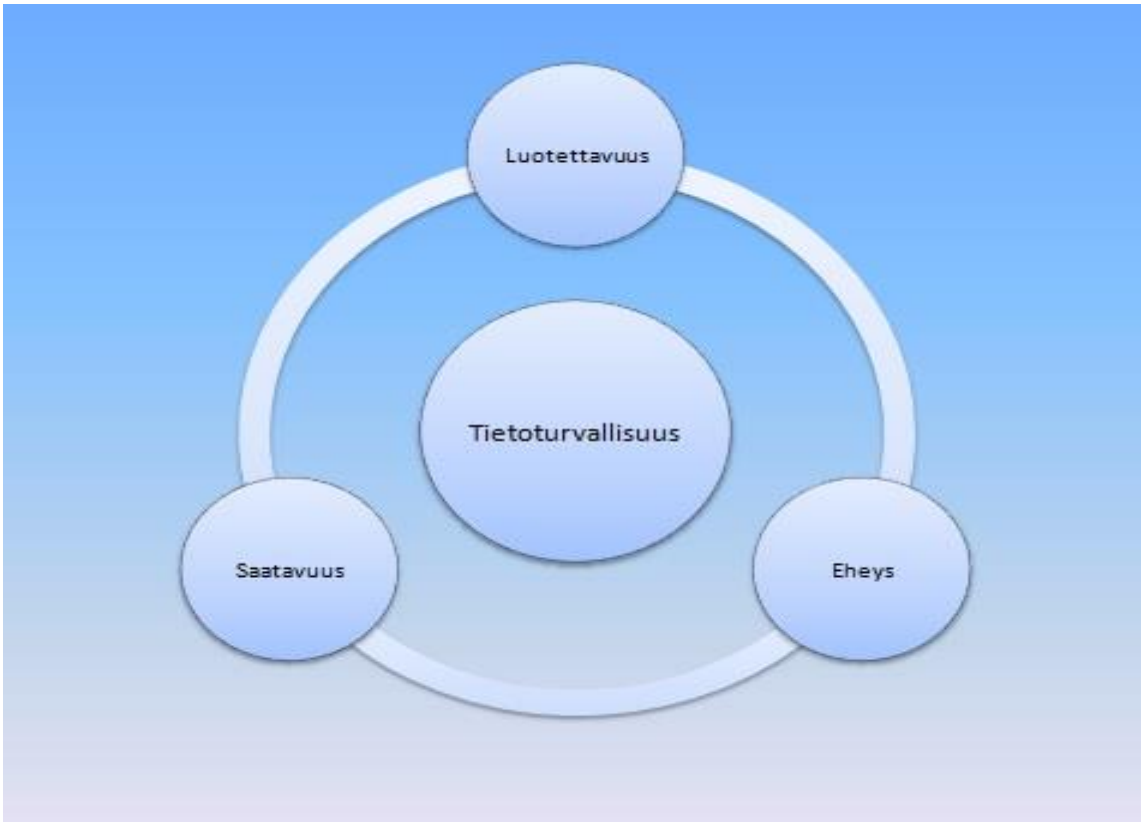
saavuttamiseksi. Strategian tarkoitus on ohjata onnistumaan tulevaisuuden toimintaympäristössä. Johtaminen nähdään prosessina, jonka tarkoitus on suunnitella ja toimeenpanna strategioita, joilla pyritään huomioimaan toimintaympäristössä tapahtuvat muutokset. (Kyrölä 2010, 16-18)

Edellä strategian määrittelyn yhteydessä mainittiin, että yhä edelleen käytetään ylhäältä alaspäin laskevaa hallinnollista johtamismallia. Tällaisessa mallissa strategiset päätökset tehdään ylimmässä johdossa. Tälläinen malli ei kuitenkaan enää toimi nykymaailmassa vaan tarpeellista olisi käyttää jatkuvaa viestintää, jotta ajantasainen strategia ja tilannekuva olisi selväkielisenä ja ymmärrettävässä muodossa myös organisaation alemmilla tasoilla. Tähän päämäärään voidaan päästä vain jakamalla päätösvaltaa ja vastuuta myös alemmille tasoille strategisten päätösten osalta. (Kaplan & Norton 1996)

3.1.2 Tietoturvallisuuden johtaminen

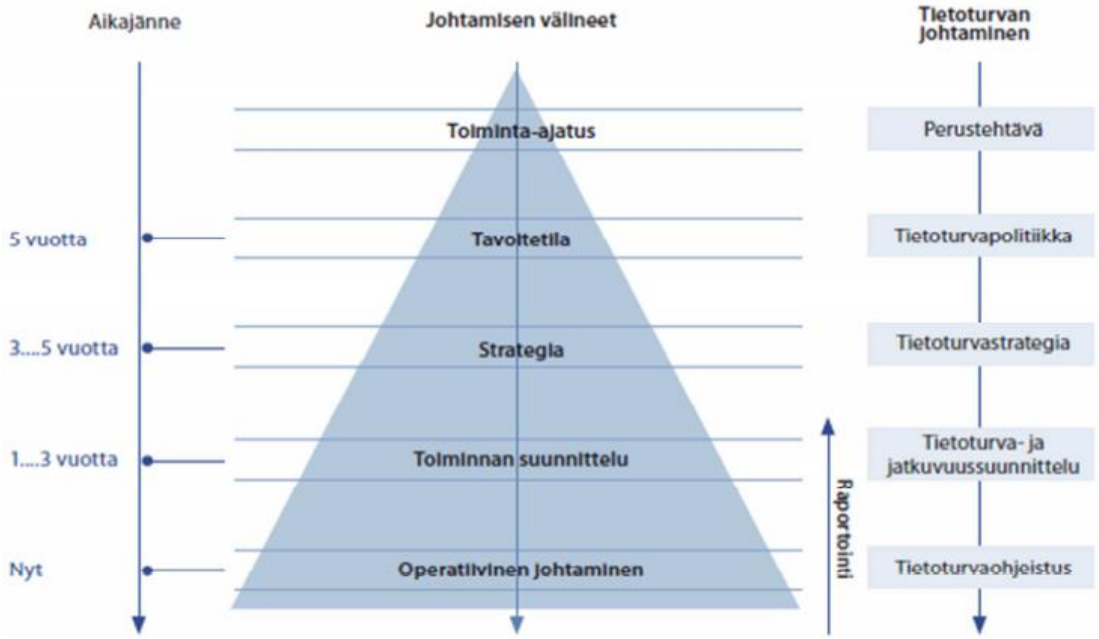
Valtionvarainministeriö (2007, 13) määrittelee yleisohjeessaan tietoturvallisuuden tarkoittavan tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä.” Määritelmällä pyritään kuvaamaan tietoturvallisuuden tärkeintä tavoitetta, joka on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen niihin kohdistuvilta erilaisilta uhilta. Tämä edellyttää tietojen, järjestelmien, tietoliikenteen sekä erilaisten palveluiden asianmukaista suojaamista (Valtiokonttori). Tutkimuksen kohderyhmänä on valtiolliset toimijat, joiden tietojärjestelmien, tietojen ja yhteiskunnalle elintärkeiden toimintojen keskeytyksetön toiminta on erityisen tärkeää. Tämä edellyttää riittävää tietoturvallisuuden tasoa.

Kansainvälinen ISO/IEC 27000 :2009 standardi määrittelee tietoturvallisuuden tavoitteet. Näihin kuuluu tiedon, datan, informaation tai tietämyksen, luottamuksellisuuden, eheyden ja saatavuuden säilyttämisen. Standardissa, kuten myös aikaisemmassa määritelmässä, luottamuksellisuudella tarkoitetaan että tiedon näkyminen pyritään estämään ulkopuolisille, eheyden tarkoitus on varmistaa, ettei tietoa pystytä muokkaamaan ilman oikeutettua pääsyä ja tiedon saatavuudella sitä, että vain oikeutetut henkilöt voivat saada tiedon käyttöönsä. Kuvio 1 osoittaa tietoturvallisuuden tavoitteet.



Kuvio 1 Tietoturvallisuuden tavoitteet

Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 13) määrittelee *tietoturvallisuuden johtamisen osaksi kaikkea johtamistoimintaa, ja tietoturvallisuudesta huolehtiminen kuuluu valtion johdon lisäksi kaikille ministeriöille sekä yhteistyöelimille.* Jotta tietoturvallisuuden johtaminen olisi mahdollista, johdolla tarvitsee olla ajantasainen tilannekuva toimintaympäristöstä, mukaanlukien arviot mahdollisista toimintaa uhkaavista riskeistä. Tämän lisäksi ylin johto on sitoutettava tietoturvallisuuden johtamiseen jotta se ylipäänsä olisi edes mahdollista. Tietoturvallisuuden johtamisen perustana tulee olla ajantasainen tietoturvalipolitiikka. Tämä onnistuu parhaiten huolehtimalla tietoturvaprosesseista alusta loppuun asti. Toimet jolla varmistetaan ajantasainen tietoturvapolitiikka kuuluu muunmuassa uusien tietojärjestelmien tietoturvatasojen määritykset, säännölliset päivitykset tietoturvakäytäntöihin sekä järjestelmistä huolehtiminen niiden hankinnasta aina niistä luopumiseen asti. Kuviossa 2 on esitetty valtionhallinnon malli johtamisjärjestelmän ja tietoturvallisuuden välisestä suhteesta.



Kuvio 2 Johtamisjärjestelmän ja tietoturvallisuuden välinen suhde (Tietoturvallisuudella tuloksia -yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 27).

Valtiovarainministeriön raportissa (2006, 11-27) mainitaan, että tietoturvallisuutta tulee tarkastella erityisesti valtion tasolla, koska digitaalisoituva maailma tuo uudenlaisia uhkia valtion eri virastoille ja laitoksille, jotka uhkaavat toiminnan jatkuvuutta sekä toiseksi, voimakas yhteiskunnan toimintojen siirryminen tietoverkkoihin luo toiminnalle tarvetta yhtenäistää ja kehittää palvelujaan. Tietoturvallisuudelle on kysyntää ja etenkin tietoturvallisuuden johtaminen korostuu nyky-yhteiskunnassa entisestään edellä mainituista seikoista johtuen. Raportin mukaan tietoturvallisuuden johtamisen tulee olla osa valtion kokonaisvaltaista riskien- ja laadunhallintaa sekä tietoturvallisuuden johtamisessa huomioidaan vahvasti strategiset tavoitteet, toiminnan luonne sekä valitut suuntalinjat.

Yleisesti puhuttaessa tietoturvallisuudesta ja sen johtamisesta kirjallisuudesta löytyy useita, toisistaan jonkin verran poikkeavia määritelmiä. Yhteistä näille kaikille määritelmille kuitenkin on, että tietoturvallisuuden johtaminen tapahtuu toimintaympäristön ylimmällä tasolla ja se tähtää tavoitteisiin joilla pyritään turvaamaan tiedon luotettavuus, eheys sekä saatavuus. Eroja löytyi ainakin sen osalta, puhutaanko hallinnollisesta kansallisesta tietoturvan johtamisesta vai pienen yrityksen tietoturvan johtamisesta. Tämä seikka myös vaikuttaa siihen, onko organisaatiossa nimettyä henkilöä, joka vastuulla tietoturvallisuuden johtaminen on. Pienissä yrityksissä ei välttämättä ole ollenkaan edes strategista suunnitelmaa tietoturvallisuudesta, kun valtiollisia toimijoita ohjaa lait ja asetukset siitä, millaisia tieturvastandardeja tulee noudattaa.

Ashenden (2008, 194-200) luonnehtii tietoturvallisuuden johtamista asiaksi, joka ei enää tähtää ainoastaan luotettavuuden, eheyden ja saatavuuden turvaamiseen vaan sen avulla pyritään luomaan todellisia liiketoimintahyötyjä suojaamalla ja helpottamalla tiedon ohjattua jakamista sekä hallita siihen liittyviä riskejä muuttuvassa uhkaympäristössä. Koska turvallisuus käsitteenä on kehittynyt sekä leveys että syvyys suunnassa, sen tulee olla upotettu kaikkiin toimintoihin. Tästä syystä se tarvitsee toimiakseen johtamista, jonka tarkoituksena on selvittää miten tavoitteet voidaan saavuttaa tehokkaasti ja johdonmukaisesti.

ISO 27001 standardi määrittelee tietoturvallisuuden johtamisen osaksi kokonaisvaltaista johtamista, joka perustuu liiketoiminnan riskien tunnistamiseen vaihvistamalla, toteuttamalla, valvomalla, tarkastamalla, ylläpitämällä ja kehittämällä tietoturvallisuutta. Siihen sisältyy organisaation rakenne, menettelytavat, suunnittelu, vastuullisuus, käytännöt, prosessit ja resurssit. (tutkijan oma käännös.)

Toisaalta tietoturvallisuuden johtamisen on tarkoitus varmistaa riitävällä tietoturvan hallinnalla, että organisaation tiedot on turvassa sekä antaa luottamus kolmansille osapuolille (ISO 27001). Yleisesti voidaan todeta, että ilman tietoturvallisuuden johtamista ei voida tietää mitä on tehty, kuka on tehnyt, miksi on tehnyt ja mikä on ollut sen tarkoitus.

Ashenden (2008, 194-200) toteaa artikkelissaan, että (Pursel, 2004) tekemässä tutkimuksessa todetaan tekijöitä, jotka vaarantavat tietoturvallisuuden johtamisen. On kiinnostaa huomata, että listan ensimmäisenä mainitaan tietämys ja kokemus ennen muita, enemmän teknisiä tekijöitä. Kun lisäksi otetaan huomioon, että menestyksekäs tietoturvallisuuden johtaminen edellyttää asiantuntijuutta, johtajuutta, näkemyksiä sekä hyviä toimintatapoja, voidaan nähdä ns. pehmeiden taitojen merkitys menestyksekkäässä johtamisessa.

3.1.3 Kyberturvallisuus ja –resilienssi

Sanan kyber katsotaan olevan peräisin Kreikan kielen sanasta ”kybereo”, joka tarkoittaa vapaasti käännettynä ohjata, opastaa tai hallita. Suomen kielen kyber sana on peräisin englanninkielisestä sanasta ”cyber”, joka viittaa informaatioteknologiaan ja virtuaaliseen todellisuuteen (Limnell 2014, 3). Kyber-sanaa käytetään lähes poikkeuksetta yhdyssanan osana, eikä niinkään yksittäin. Sanan sisällöllinen merkitys painottuu sanan loppuosaan, kuten kyberuhka tai kybertoimintaympäristö. Kokonaisturvallisuuden sanastossa (2014) kyberturvallisuus (cybersecurity) määritellään kahdeksi erilaiseksi tilaksi. Ensinnäkin se nähdään tilana, jossa uhat ja riskit ovat hallinnassa kybertoimintaympäristössä kriittisen infrastruktuurin sekä muiden ympäristössä vaikuttavien toimintojen osalta. Toiseksi se nähdään tilana, joka perustuu kybertoimintaympäristön luottamukseen ja toiminnan turvaamiseen. Kyberturvallisuuteen voidaan nähdä kuuluvan kaikki ne toimenpiteet, joilla voidaan havaita, hallita ja torjua erilaisia kyberuhkia. (Kokonaisturvallisuuden sanasto, 2014) Kybertoimintaympäristö

ymmärretään tässä yhteydessä koostuvan yhdestä tai useammasta tietojärjestelmästä, jotka kykenevät tiedonsiirtoon toisten järjestelmien kanssa (Kokonaisturvallisuuden sanasto, 2014).

Solms ja Niekerk (2013) määrittelevät artikkelissaan ”From information security to cyber security” kyberturvallisuuden koostuvan kolmesta kokonaisuudesta, jotka ovat kyberavaruus, tietojärjestelmät, jotka tukevat kyberavaruutta sekä toimenpiteistä kyberympäristön käyttäjien suojaamiseksi. Tämä kattaa sekä kansalliset että kansainväliset sekä aineettomat ja aineelliset kapasiteetit, jotka ovat alttiita niihin kohdistuville hyökkäyksille. Selventääkseni tätä määritelmää, voidaan ajatella, että kyberturvallisuudella on tarkoitus suojata kolmea tärkeää asiaa. Nämä ovat kyberavaruus, yhteydet välittävät verkot sekä niihin kiinnittyvät laitteet sekä niiden käyttäjät. Määritelmässä kapasiteetilla voidaan tarkoittaa vaikkapa pankkitiliä tai henkilön tietokoneessa olevaa tietoja sisältävää tiliä.

Solms ja Niekerk (2013) artikkelissa on tärkeää huomata, että kyberturvallisuuden osaksi katsotaan kuuluvan myös laitteet ja niiden käyttäjät, jotka liittävät digitaalisen turvallisuuden fyysiseen turvallisuuteen, kuten esimerkiksi vedenjakelulaitos. Tästä näkökulmasta katsottuna voidaan sanoa, että kyberturvallisuus on tietoturvallisuutta laajempi käsite, kun tietoturvallisuuden tarkoitus on suojata ainoastaan tietoa.

Suomen Kyberturvallisuusstrategiassa (2013) kyberturvallisuus määritellään ”tavoitetilaksi jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvataan”. Tavoitetilalla tarkoitetaan sellaista tilaa, jossa kybertoimintaympäristöstä ei aiheudu vaaraa tai haittaa tietojenkäsittelystä aiheutuvalle toiminnalle. Luottamuksella tarkoitetaan toiminnan vaatimaa riittävää tietoturvallisuutta, jotta pystytään havaitsemaan ja estämään tietoturvaan kohdistuvien uhkien toteutuminen. Samaisessa strategiassa todetaan, että kyberturvallisuudella tarkoitetaan yhteiskunnan tärkeisiin ja kriittisiin toimintoihin kohdistuvia kyberuhkia, joita pyritään ennakoivasti hallitsemaan ja tarvittaessa myös kestämään.

Edellä on pyritty selittämään kyberturvallisuuden käsitettä aikaisemmin esitettyjen määritelmien perusteella. Yhtä ainoaa oikeaa vastausta määritelmään ei ole, koska vakiintunutta merkitystä käsitteelle ei ole Suomessa vielä olemassa. Esitettyjen määritelmien perusteella, voidaan sanoa, että kyberturvallisuudella pyritään ennakoimaan, havaitsemaan, estämään, vastaamaan ja tarvittaessa myös sietämään niin sisä- kuin ulkopuolelta tulevia kyberturvallisuutta vaarantavia uhkia sekä pyrkiä turvaamaan digitaalinen toimintaympäristö, jotta ympäristössä käsiteltävä tieto olisi luotettavaa ja ajantasaista. Koska kyberturvallisuudella voidaan nähdä fyysinen yhteys yhteiskunnan toimintoihin, tulee huolehtia yhteiskunnan kriittisten toimintojen osalta niiden vaatiman turvallisuustason ylläpitämisestä ja toiminnan kehittämisestä, jotta häiriötön toiminta voidaan turvata yhteiskunnan toiminnan ja turvallisuuden takaamiseksi kaikissa tilanteissa. Tämä edellyttää ajantasaista tilannekuvaa toimintaympäristöstä sekä uhkien riittävää nopeaa havaitsemista ja analysointia. Huomiota tuli-

si myös kiinnittää kansallisten toimintojen ja järjestelmien kykyyn palautua niihin kohdistuvista uhista ja kykyyn jatkaa normaalia toimintaa.

Puhuttaessa kyberturvallisuudesta ja kyberuhista, ei voida olla puhumatta resilienssistä. Kyberresilienssi on uusi käsite, eikä sille ole vakiintunutta määritelmää olemassa. Eri yhteyksissä termiä on määritelty eri tavalla, riippuen siitä, katsotaanko sitä esimerkiksi maanpuolustuksen kannalta vai katsotaanko sitä esimerkiksi organisaation tietojärjestelmän kannalta. Tutkija määrittelee resilienssin tarkoittavan kyberuhkien sietokykyä eli tietoista kykyä, jossa pystytään sietämään ja sopeutumaan vallitsevaan häiriötilanteeseen sekä järjestelmän kykyä toipua tästä häiriötilanteesta ennen häiriön syntymistä edeltäneeseen tilaan sekä oppia tästä häiriöstä ja kehittyä. Tutkija itse ymmärtää käsitteen jatkuvana prosessin omaisena toimintana, jossa järjestelmä kehittyy aina kohdatessaan häiriön. Ajatusta resilienssin määritelmästä kyberturvallisuudessa tukee professori Jarno Limnéllin kirjoitus, jossa resilienssi määritellään kyvyksi selvitä normaalitilanteista poikkeavista häiriötilanteista ja kyvyksi palauttaa toiminnot nopeasti häiriötilannetta edeltäneelle tasolle (Limnéll 2014). Puolustusvoimien tutkimuslaitoksen julkaisu on samoilla linjoilla. Julkaisussa kuvataan kyberresilienssi sarjaksi toisiinsa liittyviä tapahtumia, jotka kehittyvät käyttäen perustana olevaa järjestelmää. Kehittyminen tapahtuu juuri silloin kun jokin häiriötila vaikuttaa järjestelmään, jolloin sen normaalitila muuttuu ja järjestelmän tulee vastata häiriöön, toipua siitä samalla kun ylläpitää toimintoja (Uusipaavalniemi & Kovâcs 2016, 1). Kyberturvallisuusstrategiassa tarkoituksenmukainen sietokyky mukautetaan siten, että kyetään luomaan kokonaisturvallisuuden päämäärien mukaista ennakointi- ja palautumiskykyä, kykyä toimia häiriötilanteissa sekä kykyä palautua häiriötilanteiden jälkeen. Tämä edellyttää strategiselta johtamiselta kykyä ennustaa kybertoimintoympäristössä tapahtuvia muutoksia. Jotta ”ennustaminen” olisi mahdollista, on tiedettävä mitä ympäristössä tapahtuu eli tarvitaan ajantasaista tilannekuvaa. Strategisten päätösten tueksi tarvitaan myös kykyä siirtää päätökset käytäntöön.

4 KYBERTURVALLISUUDEN STRATEGINEN JOHTAMINEN

Tämän luvun tarkoitus on selvittää mitä tarkoitetaan kyberturvallisuuden strategisella johtamisella. Luvun alussa pohditaan miten kyberturvallisuus ja tietoturvallisuus eroavat toisistaan. Tämän jälkeen tarkastellaan strategista johtamista tietoturvallisuuden konseptissa, jonka jälkeen siirrytään tarkastelemaan kansallista kyberturvallisuuden johtamista. Luvun lopussa rakennataan malli: kansallinen kyberturvallisuuden johtamisen prosessi.

4.1 Tietoturvallisuuden ja kyberturvallisuuden erot

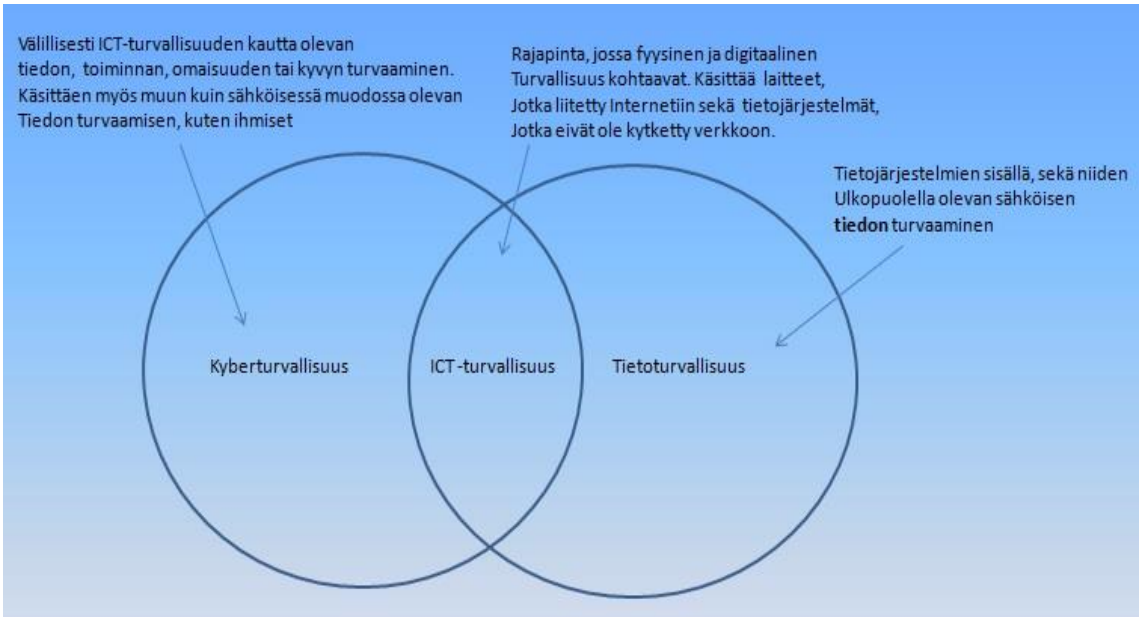
Holmgren (2016, 67–68) tutkimuksessaan mieltää kyber-sanan digitaaliseksi ”tilaksi”, jossa yhdistyy informaatioteknologia ja jossa toimitaan erilaisten tietoverkkojen välityksellä. Tämä voidaan myös ymmärtää tilaksi, joka on fyysiseen ympäristöön verrattavissa ja jossa voidaan toimia kuten fyysisessä ympäristössä.

Kyberturvallisuudella on merkittävä rooli yhteiskunnassa, jokaisen ihmisen osalta. Digitalisaatio on tuonut kyberin osaksi jokapäiväistä elämää ja siitä hyötyy niin yksittäiset ihmiset, yritykset kuin valtiotkin ja yhteiskunnan kannalta sen häiriötön toiminta on tärkeää. Solms & Niekerk (2013) artikkelissa aikaisemmin todettiin kyberturvallisuuden koostuvan kolmesta kokonaisuudesta: kyberavaruus, tietojärjestelmät, jotka tukevat kyberavaruutta sekä toimenpiteistä kybertoimintaympäristön käyttäjien suojaamiseksi. Tämä tarkoittaa sitä, että kyberturvallisuudella pyritään suojaamaan kolmea tärkeää asiaa eli kyberavaruutta, yhteydet välittäviä verkkoja sekä niihin yhteydessä olevia laitteita sekä laitteiden käyttäjiä.

Tietoturvallisuuden lähtökohdat ovat hieman erilaiset. ISO/IEC 27000 :2009 standardin määritelmästä voidaan havaita, että tietoturvallisuus nimensä mukaisesti keskittyy tietoon ja tiedon suojaamiseen sähköisessä toimintaympäristössä. Jo pelkästään näiden määritelmien pohjalta voidaan

huomata, että kyberturvallisuus on tietoturvallisuutta laajempi käsite, koska se käsittää tiedon turvaamisen lisäksi myös linkin fyysiseen maailmaan. Kybertoimintaympäristöön kohdistuva kyberhyökkäys voi näin koskettaa suoraan ihmisiä tai yhteiskunnan infrastruktuuria, kun tietoturvaympäristöön kohdistuvan hyökkäyksen vaikutus on aina epäsuoraa (Solms & Nierek, 2013).

Esimerkkinä voidaan ajatella vaikka sähköyhtiötä, jonka toimintaa ohjataan tietojärjestelmien avulla. Sähkönjakeluun kohdistuva kyberhyökkäys saattaa katkaista sähkönjakelun useilta ihmisiltä sekä tärkeiltä yrityksiltä ja laitoksilta jolloin yhteiskunnan toimintaan aiheutuu häiriö. Kyberturvallisuuden toimintaympäristössä pyritään turvaamaan siis myös mahdolliset fyysiset vahingot, jotka aiheutuvat verkon kautta tehtävistä haitallisista kybertoimista. Kuviossa 3 havainnoillistetaan kyberturvallisuuden ja tietoturvallisuuden suhdetta ja eroja. Kuvasta voidaan havaita, että sektorit menevät osittain päällekäin, jolla tarkoitetaan sitä, että niin kyberturvallisuudesta kuin tietoturvallisuudestakin voidaan erottaa sekä fyysinen että digitaalinen kohde ja tavoite. Tässä välissä olevaa aluetta kutsutaan ICT-turvallisuudeksi koska sen sisältämä sähköinen toiminta ja tietojen turvaaminen on vain yksi osa-alue kokonaisuudesta ja kokonaistavoitteesta (Solms & Nierek, 2013).



Kuvio 3 Tietoturvallisuuden, ICT -turvallisuuden ja kyberturvallisuuden erot, mukaillen (Solms & Niekerk, 2013, 101)

4.2 Strateginen johtaminen tietoturvallisuuden kontekstissa

Organisaation ylin johto on vastuussa tietoturvallisuudesta. Jos johto ei ole sitoutunut tietoturvallisuuden toteuttamiseen eikä tietoturvallisuutta ole liitetty

osaksi organisaation strategisia päämääriä, organisaation kyky tietoturvallisuuden toteuttamisessa ja tiedon suojaamisessa on hyvin rajoitettua, jos sellaista onkaan (Solms 1996, 283). Johdon tehtävä on tietoturvatavoitteiden ja periaatteiden varmistaminen osana organisaation toiminnan suunnittelua. Lisäksi johdon tehtävä on varmistaa, että toiminnassa toteutuu asianmukainen tietoturvallisuus sekä huolehtia riittävän turvallisuustason vaatimasta rahoituksesta (VAHTI 7/2009, 10).

Aikaisemmissa Luvuissa on luotu käsitys siitä mitä on strategia ja strateginen johtaminen sekä avattu tietoturvallisuuden käsitettä. Tämä osuuden tarkoitus on yhdistää tietoa siitä, mitä tarkoitetaan strategisella johtamisella tietoturvallisuuden kontekstissa eli miten johdon tulisi huomioida tietoturvallisuuden merkitys tehtäessä strategisia päätöksiä.

Tietoturvallisuuden suunnittelu ja organisointi tulee toteuttaa sillä tavalla, että se tukee organisaation strategiatavoitteiden saavuttamista. Strategisessa suunnittelussa tulee huomioida tietoturvallisuuden tavoitteet sekä toimenpiteet, joilla tavoitteet voidaan saavuttaa. Lisäksi strategisessa johtamisessa tulee arvioida tietoturvallisuuden vaatimat riskienhallintaprosessit (VAHTI–ohje).

Johdolla tulisi olla kokonaiskuva toiminnasta, jotta tiedetään, minkälainen tietoturvallisuuden johtamisjärjestelmä organisaatiossa tulisi olla. Tämä on erityisen tärkeää, koska käytössä olevat resurssit tulee kohdistaa niille alueille, joissa tarvitaan eniten turvallisuusnäkökohtien huomioon ottamista. Mukaillen Laaksonen (2006, 114–117) seuraavia kysymyksiä organisaatiossa tulisi pohtia;

1. Käsitelläänkö organisaatiossa sellaista tietoa, josta voisi olla hyötyä jollekin?
2. Miten tieto tulisi suojata, jotta siihen ei pääsisi käsiksi? Kuka tietoa mahdollisesti havittelee ja miten?
3. Voidaanko organisaation sisällä olevaa tietoa viedä ulos? Jos voidaan niin miten?
4. Velvoittaako laki organisaation tietojen suojaamista? Millä tavalla?
5. Millainen on organisaation toimintaympäristö? Millaisia uhkia toimintaympäristö voi aiheuttaa nyt ja tulevaisuudessa?
6. Miten organisaatiossa otetaan tällä hetkellä huomioon tietoturvallisuus? Voidaanko se yhdistää olemassa oleviin strategioihin paremmin?

Valtiovarainministeriön raportti Tietoturvatavoitteiden asettaminen ja mittaaminen (2006, 11-27) kiteyttää, että tietoturvallisuuden strategisessa johtamisessa tulee huomioida ylimmän johdon asettamat strategiset tavoitteet tiedon luotettavuuden, eheyden ja saatavuuden turvaamisen osalta. Strateginen johtaminen tapahtuu aina organisaatiotasolla ja siinä on tärkeää huomioida toimintaympäristön asettamat vaatimukset tietoturvallisuudelle. Organisaation tulee tunnistaa tietoturvallisuuden tarpeet ja odotukset sekä sen tulee kyetä ennakoimaan mahdollisia muutoksia niin toimintaympäristössä kuin sen ulkopuolella. Jotta strategiassa määritellyt linjaukset tietoturvallisuuden osalta voidaan toteuttaa käytännön tasolle, vaaditaan selkeää ja ymmärrettävää viestintää sekä henkilöstön kouluttamista strategiassa asetettuihin

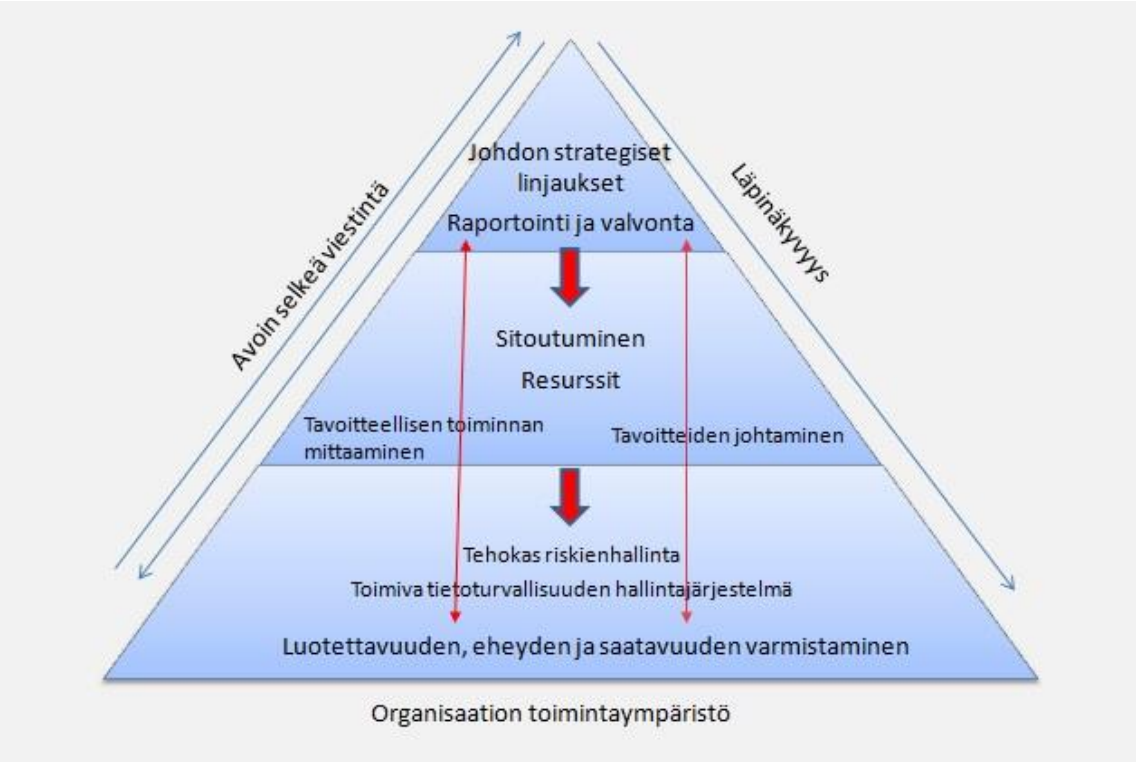
tietoturvallisuutta koskeviin linjauksiin. Tämä mahdollistaa tietoturvallisuuden liittämisen osaksi koko organisaatiota, jolloin voidaan puhua tietoturvakulttuurista. Tällöin koko organisaatio toteuttaa ja kehittää tietoturvallisuutta koskevia strategisia linjauksia (Valtiokonttorin ohje).

Strategisessa tietoturvallisuuden johtamisessa tulee nähdä kokonaiskuva tiedon turvaamisesta sekä siihen käytettävistä menetelmistä, joita on kehitettävä koko ajan muuttuvan toimintaympäristön mukaan. Laissa määritellyt tietoturvallisuutta koskevat säädökset (etenkin julkishallinnon osalta) sekä tiedon turvaamista koskevia valittuja standardeja on noudatettava täsmällisesti. Tietoturvallisuuden strategisten päätösten on oltava linjassa myös organisaation muiden strategisten linjausten kanssa, koska tietoturvallisuusajattelu on liitettävä mukaan koko organisaation toimintaan. Strategian toteuttamisessa on kiinnitettävä huomiota henkilöstön koulutukseen, jotta strategiset päätökset eivät jää ainoastaan pöytälaatikkotasolle tai että ne ovat niin vaikeasti ymmärrettävässä muodossa, ettei niiden mukaan osata toimia. (Maijanen (2015, 30), Ezingeard et al., 2005, 23).

Kuviossa 4 on esitetty tutkijan näkemys strategisesta johtamisesta tietoturvallisuuden kontekstissa. Kuviosta voidaan havaita, että strategiset päätökset tehdään ylimmässä johdossa, joka myös vastaa tehtyjen päätösten valvonnasta ja raportoinnista. Ylimmältä johdolta odotetaan läpinäkyvyyttä päätöksissään läpi koko organisaation. Sekä johdolla, että koko organisaatiolla on vastuu avoimesta ja selkeästä viestinnästä, joka edesauttaa strategisten päätösten ymmärtämistä alemmilla organisaation tasoilla sekä mahdollistaa ylimmän johdon paremman ymmärtämisen asiantuntijoiden teknisestä viestinnästä. Strateginen johtaminen edellyttää myös sitoutumista tietoturvallisuuden kehittämiseen sekä tarvittavien resurssien jakamisesta riittävän tietoturvatason saavuttamiseksi ja toiminnan eteenpäin viemiseksi. Toteuttamalla edellä kuvattua menetelmää, voidaan organisaation kaikilla tasoilla toteuttaa tietoturvallisuutta ja näin luoda tietoturvakulttuuria koko organisaatioon. Tämä taas mahdollistaa tehokkaan riskienhallinnan, jolloin kokonaisuutta voidaan luonnehtia toimivaksi järjestelmäksi, jossa hallitaan riskejä kokonaisvaltaisesti. Kuvio myös kertoo tietoturvallisuuden perimmäisen ja tärkeimmän tavoitteen eli tiedon luotettavuuden, eheyden ja saatavuuden varmistamisen koko organisaatiossa, kaikilla tasoilla.

Kuviossa 4 myös mainitaan strategisten päätösten tavoitteiden johtaminen koska sitä tulee toteuttaa organisaation välitasoilla esimiesten toimesta. Esimiehille kuuluu näin ollen myös toiminnan mittaaminen, jolloin saadaan kokonaiskäsitystä toimintaympäristön tilasta. Toimintaympäristön mittaaminen kertoo, miten hyvin strategian määrittelyssä on onnistuttu ja onko organisaatio saavuttanut toiminnalle asetettuja tavoitteita. Toimintaa voidaan mitata tulosmittareilla, jotka kuvaavat aikaansaannoksia. Tulosmittareissa on kuitenkin huomioitava, että niitä voidaan vain käyttää historiatietojen hyödyntämiseen, koska niihin sisältyy aikaviive. Suoritusmittareilla taas voidaan mitata tämän hetken tapahtumia, jolloin ne ikään kuin toimivat ennakoivasti. Molempia mittareita tarvitaan, sillä organisaation toimintaa tulee mitata niin ennakoivasti, ajantasaisesti kuin pidemmältäkin aikaväliltä katsottuna (Lindfors (2011, 8), Salminen (2008,

129–130). Tietoturvallisuuden konseptissa, jossa toimintaympäristön muutokset voivat tapahtua hyvinkin nopealla aikavälillä, on erityisen tärkeää kiinnittää huomiota sellaisten mittareiden käyttöön, jolla voidaan mitata organisaation toimintaa ja strategian toteutumista ennakoivasti.



Kuvio 4 Tietoturvallisuuden strateginen johtaminen.

Tietoturvallisuuden strateginen johtaminen on olennainen osa erilaisten tietoon kohdistuvien riskien ja tietoympäristöä uhkaavien poikkeustilanteiden kokonaisvaltaista hallintaa. Strategisella johtamisella tietoturvallisuuden konseptissa on tarkoitus ohjata organisaation eri painopistealueiden toimintaa, luoda toiminnalle pääsuunnat ja tavoitteet sekä määritellä toimintaan vaikuttavia riskejä ja resursseja. Organisaatiossa voidaan tarkastella liiketoiminnan eri osa-alueita, kuten tietojärjestelmiä tai kriittisiä toiminnan kannalta tärkeitä prosesseja ja pyrkiä kohdistamaan näihin riittävä määrä resursseja ja toimenpiteitä, jolloin kokonaisuuden johtaminen ja tiedon turvaaminen mahdollistuu.

Tietoturvallisuuden strategisella tasolla pyritään ensinnäkin arvioimaan ja tarkastelemaan organisaatiotason toimintaan vaikuttavia riskejä, toiseksi estämään ja pienentämään organisaatioon kohdistuvien riskien vaikutuksia ja lopuksi hallitsemaan kokonaisvaltaisesti näitä riskejä. Tietoturvallisuuden johtaminen tarkoittaa käytännössä riskienhallinnan toteuttamista (Tietoturvallisuudella tuloksia 2007, 15).

Strateginen johtaminen voidaan myös ajatella tapahtuvan eri organisaatiotasoilla tapahtuvaan johtamiseen. Yhden mallin mukaan jaottelu voi olla seu-

raavanlainen: konsernitason johtaminen, toimialatason johtaminen sekö operatiivisen tason johtamiseen. Jokaisella tasolla sen tason johtajat vastaavat strategisesta johtamisesta ja strategioiden tekemisestä. Alemmilla tasoilla tehtävät strategiat pohjautuvat ylimmän tason strategisiin visioihin ja tavoitteisiin ja ovat eräänlaisia suunnitelmia miten ylemmän tason strategiaa toteutetaan alemmilla tasoilla. Näin voidaan ajatella sen toimivan myös valtion tasolla. Valtion ylin johto päättää kansallisen tason strategisista tavoitteista ja päämääristä ja ministeriötason strategiset päätökset pohjautuvat näin ollen kansallisen tason strategisiin päätöksiin. (Hill 2001, 10–15) Tietoturvallisuuden johtamista voidaan myös toteuttaa tämän jaottelun mukaisesti kuviossa 4 esitetyn kaavion mukaisesti, jolloin jokaisella organisaatiotasolla huomioidaan ja toteutetaan strategisia tavoitteita, jotka on laadittu ylimmällä tasolla.

Julkisella sektorilla monet säädökset ja lait ohjaavat tietoturvallisuutta. Tietoturvallisuuden korkea taso on tärkeää niin yksityisen kansalaisen, hallinnon toiminnan kuin julkisuuskuvankin kannalta. Tästä syystä organisaatiot joutuvat noudattamaan ylhäältäpäin tulevia määräyksiä tietoturvallisuuden osalta. Yksityisellä puolella tilanne on erilainen. Kun varsinaista tietoturva lainsäädäntöä ei ole, yksityisissä yrityksissä ei myöskään välttämättä ole strategiaa tietoturvan osalta eikä näin ollen myöskään strategista johtamista tietoturvallisuuden kontekstissa (Tietoturvallisuudella tuloksia 2007, 13.)

4.3 Kansallisen tason kyberturvallisuuden johtaminen

4.3.1 Johdanto kansallisen tason kyberturvallisuuteen

Teknologian nopea kehitys ja rajat ylittävä verkottunut tiedonkulku ovat lisänneet kyberturvallisuuden merkitystä niin kansallisella kuin kansainväliselläkin tasolla tarkasteltuna. Maailmanlaajuinen turvallisuusympäristö elää voimakkaassa muutoksessa, jossa ei puhuta enää pelkästään fyysisestä toimintaympäristöstä vaan kybertoimintaympäristöstä, jossa yhdistyy fyysinen ja sähköinen turvallisuus. Informaatioteknologian rantautuminen osaksi jokaisen ihmisen elämää niin kotona, työpaikoilla kuin yhteiskunnan eri toiminnoissa on pakottanut kiinnittämään yhteiskunnan turvallisuuteen entistä enemmän huomiota. Lehto (2017, 11-13) tutkimuksen mukaan haittaohjelmat olivat vuoden 2016 voimakkaimmin kasvava trendi, joiden kasvun myötä haittaohjelmista tulee yhä monimutkaisempia ja kehittyneempiä tulevaisuudessa. Haittaohjelmiin kuuluu myös kiristysohjelmat, joiden suosio on kasvussa. Kiristysohjelmat tulevat valtaamaan uusia aloja, kuten pankki- ja rahoitustoiminnan sekä julkishallinnon ja kohdistuvat erityisesti mobiililaitteisiin ja erilaisiin päätelaitteisiin. Pahimmassa tapauksessa haittaohjelman pääsy julkisen organisaation verkkoon voi aiheuttaa mittavia vahinkoja yhteiskunnan toimintoihin. Kyberuhkia vastaantaistelu on kissa hiiri leikkiä, jossa hyökkääjät kehittävät yhä tehokkaampia haittaohjelmia kun

puolustavat osapuolet eivät ehdi reagoida uudenlaisiin uhkiin samaa vauhtia. Trendi on ollut jo vuosia samanlainen; ensin tulee haittaohjelma ja vasta sitten kyky puolustautua sitä vastaan. Tänä päivänä haittaohjelmat ovat kaikkien saatavilla, niin yksityiset henkilöt kuin valtiotkin harjoittavat kybertoimia vieraiden valtioiden järjestelmiin etsien niistä heikkouksia. Tutkimuksessa todettiin, että sisäpiiriläiset ovat organisaatiossa merkittävä kyberuhka ja IBM:n tutkimuksen mukaan jopa 60 % kaikista kyberhyökkäyksistä olivat sisäpiiriläiten aiheuttamia.

Hyökkääjien trendinä on kasvavassa määrin ollut kybertoimintaympäristössä organisaation liiketoiminnan tuhoamiseen tähtäävät hyökkäykset. Näillä tarkoitetaan hyökkäyksiä, jotka kohdistuvat tietojärjestelmiin tarkoituksena aiheuttaa merkittävää haittaa organisaation toiminnalle. Tällaisia ovat esimerkiksi kohdistetut hyökkäykset, joissa hyökkääjä hyödyntää organisaation heikkouksia tarkoituksena varastaa tai tuhota tärkeitä tietoja. Huolestuttavaa on myös havaita, että IBM:n tutkimuksen mukaan kyberhyökkäysten top-5 toimialat olivat kaikki kriittiseen infrastruktuuriin kuuluvia, kuten esimerkiksi pankki- ja rahoitusala, julkishallinto sekä liikenne. (Lehto 2017, 11-17) Huomionarvoista on myös ennusteet siitä, miten kyberuhat tulevat kasvamaan tulevaisuudessa. Elämme digitaalisessa yhteiskunnassa, jossa verkkoon liitettävien laitteiden määrä tulee kasvamaan räjähdysmäisesti tulevaisuudessa. Tämän mahdollistaa esineiden internet (IoT). Tällä hetkellä on jo raportoitu kyberhyökkäyksiä, joissa hyökkääjänä on ollut verkkoon liitetty pesukone, jonka todellinen hyökkääjä on kaapannut välineeksi hyökkäyksen toteuttamiseen. Saman suuntainen kehitystrendi on havaittavissa myös ennusteiden mukaan valtioiden kybersodankäynnin kyvykkyyksien kehittymisessä. (Lehto 2017, 21-23)

Kuten aikaisemmin on todettu, tietoturvallisuudella pyritään suojaamaan tietoa, jotta sen luotettavuus, eheys ja saatavuus voitaisiin varmistaa, mutta kuten aikaisemmin on esitetty, uudenlainen kehitys on luonut linkin sähköisestä toimintaympäristöstä fyysiseen toimintaympäristöön, kybertoimintaympäristöön, jonka johdosta on muodostunut uusia uhkia, jotka vaarantavat pahimmassa tapauksessa yhteiskunnan infrastruktuurin toiminnan. Uudet uhat, kyberuhat vaativat kansalliselta turvallisuudelta yhä tehokkaampaa turvallisuuden johtamista ja prosessien hallintaa. Kyberuhilla tarkoitetaan tässä tutkimuksessa toimia, joiden tarkoitus on vahingoittaa tietoverkkoa, tietojärjestelmää tai laitetta, joka on liitetty osaksi verkkoa. Tämä edellyttää kansallisen tason toimintaympäristön tuntemista sekä kaikkien strategisen tason toimijoiden yhteistyötä kansallisen tilannekuvan saamiseksi.

Strategisen johtamisen keinoilla tulee hallita nopeasti muuttuva toimintaympäristö, tunnistettava kriittiset yhteiskunnan osa-alueet sekä kyettävä nopeasti vastaamaan uudenlaisiin uhkiin, joiden vaikutukset voidaan nähdä suoraan yhteiskunnan toiminnoissa. *Strategisella johtamisella kyberturvallisuuden kontekstissa tulee pyrkiä turvaamaan myös paljon muutakin kuin ainoastaan sähköinen toimintaympäristö.*

Aikaisemmissa luvuissa on käsitelty tietoturvallisuuden ja kyberturvallisuuden eroja sekä selvitetty mitä strateginen johtaminen on

tietoturvallisuuden kontekstissa. Tämän luvun tarkoitus on käsitellä kansallisen tason strategista johtamista kyberturvallisuuden kontekstissa ja selvittää, mitä erityistä kyber tuo strategiseen johtamiseen tavallisen johtamisen lisäksi.

4.3.2 Strateginen johtaminen kyberturvallisuuden kontekstissa

Strategisessa johtamisessa korostuu organisaation johtaminen, johon vaikuttavat monet asiat, kuten onko organisaatio yksityinen vai julkinen, millaisessa toimintaympäristössä toimitaan, mikä on organisaation tehtävä ja millaisiin tavoitteisiin organisaatiossa pyritään. Organisaation strategiassa voidaan tunnistaa neljä ulottuvuutta : logistinen, operatiivinen, sosiaalinen sekä teknologinen. Ulottuvuuksia ei voida laittaa tärkeysjärjestykseen, vaan se mikä milloinkin on tärkeintä, riippuu organisaation sille asettamista tavoitteista ja tulevaisuuden päämääristä. (Lehto 2009, 44-45)

Kyberturvallisuuden strategisella tasolla valtio päättää kansallisista kyberturvallisuustavoitteista sekä käyttää kansallisia resursseja määritettyjen tavoitteiden saavuttamiseksi. Strategisella tasolla määritellään tarvittavat voimavarat ja toimenpiteet, joilla mahdollistetaan strategisen suunnitelman kehittäminen (Lehto 2009, 44-45). Hodge et. al. (1991, 224-230) tutkimus tukee ajatusta siitä, että strategisen johtamisen prosessissa määritellään tavoitteet ja hyödyt, tunnistetaan kentällä olevat toimijat, kartoitetaan organisaation sisäiset ja ulkoiset tekijät, tehdään tarvittavat strategiat sekä käynnistetään strategioiden mukainen toiminta.

Sisäisen turvallisuuden selonteossa (2016, 17-25) lähestytään kyberturvallisuutta kokonaisturvallisuuden näkökulmasta, jossa huomiota kiinnitetään valtioiden ja muiden toimijoiden informaatiovaikuttamisen tunnistamiseen ja kykyyn vastata tähän. Ulkomainen tiedustelutoiminta on muuttunut henkilölähteisiin perustuvasta tiedustelusta tietoverkoissa tapahtuvaan tiedusteluun ja globaalit haasteet korostavat yhteistyön merkitystä niin verkkorikollisuuden kuin muiden tietoverkoissa tapahtuvien turvallisuusuhkien torjunnassa. Erityistä huomiota tulee kiinnittää kriittisen infrastruktuuriin kohdistuviin häiriöihin. Selonteossa painotetaan häiriötilanteisiin varautumisen kehittämistä, joka edellyttää eri toimijoiden roolien selkeyttämistä. Toiminnan ja sen suunnittelun tulee perustua yhteisiin strategioihin sekä valtakunnalliseen ohjaukseen, jossa viranomaisten tulee kyetä ennakoimaan paremmin toimintaympäristön muutoksia.

Kun käsiteltiin tietoturvallisuuden johtamista strategisella tasolla, huomataan, että kaikki toimenpiteet tähtäävät tiedon luotettavuuden, eheyden ja saatavuuden turvaamiseen niihin kohdistuvilta erilaisia haavoittuvuuksia hyödyntäviltä uhilta. Koska kyberturvallisuus on tietoturvallisuuden laajentuma, joka käsittää sähköisen turvallisuuden lisäksi myös henkilökohtaiset kuin fyysisetkin ulottuvuudet, tulee kyberturvallisuuden johtamisessa ottaa huomioon myös muita vaikuttavia tekijöitä. Kyberturvallisuudella turvattavat elementit voivat vaihdella henkilöstä itsestään, yhteisessä käytössä oleviin laitteisiin ja aina koko yhteiskunnan

toimintoihin, käsittäen myös kriittiset suojattavat infrastruktuurit voidaan sanoa, että kyberturvallisuuden turvattavat elementit ovat kaikkea sitä mitä kyberavaruudesta voidaan tavoittaa (Solms & Nierek 2013, 101.)

Valtioneuvosto on määritellyt vuoden 2010 periaatepäätöksessä kriittiset infrastruktuurit. Se on määritelty tarkoittamaan sellaisia rakenteita ja toimintoja, jotka ovat yhteiskunnan toiminnan jatkuvuuden kannalta välttämättömiä. Tällaisia ovat muunmuassa fyysisiä laitoksia, kuten vesilaitos sekä sähköisiä toimintoja, kuten kansalaisia palvelevat järjestelmät esimerkiksi terveydenhuollon järjestelmät. Kriittisiksi luokitellut niin fyysiset kuin sähköisetkin palvelut ovat monimutkainen kokonaisuus eikä yksin valtion toimet riitä turvaamaan niiden häiriötöntä toimintaa vaan tarvitaan saumatonta yhteistyötä niin liike-elämän, siviiliväestön kuin valtionkin osalta. (Turvallinen Suomi 2013, 78-80)

Strategista johtamista kyberturvallisuuden kontekstissa voidaan soveltaa osaltaan myös tietoturvallisuuden johtamiseen, mutta kuten aikaisemmissa luvuissa on tullut esille, kyberturvallisuuden johtamisessa tulee kiinnittää erityistä huomiota koko yhteiskunnan käsittävään toimintaympäristöön. Toimintaympäristö poikkeaa tietoturvallisuuden toimintaympäristöstä merkittävästi. Olennaisin havaittava ero on toimintaympäristön laajuudessa sekä muutosnopeudessa. Koska toimintaympäristön muutokset saattavat koskettaa fyysisen yhteyden kautta jokaista kansalaista yhteiskunnan toimintojen kautta, strategisen johtamisen tulee perustua kokonaisvaltaiseen poikkihallinnolliseen yhteistyöhön, uhkien tunnistamiseen ja niihin vastaamiseen sekä yhteiskunnan toimintojen jatkuvuuden varmistamiseen ja niihin kohdistuvien häiriöiden vaikutuksista toipumiseen mahdollisimman nopeasti. Tätä ajatusta tukee Lehto (2016, 28-29) ilmestynyt raportti.

Mukaillen raporttia, voidaan käänteisesti nähdä ajatus, että poikkihallinnollista saumatonta yhteistyötä tarvitaan, jotta kyberuhkiin voidaan varautua ja niitä voidaan hallita. Toimintaympäristön nopeat muutokset vaikuttavat siihen, että reagoinnin tulee olla lähes viiveetöntä häiriötilanteiden hallinnan kannalta. Ajantasainen tilannekuva nostettiin myös yhdeksi tärkeistä kyberturvallisuuden johtamiseen vaikuttavista teemoista. Kyberturvallisuuden johtamisessa korostuu valtiollisten toimijoiden lisäksi elinkeinoelämä, joka tulee sisällyttää yhteiskunnan strategiseen suunnitteluun yhä tiiviimmin. Raportissa nähtiin, että isompien yritysten turvallisuus voi olla riippuvainen pienten yritysten kyvystä oppia kyberturvallisuudesta ja sen hallinnasta. Tähän tulee kiinnittää huomiota strategisia suunnitelmia tehtäessä koko yhteiskunnan turvallisuuden osalta. Kybertoimintaympäristö tulee nähdä niin kansallisena kuin kansainvälisenäkin rajat ylittävänä toimintakenttänä, jossa kyberturvallisuus alkaa rajojen ulkopuolelta. Yhteistyön merkitys korostuu myös kansainvälisessä tiedonvaihdossa. Kybertoimintaympäristössä vaikuttaa useita erilaisia toimijoita valtion lisäksi, kuten yksityiset ihmiset, yritykset ja järjestöt, joiden kaikkien päämäärä on sama, turvata kyberavaruudessa kiinni olevat sähköiset järjestelmät ja niiden kautta toimiva

fyysinen ulottuvuus. Toimintaympäristön kompleksisuus asettaa haasteita sen johtamiselle.

Tilannetietoisuus on yksi tärkeimmistä kansallisen kyberturvallisuuden johtamiseen vaikuttavista asioista. Jokainen organisaatio tarvitsee toimiakseen ajantasaista tietoa ympäristössä tapahtuvista toimista ja niiden vaikutuksista niin oman organisaation toimintaan kuin kansalliseen kyberturvallisuuteen. Tiedon tulee olla tarkoituksenmukaista, nopeasti saatavaa ja perustua oikeisiin tietoihin ja arvioihin vallitsevasta tilanteesta. Kybertoimintaympäristön nopeat muutokset vaativat nopeaa reagointia ja tehdäkseen oikeita päätöksiä, päättöksentekijällä tulee tietää mihin tehdyt päätökset perustuvat, miten ne vaikuttavat tilanteeseen ja muihin toimijoihin sekä millaisia riskejä mahdollisesti päätöksiin sisältyy. Tästä syystä on erityisen tärkeää, että käytettävissä on ajantasainen tilannetieto vallitsevasta tilanteesta, jotta siihen voidaan reagoida mahdollisimman nopeasti ja sellaisilla toimilla, jotka perustuvat oikeisiin tietoihin. Tilannetietoisuus edellyttää toimijoilta tiivistä yhteistyötä ja osaamista sekä nopeaa reagointia eli strategista ketteryyttä. Kyberturvallisuuden johtamisessa ilmentyy strategisen ketteryyden kaikki kolme tekijää, joita ovat strateginen herkkyys, johdon yhtenäisyys sekä resurssien joustava käyttö. Yhteistoiminta ja osaaminen mahdollistavat toimintaympäristön paremman seurannan, tiedon analysoinnin sekä sen jakamisen muille poikkihallinnollisille toimijoille. (Yhteiskunnan turvallisuusstrategia 2010, 54; Suomen kyberturvallisuusstrategia 2013, 21)

Strategisen johtamisen keinoin luodaan perusta myös tilannekuvan muodostamiselle kyberturvallisuuden kontekstissa. Johdon tulee luoda strategiset linjaukset, olla sitoutunut noudattamaan niitä, jakamaan tarvittavat resurssit organisaation käyttöön sekä huolehtimaan siitä, että strategiat tunnistetaan myös organisaation alemmilla tasoilla ja sisällytetään osaksi koko organisaation toimintaa. Kyberturvallisuuden strategisessa johtamisessa korostuu viestinnän merkitys. Viestinnän tulee olla avointa ja ymmärrettävää sekä sen tulee tapahtua oikea aikaisesti huomioiden toimintaympäristön nopeat muutokset. Viestinnän merkitys ei yksin rajoitu tietyn organisaation sisälle, vaan sen tulee ulottua myös poikkihallinnollisten toimijoiden suuntaan ja takaisin. Tämän merkitys korostuu, koska kyberuhille on luonteenomaista niiden moniulotteisuus eli yhden toiminnan keskeytys vaikuttaa myös muihin toimintoihin, koska yhteiskunnan toiminta perustuu hyvin pitkälti sähköisiin verkkoihin ja tiedon kulkuun. Kybertoimintaympäristö siis kosketttaa kansallisella tasolla jokaista toimijaa, ei ainoastaan yhtä organisaatiota. Juurikin tästä syystä olisi erityisen tärkeää, että toimintaympäristössä tapahtuvista muutoksista tiedotettaisiin niiden tapahtumahetkellä jokaiselle toimijalle. (Yhteiskunnan turvallisuusstrategia 2010, 55-57)

Johtamisen tarkoitus tulisi nähdä pyrkimyksenä ”jalkauttaa” kyberturvallisuusajattelua oraganisaation kaikille tasoille, jotta kyberturvallisuus olisi perusta turvallisuusajattelulle, eikä sitä nähtäisi ainoastaan erillisenä asiana muiden asioiden joukossa. Kansallisella tasolla kyberturvallisuusajattelua tulisi suunnata enenevässä määrin yhteiskunnan

kyberturvallisuuden näkökulmaan toimijan oman organisaation näkökulman asemasta. Ylimmän johdon tasolla taas strategioiden toimeenpanoa tulisi valvoa siten, että niiden vaikutukset näkysivät organisaation toiminnassa mahdollisimman pienellä viiveellä, oikeassa suhteessa toimintaympäristön muutosnopeuteen. Johdon tehtävänä tulisi olla huolehtia siitä, että strategiset linjaukset tavoittavat operatiivisen toiminnan ja päätösten käytäntöön vieminen tapahtuu oikeasti eikä vaan ”pöytälaatikossa” olevana paperina. Tämän mahdollistamiseksi, tulisi kehittää operatiivisten toimintojen johtamismalli, jolloin tiedetään kuka johtaa, mitä tehdään ja missä järjestyksessä tehdään (Lehto 2016, 25-30.)

Uhkakuvien ja toimintaympäristön muutoksessa lähtökohtana on laaja turvallisuusajattelu, jossa tulee ottaa huomioon yhteiskunnan ja sen toimijoiden voimavarojen hyödyntäminen. Yhteiskunnan elintärkeiden toimintojen turvaamisen toimintamallissa toiminnot turvataan yhteistyössä viranomaisten, järjestöjen ja yritysten kanssa. Kansalliset tietojärjestelmät pyritään rakentamaan sellaisiksi, että ne toimivat myös kriisitilanteissa ja kykenevät palautumaan häiriöistä normaalille toimintatasolle. Vakavien riskien tunnistaminen ja niistä toipuminen edellyttävät strategiselta johtamiselta määrätietoista otetta yhteiskunnan toimintojen kehittämiseksi. Strategisten päätösten toimenpanon keskeiset osa-alueet ovat toimintaympäristön muutosten seuranta (tilannekuva), riskienhallinnan ja varautumisen jatkuva kehitys sekä säännölliset toimijoiden väliset harjoitukset, joilla pyritään muodostaan skenaarioita mahdollisista tapahtumista ja keinoja niiden estämiseksi. (Turvallinen Suomi 2013, 23-25)

4.3.3 Kansallisen kyberturvallisuuden strategisen johtamisen prosessi

Strategisella johtamisella kansallisella tasolla tarkoitettiin tulevaisuuteen tähtäävien ennusteiden tekemistä sekä strategisten päätösten tekemistä, joilla ohjataan toimintaa asetettujen päämäärien ja tavoitteiden saavuttamiseksi. Strategisen johtamisen tarkoitus on ohjata valtion ylintä johtoa määrittämään toimintansa tarkoituksen ja keinot, joilla organisaatio menestyy tulevaisuuden toimintaympäristössä. Kybertoimintaympäristön muutokset ovat nopeita ja se edellyttää ylimmältä johdolta nopeaa toimintaa niin strategioiden suunnittelussa kuin toteutuksessa. Strateginen johtaminen nähdään myös prosessina, jossa strategiat suunnitellaan ja toimeenpannaan käytäntöön (Hodge et. al., 1991, 225–229.)

Strategiaprosessilla tarkoitetaan valtion ylimmän johdon työskentelyprosessia, joka tähtää strategioiden tuottamiseen ja toimeenpanoon, tarkoituksena lisätä yhteiskunnan toimijoiden kykyä saavuttaa tavoitteet. Prosessissa huomioidaan myös strategioiden kannalta tärkeiden sidosryhmien tavoitteet (Kyrölä 2010, 16; Ahola 1995, 56). Strategian kehittämiselle on rakennettava prosessit, jotta tiedetään kuinka yhteiskunnan kyberturvallisuutta ja sen toimintaa kehitetään ja mihin suuntaan sen halutaan kehittyvän. Prosessien suunnittelussa tulee huomioida kyberturvallisuuden toimintakenttään vaikuttavat tekijät, ennenkaikkea käytettävissä olevat

resurssit, ympäristössä vaikuttavat toimijat (valtio, yritykset, järjestöt), kokonaisvaltainen tilannekuva sekä kybermaailman muutosnopeus.

Strategia syntyy prosessin tuloksena, mihin osallistuu operatiivisessa toiminnassa mukana olevia henkilöitä. Strategisen johtamisen prosessi luo toimintaympäristön jossa organisaatio toimii ja mahdollistaa suunnitelmien tehokkaan käyttöönoton. Toimintaympäristössä toteutetaan strategista johtamista rakentamalla kyberturvallisuusajattelun ympärille muodostunutta kulttuuria, ymmärrettävässä muodossa olevilla ohjeilla, avoimella läpi koko hallinnon kulkevalla viestinnällä, kehittyneiden taustajärjestelmien käyttöönotolla sekä mahdollistamalla edellytykset ajantasaisen tilannekuvan syntymiselle. Strateginen johtaminen ei ole ainoastaan ylimmän johdon asia vaan siihen tulee osallistua henkilöitä myös operatiiviselta puolelta. Yleisesti on ollut käsitys, että strateginen johtaminen on ainoastaan valtion ylimmän johdon asia, mutta tässä yhteydessä se nähdään myös hieman laajempana, osana operatiivisia alueita. (Kyrölä 2010, 35-36)

Kyberturvallisuuden operatiivisten prosessimallien toiminta liittyy kybertoimintaympäristöön ja siellä tapahtuvaan riskien etsimiseen ja arviointiin. Ympäristön eri osa-alueet muodostavat toiminnan kokonaisprosessin. Alberts et al.(2000) mukaan opertatiivisilla malleilla on tunnistettavia yhteisiä piirteitä ja yleensä ne hyödyttävät tunnettuja käytäntöjä. Yhteneväisiksi voidaan todeta tilannetietoisuuden muodostaminen, valvonta sekä havainnointi ja raportointi. Raportointi koskee havaittua asiaa, sen käsittelyä sekä oppimista tästä prosessista.

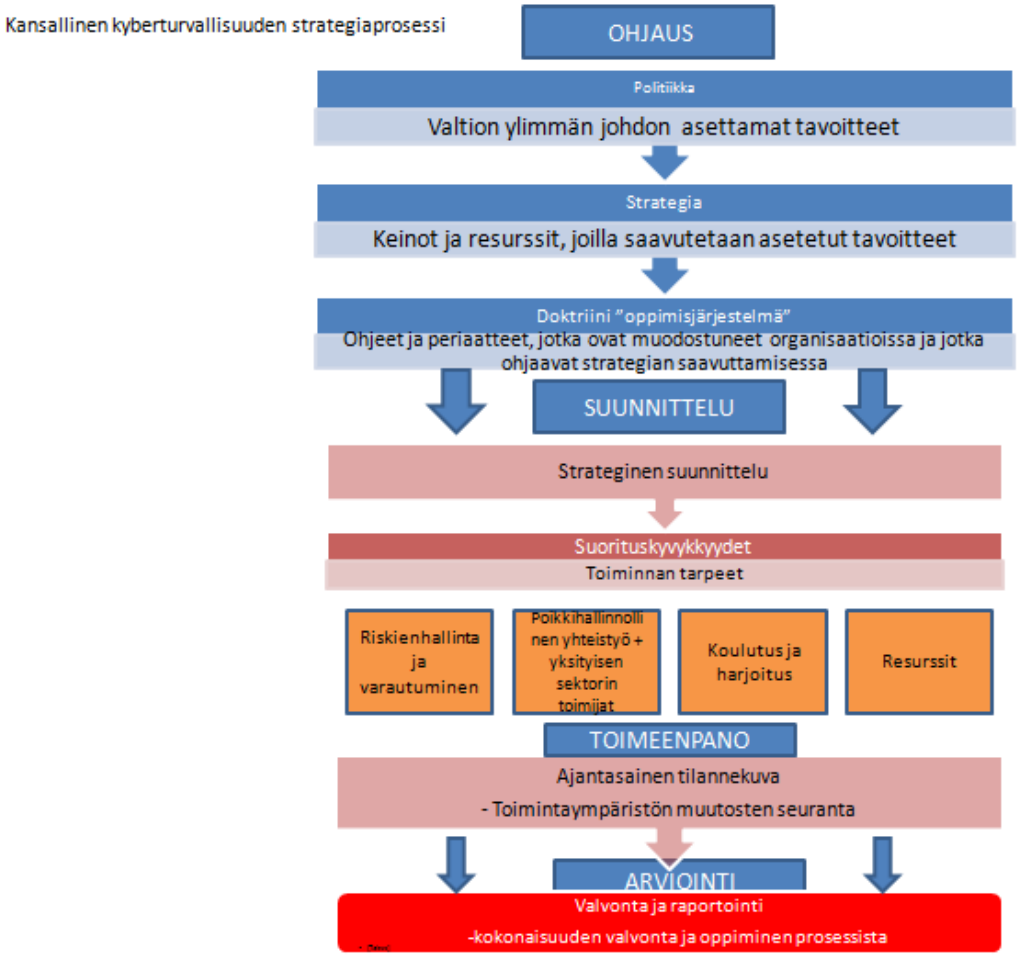
Kyberturvallisuuden kontekstissa kansallisella tasolla tarkassteltuna organisaatioiden strategioita ohjaavat usein poliittiset päätökset, jotka asettavat toiminnalle rajoja. Eduskunta ja valtioneuvosto päättävät eri ministeriöiden rahoituksesta sekä säätävät lakeja ja julkaisevat säädöksiä, jotka ohjaavat strategistisia linjauksia organisaatioissa.

Vuoden 2013 kyberturvallisuusstrategiassa (2013, 6) todetaan, että ”kyberturvallisuus perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöön sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden häiriötilanteita”. Tällä tarkoitetaan, että kyberturvallisuutta johdetaan kansallisella tasolle eri ministeriöiden johdolla, joiden tehtävä on määrittää organisaatioidensa strategiset tehtävät.

Kyberturvallisuuden johtamisen prosessi sisältää useita erilaisia prosesseja, joiden tarkoitus on varmistaa, että kyberturvallisuuden strategiset suunnitelmat sisältävät kaikki toiminnan tarpeet, ylin johto ottaa vastuun strategiasuunnittelusta ja toteutuksesta sekä huolehtii, että organisaatiolla on käytettävissään riittävät resurssit strategioiden eteenpäinviemiseksi sekä varmistaa riittävän koulutuksen ja harjoituksen järjestämisestä henkilöstölle, jotta strategioiden mukainen toiminta on tehokasta ja määrätietoista.

Edellä on selvitetty, että kansallisen kyberturvallisuuden johtamiseen vaikuttavat niin vallitsevat poliittiset päätökset kuin strategiat, jotka määrittävät miten kyberturvallisuus toteutetaan kansallisella tasolla, jotta saavutettaisiin sille asetetut tavoitteet. Strategiset päätökset saavat alkunsa politiikasta, jotka

sitten organisaatioissa muotoutuvat suunnitelmiksi siitä, mihin ollaan menossa ja millä keinoilla on tarkoitus selviytyä tulevaisuuden toimintaympäristössä. Puhuttaessa kansallisen kyberturvallisuuden strategisesta johtamisesta, edellisten lisäksi mukaan voidaan liittää myös termi doktriini, jota on enemmän käytetty sotilasterminologiassa ja jolla tarkoitetaan niitä keinoja, jolla työ pitää tehdä, jotta tavoitteet saavutetaan. Lehto (2009, 46) kuvaa julkaisussaan doktriinia varastoksi analysoitua tietoa ja kokemusta. Doktriini kuvaa sitä miten tietyt toimet on opittu tekemään tietyllä tavalla, jotta niiden hyöty olisi maksimaalinen. Lehto jatkaa, että käytännössä tällä tarkoitetaan tilannetta, jossa organisaation ylin johto laatii strategiat mutta joihin poliittiset, taloudelliset tai sosiaaliset tekijät voivat aiheuttaa uudenlaisia strategisia lähestymistapoja, jotka poikkeavat ylimmän johdon määrittelemistä toimintalinjoista. (Lehto 2009, 46) Kuviossa 5 esitetään kansallinen kyberturvallisuuden johtamisen prosessi mukaillen Lehto (2009, 47). Prosessissa on tunnistettavissa neljä eri kokonaisuutta: ohjaus, suunnittelu, toimeenpano sekä arviointi.



Kuvio 5 Kansallisen kyberturvallisuuden johtamisen prosessi (mukaillen Lehto 2009, 47).

Tässä yhteydessä käsitellään kyberturvallisuutta strategisesta näkökulmasta, jossa mukana on myös yhteys operatiiviseen tasoon. Kyberturvallisuutta ei käsitellä sotatoimena tai kybersodankäyntiä ja siksi usein sotatoimissa mainittu kolmas taso eli taktinen taso puuttuu niin mallista kuin tutkimuksesta. Kuviossa 5 oleva prosessi voidaan jakaa kahteen tasoon: Strategiseen sekä operatiiviseen. Strategiseen tasoon kuuluvat ohjaus sekä suunnittelu. Strategisella tason päätökset saavat alkunsa Valtion ylimmän johdon asettamista tavoitteista. Kansallisella tasolla ministeriöt päättävät strategisista tavoitteistaan Valtioneuvoston päätösten rajoissa sekä organisaation keinoista, joilla tavoitteisiin päästään (Yhteiskunnan turvallisuusstrategia 2010, 4).

Strategian muodostukseen prosessissa vaikuttaa myös doktriini eli organisaatioissa muodostuneet ohjeet ja perusperiaatteet, joiden mukaisesti strategiaa ohjataan. Suunnitteluun kuuluvat strategioiden suunnittelu sekä suorituskyvykkyydet, joilla määritellään kaikki toiminnan tarpeet. Toiminnan tarpeiden määrittelyssä tunnistetaan neljä eri osa-aluetta: Riskienhallinta ja varautuminen, poikkihallinnollinen yhteistyö + yksityisen sektorin toimijat, koulutus ja harjoitus sekä resurssit.

Kansallisen tason kyberturvallisuuden johtamisessa korostuu ennen kaikkea toimintaympäristön kompleksisuus sekä toimintakenttä, johon kuuluu useita toimijoita. Kuusiston (2014, 47–48) mukaan kompleksisessa toimintaympäristössä korostuu jatkuva muutos, jolloin on hankalaa, ellei jopa mahdotonta ennustaa kaikkia tapahtumia. Kompleksisessa ympäristössä voidaan tunnistaa useita järjestelmiä, jotka ovat toisistaan riippuvaisia ja toimenpiteet yhteen järjestelmään eivät mahdollista kokonaisuuden turvaamista. Tällaisessa tilanteessa on erityisen tärkeää juuri kaikkien toimijoiden välinen yhteistoiminta niin julkisen sektorin kuin yksityisenkin sektorin osalta.

Kybertoimintaympäristölle on ominaista, etteivät tietoverkoissa tapahtuvat turvallisuusriskit ja –uhkat tunne valtion rajoja. Tällaisiin haasteisiin vastaaminen edellyttää kansallisen kyvykkyyden lisäksi myös kansainvälistä tiivistä yhteistyötä, koska Suomen turvallisuus on tiiviissä yhteydessä kansainväliseen kehitykseen. Kansainvälinen toiminta kuuluu osaltaan elintärkeisiin toimintoihin (Yhteiskunnan turvallisuusstrategia 2010, 9). Tässä tutkimuksessa käsitellään kansallista kyberturvallisuuden johtamista, eikä oteta kantaa laajemmin Kansainväliseen yhteistyöhön ja siihen vaikuttaviin seikkoihin. Yhteistyössä tulee kuitenkin kiinnittää huomiota myös viestintään.

Viestintä on yksi johtamisen osa-alue ja sen merkitys korostuu entisestään kriisi- ja häiriötilanteissa. Viestinnän tulee olla selkeää ja ymmärrettävässä muodossa kerrottua, jotta se tavoittaa kaikki organisaation ja yhteistyöelinten henkilöt siinä muodossa kuin se alun perin on ollut. Viestinnän tulee olla myös kaikkien viranomaisten kohdalla samanlaista ja perustua yhteisesti sovittuihin toimintasääntöihin (Yhteiskunnan turvallisuusstrategia 2010, 56–57).

Henkilöstön koulutusta ja harjoitustoimintaa tarvitaan, jotta strategian mukainen toiminta on tehokasta ja määrätietoista. Koulutus mahdollistaa ajantasaisen tiedon ympäristössä vaikuttavista tekijöistä sekä harjoitus edesauttaa reagoimaan ympäristössä vaikuttaviin poikkeustilanteisiin riittävällä voimalla.

Molemmat yhdessä auttavat myös luomaan organisaatiossa kyberturvallisuuteen perustuvaa ajattelua, jolloin kaikilla organisaation tasoilla kyberturvallisuusajattelu on lähtökohtaista kaikkeen turvallisuusajatteluun. Tämän tyyppisten asioiden huomioiminen strategisella tasolla on erityisen tärkeää, jotta kokonaisuus olisi mahdollisimman tehokas ja toimiva.

Ilman riittäviä resursseja, toiminnalla ei ole edellytyksiä. Kansallisella tasolla Valtion ylin johto päättää alemmille tasoille jaettavista resursseista, joiden mukaan organisaatioiden tulee suunnitella toimintaansa ja määritellä alueet, joihin resursseja kulloinkin tulee kohdistaa. Resursseja ovat rahallisten resurssien lisäksi organisaation henkilöstö, organisaatiossa käytössä oleva teknologia sekä järjestelmät.

Kansallisella tasolla riskien hallinta ja varautuminen on sekä strategisen tason, että operatiivisen tason toimintaa. Strategisella tasolla suunnitellaan riskienhallinnan strategisen linjat, kun taas operatiivisella eli suorittavalla tasolla toteutetaan strategisen tason linjauksia. Riski voidaan ymmärtää jossakin toiminnassa olevaksi onnettomuuden todennäköisyydeksi, jolloin riskienhallinnalla pyritään minimoimaan tämä todennäköisyys negatiiviselle tapahtumalle sekä pienentämään, rajoittamaan tai estämään negatiivisesta toiminnasta aiheutuvia seurauksia. Toiminta tai kohde, jota pyritään turvaamaan toimintaympäristössä, on jollain tavalla arvokas yhteiskunnalle tai organisaatiolle. Esimerkiksi yhteiskunnan näkökulmasta sähkönjakelu on arvokasta omaisuutta, jota pyritään suojaamaan niihin kohdistuvalta negatiiviselta toiminnalta. Solmsin & Nierikin (2013) mukaan kyberriski voidaan määritellä riskiksi, joka uhkaa tietoverkkojen kautta suojattavaa kohdetta, joka toimii fyysisessä toimintaympäristössä. Riskienhallinnalla siis pyritään tunnistamaan ja analysoimaan sekä hallitsemaan kybertoimintaympäristössä ilmeneviä muutoksia. Kansallisen tason varautumisessa ministeriöt sekä muut elintärkeiden toimintojen turvaamiseen osallistuvien viranomaisten tulee varmistaa toimintojensa jatkuvuus kaikissa olosuhteissa hallinnollisilla, rakenteellisilla tai teknisillä toimenpiteillä (Yhteiskunnan turvallisuusstrategia 2010, 17). Varautumisen tarkoitus on myös kehittää organisaatioiden tietoverkkoja ja -järjestelmiä siten, etteivät yhteiskunnan elintärkeät toiminnot pysähdy häiriöiden vuoksi vaan kykenevät toipumaan ja palautumaan normaaliin tilaan mahdollisimman nopeasti ja jatkamaan toimintaansa häiriöstä huolimatta.

Operatiivinen taso pitää sisällään toimeenpanon, joka liittyy vahvasti toimintaympäristön muutosten seurantaan ja siitä johdettavaan ajantasaiseen tilannekuvaan kyberympäristöstä. Kansallisella tasolla tarkasteltuna tätä varten on yleensä isojen organisaatioiden tapauksessa perustettu kyberturvallisuuden tilannetta aktiivisesti seuraava yksikkö, joka kykenee myös reagoimaan ympäristössä ilmenneisiin poikkeamiin. Yksi tällainen yksikkö on Valtion tieto- ja viestintätekniikkakeskus Valtorissa. Keskuksen tehtävä on huolehtia valtion eri organisaatioiden verkkojen valvonnasta sekä poikkeuksien havainnoinnista ja analysoinnista (Jaakkola 2016, 24: Valtori 2016). Tämän lisäksi on arviointi, joka pitää sisällään niin strategioiden toimeenpanon kuin operatiivisen toiminnan valvonnan.

Kansallinen kyberturvallisuuden johtamisen strategia on prosessi, jossa valtion kyberturvallisuuden tavoitteet realisoituvat muiden tavoitteiden joukosta. Prosessin tavoite on ennen kaikkea tuottaa ne työkalut organisaatioille, joilla tavoitteisiin on mahdollista päästä. Työkalut määritellään kansallisten Valtion johdon päätöksiin perustuvien mekanismien avulla (Lehto 2009, 54). Jotta kansallisen kyberturvallisuuden johtamista voitaisiin edelleen kehittää, on Valtion tehtävä yhä tiiviimpää yhteistyötä niin omien organisaatioidensa kuin yksityisenkin sektorin kanssa. Tämän lisäksi koulutus- ja tutkimustoiminta on erityisen tärkeässä asemassa globaalin toimintaympäristön kehittyessä sekä yhteiskunnan toimintojen ja palvelujen siirtyessä yhä enemmän osaksi tietoverkkoja. Kehittymien kaipaa myös vuoropuhelua julkisissa medioissa, ideoita ja ehdotuksia uusista toimintatavoista sekä erityisesti kansallisella sektorilla työskentelevien henkilöiden aktiivista otetta organisaation toimintatapojen arvioinnissa ja yhteiskunnan turvallisuusajattelun kehittämisessä.

Kyberturvallisuuden strategisen johtamisen prosessi kuvataan jatkuvaksi toiminnaksi, joka kehittyy jokaisen osion kehittyessä. Puhutaan siis muutoksesta, joka tapahtuu prosessin aikana. Strategisella johtamisella tavoitellaan prosessissa muutosta. Seppänen (2015) määrittelee muutoksen tilasta toiseen siirtymisenä, jossa aikaisempi tila loppuu ja uusi tila alkaa. Muutos voi olla näkökulmasta ja katsojasta riippuen hyvinkin erilainen. Toiselle se voi olla askel oikeaan suuntaan, kun toiselle se on askel väärään suuntaan. Joku voi kokea muutoksen pienenä ja helppona kun jollekin toiselle se taas on ylivoimainen ja pelottava. Muutos on kuitenkin prosessi, jonka avulla pyritään muuttamaan tai uudistamaan valtion organisaatiota tai organisaation johtamismalleja. Nykyelämässä muutos on hyvin tuttua myös valtionhallinnon eri toimijoiden organisaatiossa, muutos on jatkuva prosessi. Se ei ole ajatuksena uusi sillä kreikkalainen filosofi Herakleitos uskoi, että maailma on jatkuvassa muutoksen tilassa. Muutokselle on tyypillistä sen kompleksisuus, jota on mahdotonta aina hallita. Kansallisen tason strategisella johtamisella tähdätään yhteiskuntaa koskevien tavoitteiden saavuttamiseen ja samalla pyrkien hallitsemaan sen aikana ilmenneitä muutoksia mutta epävarmuustekijöiden takia se on usein mahdotonta. Kyberturvallisuuden toimintaympäristössä on mahdonta ennustaa kaikkia muutoksia, jotka ovat usein odottamattomia ja nopeita. (Lehto 2009, 54) Tästä syystä onkin erityisen tärkeää panostaa prosessimallissa oleviin alueisiin, jolloin voidaan saavuttaa parhaan kyvyn vastata toimintaympäristössä tapahtuviin muutoksiin.

"Et voi astua kahdesti samaan virtaan." ~ Herakleitos (n. 500 eKr.).

5 KYBERTURVALLISUUDEN JOHTAMINEN SUOMESSA

Kansallisen kyberturvallisuuden johtaminen on avainasemassa kun tuotetaan turvallisia sähköisiä palveluita yhteiskunnalle ja sen kansalaisille. Kasvava trendi on osoittanut suunnan digitaalisten palveluiden kuin myös laitteiden siirtymisen osaksi tietoverkkoa. Tämä lisää tietoverkoissa tapahtuvien kyberuhkien riskiä, joilloin riskienhallinnan ja varautumisen tärkeys kasvavat. Globaali toimintaympäristö koskettaa monia toimijoita, niin yksityisiä, yrityksiä kuin valtionhallinnon organisaatioita. Erityisessä asemassa ovat yhteiskunta toiminnot sekä tärkeät suojattavat infrastruktuurit. Kybertoimintaympäristö on luonut yhteiden digitaalisesta fyysiseen maailmaan, jossa kansallisilla organisaatioilla on suuri merkitys nopeasti muuttuvan toimintaympäristön turvaamisessa. Tässä luvussa käsitellään Suomen kansallista kyberturvallisuutta sekä sen johtamista. Aluksi tutustutaan Suomen kyberturvallisuusstrategiaan vuodelta 2013, strategian visioon, toiminta- ja johtamismalliin sekä strategisiin linjauksiin. Tämän jälkeen käsitellään Suomen kansallisen kyberturvallisuuden nykytilaa kyberturvallisuuden strategisen johtamisen osalta.

5.1 Suomen kansallinen kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategia alkaa sanoilla : ”Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä, ja yhteiskuntamme elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa...”. Ensimmäinen lause kiteyttää pitkälti sen, miksi kyberturvallisuusstrategia laadittiin. Yhteiskunnan turvallisuuden kehittäminen on noussut yhdeksi keskeisimmäksi asiaksi Valtion tavoitteista. Tietoyhteiskunnan voimakas kasvu ja yhteiskunnan palveluiden ja toimintojen siirtyminen sähköisiin tietoverkkoihin on kasvattanut kybertoimintaympäristössä vaikuttavia uhkia. Globaali, maan rajat ylittävä

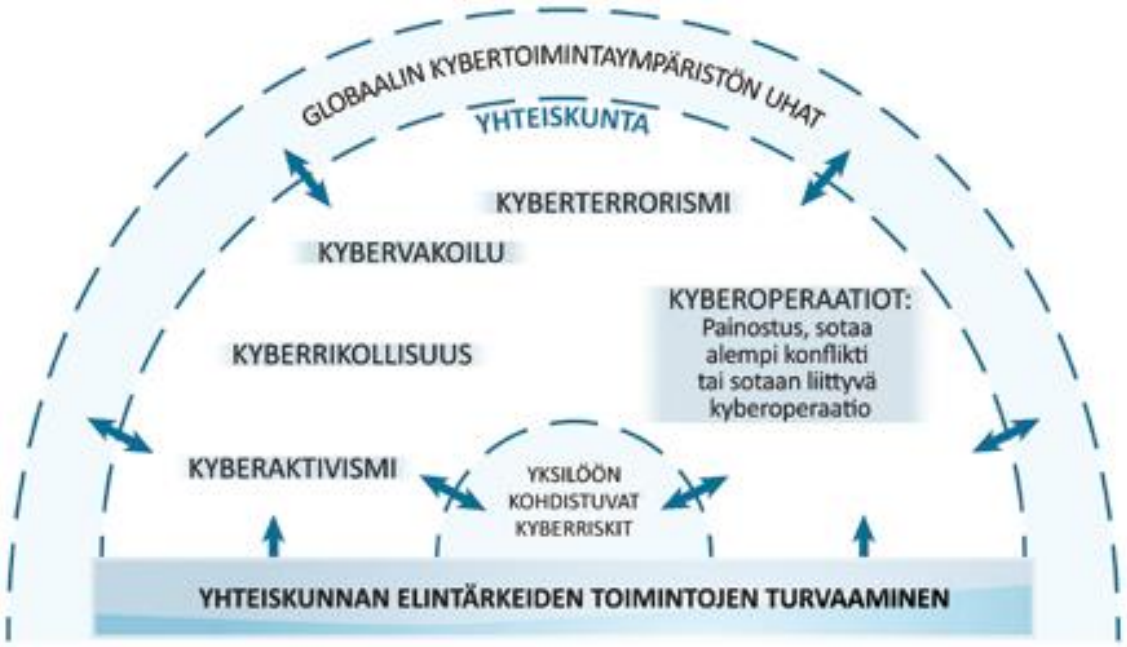
toimintaympäristö on kasvattanut valtioiden tarvetta suojautua paremmin erilaisia haavoittuvuuksia hyödyntäviä uhkia vastaan, jotka voivat kohdistua yhteiskunnan toiminnan kannalta kriittisiin kohteisiin. Strategia määrittelee keskeiset tavoitteet ja toimintalinjat, joiden avulla pyritään vastaamaan kybertoimintaympärisössä vaikuttaviin normaalista toiminnasta poikkeaviin haasteisiin. (Suomen Kyberturvallisuusstrategia 2013, 1). Strategian mukaan kriittisiä turvattavia kohteita ovat : ”Valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys” (Suomen Kyberturvallisuusstrategia 2013, 2).

Ståhle (2013, 9) mukaan strategian valmistelu ei ollut vaivatonta. Tämä johtui siitä, että strategiassa käytetyt määritelmät poikkesivat hyvinkin paljon toisistaan eri aloilla ja organisaatioissa. Tämä on vaatinut strategian suunnitteluun osallistuneelta työryhmältä sopimista yhteisesti käytettävistä termeistä ja niiden tarkoituksesta. Esimerkiksi puolustusvoivat ajatteli strategian tarkoittavan kybersodankäyntiä kun taas valtionvarainministeriö liitti kyberstrategian yhteiskunnallisiin sähköisiin palveluihin ja mielsi sen tarkoittavan suojattavia tärkeitä kohteita. Työryhmä kuitenkin sai työnsä valmiiksi ja sen pohjalta syntyi kansallinen kyberturvallisuusstrategia.

Strategia syntymiseen vaikutti merkittävästi yhteiskunnan kokonaisturvallisuus. Yhteiskunnan turvallisuusstrategia määrittelee kyberuhkan yhdeksi suurimmista yhteiskunnan kokonaisturvallisuuden uhkista (Turvallinen Suomi 2013, 109). Valtiovallan keskeisimpiä tehtäviä ovat huolehtia yhteiskunnan turvallisuudesta sekä kriittisistä suojattavista kohteista. Turvallisuus ja puolustusasiain komitean (2012, 2-3) lausunnossa todetaan, että vuodenvaihteessa 2011-2012 esiintyneet talvimyrskyt aiheuttivat laajoja tuhoja voimahuollolle katkoen laajassa mittakaavassa sähkölinjoja, jonka johdosta aiheutui mittavia vahinkoja ja ongelmia erilaisille järjestelmille. Lausunnon mukaan häiriöt olivat luonteeltaan sellaisia, että vastaavanlaisia ongelmia sähköverkossa voi aiheuttaa kyberhyökkäys sähkönjakelun järjestelmiin. Tästä syystä on muodostettu Suomen ensimmäinen kyberturvallisuusstrategia, jolla voidaan vastata konkreettisesti kyberuhkiin.

> *”Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen. ”*
> *– Suomen kyberturvallisuusstrategia 2013*

Tietoyhteiskunnan kehitys on tuonut kybertoimintaympäristön kaikkien ulottuville, niin yksittäisten ihmisten kuin pienien tai suurien valtioiden. Perinteiset asetelmat eivät enää päde, pieni valtio voi olla kybermaailmassa yhtä tehokas kuin suurikin valtio, jopa tehokkaampi. Suomi on osa tätä ympäristöä ja näin ollen myös osa mahdollisia kybertoimia, jotka kohdistuvat tietoverkojen kautta yhteiskunnan toimintoja ylläpitäviin järjestelmiin, etsien niistä haavoittuvuuksia. Strategiassa määritellään kyberuhkamalli, jonka tarkoitus on kuvata erilaisten uhkien vaikutusmekanismia, kohdetta, mistä lähteestä uhka on peräisin sekä miten se mahdollisesti vaikuttaa kohteeseen (Suomen kyberturvallisuusstrategia 2013, 18). Kuviossa 6 on esitetty Suomen kyberuhkamalli.



Kuvio 6 Suomen kyberuhkamalli (Suomen kyberturvallisuusstrategia 2013, 19).

Yhteiskunnan elintärkeisiin toimintoihin kohdistuvat kyberuhkat voivat esiintyä itsenäisinä kuten esimerkiksi palvelunestohyökkäys rahoituspalveluita tarjoavan pankin järjestelmiin, samanaikaisina, jolloin voidaan puhua esimerkiksi tapahtumasta, jossa samanaikaisesti aiheutuu kaksi vakavaa häiriötilannetta sähkönjakelun kantaverkossa tai toistensa jatkumoina, jolloin tilanne voisi olla vaikka sellainen, että hyökkääjä on aluksi selvittänyt tarkasti mitä arvokasta organisaatiossa on, millaista henkilöstöä ja millaisia järjestelmiä. Hyökkääjä etsii verkosta haavoittuvuuksia ja lopultaa löytää kohdan josta saa haittaohjelman sisälle. Organisaation verkko on murrettu. Haittaohjelma taas sammuttaa toimintoja, vaikka sähköä ohjaavia keskuksia. Tämä aiheuttaa ongelmia sähkönjakelussa ja se puolestaan vaikuttaa sen alueen sähkönsaantiin jonka järjestelmään on hyökätty. Tästä taas saattaa aiheutua mittavia ongelmia asukkaille, yrityksille tai julkisille palveluille. Uhkia voi olla myös toisenlaisia. Hyvin tyypillistä on, että kineettisiä, aseilla käytäviä sotatoimia edeltää kyberympäristössä tehty hyökkäys, jolla pyritään häiritsemään aseellisia järjestelmiä. (mukaillen Suomen kyberturvallisuusstrategia 2013, 19)

Koska kansallinen kyberturvallisuusstrategia nojaa vahvasti yhteiskunnan turvallisuusstrategiaan, on syytä hieman tarkastella asiaa. Yhteiskunnan turvallisuusstrategiassa (2017) esitetään suomalaisen yhteiskunnan varautumisen periaatteet. Varautuminen toteutetaan kokonaisturvallisuuden toimintaperiaatteella. Strategia on päivitys vuosina 2003, 2006 ja 2010 laadittuihin valtioneuvoston periaatepäätöksiin. Uudessa starategiassa ollaan yhä enemmän kiinnitetty huomiota poikkihallinnolliseen yhteistyöhön sekä

yhteiskunnan kaikkiin toimijoihin. Strategia muodostaa varautumisen sekä kriisijohtamisen yhteisen perustan yhteiskunnan kaikille toimijoille. (Yhteiskunnan turvallisuusstrategia 2017, 7) Uudessa strategiassa kiinnitetään enemmän huomiota erilaisiin toimintamalleihin, aikaisempien strategisten tavoitteiden sijasta. Toiseksi, aikaisemmat strategiat ovat pitkälti perustuneet valtionneuvosto lähtöiseen ajatteluun, mutta uusi päivitty versio painottaa yhteiskunnan näkökulmaa. Päivitetyssä versiossa myös kiinnittämään yhä enemmän painoarvoa elintärkeiden toimintojen turvaamiseen kyberympäristössä (Turvallisuuskomitea 2016.)

5.1.1 Strategian visio

Suomen kyberturvallisuus strategiassa (2013, 3) kuvataan kolmen kohdan visio, jonka pohjalta Suomen tavoite on ollut nousta yhdeksi kyberturvallisuuden kärkimaaksi. Johtamisen näkökulmasta tulee löytää oikeat strategiat ja menetelmät, joilla vision kohdat voidaan saavuttaa. Vision kohdat ovat:

- ”Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan”.
- ”Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseksi syntyvää osaamista sekä kansallisesti että kansainvälisesti.”
- ”Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.”

Vision kolmen kohdan voidaan ajatella kuvaavan niitä toimintoja, joita Suomen on kyettävä tekemään kyberturvallisuuden ollessa uhattuna : ”Suojaamaan elintärkeät toimintonsa kaikissa tilanteissa”. Kuten aiemmin on todettu, elintärkeiksi toiminnoiksi voidaan lukea kaikki yhteiskunnan toiminnan kannalta oleelliset toiminnot ja palvelut. Yksi tällainen on esimerkiksi valtion johtaminen. Valtion johtamisella tarkoitetaan yhteistyötä tasavallan presidentin, valtioneuvoston sekä eduskunnan osalta. Kun puhutaan strategian edellyttämästä tavoitetilasta, valtion johtamisen osalta sillä tarkoitetaan näiden kolmen sekä ministeriöiden yhteistoimintaa niin, että kansallisia resursseja käytetään kulloisenkin turvallisuustilanteen edellyttämässä laajuudessa. Kansallisen johtamisen tarkoitus on luoda riittävät toimintaedellytykset strategisten päätösten tekemiseksi. (Yhteiskunnan turvallisuusstrategia 2010)

Kansainvälinen toimintakyky on Suomelle tärkeä ja sen merkitys korostuu entisestään globaalissa kybertoimintaympäristössä. Yhteiskunnan turvallisuusstrategiassa (2006, 14) kansainvälinen toimintakyky määritellään kykynä ylläpitää yhteyksiä toisiin valtioihin sekä varmistaa Euroopan unionissa Suomen kannanottojen välittyminen eri toimielimissä sekä muissa kansainvälisten yhteenliittymien yhteistyöelimissä.

5.1.2 Kyberturvallisuusstrategian toiminta- ja johtamismalli

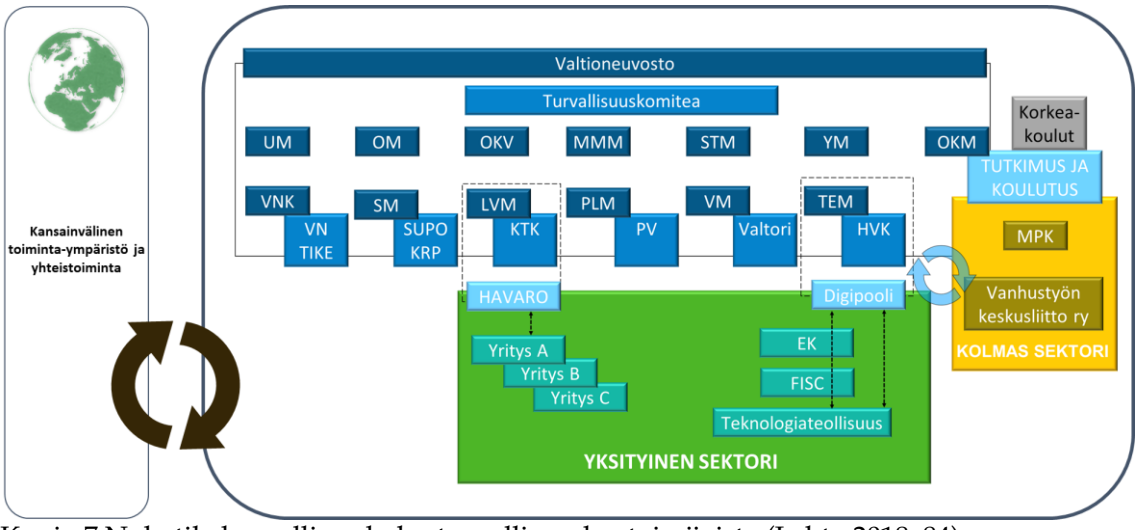
Kyberturvallisuusstrategiassa on määritelty kybervarautumisen periaatteellinen toimintamalli. Kyberturvallisuuden ylimmän tason muodostaa valtioneuvosto, joka määrittelee poliittisen ja strategisen tason linjaukset sekä voimavarat ja toimintaedellytykset. Ministeriöt vastaavat puolestaan oman hallinnonalansa kyberturvallisuuden kehittämisestä, varautumisesta sekä häiriötilanteiden hallinnasta. Kyberturvallisuuden johtaminen ja häiriötilanteiden hallinta vaativat toimiakseen tehokkaasti ajantasaista ja luotettavaa tilannekuvaa kybertoimintaympäristöstä. Strategian toimintamallin edellytys on, että valtioneuvostolla on kätettävissään strategisia päätöksiä ja linjauksia tehdessään luotettava ja ajantasainen, kaikkien toimijoiden (valtio, yritykset, järjestöt) yhteinen sekä ymmärrettävässä muodossa oleva tilannetieto kybertoimintaympäristöstä. (Lehto ym. 2017, 28; Suomen kyberturvallisuusstrategia 2013, 4)

Suomen kyberturvallisuusstrategian toimintamalli on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja noudattaa Yhteiskunnan turvallisuusstrategiassa vuodelta 2010 määriteltyjä periaatteita ja toimintatapoja (Suomen kyberturvallisuusstrategia 2013, 5). Kyberturvallisuusstrategian katsotaan olevan jatkumoa Yhteiskunnan turvallisuusstrategialle, jossa käsiteltiin uhkia lähinnä häiriöiden osalta kun kyberturvallisuusstrategia lähestyy tavoitteita kyberuhkien näkökulmasta. Vastuunjako perustuu eri viranomaisten toimintaan. Kuten edellä esitettiin, valtioneuvosto johtaa kyberturvallisuutta poliittisella tasolla strategisten linjausten sekä käytettävissä olevien resurssien ja toimintaedellytysten kautta. Kokonaismaanpuolustuksesta vastaa puolustusministeriö, joka toimii elintärkeiden toimintojen osalta eräänlaisena yhteensovittavana toimielimenä valtion, kuntien, yritysten sekä vapaaehtoisen toiminnan osalta. Turvallisuuskomitea toimii puolustusministeriön alaisuudessa ja sen tarkoitus on yhteensovittaa toimintoja sekä seurata kyberturvallisuusstrategian kehittämistä ja toimeenpanoa. Ministeriöt vastaavat oman hallinnonalansa koskevista kyberturvallisuuden päätöksistä. Kunkin ministeriön kansliapäällikön tehtävänä on johtaa ja valvoa ministeriön toimintaa sekä vastata sen valmiudesta ja turvallisuudesta. Valmiuspäällikkö avustaa näiden asioiden operatiivisen toiminnan toteutuksessa. Koska julkishallinto ja kyberturvallisuuden turvaaminen perustuu pitkälti tietojärjestelmien ja tietoverkkojen toimivuuden varmistamiseen ja turvaamiseen on Valtionvarainministeriölle annettu tehtäväksi vastata niiden ohjauksesta ja kehittämisestä. Erityistehtäviä on määritelty valtiovarainministeriölle, jonka tehtäviin kuuluu vastata tietoturvan sekä ICT-varautumisen ohjauksesta ja johtamisesta. Lisäksi liikenne- ja viestintäministeriölle, jonka vastuualueeseen kuuluu sähköiset tieto- ja viestintäjärjestelmät. Kuten aikaisemissa luvuissa on korostettu, yhteiskunnan elintärkeiden toimintojen turvaamisessa ja ajatasaisen ja luotettavan tilannekuvan saamisen edellytyksenä on eri hallinnonalojen poikkihallinnollisesta toiminnasta sekä valtion, kuntien ja yksityisten

toimijoiden välisestä yhteistyöstä, joka korostaa kokonaisturvallisuuden luomista. (Yhteiskunnan turvallisuusstrategia 2010, 6-7; Leppänen, Linderborg, Saarimäki 2016, 8.)

Viestintävirastoon perustettu kyberturvallisuuskeskus vahvistaa kansallisen tason viranomaistyötä. Keskus kerää tietoa kyberturvatilanteesta, jakaa yhdistettyä ja analysoitua kyberturvallisuuden tilannekuvaa sekä tukee toimijoita laajoissa kyberhäiriötilanteissa ja niiden hallinnassa. Yhdistetyllä tilannekuvalla tarkoitetaan tässä yhteydessä myös muilta toimijoilta kerättyä tilannekuvaa. Kyberturvallisuuden tilannekuvaa pyritään hyödyntämään yhteiskunnan kokonaisturvallisuuden sekä elintärkeiden toimintojen tilannekuvan arvioinnissa. Tilannekuvaa kehitetään kyberturvallisuuskeskuksen lisäksi valtioneuvoston kanslian tilannekuvatoiminnan sekä valtion ympärivuorokautisen tietoturvatoiminnan (SecICT) kanssa. Kyberturvallisuuskeskuksen yksi tärkeimmistä tehtävistä on hyödyntää tietoa julkisen hallinnon sekä yksityisen sektorin toimijoilta sekä osallistua kansainväliseen tiedonvaihtoon yhteiskunnan turvallisuuden hyväksi. (Turvallisuuskomitea 2004, 11–12) Valtiohallinnon tietoturvallisuuden johtoryhmän (VAHTI) tarkoitus on tukea valtioneuvostoa sekä valtiovarainministeriötä tietoturvallisuuteen liittyvässä päätöksenteossa.

Kuviossa 7 on havainnollistettu Kansallisen kyberturvallisuuden toimijat.



Kuvio 7 Nykytila kansallisen kyberturvallisuuden toimijoista (Lehto 2018, 84).

5.1.3 Suomen kyberturvallisuusstrategian strategiset linjaukset

Tässä luvussa käydään läpi Suomen kyberturvallisuusstrategiassa (2013, 7-10) määritetyt strategiset linjaukset niiden linjausten osalta, jotka liittyvät tutkimuksen kohdealueeseen johtamiseen. Muiden linjausten käsittely tässä yhteydessä on tarpeetonta. Yleisesti strategisten linjausten tarkoitus on luoda edellytykset, joilla visiot voidaan toteuttaa. Strategiset linjaukset ovat osa johtamista. Linjausten tarkoitus on kertoa, mitä meidän tulee tehdä, jotta tavoitetila voidaan saavuttaa? Johtamisen keinoin tulee löytää oikeat toimintatavat ja –periaatteet, joilla strategiset tavoitteet voidaan saavuttaa.

Linjauksia selittävässä tekstissä on mukailtu strategian tekstiä. Valtioneuvoston periaatepäätökseen kirjatut strategiset linjaukset ovat:

1. ”Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli. ”

   Yhteistoimintamallin tarkoitus on lisätä toimijoiden yhteistyötä, jonka tavoitteena on tehokkaampi uhkien torjunta sekä jaettu tilannetietoisuus toimintaympäristöstä. Osallistumista häiriötilanteiden harjoitustoimintaan kehitetään niin kansallisesti kuin kansainvälisesti. Harjoitustoiminnasta saatuja tuloksia hyödynnetään tehokkaammin tehostamalla tiedonvaihtoa toimijoiden välillä. Tehostamalla harjoitustoimintaa pyritään lisäämään kykyä havaita haavoittuvuuksia, kehittää suorituskykyään ja kouluttaa henkilöstöään.

2. ”Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä. ”

   Tilannetietoisuutta voidaan parantaa tarjoamalla ajantasaista, luotettavaa, koottua ja analysoitua tietoa toimintaympäristön haavoittuvuuksista ja häiriöistä. Tilannekuvan tulee sisältää arviot ja ennusteet toimintaympäristön uhkista. Uhkien ennakointi edellyttää arvioita eri näkökulmista, kuten poliittisen, sosiaalisen, sotilaallisen, kulttuurisen, teknisen ja teknologisen sekä taloudellisen tilanteen ariointia. Yhsitetyn tilannekuvan luomiseksi perustetaan kyberturvallisuuskeskus viestintäviraston yhteyteen. Kyberturvallisuuskeskus kerää tietoa kybertoimintaympäristöstä ja välittää sitä yhteistyökumppaneille, jonka jälkeen toimijat analysoivat tiedot oman toimintansa osana ja välittävät nämä analyysit takaisin kyberturvallisuuskeskukselle, joka kokoaa yhdistetyn tilannekuvan. Valtioneuvoston tilannekeskuksella tulee olla ajantasainen tilannekuva kybertoimintaympäristöstä. Tilannekuva koostuu kyberturvallisuuskeskuksen yhdistetystä tilannekuvasta sekä hallinnonalojen arvioista.

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.”

   Yhteiskunnan elintärkeiden toimintojen kannalta keskeiset toimijat (yritykset ja organisaatiot) ottavat turvallisuussuunnittelussaan huomioon kyberuhat, jotka liittyvät yhteiskunnan elintärkeisiin toimintoihin sekä ylläpitävät tarkoituksenmukaista suojautumiskykyä. Kohdan tavoitteena on, että mahdolliset uhkat tunnistetaan ja havaitaan, niihin reagoidaan tavalla joka minimoi uhkien haitalliset vaikutukset.

Keskeiset toimijat kehittävät sietokykyään ja toimintamenetelmiään niin, että ne kykynevät toimimaan kyberhyökkäyksen alaisena.

4. ”Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle. ”

   Kyberturvallisuuden kehittäminen edellyttää selkeää määrittelyä toimijoiden vastuista sekä tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää hallinnonaloilta haavoittuvuuksien ja riskien tunnistamista sekä miten riskejä pystytään hallitsemaan. Tulosten perusteella laaditaan toimeenpano-ohjelmat niin julkisen sektorin hallinnonaloille kuin elinkeinoelämälle yhteistyössä huoltovarmuusorganisaation kanssa.

5. ”Strategian toimeenpanoa valvotaan ja toteumaa seurataan. ”

   Vastuu toimialalleen kuuluvasta strategian toimeenpanosta, kyberturvallisuuteen kuuluvien tehtävien ja huoltovarmuusjärjestelyiden kehittämisestä ja toteutumisesta on jokaisella ministeriöllä ja virastolla. Perustettavan turvallisuuskomitean tehtävänä on seurata ja tarvittaessa yhteensovittaa strategian toimeenpanoa. Yhteensovittaminen ei anna komitealle päätösvaltaa, vaan toimivaltainen viranomainen päättää asiasta sen mukaan mitä siitä on säädetty. VAHTI käsittelee ja yhteensovittaa keskeiset linjaukset, jotka liittyvöt hallinnon tieto- ja kyberturvallisuuteen. Hallinnon organisaatiot sisällyttävät kyberturvallisuuden edellyttämät resurssit omiin toiminta- ja taloussuunnitelmiinsa.

5.2 Suomen kansallisen kyberturvallisuuden nykytila

Edellisessä alaluvussa 5.1 käytiin läpi Suomen kansallista kyberturvallisuusstrategiaa niiden kohtien osalta, jotka ovat relevantteja tutkimuksen osalta. Aluksi luotiin yleinen katsaus strategiaan ja sen syntymiseen vaikuttaneista asioista, jonka jälkeen käsiteltiin strategian toimintamallia sekä johtamismallia kansallisella tasolla. Johtamismalli osoittaa selvästi havaittavan ylhäältä alaspäin hierarkisen toimintamallin. Kyberturvallisuuden kansallinen toimintaympäristö on kompleksinen ja kentällä on paljon erilaisia toimijoita, niin hallinnollisia kuin yksityisiäkin. Valtion ylin johto päättää kyberturvallisuutta koskevista strategisista linjauksista ja jaettavista resursseista. Ministeriöt saavat strategiset linjaukset valtioneuvostolta sekä tarvittavat resurssit, joiden tulisi kattaa toimintamenot. Ministeriöt auunnittelevat hallinnonalansa strategiset linjaukset valtioneuvoston päätösten mukaisesti. Nykyisen toimintamallin ja tutkimuksessa käytettyjen aineistojen perusteella on syntynyt näkemys siitä, että kyberturvallisuuden johtamisessa keskitytään liikaa oman hallinnonalansa

kyberturvallisuuteen, eikä niinkään yhteiskunnan kyberturvallisuuteen vaan ajattelua ohjaa oman organisaation ajattelumalli. Tätä tukee 2016 ilmeistynyt raportti ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”. Raportissa tutkittiin muun muassa Suomen kansallista kyberturvallisuuden nykytilaa julkishallinnossa, jossa tarkasteltiin ja arvioitiin vuoden 2013 kyberturvallisuusstrategiassa esitettyä visiota ja toimintamallia sekä sen strategisia linjauksia analysoitujen haastattelujen perusteella (Lehto 2017, 24). Lopuksi tuotiin esiin strategian linjaukset strategisen johtamisen osalta, joiden perusteella kansallista kyberturvallisuutta on pyritty kehittämään. Tässä luvussa käytiin läpi edellä mainitun raportin pohjalta Kansallisen kyberturvallisuuden nykytilaa siltä osin, kuin se liittyy strategiseen johtamiseen.

5.2.1 Kyberturvallisuusstrategian toteutuminen ja visio

Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä ja sen merkitys on kasvanut entisestään digitalisoitumisen myötä. Uudet uhat globaalissa ja kompleksisessa toimintaympäristössä vaikuttavat niin yksittäisiin ihmiseen, yrityksiin kuin yhteiskunnan eri toimintoihin. Tästä syystä on tärkeää turvata yhteiskunnan elintärkeät toiminnot kaikissa tilanteissa. Tämä johti kyberturvallisuusstrategian muodostumiseen. Strategiassa kyberturvallisuus ymmärretään tavoitetilana, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta voidaan turvata kaikissa tilanteissa. Srategian tavoite on ollut nostaa Suomi yhdeksi kyberturvallisuuden edelläkävijäksi vuoteen 2016 mennessä (Suomen kyberturvallisuusstrategia 2013, 1-2). Strategiassa määriteltiin kolmen kohdan visio, jonka käytiin läpi alaluvussa 5.1.1.

Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI laatii vuosittain tietoturvaan liittyvän kyselyn valtion hallintoon. Tulokset ovat osoittaneet, että kehitystä on tapahtunut mutta kehitettävää silti löytyy aina. Aikaisemmissa luvuissa on esitetty, että kybertoimintaympäristöstä tekee hankalan sen nopea muutosnopeus, jolloin siellä tapahtuvia uhkia on vaikea havaita. Tämä on ollut haasteena myös valtionhallinnossa ja erityisesti kansallisen tason johtamisen osalta. Kybertoimintaympäristö muuttuu ja kehittyy paljon nopeammin kuin hallinnossa tehdyt johtamis- ja päätöksenteko prosessit saadaan vietyä käytäntöön.

Havaitut puutteet koskivat asioita, jotka ovat keskeisessä asemassa onnistuneen kyberturvallisuuden muodostamisessa. Tällaisia olivat puutteet havainnointikyvyssä, tilannekuvassa ja –ymmärryksessä sekä laaja-alaisten hyökkäysten torjunnassa. Tämä johtunee edellä mainittujen tilannekuvan ja tilannetietoisuuden heikkoudesta sekä selkeän johtamismallin puuttumisesta. (Lehto 2017,67.)

Ministeriöt johtavat kyberturvallisuustyötä omilla hallinnonaloillaan. Haasteena kuitenkin on ollut, etteivät suunnitellut strategiat välttämättä kanavoidu toiminnaksi. Tämä ilmenee siinä, että kyberturvallisuus nähdään ainoas-

taan hallinnollisena asiana, eikä organisaatioissa tiedetä mitä ja miten sen kanssa pitäisi toimia. Toiseksi se nähdään useimmiten tietoturvallisuuskysymyksenä, jolloin myös ajatellaan, että se kuuluu ainoastaan organisaation ICT-sektorille. Aineiston perusteella kyberturvallisuus nähdään edelleen suurelta osin ”ulkopuolisena” asiana, eikä niinkään asiana, joka pitäisi integroida organisaation jokapäiväisen toiminnan osaksi. (Lehto 2017, 26) Tämä viittaa siihen, että Suomen kyberturvallisuuden johtamiselta puuttuu tahtotila strategisten päätösten saattamiseksi käytäntöön ja kyberturvallisuus ajattelun integroimiseksi osaksi organisaation kaikkia tasoja. Tähän tarvitaan uudenlaista johtamismallia, jossa siirryttäisiin pois hallinnonalakohtaisesta ajattelusta kohti yhteiskunta lähtöistä ajattelumallia. Toiseksi, kuten aikaisemminkin tässä luvussa todettiin, hallinnollisten strategisten päätösten saattaminen osaksi käytännön toimintaa kestää liian kauan, kun otetaan huomioon kybertoimintaympäristön luonne nopeasti kehittyvänä globaalina ilmiönä.

Lehto (2017, 27) tutkimusraportissa mainitaan myös resurssit. Kyberturvallisuuden johtaminen ja kehittäminen on mahdotonta ilman riittäviä ja oikein kohdistettuja resursseja. Tehtävien lisääntyessä lisäresurssien saaminen kyberturvallisuuden kehittämiselle olisi välttämätöntä. Näin ei kuitenkaan ole tapahtunut. Miten kyberturvallisuutta voidaan kehittää, jos ei ole riittäviä resursseja kehitystyöhön? Toisaalta raportissa mainittiin myös, että hallinnossa ollaan tällä hetkellä tekemässä suurta taustajärjestelmien uudistamistyötä, joka osaltaan varmasti on vaikuttanut resurssien niukkuuteen. Uusissa taustajärjestelmissä on integroitu kyberturvallisuuselementti mukaan kehitykseen, joka on osaltaan vauhdittanut kehitystyötä kyberturvallisuuden jalkauttamiseksi kaikkeen toimintaan. Tästä huolimatta, kyberturvallisuutta kehitetään yhä muun työn ohessa. Tähän tulisi tulla muutos, koska kyberturvallisuus on tullut jäädäkseen. Se ei ole irrallinen projekti, jolla on alku ja loppu, vaan se on prosessi, joka jatkuu ja jota tulee kehittää koko ajan muuttuvan toimintaympäristön mukana. Kyberturvallisuuden johtamisessa tuleekin huomioida toimintaympäristön turvallisuuden varmistamiseksi riittävät, oikein kohdistetut resurssit sekä kyberturvallisuuden liittäminen osaksi kokonaisvaltaista turvallisuusajattelua.

5.2.2 Kyberturvallisuuden nykytila ja johtamiseen vaikuttavat asiat

Johtamisen kannalta merkittävimmät havainnot liittyvät valtion hallinnon strategia- ja johtamispäätösten hitauteen, jolla kyberturvallisuuden kannalta tarkoitetaan sitä, että päätöksiä viedään käytännön tasolle paljon hitaammin suhteessa kybertoimintaympäristön muutosnopeuteen. Tällöin tehdyt strategiset päätökset ehtivät jo vanhentua ennen niiden vaikutusta käytännön operatiivisella tasolla. Strategisessa johtamisessa tulisi painottaa tehokkuuteen ja järjestelmällisyyteen, jotta päätökset saataisiin vietyä käytäntöön nopeammin. Toiseksi kyberturvallisuuden johtamisen osalta puuttuu selkeä ja johdonmukainen johtamismalli. Tällä ei tarkoiteta pelkästään valtionhallintoa vaan koko kansallista kyberturvallisuuden johtamista. Strategisen johtamisen osalta tulisi nähdä selkeä ja riittävän toimivaltainen johtamismalli, jolla niin strategisten päätösten

vieminen käytäntöön kuin kokonaisuudenkin johtaminen yksinkertaistuu. Tällä hetkellä hallinnonaloilla keskitytään pitkälti oman ”tonttinsa” hoitamiseen eikä nähdä kokonaiskuvaa kybertoimintaympäristöstä. Ajattelumalli keskittyy oman organisaation kyberturvallisuuden hoitamiseen, kun sen pitäisi keskittyä koko yhteiskunnan huomioon ottavaan johtamismalliin (Lehto 2017, 67–68.)

Yhteistyö on tärkeä osa kyberturvallisuuden johtamista. Kansallisella tasolla hyviä kokemuksia on tullut kyberturvallisuuskeskuksen ja valtioneuvoston tilannekeskuksen välisestä yhteistyöstä, joka nykytilan mukaan on riittävällä tasolla. Tämän lisäksi hallinnon organisaatioissa yhteistyötä tehdään niin sisäisesti kuin myös poikkihallinnollisesti, vaikka yhteistyön toteutumista vaikeuttaa edellä kuvatut asiat esimerkiksi haasteet turvaluokiteltujen tietojenvaihdosta. Tämän hetkisen näkemyksen mukaan yhteistyö hallinnonaloilla toimii kohtalaisesti, vaikka kehitettävää vielä löytyy etenkin hallinnon ja yksityisen sektorin välisestä yhteistyöstä. Tällä hetkellä tietojenvaihto yksityisen sektorin, erityisesti kriittisten yritysten osalta voisi olla tehokkaampaa. Tehokkuutta rajoittaa erityisesti se, ettei yrityksillä ole laillista ilmoitusvelvollisuutta kyberuhkista ja erilaisista häiriötilanteista. (Lehto 2017, 67.) Strategisen johtamisen kannalta niin kansallisella kuin kansainvälisellä yhteistyöllä on paljon annettavaa. Kansainvälisiltä kyberturvallisuuden edelläkävijöiltä voimme oppia uusia työskentely- ja toimintatapoja, jotka liittämällä osaksi kansallista kyberturvallisuuden johtamista, merkittäviä parannuksia voidaan saavuttaa nykyiseen johtamismalliin.

6 AINEISTOTUTKIMUS VIRON, ISRAELIN JA ALANKOMAIDEN KYBERTURVALLISUUDEN JOHTAMISESTA

Tutkimuksen tavoite, tutkimusongelma sekä tutkimuskysymykset on esitetty aikaisemmin luvussa kaksi (2); tutkimuksen tarkoitus ja tavoitteet. Samaisessa luvussa selvitetään myös aineistotutkimuksen toteutukseen sekä analysointiin käytettyjä menetelmiä.

6.1 Tutkittavat valtiot

Tutkimukseen valittiin tarkasteltaviksi kolme valtiota: Alankomaat, Israel sekä Viro, joiden valinnassa apuna käytettiin International Telecommunication Unionin (ITU) Global Cybersecurity Indexiä (GCI) sekä ABI Researchin kyberturvallisuusindeksiä soveltuvin osin. Tutkimukseen haluttiin valita mukaan sellaisia valtioita, jotka olisivat kooltaan Suomen kokoisia ja jotka olisivat suhteellisen korkeasti luokiteltuja kyberturvallisuusindeksin perusteella. Valitut valtiot Suomi mukaan luettuna sijoittuivat vuoden 2017 indeksin Kansainvälisessä vertailussa; Suomi (16), Viro (5), Israel (20) ja Alankomaat (15). Kaikki vertailuvaltiot olivat, Israelia lukuun ottamatta Suomen edellä vuoden 2017 indeksin perusteella. Kaikkiaan vertailumaita oli 164. Vaikka indeksi ei keskity tutkittavaan osa-alueeseen kyberturvallisuuden strategisen johtamisen osalta, voidaan indeksin sijoittumisen perusteella todeta, että kaikki vertailuvaltiot ovat Kansainvälisesti tarkasteltuna kärkimaita kyberturvallisuudessa (GCI 2017, 59–65.)

Tutkimuksessa keskitytään löytämään tarkasteltavista maista sellaisia kyberturvallisuuden strategisen johtamisen käytänteitä, joita johtopäätöksissä voidaan nostaa esiin Suomen kansallisen kyberturvallisuuden johtamisen kehittämiseen. Valtioiden valintaan vaikuttivat myös tutkijan oma kiinnostus valittuja vertailuvaltioita kohtaan. Tutkimussuunnitelman mukaisesti lähdeaineis-

toa kerättiin julkisesti saatavissa olevista lähteistä. Käytetty lähdemateriaali on nähtävissä lähdeluettelosta.

6.2 Viro

Viro tunnetaan Suomen kaltaisena pienenä valtiona, jossa kansalliset yhteiskunnalliset palvelut on toteutettu kehittyneillä teknologisilla ratkaisuilla sekä innovatiivisella lähestymistavalla. Palveluiden voimakas digitalisoituminen ja siirtyminen fyysisestä maailmasta sähköiseen maailmaan on lisännyt tarvetta vahvistaa yhteiskunnallisten palveluiden turvallisuuden varmistamista kybertoimintaympäristössä vaikuttavien uhkien ja häiriöiden osalta. Digitalisaatio vaikuttaa vahvasti Viron yhteiskunnallisissa sähköisissä palveluissa, joista esimerkkeinä kansalaisten sähköinen äänestys sekä digitaalisen allekirjoituksen (X-road system) mahdollistaminen yhteiskunnallisissa palveluissa. Yhteiskunnallisten palveluiden siirtyminen osaksi tietoverkkoja on tehnyt kyberturvallisuudesta ja sen kansallisen tason strategisesta johtamisesta erityisen tärkeää. Viron pääasiallinen tavoite kyberturvallisuuden osalta on kyberturvallisuuden kyvykkyyksien vahvistaminen sekä kansalaisten tietoisuuden lisääminen kyberturvallisuuden uhkista. Näillä toimilla pyritään varmistamaan kybertoimintaympäristön jatkuva luotettavuus. (Osula 2015, 5-6.)

6.2.1 Viron kyberturvallisuusstrategia

Viro julkisti yhtenä ensimmäisistä valtioista kyberturvallisuus strategian vuonna 2008, jolloin kyberturvallisuus kuului puolustusministeriön alaisuuteen. Strategia laadittiin Viron puolustusministeriössä vuosille 2008–2013. Kyberturvallisuus on strategiassa määritelty hyvin selkeästi osaksi Viron kansallista turvallisuutta. Strategian painopiste on vahvasti suuntautunut puolustus- ja turvallisuusnäkökulmaan, johtuen pitkälti strategityön perustan olevan Puolustusministeriössä. Tämän jälkeen vastuu kyberturvallisuudesta siirrettiin Talous- ja Viestintäministeriölle, joka kertoo kyberturvallisuuden merkityksen kasvusta ja laaja-alaisemmasta käsitteen ymmärryksestä. Strategiatyö sai jatkoa vuonna 2014, jolloin julkistettiin strategian toinen versio vuosille 2014–2017. Toisessa versiossa kiinnitettiin huomiota laajemmin johtamisen tärkeyteen kansallisen kyberturvallisuuden varmistamisessa. Kehitystyössä oli mukana useita julkisia, yksityisiä sekä akateemisia tahoja (Osula 2015, 6-7) Viron kyberturvallisuusstrategian kolmas versio on tekeillä ja valmistumassa syksyllä 2019. Strategisen johtamisen osalta johtamismalli tulee noudattelemaan samaa linjaa kuin nykyinen strategia, mutta kyberturvallisuuden rooli osana yhteiskunnan talouden kehitystä korostuu entisestään (Mänd 2018). Strategia tulee keskittymään entistä enemmän päätavoitteen määrittelyyn ja sitä kautta koko strategian tavoitteiden selkeyttämiseen. Lainsäädännön uudistaminen on myös keskeinen osa kansallista kyberturvallisuutta.

Strategian toisessa versiossa (Estonia national cyber security strategy 2014, 12–14) strategisen johtamisen kannalta keskeisiä kohtia ovat:

1.1 ”Varmistaa vaihtoehtoiset ratkaisut tärkeille palveluille”

Kansalliset palvelut, jotka riippuvat ICT infrastruktuurista ja sähköisistä palveluista on päivitetty, kartoitettu sekä hallittu. Palveluita tulisi kyetä johtamaan sellaisissa tilanteissa, kun normaaleita toimintoja ei pystytä käyttämään uhkan tai toimintahäiriön aikana.

1.3 ”Varmistaa ICT infrastruktuurin ja palveluiden turvallisuus”

Valtiolle elintärkeiden palveluiden toimintaa tarvitsevat tietojärjestelmät kehitetään ja hallitaan tavalla, joka tukee toimintaympäristön turvallisuusriskejä ja tarjoaa keinot ja toimenpiteet näiden riskien hallitsemiseksi.

1.7 ”Kansainvälisen yhteistyön edistäminen kriittisen infrastruktuurin turvaamisessa”

Kyberturvallisuuden johtamisessa tulee huomioida vahvasti kansainvälinen yhteistyö. Kriittisen infrastruktuurin suojaaminen on riippuvainen yhteistyöstä kansainvälisten organisaatioiden kanssa.

2.3/3.2 ”Kansainvälisen yhteistyön kehittäminen kyberuhkien torjunnassa”

Tehokkaan ja ajantasaisen kyberuhkien torjunnan saavuttamiseksi kansainvälisessä toimintaympäristössä, tulee tiedonvaihtoa valtioiden välillä kehittää. Aktiivinen osallistuminen hankkeisiin ja projekteihin lisää kykyä torjua kansainvälisiä kyberuhkia. Tärkeässä asemassa on yhteistyö NATOn sekä Euroopan Unionin kyberturvallisuus virastojen kanssa. Tähän tavoitteeseen liittyy vahvasti myös toissijainen tavoite kansallisen kyberturvallisuuden kyvykkyyksien kehittämisestä. Tämä edellyttää käytössä olevien resurssien kohdentamista oikein kyberavaruudessa toimivien valtiollisten organisaatioiden kesken.

5/5.1 ”Lainsäädännön ja monialaisen toiminnan kehittäminen”

Kehittämällä ja sopeuttamalla sekä oikeudellisia puitteita että kyberturvallisuuden ulkopolitiikkaa, kyetään suojaamaan paremmin kriittisen infrastruktuurin palveluja.

5.3 ”Yhteistyön kehittäminen liittolaisiin ja kumppaneihin”

Kyberturvallisuudessa huomioidaan laajempi ja läheisempi suhde yhteistyökumppaneihin sekä Euroopan Unioniin. Yhteistyöllä pyritään tehostamaan Euroopan Unionin jäsenmaiden valmiutta ja kykyä torjua toimintaympäristön kyberuhkia.

6.2.2 Viron johtamismalli

Virossa kyberturvallisuuden tehtäväalueeseen liittyviä asioita käsitellään kansallisella tasolla horisonttaalisesti. Tämä tarkoittaa sitä, ettei kyberturvallisuudesta vastaa ainoastaan yksi organisaatio. Virossa kansallisen kyberturvallisuuden strategisesta johtamisesta vastaa ylimmällä tasolla kansallinen kyberturvallisuuden valiokunta (National Cybersecurity Council), jonka puheenjohtajana toimii Viron talous- ja viestintäministeriön pääsihteeri. Kyberturvallisuusvaliokunta koostuu eri ministeriöiden ja valtion laitosten edustajista, mukaanlukien Viron puolustusvoimien ja puolustusliiton edustajat. Neuvosto vastaa kyberturvallisuuden strategisista päätöksistä kansallisella tasolla. Jokaisella virallisella kokouksella on neuvostolla aikaisemmin esitelty asialista päätöskohdiltaan (Mänd 2017)

Yleisesti tarkasteltuna viisi eri ministeriötä vastaa Viron kyberturvallisuudesta. Talous- ja viestintäministeriö (The Ministry of Economic Affairs and Communications) ohjaa kyberturvallisuuspolitiikkaa ja koordinoi Viron kyberturvallisuusstrategian täytäntöönpanoa. Täytäntöönpano on kaikkien toimijoiden vastuulla, niin yksityisten kuin hallinnonalojen eri toimijoiden. Organisaatiot raportoivat ministeriölle vuosittain. Toimijoiden välistä yhteistyötä tukee turvallisuuskomitean alainen Kyberturvallisuusneuvosto, joka myös valvoo strategisella tasolla täytäntöönpanoa (Lehto 2018, 62.) Talous- ja viestintäministeriön alla toimii myös Tietojärjestelmäviranomainen (RIA), jonka tehtävänä on koordinoida valtion tietojärjestelmien ja –verkkojen kehittämistä. Tehtäviin kuuluu myös järjestää tietoturvallisuuteen liittyvää yhteistoimintaa. Tietojärjestelmäviranomaisen (RIA) toiminnan perustan muodostaa kriittisen infrastruktuurin toiminnasta huolehtiminen. Tällä tarkoitetaan yhteiskunnan tietoliikenneyhteyksien toimintavarmuudesta huolehtimista. Viranomaisen tehtäviin kuuluu myös X-Road –palveluväylän ylläpitäminen, joka on eViron perusta. Tämän lisäksi tehtäviin kuuluu myös tietojärjestelmien tietojen varmuuskopiointi yhteiskunnallisista palveluista sekä erilaisten kyberturvallisuuteen liittyvien strategioiden ja suunnitelmien tekeminen. Tietojärjestelmäviranomainen on hiljattain saanut oikeuden myös kuulustella ja sakottaa ihmisiä. Näyttöä tämän oikeuden hyödyllisyydestä ei kuitenkaan vielä ole. RIA :n alla toimii lisäksi erityinen friittisen tietoliikenneinfrastruktuurin suojaamisosasto. Osaston tehtävänä on edistää julkinen-yksityinen yhteistyötä vaihtamalla muun muassa opertatiivista tietoa, havaitsemaan kybertoimintaympäristössä vaikuttavia ongelmia sekä kehittämään havaittujen ongelmien perusteella kriittisen infastruktuurin toimintaa. (Lehto 2018, 62-63.)

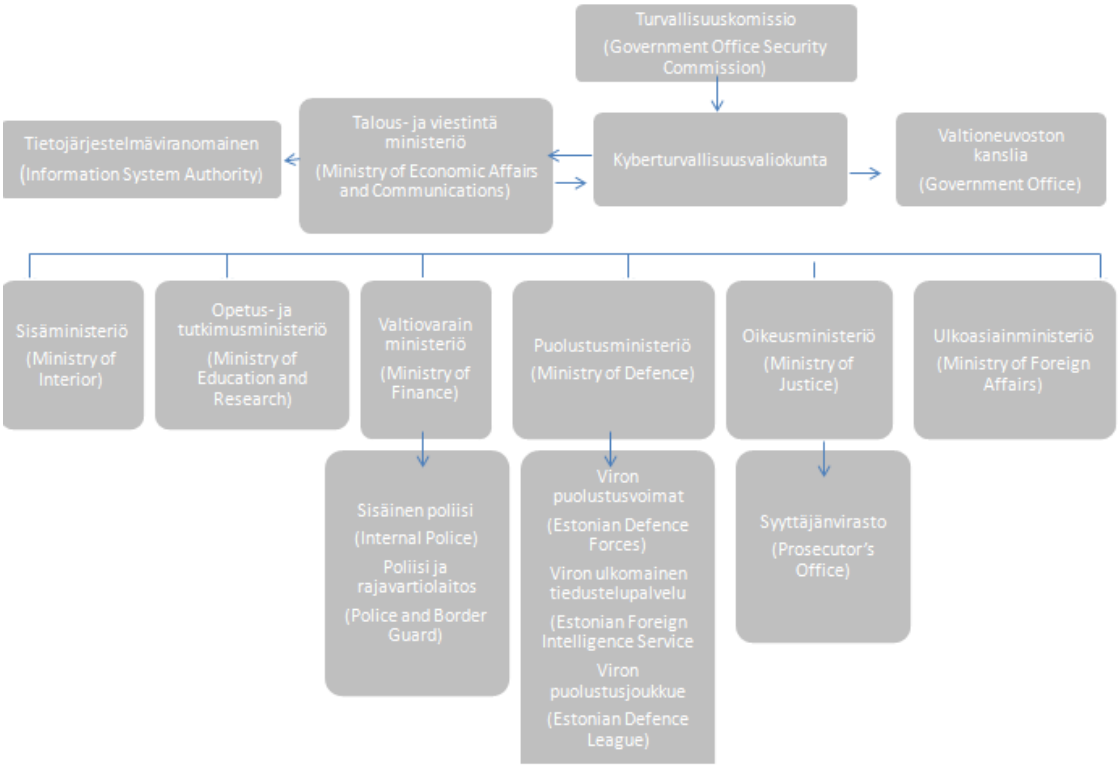
Puolustusministeriö (Ministry of Defence) koordinoi kansallista puolustusta. Puolustusministeriön yhteydessä toimii erillinen osasto, jonka tehtäviin kuuluvat muun muassa hallinnonalan tietojärjestelmien kehittäminen sekä erilaisten politiikkojen suunnittelu ja niiden koordinointi. Osastossa työskentelee sekä valtion virkamiehiä että yksityisen sektorin edustajia. Erityisesti kyberpuolustus on tulevaisuuden kannalta kehittämistä vaativa kyvykkyys. Puolustusministeriön alaisuudessa ylläpidetään kyberpuolustukseen tarkoitettua harjoitusympäristöä. Harjoitusympäristön kehittäminen toteutetaan yhteistyössä NATO:n kyberturvallisuuskeskuksen sekä yksityisen kyberyksikön kanssa (Lehto 2018, 62-63.)

Viron asevoimien tehtävänä on varmistaa strategisen tieto- ja kommunikaatioteknologian toiminnallisuus ja käytettävyys kaikissa tilanteissa. Tätä varten on perustettu erillinen Strategisen kommunikaation keskus, jonka tehtäviin kuuluvat asevoimien käytössä olevien tietojärjestelmien tietoturvallisuuden ylläpitäminen, sähköisten toimintojen tuottaminen hallinnonalan eri yksiköille, kuten esimerkiksi sähköisen sodankäynnin kehittäminen, kyberpuolustuksen suunnitteleminen sekä kyberlaboratorion toiminnan järjestäminen. Myös kansallisen tason kyberrikosten tutkinta on keskitetty yhteen osastoon, jonka kyberturvallisuuden eri osa-alueiden tutkintaa ja tiedustelutoimintaa kehitetään jatkuvasti (Lehto ym. 2018, 63-64). Oikeusministeriö (Ministry of Justice) ja sisäasiainministeriö (Ministry of Internal Affairs) vastaavat tietoverkkorikollisuutta ja kyberavaruutta koskevaan terrorismiin liittyvistä asioista. Opetusministeriö (Ministry of Education) valvoo kyberturvallisuuteen liittyvää koulutusta (Mänd 2017).

Ministeriöiden lisäksi Virossa on myös muita valtion laitoksia, jotka osallistuvat kyberturvallisuuden johtamiseen. Äskettäin mainitun Tietojärjestelmäviranomaisen (Information System Authority, RIA) lisäksi Virossa toimii RIAn alainen CERT-EE, joka vastaa Viron tietoliikenneverkoissa tapahtuvien kyberturvallisuus tapahtumien käsittelystä. Sen tehtäviin kuuluu myös Viron kansalaisten avustaminen ja neuvominen erilaisissa internetin käyttöön liittyvissä asioissa. Kuten Suomessakin, Tietojärjestelmäviranomainen julkaisee myös erilaisia kybertoimintaympäristöön liittyviä varoituksia. Viraston tehtävänä on myös toimia eräänlaisena yhteistyövirastona valtion virastojen ja yksityisen sektorin välillä, olla teknillisten ammattilasten tukena sekä lisätä kybertietoisuutta yhteiskunnassa. CERT-EE hallinnoi virtuaalista tilannehuonetta, joka toimii hallinnon eri toimijoiden välisenä yhteistyöympäristönä tarkoituksena erilaisten kriisien ennaltaehkäisy. Viron lainsäädännön mukaan kaikkien valtion organisaatioiden on ilmoitettava tietoturvaloukkaukset CERT-EE :lle ja myös NATO:n CCDCOE–kyberosaamiskeskukselle. Sen pääasiallisena tehtävänä on lisätä kyberpuolustuksen valmiuksia, yhteistyötä ja tiedon jakamista NATO:n, NATO-maiden ja kumppanien välillä koulutuksen, tutkimuksen, opittujen kokemusten sekä kuulemisten perusteella (Lehto 2018, 62-63.)

Viron kyberturvallisuuden strategiset tavoitteet nojaavat vahvasti Viron kyberturvallisuusstrategiaan. Viro valmistelee parhaillaan kolmatta painosta

kyberturvallisuusstrategiasta vuosille 2019–2022 ja sen valmistelutyöstä vastaa talous- ja viestintäministeriö. Strategiset päätavoitteet nojaavat kykyyn lisätä kybertoimintaympäristön turvallisuutta sekä yhteiskunnan tietoisuutta kybertoimintaympäristössä vaikuttavista kyberuhkista sekä varmistaa yhteiskunnan luottamus kyberavaruudessa. Uusi strategia tulee painottumaan kyberturvallisuuden johtamisen kannalta kriittisen infrastruktuurin suojelemiseen, kansainvälisen yhteistyön kehittämiseen sekä kansallisen lainsäädännön kehittämiseen vastaamaan nykytilan ja tulevaisuuden haasteita kybertoimintaympäristössä (Mänd 2017.) Viron kansallisen kyberturvallisuuden johtamisen keskiössä oleva kyberturvallisuuden valiokunta määrittelee kansallisen tason strategiset suuntaviivat. Se toimii vahvana yhdistävänä organisaationa, joka selkeästi näyttää olevan toiminnan johtamisen keskiössä. Viron johtamismallin vahvuutena toimiva valiokunta johtaa kansallista kyberturvallisuutta selkeästi ja määrätietoisesti, mikä näkyykin esimerkiksi Viron kolmannen kyberturvallisuusstrategian valmistumisena alkuvuodesta 2019. Strategiseen johtamiseen kansallisella tasolla yhdistyy monitasoinen vuorovaikutus toimintaympäristön eri vaikuttajien (yksityinen sektori, julkinen sektori, järjestöt ja yhdistykset) välillä, joka on havaittavissa Viron johtamismallissa. Aineiston perustella voidaan sanoa, että Viron kyberturvallisuuden avaintoimijoiden välillä on aktiivista, yhteiskunnan luottamusta kasvattavaa vuorovaikutusta. Alla olevasta kuviosta 8 ilmenee Viron kyberturvallisuuden johtaminen organisaatiokaavion muodossa.



Kuvio 8 Viron kansallinen kyberturvallisuuden johtaminen

6.2.3 Haasteet strategisen johtamisen kannalta

Kansallinen kyberturvallisuusstrategia määrittelee suurimmiksi haasteiksi kyberturvallisuuden johtamisen kannalta yhteiskunnan sähköisen yhteiskunnan nopean kasvun. Sähköisen toimintaympäristön nopea kehitys on luonut haasteita kyberuhkien ja erilaisten häiriöiden osalta, jotka toteutuessaan saattavat vaikuttaa yhteiskunnan sähköisten palvelujen ja toimintojen toimivuuteen. Strategiassa on määritelty yhdeksi kehittämiskohteeksi myös kansallisen viestinnän ja kansainvälisen yhteistyön kehittäminen, jotka voidaan nähdä merkittävinä strategisen johtamisen kannalta olevina kohteina (Estonia national cyber security strategy 2014, 5-6). Jotta Virossa voitaisiin kyetä tarjoamaan kansallisen tason kyberavaruuden tehokasta puolustusta, on kyettävä integroimaan valtion siviili- ja sotilasresursseja siviiliviranomaisten toimintaan sekä varmistamaan kyvykkyydet kansainvälisten yhteistyötahojen kanssa. Kyberturvallisuuden strategisessa johtamisessa tulee kyetä ennakoivasti suunnittelemaan toimintaympäristöön kohdistuvia muutoksia sekä suunnittelemaan ja investoimaan nykyaikaiseen teknologiaan. Vuoden 2017 aikana, Viro on panostanut huomattavia resursseja riskien tunnistamiseen ja aikaiseen havainnointiin, joka on mahdollistanut matalamman riskitason yhteiskunnan elintärkeille järjestelmille ja palveluille sekä nopeamman palautumisen mahdollisissa toimintaympäristöä kohtaavissa häiriötapauksissa. Vaikka parempi yhteistyö kriittisten toimijoiden välillä on parantunut, ei kaikkia kyberuhkia pystytä havaitsemaan riittävän ajoissa. Kehittämistä on edelleen, erityisesti terveydenhuollon sekä pienien yritysten osalta, joita kohdanneet kyberuhkat havaitaan vasta siinä vaiheessa, kun suurin vahinko on jo päässyt tapahtumaan. (Annual cyber security assessment 2018, 5-6)

6.2.4 Kansallisen kyberturvallisuuden strateginen kehittäminen tulevaisuudessa

Viron tasavallan ja valtion tietojärjestelmien varmistamiseksi yhteiskunnan kriittisten tietojärjestelmien tiedot kopioidaan virtuaalisiin ”lähetystöihin” eri puolilla maailmaa. Tällä pyritään varmistamaan Viron valtion jatkuvuus ”pilvipalvelussa”, joka lisää yhteiskunnan sähköisten tietojen resilienssiä kyberuhkia ja häiriöitä vastaan.

Kansallisella tasolla valtion laitosten työntekijöiden ICT-taitoja ja -tietoisuutta yhteiskuntaan vaikuttavista ilmiöistä lisätään. Kehityksessä otetaan huomioon myös tulevaisuuden trendit ja tarpeet. (Agenda 2016, 36)

Agenda 2020 (2016, 36) määrittelee kehitysalueet Viron hallinnon rakenteen kehittämiseen. Määrittely perustuu aiempien strategioiden täytäntöönpanoon sekä erilaisissa keskusteluissa esiin tulleisiin ja havaittuihin kehittämistarpeisiin. Raportista on hyvä huomioida, että agendassa kehitystarpeissa korostetaan tehokkaan koordinaation varmistamista, joka pitää sisällään tiedonkulun parantamisen sekä kaikilla tasoilla tapahtuvan yhteistyön kehittämisen. Strategisen tason johtamiseen näkisin myös sellaisen kehityksen luomisen, jolla

pyritään varmistamaan pitkän aikavälin näkökulmien kehittymisen ja toteuttamisen, jotta voidaan kehittää kyberturvallisuuden edellytyksiä koko kansallista kyberturvallisuutta ajatellen. Agendan mukaisesti pyritään myös varmistamaan strategisen suunnittelun ja täytäntöönpanon välisten yhteyksien selkeys ja johdonmukaisuus. Tavoitetilassa valtio sekä eri alojen yritykset ja organisaatiot mahdollistaisivat yhteiseen päämäärään ponnistamisen. Tämä kuitenkin vaatisi nykyistä parempaa yhteistyötä, tehokkaampaa sopimusten täytäntöönpanoa sekä huomattavasti nykyistä enemmän tavoitteellista strategista keskustelua. (Agenda 2016, 40–42) Tutkimuksia lukiessa huomaa selvästi Viron pyrkimyksen rakentaa kyberturvallisuutta maan rajojen ulkopuolelta sisälle päin. Olemalla mukana kyberturvallisuuden kansainvälisillä pelikentillä, voidaan kyberturvallisuuden rakentamiseen vaikuttaa, millaiseksi se muodostuu kansallisella tasolla. Kyberturvallisuuden johtamisessa painotetaankin vahvasti kansainvälistä yhteistyötä. Viron kyberturvallisuuden suunta on menossa painotukseltaan kyberpuolustukseen, mikä näkyy Viron puolustusministeriön vahvana roolina strategisten tavoitteiden osalta. Esimerkiksi Viron puolustusstrategiasta käy ilmi, että puolustusvoimien rauhanajan kyberammattilaisten määrä on noin 300 henkilöä, jotka työskentelevät tiiviisti osana NATO:a erilaisissa tehtävissä. Päämaja sijaitsee fyysisesti Tallinnassa mutta virtuaalisesti siellä, missä milloinkin on tarvetta (National Defence Strategy, 32). Virossa kyberturvallisuutta pyritään kehittämään ajatuksella, että sitoutetaan kaikki yhteiskunnan eri tasot (yksilö, yksityiset yritykset, valtio) mukaan, jolloin päästään parempaan kyberturvallisuuden tietoisuuteen sekä mahdollistetaan tehokkaampi tiedonkulku. (Lehto 2017, 62–64).

6.3 Alankomaat

Alankomaat nähdään yhtenä Euroopan kehittyneimmistä IT-intensiivisistä valtioista sen kehittyneen digitaalisen infrastruktuurin johdosta. Alankomaita voidaan pitää yhtenä suurimmista kansainvälisistä internet-keskuksista, jolla on maailman kilpailukykyisimmät sähköiset markkinat. Internet-käyttäjien määrässä tarkasteltuna, käyttäjien määrä on mailman huippua väkilukuun suhteutettuna. Kyberturvallisuus nähdään välttämättömänä ja merkittävänä tekijänä Alankomaiden yhteiskunnan ja talouden toimijoiden kannalta. Moitteettoman digitaalisen toiminnan kannalta avoin ja innovatiivinen toimintaympäristö ovat avainasemassa. Sekä kansallinen että kansainvälinen digitaalinen toimintaympäristö ja sen kehittäminen ovat räjähdysmäisesti kasvaneet viime vuosina, johtuen kybertoimintaympäristössä vaikuttavien uhkien merkittävästä kasvusta. Nämä uhkat eivät ainoastaan häiritse Alankomaiden kehittynyttä infrastruktuuria vaan voivat toteutuessaan vaikuttaa sen tiedon eheyteen, saatavuuteen sekä luotettavuuteen, jota yhteiskunnassa dokumentoidaan ja analysoidaan. Jotta Alankomaat pystyvät vastaamaan tulevaisuudessakin näihin yhä kasvaviin uhkiin, tulee yhteistyötä laajentaa ja voimistaa niin kansallisella kuin kansainväliselläkin tasolla

tarkasteltuna. Kyberturvallisuutta tulee tarkastella enemmän internetin vapauteen, ihmisoikeuksiin sekä yhteiskunnan sosiaalisiin ja taloudellisiin etuihin rinnastettava innovatiivisena mahdollisuutena kuin erillisenä ja eristettynä asiana (National Cyber Security Strategy 2, 7-8.) Strateginen johtaminen korostuu tämän tavoitteen saavuttamisessa, sillä ilman tiivistä yhteistyötä yksityisten ja julkisten toimijoiden välillä niin kansallisesti kuin kansainvälisesti ei voida riittävästi voimallisesti vaikuttaa kybertoimintaympäristössä tapahtuviin muutoksiin ja saavuttaa strategian mukaisia tavoitteita .

6.3.1 Alankomaiden kyberturvallisuusstrategia strategisen johtamisen näkökulmasta

Nykyinen Alankomaiden kyberturvallisuusstrategian (NCSS2) keskiössä kuvataan strategian kolme tärkeintä periaatetta avoimuus, tieto sekä sääntely. Keskiön laidoilla on turvallisuus, vapaus sekä sosio-ekonomiset edut. Strategian tavoitteiden perusteella keskiön ulkolaidoilla olevien tavoitteiden tulisi muodostaa tasapaino toimintaympäristön kaikkien toimijoiden välillä niin kansallisella tasolla kuin kansainvälisestikin. Strategiasta tulisi huomioida, että tavoitteiden tulisi toteutua kybertoimintaympäristössä, joka siis käsittää niin fyysisen kuin sähköisen ulottuvuuden. (Lehto 2017, 51-52). Strategia nojaa vahvasti visioon, jonka mukaan tavoitteena on luoda avoin ja turvallinen digitaalinen toimintaympäristö, jossa voidaan hyödyntää digitalisaation tarjoamia mahdollisuuksia ja jossa uhkia torjutaan tehokkaasti. Strategian visio korostaa selkeää hallintomallia, kansainvälistä yhteistyötä, digitaalisen maailman avoinmuutta sekä ihmisoikeuksia. Nykyinen strategia tähtää strategisen johtamisen näkökulmasta tehokkaampaan yksityisen ja julkisen sektorin osallistamiseen sekä kansainvälisen yhteistyön kehittämiseen ja osallistumiseen erilaisiin kyberturvallisuutta käsitteleviin foorumeihin kuin myös tiiviimpää kahdenkeskeistä yhteistyötä eri valtioiden kanssa. Strategisella johtamisella pyritään luomaan riittävät toimintamallit ja edellytykset kansallisen tason kyberturvallisuudelle, esimerkiksi elintärkeiden toimintojen ja prosessien turvaamiseksi (National Cyber Security Strategy 2, 4-9.) Tämän perusteella voidaan nähdä, että kyberturvallisuus alkaa maan rajojen ulkopuolelta, jossa korostuu kansainvälinen yhteistyö niin siiviliverkostojen kuin sotilaallisten verkostojen osalta. Kansallisella tasolla kyberturvallisuutta johdetaan eri toimijoiden välisellä tiiviillä yhteistyöllä, jossa korostetaan innovatiivista kehitystä erityisesti elintärkeiden palveluiden ja toimintojen turvaamisessa. Valtion rooli kyberturvallisuuden johtamisessa korostuu verkkojen ja palveluiden turvaamisessa, yhteiskunnan ja kansalaisten sekä tietosuojan turvaamisen tiedottamisessa sekä toimia keskeisenä valtiollisena keskuksena edistääkseen digitaalisten mahdollisuuksien hyödyntämistä yhteiskunnassa. Alankomaissa kyberturvallisuuden johtaminen lähtee jo aikaisemmin esitetystä näkemyksestä, missä kyberturvallisuudelle luodut säännöt ja periaatteet koskettavat niin sähköistä kuin fyysistäkin

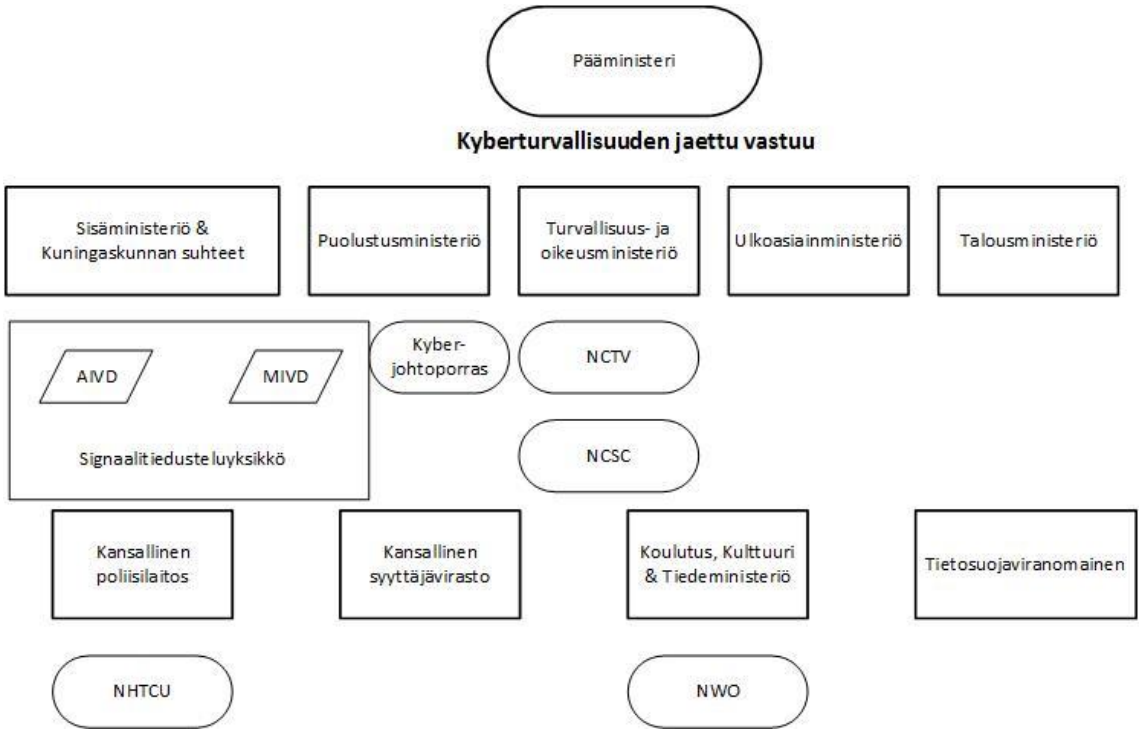
toimintaympäristöä. Vaikka turvallisuus- ja oikeusministeriö vastaa kansallisen kyberturvallisuuden koordinoimisesta, on vastuuta siirretty portaittain alaspäin niin, että se taho jota asia koskettaa, hoitaa käsittelyn, tai jos kyse on yhteiskunnallisesta häiriöstä, siitä vastaa häiriön toimintaa ohjaaja ministeriö tai vielä laajemmissa tapauksissa erillinen kriisinhallintaneuvosto (Lehto 2018, 52-54). Strategian mukaisesti kyberturvallisuuden johtamista tulee vahvistaa erityisesti yhdistämällä innovaatioita osaksi sektoreiden poliittista johtamista sekä muodostaa korkeakoulujen, valtion sekä liike-elämän yhdistävä kyberturvallisuuden innovaatioalusta, joka toimisi eräänlaisena ideointi portaalina sekä yhteyksien luojana alasta kiinnostuneiden tutkijoiden, yritysten sekä opiskelijoiden välillä. Kansallisen kyberturvallisuuskeskuksen asemaa osana kansallista kyberturvallisuutta tulisi vahvistaa, jotta tilannetietoa voitaisiin jakaa pyynnöstä entistä tehokkaammin yksityisille ja valtiollisille toimijoille. Koska kyberuhat tulevat yhä useammin maan rajojen ulkopuolelta, tulee kansallinen lainsäädäntö nykyaikaistaa sellaiseksi, että se mahdollistaa tehokkaampien keinojen käytön rikosten tutkimiseksi ja selvittämiseksi. Kyberturvallisuuden johtamisen täytyy ulottua myös maan rajojen ulkopuolelle, jolloin on välttämätöntä vahvistaa ja laajentaa kansainvälistä yhteistyötä rikosten ratkaisemiseksi. Yhteistyön lisäämiseksi Alankomaat on suunnitellut osaamiskeskuksen perustamista, joka keskittyisi erityisesti kansainväliseen lakiin ja kyberturvallisuuteen. Osaamiskeskus toimisi myös toimijoita yhdistävänä foorumina, joka mahdollista strategisen johtamisen kannalta tärkeän tiedonkulun lisääntymisen kansallisen ja kansainvälisen tiedonvaihdon osalta. Yhtenä kansallisen tason strategisen johtamisen kannalta merkittävänä asiana voidaan pitää, että strategiassa selkeästi määritellään hallinnolle velvollisuus edistää ja helpottaa aloitteita, joiden tarkoitus on kehittää kyberturvallisuutta. Alankomaiden hallinnolle on määritelty selkeä tavoite olla edistämässä niin hallinnon, kansalaisten kuin liike-elämän digitaalisen kestävyyden kehittymistä erityisesti vahvistamalla kansalaisten digitaalisia taitoja, tutkimusta ja innovaatiota sekä tukemalla demokratiaan ja vastuullista politiikkaa kyberturvallisuuden kontekstissa. Toimimalla strategisesti esitetyllä tavalla, voidaan mahdollistaa tietoisia, digitaalisesti aktiivisia ja osallistuvia yhteiskunnallisia toimijoita, jotka informoivat hallintoa kyberturvallisuuden heikkouksista. (National Cyber Security Strategy 2, 9-10,17.)

6.3.2 Alankonmaiden johtamismalli

Kyberturvallisuus kuuluu Alankomaissa Turvallisuus- ja oikeusministeriön (Ministerie van Veiligheid en Justitien) hallinnonalaan. Ministeriö vastaa kansallisen kyberturvallisuuden koordinoinnista sekä yhteensovittamisesta muiden toimijoiden kesken. Ministeriön alaisuudessa toimiva Kansallinen kriisikeskus (NCC) vastaa kriisitilanteiden päätöksenteon tukemisesta ja valmistelusta. Viestinnästä vastaaminen on annettu erilliselle toimijalle (NKC). Kyberturvallisuuden osalta ministeriön yhteyteen on perustettu erillinen Kyberturvallisuusneuvosto (CSR), jonka tehtävänä on ensisijaisesti neuvoa

kyberturvallisuuden toimeenpanoa strategisella tasolla. Sillä ei ole erityistä operatiivista roolia. Neuvoston kokoonpanoon kuuluu 18 jäsentä, joista 7 on hallinnon edustajia, 7 teollisuuden alojen edustajia ja 4 tieteellisen alojen edustajia (Cyber Rediness Index 2.0 2017, 9-10). Ylintä puhevaltaa käyttää kansallisen turvallisuus- ja vastaterrorismin koordinaattori. Päätöksentekoon osallistuu myös yksityisen sektorin edustaja (Lehto 2018, 54).

01.10.2017 voimaantulleesta Alankomaiden tietojenkäsittely- ja kyberturvallisusilmoitusvelvollisuuslaissa vahvistetaan kyberturvallisuuden tehtävät oikeus- ja turvallisuusministerille. Tehtävät koskevat elintärkeiden sähköisten tietojärjestelmien eheyden turvaamista, jotka ovat elintärkeitä Alankomaiden yhteiskunnalle sekä keskushallinnon tietojärjestelmille. Laki velvoittaa näitä hoitavia yrityksiä ja viranomaisia ilmoittamaan tietojärjestelmiin kohdistuvista uhkista. Muilta osin ilmoitusvelvollisuus on vapaaehtoista. Ministerille määritellyt tehtävät on kuitenkin ministeriön järjestelyasetuksella siirretty Kansallisen kyberturvallisuuskeskuksen (NCSC) vastuulle (Operational framework, 2018.) Kuviosta 9 selviää alankomaiden kansallisen kyberturvallisuuden johtamisen hierarkinen malli. Mallista on nähtävissä, että pääministerin johtaa hallintoa ja jokaiselle eri hallinnonalan ministeriölle on oma vastuualueensa kyberturvallisuuden johtamisessa. Äskettäin on myös perustettu erillinen Digital Trust Center, jonka tehtävänä on jakaa riippumatonta tietoa kyberturvallisuuskysymyksistä ja edistää kyberturvallisuutta yritysten välisissä yhteyksissä. Se on talous- ja ilmastoministeriön ylläpitämä yhdessä oikeus- ja turvallisuusministeriön kanssa.



Kuvio 9 Alankomaiden kansallinen kyberturvallisuuden johtaminen (mukaillen Cyber Rediness Index 2.0 2017,12).

Kansallinen kyberturvallisuuskeskus (NCSC) on Alankomaiden tietoverkkoturvallisuuden keskeinen osaamiskeskus. NCSC on osa tietoturvaosastoa (Cyber Security Department, DCS), joka taas on osa kansallista turvallisuus- ja terrorisminvastaisen toiminnan koordinaattoria (NCTV). Nämä kaikki toimivat oikeus- ja turvallisuusministeriön alaisuudessa (Operational framework, 2018, 1). Kansallisella tasolla NCSC :n keskeisenä tehtävänä on myötävaikuttaa yhteiskunnan kestävyyden parantamiseen digitaalialalla ja siten luoda turvallinen, avoin ja vakaa tietoyhteiskunta. Tämän toteutumisen kannalta on merkityksellistä, että kansallisella tasolla johtamisen lähtökohtana on toimintaympäristön ajantasainen tilannekuva. Ilman tilannekuvaa on mahdotonta ennakoida, tunnistaa ja torjua toimintaympäristön uhkia, joilla saattaa olla hyvinkin laajoja vaikutuksia kansallisiin palveluihin ja toimintoihin. Tilannekuvan tuottamiseen osallistuu Kyberturvallisuuskeskuksen lisäksi myös sotilas- ja siviilitiedustelu sekä turvallisuuspalvelu. Yhdessä nämä muodostavat signaalitiedustelun kyberyksikön (JSCU) (Lehto 2018, 53-54)

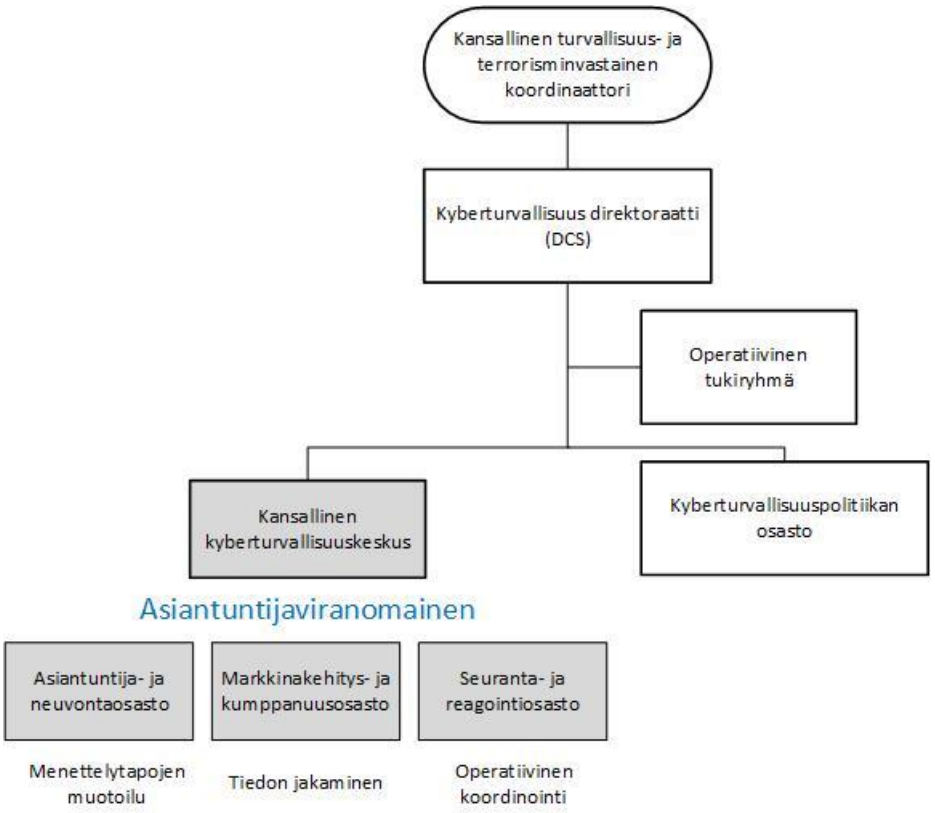
Kansallisella tasolla kyberturvallisuuskeskus tekee tiivistä yhteistyötä sekä hallituksen tasolla että yksityisten organisaatioiden kanssa. Kansallisen tason kumppaneita ovat muun muassa: Kansallinen poliisi, yleinen tiedustelupalvelu (AIVD), sotilastiedustellupalvelu (MIVD), hollantilainen tietoliikenneviranomainen (ACM), Alankomaiden radioviestintävirasto, erilaiset internetpalveluntarjoajat sekä elintärkeisiin toimintoihin liittyvät kansalliset järjestöt ja yksityiset yritykset (Operational framework, 2018).

Kyberturvallisuuskeskuksen roolin voidaan nähdä olevan kansallisella tasolla merkittävä. Yhteenvetona voidaan todeta, että kyberturvllisuuskeskus ylläpitää hallinnon sekä elintärkeiden sektoreiden verkostoja sekä osallistuu hyvin laajasti havainnointi,- tiedonjako- ja analyysikeskusten toimintaan sekä toimimalla Alankomaiden CERT – keskuksena, GovCERT –keskuksena sekä kansallisena turvallisuusoperaatiokeskuksena (NSOC) (Lehto 2018, 54).

Kyberrikosten tutkinnan hoitaa kansallinen poliisiviranomainen, jonka yhteyteen on perustettu erillinen kyberrikosyksikkö. Yksikön toiminta on osaltaan sidoksissa kyberturvallisuuskeskuksen toimintaan ja kansallinen oikeusjärjestelmän toiminnan varmistaa erillinen ohjauskomitea, jonka vastuulla on varmistaa, että selvitystyössä on käytettävissä riittävä ja ajantasainen asiantuntemus (Lehto 2018, 55).

Kansainvälisesti tarkasteltuna kyberturvallisuuskeskuksen tehtävänä on toimia eräänlaisena yhteyspisteenä Alankomaiden tietoverkkoturvallisuuden alalla. Keskeisiin tehtäviin kuuluu myös vastata operatiivisesta koordinoinnista kriisitilanteissa, joskin kriisinhallinta perustuu osittain julkisen ja yksityisen sektorin kumppanuuksiin. Tätä varten on perustettu erillinen neuvoa-antava komitea ICT Responce Board (IRB). Komitean tarkoituksena on analysoida meneillään olevaa kriisitilannetta ja antaa neuvoja kansallisen päätöksenteon tueksi. Tämän lisäksi kyberturvallisuuskeskus toimii Hollannin keskushallinnon CERT – tiimissä (NCSC 2019, 16-17.)

Kuviosta 10 on nähtävissä Alankomaiden kyberturvallisuuskeskuksen hierarkinen organisaatiokaavio. Kyberturvallisuuskeskus on osa kyberturvallisuusdirektoraattia, joka taas kuuluu kansallisen turvallisuus- ja terrorisminvastaisen koordinaattorin alaisuuteen. Näiden yläpuolella on turvallisuus ja oikeusministeriö, jonka hallinnonalaan toiminta sisältyy.



Kuvio 10 Alankomaiden kyberturvallisuuskeskuksen organisaatiokaavio (mukaillen Cyber Rediness Index 2.0 2017, 11).

Kun puhutaan digitaalisen toimintaympäristön puolustamisesta, ei tarkoiteta ainoastaan sotilaallista puolustusta, vaan myös laajaa yksityisen sektorin turvallisuuspalveluita sekä olemassa olevaa tietoa, kansallista kyberturvallisuuskeskusta, kansallista poliisia sekä muita toimijoita. Kyberturvallisuus ja sen puolustaminen vaikeasti hallittavassa toimintaympäristössä asettaa vaatimuksia hyville sopimuksille ja toimivalle yhteistyölle niin kansallisesti kuin kansainvälisestikin. Sotilaallinen kyberpuolustuksesta vastaa asevoimat, jonka tehtävät ohjaavat sen toimintaa myös digitaalisessa toimintaympäristössä. Sotilaallista toimintaa koordinoi puollustushaarojen yhteinen komentokeskus, jonka pääasiallisena tehtävänä on tiedottaminen puolustushallinnolle sekä tilannekuvan ylläpitäminen. Komentokeskusta voidaan pitää myös keskeisenä toimielimenä erilaisten kyberkykyjen ja sotilastiedustelun kehittämisessä. Sotilaallisia kykyjä voidaan

hyödyntää myös kansallisesti, mikäli kyseessä on uhka, joka kohdistuu elintärkeisiin yhteiskunnan toimintoihin tai palveluihin (Lehto 2018, 55).

6.3.3 Haasteet kansallisessa strategisessa johtamisessa ja tulevaisuuden kehitystyö

Alankomaiden kyberturvallisuusstrategia ja kansallinen johtamismalli nähdään innovatiivisena, turvallisuuteen, vapauteen ja sosio-ekonomisiin etuihin tähtäävänä yhteiskunnan eri toimijat yhdistävänä sekä kannustavana visiona miten kyberturvallisuutta tulisi johtaa kansallisesti ja kansainvälisesti. Puutteena strategiassa kuitenkin on se, etteivät Alankomaiden periaatteet kaiken yhdistävästä tasapainosta välity toimintasuunnitelmatasolle, jota tulisikin terävöittää seuraavia päämääriä määriteltäessä, jotta voidaan vahvistaa strategisten tavoitteiden ja toimeenpanosuunnitelman välistä yhteyttä. Tärkeää olisi, että kansalliset strategiset linjaukset kyettäisiin viemään riittävän selkeästi ja voimallisesti alemmille toimeenpaneville tahoille.

Tulevaisuuden kehitystyössä nähdään erityisesti kyberturvallisuuden kokonaisuuden kehittäminen tärkeäksi. Kokonaisuutta on tarkoitus parantaa erityisesti panostamalla hallinnon ja yksityisen sektorin välisen yhteistyön kehittämiseen. Kansallisella tasolla myös kyberturvallisuuden jalkauttaminen kaikkille opetusasteille koetaan tärkeänä, jolla voidaan saavuttaa parempaa resilienssiä tietoisuuden kasvaessa sekä kehittää omia innovatiivisia ratkaisuja asiantuntijoiden määrän kasvaessa. Opetusta tulisi myös tukea enemmän luomalla mahdollisuuksia esimerkiksi lopputöiden tekemiseen. Tätä varten on suunniteltu erillistä iskuryhmää, jonka tehtävänä olisi pääasiassa neuvojen antaminen (National Cyber Security Strategy 2, 9, 25-28) Vaikka Alankomaiden osalta on nähtävissä laaja-alaiseen yhteydenpitoon tähtäävä päämäärä, tulisi tulevaisuuden strategiatyössä panostaa entistä enemmän kaikkia toimijoita yhdistävään verkostotyön kehittämiseen. Keskeisenä tavoitteena tulisi olla koko yhteiskunnan kattava kyberturvallisuusverkosto, joka ideaali tilanteessa näkyisi kaikilla kyberturvallisuuden tasoilla. Tämän tyyppisellä verkostotyöllä voidaan saavuttaa yhteiskunnan eri toimijoiden keskuudessa kattavampaa kyberturvallisuusajattua (Lehto 2017, 52).

Vuonna 2017 laaditussa indeksissä painotetaan erityisesti tarvetta julkisten varojen kohdentamista ja kasvattamista kansallisen kyberturvallisuuden parantamiseksi. Rahoitusta määriteltäessä tulisi kokonaisuutta tarkastella erityisesti siltä pohjalta millaisia edellytyksiä ja tarpeita kyberturvallisuudella on tulevaisuudessa, jotta strategiassa määritellyt tavoitteet voidaan saavuttaa. Jotta kansainvälinen kyberturvallisuuden johtoasema voidaan saavuttaa tulisi Lehdon (2017, 53) mukaan käyttää kasvavan digitalisaation tuomat mahdollisuudet optimaalisesti hyväksi, panostaa voimakkaammin kansainvälisiin yhteistyöelimiin ja osallistumalla niiden tarjoamaan toimintaan sekä edistämällä yritysten ja tutkimusyhteisöjen asemaa kansallisissa ja kansainvälisissä verkostoissa. Alankomaiden tavoitteena on avoin ja turvallinen digitalisaatio, jossa hyödynnettäisiin sen tuomia mahdollisuuksia yhteiskunnan

taloudellisen aseman kehittämiseksi sekä kilpailukyvyn parantamiseksi. Alankomaat julkaisee tälläkin hetkellä vuosittain ilmestyvää kyberturvallisuusarviota, jonka tarkoituksena on mitata strategian ja toimeenpanon välistä tasoa sekä tuoda esille kybertilannekuva kuluneelta tarkastelujaksolta. Näiden pohjalta voidaan kehitystoimenpiteitä kohdistaa tarpeellisille alueille kansallisen kyberturvallisuuden parantamiseksi. Kansallisesti on olemassa kyberturvallisuusagenda, jossa muunmuassa edistetään tutkimusmaailman ja kyberturvallisuustarpeiden välistä yhteyttä kokonaisturvallisuuden kehittämiseksi. Tämän lisäksi tulisi tutkimuksilla ja kehitystyoiminnalla saavutettuja tuloksia saatttaa osaksi käytännön kyberturvallisuutta.

Kyberturvallisuuden vahvistamiseksi ja digitaalisen joustavuuden parantamiseksi tarvittaisiin monivaiheinen ohjelma, johon tulee sisällyttää myös investointiohjelma. Ohjelman tulisi laatia ensisijaisesti hallitus yhteistyössä yksityisten organisaatioiden ja paikallisten viranomaisten kanssa. Ohjelmassa tulisi huomioida erityisesti kysymykset, jotka liittyvät kansalliseen digitaaliseen turvallisuuteen sekä yksityisyyden suojaan. Saatavilla oleva tutkimusmateriaali ei kerro Alankomaiden valtuuksista tutkinta-, ja tiedustelupalveluiden osalta, mutta digitalisaation voimakas kehitys on osoittanut tarvetta uudistaa myös näitä kyvykkyyksiä, jotta kyetään vastaamaan niihin kyberuhkien haasteisiin, joita tänäpäivänä tekevät niin lapset, yksityiset toimijat kuin valtiotkin. Tämän ohjelman lisäksi tarvitaan sellaisia toimijoita, jotka kykenevät viemään strategiset linjaukset ja tavoitteet käytännön tasolle. Yhteiskunnan kyberturvallisuuden lisäämiseksi voitaisiin myös määrätä, että yhteisöt investoisivat vuosittaisista ICT–budjeteistaan 10 % kyberturvallisuuden kehittämiseen.

6.4 Israel

Israel nähdään maailman laajuisesti informaatioteknologian edellä kävijänä. Israelin valtio on yksi ensimmäisistä maista, jotka tunnustivat kriittisten tietojärjestelmien suojaamisen tärkeyden ja vuonna 2002 toteutettiinkin ensimmäinen kansallisen kyberavaruuden puolustuksen perusta kun hallinto nimitti tietoturvaviranomaisen (ISA) vastaamaan niiden laitosten óhjaamisesta, jotka käyttävät kriittisiä tietojärjestelmiä kansallisella tasolla. Israelin edelläkävijyys perustuu tutkimusten mukaan erityisesti teknologisten innovaatioiden kehitykseen ja tutkimustyöhön, joka Israelissa on hyvin korkealla tasolla. Israelissa otettiin käyttöön vuonna 1997 varhaisessa vaiheessa sähköisen hallinnon foorumi, joka palvelee niin valtion virastoja sekä luo kansalaisille mahdollisuuden asioida julkisissa palveluissa hyödyntäen sähköistä alustaa. Järjestelmä on sittemmin kehitetty nykyiseksi gov.il –portaaliksi, jota hallinnoi valtion tieto- ja viestintätekniikan viranomaiset. Vuonna 2009 tuli voimaan laki biometrisista tunnisteista ja lain puitteissa perustettiin hallintoviranomainen, joka valvoo tietokannan käyttöä virallisissa

henkilöllisyystodistuksissa. Biometrisiin tunnisteisiin asiakirjoissa siirryttiin kuitenkin vasta vuodesta 2013 lähtien, jolloin Israel pystyi tarjoamaan koko väestölle kehittyneitä digitaalisia palveluita sekä tehokkaan valokuituverkon. Israelin lainsäädännössä on huomattavia määriä erilaisia lakeja, jotka koskevat tietoturvallisuutta. Eri hallinnon sektoreiden ministeriöt ovat antaneet omia kyberturvallisuuteen ja riskienhallintaan liittyviä direktiivejä ja ohjeistuksia, mikä osaltaan on vaikuttanut Israelin hallinnon nopeampaan reagointiin kansallisen tason lakien säätämisessä (Housen-Couriel 2017, 5-12).

Israelin innovaatio järjestelmä nähdään tutkimusten mukaan yhtenä kehittyneimmistä. Tieteellisistä tutkimusta tekevissä yliopistoissa, on jokaisella oma teknologiansiirtoyhtiö, jonka tehtävänä on suojella ja aktiivisesti pyrkiä kaupallistamaan tieteellisiä innovaatioita. Neljä yliopistoa kuuluu TOP50 yliopistoihin maailmassa joissa on edistyksellinen tietotekniikan osasto. (Tabansky 2016, 56-57)

6.4.1 Kyberturvallisuusstrategia ja strateginen johtaminen

Israelin kyberturvallisuusstrategiassa kuvataan selkeästi visio, jonka mukaan Israel haluaa olla johtava kansakunta, joka hyödyntää kyberavaruutta taloudellisen kasvun, sosiaalisen kasvun sekä kansallisen turvallisuuden kehityksen moottorina. Strategian rooli nähdään erityisesti tavoitteena vahvistaa kansallista turvallisuutta, vahvistaa kansainvälistä yhteistyötä sekä olla mukana kehittämässä innovaatioita, joiden avulla voidaan kehittää kyberavaruutta. Kuten Lehto (2018, 57) on tutkimuksessaan todennut, on Israelin asema hyvin poikkeuksellinen muihin tarkasteltuihin valtioihin verrattuna. Israel kokee alati olevansa sodassa ja hyökkäyksen kohteena. Tämä erilainen asetelma on on otettu huomioon jo stregisia tavoitteita mietittäessä. Israelin kyberturvallisuusstrategia perustuu yleiseen käsitteelliseen runkoon kyberturvallisuuden toimenpiteistä. Runko perustuu kolmeen kerrokseen ja eroavat toisistaan tavoitteiden suhteen. Ensimmäinen kerros määrittelee erityisesti yksityisen sektorin osalta toimintatavat kriittisten järjestelmien osalta, standardit sektoreille, jotka toimivat yhteiskunnan kannalta aloilla, joissa kyberturvallisuus on erityisen tärkeää sekä vahvistaa yleistä ymmärrystä kyberturvallisuudesta yksityisellä sektorilla. Toinen kerros tähtää niihin toimiin, joilla pyritään ennakoimaan, havaitsemaan, kestämään ja toipumaan (palautumaan) kybertoimintaympäristöön kohdistuvista uhkista. Tässä erityisen tärkeää on kansallisella tasolla varmistaa oikea-aikainen, oikea sisältöinen ja riittävän laajuinen tiedonkulku niin hallinnon sektoreilla kuin yksityisten toimijoidenkin osalta. Kolmas kerros käsittää kansallisen tason kyberpuolustuksen uhkia vastaan, jotka vaikuttavat kansallisten kriittisten järjestelmien toimintaan. Strategia painottaa kansallisen ja kansainvälisen yhteistyön merkityksen tärkeyttä, uusien innovaatioiden kehittämistä ja tavoitteellisesti pyritään kehittämään yhteiskunnan kykyä vastata kyberavaruuden uhkia vastaan. Tähän pyritään erityisesti kahden tavoitteen voimin, tutkimalla, kehittämällä ja ottamalla käyttöön toimintatapoja ja

teknologioita, joilla pyritään luomaan turvallisempi kansallisen tason toimintaympäristö sekä tukemalla ja vahvistamalla kansallista tieteellistä tutkimusta ja koulutusta sekä luomalla näiden välille verkoston, jonka tarkoituksena on tukea kansallisella tasolla niin yksityisiä ihmisiä, yrityksiä kuin valtiollisia toimijoita kyberturvallisuuden alalla. Strategian kolmanteen kerrokseen liittyi vahvasti yhteistyön merkitys. Koska kyberturvallisuus nähdään maan rajat ylittävänä ilmiönä, se luo maailmanlaajuisia haasteita. Israelin kyberstrategiassa korostetaan kansainvälisen yhteistyön merkitystä ja Israel onkin sitoutunut auttamaan kumppanimaita vahvistamaan omaa kansallista kyberturvallisuuttaan (Israel National Cyber Security Strategy 2017, 5-16)

6.4.2 Israelin johtamismalli

Israelin hallituksen päätöslauselma 3611, joka annettiin 7.8.2011 – Kansallisen kapasiteetin edistäminen kyberavaruudessa – on ensimmäinen Israelin kansallinen kyberstrategia. Tämän johdosta pääministerin toimiston alaisuuteenvon on perustettu toimisto Israel National Cyber Bureau (INCB), jonka toimivalta on toimia pääministerin, ministeriöiden sekä muiden hallinnon yksiköiden neuvoa-antavana virastona sekä lujittaa siviilikyberturvallisuutta kansallisella tasolla (Tabansky 2016, 59 ; Housen-Couriel 2017, 11). Tuolloin ei vielä ollut erillistä toimijaa, joka hoitaisi kansallisella tasolla kansalaisten ja yksityisten tajojen kyberturvallisuutta. Piakkoin kuitenkin perustettiin National Cyber Security Author (NCSA), jonka tehtävänä on vastata kyberavaruuden puolustamisesta. NCSA toiminta keskittyi aluksi lähinnä tiedottamiseen, mutta myöhemmin tarjosi kyberuhkien käsittelyyn palveluja sekä osaltaan pyrki edistämään talouden kriittisen infrastruktuurin kestävyyttä. NCSA on vastuussa Israel National Cyber Event Readliness Teamin (CERT-IL) toiminnasta, joka perustettiin 2016 ja on kansallinen yhteyspiste tietoverkkoturvallisuustapahtumia varten. CERT-IL on osaltaan vastuussa kansalliseen kyberturvallisuuteen liittyvien tapahtumien hallinnasta sekä tietojen jakamisesta kansallisten ja kansainvälisten kumppaneiden kesken. Fyysisesti CERT-IL sijaitsee ICT-alan keskittymässä, jossa sijaitsee muun muassa yliopisto, tutkimuslaitoksia, julkishallinnon virastoja sekä yksityisiä ICT-alan yrityksiä (Lehto 2018, 57). Vuoden 2017 lopulla Israelin hallitus päätti yhdistää NCSA :n toiseen yksikköön, Israelin kansalliseen kybertoimistoon, jonka johdosta syntyi yksi yksikkö, National Cyber Directorate (INCD) (Israel National Cyber Directorate.) Kansallinen kyberdirektoraatti vastaa erityisesti tietoverkkotapahtumista siviilialalla sekä teknologisen voiman rakentamisesta operatiivisen puolustuksen käyttöön kansallisen tason kyberturvallisuudessa (Israel National Cyber Directorate 2018 ; Housen-Couriel 2017, 12).

Kansallinen tietoturvavirasto (NISA) perustettiin toimeenpanemaan säännöksiä, jotka kirjoitettiin lakiin, joka käsittelee yleisen turvallisuuden sääntelyä. Säännökset koskevat kriittisten tietojärjestelmien riittävän suojan ja valvonnan tasoa ja NISAn tehtävä onkin laatia erilaisia kyberturvallisuus

tavoitteita sekä kehittää menetelmiä niiden toteuttamiseksi sekä valvoa niiden toimeenpanoa. NISAlla on oma erillinen valvontakomitea (Housen-Couriel 2017, 13).

Ministeriö on nimittänyt erillisen kyberturvallisuuskoordinaattorin vastaamaan kansainvälisen yhteistyön kehittämisestä (Lehto 2018, 57). Israelin siviilikriisinhallinta ja hätätilanteisiin varautuminen on annettu puolustusministeriön (Ministry of Defence), yleisen turvallisuuden ministeriön (Ministry of Public Security) sekä kotitalouksien edunvalvotaviraston (Home Front Command) vastuulle ja Kansallinen hätätilavalvonta viranomainen (National Emergency Management Authority) järjestää säännöllisesti harjoituksia, joissa harjoitellaan hyökkäyksiä kriittiseen infrastruktuuriin valmiustason korkean tason ylläpitämiseksi. Israelin puolustusvoimat on liittänyt kyberpuolustuksen kiinteäksi osaksi muuta puolustusstrategiaa niin strategisella, operatiivisella kuin taktisellakin sektorilla ja strategian voidaan nähdä toimivan niin fyysisessä kuin digitaalisessakin toimintaympäristössä. Israelin sotilashallinto vastaa myös tiedustelutoiminnasta sekä tietoverkkotiedon keräämisestä ja käsittelystä. Israelin puolustushallinnolla on useita sotilaallisia digitaalisen puolustuksen harjoitteluohjelmia kansallisen kyberturvallisuuden osalta. (Housen-Couriel 2017, 14) Israel on osallistunut kansainvälisellä tasolla kyberturvallisuuden eri maiden edustajista koostuviin asiantuntijaryhmiin sekä solminut kahdenvälisiä yhteistyösuhteita kyberturvallisuuden ja yhteistyön edistämiseksi (Housen-Couriel 2017, 10).

6.4.3 Haasteet ja tulevasisuuden kehitystyö

Kyberturvallisuuden toimintaympäristön nopeat muutokset ja kehittyneet ominaisuudet haastavat nykyisiä kansallisia rakenteita, jotka ovat rakennettu vaikkakin vaan muutamia vuosia sitten tiedossa olevien uhkien torjumiseksi. Tämän johdosta myös Israelissa on käyty keskustelua uuden kansallisen kyberturvallisuusviranomaisen (CCA) perustamisesta. Perustettava viranomainen olisi erityinen siviilikokonaisuus, jolla olisi konkreettisia operatiivisia valmiuksia ja joka olisi vastuussa kansallisen kyberavaruuden puolustamisesta (Matania & Yoffe & Goldstein 2017.) Israelin hallitus on pitkään suunnitellut uudistavansa kyberturvallisuuslainsäädäntönsä vastaamaan nykyajan kyberturvallisuuden haasteisiin. Lakia on valmisteltu pitkään ja valmisteluissa on huomioitu myös strategisesti tärkeä yhteistyön merkitys. Ennen luonnoksen laatimista yksityisiltä toimijoilta on kysytty mielipidettä lakiin kirjoitettavista kohdista yhteistyössä hallituksen toimijoiden kanssa. Ehdotetussa laissa muun muuassa halutaan vahvistaa edelleen NCD :n asemaa Israelin johtavana kyberviranomaisena. Laissa halutaan lisätä valvontavaltuuksia suhteessa muihin valtion sääntelyviranomaisiin nähden. NCD :n katsotaan jopa mahdolliseksi antaa kansallisia ohjeita kyberturvallisuuteen liittyvissä asioissa muiden viranomaisten laajuudessa. Tällaisia voivat olla esimerkiksi rahoitus, liikenne, energia sekä viestintä. Valmisteilla olevasta lainsäädännöstä voidaan löytää kaksi erityistä periaatetta,

jotka on määritelty. Toisen mukaan on suuri tarve kehittää uusia lähestymistapoja kyberturvallisuuteen ja sen puitteissa tulee käynnistää uusia yhteistyömuotoja hallituksen ja yksityisen sektorin toimijoiden välillä sekä lisätä kansallisia voimavaroja tehostaakseen kyberuhkien ennaltaehkäisyä ja lieventää niitä seuraavia kybertapahtumia. Lain puitteissa on tarkoitus myös perustaa uusi valvontaviranomainen, joka keskittyisi varhaisvaroitusten ja hyökkäysvaikutusten vähentämisen havaitsemis- ja todentamiskeskus. Uusi viranomainen käytännössä luo tietokantaa niistä kansallisista indikaattoreista, jotka voivat aiheuttaa uhkaa kansalliselle kyberturvallisuudelle (Housen-Couriel 2018.) Erityisen tärkeänä on tulevaisuuden strategista johtamista ajatellen pidettävä, että valmisteilla olevassa lainsäädännössä eriytetään selkeästi yksityisen sektorin toimijat ja heidän vastuunsa sekä sotilaalliset toimijat ja –tehtävät. Huomioon otettavaa olisi myös selkeästi määritellä, missä kohdassa ykstyisten toimijoiden toimivalta loppuu ja sotilaspuolustuksen alkaa. IDF :n tehtäviä puolustaa kyberavaruutta ja erityisesti toimivaltaa sodan aikana olisi säänneltävä sekä kansallisten muiden viranomaisten, kuten poliisin, salaisen palvelun ja armeijan väliset rajapinnat tulisi määritellä nykyistä paremmin. Kyberturvallisuuskomitea on ehdottanut, että IDF :n pääasiallisena tehtävänä olisi johtaa kyberturvallisuutta sodassa, joka on ristiriidassa nykyisen todellisuuden kanssa. Kansallisen kyberturvallisuuden tilan muuttuessa rutiinista hätätilaan, ei ole pystytty riittävän tehokkaasti ottamaan vastuuta tehtävästä (Even & Siman-Tov & Siboni 2016, 3).

Investointien osalta tulisi määritellä käytettävissä olevat henkilöstöresurssit ja resursseihin tehtävät investoinnit sekä huomioida teknologisten välineiden ja menetelmien kehittäminen koko prosessissa niin, että ne tulisivat integroiduksi osaksi kansallisia resursseja yhteiskunnan kyberturvallisuuden vahvistamiseksi. Israelin valtion käytössä olevien teknisten- ja henkilöstöresurssien tulisi olla määritelty niin, että ne tukisivat kyberturvallisuuden kansallisia päämääriä ja tavoitteita. Kansallisessa kyberturvallisuudessa tulisi huomioida myös investointien tarpeellisuus uuteen teknologiaan sekä asiantuntijoiden koulutukseen (Siboni & Assaf 2016, 23-26).

7 AINEISTOTUTKIMUKSEN ANALYYSI VERTAILUMAISTA

Tutkimuksessa määriteltiin tavoitetila, jonka mukaan vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaa kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti (Lehto 2017, 2). Aineistotutkimuksessa pyrittiin selvittämään, miten kyberturvallisuuden johtaminen on toteutettu tarkastelun kohteena olevissa Virossa, Israelissa ja Alankomaissa.

Lehdon (2018, 64) mukaan strategisen johtamisen keskiössä voidaan kansainvälisen referenssiarvioinnin perusteella tunnistaa ainakin kyberuhkien ja toimintaympäristön ennakointi ja aikainen havainnointi, uhkien torjuminen ennakoivasti, uhkatilanteisiin vastaaminen, sekä yhteiskunnan sietokyvyn parantaminen. Aineistotutkimuksessa tarkastelluissa valtioissa **kyberturvallisuutta tuotetaan kokonaisvaltaisesti, kansainvälisistä kumppanuuksista yksityisiin kansalaisiin**. Kyberturvallisuuden johtaminen on tarkastelluissa valtioissa organisoitua, Virossa hajautettua, Alankomaissa hajautettua mutta keskitetysti johdettua ja Israelissa keskitettyä. Organisaatiorakenteet ovat lyhyessä ajassa muuttuneet voimakkaasti ja muuttuvat edelleen, mutta havaittavissa on suuntaus, jossa pyritään **yksinkertaistamaan organisaatiorakennetta keskittämällä tärkeitä toimintoja ja karsimalla sellaisia organisaatioita, joiden toimintaa voidaan yhdistää**. Kyberturvallisuuden johtaminen kuuluu valtion ylimmän johdon vastuulle. Vertailumaissa johtaminen tapahtuu pääsääntöisesti ministeriöiden toimesta, Alankomaissa ja Israelissa pääministeri vastaa johtamisesta, Virossa ylin johtaminen on kansallisen kyberturvallisuuden valiokunnan vastuulla. Tarkemmin tarkasteltuna kyberturvallisuuden koordinointi ja yhteensovittaminen kuuluu Alankomaissa Turvallisuus- ja oikeusministeriön vastuulle, Virossa Talous- ja viestintäministeriölle ja Israelissa kyberdirektoraatille, joka toimii pääministerin toimiston alaisuudessa. Tarkastelluissa valtioissa yhteiskunnan palvelut, erityisesti kriittisen infrastruktuurin palvelut ovat siirtyneet digitalisaation toimesta sähköiseen muotoon. Tästä syystä **kyberturvallisuuden johtamisessa korostuu erityisesti yhteiskunnan kokonaisturvallisuuden varmistaminen kybertoimintaympäristössä**. Kyberuhkiin varaudutaan yhdessä,

yhteistyössä kansainvälisten kumppaneiden kanssa sekä kansallisesti julkis-siviiliyhteistyötä korostaen. Tiedonvaihto eri toimijoiden välillä koetaan tärkeäksi ja kyberympäristössä tapahtuvaa kansallista ja kansainvälistä harjoittelutoimintaa tehdään yhdessä. Asevoimien osallisuus johtamiseen vaihtelee, (Israelissa asevoimat on vahvimmin mukana) mutta vastuu kyberpuolustuksesta kuuluu puolustusvoimille. Laadittujen strategioiden siirtymistä operatiiviselle tasolle seurataan vuosittaisen raportoinnin avulla, jonka perusteella kyberturvallisuutta kehitetään. **Kybertietoisuutta pyritään lisäämään yhdessä yhteiskunnan kaikilla tasoilla**, sekä kehittämällä kyberturvallisuuden opetusta koulutusasteissa ja tukemalla tulevia ammattilaisia opinnoissaan. Tutkimusmateriaalin perusteella on nähtävissä, että tarkastellut valtiot ovat samoilla linjoilla siitä, että tulevaisuuden suurina **haasteina nähdään johtamisen kannalta kyberympäristön nopea kasvu, joka luo mittavia haasteita kyberuhkien ja häiriöiden tunnistamisessa**. Toiseksi kansallisen viestinnän kehittäminen eri toimijoiden välillä sekä kansainvälinen yhteistyö eri toimijoiden kesken nähdään tulevaisuuden strategisina tavoitteina (mukaillen Lehto 2018, 60-64).

Materiaali tuo esille selkeästi ongelman kyberturvallisuuden toimijoiden keskinäisen yhteistyön ja erityisesti vastuun osalta, ja välillä toimintaympäristö näyttäytyy hyvinkin sekavana kokonaisuutena. Erityisesti Virossa on pyritty vaikuttamaan yhteistyön tehostamiseen integroimalla sotilas- ja siviiliresursseja viranomaisten toimintaan sekä varmistamaan riittävät kyvykkyydet lisäämällä investointeja teknologiaan, jolla voidaan tunnistaa ja havainnoida riskejä. Vertailumaiden kansallisen kyberturvallisuuden johtamisessa on mukana niin hallinnollisia kuin siviilitoimijoita ja ongelmat viestinnässä ja vastuunottamisessa näyttäytyvät sitoutumisen puutteena, ongelmina tunnistaa kenen vastuulla asian hoitaminen on sekä kyvyttömyytenä koordinoida ja jakaa vastuuta oikeille toimijoille. Hyvää sektorikohtaisessa johtamisessa olisi, että eri hallinnonalat tuntevat oman toimialansa parhaiten ja kykenevät näin tunnistamaan ja havainnoimaan uhat ja häiriöt sekä toimimaan niiden edellyttämällä tavalla, mikä auttaa yhteistyössä onnistumista.

Kokonaisvaltainen toiminnan koordinointi edellyttää riittäviä toimivaltuuksia sekä toiminnan kehittäminen riittäviä resursseja ja investointeja. Nämäkin asiat olivat tunnistettu tarkasteltavissa valtioissa. Kyberturvallisuuskeskukset ovat olleet keskeisessä asemassa kansallisen kyberturvallisuuden rakentamisessa. Keskuksen rooliin ja hallinnolliseen sijoittamiseen osana kansallista kokonaisuutta, käytettävissä oleviin resursseihin sekä valtuuksiin voidaan löytää erilaisia ratkaisuja. Tarkastelluissa valtioissa oli omat keskuksensa, joiden rooli oli hyvin pitkälti vastata tietoliikenneverkoissa tapahtuvien tapahtuminen käsittelystä sekä toimia valtion virastojen ja yksityisen sektorin välisenä yhteistyövirastona sekä edistää kyberturvallisuuden tuntemusta yhteiskunnassa (Lehto 2018, 64). Kansainvälisesti tarkastelluissa valtioissa keskukset ovat hallinnollisesti sijoittuneet ministeriön alaisuuteen, Virossa Talous- ja viestintäministeriön, Alankomaissa Turvallisuus- ja oikeusministeriö sekä Israelissa pääministerin toimisto. Kaikissa kyberturvallisuuskeskuksissa on oma CERT – palvelunsa.

Lehto (2018, 64) tutkimuksessa mainitaan kehitettäväksi kohteeksi kolmannen sektorin ja yritysten tuominen mukaan strategisen kyberturvallisuuden suunnitteluun, toteuttamiseen sekä johtamiseen. Israelissa on edetty tähän suuntaan tarkoituksena lähitulevaisuudessa perustaa kansallinen kyberturvallisuusviranomainen (CCA), joka olisi erityinen siviilikokonaisuus. Tämän lisäksi uuden lainsäädännön valmistelutyöhön on otettu mukaan yksityisiä toimijoita. Alankomaiden tulevassa strategiassa on myös nähtävissä laaja-alaiseen yhteydenpitoon tähtäävä päämäärä. Päämäärään pyrkiessä on kuitenkin kiinnitettävä huomiota riittävän vahvaan toimeenpanosuunnitelmaan, jotta päämäärät voidaan saattaa koko yhteiskunnan kattavaksi kyberturvallisuusverkostoksi. Virossa suunnitelmat ovat samansuuntaisia yksityisen sektorin toimijoiden ja valtion hallinnon tiiviimmän yhteistyön osalta. Näillä toimilla voitaisiin saavuttaa kokonaisvaltaisempaa kyberturvallisuuden hallintaa ja varautumista. Tiiviimpi yhteiskunnallinen yhteydenpito lisäisi tilannetiedon nopeampaa saavutettavuutta toimijoiden keskuudessa, mikä parantaisi merkittävästi kyberavaruuden häiriöiden ennakointia. Tarkastelluissa valtioissa digitalisaatio on kehittynyt voimakkaasti suhteellisen lyhyessä ajassa. Kehitystä on seurannut sähköisten palveluiden tuleminen osaksi yhteiskunnan toimintoja. Kansallisen tason kyberturvallisuutta rakennetaan paikoin hyvinkin hitaasti. Valtionhallinnon päätöksenteko on hidasta ja päätösten vieminen toimeenpanoon monesti vie paljon aikaa. Kyberturvallisuuden kehitys ei monesti ehdi vastata digitalisaation mukanaan tuomiin vaatimuksiin, joka vaikuttaa kybertoimintaympäristön suojaamisen heikentymiseen. Tulevaisuuden kannalta olisikin merkittävää pyrkiä arvioimaan digitalisaation mahdollisuuksia ja riskejä osana kansallisen tason strategisen kyberturvallisuuden suunnittelua.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa esitetään yhteenvetona tutkimuksen tulokset. Lopuksi esitetään tutkimukselle mahdollisia aiheita jatkotutkimusta varten.

8.1 Tulosten pohdinta

Tutkimuksessa kartoitettiin kirjallisuuskatsauksen menetelmin kyberturvallisuuden johtamista Virossa, Israelissa ja Alankomaissa. Tutkimuksella pyrittiin lisäksi selvittämään voidaanko tulosten perusteella löytää sellaisia strategisen johtamisen tekijöitä, joita edelleen voidaan jalostaa kansallisen strategisen kyberturvallisuuden kehittämisajatuksiksi.

Tutkimuksessa kävi ilmi, että kyberturvallisuuden toimintakenttä on keskeinen osa yhteiskunnan turvallisuutta. Digitalisaation voimakas kehittyminen ja sähköisten palveluiden juurtuminen osaksi yhteiskunnan palveluja kasvattavat entisestään kyberturvallisuuden merkitystä. Toimintaympäristössä vaikuttaville uhkille ja häiriötilanteille on ominaista suuri muutosnopeus ja ennakoimisen vaikeus, jonka johdosta kansalliselta turvallisuudelta vaaditaan yhä tehokkaampaa strategista ja opertatiivista johtamista ja prosessien hallintaa. Johtamisessa tulee nähdä kokonaiskuva yhteiskunnan turvaamisesta sekä siihen käytettävistä menetelmistä, joita tulee kehittää nopeasti muuttuvan toimintaympäristön mukaan. Kyberturvallisuuden johtaminen on osa kokonaisturvallisuuden johtamista, jossa huomiota tulee kiinnittää erityisesti yhteistyöhön niin kansainvälisellä kuin kansallisella tasolla. Yhteistyössä korostuu kansainväliset kumppanuudet sekä kansallisella tasolla yksityiset toimijat, joiden osaaminen ja asiantuntijuus ovat erityisessä asemassa uhkien torjunnassa ja niihin varautumisessa. Jotta strategiset tavoitteet voidaan saavuttaa on yhteiskunnan toimijat voitava osallistaa yhteiseen päätöksentekoon yhä tiiviimmin. Yhteiskunnan turvaamisessa on kysymys kyberkyvykkyyksien kehittämisestä. Tutkimuksen perusteella tämä edellyttää riittäviä resursseja, vahvaa osaamista, tehtävien ja

vastuiden yhteensovittamista sekä kykyä toimeenpanna strategisia tavoitteita. Koska yhteiskunnan toimintaa ohjaa erilaiset lait ja säädökset, tulee kyberturvallisuutta, sen toimijoita ja toimivaltuuksia koskeva lainsäädäntö olla ajantasainen, mikä nousi tutkimuksessa keskeiseksi asiaksi. Tutkimuksen mukaan tilannetietoisuus nousee yhdeksi tärkeimmistä kansallisen kyberturvallisuuden johtamiseen vaikuttavista tekijöistä. Toimintaympäristön nopeat muutokset vaativat nopeaa reagointia, ja ilman ajantasaista tietoa vallitsevasta tilanteesta, ei kyetä tekemään oikeaita päätöksiä. Tämä edellyttää toimijoilta strategista ketteryyttä. Strategiseen ketteryyteen vaikuttaa johdon yhtenäisyys ja osaaminen sekä toimijoiden välinen yhteistoiminta.

Tutkimus osoittaa, että valtioiden strategisessa johtamisessa korostuu kyberturvallisuuden johtamisen tuottaminen kokonaisvaltaisesti, organisaatiorakenteiden yksinkertaistaminen sekä kansalaisten ja siviilitoimijoiden osallistaminen strategisten tavoitteiden ja päämäärien suunnitteluun. Tätä tukee myös Lehdon (2018, 81-82) tutkimus kyberturvallisuuden strategisesta johtamisesta.

Onnistuneen kyberturvallisuuden strategisen johtamisen edellytys on tunnistaa toimintaympäristössä vaikuttavia häiriötekijöitä ja tulevaisuuteen tähtäävien ennusteiden tekemistä sekä kyetä tunnistamaan ja asettamaan tavoitteita, joilla näihin tekijöihin voidaan vastata. Selkeä strateginen visio vastuineen ja vision toimeenpanon turvaaminen on edellytys kyberturvallisuuden strategiselle johtamiselle. Toimeenpanon onnistuminen vaatii lisäksi poikkihallinnollista viestintää toimijoiden kesken sekä toimeenpanon seurantaa ja säännöllistä raportointia. Kyberturvallisuuden johtamiseen kuuluu myös kansallisen kybertietoisuuden lisääminen sekä erityisen identiteetin luominen ja vahvistaminen yhteiskunnan sisällä ja kansainvälisesti (Lehto 2018, 82).

Strategisen johtamisen yksi tarkoitus on ohjata valtion ylintä johtoa määrittämään toiminnan tarkoituksen ja keinot, joilla voidaan menestyä muuttuvassa toimintaympäristössä. Strategiat saavat alkunsa politiikasta. Koska kyberturvallisuuden johtaminen kansallisella tasolla on valtion ylimmän johdon vastuulla, siihen vaikuttavat sen hetkiset poliittiset päätökset. Nämä päätökset määrittävät miten kyberturvallisuutta toteutetaan kansallisella tasolla. Tutkimuksen tuloksissa korostuu yksityisen sektorin merkitys kansallista kyberturvallisuutta rakennettaessa. Yksityisellä sektorilla on merkittävä määrä osaamista ja vastuuta kriittisestä infrastruktuurista. Yksityisen sektorin ja valtion hallinnon välillä on nähtävissä vahvoja siteitä, jotka perustuvat vahvaan luottamukseen. Yhteistyötä vahvistavat yhteiset tavoitteet ja päämäärät sekä erilaiset kybertoimintaharjoitukset ja koalitiot. Yhteistyön vahvistaminen ja ylläpitäminen ovat onnistuneen strategisen johtamisen tavoite. Kuten aikaisemmissa luvuissa on todettu, johtamisen vastuiden tulisi olla selkeitä ja tunnistettavia niin normaalitilanteessa kuin vakavien häiriötilanteidenkin aikana. Tutkimuksen analyysi osoitti, että koulutus ja harjoitustoimintaa tarvitaan, jotta tavoitteiden mukainen toiminta on tehokasta ja määrätietoista.

Koulutus mahdollistaa ajantasaisen tiedon vaikuttavista tekijöistä ja harjoitustoiminta mahdollistaa paremman reagoimisen poikkeustilanteisiin.

8.2 Kehitysideoita kansallisen kyberturvallisuuden johtamiseen

Tutkimusongelmassa esitettiin tutkimuskysymys, jossa pyrittiin selvittämään, voidaanko tutkimuksen perusteella löytää kehittämisajatuksia, joita jalostamalla Suomen kansallista kyberturvallisuuden johtamista voisi kehittää. Tässä luvussa on tarkoitus nostaa esille tutkimuksessa esiin tulleita strategisen kyberturvallisuuden johtamisen toimintatapoja tai käytänteitä, sisällyttäen ne Suomen kyberturvallisuuden johtamismalliin. Luvun teksti nojaa tutkimusmateriaalin lisäksi vahvasti (Lehto 2018) tutkimukseen kyberturvallisuuden strategisesta johtamisesta ja erityisesti alalukuun 6.2 jossa käsitellään kyberturvallisuuden strategisen johtamisen malleja.

Suomen yhteiskunnan turvallisuusstrategian (2017, 7) mukaan "kokonaisturvallisuus on Suomalaisen varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä."

Kuten muissakin tutkimuksessa esiintyneissä valtiossa, myös Suomessa kyberturvallisuus on yhteiskunnan turvallisuuden kannalta keskeinen. Suomen kyberturvallisuusstrategia määrittelee keskeisiksi turvattaviksi kohteiksi ”Valtion johtamisen, kansainvälisen toiminnan, Suomen puolustuskyvyn, sisäisen turvallisuuden, talouden ja infrastruktuurin toimivuuden, väestön toimeentulon sekä henkisen kriisinkestävyyden” (Suomen kyberturvallisuusstrategia 2013, 2). Kuten aikaisemmin on esitetty, Suomessa kyberturvallisuuden ylimmän tason muodostaa valtioneuvosta, joka päättää poliittiset ja strategisen tason linjaukset sekä voimavarat. Ministeriöt päättävät oman hallinnonalansa kyberturvallisuudesta yhdessä yksityisen sektorin toimijoiden kanssa tehtyjen sopimusten mukaisesti. Valtioneuvosto määrittelee vuosittain budjetit ministeriöille, mutta budjettien ulkopuolisia resursseja ei kyberturvallisuuden kehittämiseen suunnata. Turvallisuuskomitea toimii Valtioneuvoston ja ministeriöiden tukena sekä koordinoi kokonaisturvallisuuden tuottamista. Tämän lisäksi se vastaa yhteiskunnan turvallisuusstrategiasta sekä valtion hallinnon kybervarautumisen yhteensovittamisesta. Häiriötilanteiden hallinta ja vastuu viestinnästä kuuluu asianomaiselle ministeriölle. Tarvittaessa koolle voidaan kutsua myös valmiuspäällikkökokous sekä vahventaa valtioneuvoston tilannekeskuksen toimintaa saatavan tilannetiedon varmistamiseksi. Kyberturvallisuuden tuottamiseen osallistuvat viranomaiset ja yksityiset toimijat säilyttävät normaaliolojen tehtävät poikkeustilanteesta riippumatta, joskin jokaisen toimintaa tullaan tehostamaan (Lehto 2018, 84-85).

Edellä on kuvattu Suomen kansallisen kyberturvallisuuden nykytila strategisen johtamisen osalta. Seuraavaksi on lueteltu kohtia, joita voidaan tutkimuksen tulosten analysoinnin sekä Lehdon (2018, 84-86) tutkimuksen perusteella jatkojalostaa kansallisen kyberturvallisuuden kehittämiseksi.

1. Kansallisen kyberturvallisuuden johtamista tulisi selkeyttää erityisesti vastuiden ja tehtävien osalta. Kyberturvallisuuden strategisesta johtamisesta vastaa yksi virkamies, kyberturvallisuusjohtaja, jonka vastuulle kuuluisi kyberturvallisuuden koordinointi ministeriöiden välillä. Tapahtumiin reagoitaisiin edelleen hallinnonaloittain, mutta kyberturvallisuusjohtajalla olisi tilanneymmärrys toiminnasta. Malli muuttaisi nykyistä johtamisrakennetta sekä vaatisi nykylainsäädäntöön muutoksia tehtävien ja vastuiden suhteen.
2. Nykyisiä organisaatiorakenteita tulisi yksinkertaistaa nopeamman päätöksenteon ja tiedonkulun saavuttamiseksi. Keskitetään tärkeitä toimintoja ja lopetetaan sellaisia organisaatioita, joiden toimintoja voidaan yhdistää muihin.
3. Kyberturvallisuudelle olisi määriteltävä riittävät resurssit sekä varata lisärahoitus esimerkiksi laajamittaisten häiriötilanteiden hoitamiseen.
4. Strategisen päätöksenteon tueksi tulee perustaa erillinen virasto, jonka vastuulla on kerätä tilannetietoa, analysoida kerättyä tietoa sekä tuottaa laajempaa tilanneymmärrystä. Keskus toimisi suoraan valtioneuvoston alaisuudessa.
5. Lisätään nykyisen kyberturvallisuuskeskuksen toimivaltuuksia. Keskus tekisi tiivistä yhteistyötä strategisen tason päättäjien kanssa sekä tukisi strategista johtamista poikkihallinnollisesti. Tärkein lisä olisi tuottaa analysoitua strategista tilannetietoa laaja-alaisemman tilannekuvan saamiseksi.
6. Kyberturvallisuuden strategisen johtamisen suunnitteluun tulisi osallistaa enemmän yksityisen sektorin toimijoita sekä yksittäisiä kansalaisia, joka mahdollista laaja-alaisempaa kyberturvallisuuden kentän huomioimista.
7. Kyberturvallisuuden tietoutta tulisi lisätä koko yhteiskunnassa. Perustetaan kansallisia sekä globaaleja yhteisöjä yksityisille toimijoille, joissa voidaan luoda uusia innovaatioita ja keskustella ajankohtaisista asioista.
8. Järjestetään kansalaisille kyberturvallisuuteen liittyviä yhteisiä harjoituksia, joka lisäisi osaamista sekä kansalaisten varautumista kyberuhkien torjunnassa.
9. Lisätään kyberturvallisuuden koulutusta, erityisesti peruskoulutasolla sekä ammattikouluissa. Kohtien 7, 8 ja 9 vastuun voisi sisällyttää kyberturvallisuuskeskuksen sisällä toimivalle erilliselle siviiliyhteistyövironomaiselle.

8.3 Jatkotutkimusaiheet

Tutkimuksessa tarkasteltiin kyberturvallisuuden strategista johtamista Virossa, Israelissa ja Alankomaissa. Jatkkotutkimuksena olisi mielenkiintoista selvittää, miten kyberturvallisuuden poliittista kuvaa voidaan rakentaa osana kyberturvallisuuden johtamista. Lisäksi merkityksellistä olisi tutkia

analysoidun tilannekuvan nykytilaa ja kehittämistä kyberturvallisuuden johtamisessa.

LÄHTEET

Alberts, D. S., Garstka, J. J. & Sten, F. P. (2000). Network Centric Warfare – Developing and Leveraging Information Superiority. Washington D.C: CCRP Publication Series.

Ashenden, D. (2008). Information Security Management: A human challenge? Information security technical report 13/195–201. ScienceDirect.

Cyber Security Assessment, Netherlands (2018). National Coordinator for Security and Counterterrorism.

Digital Agenda 2020 for Estonia. Ministry of Economic Affairs and Communication.

Estonian Information System Authority. (2018). Annual cyber security assessment 2018.

Even, S., Siman-Tov, D. & Siboni, G. (2016). Structuring Israel Cyber Defense. INSS Insight No. 856.

Global Cybersecurity Index (CGI) 2017. PDF-tiedosto. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (Luettu 20.5.2019)

Hathaway, M. & Spidalieri, F. (2017). The Netherlands Cyber Rediness At a Glance. Potomac Institute for Policy Studies. PDF-tiedosto. http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf (Luettu 24.6.2019)

Holmgren, P. (2016). "Pelkästä tietoturvallisuudesta ei enää seuraa kyberturvallisuutta". Käsiteanalyysi kyberturvallisuudesta. Viestintätieteiden pro gradu -tutkielma. Vaasan Yliopisto.

Housen-Couriel, D. (2018). A Look At Israel New Draft Cybersecurity Law. Member of advisory board of the Hebrew University Cyber Security. www-sivu. https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law (Luettu 26.6.2019)

Housen-Couriel, D. (2017). National Cyber Security Organization : Israel. Tallinn 2017. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia.

Israel National Cyber Directorate www-sivu <https://www.gov.il/en/departments/about/newabout > (Luettu 26.6.2019)

Jaakkola, J. (2016): Pikaviestintä ja viestinnän analysointi valtiohallinnon tieto- ja kyberturvallisuuden johtamisessa. Diplomityö. Tampereen teknillinen yliopisto.

Kaplan, R., Norton, D. (2002). Strategialähtöinen organisaatio. Tehokkaan strategiaprosessin toteutus. Jyväskylä: Talentum. Gummerus kirjapaino.

Kaplan, R., Norton, D. (1996). Using the Balanced Scorecard as a Strategic Management System. Harvard Business Review. January-February 1996.

Kokonaisturvallisuuden sanasto (2014). Sanastokeskus TSK ry, Suomen Pelastusalan Keskusjärjestö SPEK. www- sivu. www.spek.fi/loader.aspx?id=1c66e01d-a75e-4a9a-80ec-9816340ce752 (Luettu 20.1.2017)

Kroll, M., Parnell, J., Wright, P. (1998): Strategic Management, Concepts. Prentice Hall, New Jersey.

Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015.

Kyrölä, T. (2010). Liiketoiminnan strateginen johtaminen: Strategiset päätökset jatkuvuudenhallinnan johtamiseksi. Lisensiaattityö. Aalto-yliopiston kauppakorkeakoulun julkaisuja B, 121.

Laaksonen, M., Nevasalo, T. & Tomula, K. (2006). Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Leppänen, A., Linderborg, K., Saarimäki, J. (2016). Tietoverkkorikollisuuden tilannekuva. Valtioneuvoston selvitys- ja tutkimustoiminta. Julkaisusarja 17/2016. Valtioneuvoston kanslia.

Limnêll, J. (2014). Kyberturvallisuus tarvitsee johtajuutta ja tekoja. Blogi - kirjoitus. http://www.aaltopro.fi/blog/kyberturvallisuus-tarvitsee-johtajuutta-ja-tekoja (Luettu 4.4.2017)

Lindfors, Susanna (2011). Tietohallintostrategia CASE: Kokkolan kaupunki. Opinnäytetyö. Keski-Pohjanmaan Ammattikorkeakoulu. Liiketalouden koulutusohjelma.

Lehto, M. (2009) Sotilaallisen strategian perusteita. Teoksessa Terho, S. (toim.) 2009: Strategian jäljillä. Maanpuolustuskorkeakoulu. Johtamisen ja sotilaspeda-

gogiikan laitos, Julkaisusarja 2. Artikkelikokoelmat No 1. Helsinki, Edita Prima Oy, 44- 67.

Lehto, M., Limnell, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Valtioneuvoston kanslia.

Lehto, M., Limnell, J., Kokkomäki, T., Pöyhönen, J., Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. Valtioneuvoston kanslia.

Matania, E., Yoffa, L. & Goldstein, Tal. (2017). Structuring the national cyber defence: in evolution towards a Central Cyber Authority. Journal of cyber policy. Volume 2, 2017. Issue 1. https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1299193?scroll=top&needAccess=true (Luettu 4.7.2019)

Metsämuuronen, J. (2000). Laadullisen tutkimuksen perusteet. Methelp International Oy. Helsinki.

Metsämuuronen J. (2003). Tutkimuksen tekemisen perusteet ihmistieteissä. 2. uudistettu painos. Gummerus. Jyväskylä, ISBN 952-5372-15-4

Mänd, M. (2017). Head of IT Policy Department. Ministry of Economic Affairs and Communication. Republic of Estonia. Vastaus tiedusteluun Viron kyberturvallisuuden strategisesta johtamisesta 14.8.2017.

NCSC. (20.3.2019). www-sivusto. What is the NCSC? https://www.ncsc.nl/english/organisation (Luettu 20.3.2019)

Osula, A-M. (2015): National Cyber Security Organization: Estonia. CCDCOE NATO Cooperative Cyber Defense Centre of Excellence. Tallinn, Estonia.

Operational Framework NCSC-NL (2018). National Cyber Security Centre. Ministry of Justice and Security.

Purser Steve (2004). A practical guide to managing Information Security. Artech House.

Seppänen, L. (2015). Organisaation kehittäminen. Aalto-yliopisto.

Siboni, G. & Assaf, O. (2016). Guidelines for a National Cyber Strategy. Memorandum No. 153. Institute for National security Studies. Ramat Aviv.

Ståhle Riittamaija, Kyberstrategian voimalla, Sähkö & Tele, 1/2013 http://www.sahkotelelehti.fi/lehdet/st12013 (Luettu 29.3.2017)

Suomen Kyberturvallisuusstrategia (2013). Valtioneuvosto. www-sivu www.yhteiskunnanturvallisuus.fi (Luettu 21.11.2016)

Tabansky, L. (2016). Towards a Theory of Cyber Power : The Israeli Experience with Innovation and Strategy. 2016 8th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn.

Terho, S. (2009): Strategian jäljillä. Maanpuolustuskorkeakoulu. Johtamisen ja sotilaspedagogiikan laitos. Julkaisusarja 2/2009.

Tietoturvatavoitteiden asettaminen ja mittaaminen. Valtiohallinnon tietoturvallisuuden johtoryhmä VAHTI 6/2006. Valtiovarainministeriö.

Tietoturvallisuuden käsite ja merkitys. Valtiokonttori. www-sivu www.valtiokonttori.fi/download/noname/%7B3B7C8612-9254-4AA3-9F25.../84888 (Luettu 2.3.2017)

Tuomi Jouni, Sarajärvi Anneli (2009): Laadullinen tutkimus ja sisällönanalyysi, Gummerus kirjapaino Oy, Jyväskylä

Turvallisuus ja puolustusasiain komitea (2012). Kyberturvallisuus MNE7- esite www.yhteiskunnanturvallisuus.fi. (Luettu 19.3.2017)

Turvallisuuskomitea 2016. Yhteiskunnan turvallisuusstrategia – päivitys. Kuulemistilaisuus 25.5.2016. PDF-tiedosto. http://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahU-KEwjl4rarkIPTAhUHCpoKHaDADWoQFggeMAA&url=http%3A%2F%2Fwww.turvallisuuskomitea.fi%2Fimages%2Fpm_site%2Fpdf%2FYTS-kuulemistilai-suus_muokattu.pdf&usg=AFQjCNGic_cR6ZLrLgPhlXLz6c7eLxwhBw (Luettu1.4.2017)

Turvallisuuskomitea. Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma. 11.3.2014. Puolustusministeriö.

Uusipaavalniemi Sari, Kovâcs Gyöngyi (2016). Toimitusketjun hallinnan trendeistä. Puolustusvoimien tutkimuslaitos. Tutkimuskatsaus 1-2016.

Valtiokonttori. Yhteisten osaamisten määritelmät. (Luettu 9.3.2017) www.valtiokonttori.fi/download/noname/%7B3C355D33-37C7-4D35-90C0.

Valtionvarainministeriö (2007). Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI-julkaisu 3/2007. Edita Prima Oy. Helsinki

Valtioneuvoston selonteko sisäisestä turvallisuudesta. Sisäministeriön julkaisu 8/2016. Sisäinen turvallisuus.

Valtioneuvosto, (2009). Valtioneuvoston periaatepäätös 7/2009 valtionhallinnon tietoturvallisuuden kehittämisestä. Valtionvarainministeriö.

Valtioneuvosto, (2010). Yhteiskunnan Turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010, Valtioneuvosto, Puolustusministeriö, Helsinki

Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtiohallinnon tietoturvallisuuden kehittämisestä. VAHTI 7/2009.

Valtiovarainministeriö. VAHTI – ohje. PDF-tiedosto. https://www.vahtiohje.fi/web/guest/johdanto-tietoturvallisuuden-johtamiseen (Luettu 9.3.2017)

Valtori, (2016). Valtorin tietoturvavalvomo (SOC). www-sivu. http://www.valtori.fi/fi-FI/Palvelut/Tulossa_olevat_palvelut/Valtorin_tietoturvavalvomo_SOC (Luettu 28.3.2017).

Varto, J. (1992). *Laadullisen tutkimuksen metodologia*. Helsinki: Kirjayhtymä

Von Solms, R. (1996). Information security management: The second generation. Computers & Security, 15(4), 281–288. http://dx.doi.org/10.1016/0167-4048(96)88939-5 (Luettu 9.3.2017)

Von Solms, R, Van Niekerk J. (2013). From information security to cyber security. Computers & Security, volume 38. Pages 97–102

Yhteiskunnan turvallisuusstrategia (2010). Valtioneuvoston periaatepäätös. Puolustusministeriö.