VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen

Kyberturvallisuuden strateginen johtaminen Suomessa

Maaliskuu 2018

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018

KUVAILULEHTI

Julkaisija ja julkaisuaika	Valtioneuvoston kanslia, 29.3.2018		
Tekijät	Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen		
Julkaisun nimi	Kyberturvallisuuden strateginen johtaminen Suomessa		
Julkaisusarjan nimi ja numero	Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018		
Asiasanat	Kyberturvallisuus, strateginen johtaminen, tilannekuva		
Julkaisun osat/ muut tuotetut versiot	Maaliskuu, 2018		
Julkaisuaika	Maaliskuu, 2018	**Sivuja** 105	**Kieli** Suomi

Tiivistelmä

Tutkimushankkeen tavoitteena oli määritellä mitä kyberturvallisuuden strateginen johtajuus on ja miten sitä toteutetaan kokonaisturvallisuuden vastuumallissa, miten yleinen häiriötilanteiden hallintamalli toteutetaan laajoissa kyberturvallisuuden häiriötilanteissa, miten kyberturvallisuuden strateginen johtaminen on organisoitava ja millainen on valtionhallinnon kyberturvallisuuden johtamisen rakenne. Lisäksi tavoitteena oli selvittää kansainväliset ja kansalliset kyberturvallisuuden mittaamisen kehikot ja menetelmät. Tässä selvityshankkeessa laadittiin toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, kybertoimintaympäristön laajojen häiriötilanteiden hallintaan sekä kyberturvallisuuden tilan mittaamiseen. Tutkimuksessa myös analysoitiin ulkomaisia kyberturvallisuusratkaisuja ja -tilannekuvamalleja. Tutkimuksen perusteella kansallisella kyberkyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Kansallisen kehittämisen ja varautumisen perustaksi sekä erilaisten kybertoimintaympäristön normaaliaikojen ja poikkeusolojen vakavien ja laajamittaisten häiriötilanteiden johtamiseksi tarvitaan selkeä strategisen tason johtamismalli ja johtamista tukeva tilannekuva.

Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista.

Kyberturvallisuudessa menestyäkseen yhteiskunnan on kyettävä osallistamaan eri toimijat sekä yhteensovittamaan voimavarat ja toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi. Kyse on koko yhteiskunnan kyberkyvykkyyden kehittämisestä. Tämä edellyttää strategista yhteensovittamista, johtamista ja toimeenpanokykyä. Kyberturvallisuuden strategisen johtamisen mallien muodostamista ovat ohjanneet Suomen kyberturvallisuusstrategiassa esitetyt tavoitteet. Vaihtoehtoisiksi malleiksi valikoituivat: nykymalli, kansallinen kyberturvallisuusjohtaja, kansallinen kyberturvallisuusyksikkö, vahvennettu Kyberturvallisuuskeskus ja Kyberturvallisuusvirasto.

Tutkimuksessa tarkastellut mallit eivät tarjoa kaikenkattavaa ratkaisua kyberturvallisuuden strategisen johtamisen toteuttamiseksi. Jonkin johtamismallin käyttöönotto edellyttää syvällisempää analyysiä muun muassa resurssitarpeista, toimivaltuuksista ja rakenteista.

Tämä julkaisu on toteutettu osana valtioneuvoston vuoden 2017 selvitys- ja tutkimussuunnitelman toimeenpanoa (tietokayttoon.fi).

PRESENTATIONSBLAD

Utgivare & utgivningsdatum	Statsrådets kansli, 29.3.2018
Författare	Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen
Publikationens namn	Strategisk ledning av cybersäkerheten i Finland
Publikationsseriens namn och nummer	Publikationsserie för statsrådets utrednings- och forskningsverksamhet 28/2018
Nyckelord	Cybersäkerheten, strategisk ledning, lägesbild
Publikationens delar /andra producerade versioner	
Utgivningsdatum	Mars, 2018 **Sidantal** 105 **Språk** Finska

Sammandrag

Syftet med forskningsprojektet var att definiera cybersäkerhetens strategiska ledning och hur den ska verkställas som en del av ansvarsmodellen kring den övergripande säkerheten, hur en allmän modell för hantering av störningssituationer tillämpas vid omfattande störningssituationer, hur den strategiska ledningen av cybersäkerheten ska organiseras, och hurdan ledningsstrukturen för statsförvaltningens cybersäkerhet är. Därtill är syftet att utreda de internationella och de nationella ramverken och metoderna för att mäta cybersäkerheten. I utredningen utarbetades åtgärdsförslag för att leda samhällets och den offentliga förvaltningens strategiska cybersäkerhet, hantering av omfattande störningssituationer i cybermiljön samt att mäta cybersäkerhetsläget. Även utländska cybersäkerhetslösningar och modeller för lägesbilden analyserades. Undersökningen visar att den nationella cyberkompetensen framöver blir allt viktigare när det gäller att trygga den övergripande säkerheten och livsviktiga samhällsfunktioner. Det behövs en klar och tydlig ledningsmodell på strategisk nivå och en lägesbild som stöder ledningen som grund för det nationella utvecklings- och beredskapsarbetet. Dessa är nödvändiga även för ledandet av allvarliga, omfattande störningssituationer i cybermiljöer i normala och i exceptionella förhållanden.

Strategisk ledning av cybersäkerheten innebär att identifiera och sätta upp mål som syftar till att skydda den digitala verksamhetsmiljön. Därtill gäller det att samordna verksamheten och beredskapen samt leda hanteringen av omfattande störningar.

För att trygga cybersäkerheten och uppnå de strategiska målen ska samhället kunna engagera olika aktörer och samordna sina resurser och verksamhetsmetoder så effektivt som möjligt. Det gäller att utveckla cyberkompetensen i hela samhället. Detta åter förutsätter strategisk samordning, ledarskap och handlingsförmåga. Målen i Finlands cybersäkerhetsstrategi har styrt utarbetandet av modeller för strategisk ledning av cybersäkerheten. Följande alternativa modeller utvaldes: den nuvarande modellen, en nationell cybersäkerhetsledare, en nationell cybersäkerhetsenhet, ett förstärkt Cybersäkerhetscenter och en IT-säkerhetsmyndighet. Modellerna som granskats i undersökningen erbjuder inte en övergripande lösning för strategisk ledning av cybersäkerheten. För att ta i bruk någon av ledningsmodellerna krävs en djupare analys av bland annat resursbehovet, befogenheter och strukturer.

Den här publikationen är en del i genomförandet av statsrådets utrednings- och forskningsplan för 2017 (tietokayttoon.fi/sv).

DESCRIPTION

Publisher and release date	Prime Minister´s Office, 29.3.2018
Authors	Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen
Title of publication	Strategic management of cyber security in Finland
Name of series and number of publication	Publications of the Government´s analysis, assessment and research activities 28/2018
Keywords	Cyber security, strategic management, situational picture
Other parts of publication/ other produced versions	
Release date	March, 2018 **Pages** 105 **Language** Finnish

Abstract

The aim of the research project was to define what the strategic management of cyber security is and how it is implemented as part of the responsibility model of comprehensive security, how a general incident management model is applied to extensive cyber security incidents, how the strategic management of cyber security must be organised, and what the structure of cyber security management in state administration is. In addition, the aim was to map international and national frameworks and methods for measuring cyber security. This research project provided action proposals for managing strategic cyber security in society and public administration, for managing large disruptions in the cyber operating environment, and for measuring the state of cyber security. International cyber security solutions and scenario models were also analysed in the study. The study indicates that national cyber capability will be increasingly important in the future for comprehensive security and for ensuring the vital functions of society. As a basis for national development and preparedness, it is necessary to have a clear strategy-level management model and situation awareness that supports management. They are also necessary for the management of serious, extensive disruptions in both normal and exceptional conditions of the cyber operating environment. **The strategic management of cyber security implies identifying and setting goals based on the protection of the digital operating environment. Furthermore, it implies coordinating actions and preparedness as well as managing extensive disruptions.**

In order to ensure cyber security and achieve the set strategic goals, society must be able to engage different parties and reconcile resources and courses of action as efficiently as possible. Cyber capability must be developed in the entire society, which calls for strategic coordination, management and executive capability. The goals presented in Finland's Cyber Security Strategy have guided the creation of strategic management models for cyber security. The following were chosen as alternative models: the present model, a national cyber security manager, a national cyber security unit, a strengthened National Cyber Security Centre, and a Cyber Security Agency. The models examined in the study do not offer a comprehensive solution for the strategic management of cyber security. The adoption of some of the management models calls for a deeper analysis of, for example, resource needs, authorisations and structures.

This publication is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2017 (tietokayttoon.fi/en).

SISÄLLYS

1. JOHDANTO

1.1 Tutkimuksen tausta ja tavoitteet

1.1.1 Tutkimuksen tausta

Suomen Kyberturvallisuusstrategia julkaistiin vuonna 2013 ja sen toimeenpano-ohjelma vuonna 2014. Päivitetty toimeenpano-ohjelma vuosille 2017-2020 hyväksyttiin Turvallisuuskomiteassa 10.4.2017. Päivitetty toimeenpano-ohjelma sisältää 22 toimenpidettä, joihin lukeutuvat seuraavat toimenpiteet: Strateginen johtajuus on määritetty (nro 1), valtionhallinnon kyberturvallisuuden johtamisen malli on luotu ja organisoitu (nro 2), julkisen hallinnon kyberhäiriötilanteiden operatiivinen hallintamalli on toteutettu ja toiminnassa (nro 3) ja toimeenpano-ohjelman seurantamittaristo on luotu (nro 7). Näiden toimenpiteiden toteuttaminen vaatii tutkimus- ja selvitystyötä.

Helmikuussa 2017 julkaistussa valtioneuvoston selvityksessä ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” todetaan: ”Kyberturvallisuuden kokonaisvaltainen, koko yhteiskunnan eri kybertoiminnot kattava ja yhdistävä johtajuuden epämääräisyys ja puuttuminen nousivat tutkimuksessa vahvasti esille. Johtopäätöksenä voi todeta, että strategisen johtajuuden selkeyttäminen ja vahvistaminen ovat hyvin oleellinen asia Suomen kyberturvallisuuden vision saavuttamisen varmistamisessa.”

Valtioneuvoston periaatepäätöksessä kokonaisturvallisuudesta 5.12.2012 on kuvattu kokonaisturvallisuuden vastuiden jakautuminen, varautumisen sekä häiriötilanteiden hallinnan vastuumalli.

Kansallisella kyberkyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Kansallisen kehittämisen ja varautumisen perustaksi sekä erilaisten kybertoimintaympäristön normaaliaikojen ja poikkeusolojen häiriötilanteiden johtamiseksi tarvitaan selkeä strategisen tason johtamismalli ja tilannekuva.

1.1.2 Tutkimuksen tavoitteet

Kyberturvallisuuden strategian toteutumisen ja hallinnonalojen sitoutumisen kannalta Suomessa ollaan eri tilanteessa kuin ensimmäisen kyberturvallisuusstrategian laatimisen aikaan vuonna 2013. Hallinnonaloilla on tunnistettu laajasti kyberturvallisuuden merkitys arjen työssä. Vuoden 2013 strategian laatimisen aikana hallinnonaloilla oli erilaisia näkemyksiä kyberturvallisuudesta, mutta sen julkaisemisen jälkeen maailma on muuttunut erittäin nopeasti. Strategiatyössä yksityisen sektorin osallistuminen on ensiarvoista, jotta yritysten ja kansalaisyhteiskunnan tarpeet ja julkisesta toimintapolitiikasta niille aiheutuvat vaikutukset voidaan luotettavasti arvioida. Tällaisia esimerkkejä ovat hallitusohjelman toimeenpanotyössä laadittu tietoturvastrategia ja lainsäädännön valmistelun osalta EU:n tietosuoja-asetus.

Tässä selvityshankkeessa laadittiin toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, kyberturvallisuuden tilan mittaamiseen ja varautumiseen sekä laajalti vaikuttavien kybertoimintaympäristöä koskevan häiriötilanteiden hallintaan.

Keskeisiä tarkasteltavia tutkimuskysymyksiä olivat:

- Mitä on kyberturvallisuuden strateginen johtajuus ja miten sitä toteutetaan kokonaisturvallisuuden vastuumallissa?
- Miten yleinen häiriötilanteiden hallintamalli toteutetaan laajoissa kyberturvallisuuden häiriötilanteissa?
- Miten kyberturvallisuuden strateginen johtaminen on organisoitava?
- Mikä on valtionhallinnon kyberturvallisuuden johtamisen rakenne?
- Mikä on kyberhäiriötilanneymmärryksen analysoinnin prosessi ja toimijat?
- Mikä on tarkoituksenmukaisin menettely ja mittaristo kyberturvallisuuden tilan jatkuvalle arvioimiselle Suomessa ja kyberturvallisuuden toimeenpanon edistymiselle, ottaen huomioon olemassa olevat kansainväliset indeksit ja mittarit?

1.2 Aineistot ja menetelmät

Tutkimushankkeessa kerättiin hyvin monipuolinen ja laaja-alainen aineisto. Keskeisimmät aineistokokonaisuudet olivat eri turvallisuuteen liittyvät strategiat ja ohjeet, olemassa oleva tutkimustieto sekä julkisen sektorin toimijoiden ja alan asiantuntijoiden haastattelut. Tutkimushankkeessa haastateltiin yhteensä 40 yksityisten ja julkisten organisaatioiden johtohenkilöitä ja tieto/kyberturvallisuudesta vastaavia henkilöitä. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville luvattiin täysi anonymiteetti. Haastatteluaineiston, asiakirja-analyysin sekä kansainvälisen vertailutiedon perusteella luotiin analysoitu tietoaineisto, johon tässä tutkimuksessa esitetyt havainnot, esitykset ja mallit perustuvat.

Haastattelut kohdistuivat seuraaviin organisaatioihin:

1. CGI Finland Oy
2. Elinkeinoelämän keskusliitto
3. ELISA Oyj
4. F-Secure Oyj
5. Fingrid Oyj
6. Finnish Information Security Cluster
7. Huoltovarmuuskeskus
8. Hätäkeskuslaitos
9. Insta Group Oyj
10. Keskusrikospoliisi
11. Liikenne- ja viestintäministeriö
12. Poliisihallitus
13. Puolustusministeriö
14. Puolustusvoimat
15. Sisäministeriö
16. SSH Communications Security Oyj
17. Suomen Erillisverkot Oy
18. Teknologiateollisuus ry
19. Tieto Oyj
20. Turvallisuuskomitea
21. Valtioneuvoston kanslia
22. Valtion tieto- ja viestintätekniikkakeskus Valtori
23. Valtiovarainministeriö
24. Viestintävirasto (ml. Kyberturvallisuuskeskus)
25. Ulkoministeriö

Kansainvälistä vertailutietoa strategisen kyberturvallisuuden johtamista varten kerättiin kuudesta maasta: Alankomaat, Australia, Israel, Ruotsi, Singapore ja Viro. Tutkimusaineisto käsitti kunkin maan kyberturvallisuusstrategian, vastaavia turvallisuusdokumentteja ja

asiakirjoja sekä aiheeseen liittyviä tutkimuksia. Kybertilannekuvan tutkimusta varten kerättiin vertailutietoa Isosta-Britanniasta, Ranskasta ja Saksasta.

Tutkimuksessa on hyödynnetty Suomen kyberturvallisuusstrategiaa (2013) ja sen toimeenpano-ohjelmaa 2017-2020, Yhteiskunnan turvallisuusstrategiaa (2017), Valtionhallinnon viestintä häiriötilanteissa ja poikkeusoloissa -raporttia (2013), Suomalaisen tiedustelulainsäädännön suuntaviivoja - Tiedonhankintalakityöryhmän mietintöä (2015) sekä Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomusta Kybersuojauksen järjestäminen (2017). Lisäksi keskeistä dokumenttiaineistoa ovat olleet muut valtionhallinnon strategiat (Suomen tietoturvallisuusstrategia, 2016 ym.), aiemmat tutkimukset ja selvitykset sekä erilaiset kansainväliset kyberturvallisuuskyvykkyysmittarit.

2. KYBERTURVALLISUUDEN STRATEGINEN JOHTAMINEN

2.1 Strateginen johtaminen

Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS 2017) määritettyjä periaatteita ja toimintatapoja.

1. Kyberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin eli kyberturvallisuuden edellytyksenä on jokaisen kybertoimintaympäristössä toimivan tahon toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut.

2. Kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa.

Teknistaloudellinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Tehokas ja optimoitu verkostotalous perustuu nopeasti kehittyvään tieto- ja viestintäteknologiaan, joka on häiriöherkkä monille uudenlaisille uhkille ja riskeille. Kyberhyökkäykset, haittaohjelmat, palvelunestohyökkäykset ja erilaiset informaatiovaikuttamisen muodot lisääntyvät jatkuvasti. Tietoliikenteen, tietojärjestelmien ja viestinnän toimintavarmuus on nykyaikaisen yhteiskunnan häiriöttömän toiminnan, turvallisuuden ja kansalaisten toimeentulon välttämätön edellytys. Kyse on myös kansalaisten luottamuksen ylläpitämisestä yhteiskunnan toimintaan. Merkittävä osa tietoyhteiskunta-alan parissa tehtävästä huoltovarmuustyöstä koostuu yritysten jatkuvuudenhallinnan kehittämisestä. Tämän kehityksen vuoksi varautumista yhteiskunnalle välttämättömien tietoteknisten järjestelmien ja rakenteiden toimivuuteen kyberuhka ja -häiriötilanteissa tulee tehostaa jo normaalioloissa. On erityisesti otettava huomioon, että suomalaisen yhteiskunnan ja yritysten riippuvuus kybertoimintaympäristöstä kasvaa entisestään tulevina vuosina.[1]

Kyberturvallisuuden johtaminen sisältää erityispiirteitä, jotka poikkeavat muista normaaliaikojen ja poikkeusolojen häiriötilanteista. Keskeisin tekijä on aika. Kyberhyökkäyksen valmistelu on mahdollista toteuttaa salassa ja pitkän ajan kuluessa, mutta itse hyökkäys voidaan toteuttaa erittäin lyhyessä ajassa. Tammikuussa 2003 verkkomato Slammer levisi 10 minuutissa hyökkäyksen aloittamisesta arviolta 90 prosenttiin suunnitelluista kohteista (75 000 uhria). Hyökkäys alkoi aikaisin lauantaiaamuna, mikä osaltaan hankaloitti viranomaistoimenpiteitä. Arvioiden mukaan Slammer-verkkomadon kustannukset nousivat 750 miljoonaan euroon. Slammer aiheutti internetin toiminnan maailmanlaajuisen hidastumisen ja muun muassa Bank of American pankkiautomaattiverkkoon kahden päivän toimintakatkoksen ja jopa 90 minuutin viiveitä Yhdysvaltojen lentoliikenteessä, Seattlen aluehälytyskeskuksen kaatumisen 14 tunniksi ja Davis-Bessen ydinvoimalan reaktorin turvajärjestelmän kaatumisen.

Lähes 15 vuotta myöhemmin toukokuussa 2017 levisi internetin kautta WannaCry kiristyshaittaohjelma, joka saastutti yli 200 000 konetta yli 150 maassa. Tämäkin verkkohyökkäys alkoi viikonloppuna ja tilanteen vakavuus paljastui vasta maanantaina. Kiristysohjelma aiheutti

[1] https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/toiminnan-perusteet/

ongelmia Ison-Britannian sairaalajärjestelmissä, ja lisäksi kohteeksi ilmoittivat joutuneensa muiden muassa Venäjän sisäministeriö, autonvalmistajat Renault ja Nissan, ruotsalainen teollisuuskonserni Sandvik, Saksan rautatieyhtiö Deutsche Bahn, kuljetusyhtiö FedEx ja espanjalainen teleyhtiö Telefonica. Arvioiden mukaan hyökkäyksen taloudelliset menetykset voivat nousta 4 miljardiin dollariin.

Kybertoimintaympäristön ominaisuuksiin kuuluu kehityksen suuri nopeus, tapahtumien hektisyys ja eri järjestelmien kompleksisuus. Informaatioteknologian kehityssykli on lyhyt ja sama trendi koskee eri kyberhyökkäysmuotoja ja haittaohjelmia. Kybertoimintaympäristölle on leimallista muutosnopeus, mikä edellyttää strategiselta muutokselta nopeaa reagointikykyä – ketteryyttä, sekä varautumista myös tilanteisiin, joita ei täysin kyetä ennakoimaan. Kyberturvallisuuden johtamisessa ilmentyy kolme tekijää, joita ovat strateginen herkkyys, resurssien joustavuus ja johtamisen yhtenäisyys.

Strateginen herkkyys edellyttää kybertoimintaympäristössä kykyä nopeaan tilannekuvan muodostamiseen ja tilannetietoisuuden luomiseen päätöksenteon ja toimenpiteiden perustana. Kybertilannekuvaympäristön rakentaminen edellyttää jaettua tilannetietoisuutta, koordinoitua ja verkostoitunutta johtamista sekä riittävää osaamista kyberturvallisuuden eri alueille.[2]

Resurssien joustavuus tarkoittaa kykyä nopeaan osaamisen ja taloudellisten resurssien allokointiin. Resursseja voidaan käyttää joustavasti vain, jos tiedetään missä ja miten on käytettävissä yhteinen kyberkyvykkyys. Kybertoimintaympäristössä tulee päästä irti osaoptimoinnista, resurssien siiloutuneista rakenteita ja kangistuneista toimintatapamalleista. Kybermaailmassa eri toimintarakenteiden tulee olla modulaarisia, jotta strategisen johtamisen nopeus voidaan turvata. Yhteiskunnassa tulee voida käyttää hyväksi valtiohallinnon resursseja ja myös sopimussuhteisia PPP-yhteistyömuotoja.[3]

Johtamisen yhtenäisyys edellyttää yhteistä agendaa ja tavoitteita sekä keskinäisen riippuvuuden aitoa tunnustamista. Kybermaailman strateginen johtaminen edellyttää kaikilta toimijoilta kollektiivista sitoutumista, joka menee yli henkilökohtaisen tai oman organisaation edun. Strategisen tason johdon yhteistyökyky on ratkaisevaa kybertoimintaympäristön nopeaa päätöksentekoa edellyttävissä uhkatilanteissa.[4]

Kansallinen kyberturvallisuuden strateginen johtaminen muodostuu kahdesta kokonaisuudesta: Kyberturvallisuuden varautumisen johtaminen sekä vakavien ja laajamittaisten häiriötilanteiden hallinnan johtaminen normaali- ja poikkeusoloissa.

Varautumiseen yhdistyvät myös huoltovarmuuden ja kyberomavaraisuudesta huolehtimisen näkökulmat. Tämä tarkoittaa väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen ja niihin liittyvien teknisten järjestelmien turvaamista poikkeusolojen ja niihin verrattavissa olevien vakavien kyberhäiriöiden varalta. Varautumisen johtamiseen kuuluu nykytilan johtamisen parantamista (yhteiset mallit, yhteistyöverkostot, yhteisten kyvykkyyksien tunteminen) sekä pitkän aikavälin strategisten tavoitteiden asettaminen, resurssointi, kansallisen kyberturvallisuuspolitiikan asettaminen ja kansainvälisen kyberturvallisuustoiminnan ohjaaminen.

[2] Suomen kyberturvallisuusstrategia ja taustamuistio, 24.1.2013

[3] Ibid.

[4] Ibid.

2.2 Valtion johtamisen yleiset periaatteet

Johtaminen on kiinteä osa varautumista ja valmiutta. Elintärkeisiin toimintoihin kohdistuvien uhkien hallinta edellyttää kaikkien tarvittavien turvallisuustoimijoiden yhteistoimintaa johtamisen tukena. Varoitus- ja ennakointijärjestelmien tiedon jakaminen hyvissä ajoin edesauttaa häiriötilanteiden ennaltaehkäisyä ja vähentää haittavaikutuksia.[5]

Hyvä johtaminen edellyttää seuraavia osatekijöitä[6]:

- Selkeät johtovastuut, toimijoiden roolitus ja toimivaltaisen viranomaisen päätöksentekokyky
- Tilannekuvan muodostaminen (tilanneymmärrys, arvio tilanteen kehittymisestä),
- Kriisiviestintä,
- Tiedon jakaminen ja sitä tukevia teknisiä ratkaisuja,
- Toiminnan jatkuvuudenhallinta ja
- Yhteistoiminta

Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta (UTVA) käsittelee valmistelevasti tärkeät ulko- ja turvallisuuspolitiikkaa ja muita Suomen suhteita ulkovaltoihin koskevat asiat, näihin liittyvät tärkeät sisäisen turvallisuuden asiat sekä tärkeät kokonaismaanpuolustusta koskevat asiat. Yhteiskunnan elintärkeiden toimintojen turvaamiseen liittyviä asioita valmistellaan myös muissa ministerivaliokunnissa.

Yhteiskunnan elintärkeiden toimintojen turvaamista johtaa, valvoo ja sovittaa yhteen valtioneuvosto sekä toimivaltainen ministeriö hallinnonalallaan. Varautumiseen ja toiminnan käynnistämiseen kukin toimivaltainen viranomainen käyttää laissa säädettyjä normaaliolojen toimivaltuuksia.

Toimivaltainen viranomainen johtaa operatiivista toimintaa, käynnistää häiriötilanteen hallintaan liittyvät toimenpiteet, vastaa viestinnästä ja tiedottaa tilanteesta sovittujen käytäntöjen mukaisesti. Muut viranomaiset sekä valtion ja kuntien laitokset osallistuvat toimintaan ja antavat virka-apua tilanteen hallinnan edellyttämässä laajuudessa. [7]

Monimuotoisten ja nopeasti kehittyvien häiriötilanteiden hallinta edellyttää oikea-aikaista ja joustavaa reagointia. Toiminnan koordinointi ja tiedonkulku on varmistettava eri viranomaisten ja muiden turvallisuustoimijoiden yhteistoiminnalla. Valtioneuvostossa toimivaltainen ministeriö tai valtioneuvoston kanslia kutsuu tarvittaessa koolle ylimääräisen valmiuspäällikkökokouksen. [8]

Yleisiä häiriötilanteiden hallinnan periaatteita noudatetaan valtiojohdon toimintatasoa mukaillen myös alue- ja paikallistasolla, jolloin ne käsittävät ensisijaisesti paikallisia toimia. Johtamisvastuut ja tilannekuvan kokoamisen sekä jakamisen periaatteet korostuvat kuntien ja alueiden (tulevien maakuntien) johtamisessa.[9]

[5] Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 2.11.2017

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

2.2.1 Kyberturvallisuuden varautumisen ja huoltovarmuuden johtaminen

Ministeriöt johtavat hallinnonalansa varautumista ja sisällyttävät periaatepäätöksen edellyttämät toimenpiteet hallinnonalansa toiminnan ja talouden suunnittelu- sekä toimeenpano-asiakirjoihin.

Valtioneuvoston ohjesäännön mukaan ministeriö käsittelee oman toimialansa toiminta- ja taloussuunnitteluasiat, tulosohjausasiat, lainvalmisteluasiat, tietoyhteiskunta-asiat, hallintoasiat, viestintäasiat, tietohallintoasiat, tutkimusta, kehittämistä ja seurantaa koskevat asiat, kansainväliset asiat sekä toimialansa hallinnassa olevan valtion varallisuuden omistaja-asiat samoin kuin muut sellaiset asiat, joiden on katsottava kuuluvan toimialan tehtävien hoitamiseen.[10]

Valtioneuvoston yleisistunto ratkaisee viranomaisten yhteistoimintaa koskevat asiat, kuten kysymyksen siitä, minkä ministeriön käsiteltäviin jokin asia kuuluu, sekä tarvittaessa asian määrääminen valmisteltavaksi yhteisesti kahdessa tai useammassa ministeriössä. Yleisistunnossa käsitellään myös kahden tai useamman ministeriön toimialaan kuuluva asia, joista ministeriöt eivät pääse sopimukseen keskenään.[11]

Tavoitteena on, että yhteiskunnan elintärkeiden toimintojen kannalta keskeiset yritykset ja organisaatiot ottavat jatkuvuudenhallinnassaan huomioon niihin kohdistuvat kyberuhat ja pitävät yllä tarvittavaa suojautumiskykyä. Huoltovarmuuskeskus ja muu huoltovarmuusorganisaatio tukevat toimintaa selvityksin, ohjeistuksin ja koulutuksella.[12]

Yhteiskunnan elintärkeistä toiminnoista vastaavien ministeriöiden tulee yhdessä huoltovarmuusorganisaation kanssa tunnistaa kriittisimmät ICT -rakenteet, -palvelut, tekninen ylläpito ja näihin liittyvä osaaminen sekä tietovarannot. Näihin liittyvät riskit, haavoittuvuudet ja kansainväliset riippuvuudet sekä niiden vaikutukset tulee tunnistaa ja arvioida. Viranomaiset ja huoltovarmuusorganisaatio laativat kriittisten tieto- ja viestintäjärjestelmien sekä näihin liittyvien palveluiden varmistamiselle, turvallisuudelle ja jatkuvuudelle yhtenäiset kansalliset vaatimustenhallinnan perusteet. Julkisen sektorin ICT -järjestelmistä vastaavat organisaatiot käyttävät näitä huoltovarmuuden kannalta kriittisten järjestelmien rakenteen määrittämiseen, palveluiden järjestämiseen, kilpailutukseen ja ulkoistamiseen. Huoltovarmuusorganisaatio edistää niiden soveltamista myös yksityisellä sektorilla.[13]

Normien lisäksi varautumisen ohjauksessa ja vaatimusten muodostamisessa keskeisessä osassa ovat valtioneuvoston periaatepäätökset valtionhallinnon tietoturvallisuuden kehittämisestä (2009) ja yhteiskunnan turvallisuusstrategiasta (YTS 2017). Strategiassa määritetään yhteiskunnan elintärkeät toiminnot, jotka tulee varmistaa niin normaaliajan kuin poikkeusolojen häiriötilanteissa. Elintärkeiden toimintojen hoitamiseksi hallinnonaloille on määritetty strategiset tehtävät. Kullakin virastolla ja organisaatiolla voi näiden lisäksi myös olla muita oman toimintansa kannalta kriittisiä palveluja ja tehtäviä.[14]

Huoltovarmuustyön tavoitteena on, että vakavimmat poikkeusolot voidaan hoitaa kansallisin toimenpitein. Huoltovarmuusorganisaatio koostuu Huoltovarmuuskeskuksesta, huoltovarmuusneuvostosta, sektoreista ja pooleista. Huoltovarmuuskeskus kokoaa ja ylläpitää yhteistyössä Turvallisuuskomitean ja muiden viranomaisten sekä yritysten ja järjestöjen kanssa ajantasaista ja ennakoivaa tietoa huoltovarmuudelle kriittisestä tuotannosta, palveluista ja

[10] Valtioneuvoston ohjesääntö, 3.4.2003/262, 11 §

[11] Ibid., 8 §

[12] Valtioneuvoston päätös huoltovarmuuden tavoitteista, 857/2013, Helsinki 5.12.2013

[13] Ibid.

[14] http://vm.fi/varautuminen

infrastruktuureista sekä huoltovarmuuteen vaikuttavista uhkista, riippuvuuksista ja muutoksista. Osana huoltovarmuusorganisaatiota sen tehtävänä on tukea poolien ja sektorien toimintaa sekä hoitaa muut sille lainsäädännössä annetut tehtävät. Huoltovarmuuden kehittäminen ja varautumistoimien yhteensovittaminen kuuluvat työ- ja elinkeinoministeriölle. Ministeriöt kehittävät huoltovarmuutta omalla toimialallaan. Järjestelyillä turvataan väestön asema siltä varalta, että markkinoiden normaali toiminta ei tuota riittävää huoltovarmuutta. Suomen huoltovarmuustoimenpiteiden lähtökohtana on EU:n sisämarkkinoiden toimivuus.[15]

2.2.2 Normaaliaikojen ja poikkeusolojen häiriötilanteiden johtaminen

Häiriötilanteita voi esiintyä sekä normaalioloissa että poikkeusoloissa. Normaalioloissa esiintyvät häiriötilanteet hallitaan viranomaisten tavanomaisin toimivaltuuksin tai voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliolojen häiriötilanteiden hallinnassa. Poikkeusoloissa tilanteen hallitseminen voi edellyttää lisätoimivaltuuksia tai voimavaroja.

Yhteiskunnan haavoittuvuuden lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti. *Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki.* Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta.

Kyberhäiriötilanteiden hallinnassa noudatetaan laillisuusperiaatetta ja voimassaolevaa toimialajakoa. Samoja häiriötilanteen hallinnan periaatteita noudatetaan sekä normaali- että poikkeusoloissa. Viranomaisten vastuujako ja yhteistyöelimien toimintamallit säilytetään normaaliolojen mukaisina. Tilanteita johdetaan ennakoivasti ja käyttöön otetaan heti riittävät voimavarat. Toimivaltainen viranomainen johtaa operatiivista toimintaa ja poikkihallinnolliset yhteistyöelimet tukevat vastuuviranomaista. Toimintaa johtava taho vastaa myös viestinnästä. Muut viranomaiset, yritykset ja järjestöt osallistuvat toimintaan tilanteen hallinnan edellyttämässä laajuudessa. Operatiivisten toimien ohella häiriötilanteiden hallinnan yhteydessä korostuu tiedonkulun varmistaminen toimijoiden välillä sekä valtiojohdon riittävä informointi.[16]

Häiriötilannetta voi olla tarpeen käsitellä mahdollisimman nopeasti hallituksen neuvottelussa siten, että kaikilla valtioneuvoston jäsenillä on mahdollisuus saada samanaikaisesti tarkka ja oikeansisältöinen käsitys asiasta. Tämä on olennaista valtioneuvoston jäsenten työn ja ministerinvastuun kantamisen kannalta. Tässä yhteydessä voidaan käsitellä tilannetiedon lisäksi valmisteluvastuita sekä jatkokäsittelyä. Jatkokäsittelyyn kuuluu muun muassa ministeriöiden riittävän yhteistyön järjestäminen sekä käsittelyt ministerivaliokunnissa.

Valtioneuvostoa ja ministeriöitä tukee valtioneuvoston johtokeskus. Se koostuu johto-osasta sekä valtioneuvoston kanslian johdossa toimivista tilannekeskuksesta ja viestintäkeskuksesta. Johto-osa voi kokoontua valmiuspäälliköiden, kansliapäälliköiden tai valtioneuvoston jäsenten tasolla (ministerivaliokunta, hallituksen neuvottelu, valtioneuvoston yleisistunto). Valtioneuvoston tilannekeskus toimii ministeriöiden varallaolopäivystyksen yhteyspisteenä. Se informoi ympärivuorokautisesti hallinnonaloja havaituista tapahtumista ja kutsuu tarvittaessa koolle yhteistyöelimet sekä tarvittavat asiantuntijat eri hallinnonaloilta ajantasaisen

[15] Valtioneuvoston päätös huoltovarmuuden tavoitteista, 857/2013, Helsinki 5.12.2013

[16] Suomen kyberturvallisuusstrategia ja taustamuistio, 24.1.2013

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 2.11.2017

tiedonsaannin turvaamiseksi. Tilannekeskus myös koordinoi tarvittaessa tilannekuvan laatimisen, häiriötilanteen hallintaan osallistuvien viranomaisten ja muiden toimijoiden tuella.

Vastuuviranomainen käynnistää häiriötilanteen hallintaan liittyvät toimenpiteet, informoi tilanteesta tarvittavassa laajuudessa muita viranomaisia ja toimijoita sekä kytkee toimintaan muut häiriötilanteen hallinnan edellyttämät toimijat. Tilanteen edellyttäessä voidaan ottaa käyttöön valmiuslain mukaisia poikkeusolojen toimivaltuuksia.

2.3 Nykyinen johtamismalli normaaliajan ja poikkeusolojen häiriötilanteissa

2.3.1 Normaaliolojen toimivaltuudet

Suomessa viestintäpalveluita ja digitaalista infrastruktuuria koskeva sääntely sisältyy keskeisin osin lakiin sähköisen viestinnän palveluista, joka sisältää laajan keinovalikoiman puuttua viestintäverkkojen ja -palvelujen häiriötilanteisiin normaalioloissa. Laki sähköisen viestinnän palveluista muun muassa edellyttää, että yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista. Laissa sähköisen viestinnän palveluista säädetään myös toimenpiteistä, joihin teleyrityksellä, yhteisötilaajalla ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä tietoturvasta huolehtimiseksi, teleyrityksen tai muun viestintäverkon tai laitteen haltijan velvollisuudesta korjata häiriö, teleyrityksen ja lisäarvopalvelun tarjoajan velvollisuudesta tehdä häiriöilmoituksia käyttäjille ja viranomaisille. Viestintävirasto valvoo säännösten noudattamista.[17]

Laki sähköisen viestinnän palveluista[18] sisältää varsin laajan keinovalikoiman puuttua häiriötilanteisiin normaalioloissa. Teleyrityksellä, yhteisötilaajalla ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi:

- Viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;
- Viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai
- Viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Tarkoitetut toimet voivat käsittää:

- Viestin sisältöä koskevan automaattisen selvittämisen;
- Viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;
- Tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;

Viestintävirasto voi häiriötilanteita varten asettaa yhteistoimintaryhmän, jossa ovat edustettuina teleyritykset, sähkömarkkinalaissa (588/2013) tarkoitetut verkon- ja jakeluverkonhaltijat ja em. lukuun toimivat urakoitsijat. Ryhmän tehtävänä on:

- Suunnitella ja sovittaa yhteen valmiuslain mukaisten poikkeusolojen sekä normaaliolojen häiriötilanteiden hallinnassa tarvittavia toimenpiteitä;

[17] Laki sähköisen viestinnän palveluista, 7.11.2014/917

[18] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#L33P272

- Hankkia ja toimittaa häiriötilanteiden hallinnassa tarpeellisia tietoja Viestintäviraston päätöksenteon tueksi; sekä
- Välittää ryhmän kokoamaa ja analysoimaa häiriötilanteita koskevaa tietoa sellaisille toimijoille, jotka voivat vähentää häiriötilanteiden haitallisia vaikutuksia yhteiskunnalle.

Laki sähköisen viestinnän palveluista antaa myös perusteita velvollisuudesta varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin.

2.3.2 Valmiuslain antamat toimivaltuudet

Valmiuslaki antaa toimivaltuuksia koskien sähköisten tieto- ja viestintäjärjestelmien toimivuutta, valtion tietohallinnon ohjausta sekä viestintää poikkeusoloissa. Viranomaiset voidaan oikeuttaa poikkeusoloissa käyttämään vain sellaisia toimivaltuuksia, jotka ovat välttämättömiä ja oikeasuhtaisia säädetyn tarkoituksen saavuttamiseksi. Toimivaltuuksia voidaan käyttää vain sellaisin tavoin, jotka ovat välttämättömiä lain tarkoituksen saavuttamiseksi ja oikeassa suhteessa toimivaltuuden käyttämisellä tavoiteltavaan päämäärään nähden. Tämän lain mukaisia toimivaltuuksia voidaan käyttää vain, jos tilanne ei ole hallittavissa viranomaisten säännönmukaisin toimivaltuuksin.[19]

Sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi ja niihin kohdistuvien tietoturvauhkien torjumiseksi **liikenne- ja viestintäministeriöllä** (LVM) on toimivaltuuksia teleyrityksiä kohtaan. LVM voi velvoittaa teleyrityksiä: [20]

1) Tuottamaan verkko- ja viestintäpalveluja sekä antamaan viranomaiselle verkko- ja viestintäpalveluiden käyttöä koskevan tilannekuvan;
2) Pitämään kunnossa tai rakentamaan taikka jättämään rakentamatta viestintäverkkoja;
3) Luovuttamaan viranomaiselle tai toiselle teleyritykselle käyttöoikeuden viestintämarkkinalain 4 luvussa tarkoitettuun omaisuuteen;
4) Järjestämään kansainväliset verkko- ja viestintäpalveluyhteytensä liikenne- ja viestintäministeriön yksilöimällä tavalla;
5) Sopimaan kansallisista tai kansainvälisistä verkkovierailuista liikenne- ja viestintäministeriön osoittamalla tavalla;
6) Liittämään viestintäverkon yhteen toisen viestintäverkon kanssa tai purkamaan yhteen liittämisen;
7) Katkaisemaan määräajaksi tai toistaiseksi verkko- tai viestintäpalveluyhteydet tiettyyn maahan tai kansainvälisiin verkko- ja viestintäpalveluihin;
8) Ylläpitämään järjestelmiä ja palveluita tietyistä paikoista.

Sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi ja niihin kohdistuvien tietoturvauhkien torjumiseksi liikenne- ja viestintäministeriö voi poikkeusoloissa päätöksellään velvoittaa laissa sähköisen viestinnän palveluista (7.11.2014/917) tarkoitetun teleyrityksen, lisäarvopalvelun tarjoajan tai muun kuin valtionhallinnon yhteisötilaajan taikka näiden lukuun toimivan henkilön:[21]

- Estämään tilapäisesti sähköpostiviestien, tekstiviestien ja muiden vastaavien viestien tai vertaisverkkoliikenteen lähettämisen, välittämisen tai vastaanottamisen;
- Salaamaan tai olemaan salaamatta verkko- ja viestintäpalvelunsa;

[19] Valmiuslaki, 29.12.2011/1552, 4 §

[20] Ibid., 60 §

[21] Ibid., 62 §

- Ryhtymään muihin vastaaviin välttämättömiin toimiin tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi.

Sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi liikenne- ja viestintäministeriö voi poikkeusoloissa päätöksellään velvoittaa yksityisen henkilön tai muun kuin valtionhallintoon kuuluvan yhteisön luovuttamaan viranomaiselle tai viranomaisen nimeämälle taholle käyttöoikeuden ohjelmistoon, päätelaitteeseen, tietojärjestelmään, radiolähettimeen, varavoimalaitteeseen taikka näiden osiin tai lisävarusteisiin, jos luovutus on välttämätön yhteiskunnan elintärkeiden toimintojen ylläpidossa käytettävien verkko- ja viestintäpalveluiden toiminnan turvaamiseksi.[22]

Valtiovarainministeriö voi määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä. Valtiovarainministeriön ohjaus ei koske kuitenkaan puolustusvoimien, rajavartiolaitoksen, poliisin, pelastusviranomaisten ja hätäkeskusten toiminnallisia tietojärjestelmiä.[23]

Väestön tiedonsaannin turvaamiseksi ja viranomaisten viestinnän yhteensovittamiseksi poikkeusoloissa valtionhallinnon viestinnän välitön johto kuuluu **valtioneuvoston kanslialle**. Valtioneuvoston asetuksella voidaan tarvittaessa perustaa Valtion viestintäkeskus. Valtioneuvoston kanslia ja Valtion viestintäkeskus voivat antaa viestinnän sisältöä koskevia määräyksiä valtionhallinnon viranomaisille. Poikkeusoloissa valtioneuvoston kanslia ja Valtion viestintäkeskus voivat velvoittaa valtioneuvoston alaisen viranomaisen tai kunnallisen viranomaisen omassa viestinnässään julkaisemaan tietynsisältöisen viestin tai kieltää tietynsisältöisen viestin julkaisemisen.[24]

2.4 Euroopan unionin asettamia vaatimuksia

Euroopan komissio antoi yhdessä ulko- ja turvallisuuspolitiikan korkean edustajan kanssa 7.2.2013 tiedonantona Euroopan unionin kyberturvallisuusstrategian, ”Avoin, turvallinen ja vakaa verkkoympäristö.” Kyberturvallisuusstrategian tarkoituksena on esittää EU:n kattava visio siitä, miten verkon häiriöitä ja verkkohyökkäyksiä voidaan parhaiten ehkäistä ja torjua. Erityistoimilla pyritään parantamaan tietojärjestelmien sietokykyä ja vähentämään verkkorikollisuutta sekä vahvistamaan EU:n kansainvälistä kyberturvallisuuspolitiikkaa ja -puolustusta. Strategia koostuu viidestä painopistealueesta: [25]

1. Tietoliikenneverkon vakaus
2. Tietoverkkoverkkorikollisuuden huomattava vähentäminen
3. Verkkopuolustuspolitiikan ja yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvien valmiuksien kehittäminen
4. Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen
5. Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU:n keskeisten arvojen edistäminen.

Tietoliikenneverkon vakauden osalta strategia edellyttää, että julkisten viranomaisten ja yksityisten toimijoiden tulee parantaa valmiuksiaan toimia tehokkaasti yhteistyössä. Saavutetusta edistyksestä huolimatta jäsenmaiden valmiudessa on edelleen puutteita. Tämän johdosta jäsenmailla tulee olla **koordinoidut mekanismit tietoturvallisuusriskien ehkäisyyn,**

[22] Valmiuslaki, 29.12.2011/1552, 63 §

[23] Ibid., 105 §

[24] Ibid., 106 §

[25] Euroopan unionin kyberturvallisuusstrategia - Avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013) 1 final, 7.2.2013

paljastamiseen ja niihin vastaamiseen yhteistyössä eri viranomaisten kesken. Kansallisten tietoturvallisuusviranomaisten tulee toimia EU-tasolla yhteistyössä unionin tietoturvallisuutta koskevan yhteistyösuunnitelman mukaisesti rajat ylittävissä tilanteissa. Lisäksi jäsenmailla tulee olla rakenteet, joiden avulla ne voivat käsitellä verkkojen sietokykyä, verkkorikollisuutta ja puolustusta, ja näiden rakenteiden avulla jäsenmaiden tulisi selvitä turvapoikkeamista. Tietojen vaihdosta jäsenmaan viranomaisten kesken ja yksityisten toimijoiden välillä tulee huolehtia.[26]

Euroopan parlamentti antoi päätöslauselman Euroopan unionin kyberturvallisuusstrategiasta 6.9.2013, todeten mm., että ”tietoverkkojen ja tietoverkkoturvallisuuden pitää muodostaa yksi EU:n ja kunkin jäsenvaltion turvallisuus- ja puolustuspolitiikan strategisista pilareista. Tarvitaan verkko- ja tietoturvan korkeaa tasoa, jotta voidaan ylläpitää yhteiskunnan asianmukaisen toiminnan edellyttämiä palveluita. Vain unionin toimielinten ja jäsenvaltioiden yhdistetty johtajuus ja poliittinen omistajuus mahdollistavat verkko- ja tietoturvan korkean tason koko unionissa ja edistävät näin yhtenäismarkkinoiden toimintavarmaa ja häiriötöntä toimintaa.”[27]

Euroopan komission tiedonannossa 13.9.2017 (EU:n resilienssin kasvattaminen kyberhyökkäysten varalta) todetaan, että ”vahva kyberresilienssi edellyttää kollektiivista ja laaja-alaista lähestymistapaa. Sitä varten rakenteiden on oltava kestävämpiä ja tehokkaampia kyberturvallisuuden edistämiseksi ja kyberhyökkäyksiin reagoimiseksi jäsenvaltioissa ja myös EU:n omissa toimielimissä, virastoissa ja elimissä. Se edellyttää myös kattavampaa ja monialaista lähestymistapaa kyberresilienssiä ja strategista riippumattomuutta rakennettaessa, vahvoja sisämarkkinoita, EU:n teknologisen valmiuden mittavia parannuksia ja osaavien asiantuntijoiden paljon suurempaa määrää. Keskeistä on hyväksyä yleisesti, että **kyberturvallisuus on yhteinen yhteiskunnallinen haaste**, jotta hallinnon, talouden ja yhteiskunnan eri kerrokset saadaan osallistumaan. Päätelmien mukaan EU:n varautuminen kyberuhkiin on keskeistä sekä digitaalisten sisämarkkinoiden että turvallisuus- ja puolustusunionin kannalta. Euroopan kyberturvallisuuden tehostaminen ja sekä siviili- että sotilaskohteisiin kohdistuviin uhkiin puuttuminen on välttämätöntä.”[28]

Eurooppa-neuvoston 19. lokakuuta 2017 annetuissa päätelmissä huomioitiin kyberturvallisuuspaketin aloitteet. Neuvosto hyväksyi 20. marraskuuta 2017 päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”. Neuvoston kanssa on aloitettu keskustelut ehdotetusta ”kyberturvallisuusasetuksesta”.[29]

Euroopan unionin verkko- ja tietoturvadirektiivi, eli NIS-direktiivi, annettiin heinäkuussa 2016 ja jäsenvaltioiden on otettava sen velvoitteet osaksi kansallista lainsäädäntöä viimeistään 9. toukokuuta 2018. Direktiivin tavoitteena on parantaa jäsenmaiden tietoturvaa ja sitä kautta sisämarkkinoiden toimintaedellytyksiä. Direktiivillä jäsenvaltiot velvoitetaan laatimaan kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskinäiseen yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi. Lisäksi jäsenvaltioiden on määriteltävä nk. keskeisten palveluiden tarjoajat direktiivin soveltamisalan mukaisilla toimialoilla sekä velvoitettava nämä

[26] Euroopan unionin kyberturvallisuusstrategia - Avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013) 1 final, 7.2.2013

[27] Euroopan parlamentin päätöslauselman Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö, 6.9.2013

[28] Euroopan komissio, Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle, JOIN(2017) 450 final, 13.9.2017,

[29] Komission tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle, Kahdestoista raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia, COM(2017) 779 final/2, Bryssel 18.1.2018

huolehtimaan tietoturvallisuuteen liittyvästä riskienhallinnasta ja häiriöraportoinnista. Suomessa direktiivin implementoiva hallituksen esitys parhaillaan eduskunnan käsiteltävänä.[30]

Joulukuussa 2017 annetussa hallituksen esityksessä Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanosta (HE 192/2017 vp) ehdotetaan eräille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille uusia velvoitteita tietoturvallisuuteen liittyvien häiriöiden ilmoittamisesta. Nämä velvoitteet koskisivat esimerkiksi sähkön jakelua, eräitä vesihuoltolaitoksia, merkittäviä satamia ja lentoasemia sekä liikenteen ohjaukseen liittyviä palveluita. Häiriöistä olisi ilmoitettava sektorikohtaisille valvontaviranomaisille (Trafi, ELY-keskukset, Energiavirasto).[31]

EU:n tietosuojalainsäädäntö uudistui 24.5.2016, kun yleinen tietosuoja-asetus astui voimaan. Asetus tulee sovellettavaksi ja jäsenvaltioiden on saatettava asetuksen noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset voimaan viimeistään 25 päivänä toukokuuta 2018. Asetuksen tarkoituksena on yhdenmukaistaa luonnollisten henkilöiden henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua ja varmistaa henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä.[32]

Oikeusministeriön asettama työryhmä ehdottaa, että säädettäisiin uusi henkilötietojen suojaa koskeva yleislaki, tietosuojalaki, jolla täsmennettäisiin ja täydennettäisiin Euroopan parlamentin ja neuvoston keväällä 2016 antamaa yleistä tietosuoja-asetusta. Tietosuojalailla säädettäisiin kansallisesta valvontaviranomaisesta, oikeusturvasta ja seuraamuksista sekä joistakin tietojenkäsittelyn erityistilanteista. Valvontaviranomaisen osalta työryhmä ehdottaa tietosuojavaltuutetun toimiston laajentamista tietosuojavirastoksi. Virastoa johtaisi nykytilaa vastaavasti tietosuojavaltuutettu ja sinne perustettaisiin lisäksi uusi apulaistietosuojavaltuutetun virka ja nykyinen tietosuojalautakunta lakkautettaisiin.[33]

2.5 Kyberhäiriötilanteiden hallintaan osallistuvat organisaatiot ja niiden työnjako

2.5.1 Valtioneuvoston taso

Valtioneuvoston tasolla toimivaltainen ministeriö johtaa toimintaa ja tarpeen mukaan ministeriöiden yhteistoimintaa. Ministeriöiden työn järjestäminen on keskeisesti kansliapäälliköiden vastuulla, joten kansliapäällikkökokouksen käsittely häiriötilanteen hallintaan mahdollisesti liittyvässä organisointivaiheessa voi olla tarpeellinen. Tarvittaessa valtioneuvoston yleisistunnossa ratkaistaan mahdollinen erimielisyys, minkä ministeriön vastuulle jokin asia kuuluu tai mikä ministeriö toimii laajakantoisen asian käsittelijänä. Häiriötilanteiden hallintaan liittyvän valmistelun tukena voidaan hyödyntää poikkihallinnollisia yhteistyöelimiä. Ministeriöiden toimintaa turvallisuusasioissa tukeva keskeinen yhteistyöelin on ministeriöiden valmiuspäällikkökokous. Lisäksi ministeriöissä tai keskusvirastoissa voi olla johtoryhmiä, jotka voivat häiriötilanteen hallinnan edellyttäessä kokoontua myös sidosryhmillä laajennetulla kokoonpanolla.

Valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä valmiuslain 6

[30] Euroopan parlamentin ja neuvoston direktiivi 2016/1148, Toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, 6 päivänä heinäkuuta 2016

LVM, Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti, 20.4.2017

[31] Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, HE 192/2017 vp

[32] Euroopan parlamentin ja neuvoston asetus 2016/679, Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), 27 päivänä huhtikuuta 2016

[33] http://oikeusministerio.fi/artikkeli/-/asset_publisher/tyoryhma-ehdottaa-uutta-tietosuojalakia

§:ssä tarkoitetun poikkeusolojen toteamisen ja käyttöönottoasetuksen antamisen yleinen yhteensovittaminen.[34]

Kesäkuun 6. päivänä 2017 voimaan tulleen valtioneuvoston asetuksen valtioneuvoston ohjesäännön muuttamisesta mukaan valtioneuvoston yleisistunto käsittelee ja ratkaisee valmiuslain (1552/2011) 3 §:ssä tarkoitettujen poikkeusolojen toteamisen ja poikkeusoloista johtuvien, kansainvälisten ihmisoikeusvelvoitteiden noudattamista koskevien ilmoitusten antamisen.[35]

Ministeriöiden ja niiden hallinnonalojen tulee tunnistaa kriittinen infrastruktuurinsa, niiden kriittisyys, analysoida riskinsä ja haavoittuvuutensa, varmistaa tiedonkulku yhteistyökumppaneiden kanssa ja määrittää kyberturvallisuustehtäviä toteuttavat varautumistehtävänsä. Näitä ovat muun muassa ennakoivat, torjuvat ja palauttavat toimet. Laadittuja suunnitelmia päivitetään ja harjoitellaan säännöllisesti. Kokonaisriskienhallinta edellyttää myös yhteiskunnan elintärkeiden toimintojen näkökulmasta kriittiset tietojärjestelmien priorisointia, näiden säännöllistä auditointia ja itsearviointia riskienarvioinnilla sekä kolmansien osapuolten toteuttamana. Tunnistettuihin riskeihin reagoidaan asianmukaisesti ja ne saatetaan hyväksyttävälle tasolle. Hallinnonalojen yhteistyö ja tehtävien koordinointi ovat erityisen tärkeitä, jotta vastuut olisivat selvillä.[36]

Turvallisuuskomitea hyväksyi kokouksessaan 10.2.2014 ministeriöiden kyberturvallisuustehtävät. Tehtävien määrittäminen oli osa vuoden 2013 kyberturvallisuusstrategian toimeenpanoa. Strategian mukaisesti kukin hallinnonala on määrittänyt vastuita ja tehtäviä omista lähtökohdistaan.[37]

2.5.2 Turvallisuuskomitea

Puolustusministeriön yhteydessä toimiva Turvallisuuskomitea on kokonaisturvallisuuteen liittyvä ennakoivan varautumisen pysyvä ja laajapohjainen yhteistoimintaelin. Sen tehtävänä on avustaa valtioneuvostoa ja ministeriöitä. Turvallisuuskomitea toimii tarvittaessa yhteiskunnan eri häiriötilanteissa asiantuntijaelimenä. Turvallisuuskomitea vastaa yhteiskunnan turvallisuusstrategiasta, joka yhteen sovittaa valtion, kuntien, järjestöjen ja elinkeinoelämän varautumista eri turvallisuustilanteissa. Komitea seuraa ja yhteen sovittaa kyberturvallisuusstrategian toimeenpanoa.[38]

Turvallisuuskomitean tehtävänä on:

- Avustaa valtioneuvostoa ja sen ministeriöitä kokonaisturvallisuuden hallintaan tähtäävässä varautumisessa ja varautumisen yhteen sovittamisessa;
- Seurata ja arvioida Suomen turvallisuus- ja puolustuspoliittisen ympäristön ja yhteiskunnan muutosten vaikutuksia kokonaisturvallisuuden järjestelyihin;
- Seurata hallinnon eri alojen ja tasojen toimia kokonaisturvallisuuteen liittyvän varautumisen järjestelyjen ylläpitämiseksi ja kehittämiseksi;
- Sovittaa tarvittaessa yhteen laajoja ja tärkeitä varautumista koskevia asiakokonaisuuksia, kuten valtakunnallisen varautumisen yhteensovittaminen sekä yhteistyömuotojen, toimintamallien, tutkimuksen ja harjoitustoiminnan kehittäminen.

[34] Valtioneuvoston ohjesääntö, 3.4.2003/262, luku 3

[35] Valtioneuvoston asetus valtioneuvoston ohjesäännön muuttamisesta, 333/2017, 1.6.2017, 3 §

[36] Ministeriöiden kyberturvallisuustehtävät, 10.2.2014

[37] Ibid.

[38] http://www.turvallisuuskomitea.fi/index.php/fi/turvallisuuskomitea

Komitea voi tehtävänsä toteuttamiseksi antaa lausuntoja ja tehdä aloitteita kokonaisturvallisuutta koskevissa asioissa ja ennakoivaa varautumista koskevien laajojen ja tärkeiden asiakokonaisuuksien yhteensovittamista koskevista kysymyksistä.[39]

2.5.3 Valtiovarainministeriö

Valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä ja valtionhallinnon tietoturvallisuuden ohjauksesta sekä ohjaa tietohallinnon kehitystä valtion- ja kunnallishallinnossa, tukenaan laki julkisen hallinnon tietohallinnon ohjauksesta. Valtiovarainministeriön tehtävänä on lain mukainen julkisen hallinnon viranomaisten tietohallinnon yleinen ohjaus.[40]

Valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta.[41]

Valtioneuvosto antoi 16.11.2017 asetuksen Väestörekisterikeskuksen eräistä tehtävistä. Digitalisaatiota tukevia asiantuntijatehtäviä kootaan Väestörekisterikeskukseen 1.1.2018 alkaen. Asetuksen avulla valtiovarainministeriö haluaa kehittää toiminnan digitalisaation toimeenpanoa hallinnonalallaan siten, että valtiovarainministeriö keskittyy jatkossa selkeämmin strategisiin sekä linjaaviin tehtäviin ja Väestörekisterikeskus toimeenpaneviin ja kehittäviin tehtäviin. Jatkossa Väestörekisterikeskus valmistelee ja kehittää julkisen hallinnon tietohallintoa, tiedonhallintaa, digitaalista turvallisuutta ja sähköistä asiointia koskevia menetelmiä, arkkitehtuurikuvauksia, suosituksia ja ohjeita. Lisäksi Väestörekisterikeskus tarjoaa näitä koskevia asiantuntijapalveluja sekä kokoaa yleistä tilannekuvaa. Valtiovarainministeriöstä siirtyvät tehtävät koskevat JHS- ja VAHTI-toimintaa sekä hankearviointia ja kokonaisarkkitehtuurimenetelmän kehittämistä. Valtorista siirtyvät Valtorin ulkopuolisten konsulttien tuottamat tietoturvallisuuden asiantuntijapalvelut.[42]

VAHTI toimii julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTI edistää myös julkishallinnon toiminnan digitalisaatiota huolehtimalla tarkoitustenmukaisen turvallisuuden vaatimuskehikon laatimisesta ja ylläpitämisestä. Tähän kuuluvat myös turvallisuuteen sekä ICT-toiminnan jatkuvuuteen liittyvien tarkastukset, hyväksynnät ja arvioinnit sekä tieto- ja kyberturvallisuusharjoitustoiminnan edistäminen.[43]

Suomen Erillisverkot -konserniin kuuluvan Tietoliikennepalvelut - Virven ohjaus siirtyi 31.12.2017 sisäministeriöstä valtiovarainministeriön JulkICT-osastolle. Muutoksella Virve-palvelujen ohjaus liitetään osaksi olemassa olevaa valtiovarainministeriön turvallisuusverkkotoiminnan ohjausta, joka Erillisverkoissa on kohdistunut aiemmin Tietoliikennepalvelut - Stuven toimintaan. Lisäksi muutoksella varaudutaan tulevaisuuden viranomaispalvelujen ja viranomaisviestintätoimintamallien kehittämiseen.[44]

Valtori

[39] Valtioneuvoston periaatepäätös kokonaisturvallisuudesta, Helsinki 5.12.2012

[40] Valtioneuvoston asetus valtiovarainministeriöstä, 26.6.2003/610

[41] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, 1406/2011, 5§

[42] http://vm.fi/artikkeli/-/asset_publisher/digitalisaatiota-tukevia-asiantuntijatehtavia-siirretaan-vaestorekisterikeskukseen-1-1-2018-alkaen

[43] http://vm.fi/vahti

[44] http://vm.fi/artikkeli/-/asset_publisher/valtiovarainministerio-ohjaa-jatkossa-viranomaisverkko-virvea

Valtion tieto- ja viestintätekniikkakeskus Valtori on valtiovarainministeriön hallinnonalalla toimiva palvelukeskus ja valtion virasto. Valtori tuottaa valtionhallinnon toimialariippumattomat ICT-palvelut. Sen tavoitteena on, että palvelut tuotetaan asiakkaan tietosuojan ja tietoturvan vaatimukset huomioiden. Palveluiden tuottamisessa huomioidaan valtion hallinnon turvallisuuden ja varautumisen erityistarpeet.[45]

Valtorin TUVE-yksikkö tuottaa laissa julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) nimetyille valtion virastoille ja laitoksille korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja sekä integraatiopalveluja. TUVE on valtion omistuksessa ja hallinnassa oleva viranomaisverkko, johon kuuluu viestintäverkko, siihen liittyvät laitetilat ja laitteet sekä yhteiset tieto- ja viestintätekniset palvelut. Turvallisuusverkolla mahdollistetaan jokapäiväinen työskentely sekä operatiivisessa toiminnassa että hallinnollisissa tehtävissä. Palvelut ovat käytettävissä koko valtakunnan alueella ja niitä voidaan käyttää myös kansainvälisissä tehtävissä. Turvallisuusverkon verkko- ja infrastruktuuripalveluja tuottaa valtion kokonaan omistaman Suomen Erillisverkot Oy:n (ERVE) tytäryhtiö Suomen Turvallisuusverkko Oy (STUVE).

TUVE-palveluiden käyttäjiä ovat valtion ylimmän johdon ja ministeriöiden lisäksi valtion yleisen järjestyksen ja turvallisuuden, pelastustoiminnan, meripelastustoiminnan, rajaturvallisuuden, hätäkeskustoiminnan, maahanmuuton, ensihoitopalvelun sekä maanpuolustuksen kannalta keskeiset viranomaiset. Turvallisuusverkko varmistaa turvallisuusviranomaisten tietoliikenteen käytettävyyden ja suojauksen sekä viestinnän jatkuvuuden ja häiriöttömyyden kaikissa turvallisuustilanteissa.[46]

2.5.4 Liikenne- ja viestintäministeriö

Liikenne- ja viestintäministeriö huolehtii käyttäjien tarpeita vastaavista toimivista, turvallisista ja edullisista liikenne- ja viestintäyhteyksistä ja palveluista Suomessa. Ministeriö valmistelee toimialaansa liittyvät poliittiset ja strategiset linjaukset ja lainsäädännön sekä ohjaa hallinnonalansa virastojen ja laitosten toimintaa.

Liikenne- ja viestintäministeriön alainen **Viestintävirasto** huolehtii operatiivisella tasolla siitä, että Suomessa on monipuoliset, toimivat ja turvalliset viestintäyhteydet. Viestintävirasto ja erityisesti sen osana toimiva kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Se tuottaa tilannekuvaa tietoturvallisuuden ilmiöistä ja tiedottaa niistä sekä toimii tietoliikenneturvallisuusviranomaisena. Viestintäviraston tehtävänä on valvoa tietoyhteiskuntakaaren sekä sen nojalla annettujen säännösten ja määräysten noudattamista. Nämä säännökset koskevat muun muassa:

- Viestinnän luottamuksellisuutta ja yksityisyyden suojaa
- Viestintäverkkojen ja viestintäpalvelujen laatuvaatimuksia
- Tietoturvaa ja häiriöiden hallintaa sekä häiriöistä ilmoittamista
- Varautumista

Lisäksi Viestintävirasto toimii määrättynä turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena (NCSA, National Communications Security Authority), joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista

[45] http://www.valtori.fi/fi-FI/Tietoa_Valtorista

[46] http://www.valtori.fi/fi-FI/Palvelut/TUVE-palvelut

Sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi, niihin kohdistuvien tietoturvauhkien torjumiseksi ja yhteiskunnan elintärkeiden toimintojen turvaamiseksi poikkeusoloissa työ- ja elinkeinoministeriö voi liikenne- ja viestintäministeriön esityksestä perustaa elinkeino-, liikenne- ja ympäristökeskuksiin alueellisia tietojärjestelmäalan valmiusyksiköitä. Tietojärjestelmäalan valmiusyksiköitä johtaa ja valvoo Viestintävirasto. [47]

Tietojärjestelmäalan valmiusyksikön tehtävänä on:

1) Pitää yhteyttä läänien johtokeskuksiin tai niiden osiin, puolustusvoimien alueorganisaatioon ja muihin alueellisiin viranomaisiin sekä alueen yrityksiin ja yhteisöihin;

2) Sovittaa alueellisesti yhteen liikenne- ja viestintäministeriön sekä Viestintäviraston tämän lain nojalla antamien määräysten ja päätösten täytäntöönpanoa;

3) Koota ja ylläpitää alueellista tilannekuvaa verkko- ja viestintäpalveluiden tarjontaan ja käyttöön vaikuttavista asioista; ja

4) Tiedottaa verkko- ja viestintäpalveluiden tarjonnassa tai käytössä tapahtuvista muutoksista.

Liikenne- ja viestintäministeriö on pyytänyt lausuntoja luonnoksen hallituksen esitykseksi Liikenne- ja viestintäviraston perustamisesta. Esityksessä ehdotetaan, että Liikenteen turvallisuusvirasto Trafi, Viestintävirasto (Kyberturvallisuuskeskus) sekä Liikenneviraston tietyt toiminnot yhdistettäisiin uudeksi virastoksi, Liikenne- ja viestintävirastoksi. Uusi virasto aloittaisi toimintansa 1.1.2019. Esityksen mukaan ” Tietoliikenteen, tietojärjestelmien, viestinnän ja liikennejärjestelmän toimintavarmuus on nykyaikaisen yhteiskunnan häiriöttömän toiminnan ja turvallisuuden välttämätön edellytys. Liikenteen- ja viestinnän viranomaistoimintojen yhdistämisellä vahvistetaan osaltaan yhteiskunnan huolto- ja toimintavarmuutta kokoamalla virastojen varautumistehtävät yhteen. Tämä vahvistaa varautumisen tehtäväkokonaisuuden johtamista ja mahdollistaa sen laajemman arvioimisen ja resurssien kohdentamisen varautumisen kannalta keskeisiin kokonaisuuksiin, kuten kyberturvallisuuteen.”[48]

2.5.5 Huoltovarmuuskeskus

Kansallinen kyberturvallisuuden johtaminen edellyttää kiinteää yhteistoimintaa kriittisen infrastruktuurin toimijoiden kanssa (PPP-yhteistyö). Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Jatkuvuudenhallinnan toimenpiteillä avulla organisaatio ennalta suunnitelluilla ja toteutetuilla järjestelyillä ja johtamismalleilla hallitsee erilaiset toimintaansa uhkaavat häiriötilanteet.[49]

Huoltovarmuuskeskuksen vuonna 2016 käynnistämän Kyber 2020 -ohjelman tavoitteena on parantaa suomalaisen yhteiskunnan kykyä torjua kyberuhkia sekä toipua vaurioista.

[47] Valmiuslaki, 29.12.2011/1552, 66 §

[48] https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0246e40f-4e8a-46d4-81fb-6b255600b34b

[49] https://www.huoltovarmuuskeskus.fi/organisaatio/

Ohjelmaan kuuluu konkreettisia toimenpiteitä, jotka parantavat huoltovarmuusorganisaation kriittisten yritysten kyberturvallisuutta. Ohjelman seitsemän keskeistä teemaa: [50]

1. Ohjelman ohjaus ja seuranta
2. Luottamus kyberriskien hallintaan
3. Kyberosaaminen ja kyvykkyydet
4. Kansallinen havainnointikyky
5. Viestintä, tilannekuva ja tiedonvaihto
6. Kansainvälinen yhteistyö
7. Tulevaisuuden huomioiminen

2.5.6 Tietoturvasta vastaavat muut viranomaiset

Kansainvälisten tietoturvavelvoitteiden kokonaisvastuu on **ulkoasiainministeriöllä.** Se toimii kansallisena turvallisuusviranomaisena (NSA, National Security Authority), joka:

- Ohjaa kansallista toimintaa
- Vastaa kansainvälisten turvallisuussopimusten valmistelusta
- Ohjaa ja valvoo, että kansainväliset erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti.

Puolustusministeriö, suojelupoliisi ja pääesikunta ovat niin sanottuja määrättyjä turvallisuusviranomaisia (DSA, Designated Security Authority).

Tietosuojavaltuutettu valvoo henkilötietojen käsittelyä. Tietosuojavaltuutetun tehtävänä on käsitellä ja ratkaista henkilötietojen ja luottotietojen käsittelyä koskevat asiat siten kuin henkilötietolaissa ja luottotietolaissa säädetään. Hänen ensisijainen tehtävänsä on vaikuttaa ennakkoon rekisterinpidon lainmukaisuuteen, kehittää hyvää tietojenkäsittelytapaa ja ehkäistä tietosuojaloukkausten tapahtumista. Valmisteilla oleva uusi henkilötietojen suojaa koskeva yleislaki, tietosuojalaki määrittelee uudelleen toiminnan organisointia. Asiaa valmistellut työryhmä ehdottaa tietosuojavaltuutetun toimiston laajentamista tietosuojavirastoksi.[51]

2.6 Kyberturvallisuuden strategisen johtamisen analyysi tutkimuksen perusteella

2.6.1 Tutkimuksen lähtökohta

Analyysi toteutettiin asiantuntijahaastatteluin etsimällä vastauksia kysymyksiin:

- Mikä on valtionhallinnon kyberturvallisuuden johtamisen rakenne ja
- Mitä on kyberturvallisuuden strateginen johtajuus ja miten sitä toteutetaan kokonaisturvallisuuden vastuumallissa?

Tutkimuskysymysten ja tutkimuksen jäsentelyn avuksi teemoiksi valittiin 1) mikä on kyberturvallisuuden strategisen johtamisen nykytila, 2) mitä tietoa käytetään päätöksenteon perustana ja 3) miten kyberturvallisuuden strateginen johtaminen tulisi järjestää tulevaisuudessa

[50] Räsänen Erkki. Varautuminen sopimuksin kyberturvallisuusuhkiin, 14.4.2016

[51] http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat.html

2.6.2 Kyberturvallisuuden strategisen johtamisen määritelmä

Kyberturvallisuuden strategisen johtamisen tavoitteena on osaltaan vastata kyberturvallisuusselvityksessä keväällä 2017 havaittuun tarpeeseen strategisen johtajuuden selkeyttämisestä.[52] Johtamisella varmistetaan jatkossa kyberturvallisuusstrategian päivitetyssä toimeenpano-ohjelmassa esitettyjen tavoitteiden saavuttaminen.[53] Kokonaisturvallisuuden haasteet muun muassa nykyisten johtamisrakenteiden ja toiminnan mittaamisen osalta on tunnistettu ja otettu huomioon tutkimuksen aikana.

On tarpeellista huomioida, että **strateginen johtajuus**[54] **ei ole yksiselitteinen käsite.** Se voidaan määritellä ja ymmärtää monella tavalla. Myös **strategisen ja operatiivisen johtamisen ”rajat” eivät kaikissa tilanteissa ole kyberturvallisuuden johtamisessa aina selkeät** vaan ajoittain vaikeasti (jopa tarpeettomasti) erotettavissa toisistaan. Strategisen johtajuuden määrittelyn moninaisuus ja rajauksen vaikeuden tekeminen operatiiviseen toimintaan nousivat esille myös muun muassa tähän tutkimukseen tehdyissä haastatteluissa sekä kansainvälisesti vertailluissa referenssimaissa. Kyberturvallisuuden strategista johtamista kuvattiin haastatteluissa esimerkiksi seuraavalla tavalla: ”*strateginen johtaminen on jonkin ilmiön johtamista ylätasolla siten, että johtamisessa pyritään mahdollisimman kokonaisvaltaisesti määrittelemään pitkän aikavälin visio ja tavoitteet*”.

Kyberturvallisuus on osa yhteiskunnan ja yritysten turvallisuutta, ja tärkeässä roolissa pohdittaessa organisaation strategisia päämääriä digitalisoituvassa yhteiskunnassa. Kyberturvallisuuden strategisen johtamisen kuvattiin tutkimusaineistossa usein olevan valtion kyvykkyyksien ja elintärkeiden toimintojen turvaamista, ja tämän myötä myös yksityinen sektori ja kolmas sektori pystyvät rakentamaan toimintaansa toimivien ja turvallisten tietoverkkojen varaan. Tutkimusaineiston perusteella kyberturvallisuuden strategisen johtamisen tärkeimmäksi tehtäväksi määrittyy vision ja kansallisen ajattelutavan luominen, jotka tunnistetaan kaikilla kyberturvallisuustyöhön osallistuvilla toimijatasoilla, ja mikä ohjaa toimintaa niin normaali- kuin häiriötilanteissa.

Strateginen johtaminen on Suomen kyberturvallisuusstrategian – ja suomalaisen kyberturvallisuuden – **pitkän tähtäimen toimeenpanoa**. Strateginen johtaminen vie yhteiskuntaa kohti asetettua tavoitetilaa. Strategisen johtajuuden toimeenpanotehtävän perustana on digitaalisen toimintaympäristön turvaamisesta johdettujen **tavoitteiden tunnistaminen ja asettaminen**.

Toiseksi strateginen johtaminen **yhteensovittaa, osallistaa ja koordinoi eri toimijoiden yhteistyötä** kyberturvallisuuteen liittyvässä toiminnassa ja varautumisessa. Kyberturvallisuuden ollessa laaja yhteiskunnallinen ilmiö ja sitoessaan hyvin monia toimijoita yhteen, korostuu yhteistyön koordinointi niin normaalioloissa kuin häiriö- ja poikkeustilanteissa[55]. Toiminnassa korostuu riittävät edellytykset päätöksentekoon sekä selkeästi määriteltyihin toimivaltuuksiin.

Kolmanneksi kyberturvallisuuden strateginen johtaminen, kyberturvallisuuden ollessa strateginen asia suomalaisessa yhteiskunnassa, on läheisessä **vuorovaikutuksessa niin poliittiseen päätöksentekoon kuin operatiiviseen toimintaan.** Strategiseen johtamiseen yhdistyy myös suomalaisen **kyberturvallisuusidentiteetin vahvistaminen** niin kansallisesti kuin kansainvälisesti. Kyberturvallisuusidentiteettiin yhdistyy myös **kansallisesta**

[52] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017.

[53] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020.

[54] Ks. Strategisen johtajuuden määritelmistä mm. Juuti Pauli, Luoma Mikko, Strateginen johtaminen, Kustannusyhtiö Otava, Keuruu 2009, s, 24.27

[55] Normaaliaikojen ja poikkeusolojen vakavat ja laajamittaiset kyberhäiriötilanteet tarkoittavat uhkaa tai tapahtumaa, joka vaarantaa yhteiskunnan turvallisuutta, toimintakykyä tai väestön elinmahdollisuuksia ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää.

kyberomavaraisuudesta huolehtiminen niin kotimaisten tuote- ja palveluratkaisuiden kuin osaamisen ja tutkimuksen osalta. Kotimainen ja kansainvälinen **viestintä on tärkeässä roolissa** luotaessa suomalaista kyberturvallisuusidentiteettiä sekä luottamukseen perustuvaa uskottavuutta. Useat kansainväliset mittarit mittaavatkin juuri kyberturvallisuusidentiteettiä ja -kyvykkyyttä. Yksi strategisen johtamisen tavoite onkin kansallisen kyberkyvykkyyden (kokonaisuudessaan) tilan **jatkuva seuraaminen** nykytilan tason ymmärtämiseksi ja **kyvykkyyden kehittämiseksi**.

Neljänneksi strategisella johtamisella **luodaan johdonmukaisuutta ja jatkuvuutta** Suomen niin kansalliseen kuin kansainväliseen yhteistoimintaan. Strateginen johtaminen kokoaa kaikki käytettävissä olevat voimavarat yhteen **asetettujen tavoitteiden saavuttamiseksi.**

Tiivistetysti: ***Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista.***

2.6.3 Kyberturvallisuuden strategisen johtamisen nykytilan analyysi tutkimuksen perusteella

Kokonaisturvallisuudessa tai yleisimmin turvallisuuden määrittelyssä tulevat nykyisin yhä vahvemmin esille geopoliittiset ulottuvuudet ihmisten, esineiden ja asioiden siirtyessä nopeasti yli valtioiden rajojen. Kybertoimintaympäristössä suvereenien valtioiden alueellinen geopolitiikka on murroksessa. Kansainvälisten siirtymien, globaalivirtojen, luotettavuus ja turvallisuus riippuvat siitä, miten kybertoimintaympäristössä toimitaan.[56]

Valtioneuvoston kanslia vastaa valtion ylimmän johdon toimintaedellytysten turvaamisesta. Valtioneuvoston kanslia avustaa pääministeriä valtioneuvoston yleisessä johtamisessa ja ylläpitää valtionjohdon tilannekuvaa. Valtioneuvoston kanslia kerää salassapitosäädösten estämättä toimivaltaisilta viranomaisilta välttämättömiksi arvioidut tiedot turvallisuustapahtumista, analysoi kerätyn tiedon ja edelleen jakaa yhteen sovitettua tilannekuvaa tasavallan presidentille, valtioneuvostolle ja viranomaisille. Strategisen tason tilannekuva on päätöksenteon ja kriisijohtamisen perusta.[57] Haastateltujen asiantuntijoiden mukaan hallinnonalojen sisällä laaditaan valtioneuvoston asettamien ylimpien strategisten tavoitteiden perusteella ministeriön strategia, jonka tavoitteet virastot panevat täytäntöön operatiivisessa toiminnassaan.

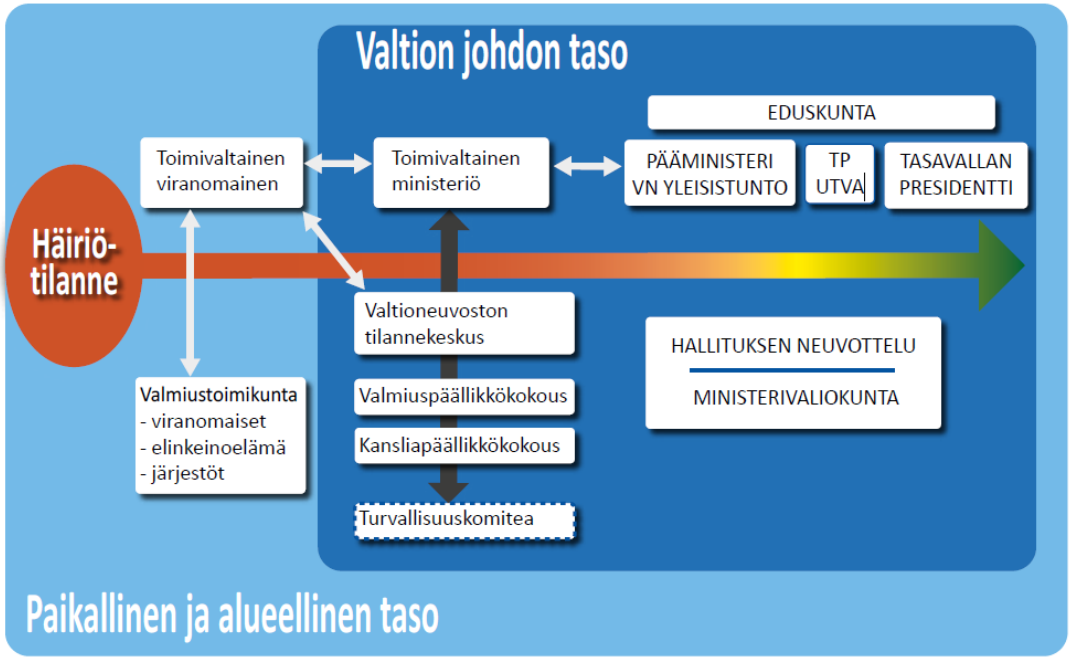
Valtioneuvoston asettaman Hallbergin komiteamietinnössä korostettiin ”normaalien toimivaltasuhteiden säilyttämistä varautumisessa ja häiriötilanteiden hallinnassa.[58] Yhteiskunnan turvallisuusstrategiassa 2017 on esitetty häiriötilanteiden hallinnan ja johtamisen yleinen toimintamalli, jossa kuvataan valtion ylimmän johdon sekä paikallisen ja alueellisen tason johtamisen välisiä suhteita (kuva 1). Valtioneuvoston kanslia on merkittävässä roolissa viranomaisten toiminnan yhteensovittamisessa ja valtion johdon päätöksenteon tukemisessa.[59]

[56] Aaltola, Käpylä, Mikkola & Behr, 2014.

[57] Yhteiskunnan turvallisuusstrategia, 2017.

[58] Valtioneuvoston asettaman komitean mietintö 22.12.2010.

[59] Yhteiskunnan turvallisuusstrategia, 2017



Kuva 1. Häiriötilanteiden hallinnan ja johtamisen yleinen toimintamalli[60]

Keväällä 2017 julkaistun kyberturvallisuusselvityksen mukaan Suomesta puuttuu nykyisin pitkän aikavälin poliittinen tahtotila ja johtamismalli siitä, kuinka maata tulisi rakentaa kyberturvallisena digiyhteiskuntana. Tämän seurauksena hallinnonalat taas toimivat siiloissaan ja määrittelevät tavoitteensa ja toimintatapansa omista lähtökohdistaan. Tutkimuksissa ja selvityksissä on todettu, että vakavien ja laaja-alaisten hyökkäysten torjuntakyky on nykyisin heikko, johtuen havainnointikyvyn ja tilannekuvan puutteista sekä selkeän kansallisen johtamismallin puutteesta. [61]

Keskeinen haaste yhdistyy johtamiseen erityisesti laaja-alaisissa ja vakavissa kyberhäiriötilanteessa ja siihen yhdistyvissä toimivaltuuksissa. Käytännön toiminnasta kyberhäiriötilanteissa ei ole olemassa selkeää toimintamallia ja resursseja. Asiantuntijahaastattelujen perusteella meiltä puuttuu tehokas toimintamalli resursseineen nopeita päätöksiä vaativissa kyberhäiriötilanteissa määritellä, mikä on kaikkein kriittisintä kriittisen infrastruktuurin toimintakyvyn ylläpitämisessä. Ts. mihin kansalliset resurssit kyberhäiriötilanteessa ensisijaisesti ohjataan tai mikä/kenen yhteiskunnan elintärkeiden toimintojen kannalta kriittiset järjestelmät nostetaan ensiksi pystyyn.[62]

Valtiotalouden tarkastusviraston tarkastuskertomuksen mukaan laajavaikutteisen kyberloukkaustilanteen operatiivista johtamista ei ole määritelty. Tämä heijastuu myös strategiselle tasolle. Useampaan eri hallinnonalaan kohdistuvien laajojen hyökkäysten vastatoimia ei ole suunniteltu ja vastuutettu. Kyberloukkauksiin vastaaminen noudattaa työn- ja vastuunjakoa valtioneuvoston ohjesäännössä. Tulkinnanvaraisissa tilanteissa kyberloukkausten käsittely on selvitetty ministeriöiden välisissä neuvotteluissa. Toimivaltaisen viranomaisen määrittelemineen voi olla hankalaa. Ministeriöiden välille saattaa syntyä eturistiriitoja esimerkiksi alas ajettavan palvelun suhteen. Vastuu johtamisesta on viimekädessä valtioneuvostolla.[63]

[60] Ibid.

[61] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[62] Ibid.

[63] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomus: Kybersuojauksen järjestäminen, 2017

Haasteet kyberturvallisuuden johtamisessa ovat erityisesti strategisen johtamisen tasolla. Nykytilan haasteita kuvaavat useissa tutkimushaastattelussa esille tuodut näkemykset (1) selkeistä ja konkreettisista toimenpide-esityksistä kyberturvallisuuden strategisen johtamisen rakenteiksi sekä (2) asian tärkeyden ja vaadittavien toimenpiteiden nostamisen esille rehellisesti ja suorasanaisesti. Eräässä haastattelussa todettiin: ”toivottavasti kukaan (haastatteluun osallistuva asiantuntija) ei ole sitä mieltä, että meidän tulisi jatkaa samalla tavalla kuin ennenkin”. Toisaalta ratkaisumalleja strategisen johtajuuden toteuttamiseksi tuotiin haastatteluissa esille useita erilaisia.

Strategisen johtamisen tasolla on kaksi perusongelmaa:

(1) Toimijoita on paljon ja kyberturvallisuuden strateginen johtaminen on tämän vuoksi hajallaan ilman selkeää johtajuutta. Ministeriöt toteuttavat itsenäisesti kyberturvallisuuden strategista johtamista omilla sektoreillaan, jolloin kokonaisvaltainen strateginen johtajuus puuttuu ja toiminta tapahtuu pitkälti hallinnonaloittain.

(2) Kyberturvallisuuden strategisen johtamisen tasolla ei ole tehokkaasti toimivaa yhteistyörakennetta. Tämä yhdistyy osittain ensimmäiseen kohtaan. Ministeriöt tarkastelevat kyberturvallisuutta omien tarpeidensa perusteella, jolloin laajempi yhteiskunnallinen näkökulma häviää ja aiemmin mainitut (luku 2.6.2) strategisen johtamisen määritelmälliset tavoitteet jäävät saavuttamatta.

Tutkimukseen tehtyjen haastatteluiden perusteella kyberturvallisuuden strategisen johtajuuden tulee olla tunnistettavissa, jotta hallinnonaloille ei synny tilannetta, jossa johtajaa ei löydy ja tarvittavia toimenpiteitä ei kyetä tekemään. Nykytilassa kyberturvallisuuden strategisen johtamisen oletetaan hoituvan itsestään, vaikka näin ei välttämättä tapahdu. Yhteiskunnan eri toimijoiden välisiä keskinäisriippuvuussuhteita ei ole nykytilassa kuvattu. Organisaatioiden ja toimintojen suhteiden kuvaamisen kautta on mahdollista ennakoida päätösten vaikutuksia yhteiskunnan toimintoihin. Asiantuntijoiden mukaan keskinäisriippuvuuden suhde tulisi avata tutkimuksen keinoin mahdollisimman nopeasti. Yhteistyötahojen ja tietoa tuottavien toimijoiden sekä koko kyberhavaintojärjestelmän tunnistaminen olisivat tärkeitä ensimmäisiä askelia kohti todellista koko yhteiskunnan läpileikkaavaa turvallisuusstrategiaa. Organisaatioiden rajat ylittävän koordinointielimen/-toiminnon osalta tulee tutkimushaastatteluiden perusteella käyttää harkintaa, jottei todellinen rooli jää näennäiseksi ja tarpeetonta lisätyötä aiheuttaen.

Aiemmassa tutkimuksessa nousi esille erityisesti näkemys tarpeesta keskittää Suomen kyberturvallisuuden johtaminen valtioneuvoston kansliaan.[64] Haastateltujen asiantuntijoiden mukaan valtioneuvoston kanslian suora keskusteluyhteys ja rooli valtion ylintä johtoa tukevana toimintona luovat VNK:lle muita hallinnonaloja tai organisaatioita paremman mahdollisuuden strategiseen johtamiseen. Nykyiseen malliin liittyy myös EU-tason kyberturvallisuusmalleja, joita VNK sovittaa yhteen kansallisten mallien kanssa. Valtioneuvoston kansliassa tehtävä kyberturvallisuustyö nivoutuu vahvasti yhteen valtioneuvostossa tehtävän kyberturvallisuustyön kanssa. Valtioneuvosto palvelee hallinnonaloja tasapuolisesti ja sovittaa yhteen hallinnonalojen välistä yhteistoimintaa. Mallit ja käytänteet, jotka suunnitellaan valtioneuvoston kansliaan ovat melko samankaltaisia kuin valtioneuvostossa. Valtioneuvoston kanslialla ei kuitenkaan ole suoraa käskyvaltaa eri ministeriöihin, jolloin toimenpide-ehdotuksia jalkautetaan neuvojen ja ohjeistuksen kautta. **Haastateltujen asiantuntijoiden mukaan nykyinen malli ei ole riittävän nopea häiriötilanteiden hallinnan osalta**. Valtiontalouden tarkastusviraston suosittaa, että ”valtiovarainministeriö määrittelee ja toteuttaa valtionhallinnon ICT-

[64] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomus: Kybersuojauksen järjestäminen, 2017

palveluiden osalta laajavaikutteisten kyberhäiriötilanteiden operatiivisen hallinta- ja johtamismallin.[65]

Kyberturvallisuuden strategisen johtamisen toiminnallisuuden kannalta on erityisen tärkeää löytää rakenteet, joilla on mahdollisuus vastata toimintaympäristön asettamiin toiminnallisiin vaatimuksiin. **Kybertoimintaympäristölle on ominaista kiihtyvä muutosnopeus, ilmiöläheisyys, kompleksisuus ja osittainen ennalta-arvaamattomuus.** Haastatteluissa nostettiin esille, että nykyisellä strategisella johtamisella ei kyetä vastaamaan kiihtyvään muutosvauhtiin. Päätösten perustana olevan tiedon, päätöksen ja päätöksen toimeenpanon muodostama silmukka kestävät nykyisin liian pitkään. ”Yhteiskunnan haavoittuvuuden lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti”.[66]

Haastateltujen asiantuntijoiden mukaan Valtioneuvoston kanslian nykyinen rooli edellyttää, että kiireellisessä kybertoimintaympäristön kriisitilanteessa tulee olla muodostettu neuvottelujen kautta yhteistyömuotoja ja -tapoja. Kiireellisissä kriisitilanteissa ei ole juuri koskaan mahdollisuutta neuvotella toimenpiteistä, vaan toimenpiteiden suorittamiseksi tulee olla mandaatti ja varautumisen aikana koetellut toimintamallit. Viestintäviraston Kyberturvallisuuskeskuksessa on olemassa vakiintuneet menetelmät poikkeamien hallintaan yhdessä yksityisen sektorin toimijoiden kanssa. Menettely ei perustu käskyvaltasuhteeseen vaan yhteistyöhön, jossa Kyberturvallisuuskeskus toimii yhteyspisteenä.

Tutkimushaastatteluiden perusteella voidaan todeta, että **strateginen johtaminen perustuu luottamuksen rakentamiseen ja sen ylläpitämiseen.** Kyberuhkien torjuminen perustuu jo nykyisin syvään luottamukseen ja yhdessä tekemiseen. Syvä luottamus on Suomessa mahdollistanut poikkeuksellisen hyvän yhteistyön yhteiskunnan eri toimijoiden välillä ja tällä yhteistyöllä on Suomessa pitkä perinne. Kyberturvallisuuskeskus on hyvä esimerkki siitä, että luottamuksella saa aikaiseksi enemmän kuin ”pakottamalla”. Kybertoimintaympäristön turvaaminen on toistaiseksi perustunut avaintoimijoiden tunnistamiseen ja toimijoiden väliseen neuvotteluun eikä niinkään kyberturvallisuuden johtamisrakenteisiin. Haastatteluissa jopa kyseenalaistettiin kyberturvallisuuden strateginen johtaminen toimintaympäristöstä johtuvien tekijöiden vuoksi. Järjestelmällinen tapa toimia tarvitaan, mutta kysymys valtionhallinnon kyberturvallisuuden strategisesta johtamisesta todettiin haasteelliseksi.

Useiden toimijoiden malli ja hallinnonalojen kyberturvallisuustyön siiloutuminen, takaavat nykyisellään sen, ettei kenellekään ole absoluuttista valtaa tai vastuuta. Strategisessa johtamisessa tulee kuitenkin löytää optimitila sille, millä oikeat toimet kyetään tekemään oikea-aikaisesti, koska koko yhteiskunnan etu on päätöksenteon keskiössä. Päätöksentekijän neutraali asennoituminen ja johtamisen (mahdollinen) hallinnonalasidonnaisuus herättivät tutkimushaastatteluissa laajaa keskustelua. Esimerkiksi, johtajuuden vieminen yksittäisen ministeriön alle saattaa viedä kyberturvallisuuden strategista johtamista kohti yksittäisen ministeriön strategisia tavoitteita kokonaisvaltaisuuden tavoittelun sijasta. Nykytilassa yksittäisen ministeriön strategiset tavoitteet voivat olla koko yhteiskunnan kyberturvallisuusstrategian kanssa ristiriidassa. Kansainväliseen yhteistoimintaan liittyy puolestaan aina poliittinen arvopohja. Yhteisen kansallisen näkemyksen koordinaatio on tärkeää, koska ”kansainvälinen kybertoimintaympäristö on miinoitettu kyberturvallisuuteen liittyvän keskustelun suhteen”.

Operatiiviselta tasolta kerätyn tiedon haasteena on usein juuri annetun palautteen vähäisyys. Operatiiviset toimijat eivät näe yhteyttä keskushallinnolle välittämänsä tiedon ja oman toimintansa välillä, mikä toisinaan aiheuttaa turhautuneisuutta ja tiedonvälityksen vähenemistä.

[65] Ibid.

[66] Suomen kyberturvallisuusstrategia ja taustamuistio, 24.1.2013.

Tiedonvälityksen vähentyminen taas aiheuttaa epätahtisuutta ja vääristymiä strategisessa päätöksenteossa.

Useissa haastatteluissa nostettiin esiin, että yhteiskunnan ja erityisesti uusien teknologioiden kehitystä ei ole ymmärretty nykyisin. Tekoälyn käyttömahdollisuudet ja sen vaikutus tulevaisuuden työhön nostettiin erityisesti esille. Strategisen johdon puuttuessa ei yhteiskunnan tai teknologioiden tunnistettuja kehityssuuntauksia kyetä täysimääräisesti viemään toiminnaksi ja uuden liiketoiminnan perustaksi. **Tutkimushaastatteluissa peräänkuulutettiin niin teknologian kehityksen kuin kyberturvallisuuden strategisen analyysin merkityksellisyyttä.** Tutkimukset rajoittuvat nykyisin liian tiukasti tutkittavien käsitteiden ja määritelmien mukaan, jolloin esimerkiksi kyberturvallisuuden merkitys osana tuotetta tai palvelua katoaa.

2.6.4 Näkemyksiä yksityisen sektorin kanssa tehtävästä kyberturvallisuustyöstä

Yksityinen sektori hoitaa nykyisin oman tehtävänsä hyvin valtiollisen kyberturvallisuuden edistämiseksi. Viranomaisten ja yksityisen sektorin välille on luotu yhteistoimintamalleja, jotka ovat kansainvälisesti vertailukelpoisia ja korkealuokkaisia. Viestintäviraston Kyberturvallisuuskeskus, Keskusrikospoliisin Kyberrikostorjuntakeskus ja Puolustusvoimien kyberoperaatiokeskus ovat tunnistettuja yhteyspisteitä valtionhallinnon suuntaan. Huoltovarmuuskeskus ja eri poolit, erityisesti digipooli, tukevat kybertoimintaympäristön tilannekuvan ylläpitämisessä. Huoltovarmuuskeskus yhdistää jo toiminnan tavoitteiden vuoksi merkittävän osan viranomaisista sekä tietotekniikka- ja tietoverkkoalan yrityksistä.[67] Yhteistyöelimistä nostettiin esille lisäksi tietoturvallisuusklusteri FISC ry. FISC kokoaa yhteen jäsenet kansallisesti merkittävistä tieto- ja kyberturvatuotteita ja -palveluita tarjoavista yksityisistä organisaatioista. FISC:n tavoitteena on kasvattaa ja kansainvälistää jäsenistön liiketoimintamahdollisuuksia, sekä edistää kyberturvaosaamisen laajamittaista hyödyntämistä yhteiskunnassa.[68]

Merkittävimpinä onnistumisena haastatteluissa tuotiin esille Viestintäviraston Kyberturvallisuuskeskuksen perustaminen. Kyberturvallisuuskeskus toimii Huoltovarmuuskeskuksen tavoin tiiviissä yhteistyössä yksityisen sektorin eri toimijoiden kanssa. CERT-toiminto tuottaa yksityiselle sektorille suoraa operatiivista tukea ja toiminnon avulla tuotetaan myös valtion eri hallinnonaloille ajantasaista tietoa valtion toimintoihin vaikuttavista loukkauksista. Hyödyt ovat jo nykyisin kiistattomia. Lainsäädännön ja Kyberturvallisuuskeskuksen toiminnan kehittämisen kautta on saavutettavissa entistä parempi kokonaiskuva tietoverkkojen turvallisuudesta. Ajantasaisempi ja kokonaisvaltaisempi tilannekuva on mahdollista saavuttaa esimerkiksi asettamalla yksityiselle sektorille vaatimuksia toiminnan järjestämisen ja raportoinnin osalta.

Suomella on haastateltujen asiantuntijoiden mukaan erinomaiset mahdollisuudet menestyä kyberturvallisuudenalalla niin valtiona kuin yritysten kasvualustana. Tämä on tunnistettu myös aiemmassa tutkimuksessa *Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen*.[69] Suomen kyberomavaraisuus ja sen puute nousivat kuitenkin vahvasti esille. Kyberomavaraisuuden nykyinen taso on tunnistettava ja tarvittavia muutoksia on tehtävä, jotta osaajia on jatkossa saatavilla. Kyberturvallisuusosaajien tarpeesta on esitetty erilaisia arvioita, mutta varovaisissakin arvioissa esitetään kymmenien tuhansien uusien osaajien tarve. Yksityisen sektorin osaaminen on elintärkeää valtionhallinnon kyberturvallisuustyössä. Valtiolla ei ole vastaavaa osaamista ja resursseja kuin yksityisellä sektorilla. Valtion ja yksityisen sektorin yhteistyötä on tiivistettävä ja julkisia hankintoja tulee hyödyntää alan osaamisen

[67] Huoltovarmuuskeskus, 2017

[68] Finnish Information Security Cluster ry (fisc.fi, 2017)

[69] VTT, Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016

vahvistamisessa.[70] Valtion ja yksityisen sektorin välillä on usein kyse tietynlaisesta vaihtokaupasta, koska tiivis yhteistyö saattaa jatkossa tuoda yksityiselle sektorille tilauksia valtion ollessa potentiaalinen ostaja.

Yksityisen sektorin merkitys ja haasteet on ymmärrettävä kyberturvallisuuden ja sen strategisen johtamisen kontekstissa. Haastateltujen asiantuntijoiden mukaan on ollut tilanteita, joissa valtionhallinnosta tai ylipäätään Suomesta ei ole löytynyt riittävää osaamista ja asiantuntemus on jouduttu hankkimaan ystävällismielisiltä mailta. Lähialueillamme on ollut myös tapauksia, joissa valtio on hankkinut yksityiseltä sektorilta palveluita ja myöhemmin kyseinen yritys on myyty kolmannelle taholle. Sensitiivisiä tietoja on yrityskaupan yhteydessä päätynyt tahoille, joille tietojen ei olisi pitänyt päätyä. Samaan yhteyteen täytyy ymmärtää myös alihankintaketjujen riskit. Tähän ei ole haastattelujen perusteella kiinnitetty riittävästi huomiota, vaikka käsiteltävät tiedot ovat olennainen osa valtionhallinnon eri toimijoiden arkea. Keskeinen haaste on vakuuttaa yksityinen ja julkinen sektori siitä, että digitaalisessa maailmassa tietoturvallisuus on aito kilpailutekijä ja tietoturvallisten tuotteiden sekä palveluiden saatavuutta tulee edistää sekä EU:ssa että globaalisti. Yksityinen sektori tulee saada tähän mukaan ja vaikuttamistyötä tulee tehdä ennen kaikkea tuotteiden ja palveluiden loppukäyttäjien näkökulmasta.

Haastateltujen asiantuntijoiden mukaan kansainvälisillä yrityksillä on nykyisin valtaa kuin kansallisvaltioilla. Kansallisen edun ja globaalisti toimivien yritysten edun välistä suhdetta on arvioitava aktiivisesti. Suomessa tulee tunnistaa arvoketjut ja oma viiteryhmämme. Ymmärrys paikastamme osana arvoketjuja tuo esille myös muiden valtioiden ja yritysten vaikuttamisyritykset.

2.6.5 Kyberturvallisuuden strateginen johtaminen tulevaisuudessa

Euroopan komissio analysoi pohdinta-asiakirjassaan kesällä 2017 tulevaisuuden uhkamaailmaa. Sen mukaan **teknologian kehitys muuttaa merkittävästi niin turvallisuuden kuin puolustuksen luonnetta.** Big data, pilviteknologia, miehittämättömät ajoneuvot ja muun muassa tekoäly mullistavat puolustussektoria vahvistaen myös siviiliteknologian merkitystä puolustusalalla. Tämän verrattain helposti saatavilla olevan teknologian käyttö mahdollistaa epätavanomaisten, valtioiden rajat ylittävien ja epäsymmetristen uhkien nopean kasvun. Näitä ovat muun muassa hybridi- ja kyberuhat, terrorismi sekä kemialliset, biologiset ja radiologiset iskut. Internetin käyttäjien määrän nopean kasvun myötä kyberrikollisuudesta ja internetin terrorikäytöstä on tullut 2000-luvulla sodankäynnin uusia muotoja.[71]

Uudet teknologiat haastavat nykyisen lainsäädännön ja tuovat mukanaan eettisiä kysymyksiä esimerkiksi kyberhyökkäyskyvykkyyden, itseohjautuvien ajoneuvojen, tekoälyn ja lisätyn todellisuuden osalta.[72] Teknologioiden myötä kybertoimintaympäristö on jatkuvassa muutoksessa, mikä haastateltujen asiantuntijoiden mukaan hankaloittaa pysyvien ja yksiselitteisten toimintamallien luomista. Oman toiminnan monimuotoistaminen, ryhmäprosessit sekä oikeanlainen tasapaino toiminnan mekaanisuuden ja orgaanisuuden välillä ovat keinoja hallita kompleksisuutta.[73]

[70] Ibid.

[71] Euroopan komissio (2017). Pohdinta-asiakirja Euroopan puolustuksen tulevaisuudesta. https://www.eduskunta.fi/FI/tiedotteet/Sivut/komission-pohdinta-euroopan-puolutuksen-tulevaisuudesta.aspx, (23.7.2017).

[72] NATO, Strategic Foresight Analysis 2017, 47.

[73] Hanén, Tom. Yllätysten edessä. Kompleksisuusteoreettinen tulkinta yllättävien ja dynaamisten tilanteiden johtamisesta, 2017. Julkaisusarja 1: Tutkimuksia nro 11. Maanpuolustuskorkeakoulu. Helsinki.

Kyberturvallisuuden strateginen johtaminen vaatii tutkimushaastatteluiden, tutkimuskirjallisuuden sekä kansainvälisen referenssimaiden analyysin perusteella toteutuakseen:

1) Toimivan lainsäädännön,
2) Riittävät toimivaltuudet,
3) Sidonnaisuuden poliittiseen päätöksentekoon,
4) Kyvykkyyden ja osaamisen sekä
5) Taloudellisia resursseja.

Tietoturvallisuudesta säädetään useissa niin julkista hallintoa kuin elinkeinoelämää koskevissa normeissa. Tietoturvariskien hallintaan liittyviä velvoitteita on hallinnon yleislaeissa (viranomaisten toiminnan julkisuudesta annettua laki, henkilötietolaki), yleisissä palveluiden laatuvaatimuksia tai turvallisuusvelvoitteita koskevissa laeissa (esimerkiksi tietoyhteiskuntakaaressa viestintäpalvelujen ja viestintäverkkojen tietoturvallisuudesta ja liikennealan laeissa liikenneturvallisuuteen liittyviä velvollisuuksia), riskienhallintaa koskevissa laeissa (esimerkiksi luottolaitosten operatiivista riskienhallintaa koskeva sääntely) sekä häiriöihin varautumista koskevissa laeissa (esimerkiksi vesihuoltolaitoksen häiriöihin varautumisvelvoite). Velvoitteiden sisältö vaihtelee. EU:n tasolla tietoturvallisuutta koskevaa sääntelyä sisältyy verkko- ja tietoturvadirektiiviin, jonka kansallinen täytäntöönpano on parhaillaan käynnissä liikenne- ja viestintäministeriössä”.

Tutkimushaastatteluissa tunnistettiin **kyberturvallisuuden strategisen johtamisen menestystekijäksi kyvykkyys johtamiseen.** Historiassa on asiantuntijoiden mukaan tapauksia, joissa päätöksiä on tehty väärin perustein ymmärtämättä sitä, miten päätökset vaikuttavat yhteiskuntaamme. Valtion poliittisen johdon ja toisaalta operatiivisesta toiminnasta vastaavien toimijoiden tulisi strategisen johtajuuden myötä olla vuorovaikutuksessa siten, että molemmat osapuolet ymmärtävät toisiaan ja toiminta on yhdensuuntaista. Asiantuntijoiden mukaan yksi johtajuuden näkökulma on, että kyberturvallisuuden ylin kansallinen johtaminen, kyberturvallisuuden strateginen johtaminen, tulee vastuuttaa ministeriölle, jolla on tosiasiassa kyky johtaa toimintaa.

Haastateltujen asiantuntijoiden mukaan Kyberturvallisuuskeskuksessa on kyvykkyyksiä, joita muualla ei ole ja tästä syystä keskuksen operatiivista roolia tulisi vahvistaa. Kyberturvallisuuskeskuksen sijoittuminen Liikenne- ja viestintäministeriön hallinnonalalle nähtiin osittain haasteellisena. Kansallisesti tulee olla olemassa keskus, joka palvelee kaikkia hallinnonaloja ja tekee kansainvälistä yhteistyötä. Toiminnan tulee kuitenkin olla selkeästi ministeriön johdettavana. Kyberturvallisuuskeskuksen kaiken toiminnan ei nähty suoranaisesti olevan liikenne- ja viestintäministeriön muuta toimintaa tukevaa. On korostettava, että Kyberturvallisuuskeskuksen hallinnollisesta sijoittumisesta esitettiin erilaisia näkemyksiä tutkimushaastatteluissa. Kyberturvallisuuskeskus on joka tapauksessa nykyisin paikka, joka yleisesti yhteiskunnassa tunnetaan ja jossa on konkreettisia toimintavalmiuksia jo olemassa. Osa haastatelluista asiantuntijoista ehdotti myös mallia, jossa kyberturvallisuuskeskus säilyisi LVM:n ohjauksessa, mutta kyberturvallisuuden strateginen johtaminen olisi sijoitettu toiselle hallinnonalalle.

Haastatteluissa nousi esille erilaisia kyberturvallisuuden strategisen johtamisen nimikkeitä, kuten ”kybertsaari” tai ”kyberkansleri”. Kyse olisi yksittäisestä henkilöstä, joka johtaisi kyberturvallisuutta strategisella tasolla ja käyttäisi ylintä päätösvaltaa muun muassa vakavissa häiriötilanteissa. Eräässä haastatteluista todettiin, että strategisen johtajuuden osalta tämä henkilö tulisi nimetä esimerkiksi ”kybervaltakunnansovittelijaksi”, koska kyseinen nimike kuvaa henkilöltä edellytettäviä ominaisuuksia. Ajatus kyberturvallisuutta johtavasta yksittäisestä henkilöstä nostettiin haastatteluissa esille myös toisesta näkökulmasta. Suomen vahvuus on

aina ollut ja on tulevaisuudessakin hallinnonalojen välinen yhteistyö sekä hallinnonalojen toiminta kaikissa oloissa omalla vastuualueellaan. Kyberturvallisuuden strategisen johdon vastuuttaminen yhdelle johtajalle nähtiin negatiivisena kehityskulkuna. Asiantuntijoiden mukaan strateginen johtajuus on yhteensovittamista, eräänlaista verkostojohtajuutta, eikä vain yhden henkilön työtä. ”Superministeriön” tai ”yksinvaltiaan” ei tässä yhteydessä arvioitu tuottavan erityistä tehokkuutta päätöksentekoon samalla tavalla kuin yhdessä luodut strategiat ja strategioiden pohjalta tehdyt yksityiskohtaisemmat toimenpideohjelmat. Tutkimushaastatteluissa nousi esille näkemys, että ”pelkillä rakenteilla ei kybertoimintaympäristön haasteita ratkaista.” Hallinnonaloilla tulee olla jatkossakin riittävä kyvykkyys rakentaa ja ylläpitää kyberturvallisuutta.

Tutkimukseen haastatellut asiantuntijat tunnistivat poikkihallinnollisen strategisen analyysin / analyysikeskuksen tarpeen. Kyberturvallisuuden strategisen johtamisen perustana olevan tiedon tulisi olla analysoitua myös strategisella tasolla ja yhteiskunnan muuta kehitystä seuraavaa. Tilannekuvan ja tilannetietoisuuden suppeahkoista käsitteistä tulisi pyrkiä kohti laajempaa tilanneymmärrystä, strategista ymmärrystä. Historiatiedon ja analysoidun nykytiedon perusteella tulee kyetä ennakoimaan tulevia muutoksia. Tämä voi näkyä esimerkiksi erilaisten hyökkäysmenetelmien ja niiden aiemman käytön arviointina. Näin strateginen johto saa analysoidun tiedon siitä, mitä havainnot tarkoittavat kriittisen infrastruktuurin suojaamisen kannalta. Tämä edellyttää nopeutta hallinnonalojen välisen tiedon välittämisessä, analysoinnissa ja viestinnässä. Haasteeseen voidaan vastata luomalla poikkihallinnollinen analyysikeskus, joka etsii vastauksia koko yhteiskunnan toiminnan kannalta kriittisiin kysymyksiin.

Kyberturvallisuuden osalta valmiuspäällikkökokous tai TP-UTVA ovat liian kankeita mekanismeja. Strategisten päätösten tulee muuttua toiminnaksi erittäin nopeasti, käytännössä välittömästi, jotta operatiivisilla toimijoilla on riittävästi aikaa tarvittavien toimenpiteiden toteuttamiseksi.

Strateginen johtaminen on kyberturvallisuusstrategian ja sen toimeenpano-ohjelman viemistä käytäntöön yhdessä yhteiskunnan eri toimijoiden kanssa. Strateginen johtaja kokoaa kansalliset toimijat organisaatiosta riippumatta yhteen toteuttamaan kyberturvallisuuden visiota.

Haastateltujen asiantuntijoiden mukaan yhteiskuntaamme kohdanneissa kriiseissä päätöksiä ovat kentällä tehneet yksittäiset virkamiehet ennalta harjoiteltuja toimintamalleja käyttäen ja kokonaiskuva tiedostaen.

Kybertoimintaympäristön infrastruktuurin turvaamisesta on laajennettava näkemystä kohti laajempia kokonaisuuksia. Hallinnonalojen strategioita on mahdollista koota esimerkiksi ”strategiaperheiksi”, joiden koordinoinnilla kyetään kuitenkin yhteen sovittamaan eri toimijoiden työtä yhteisten tavoitteiden saavuttamiseksi. Syksyllä 2017 päivitetty yhteiskunnan turvallisuusstrategia toimii tässä viitekehyksenä. Yksittäisistä turvattavista järjestelmistä tai hallinnonaloista voidaan laajentaa ajattelua esimerkiksi erilaisiin palvelukokonaisuuksiin, jolloin turvallisuuskeskustelu käydään eri tasolla. Turvallisuustyössä ja sen johtamisessa tulee laajentaa näkemystä turvallisuudesta itsenäisenä osajärjestelmänä kohti yhteiskunnan eri järjestelmien välistä yhteistoimintaa. Eriyttäminen mahdollisesti lisäisi kompleksisuutta, kun tavoitteena tulisi nähdä yhteiskunnan osajärjestelmien saumaton toiminta.[74] Haastateltujen asiantuntijoiden mukaan nykyisiin kyberturvallisuuden palveluntuotannon malleihin on mahdollista hakea mallia yksityiseltä sektorilta. Yksityisellä sektorilla on toiminnassa ketteryyttä, jota on

[74] Hanén, Tom. Yllätysten edessä. Kompleksisuusteoreettinen tulkinta yllättävien ja dynaamisten tilanteiden johtamisesta, 2017. Julkaisusarja 1: Tutkimuksia nro 11. Maanpuolustuskorkeakoulu. Helsinki.

mahdollista hyödyntää ja josta on mahdollista ottaa oppia Suomen kyberkyvykkyyden rakentamisessa. Ketteryys näkyy muun muassa hallinnon johtamistasojen karsimisena.

Kyberomavaraisuuden vahvistaminen on yksi yhteiskunnan menestymisen edellytys kyberturvallisuudessa. Strategisella tasolla on lisäksi tunnistettava yhteiskunnan toiminnan kannalta kriittiset osaamisalueet, koulutettava riittävästi osaavia ihmisiä ja tuettava ihmisten siirtymistä yhteiskunnan toiminnan kannalta tärkeisiin organisaatioihin. Tiivistäen voi todeta, ettei yhteiskunnalla voi olla uskottavaa kyberturvallisuutta ilman riittävää kansallista kyberliiketoiminnan kenttää. Valtion on mahdollista tukea kriittisen infrastruktuurin ja kriittiseen infrastruktuurin turvaamiseen palveluja tuottavien yritysten toimintaa omistajuudella. Valtion omistusosuudet tuovat pysyvyyttä toiminnalle ja kanavoivat samalla tahtotilaa kyberturvallisuuden yhteiskunnallisen merkityksestä kaikille kyberturvallisuustyöhön osallistuville.

2.6.6 Yhdistelmä

Aiemmassa, tammikuussa 2017 julkaistussa, Valtioneuvoston kanslian tutkimuksessa on todettu, että Suomessa ei ole toimivia johtamisrakenteita laajavaikutteisiin ja yhteiskunnan eri toimintoja poikkileikkaaviin kyberhyökkäyksiin. Näkemystä tukee Valtiontalouden tarkastusviraston Kybersuojauksen järjestämiseen liittyvä tuloksellisuustarkastuskertomus. Haastateltujen asiantuntijoiden mukaan **kyberturvallisuuden strategisen johtajuuden malli on muodostettava, koska nykyisin kyberturvallisuuden strategista johtajuutta ei ole.**

Keskeinen kysymys yksinkertaistaen on, että tuleeko johtajuus keskittää yhdelle toimijalle vai hajauttaa usealle eri toimijalle. Riittävän voimakkaan ja määrätietoisen strategisen johtamisen puuttuminen on jo aiemmin vaikeuttanut kyberturvallisuusstrategian toimeenpano-ohjelman toteutumista. Globaaliin kyberturvallisuuden haasteeseen etsitään nykyisin ratkaisuja yksittäisten hallinnonalojen sisällä ja näin ollen kansallinen näkemys tavoitteista puuttuu. Nykyinen malli johtaa toiminnan siiloutumiseen, keskinäisriippuvaisuuden huomioimatta jättämiseen ja koordinoinnin puutteeseen. Toiminnan yhdenmukaisuus ja yhteinen tilannekuva ovat merkittävässä asemassa.

Kyberturvallisuus on osa muita kokonaisturvallisuuden osa-alueita yhteiskunnan digitaalisten ratkaisujen lisääntyessä ja teknologioiden kehittyessä. Erilaisten asiakokonaisuuksien ja palveluiden tarkastelun kautta on mahdollista kehittää yhteiskuntaa. Kyberturvallisuustyöhön osallistuu jo nykyisin laajasti yhteiskunnan eri toimijoita niin valtionhallinnosta kuin yksityiseltä sektorilta. Haastateltujen asiantuntijoiden mukaan valtionhallinnon päätöksenteon mekanismit niin varautumisen kuin kriisin aikana on avattava ja toimintaa yksinkertaistettava. Mandaatti on saatava toimijalle, jolla on paras kyky jalkauttaa strategiaa ja tarvittaessa sovittaa yhteen laajojen kybertoimintaympäristöön vaikuttavien loukkausten selvittämistä rauhan aikana.

Operatiivisen tason toiminnassa on jo nykyisin kyetty muodostamaan toimivia rakenteita ja toiminnallisuuksia. Kybertoimintaympäristöön kohdistuvan loukkauksen jälkeen korjaavat toimenpiteet on kuitenkin käynnistettävä nopeasti ja määrätietoisesti. Tämä edellyttää, että mandaatti päätösten tekemiseen on siellä, missä poikkeamat havaitaan. Strategisten päämäärien viestiminen operatiiviselle tasolle on erittäin tärkeää. Toiminnan tulee olla selkeytynyt varautumisen ja harjoitusten aikana, koska kriisissä ei ole enää mahdollisuutta harjoitella. Harjoituksissa havaittuja ongelmakohtia ja prosessien puutteita ei ole kyetty viemään käytäntöön. Haastateltujen asiantuntijoiden mukaan muutokset tarvitsevat lisää resursseja toiminnan kaikilla tasoilla.

Yksityisen sektorin haastatteluissa korostettiin yhteisen tilannekuvan merkitystä ja kyberomavaraisuuden kasvattamista. Valtionhallinnon ja yksityisen sektorin nykyistä vahvempi jaettu

tilannekuva riskeistä on motivaatiotekijä yksityiselle sektorille. Tilannekuva mahdollistaa yrityksille yhteiskunnassa havaitun tarpeen perusteella tapahtuvan tuotekehityksen. Kyberomavaraisuus nähtiin haasteena, jonka ratkaisemiseksi tarvitaan korkeakoulutuksen ja tutkimuksen vahvistamista sekä yrityksille suunnatun tuen lisäämistä. Yritysten tukeminen ja valtion omistajuuden lisääminen edesauttavat yritysten pysyvyyttä Suomessa ja tätä kautta kansalliseen turvallisuuden vahvistamiseen sitoutumista.

On huomioitava, että tutkimushaastatteluissa esiintyi monenlaisia näkemyksiä kyberturvallisuuden strategisen johtajuuden toteuttamisesta Suomessa. Haastatteluissa esitetyissä strategisen johtamisen malleissa kyberturvallisuuden strategisen johtamisen kriteerit (luku 2.6.5) näyttäytyvät eri tavoin. Erilaisia johtamisen malleja on esitetty ja analysoitu tämän tutkimuksen luvussa 6.2.

3. HÄIRIÖTILANTEEN HALLINTAAN LIITTYVÄ TILANNEKUVA JA -YMMÄRRYS SEKÄ ANALYSOINTI

3.1 Johdanto

3.1.1 Kriittisen infrastruktuurin merkitys ja sen tunnistaminen

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja siten korkean käyttövarmuuden omaavista sähköjärjestelmistä ja tiedonsiirtoverkostoista sekä muista luotettavista ja tietosisällöltään eheistä hallinnon ja kansalaisten palveluista. Kriittinen infrastruktuuri muodostaa toimintaympäristön, jonka kyberturvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti muuttavat. Globaalin digitalisaation nopea kehityskulku on merkinnyt sitä, että modernin yhteiskunnan toiminta on täysin sidoksissa dynaamiseen kybertoimintaympäristöön.

Kriittisen infrastruktuurin toiminnan jatkuvuuden turvaaminen ja nopea häiriötilanteista palautuminen on erityisen tärkeää, jotta palvelukatkosten heijastusvaikutukset yhteiskunnan toimintaan kyetään pitämään mahdollisimman pieninä. Kriittisen infrastruktuurin toiminnan eri vastuutahoilla tapahtuva kyberturvallisuuden tilannetietoisuuden muodostaminen, ylläpitäminen ja tilannekohtaisesti tarvittavien päätösten aikaan saaminen ovat toiminnan jatkuvuuden hallinnassa keskeisessä roolissa. Kriittisen infrastruktuurin sisältämät monitahoiset riippuvuussuhteet edellyttävät laajaa ja kattavaa tilannetietoisuuden aikaansaamista kansallisesta kyberturvallisuustilanteestaan ja siihen vaikuttavista tekijöistä.

Kriittiset infrastruktuurit ovat rakenteiltaan yhä monimutkaisimpia ja ovat yhä vahvemmin keskinäisriippuvaisia, jonka vuoksi häiriöt yhdessä järjestelmässä vaikuttavat moninkertaisesti useissa muissa järjestelmissä. Infrastruktuurien ylläpidon lisäksi tulisi kiinnittää huomiota myös niitä suojaavaan varautumiseen sekä rakenteellisia muutoksia tehdessä uusien haavoittuvuuksien minimointiin ja sietokyvyn parantamiseen. Kriittisten infrastruktuurien toiminta ja niihin vaikuttavat uhkat eivät rajoitu pelkästään organisaatioihin tai kuntarajoihin. Tästä huolimatta alueelliset toimijat ja viranomaiset vastaavat alueen kehittämisestä ja varautumisesta, jolloin on tarvetta laajapohjaiselle tarkastelulle ja toiminnalle.[75]

Valtionjohdon ja viranomaisten oikea-aikaista päätöksentekoa tuetaan muodostamalla yhteiskunnan elintärkeiden toimintojen turvaamisen johtamisessa tarvittava kybertilannekuva. Tilannekuvajärjestelmää käytetään erilaisten poikkeus- ja häiriötilanteiden hallintaan, tiedonkeruuseen ja analysointiin, viestintään, päätöksentekoon ja johtamiseen.

3.1.2 Kyberturvallisuuden strategisen johtamisen perustana käytettävä tieto ja sen kerääminen

Valtiot pyrkivät kyberturvallisuuden strategioissaan tietoperusteiseen päätöksentekoon. Nopeat strategiset päätökset perustuvat käytettävissä olevaan reaaliaikaiseen tietoon, useisiin vaihtoehtoisiin ratkaisuihin, neuvonantajien tukeen ja yksimielisyyteen päätöksen

[75] Virrantaus K., Seppänen H. Yhteiskunnan kriittisen infran dynaaminen haavoittuvuusmalli. Tiivistelmäraportti. MATINE.

oikeutuksesta. Strategisten päätösten yhteys muihin organisaation päätöksenteon tasoihin tuottaa tarvittavaa nopeutta strategiseen päätöksentekoon.[76]

Kyberturvallisuusuhat ovat myös osa hybridivaikuttamista. Laaja-alainen yhteistyö riskianalyysissä ja tilanteenmukaiset ratkaisut korostuvat muuttuvan uhkadynamiikan myötä.[77] Kyberriskit tulee arvioida ja vertailla muiden toimintaympäristön riskien kanssa. Uhkien välisten suhteiden ymmärtäminen edellyttää vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä. Kyberturvallisuuden strategisessa johtamisessa tarvitaan tilanneymmärrystä, selkeitä johtamisvastuita ja -rooleja, saumatonta tiedonkulkua ja -vaihtoa. Lisäksi lainsäädännön tulee kaikilta osin tukea koko **kansallista kyberturvallisuusprosessia**.[78]

Haastatteluissa nousi esille, että johtamista ei toteuteta riittävän horisontaalisesti toimijoiden välillä. Tiedon tulee kulkea toimijoiden välillä, jotta päätöksellä olisi yhteiskunnallisesti näkökulmasta katsottuna suurin mahdollinen vaikutus ja riskit ovat hallittavissa. Haastatteluissa mainittu näkökulma on tunnistettu myös syksyllä 2017 julkaistussa Valtiontalouden tarkastusviraston raportissa. Raportin mukaan virastojen ja laitosten vastuulla on oman kybersuojauksen järjestäminen. Kybersuojausta on keskitetty valtion palvelukeskuksiin ja kybersuojauksen riskienhallinnan käytännöt vaihtelevat virastoittain. Riskienhallinnasta puuttuu yhdenmukaisuus, jolloin muun muassa arkaluonteisten tietojen suojauksessa voi olla aukkoja. Yhtenäisemmän ja kattavamman riskienhallinnan tarve kasvaa.[79]

Kyberturvallisuuden kokonaiskuvan kannalta on huomattava, että kerättyä poikkeamadataa syntyy eri hallinnonaloilla jo nykyisin. Kyberturvallisuuskeskuksella on osittainen näkymä verkossa tapahtuvaan liikenteeseen, mutta asiantuntijoiden mukaan yksittäisten ihmisten tekemiä havaintoja ei nykyisin kerätä keskitetysti. Tilannetta kuvaa se, että hallinnonalojen sisällä ei ole saatu muodostettua toimivaa ketjua poikkeaman havaitsemisesta keskitettyyn tilannekuvatoimintoon. Hallinnonalat toteuttavat poikkeamien käsittelyä toisistaan riippumatta. Poikkeamahavaintojen lisäksi tarvitaan tietoa muualla tunnistetuista kyberuhkista, orastavista ilmiöistä niin kybertoimintaympäristössä kuin reaalimaailmassa, järjestelmien toiminnasta sekä niiden keskinäisistä suhteista. Jokaisen viranomaisen näkökulma, näkymä ja analyysi ovat tärkeitä kokonaiskuvan muodostamisessa.[80]

Kyberturvallisuuden strategisen johtamisen perustana käytettävän tiedon hahmottamiseksi erilaiset korkean tason harjoitukset nähtiin haastatteluissa erinomaisena mahdollisuutena. Harjoitusten aikana voidaan käytännössä nähdä mitä on päätösten perustaksi tarvittava tieto ja mistä tämä tieto on saatavissa. Harjoituksissa tehtyjä havaintoja ei ole kuitenkaan saatu riittävällä tavalla vietyä organisaatioiden toimintaan. Keskitetymmän johtamisen avulla tätä ongelmaa voitaisiin tehokkaammin parantaa.

3.1.3 Tilannekuva

Tilannekuva on tarpeen perusteella valittu yksittäisistä tiedoista koottu esitys tilanteesta tai suorituskyvyistä, mikä antaa perusteet tilannetietoisuudelle. Vastaavasti tilanneymmärrys on päättäjien ja heitä avustavien henkilöiden ymmärrys tapahtuneista asioista, niihin

[76] Eisenhardt, K. Making Fast Strategic Decisions in High-Velocity Environments, 1989. The Academy of Management Journal, 32(3), 543-576

[77] Yhteiskunnan turvallisuusstrategia, 2017

[78] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[79] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomusta Kybersuojauksen järjestäminen, 2017

[80] Leppänen, A., Linderborg, K. & Saarimäki, J. Tietoverkkorikollisuuden tilannekuva, 2016. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, 17/2016, s.17

vaikuttaneista olosuhteista, eri osapuolien tavoitteista ja tapahtumien mahdollisista kehitysvaihtoehdoista, joita tarvitaan päätösten tekemiseksi tietystä asiasta tai asiakokonaisuudesta.

Tilannekuva on kaksitahoinen. Ensiksi se on yhteinen turvallisuustilannetta koskeva reaaliaikainen kuva vallitsevista tapahtumista. Tieto tilannekuvaa varten kootaan havainnointijärjestelmistä, julkisista lähteistä ja organisaation omista tietolähteistä. Toiseksi tilannekuva sisältää nykytilan analyysin, arvion tulevista tapahtumista. Tilannekuva antaa kokonaiskäsityksen siitä, mitä on tapahtunut, tapahtumassa tai tulee tapahtumaan.[81]

Tilannekuva voi olla määräajoin laadittu yleisarvio tai ajankohtaisen aiheen tai aiheiden yksityiskohtaisempi analyysi, jossa arvioidaan tapahtumia ja niiden vaikutuksia. Tällainen kuvaileva (strateginen) tilannekuva voidaan antaa päättäjille säännöllisin väliajoin (esimerkiksi kolme kertaa vuodessa, kerran kuukaudessa tai kerran viikossa). Tilannekuva voi olla myös tiheämmin (esimerkiksi päivittäin) laadittu katsaus tai tietojärjestelmässä toimijoiden saatavilla oleva tapahtumakoonnos. Tällöin siihen ei yleensä sisällytetä arvioita tilanteen kehittymisestä tai toimenpidesuosituksia.

Operatiivista tilannekuvaa muodostetaan ja päivitetään mahdollisimman reaaliaikaisena häiriötilanteen aikana. Tällöin sen tulee jatkuvan seurannan ja päivittämisen kautta antaa kuva tapahtumien kehityksestä ja tällä tavoin mahdollistaa tilanteen hallinta ja tilanteen selvittämisen edellyttämä johtamistoiminta. Päättäjän on kyettävä luottamaan siihen, että sille välitetty tilannekuva on yksityiskohtineen luotettava ja analyysit parhaalla mahdollisella asiantuntemuksella laaditut.

Tutkimuksessa ”Kriittisen infrastruktuurin tilannetietoisuus” on kuvattu tilannekuvalle esitettyjä vaatimuksia.[82] Oheisessa listauksessa on koottu tämän tutkimuksen kannalta katsoen tärkeimmät vaatimukset:

- Tilannekuva on sarja esityksiä, joiden muodolla ei ole väliä. Olennaista on, että joku hallinnoi sitä, tekee analyysiä ja päätöksiä.
- Tilannekuvajärjestelmään tuotetaan tietoa yhteistyönä. Jokainen toimija vastaa itsenäisesti oman osaamisalueensa tiedon tuottamisesta ja oikeellisuudesta.
- Tiedon on oltava prosessoitua, analysoitua ja ymmärrettävää. Sillä on oltava merkitys sekä itselle että muille vastaanottajille.
- Tietojen pitäisi olla esitettyinä visuaalisesti ja selkeästi.
- Tiedot on esitettävä ilman tarpeettomia teknisiä yksityiskohtia. Tiedon on oltava ymmärrettävää muiden alojen ihmisille.
- Tilannekuvajärjestelmän pitäisi olla dynaaminen sekä käyttäjittäin tai toimialoittain räätälöity. Tiedoista pitäisi saada eritasoisia näkymiä.
- Terminologian ja luokitusten pitäisi olla yhdenmukaista.

[81] Kuusisto Rauno, Tilannekuvasta täsmäjohtamiseen, - Johtamisen tietovirrat kriisihallinnan verkostossa, Liikenne- ja viestintäministeriö, Helsinki 2005

[82] Horsmanheimo S., Kokkoniemi-Tarkkanen H., Kuusela P., Tuomimäki L., Puuska S., Vankka J. Kriittisen infrastruktuurin tilannetietoisuus. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 19/2017

- Tilannekuvajärjestelmän olisi oltava sisällytettävissä organisaatioiden prosesseihin siten, että tilannekuvajärjestelmän ylläpitämisestä ei tule ylimääräistä tehtävää suurhäiriötilanteisiin.

- Eri toimijoiden pitäisi pystyä määrittelemään, mitä tietoa he tarvitsevat ja mitä tietoa he pystyvät järjestelmään syöttämään.

- Tilannekuvajärjestelmällä pitäisi voida vaihtaa tietoja eri toimijoiden välillä eri organisaatiotasoilla. Tietoa pitäisi pystyä jakamaan myös valvoviin organisaatioihin.

- Tilannekuvajärjestelmästä pitäisi saada ennusteita siitä, mitä tapahtuu 3, 6, 12 tunnin päästä.

- Tilannekuvajärjestelmässä pitäisi pystyä esittämään ajallinen dimensio, miten asiat ovat kehittyneet - ollaanko menossa huonompaan suuntaan vai parempaan.

Kyberturvallisuuden osalta Suomessa ei ole yhteistä tilannekuvajärjestelmää vaan kokonaisuus muodostuu erillisistä tilannekuvajärjestelmistä, joiden välillä yhteistoiminta on sopimuksin järjestetty.

3.1.4 Tilannetietoisuus ja -ymmärrys

Jokainen organisaatio tarvitsee toimiakseen tietoa ympäristöstään ja sen tapahtumista sekä niiden vaikutuksesta omaan toimintaansa. Tarkoituksenmukainen ja nopea, oikeisiin tietoihin ja arvioihin perustuva tilannetietoisuus korostuu häiriötilanteissa, jolloin joudutaan nopeasti tekemään hyvinkin laaja-alaisesti vaikuttavia päätöksiä. Voidakseen tehdä oikeita ratkaisuja päätöksentekijöiden on tiedettävä päätöstensä perusta, seuraukset, miten muut niihin reagoivat ja mitä riskejä päätöksiin sisältyy. Tästä syystä päätöksentekijöillä tulee olla kaikilla toimintatasoilla riittävä tilannetietoisuus ja -ymmärrys, joka on väline oikea-aikaiseen päätöksentekoon ja toimintaan. Tilannetietoisuus ja -ymmärrys edellyttävät yhteistoimintaa ja osaamista, jotka mahdollistavat kokonaisvaltaisen toimintaympäristön seurannan, informaation analysoinnin ja kokoamisen, tiedon jakamisen, tutkimustarpeiden tunnistamisen ja verkostojen hallinnan. Tietojärjestelmien tulee mahdollistaa systemaattinen tietolähteiden käyttö ja yhteistoiminta sekä siihen liittyvä joustava tilannetietojen jakaminen.

Organisaatioiden ja päätöksentekijöiden tilannetietoisuuden muodostamista tuetaan tilannekuvajärjestelyillä. Yleisesti tilannekuva tarkoittaa asiantuntijoiden kokoamaa kuvausta vallitsevista olosuhteista ja eri toimijoiden toimintavalmiuksista, häiriötilanteen synnyttäneistä tapahtumista, sitä koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista. Tilannekuvaan saattaa liittyä tietojen analysointiin perustuvia toimintasuosituksia. Kokonaisuus muodostetaan verkostoitunutta toimintamallia hyväksikäyttäen eri lähteistä. Prosessi muodostuu tiedon keräämisestä, informaation kokoamisesta, luokittelusta ja analysoinnista sekä analysoidun tiedon oikea-aikaisesta ja tehokkaasta jakamisesta sitä tarvitseville. Ympäröivä ”tietoavaruus” järjestetään siten, että tieto ymmärretään oikein ja toimijoilla on mahdollisuus saada oman toimintansa kannalta tärkeä tieto.

3.1.5 Havainnointikyvyn puutteet

Digitalisaation seurauksena Suomen turvallisuusympäristö on viime vuosina merkittävästi muuttunut ja monimutkaistunut. Sisäiseen ja ulkoiseen turvallisuuteen kohdistuvat uhat limittyvät toisiinsa entistä läheisemmin. Kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat

ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä maamme ulkopuolelle. Uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja niiden toiminnan ennakoiminen on vaikeutunut. Tietotekniikan kehitys on antanut pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Teknologian kehittyminen on mahdollistanut kansallista turvallisuutta vaarantavien tekojen toteuttamisen entistä lyhyemmällä valmisteluajalla ja vakavimmin seurauksin.[83]

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden toimijoiden kyky havaita ja torjua kyberuhkia ja -häiriötilanteita on keskeinen kyvykkyys. Suomessa on edellytyksiä ennaltaehkäisyyn ja parempaan havainnointikykyyn uhkien torjumiseksi. Kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen toimivaltuuksien puutteiden vuoksi. Siksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä ovat rajalliset. Yrityksillä ja organisaatioilla on entistä vaikeampi havaita kehittyneitä kyberhyökkäyksiä (APT). Tällä hetkellä yritysvakoiluun tähtääviä APT-hyökkäyksiä toteuttavat rikollisisorganisaatioiden lisäksi valtiolliset tiedusteluorganisaatiot.[84]

Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Sekä tietoliikennetiedustelun että ulkomaantiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhista. Toiminnalla tuettaisiin valtion ylimmän johdon päätöksentekoa ja varmistettaisiin sen perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon. Toiminnalla myös mahdollistettaisiin toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan. Tietoliikennetiedustelu tulisikin toteuttaa siten, että tietoliikenteen joukosta voitaisiin seuloa mahdollisimman tehokkaasti tiedustelutehtävän kannalta olennainen liikenne ja estää tehtäviin kuulumattoman liikenteen päätyminen analysoinnin kohteeksi.[85]

Tammikuussa 2018 hallitus lähetti siviili- ja sotilastiedustelulait eduskunnan käsittelyyn. Uutta lainsäädäntöä perustellaan sillä, että ”Suomen turvallisuusympäristö on muuttunut nopeasti johtuen muun muassa globalisoitumisesta ja digitalisaation voimakkaasta kehityksestä. Kansallista turvallisuutta vaarantavia tekoja voidaan nykyään toteuttaa entistä lyhyemmällä valmisteluajalla ja vakavammin seurauksin. Turvallisuusviranomaisillamme pitää olla riittävät toimivaltuudet kehittyvissä tietoverkoissa.” Tiedustelua koskevan lainsäädäntöhankkeen keskeisin tavoite on kansallisen turvallisuuden parantaminen antamalla viranomaisille riittävät toimivaltuudet havaita, ennalta estää ja paljastaa terrorismiin, laittomaan tiedustelutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin sekä valtion turvallisuutta vaarantavaan järjestäytyneeseen rikollisuuteen kytkeytyviä hankkeita.[86]

3.1.6 Euroopan unionin vaatimuksia

Euroopan parlamentti päätöslauselmassa Euroopan unionin kyberturvallisuusstrategiasta todetaan mm., että kyberturvallisuuteen liittyvien vaaratilanteiden havaitseminen ja niistä ilmoittaminen ovat keskeisellä sijalla edistettäessä tietoverkkojen kestävyyttä unionissa. Parlamentin mielestä olisi määritettävä suhteellisuutta ja tarvittavaa tietojen julkistamista koskevat vaatimukset, jotta kansallisille viranomaisille voidaan ilmoittaa tapauksista, joihin liittyy merkittäviä tietoturvan loukkauksia, mikä mahdollistaa kyberrikosten seurannan parantamisen ja edistää tietämyksen parantamista kaikilla tasoilla.[87] NIS-direktiivin katsotaan olevan tärkeä osa

[83] Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö, 14.1.2015

[84] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[85] Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö, 14.1.2015

[86] http://intermin.fi/tiedustelu

[87] Euroopan parlamentin päätöslauselma Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö, 6.9.2013

EU:n kyberstrategiaa, jonka tavoitteena on kehittää avoin ja turvallinen kyberympäristö, joka reagoi kyberhäiriöihin ja -hyökkäyksiin sekä pyrkii ehkäisemään niitä.[88]

NIS-direktiivin mukaisesti jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat ilmoittavat niistä turvapoikkeamista, joilla on merkittävä vaikutus niiden tarjoaman (direktiivin soveltamisalaan kuuluvan) palvelun tarjoamiseen (16 artiklan 3 kohta). Velvoitteilla, vaatimuksilla ja sanktioilla pyritään saavuttamaan NIS-direktiiville asetetut tavoitteet. Direktiivi asettaa listan velvoitteita, kuten ilmoitusvelvollisuus, niin jäsenmaille kuin valituille yksityisen ja julkisen sektorinkin toimijoille. Se myös esittää vaatimuksia direktiivin alaisille toimijoille esimerkiksi vaatien toimenpiteitä verkko- ja tietojärjestelmäturvallisuuden riskien vaikutusten minimoimiseksi. [89]

3.1.7 Nykytilan haasteita

Tilannekuva kybertoimintaympäristöstä on fragmentaarinen ja sen kokonaisuuden hahmottuminen perustuu jaettuun tietoon viranomaisten, yksityisen sektorin, tutkijoiden ja asiantuntijoiden välillä. Kybertilannetietoisuudesta oli erilaisia käsityksiä. Joidenkin mukaan kansallinen kybertilannekuva on hajanainen ja epätäydellinen. Kaikkia valtakunnallisia kybertoimijoita kattava tilannekuvan kokoaminen, analysointi ja päätöksentekokyvykkyys puuttuvat. Toimivaltuuksien puute estää tehokkaan havainnointikyvyn luomisen ja siten johtamisen kannalta tehokkaan kybertilannekuvan luomisen. Eri toimijoilla on oma niiden käyttöön rakennettu järjestelmä, mutta kansallinen jaettu tilannetietoisuus puuttuu käytettäväksi sekä strategisella että operatiivisella tasolla. Osa haastatelluista koki tilannekuvan yleisesti ottaen hyväksi tai ainakin riittäväksi. Nykyisellä toimintamallilla voidaan hallita pieniä kyberhyökkäystilanteita, mutta monimutkaisten ja laaja-alaisten hyökkäyksien torjuntaan tilannetietoisuus ja -ymmärrys ovat puutteellisia. [90]

Tilannetietoisuuden ylläpitämisen rakennetta on kehitetty strategian myötä, mutta käytännön tasolla siinä on kuitenkin puutteita. Joidenkin haastateltujen mielestä jaettu tilannetietoisuus ei toteudu ministeriötasolla. Hallinnonaloilla ei välttämättä ole kuvaa kyberturvallisuuden kokonaisuudesta yhteiskunnassa, mutta sen sijaan käsitys omilta toimialoilta on suhteellisen hyvä. Tiedonliikkumisen koettiin osin olevan myös henkilösidonnaista. Toisaalta jaetun tilannekuvan ylläpitoon liittyy vielä ratkaisemattomia kysymyksiä, kuten mitä tietoa kukin tarvitsee ja millä syklillä ja minkä tyyppistä tietoa tarvitaan. Tiedon luonteen osalta kaivattiin enemmän analysoitua tietoa uhkista sekä tapahtumattomista että toteutuneista häiriöistä ratkaisumalleineen. Kybervarautumisen parantamisen näkökulmasta pitää voida luottaa siihen, että häiriötilanteissa tieto kulkee ja toimijat osaavat siihen reagoida tehtäviensä mukaisesti. [91]

Kysyntää olisi myös sektorikohtaiselle tilannekuvapalvelulle, mutta Kyberturvallisuuskeskus ei tällä hetkellä pysty kaikilta osin vastaamaan kysyntään. Toiminnassa tulisikin kehittää kyvykkyyttä häiriötilanteiden vaikutusten laaja-alaiseen tunnistamiseen muilla yhteiskunnan osa-alueilla kuin sillä, johon häiriötilanne erityisesti kohdistuu. Kyberturvallisuuskeskus tarvitsee lisää resursseja sektorikohtaisen tilannekuvatiedon ja tilannekuvavarantojen kehittämiseen. Haastateltujen asiantuntijoiden mukaan Valtioneuvoston tilannekuvakeskusta (VN-TIKE) tulee kehittää kyberturvallisuuden tilannekuvan osalta paikkana, joka kykenee reaaliaikaiseen

[88] Rantala Jonna, NIS-direktiivin kahdet kasvot – riskit ja riskienhallinta, Jyväskylän yliopisto, Tietotekniikan pro gradu -tutkielma 24.9.2017

[89] Euroopan unionin verkko- ja tietoturvadirektiivi (NIS-direktiivi), 17.6.2016

[90] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[91] Ibid.

laajojenkin häiriötilanteiden tilannetietoisuuden muodostamiseen osana hybridivaikuttamisen torjuntaa.[92]

Strategisen tason tilannekuvan kannalta on ongelmallista, että yksityisen sektorin toimijat eivät tuo laajasti havaitsemiaan loukkauksia tai tietomurtoja viranomaisten tietoon. Syy tähän löytyy usein tiedon luottamuksellisuudesta ja maineriskeistä. Kybertoimintaympäristön monimutkaisuuden vuoksi olisi tärkeää saada analysoitavaksi kaikki havainnot, koska ainoastaan analysoidun kokonaiskuvan avulla on mahdollista ymmärtää kybertoimintaympäristön tapahtumia. Valtiontalouden tarkastusvirasto on suosittanut valtionhallinnon osalta, että ” Valtori parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä”.[93]

3.2 Tutkimukseen liittyviä kansainvälisiä referenssejä

3.2.1 Iso-Britannia

NCSC, National Cyber Security Center, on osana Iso-Britannian tiedustelu- ja turvallisuuspalveluorganisaatiota (Government Communications Headquarters, GCHQ), joka puolestaan on vastuussa hallituksen ja asevoimien puolesta tehdystä signaalitiedustelusta ja tietoturvasta. NCSC:n tehtävät liittyvät kyberturvallisuuden asiantuntijapalveluihin, luottamukselliseen ja riippumattomaan ohjaukseen kuningaskunnan ministeriöille, kriittiselle kansalliselle infrastruktuurille ja muille yksityisen sektorin toimijoille (ml. pk-yritykset). Ohjeet ovat luonteeltaan neuvoja.

Lisäksi NCSC tehtävänä on tunnistaa ja reagoida kyberturvallisuutta uhkaaviin tapahtumiin auttamalla niiden vaikutusten lieventämisessä ja rakentamalla ymmärrystä tietoturvauhista. Laajoissa tietoverkkoturvahäiriöiden tapauksissa NCSC tarjoaa suoraa teknistä tukea ja vastatoimien koordinointia viranomaistahoille.

NCSC raportoi verkostostaan saamiensa tietojen perusteella uusimmista haittaohjelmatyypeistä ja viimeisimmistä uhista yrityksille, muille eri organisaatioille ja laajalle yleisölle. NCSC:n ylläpitämä Cyber Security Information Sharing Partnership (CiSP) on julkisen sektorin ja teollisuuden luottamuksellinen yhteistyöfoorumi, jossa voidaan jakaa tietoa kyberturvallisuuden uhkista ja haavoittuvuuksista reaaliajassa. Iso-Britannian tietosuojalainsäädäntö velvoittaa osaa organisaatioista raportoimaan kyberturvallisuushäiriöistä NCSC:lle.

NCSC:n tehtävänä on edistää kansallista kyberturvallisuutta niin julkisen sektorin kuin kriittistenkin yksityisen sektorin toimijoiden osilta sekä edistää yleistä tietämystä kyberturvallisuusuhkista. NCSC hyödyntää verkostojaan ja osalla organisaatioista on raportointivelvollisuus sille havaitsemistaan kyberturvallisuuden häiriöistä. NCSC:lle muodostuu kansallinen analysoitu kyberturvallisuustilannekuva. NCSC:n tilannekuvan reaaliaikaisuus ja häiriötilanteiden johtamisprosessi vaativat lisäselvityksiä.

3.2.2 Saksa[94]

BSI, Bundesamt für Sicherheit in der Informationstechnik, on Saksan liittovaltion tietoturvaviranomainen. Sen päätehtävänä on kansallisen kyberturvallisuuden edistäminen

[92] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[93] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomusta Kybersuojauksen järjestäminen, 2017

[94] BSI, German Federal Office for Information Security. https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

ennaltaehkäisemällä haittavaikutuksia sekä havaitsemalla ja reagoimalla eri uhkatekijöihin. Tavoitteena on viranomaisten, yritysten ja koko yhteiskunnan toimintakyvyn varmistaminen.

BSI on ennen kaikkea Saksan liittohallituksen keskeinen tietoturvapalvelujen tarjoaja. BSI tarjoaa myös palveluja yksityiselle sektorille (alan teollisuudelle ja käyttäjille). Toiminnan tavoitteena on tehokas suojaus kybertoimintaympäristössä siten, että kaikki mukana olevat osallistuvat turvallisuusratkaisujen toteutukseen kokonaistavoitteen saavuttamiseksi. Siksi BSI haluaa työskennellä yhä tiiviimmässä yhteistyössä IT- ja Internet-alan eri toimijoiden kanssa.

BSI:n alaisuudessa ovat neljä yksikköä, jotka vastaavat Saksan kyberturvallisuuden kriisinhallinnasta: CERT-Bund (National Computer Emergency Response Team), IT-tilannekeskus (seuranta ja ennakkovaroitus), Kriisinhallintakeskus (kansallinen kriisinhallinta) ja Cyber Response Center (yhteistyö muiden liittovaltion virastojen kanssa).

CERT-Bund on keskeinen yhteysviranomainen kyberturvallisuuteen liittyvien ennaltaehkäisevien ja reaktiivisten toimenpiteiden osalta. CERT-Bund saa päivittäin tietoja kumppaneiltaan ja luotettavilta lähteiltään tietoturvahäiriöistä, jotka voivat vaikuttaa tai vaikuttavat Saksassa. CERT-Bund tarjoaa neuvoja raportoitujen ongelmien korjaamiseksi ja pyrkii etsimään vastauksia tapauksiin liittyviin ja usein kysyttyihin kysymyksiin.

IT-tilannekeskuksen tehtävät liittyvät Saksan kansallisen kyberturvallisuuden strategiseen tavoitteeseen, joka on tahokas reagoiminen tietoturvahäiriöihin. Toimenpiteet liittyvät häiriöiden tunnistamiseen, analysointiin ja raportointiin sekä niiden perusteella tehtäviin ilmoituksiin ja varoituksiin eri osapuolille. IT-tilannekeskuksen tavoitteena on muodostaa luotettava kuva tietoturvatilanteesta Saksassa, arvioida eri toimenpiteiden tarvetta ja luoda mahdollisuuksia tietoturvahäiriöiden pienentämiseksi valtion tasolla ja yksityisellä sektorilla nopeasti ja asiantuntevasti. Näiden tavoitteiden saavuttamiseksi Saksassa on toteutettu seuraavat toimenpiteet:

1. IT-tilannekeskus on tavoitettavissa liittovaltion virastoille, kriittisille infrastruktuurin toimijoille ja kumppaneille 24 tuntia vuorokaudessa.
2. Se on miehitetty päivittäin virka-aikana ja yöllä tilannetta valvoo Saksan yhteinen tiedotus- ja tilannekeskus (GMLZ), joka on itsenäinen osa liittovaltion pelastuspalveluja katastrofiaputoimistoa (BBK).
3. Käytetään avoimia ja luottamuksellisia lähteitä IT-tilanteen analysoimiseksi.
4. Seurataan valtakunnallisia verkkoja ja kumppanuusverkostoja teknisillä sensoreilla sekä asiaankuuluvia verkkosivustoja seuraamalla.
5. Tärkeät tiedot ja asiantuntija-analyysit kootaan kuukausittaisiin johdon raportteihin.
6. IT-tilannekeskus ylläpitää läheistä yhteyttä kansallisiin ja kansainvälisiin kumppaneihin CERT-Bundin kautta.

Lisäksi IT-tilannekeskuksella on valmius liittyä toimimaan osana IT-kriisien reagointikeskusta (Cyber Response Center). IT-kriisien reagointikeskus on perustettu vastaamaan kriittisen infrastruktuurin häiriöihin ripeästi ja tehokkaasti sekä varmistamaan välittömät ja oikea-aikaiset toimenpiteet vakavien vahinkojen estämiseksi. Lisäksi keskus koordinoi yhteistyössä eri toimijoiden kanssa yritysten kriisinhallintatoimenpiteitä yhden luukun periaatteella (Single Contact Points). Kriisitilanteissa, jotka ovat vaikutuksiltaan laajoja ja vaikuttavat suuressa osassa liittovaltion hallintoa, tarvittavat vastatoimet koordinoidaan toimivaltaisten yksiköiden muodostamassa komiteassa. IT-kriisien reagointikeskuksella on mandaatti kutsua koolle erillinen tilanteen selvittämiseen tarvittava komitea, jota voidaan laajentaa tarvittaessa kriittisissä tilanteissa ja komitea voi myös kuulla muita asiantuntijoita tarpeen vaatiessa. Keskuksen tarpeisiin sopivat tilat sekä tarvittava tekninen infrastruktuuri, kuten keskeytymättömät virtalähteet, hätäpuhelimet ja videoneuvottelutilat ovat valmiiksi varatut. Myös samanaikaisesti ovat käytettävissä redundanttiset tietoliikennejärjestelmät kuten puhelinjärjestelmät, matkapuhelimet

ja satelliittiviestintä. Säännöllinen toiminta ja koulutukset edesauttavat henkilöstön osaamista ja organisaation jatkuvaa parantamista.

BSI toimii kansallisen kyberturvallisuuden referenssinä niin kokonaisjärjestelyjen kuin tilannekuvan muodostamisen, analysoinnin ja häiriötilanteiden selvittämisen osilta.

3.2.3 Ranska

Ranskassa on hyväksytty 2013 laki (laki n:o 2013-1168), joka mahdollistaa kansallisten julkisten ja yksityisen sektorin toimijoiden kyberturvallisuuden kehittämisen. Sen mukaan ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ja muut valtion elimet velvoiteteen tukemaan kansallisesti kriittisiä toimijoita kyberhäiriötilanteissa. ANSSI on Ranskan kansallinen kyberturvallisuusviranomainen, jonka tehtävänä on edistää koordinoitua, vaikuttavaa ja ennakoivaa kyberturvallisuustoimintaa Ranskassa. ANSSI tukee yrityksiä teollisuuspolitiikan ja sääntelyn avulla tarjoamalla turvallisuustuotteita ja luotettavia palveluja. Laissa on säädetty toimenpiteistä, joilla tehostetaan keskeisten toimijoiden turvallisuutta ja annetaan pääministerille toimintavaltuuksia häiriötilanteeseen reagoimiseksi.

Lain mukaan valtion tulee tarjota omien tietoverkkojen turvallisuusratkaisuiden lisäksi turvallisuuspalveluita myös kansallisesti tärkeille operaattoreille (= sen käytettävyyden menetys voi vaarantaa talouden tai sotilaallisen toiminnan, yhteiskunnan turvallisuuden tai resilienssin). Laki edellyttää, että näiden elintärkeiden toimijoiden tietoverkoissa ja -järjestelmissä tulee noudattaa ANSSI:n määrittämiä turvallisuusstandardeja ja toimijoiden tulee raportoida poikkeamatapahtumista ANSSI:lle.

ANSSI voi suorittaa tai pyytää suorittamaan järjestelmäauditointeja kyberturvallisuuden varmistamiseksi. Kansallisen kriisin sattuessa ANSSI voi pyytää hallituksen määrittämään tarvittavien toimenpiteiden toteuttamista.

ANSSI:n valtuudet tehdä aloitteita laajojen häiriötilanteiden selvittämiseksi ja sen muut sen vastuulla olevat toimenpiteet sopivat referenssiksi, koska niiden avulla edistetään kansallista kyberturvallisuutta niin julkisen sektorin kuin kriittistenkin yksityisen sektorin toimijoiden osilta. Edellä esitettyjen tietojen perusteella ANSSI:lle muodostuu kansallinen kyberturvallisuustilannekuva kriittisten organisaatioiden osalta sen määrittämien raportointiprosessien ja häiriöiden havaitsemismekanismien kautta. Lisäselvitystä vaatii tilannekuvan reaaliaikainen toimivuus.

3.3 Tilannekuvaympäristöt

3.3.1 Valtionhallinnon tilannekuva

Valtioneuvoston kanslia huolehtii valtioneuvoston yhteisen tilannekuvan tuottamisesta sekä siihen liittyvien teknisten ja hallinnollisten järjestelmien rakentamisesta ja ylläpitämisestä. Valtiojohdon tilannekuvan ylläpitäminen on valtioneuvoston kanslian strateginen tehtävä. Valtioneuvoston kansliassa toimii valtioneuvoston tilannekeskus, joka tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille. Tilannekeskus toimii myös Suomen kansallisena yhteyspisteenä muun muassa Euroopan unionin suuntaan erikseen määritellyllä tavalla.[95]

[95] http://vnk.fi/turvallisuus-ja-varautuminen/tilannekeskustoiminta

Muut ministeriöt huolehtivat hallinnonalansa johtamistoiminnan edellyttämän tilannekuvan järjestämisestä toimialoillaan. Ministeriöiden tilannekuvajärjestelmien tulee tukea tarkoituksenmukaisella tavalla valtion ylimmän johdon tilannekuvaa. Kunkin hallinnonalan on jäsennettävä myös se, mitä tilannekuvatietoa niiden on tarkoituksenmukaista vaihtaa elinkeinoelämän ja järjestöjen kanssa.

Viranomaisten yhteistyöverkosto, VIRT on perustettu julkisen hallinnon organisaatioiden poikkihallinnollista operatiivisen tason yhteistoimintaa varten. Sen avulla varaudutaan vakaviin ja laajavaikutteisiin tietoturvapoikkeamatilanteisiin. Toiminnassa suunnitellaan ja harjoitellaan toimimista erilaisissa tietoturvapoikkeamatilanteissa. Toiminta käynnistettiin syksyllä 2014 pilotoimalla sitä pienellä eri hallinnonalat kattavalla kokoonpanolla. Konseptin valmistuttua vuoden 2016 aikana mukaan on tullut muita viranomaisia. Suunnitelmissa on laajentaa toimintaa myöhemmin kuntiin ja SOTE-alueisiin. VIRT-toiminnan avulla suunnitellaan ja harjoitellaan yhteistoimintaa laajavaikutteisiin ICT-poikkeamatilanteisiin, suunnitellaan yhteistyössä toiminnan tueksi tarvittavia palveluja, jaetaan tietoa, opitaan tapahtuneista, verkostoidutaan ja saadaan sekä ammatillista että henkistä tukea. VIRT-yhteistyöverkoston toimintaa koordinoi Viestintäviraston Kyberturvallisuuskeskus.[96]

Keskushallinnon lisäksi tarkoituksenmukainen tilannekuvajärjestelmä luodaan **aluehallintoon**. Järjestelmän tulee palvella aluehallinnon yhteisiä tarpeita sekä mahdollistaa tarvittavan tiedon joustava siirtyminen myös paikallis- ja keskushallintoon. Valtion keskus- ja aluehallinnon tilannekuvat tulee suunnitella ja toteuttaa siten, että ne tukevat myös kuntien sekä elinkeinoelämän tilannetietoisuutta. Järjestelmien välinen tilannetietojen vaihto ja hyödyntäminen tulee suunnitella varautumisen yhteydessä tarkoituksenmukaisella tavalla. Tilannekuvajärjestely luodaan yhteistyössä toimivaltaisten ministeriöiden, asianomaisten viranomaisten, kuntasektorin, elinkeinoelämän ja järjestöjen toimenpitein.

Tilanteessa, jossa häiriötilanteen hallinta toteutetaan paikallisella tasolla, paikallisten toimijoiden ohella alue- ja keskushallinnolta edellytetään häiriötilanteissa usein tilannetietoisuutta sekä joskus myös konkreettisia toimenpiteitä ja tehostettua viestintää. Tämän vuoksi yleisenä toimintaohjeena on, että paikallistasolta saatetaan mahdollisimman nopeasti alue- ja keskushallintoon tieto sellaisista häiriötilanteista sekä muista tapahtumista ja uhkista, jotka vaikuttavat tai saattavat vaikuttaa merkittävästi väestön turvallisuuteen tai viranomaistoimintaan ja jotka edellyttävät tai saattavat edellyttää asianomaisten viranomaisten toimenpiteitä. Samoin tilanteista, jotka herättävät tai saattavat herättää merkittävää julkista mielenkiintoa Suomessa tai kansainvälisesti tulee informoida viivytyksettä.

3.3.2 Valtorin tietoturvavalvomo (SOC)

Valtorin tietoturvapalveluita laajennetaan tulevaisuudessa paremman tilannekuvan saamiseksi valtion organisaatioiden tietoturvatilanteesta. Näin tietoturvauhkia ja -poikkeamia havaitaan paremmin ja niiden ennakointi tehostuu. Laajennettu tietoturvauhkien havainnointijärjestelmä tulee seuraamaan VY-verkon sisäistä ja internet-verkkoon suuntautuvaa liikennettä. Käytettävä järjestelmäkokonaisuus luo automaattisesti hälytyksiä havaitessaan mahdollisesti poikkeavaa tai haitallista liikennettä. Tietoturvapalveluihin kuuluva tietoturvavalvomo (SOC) kokoaa jatkossa hälytykset sekä pystyy yhdessä muun keräämänsä tiedon sekä yhteystyötahojen toimittamien uhkatietojen avulla reagoimaan tehokkaasti tietoturvapoikkeamiin ja ratkaisemaan uhkatilanteet yhteistyössä lähituen sekä verkkoylläpidon kanssa. Tietoturvavalvomo analysoi uhkat ja koordinoi korjaavien toimenpiteiden toteutuksen. Asiakasorganisaatioiden

[96] Janhunen K. Valtionvarainministeriö. VAHTI-päivä. Valtionhallinnon häiriötilanteiden hallinta – miten VIRT-toimintaa kehitetään?

tietoturvavastaavia pidetään ajan tasalla tilanteessa käyttäen virastojen sirt-sähköpostiosoitteita.

3.3.3 Kyberturvallisuuskeskus

Viestintäviraston Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka ennaltaehkäisee, kerää tietoa ja selvittää yleisiin viestintäverkkoihin liittyviä ja niiden kautta suomalaisiin tahoihin suuntautuvia tietoturvaloukkauksia sekä tiedottaa merkittävistä tietoturvauhkista. Kyberturvallisuusstrategian mukaan Kyberturvallisuuskeskuksen tehtävänä on myös yhdistetyn kyberturvallisuuden tilannekuvan tuottaminen ja ylläpitäminen. Kyberturvallisuuskeskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille sekä muodostaa ja jakaa kyberturvallisuuden yhdistettyä tilannekuvaa. Tilannekuvan muodostamisessa hyödynnetään kansallisten lähteiden lisäksi Kyberturvallisuuskeskuksen vapaaehtoisuuteen ja molemminpuoliseen luottamukseen perustuvaa kansainvälistä yhteistyöverkostoa.[97]

Kyberturvallisuuskeskuksen toiminnassa yhdistyvät erilaiset kansalliset tietoliikenteen turvallisuusviranomaistehtävät ja tietoturvayhteyspisteenä toimiminen, mikä mahdollistaa kansainvälisestikin arvioituna merkittäviä synergiaetuja. Esimerkiksi keskuksen valmistellessa tietoturvasäädöksiä tai valvoessa niiden noudattamista, keskus pystyy hyödyntämään erityistä asiantuntijuuttaan ajankohtaisista tietoturvailmiöistä ja toisaalta keskus pystyy käyttämään viranomaistoimivaltaansa tietoturvauhkilta suojautumiseen ja niiden negatiivisten vaikutusten hillitsemiseen. Keskuksen kokonaisvaltaisten toimintaedellytysten ansiosta useiden kansainvälisesti merkittävää vahinkoa aiheuttaneiden kyberuhkien vaikutukset ovat jäänet verrattain vähäisiksi Suomessa.

Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team) huolehtii Viestintävirastolle tietoyhteiskuntakaaressa (917/2014) säädetyistä tietoturvaloukkausten ennaltaehkäisy-, selvitys- ja tiedotustehtävistä:

1. Kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista.

2. Tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta.

3. Selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

4. CERT-toiminnon pääasiallisena tarkoituksena on kyberturvallisuuden tilannekuvan tuottaminen ja ylläpitäminen yhdessä luotettujen koti- ja ulkomaisten yhteistyökumppaneiden ja vastintahojen kanssa. Keskus kerää laaja-alaisesti tietoa kybertapahtumista, välittää sitä eri toimijoille sekä muodostaa ja jakaa eri lähteistä yhdistettyä tilannekuvaa. Olennaisena osana toimintaa on tietoturvaloukkausten ja -uhkien kansallisena yhteyspisteenä toimiminen, näiden tapausten selvittäminen ja asianosaisten auttaminen.

Kyberturvallisuuskeskuksen NCSA-toiminto vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Vastuu kansainvälisistä tietoturvavelvoitteista on hajautettu Suomessa useille eri viranomaisille. Kyberturvallisuuskeskuksen

[97] Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö, 14.1.2015

NCSA-toiminto on osa Suomen turvallisuusviranomaisorganisaatiota. NCSA-toiminnon kansainvälisiin tietoturvavelvoitteisiin kuuluvat tehtävät

- Kansalliseen turvallisuustoimintaan liittyvä ohjeistus- ja sopimusvalmistelu
- Kansainvälisen turvaluokitellun tietoaineiston käsittelemiseen liittyvä ohjeistus
- Salausteknisen aineiston jakeluverkon hallinnointi, kirjanpito sekä ohjeistus aineiston turvalliseen käsittelyyn (CDA)
- Salaustuotteiden hyväksyntä kansainvälisen turvaluokitellun tiedon suojaamiseksi Suomessa (CAA)
- Kansainvälistä turvaluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä (SAA) (Menettelyn piiriin kuuluvat valtionhallinnon järjestelmät niiltä osin, kun ne liittyvät kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen, sekä sellaiset kansainvälisiin tarjouskilpailuihin osallistuvien yritysten järjestelmät, joilta edellytetään kansallisen tietoturvaviranomaisen hyväksyntää.)
- Kansallisen TEMPEST-toiminnan koordinointi ja ohjeistus (NTA).

Kyberturvallisuuskeskus hoitaa Viestintäviraston tietoturvallisuussääntelytehtävät. Keskus toimii teleyritysten, vahvojen sähköisten tunnistuspalveluntarjoajien, luottamuspalveluntarjoajien ja verkkotunnusvälittäjien kansallisena valvontaviranomaisena (National Regulatory Authority, NRA) eli ohjaavana ja valvovana viranomaisena. Ohjausta toteutetaan laatimalla määräyksiä, ohjeita ja suosituksia, antamalla tulkintoja ja neuvoja sekä järjestämällä sidosryhmätapaamisia. Valvontakeinoja taas ovat kirjalliset selvitykset, tapaamiset, valvontakyselyt ja tarkastukset.

HAVARO, Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä palvelee huoltovarmuuskriittisiä toimijoita ja valtionhallintoa. HAVARO-järjestelmässä Kyberturvallisuuskeskuksella on käytännössä näkyvyys kaikkeen tulevaan ja lähtevään liikenteeseen (metatieto ja sisältötieto). Kyberturvallisuuskeskusta kohtaan tunnettua luottamusta kuvastaa se, että useat huoltovarmuuskriittiset yritykset ja valtionhallinnon toimijat ovat ottaneet käyttöönsä HAVARO-palvelun. Palvelun avulla he ovat automatisoineet organisaatioon kohdistuvien tietoturvaloukkausten raportoinnin viranomaiselle ilman mahdollisuutta sensuroida viranomaisen tietoon tulevia poikkeamia etukäteen. Järjestelmä on toteutettu yhdessä Huoltovarmuuskeskuksen kanssa.

HAVARO-toimintaan osallistuville yrityksille ja julkishallinnon toimijoille toiminta on vapaaehtoista. Järjestelmän toiminta perustuu eri lähteistä saataviin tietoturvauhkia koskeviin tunnisteisiin, joiden avulla organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä. Kyberturvallisuuskeskus vastaanottaa tiedot poikkeamista ja analysoi ne. Jos kyseessä on tietoturvauhka, siitä varoitetaan organisaatiota. HAVARO:sta saatavan tiedon perusteella voidaan myös varoittaa muita toimijoita havaitusta uhasta. Siten järjestelmä auttaa yksittäisten organisaatioiden lisäksi muodostamaan kokonaiskuvaa suomalaisiin tietoverkkoihin kohdistuvista tietoturvauhkista.

Tietoturvauhkien havainnointikyky on tärkeä osa kokonaisvaltaista riskienhallintaa. HAVARO turvaa omalta osaltaan organisaation liiketoiminnan jatkuvuuden digitaalisen toimintaympäristön uhkia vastaan. HAVARO ei kuitenkaan ole tarkoitettu organisaation ainoaksi tietoturvaratkaisuksi, vaan se on suunniteltu täydentämään tietoturvaan panostavan organisaation muita tietoturvaratkaisuja.

Lisäksi Viestintävirasto tarjoaa valtionhallinnon toimijoille **GovHAVARO**-palvelua, jonka avulla täydennetään valtionhallinnon internet-tietoliikenteen tieto- ja kyberturvallisuusuhkien havainnointia. Palvelutuottajina ovat Viestintävirasto, Valtori ja Telia.

GovCERT-palvelujen tehtävänä on tukea valtion ympärivuorokautista tietoturvatoimintoa tuottamalla tietoturvaloukkausten ennaltaehkäisyn, havainnoinnin ja selvittämisen tukipalveluja osana GovSOC-toimintoa; palvelutuottajana Viestintävirasto ja Valtori.

Toimialakohtaiset tietoturva-asioiden tiedonvaihtoryhmät (ISAC, Information and Analysis Centre) ovat eri toimialoille perustettuja organisaatioiden välisiä yhteistyöelimiä. Se mahdollistaa:

1. Tietoturva-asioiden luottamuksellisen käsittelyn osallistujien kesken
2. Organisaatioiden tietoturvaosaamisen lisäämisen
3. Kyberturvallisuuskeskuksen kokonaistilannekuvan kehittämisen

Toiminta perustuu säännöllisiin tapaamisiin sekä määritettyihin toimintamalleihin ja osallistujiin. ISAC-tiedonvaihtoryhmiä on perustettu seuraaville toimialoille: Valtionhallinto (VIRT), Internet-palveluntarjoajat, kemia ja metsäteollisuus, pankit, media, energia-ala. elintarviketuotanto ja -jakelu, SOTE sekä ohjelmistovalmistajat.

Yksityisen sektorin ja Kyberturvallisuuskeskuksen yhteistyö koetaan erittäin toimivaksi. Kyberturvallisuuskeskus on toimiva linkki yksityisen sektorin ja valtionhallinnon välillä. Kyberturvallisuuskeskuksen ja yksityisen sektorin välisen tiedonvaihdon kautta saatu tieto tulisi saada mahdollisimman kattavasti strategisen päätöksenteon perustaksi. Kyberturvallisuuskeskuksen, muiden viranomaisten ja yksityisen sektorin välinen yhteistyö on erittäin hyvää, mutta uusia datan ja tiedon lähteitä sekä toiminnallisuuksia tulee haastatteluiden perusteella tarkastella ja arvioida aktiivisesti. Tietoverkoista kerätyn käsittelemättömän datan tuominen päätöksentekijöille ei välttämättä ole tähän ratkaisu, vaan päätöksenteon perustaksi tulisi saada jalostettua ja analysoitua tietoa. Näkymä kokonaiskuvaan tuottaa todennäköisemmin strategisen tason päätöksentekoon tarvittavia elementtejä. Valtioneuvoston kanslian tilannekeskuksen ja Kyberturvallisuuskeskuksen yhteistyö nähtiin hyvänä käytänteenä, mutta samalla todettiin, että nykytilassa ei ole varmuutta siitä, onko kaikki tarpeelliset tilannekuvan tuottamiseen tarvittavat toimijat ja havaintojärjestelmät tunnistettu. Valtiontalouden tarkastusvirasto on suosittanut, että ” valtiovarainministeriö parantaa kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle”[98].

Suomen kyky tunnistaa tietoturvauhkia ja varoittaa niistä pohjautuu laaja-alaiseen ja tehokkaasti toimivaan kansalliseen ja kansainväliseen kumppaniverkostoon. Yhteistyö perustuu Viestintävirastoa ja sen henkilöstöä kohtaan tunnettuun luottamukseen. Luottamuksen jatkuminen on varmistettava kaikissa tilanteissa. Toimiva sidosryhmä- ja yhteistoiminta sekä kansallisesti että kansainvälisesti on Kyberturvallisuuskeskuksen välttämätön toimintaedellytys niin poikkeamanhallinnassa, tilannekuvatuotannossa kuin toiminnan kehittämisessä. Jotta verkostoista saadaan tarvittava lisäarvo, on niiden toiminnan ja tiedonvaihdon oltava aidosti luottamuksellista ja vuorovaikutteista.

3.3.4 Erillisverkot

Erillisverkot on valtion kokonaan omistama erityistehtäväyhtiö ja sen tehtävänä on turvata yhteiskunnan kriittistä johtamista ja tietoyhteiskunnan palveluja kaikissa olosuhteissa. Se tarjoaa viranomaisille ja huoltovarmuuskriittisille toimijoille turvalliset ja toimintavarmat ICT-palvelut. Tilannekuvan ja johtamisen alueella ERVE tarjoaa KRIVAT-palvelua.

[98] Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomusta Kybersuojauksen järjestäminen, 2017

KRIVAT-palvelu on tarkoitettu kriittisen infrastruktuurin organisaatioille siten, että toimijat muodostavat keskenään toimintaverkoston. Tarkoituksena on tehostaa organisaatioiden yhteistyötä suurhäiriötilanteissa ja nopeuttaa niistä toipumista. KRIVAT on palvelualusta ja siihen kuuluvien toimijoiden yhteisö, toimintamalli ja informaatiokanava. KRIVAT auttaa yrityksiä ennakoimaan paremmin häiriötilanteita, kuten myrskyjä ja kyberhyökkäyksiä, sekä hallitsemaan työnjakoa kriisin keskellä. Palvelu tukee myös päivittäistä yhteistyötä.

Palvelu tarjoaa reaaliaikaisen tilannekuvan, joka rakentuu mukana olevien organisaatioiden yhdessä muodostamista tiedoista. KRIVAT:in avulla voidaan jakaa kriittistä tietoa nopeasti päätöksistä vastaaville henkilöille. KRIVAT toimii julkisen internetin ja matkapuhelinverkon ulkopuolella Erillisverkkojen ylläpitämässä toimintavarmassa kiinteässä laajakaistaisessa tietoliikennepalvelussa. Julkisten verkkojen häiriöt eivät vaikuta KRIVAT:in toimintaan.

3.3.5 Keskusrikospoliisin kyberrikosten torjuntakeskus

Keskusrikospoliisissa toimii Kyberrikosten torjuntakeskus. Sen päätehtävinä kyberrikollisuuden torjunnassa ovat:

1. Vakavimpien tietoverkkorikosten tutkinta
2. Tietoverkkorikollisuuden tilannekuvan ylläpito
3. Internet- ja verkkotiedustelu
4. Tietotekninen tutkinta
5. Esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille.

Poliisi tekee tiivistä yhteistyötä Viestintäviraston kyberturvallisuuskeskuksen kanssa. Poliisi seuraa tietoverkoissa tapahtuvaa rikollisuutta ja tiedottaa aktiivisesti seurantaan liittyvistä ajankohtaisista uhkista. KRP:n tilannekuva perustuu rikosilmoituksiin, alan kansainväliseen raportointiin, yhteistyöhän Europolin ja Interpolin kanssa sekä kansainväliseen kahdenkeskiseen yhteistyöhön.

3.3.6 Puolustusvoimat

Puolustusvoimien tilannekeskus kokoaa puolustusvoimien yhteisen tilannekuvan, johon on liitetty kyberturvallisuuden tilannetietoja. Tilannekeskus toimii yhteistyössä Kyberturvallisuuskeskuksen ja Valtioneuvoston tilannekeskuksen kanssa.

Puolustusvoimien johtamisjärjestelmäkeskus (PVJJK) mahdollistaa puolustusvoimien johtamisen ja järjestää puolustusvoimien tietotekniset palvelut. Keskuksen päätehtäviin kuuluu myös kyberpuolustus. Johtamisjärjestelmäkeskuksen kyberosasto suojaa tietoverkkoja ja -palveluita sekä kehittää kyberpuolustusta. Osasto ylläpitää puolustusvoimien kybertilannekuvaa.

3.3.7 Hätäkeskuslaitos

Hätäkeskuslaitos on tärkeä toimija yhteiskunnan turvallisuuskentässä ja sisäisen turvallisuuden tilannekuvan tuottamisessa. Joulukuussa 2017 aloittaneen Hätäkeskuksen johtokeskuksella on tärkeä rooli kansalaisturvallisuuden tiedonkulun keskipisteenä. Se muodostaa yhteiskunnan kriisinsietokyvyn näkökulmasta tahon, joka sovittaa yhteen kiireellisten hälytysviranomaisten toimintaa ja huolehtii rajallisten resurssien priorisoinnista eri viranomaisten antamien ohjeiden mukaisesti. Johtokeskuksen perustaminen parantaa osaltaan Hätäkeskuslaitoksen toimintavalmiutta ja sillä on merkittävä rooli varautumisessa ja reaaliaikaisen

tilannekuvan muodostamisessa. Johtokeskus toimii operatiivisen toiminnan tukena ympäri vuorokauden. Siinä työskentelevät johtokeskuksen päällikkö sekä kahdeksan johtokeskuspäivystäjää.

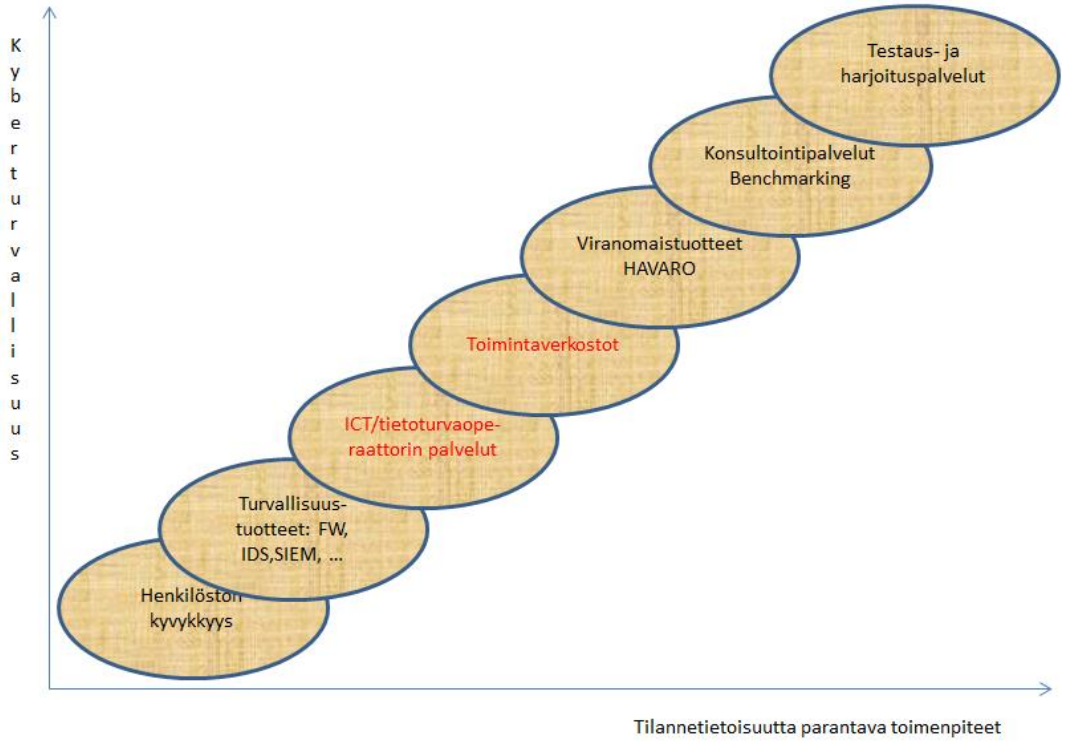
Johtokeskuksen perustehtäviin kuuluu muun muassa hätäkeskusverkoston tilannejohtaminen. Johtokeskus voi seurata hätäkeskusten tilannekuvaa puhelu- ja tehtävämäärien sekä henkilöstötilanteen osalta valtakunnallisesti verkottuneen hätäkeskustietojärjestelmä ERICA:n avulla. Lisäksi johtokeskus ylläpitää kaikkien hätäkeskustoimintaan liittyvien järjestelmien tilannekuvaa.

Johtokeskus tekee yhteistyötä eri viranomaisten tilanne-, johto- ja valmiuskeskusten kanssa. Myös yhteiskunnan tilannekuvan seuranta sekä operatiiviseen toimintaan liittyvä tiedotustoiminta ja väestön varoittaminen on suunniteltu johtokeskuksen vastuualueelle.

3.4 Kyberturvallisuuden tilannekuvan, -tietoisuuden ja -ymmärryksen nykytilan analyysi

Kansallisen tilannetietoisuuden kehittämiseen liittyvien eri osapuolten on kyettävä parantamaan toimintaansa aiempaa tehokkaammilla teknillisillä menetelmillä, vahvistettava verkostomaista toimintaa sekä parannettava yhteiskäyttöisten teknillisten menetelmien hyödyntämistä.

Suomalaisiin yhteiskunnan toimintakykyyn liittyvien merkittävimpiin organisaatioihin on kehittynyt kohtalaisen hyvä tilannekuvan havainnointikyky teknisten valmiuksien osalta. Sitä parantaa myös niiden verkostoituminen toimialakohtaisesti ja osittain myös laajemmin, jota tuetaan hyvällä viranomaisten ja yksityisen sektorin yhteistyöllä. Eri organisaatioiden tilannekuvien kautta muodostuvan tilannetietoisuuden (tilannekuva ja sen analysointi) merkitys koko kansallisen kyberturvallisuuden johtamisen osalta on aivan keskeinen tekijä. Kuvaan 2 on koottu tutkimuksessa esiin tulleita organisaation kyberturvallisuutta edistäviä tekijöitä. Lähtökohtana on aina organisaation oman henkilöstön kyvykkyys tunnistaa käytössä olevissa järjestelmissä mahdollisesti esiintyvää poikkeavaa toimintaa sekä toimia luotettavasti ja järjestelmällisesti eri käyttötilanteissa. Tutkimuksen mukaan ideaalitapauksessa toimintaa tuetaan teknillisillä järjestelmillä, käytettävissä olevin ICT- tai tietoturvaoperaattorien palveluin, toimintaverkostoa hyödyntämällä, viranomaisyhteistyöhön osallistumalla, hyödyntämällä konsultointipalveluja, benchmarking-toimintaa sekä testaamalla ja harjoittelemalla toimintaa.



Kuva 2. Organisaation kybertilannetietoisuuden kehittäminen osana kokonaisvaltaista kyberturvallisuutta.

Tutkimuksessa on korostunut aiemminkin esille tullut kansallinen vahvuus organisaatioiden mahdollisuuksista erilaisten verkostojen hyödyntämiseen kyberturvallisuuden tilannetietoisuuden osalta.[99] Toiminnassa on havaittavissa ainakin kolmenlaisia luottamuksellisen tiedon vaihtoon liittyviä verkostoja, joita hyödynnetään aktiivisesti. Ne ovat muodostuneet liiketoiminnan yhteyteen tai jonkun toimialan yritysten välille on perustettu erillinen luottamusverkosto, joka voi ulottua myös kansainväliseen yhteistyöhön. Lisäksi kansallisesti toimii viranomaisten ja yksityisen sektorin välinen luottamusverkosto (PPP-yhteistyö).

Kansallinen häiriötilanteiden hallinta koostuu eri organisaatioiden käyttämistä tekniikoista, häiriötilanteiden reagointiin kehitetyistä menettelytavoista ja eri luottamusverkostojen havaintotiedoista. Tätä hajallaan olevaa organisaatiokohtaista tilannekuvan havainnointikykyä ja sen sisältämää datavarantoa voitaisiin hyödyntää myös laajamittaisten häiriötilanteiden hallinnan analysointivaiheessa. Järjestely edellyttäisi yhteisten toimintamallien luontia ja vapaaehtoiseen tietojen vaihtoon pohjautuvaa järjestelyä. Yhteinen datavaranto mahdollistaa tiedon jatkojalostuksen laajamittaisen häiriötilanteen analysoimiseksi. Tarvittava analysointikyvykkyys voitaisiin toteuttaa verkostomaisena toimintana (virtuaalianalysointi).

[99] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

4. KYBERTURVALLISUUDEN JOHTAMINEN JA TILANNEKUVAN MUODOSTAMINEN VERTAILUMAISSA

4.1 Tutkimuksen perusteet

Tutkimuksen kansainvälisessä strategisen johtamisen analyysissa nostetaan kustakin vertailuun valitusta valtiosta esiin käytäntöjä, joita voitaisiin harkita sovellettaviksi myös suomalaisessa turvallisuusympäristössä. Tarkoituksena ei siten ole vertailla valtioiden kyberturvallisuuden johtamistapoja ja/tai -malleja keskenään. Analyysi on tehty vertailuun valittujen valtioiden (1) kansallisten strategiapapereiden ja niissä asetettujen tavoitteiden saavuttamiseksi luotujen toimenpideohjelmien pohjalta sekä (2) olemassa olevaan tutkimukseen tukeutuen.

Vertailussa vastataan kysymykseen: Kuinka kyberturvallisuuden strateginen johtaminen on toteutettu Suomen keskeisiin vertailumaihin verrattuna? Vertailtaviksi valitut maat ovat (aakkosjärjestyksessä) Alankomaat, Australia, Israel, Ruotsi, Singapore ja Viro. Valtioiden valintaan ovat vaikuttaneet (1) kansainvälisissä kyberturvallisuusindeksilistauksissa tunnistettu korkea kyberturvallisuuden taso, (2) saatavilla oleva tutkimusmateriaali, sekä (3) valtioiden (sosio-kulttuurinen, taloudellinen ja poliittis-strateginen) samankaltaisuus/erilaisuus Suomeen verrattuna. Pääpaino analyysissa on kansallisen kyberturvallisuusjohtamisen organisaatiorakenteessa ja valtuutuksessa (mandaatti).

4.2 Kyberstrategioiden vertaisanalyysi

4.2.1 Alankomaat

Alankomaiden sietokykyä ja tehokasta vastauskykyä painottavassa lähestymistavassa kyberturvallisuus kietoutuu yhteen vapauksien yhteiskunnallisten ja taloudellisten hyötyjen kanssa. Perusoikeuksien ja -arvojen turvaaminen, oikeusvaltioperiaate ja koko keinovalikoiman hyödyntäminen ohjaavat niin kansainvälistä kuin kansallista kyberturvallisuustoimintaa. Turvallisuuden tuottaminen alkaa kansainväliseltä tasolta, diplomaattisista suhteista ja tehokkaan (siviili-sotilas) yhteistyöverkoston luomisesta (erityisesti NATO ja EU). Kansallisesti sitä tuotetaan tiiviissä sektoreiden välisessä yhteistyössä. Elintärkeät palvelut ja prosessit ovat keskeisiä turvattavia kohteita. Valtion roolina on (1) ylläpitää verkkojensa ja palveluidensa turvallisuutta; (2) edistää vuoropuhelua ja toimia, mikäli yritysten tai kansalaisten turvallisuus tai tietosuoja on uhattuna; sekä (3) kehittää turvallisuusviitekehyksiä silloin, kun toimialojen itseregulaatio ei riitä. Tavoitteena on pitää valtio globaalina digitaalisena solmukohtana ja hyödyntää digitalisoituvalle yhteiskunnalle avautuvat mahdollisuudet maksimaalisesti.

Kyberturvallisuuden johtamisen periaatteena on, että fyysiseen ympäristöön luodut vastuut pätevät myös digitaalisessa ympäristössä. Olemassa olleita ratkaisuja on tarpeen mukaan täydennetty. Kyberturvallisuustapauksien käsittelyn hoitaa ensisijaisesti se (julkinen tai yksityinen) taho, jota tapaus koskee. Mikäli tapauksesta voi seurata yhteiskunnallinen häiriö tai vahinkoa kriittisille rakenteille, toiminnalle ja/tai henkilöille, vastuunalainen julkishallinnon organisaatio osallistuu sen hoitamiseen. Mikäli seurauksena voi olla usean yhteiskunnallisen

sektorin toiminnan vaarantava siviilikriisi, Ministereistä koostuva kriisinhallintaneuvosto koordinoi toimintaa ja tekee tarvittavat päätökset.[100].

Turvallisuus- ja oikeusministeriö vastaa kansallisen kyberturvallisuuden yhteensovittamisesta ja koordinoimisesta. Se toimii muissakin kriisitilanteissa ministeritason tiedonvaihdon keskuksena ja toiminnan koordinoijana. Toiminta keskittyy Kansalliseen kriisikeskukseen (NCC), jonka tehtävänä on tukea ja ennalta valmistella päätöksentekoa. Kansallinen operatiivisen koordinaation keskus (LOCC)[101] toimii kriisitilanteissa 24/7 Kansallisen turvallisuus- ja vastaterrorismin koordinaattorin alaisena. Kriisiviestintää hoitaa erillinen ydinyksikkö (NKC). Kybertuvallisuuden koordinoimisessa ministeriötä tukee Kyberturvallisuusneuvosto, joka koostuu keskeisten kyberturvallisuustoimijoiden (hallinnossa, yritysmaailmassa, muissa organisaatioissa ja akatemiassa) edustajista. Sillä on oma sihteeristönsä. Neuvoston tehtävänä on neuvoa (pyydettäessä tai omasta aloitteestaan) ja valvoa kyberturvallisuuden toimeenpanoa strategisella tasolla. Puhetta neuvostossa johtaa kansallinen turvallisuus- ja vastaterrorismin koordinaattori yhdessä yksityisen sektorin edustajan kanssa.

Kansallinen kyberturvallisuustoiminta perustuu riskiarviointeihin sekä asian- ja ajanmukaiseen tilannekuvaan (ml. kyberrikollisuuden tilannekuva), jota kokoaa ja ylläpitää Turvallisuus- ja oikeusministeriössä **Kansallisen turvallisuus- ja vastaterrorismin koordinaattorin** alle järjestetty **Kansallinen kyberturvallisuuskeskus (NCSC)**[102]. Sotilas- ja siviilitiedustelu- ja turvallisuuspalvelut osallistuvat myös tilannekuvan tuottamiseen. Palvelut ovat yhdistäneet kyberkykynsä yhteiseen signaalitiedustelun kyberyksikköön (JSCU). NCSC seuraa digitaalisen ympäristön kehitystä ja kehittää kansallista kyberturvallisuusjärjestelmää[103], jotta tarvittavat kyvyt uhkien estämiseksi ja häiriöihin vastaamiseksi ovat olemassa. Joko omasta aloitteestaan tai pyydettäessä se tukee niin yksityisiä kuin julkisia tahoja laaja-alaisten kyberturvallisuustapausten hoitamisessa. Etenkin keskuksen osaksi kuuluva julkinen-yksityinen kumppanuus, ICT Response Board (IRB), neuvoo vastatoimenpiteissä[104]. Yhteistyökumppaneidensa kanssa kyberturvallisuuskeskus ylläpitää keskushallinnon ja elintärkeiden sektoreiden havainnointi- ja vastaamisverkostoja[105], ml. osallistuminen sektorikohtaisten Tiedonjako- ja analyysikeskusten[106] toimintaan. Se toimii CERT:inä, GovCERT:inä sekä kansallisena turvallisuusoperaatiokeskuksena (NSOC[107]) ja ylläpitää mm. kyberturvallisuusvaroituksia antavaa sivustoa. Kyberkriisitilanteissa keskuksen toimintavaltuudet vahvistuvat ja siitä tulee osa kansallista kriisinhallintarakennetta.

Kyberturvallisuuden tuominen Kansallinen turvallisuus- ja vastaterrorismin koordinaattorin alle yhdisti sen muuhun kansallisen turvallisuuden rakenteeseen. Koordinaattori[108] varmistaa kriittisen infrastruktuurin toiminnan jatkuvuuden. Sen osana toimii Kyberturvallisuusjaosto (johon kansallisen kyberturvallisuuskeskuksen ohella kuuluu kyberturvallisuusstrategiaa kehittävä Politiikkaosasto ja erillinen operatiivinen tukiryhmä). Jaosto ohjaa yhteiskunnallisen

[100] Kyberkriisinhallinnassa toimitaan Kansallisen turvallisuusstrategian mukaisesti. Päätöksenteko on kuvattu Kansallisessa kriisitilanteiden päätöksenteko-ohjeistuksessa, jota täydentää mm. Kansallinen kyberturvallisuustapauksiin vastaamissuunnitelma (National Crisis Plan – ICT).

[101] Koostuu poliisin, pelastusviranomaisten, Puolustusministeriön ja kuntien edustajista.

[102] Keskuksen toiminta keskittyy elintärkeiden sektoreiden kuten rahoitus, energia ja viestintä ympärille, mutta myös Talous- ja ilmastoasioiden ministeriö, Maatalous-, luonto- ja ruoanlaatuministeriö, Sisä- ja kuningaskunnan asioiden ministeriö, Ulkoasiainministeriö ja Puolustusministeriö ovat sen yhteistyökumppaneita.

[103] Teknisen havainnointiverkoston rakentaminen on meneillään. Kun se on valmis, n. 250 julkisen hallinnon organisaatiota on kytketty siihen.

[104] IRB:n jäseninä on kyberasiantuntijoita useilta kriittisiltä sektoreilta kuten ICT-, energia-, vesi- ja rahoitussektorit sekä asianmukaisista julkishallinnon organisaatioista. Se aktivoituu laaja-alaisissa kyberkriisitilanteissa.

[105] Vastaamisverkoston jäseniä ovat Kuntien tietoturvapalvelu, SURF (koulutus- ja tutkimuslaitosten yhteistyöperusteinen ICT-organisaatio), Vero- ja tullihallinto, Puolustusministeriö, Infrastruktuuri- ja vesihallinnan ministeriö sekä Kyberturvallisuuskeskus.

[106] Tiedonjako- ja analyysikeskukset ovat julkinen-yksityinen kumppanuuksia, joiden puitteissa voidaan vaihtaa kyberturvallisuustietoa ja -kokemuksia sekä sektorikohtaista, taktisen tason tilannekuvaa. NCSC:n ohella niiden toimintaan osallistuvat Siviilitiedustelu- ja turvallisuuspalvelu sekä poliisiviranomaisen kyberrikollisuusyksikkö.

[107] Security Operations Centre:n tehtävänalaan kuuluu kyberuhkiin vastaamisen lisäksi (tilanne)tietoisuus, sietokyky, havainnointi, hälyttäminen, raportointi ja kriisinhallinta. Se on 24/7 toimintavalmiudessa.

[108] Vastaa vastaterrorismista, kyberturvallisuudesta, kansallisesta turvallisuudesta ja kriisinhallinnasta.

kyberkriisin hallintaa strategisella ja taktisella tasolla kansallisen kriisinhallintarakenteen ja -ohjeistuksen mukaisesti.

Kyberrikollisuuden tutkinta ja syyttäminen on integroitu lainvalvonta- ja oikeusjärjestelmään (mm. Kansallisen poliisiviranomaisen alainen kyberrikollisuusyksikkö). Rikostutkinta ja yleinen syyttäjä osallistuvat kyberturvallisuuskeskuksen toimintaan. Kansallisesti merkittävimmän rikollisuuden ohjauskomitea varmistaa, että oikeusjärjestelmällä on käytettävissään riittävä kyberasiantuntemus. Komitean puheenjohtaja kuuluu Kyberturvallisuusneuvostoon.

Kokonaisvaltainen kyberpuolustus koostuu sotilaallisten kykyjen (sietokyky, puolustus- ja hyökkäyskyky sekä tiedustelu – voidaan käyttää myös kansainvälisissä operaatioissa ja/tai kohdevaltion oman toiminnan kehittämisessä) ohella siviiliviranomaisten laaja-alaisista kyvyistä, ml. tiedustelu- ja turvallisuuspalvelu[109], poliisi ja kansallinen kyberturvallisuuskeskus, sekä yritysten vastauskyvyistä. Asevoimien päätehtävät ohjaavat sen toimintaa myös digitaalisessa ympäristössä. Puolustuksellista toimintaa koordinoi puolustushaarojen yhteinen tietohallinnon komentokeskus, jonka osana mm. DefCERT toimii. DefCERT monitoroi sotilasverkkoja 24/7 valmiudessa, neuvoo puolustushallintoa ja ylläpitää tilannekuvaa, jonka tuottamiseen osallistuu myös Sotilastiedustelu- ja turvallisuuspalvelu – keskeinen toimija hyökkäyksellisten kyberkykyjen ja sotilastiedustelun kehittämisessä. Puolustushallinnolla on myös oma SOC.

Sotilaallisia kykyjä voidaan pyynnöstä hyödyntää myös elintärkeän kansallisen siviili-infrastruktuurin suojaamisessa. Toiminnan koordinoimiseksi ja kybervalmiuden ylläpitämiseksi on perustettu puolustushaarojen yhteinen (organisatorisesti maavoimien alainen) kyberkomentokeskus[110]. Siviiliyhteistyötä edistetään jatkuvasti ja puolustushallinto osallistuu niin Kyberturvallisuusneuvoston kuin kyberturvallisuuskeskuksen toimintaan.

4.2.2 Australia

Kyberturvallisuuden tuottamista Australiassa ohjaavat (1) pyrkimys tiiviiseen alueelliseen (Australaasia ja lähivaltiot; mm. Asia Pacific CERT, jossa osallisena on 12 alueen valtiota) ja kansainväliseen (erit. UKUSA-valtiot ja Commonwealth) yhteistyöhön, (2) liittovaltiorakenne ja maantieteelliset erityispiirteet (laaja alue, jossa vähäinen asutus keskittyy saaren rannikoille), (3) riippuvuus tuontiteknologiasta, (4) paikallisen kyberturvallisuustiedon ja -osaamisen vahvistaminen (mm. kyberturvallisuuden kasvukeskuksen perustaminen) sekä (5) internetin avoimuuden, vapauden ja turvallisuuden sekä digitaalisen toiminnan lainmukaisuuden edistäminen. Tavoite on hyödyntää digitalisaation avaamat mahdollisuudet maksimaalisesti ja siten lisätä valtion vetovoimaa liiketoiminnassa. Kyberturvallisuuteen investoidaan niin sotilas- kuin siviilihallinnon puolella. Kokonaisvaltaista toimintaa tuetaan mm. organisaatioille vapaaehtoisella kyberturvallisuusohjeistuksella, joka perustuu signaalidirektoraatin kehittämiin kyberturvallisuustapahtumien hallintastrategioihin. Hallinnolle näiden strategioiden noudattaminen on pakollista ja sitä seurataan jatkuvasti.

Strategista kyberturvallisuustoimintaa Australiassa johtaa Pääministerin ja hallituksen ministeriö[111]. Johtaminen on keskitetty **Kyberturvallisuusneuvostoon**, jonka puheenjohtajana toimii em. ministeriön sihteeri. Ministeriöön on perustettu kaksi kyberturvallisuuteen keskittyvää tehtävää: Pääministeriä kyberturvallisuusasioissa avustava ministeri sekä **Kyberturvallisuuden erityisasiantuntija**, joista jälkimmäisellä henkilökuntineen on keskeinen rooli

[109] Toimii Sisä- ja kuningaskunnan asioiden ministeriön alaisuudessa. Kyseinen ministeriö on vastuussa muiden (paitsi kyber-) yhteiskunnallisten kriisien hallinnan koordinoimisesta.

[110] Komentokeskus johtaa asevoimien kokonaisvaltaista kybertoimintaa, joskin hyökkäykselliset kyvyt on alistettu suoraan Asevoimien komentajalle.

[111] Department of the Prime Minister and Cabinet

(poikki)hallinnollisten ja yksityinen-julkinen kyberturvallisuusjärjestelyiden koordinoimisessa. Kansalliset kyberturvallisuuden toimintalinjaukset päätetään vuosittain hallituksen, yritysmaailman ja tutkimusyhteisön yhteisissä kyberturvallisuuskokouksissa. Ennen siirtämistä em. ministeriöön, kyberturvallisuustoiminta oli pitkään Oikeusministeriön alainen (ml. CERT Australia).

Puolustushallinnon johtama **Australian kyberturvallisuuskeskus** kokoaa yhteen hallinnon operatiivisen tason kyberturvallisuustoimintoja kuten kansallinen siviilistatuksella toimiva CERT Australia, jonka toiminta keskittyy kriittisten yritysten avustamiseen. Maassa on myös eri organisaatioiden perustama, Queenslandin yliopiston hallinnoima AusCERT[112], joka palvelee omia jäseniään, CERT Australiaan on liitetty signaalidirektoraatin alla toiminut **kyberturvallisuusoperaatiokeskus**. Australian rikosvaliokunta, liittovaltion poliisi, turvallisuustiedusteluorganisaatio, signaalidirektoraatti ja puolustustiedusteluorganisaatio osallistuvat keskuksen toimintaan. Se jakaa ajanmukaista tietoa kyberuhkista, neuvoo organisaatioita kyberturvallisuusjärjestelyissä ja tekee asiakastutkimusta kyberturvallisuustason arvioimiseksi.

Alueellisen kattavuuden ja ajanmukaisen (julkinen-yksityinen) tiedonkulun parantamiseksi Australiassa on järjestetty paikallisia kyberuhkatiedon jakamiskeskuksia sekä eritasoisia online portaaleja, jotka palvelevat eri sidosryhmiä (mm. kyberrikosten raportointiverkosto Australian Cybercrime Online Reporting Network, ACORN; kriittisen infrastruktuurin suojaamiseksi luotu Trusted Information Sharing Network, TISN; sekä hallinnon kyberturvallisuustapausten raportointijärjestelmä OnSecure). Paikallisissa uhkatiedon jakamiskeskuksissa on edustettuna organisaatioita mm. energia-, vesi-, rahoitus-, kuljetus- ja kaivannaisteollisuudesta, osavaltion hallinnosta, CERT Australiasta, liittovaltion poliisista sekä rikollisuustiedusteluvaliokunnasta. Kyberturvallisuuskeskuksen kanssa nämä muodostavat yhteiskunnan kerroksittaisen kyberturvallisuusratkaisun.

Niin ikään puolustushallinnon alainen signaalidirektoraatti (ASD) tuottaa tietoa kyberuhkista ja -haavoittuvuuksista yhteiskunnan kyberturvallisuustoiminnan tueksi. Puolustushallinnon tehtävänä on omien järjestelmiensä ja verkkojensa turvaamisen ohella suojata muita hallinnon kriittisiä järjestelmiä ja verkkoja. Tiedustelutehtävää hoitavan direktoraatin mandaatissa kyberturvallisuus korostui vuonna 2013. Samalla sen toimintaa asetettiin valvomaan Oikeusministeriön alainen komitea.

Oikeusministeriön alaisuudessa toimii **Kriittisen infrastruktuurin keskus**, joka yhdessä Kyberturvallisuuskeskuksen kanssa tekee yhteistyötä kriittisten yritysten kanssa haavoittuvuuksien havaitsemiseksi sekä riskikartoitusten ja hallintastrategioiden kehittämiseksi. Kriittisen infrastruktuurin sietokyvyn lisäämiseksi on luotu oma strategia ja parhaillaan kehitetään toimintaohjelmaa kyberrikollisuuden torjumiseksi. Kansainvälisiä diplomaattisia ponnisteluita vetää Kyberturvallisuussuurlähettiläs, joka toimii Ulkoasiain- ja kauppaministeriön alaisuudessa.

Australian osalta on esitetty kritiikkiä, että kyberturvallisuutta on rakennettu liikaa sotilas- ja tiedusteluorganisaatioiden varaan ja ”siviilitoimintaympäristö” on saanut osakseen liian vähän huomiota ja jätetty toimialan itsesääntelyn varaan. Puolustus- ja tiedustelupuolen korostunut rooli hankaloittaa tiedonvaihtoa tiedonkulun ollessa yksisuuntaista (siviilipuolelta sotilaspuolelle), hallinnon läpinäkyvyyttä ja luottamuksen syntymistä. Siviili-sotilasyhteistyötä ei ole tositilanteessa jouduttu testaamaan.[113]

[112] Yhdysvaltalaisen mallin mukaan perustettu AusCERT toimi kansallisena CERT:nä 1993-2010.

[113] Smith & Ingram 2017, pp. 643–644; 651-654

4.2.3 Israel

Israelin strategis-poliittinen asema on poikkeuksellinen muihin vertailumaihin verrattuna. Se kokee olevansa alati hyökkäyksen kohteena[114], minkä vuoksi turvallisuuden (niin fyysinen kuin digitaalinen) tuottaminen on integroitu koko yhteiskuntaan. Kyberpuolustuksen, valtionhallinnon ja kriittisen infrastruktuurin suojaamisen sektorikohtaisen turvallisuuden saavutettua tavoiteltu taso keskitytään kokonaisvaltaisen kyberturvallisuuden kehittämiseen siviiliyhteiskunnassa. Kyberturvallisuus jäsennetään ekosysteemiksi, joka kattaa toiminnan mm. koulutuksesta asepalvelukseen ja julkishallinnosta yritystoimintaan. Yhteiskunnan suojaamisen ohella ekosysteemi pyrkii tuottamaan vahvaa kyberturvallisuusosaamista (vientituotteeksikin). Valtiolla on sen ohjaamisessa keskeisin rooli.

Israelilla ei pitkään ollut julkista kyberturvallisuusstrategiaa, mutta hallituksen periaatepäätös 3611 toimi de facto sellaisena. Vuoden 2017 strategia[115] koostuu kolmesta, toisiinsa limittyvästä osiosta, joita ovat operaatiot, rakenne ja kyvykkyyden luominen.

Operaatiot kattaa kolme tasoa, joilla kyberturvallisuutta tuotetaan: kestävyys, sietokyky ja puolustus. Näistä ensimmäinen tarkoittaa organisaatioiden kykyä toimia häiriöttömästi kaikissa tilanteissa; toinen kykyä toimia realisoituneiden uhkien suhteen siten, että paluu normaalitilaan tapahtuu nopeasti (organisaatiot ja valtio yhteistyössä); ja kolmas valtion toimintaa välittömästi kansallisia etuja koskevissa tilanteissa (puolustus ja hyökkäys). Kyvykkyyden luominen viittaa kyberturvallisuuden ekosysteemin tehokkaaseen toimintaan.

Hallinnonaloille hajautetun kyberturvallisuuden johtamisjärjestelmän sijaan Israelissa kyberturvallisuus on keskitetty yhteen organisaatioon Pääministerin toimistossa[116]. **Kansallisen kyberdirektoraatin**, joka koordinoi kyberturvallisuustoimintaa, muodostavat **Kansallinen kybertoimisto** (INCB) ja **Kansallinen kyberturvallisuusviranomainen** (NCSA). INCB vastaa siviilipolitiikkojen suunnittelusta, koordinoinnista ja hallituksen neuvomisesta. NCSA:n tehtävänä on edistää kokonaisvaltaista kansallista kyberturvallisuutta operatiivisella tasolla, mm. yhteistyössä (siviili- ja sotilas)tiedusteluorganisaatioiden kanssa. Se kehittää kyberturvallisuuden konseptia ja teknologiaa yhteistyökumppaneidensa kanssa ja vastaa myös kriittisen infrastruktuurin suojaamisesta[117]. Pääministerin toimiston alaisuuteen on siirretty myös aiemmin Talousministeriön alla toiminut Hallituksen ICT-viranomainen, jonka pääasiallisena tehtävänä on ylläpitää sähköisiä palveluita.

Kansallisen kyberturvallisuusviranomaisen alla toimii CERT-IL, joka fyysisesti on sijoitettu Be'er Shevan ICT-alan keskittymään (samalla alueella toimii yliopisto, tutkimuslaitoksia, eri kokoisia kyberturvallisuus- ja ICT-alan yrityksiä sekä julkishallinnon organisaatioita ja asevoimien yksiköitä). CERT-IL on kyberturvallisuuden keskeinen julkinen kontaktipinta, joka vastaa mm. kansallisten kyberturvallisuustapausten hoitamisesta, tiedonvaihdosta luotettujen kansallisten ja kansainvälisten kumppaneiden kanssa sekä tietoisuuden lisäämisestä. NICB tukee rahallisesti mm. Be'er Shevan keskittymän kehittämistä ja yliopistojen kybertutkimuskeskuksia[118]. Se myös sääntelee kyberturvallisuusosaamista, -tuotteita ja -palveluita.

Kansainvälistä yhteistyötä (rajoitettu rooli kyberturvallisuuden tuottamisessa) kehittämään ulkoministeriö on nimittänyt **Kyberturvallisuuskoordinaattorin**. Kansallisen poliisin

[114] Ks. esim. Israelin asevoimien strategia vuodelta 2015.

[115] Ks. esim. Matani, Yoffe & Mashkautsan 2016; Matani, Yoffe & Goldstein 2017; Adamsky 2017.

[116] Sektorikohtaiset ministeriöt kuitenkin vastaavat kyberturvallisuuden sääntelystä omalla hallinnonalallaan. Jokainen ministeriö on myös hallinnon sisäinen, sektorikohtainen yhteyspiste kyberturvallisuuspolitiikkojen täytäntöönpanossa.

[117] Määrittää kyberturvallisuustavoitteet, suunnittelee niiden toteuttamisen ja valvoo toteuttamista yhdessä vastuunalaisen ministeriön kanssa.

[118] Seitsemästä olemassa olevasta yliopistosta viidessä on tällainen keskus.

eliittidivisioonan (Lahav) yhteyteen on perustettu **Kyberdivisioona**, jonka tehtävänä on kyberrikollisuuden vastainen toiminta ja digitaalisen rikostutkinnan kehittäminen.

Varautuminen ja siviilikriisinhallinta kuuluvat Israelissa Yleisen turvallisuuden ministeriön, Puolustusministeriön ja Asevoimien kotirintaman komentokeskuksen vastuualueille. NCSA ja Yleisen turvallisuuspalvelun alainen Kansallinen tietoturvayksikkö (NISA) ovat myös vastuussa toimivaltojensa puitteissa. Israelin asevoimilla on pitkä kokemus kybersodankäynnistä, mutta organisaation rakentaminen on kesken. 2015 tuotiin julki tavoite kyberyksiköiden tuomisesta yhden kyberkomennon alle puolustus- ja hyökkäyskykyjen integroimiseksi[119]. Komentokeskus alistetaan suoraan asevoimien komentajalle, mutta sen tarkka mandaatti on epäselvä. Kyberpuolustukseen ja -hyökkäykseen panostetaan koko ajan niin taktisella, operatiivisella kuin strategisella tasolla. Rauhan aikana Kansallinen kyberdirektoraatti on vastuussa kokonaisvaltaisen kyberpuolustusjärjestelmän johtamisesta (tällöinkin muut sotilas- ja turvallisuusorganisaatiot suorittavat hyökkäyksellistä toimintaa). Kriisitilanteissa Israelin asevoimat vastaa kansallisen tason puolustuksen ja hyökkäyksen yhteen sovittamisesta.

Israelissa käydään keskustelua tulevaisuuden kehityksestä ja tavoitteeksi voi tulla kansallisen keskitetyn kyberviranomaisen (CCA) luominen. Se olisi siviiliviranomainen, jolla olisi operatiiviset kyvyt, vastuu kansallisen kyberavaruuden puolustamisesta ja kansallisten kyberturvallisuustoimien johtamisvastuu[120]. Kyberturvallisuustapausten hoitaminen ja kansallisen sietokyvyn kehittäminen olisi keskitetty CCA:han, joka saisi käyttöönsä riittävät resurssit. Siltä kuitenkin puuttuisi tutkintaoikeudet. Sääntely säilyisi nykyisillä (sektorikohtaisilla) viranomaisilla, joita CCA ohjeistaisi.

4.2.4 Ruotsi

Kyberturvallisuus on Ruotsissa integroitu kokonaisturvallisuuden tuottamisen rakenteisiin ja järjestelyihin[121]. Se on tärkeä osa varautumista ja valmiuden ylläpitämistä. Lähestymistavassa kyberturvallisuus skaalautuu kansalaisten ja organisaatioiden tietoturvasta kansainväliseen kyberturvallisuuteen (erityisesti EU ja NATO). Tavoitteena on suojella väestöä, yhteiskunnan toimivuutta ja kykyä ylläpitää perustavanlaatuisia arvoja. Myös taloudellinen kasvu riippuu kyberturvallisuudesta. Vahvat ja suhteessa toisiinsa itsenäiset toimialakohtaiset viranomaiset sääntelevät ja valvovat toimialaansa. Ne säilyttävät tehtävänsä myös kriisiaikoina[122]. Samoin rauhan aikana luodut yhteistyöjärjestelyt pysyvät häiriö- ja kriisitilanteissa (niin viranomaisten kesken kuin julkisen ja yksityisen sektorin välillä). Tavoitteena on myötävaikuttaa siihen, että internet on globaali, saavutettavissa oleva, avoin ja kestävä sekä ihmisoikeuksia kunnioittava.

Ruotsissa on vahva signaalitiedustelu- ja salausosaaminen. Valtio tiivistää turvallisuus- ja puolustusyhteistyötään mm. muiden Pohjoismaiden kanssa (ml. CERT-yhteistyö) ja vahvistaa niin siviili- kuin sotilaspuolustuskykyään[123]. Kyberturvallisuuden tuottamisessa priorisoidaan:

- Kokonaisvaltaisen, systeemisen toiminnan varmistaminen riskiperusteisesti
- Verkko-, järjestelmä- ja tuoteturvallisuuden lisääminen

[119] Nykyisin yleisesikunnan alainen C4I (command, control, communications, computers, intelligence) vastaa kaikkien tieto- ja viestintäjärjestelmien puolustuksesta, mutta tiedusteluorganisaatio hyökkäyskyvystä ja tiedustelusta. 2017 ilmoitettiin, että organisaation vastuut käännettäisiin päin vastaisiksi: C4I vastaisi jatkossa hyökkäyksestä ja tiedustelusta, tiedusteluyksiköt puolustuksesta. Lopputulema lienee vielä auki.

[120] Kuitenkin tehden yhteistyötä tiedusteluorganisaatioiden ja lainvalvontaorganisaatioiden kanssa.

[121] Ks. esim. Förutsättningar för krisberedskap och totalförsvar i Sverige (2011).

[122] Kokonaisturvallisuuden tuottamisessa toimitaan vastuuperiaatteen mukaisesti, eli normaaliaikoina jostakin asiasta vastuussa oleva taho on vastuussa siitä myös häiriötilanteissa, kriisiaikoina ja sodassa.

[123] Ks. esim. vuoden 2017 Nationell säkerhetsstrategi ja Regeringens proposition 2014/15:109. Försvarspolitisk inriktning – Sveriges försvar 2016–2020.

- Kyberhyökkäysten ja muiden kyberturvallisuustapausten estämis- ja havainnointikyvyn sekä hallinnan parantaminen
- Kyberrikollisuuden vastainen toiminta
- Tietoisuuden ja osaamisen lisääminen
- Kansainvälisen yhteistyön kehittäminen

Vastuu tietoturvallisuudesta on yksittäisillä organisaatioilla, mutta valtio voi parantaa kokonaisjärjestelmäympäristöä ja kyberturvallisuustoiminnan koordinointia. Keskeisin turvallisuuskoordinoija on **Tietoturvallisuuden koordinaatioryhmä (SAMFI)**, johon kuuluvat Yhteiskuntasuojelun ja -valmiuden viranomainen (MSB), Puolustusvoimien materiaalilaitos, Puolustusvoimien radiolaitos (FRA), poliisi, Posti- ja telehallitus (PTS) ja Turvallisuuspoliisi[124]. SAMFI:n tehtävänä on edesauttaa, että yhteiskunnassa tiedon luottamuksellisuus, oikeellisuus ja saatavuus on varmistettu. Sen toimintamuotoina ovat tiedonvaihto ja yhteistyö osallistuvien viranomaisten kesken. Hallinnollisesti toimintaa johtaa MSB, jonne on sijoitettu CERT-SE. Se toimii Ruotsin kansallisena CSIRT:nä tehtävänään tukea yhteiskuntaa tietoturvatapahtumien hallinnassa ja estämisessä sekä GovCERT:inä. Se jakaa uhkatietoa, koordinoi yhteistyötä ja toimii kansainvälisenä kontaktipintana.

MSB on keskeinen turvallisuuskoordinoija Ruotsissa. Hallinnollisesti se jakautuu neljään osastoon: yhteiskunnan turvallisuuden kehittäminen, valmiuden kehittäminen, operatiivinen osasto ja tukiosasto. MSB:n tehtävänä on kehittää yhteiskunnan kykyä estää ja hallita kriisejä. Se toimii yhteistyössä mm. kuntien, maakäräjien, viranomaisten ja eri organisaatioiden kanssa ja sillä on keskeisiä tehtäviä siviilipuolustuksessa. Se pyrkii vähentämään häiriötilanteiden vaikutuksia, seuraa ja arvioi yhteiskunnan kriisivalmiutta ja varmistaa, että annettu koulutus ja tuki vastaavat tarpeita. MSB vastaanottaa julkishallinnon pakolliset ilmoitukset vakavista tietoturvatapahtumista ja laatii vuosittaisen raportin[125] hallitukselle. Vapaaehtoista julkinen-yksityinen kumppanuutta varten se on järjestänyt useamman sektorikohtaisen tiedonvaihtofoorumin (FIDI)[126]. Vuonna 2017 annetun ehdotuksen mukaan MSB voisi tukea kriittisen infrastruktuurin toimijoiden kyberturvallisuustapausten havainnointia ja hallintaa sensorijärjestelmillä, pl. toimijat, joiden toimintaa FRA jo tukee.

Kansallinen koordinointineuvosto vakavia ICT-uhkia vastaan (NSIT) analysoi ja arvioi vakavimpia uhkia keskeisimmille toiminnoille ja näiden haavoittuvuuksia. Yhteistyöfoorumiin osallistuvat FRA, Turvallisuuspoliisi ja Puolustusvoimien sotilastiedustelu- ja turvallisuuspalvelu (MUST). ICT-toimialalla on oma kansallisen tason tiedonvaihtofoorumi, Nationella telesamverkansgruppen (NTSG). Vapaaehtoisuuteen pohjautuvan foorumin tarkoituksena on tukea alan kriittisen infrastruktuurin toimintaa kriisitilanteissa. Sen jäseninä on organisaatioita, joilla on infrastruktuurin toimintaan vaikuttavaa teknistä kykyä, laitteistoa ja resursseja[127]. Keskeisillä kriittisen infrastruktuurin toimijoilla on velvollisuus jatkuvuudenhallinnan suunnitteluun. Tieto- ja viestintäverkkojen toiminta on keskeistä kaikissa turvallisuustilanteissa, minkä vuoksi niiden sietokykyä ja varajärjestelmiä kehitetään. PTS valvoo kehitystä omalla toimialallaan tehden tiivistä yhteistyötä yksityisen sektorin kanssa. Se mm. edistää turvallisten ja tehokkaiden viestintävälineiden ja palveluiden käyttöä, sääntelee ja valvoo toimialaa sekä pyrkii vähentämään digitaaliseen viestintään liittyviä riskejä.

[124] Hyvä kuvaus viranomaisten tehtävistä löytyy SOU 2015:23 sivuilta 93-123. Viranomaistehtävistä suojelevan turvallisuuslain alaisessa toiminnassa taas SOU 2015:25 sivuilta 183-197.

[125] Raporttia varten MSB saa tapahtumatiedot myös Turvallisuuspoliisilta ja Puolustusvoimilta. Tulevaisuudessa raportointi tehdään NIS-direktiivin vaatimusten mukaisesti.

[126] FIDI Telekom, Svenskt CERT-forum, FIDI Finans, FIDI Vård & Omsorg, FIDI Drift sekä FIDI Supervisory Control And Data Acquisition (SCADA).

[127] Vuonna 2015 foorumiin osallistuivat ComHem, Hi3G, IP-Only, Netnod, Skanova, Stokab, Svenska Kraftnät, Svenska Stadsnätsföreningen, TDC, Tele2, Telenor, TeliaSonera, Teracom, Trafikverket, ICT, Försvarsmakten, Myndigheten för samhällsskydd och beredskap sekä Post- och telestyrelsen.

Suojelevan turvallisuuslain mukaan pääasiallisessa vastuussa kovimman turvallisuusytimen toiminnasta ovat Puolustusvoimat ja Turvallisuuspoliisi. Tilanteen mukaan toiminnasta päätetään yhteisymmärryksessä muiden keskeisten toimijoiden kanssa (Affärsverket svenska kraftnät, PTS, Liikennehallitus ja lääninhallitukset). Nämä voivat neuvoa ja ohjeistaa muita toimijoita myös ohi toimialakohtaisten viranomaisten. Kyberpuolustuksen perustana on kyky varmistaa yhteiskunnan elintärkeät toiminnot kaikissa tilanteissa. Tämä vaatii tehokasta tiedustelu-, puolustus- ja hyökkäyskykyä kyberympäristössä. Puolustusvoimat huolehtii em. sotilastoiminnoista muiden viranomaisten tukiessa – yhtä lailla puolustusvoimien kykyä ja resursseja voidaan käyttää siviilipuolustuksen tukemiseen tai kansainvälisissä operaatioissa. Puolustusvoimat turvaa omat järjestelmänsä ja verkkonsa, ylläpitää erillistä viestintäverkkoa (johon on pääsy myös muilla keskeisillä turvallisuusviranomaisilla), tukee tiedustelu- ja salauspalvelujen tuottamista koko yhteiskunnassa, ylläpitää FM-CERT (sotilasCERT) toimintoa ja tekee kansainvälistä yhteistyötä.

Puolustusvoimien materiaalilaitos toimii kriittisten ICT-tuotteiden ja -palveluiden sertifioijana ja osallistuu tiedustelutoimintaan. FRA:n tehtäviin kuuluu mm. signaalitiedustelu ja sen kehittäminen, havainnointi- ja varoitusjärjestelmän ja ohjeistuksen tarjoaminen kaikkien kriittisimmille yhteiskunnan toiminnoille niin hallinnossa kuin valtio-omisteissa yrityksissä, tietoturvallisuustiedon tuottaminen ja kansainvälinen yhteistyö. Sotilastiedustelupalvelu puolestaan mm. vastavaikuttaa Puolustusvoimiin kohdistuviin uhkiin ja tukee viranomaisia viestinnän turvaamisessa.

Kyberrikosten ehkäiseminen ja selvittäminen on poliisin ja turvallisuuspoliisin[128] tehtävä. Poliisin alaisuudessa toimii Kansallinen kyberrikoskeskus (SC3), joka kehittää ja tukee rikostutkimusta, kansainvälistä yhteistyötä (erityisesti Europol ja Eurojust) ja toiminnan yhtenäisyyttä. Poliisin ja tuomioistuinten kyberosaamista kehitetään edelleen, sillä mm. Rikollisuuden vähentämisen neuvosto on raportissaan[129] arvioinut tulevaisuuden haasteiden olevan niin suuria, ettei niihin kyetä nykyisillä panostuksilla vastaamaan. Turvallisuuspoliisin tehtävät liittyvät mm. digitaalisen vakoilun vastavaikuttamiseen ja kriittisten toimintojen ICT-infrastruktuurin suojaamiseen.

4.2.5 Singapore

Singaporessa kyberturvallisuuden tuottaminen lähtee liikkeelle ekosysteemiajattelusta, valtion aseman ylläpitämisestä digitaalisena keskuksena ja vahvojen kansainvälisten kumppanuuksien rakentamisesta (erityisesti ASEAN-maat[130]). Tavoitteena on parantaa kriittisen infrastruktuurin sietokykyä ja turvata kyberavaruus mm. kyberuhkien ja -rikollisuuden vastaisilla toimilla sekä tietosuojaa parantamalla. Valtion ”älykäs kansakunta” strategia rinnastuu pinta-alaltaan suurempien valtioiden ”älykkäiden kaupunkien” strategioihin. Kyberturvallisuuden tuottajina toimivat hallinnon ja yritysten ohella yksityiset kansalaiset ja yhteisöt. Kyberturvallisuuden innovaatiot ovat keino luoda taloudellisia mahdollisuuksia.

Kyberturvallisuuden tuottaminen on Singaporessa keskitetty **Kansalliseen kyberturvallisuustoimistoon (CSA)**, joka toimii Pääministerin toimiston yhteydessä. Hallinnollisesti sitä johtaa Viestintä- ja informaatioministeri. Sen tehtävänä on kyberturvallisuustoimien kehittäminen, kriittisen infrastruktuurin ja välttämättömien palveluiden suojaaminen, sekä vastuksen koordinoiminen laaja-alaisissa kyberhäiriötilanteissa. Tilannekuvatoimintonsa ansiosta se pystyy myös varoittamaan nopeasti ylisektorisista uhkista. CSA kehittää ja toimeenpanee

[128] itsenäinen (ei poliisin alainen) hallinnollinen yksikkö

[129] Brå 2016:17 It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem.

[130] Esim. ASEAN Network Security Action Council (ANSAC) edistää CERT-yhteistyötä ja osaamisen jakamista. Australian tavoin Singapore panostaa alueen teknisen kyberkyvykkyyden rakentamisohjelmaan.

kyberturvallisuussäännöstöä, -politiikkoja ja -käytäntöjä. Se koordinoi kokonaisvaltaista kyberturvallisuutta poikkihallinnollisesti ja kansainvälisesti. CSA:n osana toimiva SingCERT antaa teknistä apua ja koordinoi vastausta kyberturvallisuustapauksiin, tekee yhteistyötä muiden turvallisuustoimijoiden kanssa, identifioi turvallisuustrendejä ja jakaa ajanmukaista uhkatietoa, sekä pyrkii lisäämään yleistä tietoisuutta.

Singaporella on kansallinen vastaussuunnitelma kyberturvallisuustapauksiin, mikä mahdollistaa nopean reagoinnin ja aloitteen ottamisen paikallisella tasolla. Kokonaisvaltaista toimintaa tuetaan strategisella koordinaatiolla sektorikohtaiselta ja kansalliselta tasolta. Suunnitelmaan kuuluu kolme vastaustasoa:

- Kybertoiminta, joka uhkaa kansallista turvallisuutta;
- Sektorikohtaiset kyberhyökkäykset;
- Kyberhyökkäykset yksittäistä toimijaa kohtaan.

Kansallista laajamittaisen kyberhyökkäyksen torjuntaa johtaa poikkihallinnollinen **Kyberturvallisuuden kriisinhallintaryhmä (CMG [Cyber])**. Sitä johtaa Viestintä- ja informaatioministeriön kansliapäällikkö (Permanent Secretary). CSA tukee sen toimintaa. Ryhmään kuuluu päättäjiä hallinnon organisaatioista, jotka valvovat kriittisiä sektoreita. CMG (Cyber):llä on kaksi tehtävää: (1) se kehittää kyberturvallisuuspolitiikkoja ja -standardeja sekä valvoo kyberturvallisuustoimia kriittisillä sektoreilla, ja (2) kyberhäiriötilanteissa se laittaa liikkeelle tarvittavat resurssit sekä ohjaa ja koordinoi operatiivista vastausta.

Meneillään olevassa kyberlainsäädännön uudistuksessa CSA:lle pyritään antamaan lisävaltuuksia. Parhaiden käytäntöjen, standardien ja ohjeiden antamisen sekä kriittisen infrastruktuurin auditoinnin ohella sille tulisi valtuudet estää ja tutkia turvallisuusloukkauksia. Kyberturvallisuustapausten hoitaminen ulottuisi kaikkiin tietojärjestelmiin, ei vain kriittiseen infrastruktuuriin. Kyberturvallisuusvaltuutetulla olisi oikeus tutkia yksityisiä henkilöitä, tarkistaa tiloja ja niissä olevia laitteita, sekä vaatia yksityisiä henkilöitä avustamaan tutkimuksissa.

Singaporen tavoitteena on perustaa lisää kansallisia CIRT:ejä ja parantaa kriittisten sektoreiden jatkuvuudenhallintaa. Kyberturvallisuuslaki vahvistaisi kriittisen infrastruktuurin[131] omistajien ja operoijien velvollisuutta suojata omat järjestelmänsä ja verkkonsa. Se myös edesauttaisi kyberturvallisuustiedon jakamista CSA:n kanssa ja valtuuttaisi toimiston yhdessä sektorikohtaisten viranomaisten kanssa auttamaan kyberturvallisuustapauksen kohteeksi joutunutta tahoa sen selvittämisessä. CIRT:it koostuvat asiantuntijoista CSA:n kyberturvallisuustapauksiin vastaavasta yksiköstä, Hallituksen teknologiavirastosta (GovTech), Sisäasioiden ministeriöstä ja Puolustusministeriöstä. Ne ovat osa ykkös- ja kakkosvastaustason toimintaa.

Kyberrikollisuuden vastaista toimintaa on parannettu mm. erityisellä toimintaohjelmalla (NCAP). Sisäasioiden ministeriön alle on perustettu Kyberrikoskomentokeskus[132], joka on osa Singaporen kansallisen poliisin Rikostutkimusosastoa. Rikostutkinnassa se tekee yhteistyötä muiden lakia toimeenpanevien organisaatioiden (mm. Interpol) ja teollisuuden toimijoiden kanssa. Paikallistasolla poliisikeskukset osallistuvat jatkuvasti paikallisten yhteisöjen toimintaan.

Siviilihallinnossa nettisurffailuun käytettävät verkot erotetaan verkoista, joissa käsitellään suojattua dataa. Valvonta ja operaatiokeskus (MOCC), **Kybervalvontakeskus (CWC)**[133] ja Uhka-arviokeskus (TAC) tuottavat hallinnolle tilannekuvaa sen omista verkoista. Niiden

[131] Singaporessa on identifioitu 11 kriittisen infrastruktuurin sektoria, jotka poikkileikkaavat yleisinfrastruktuurin.

[132] Keskus perustetiin integroimalla Kansallisen poliisin kyberrikosten tutkinta-, analyysi-, tiedustelu- ja ennaltaehkäisykyvyt yhden komennon alle.

[133] CWC:n tehtävänä on valvoa hallinnon verkkoja ja varoittaa kyberuhkista niitä kohtaan.

tekniseen kyvykkyyteen panostetaan ja käyttöön otetaan kehittyviä teknologioita. Tavoitteena on parantaa turvallisuusvalvonnan tehokkuutta julkisella sektorilla ja tietoturvallisuustiedon kattavuutta, yksityiskohtaisuutta ja ajanmukaisuutta.

4.2.6 Viro

Viron lähestymistapaa kyberturvallisuuteen leimaavat (1) yhteiskunnan hyvin pitkälle edennyt digitalisaatio ja (2) yhteiskunnan turvallisuuden alttius kansainvälisen toimintaympäristön vaikutuksille. Jälkimmäisellä tarkoitetaan Viron vahvaa tukeutumista NATO:on ja EU:iin valtion turvallisuuden järjestämisessä sekä yhteistyötä Pohjoismaiden ja Baltian maiden kanssa. Kansantalouden tila reagoi myös herkästi globaaleihin kehityskulkuihin. Viroa pidetään oikeutetusti edelläkävijänä digitaalisten mahdollisuuksien hyödyntämisessä ja palveluiden kehittämisessä. Arvioiden mukaan kyberturvallisuutta ei kuitenkaan ole aina onnistuttu tuottamaan tavoitteiden mukaisesti.[134]

Virossa kyberturvallisuus on integroitu osaksi kansallista turvallisuutta. Puolustus ja sisäinen turvallisuus ovat riippuvaisia yksityisten sektorin infrastruktuurista ja resursseista, mikä lisää julkinen-yksityinen-kolmas sektori kumppanuuksien tärkeyttä. Valtio ei voi valvoa sen rajojen ulkopuolella tuotettuja palveluita tai näiden osia, mutta sen on varmistettava, että tarvittava tieto ja tietojärjestelmät ovat saatavilla kaikissa tilanteissa. Se voi avustaa elintärkeiden toimintojen ja kriittisen infrastruktuurin ylläpitäjiä koordinoimalla ja sovittamalla eri tahojen intressejä yhteen. Sen keskeiset toiminta-alueet ovat:

- Elintärkeiden toimintojen turvaaminen,
- Kyberrikollisuuden vastainen toiminta ja
- Kansallisen puolustuksen vahvistaminen.

Perusoikeuksien ja -vapauksien kunnioittaminen ja yksilönsuojan varmistaminen ohjaavat kyberturvallisuuden tuottamista. Häiriötilanteissa kyberturvallisuustoimijat säilyttävät roolinsa ja toimintavaltuutensa.

Kriisitilanteiden johtamista ohjaavat häiriötilannelaki ja poikkeustilalaki, joista kumpikin keskittyy kokonaisvaltaiseen häiriötilanteiden hoitamiseen (niissä ei mainita erikseen kyberhäiriötilanteita.). Toimintaa valvoo Sisäministeriön johtama **Kansallinen kriisinhallintakomitea**. Sisäministeriöllä on koordinaatiovastuu merkittävissä kriisitilanteissa. Tietojärjestelmäviranomainen hoitaa riskiarvioinnit ja Talous- ja viestintäministeriö vastaa häiriötilanteisiin varautumisen suunnittelusta.

Talous- ja viestintäministeriö ohjaa kyberturvallisuuspolitiikkaa ja koordinoi strategian toimeenpanoa[135]. Toimeenpano on kaikkien hallinnonalojen tehtävä; kansalaisjärjestöt, yritykset ja koulutusinstituutiot osallistuvat kuten tarpeelliseksi katsotaan. Osallistuvat organisaatiot raportoivat talous- ja viestintäministeriölle vuosittain. Valtionhallinnon turvallisuuskomitean alainen Kyberturvallisuusneuvosto tukee strategisella tasolla hallinnon yksiköiden yhteistyötä ja valvoo kyberturvallisuusstrategian toimeenpanoa. Se raportoi hallitukselle vuosittain.

Talous- ja viestintäministeriön alainen **Tietojärjestelmäviranomainen (RIA)** koordinoi valtion tietojärjestelmien ja -verkkojen kehittämistä ja hallinnointia (neuvoo ja valvoo) sekä järjestää tietoturvaan liittyvää toimintaa ja tuottaa julkaisuja. Sen toiminnan lähtökohtana on yhteiskunnan elintärkeiden toimintojen ylläpitäminen tukemalla tietoliikenneinfrastruktuurin

[134] Pernik, Piret & Emmet Tuohy (2013) Cyber Space in Estonia: Greater Security, Greater Challenges. Report. International Centre for Defence Studies.

[135] Vuoteen 2011 asti kyberturvallisuus kuului Puolustusministeriön hallinnonalaan.

toimintavarmuutta. Viranomainen myös ylläpitää e-Viron selkärankaa, X-Road palveluväylää, ja huolehtii valtion tietojärjestelmien varmuuskopioinnista. Se kehittää digitalisaatioon ja kyberturvallisuuteen liittyviä strategioita, politiikkoja, tutkimusta ja käytännön toimintaa. Sillä on myös oikeus mm. sakottaa, kuulustella henkilöitä ja tarkastaa tiloja[136].

RIA:n alainen CERT-EE vastaa Viron tietojärjestelmissä ja -verkoissa tapahtuvien turvallisuustapausten käsittelyä, mm. priorisoimalla tapaukset, analysoimalla ja vastaamalla niihin, sekä antamalla teknistä tukea tapausten ratkaisemiseen. Sen tehtäviin kuuluu myös avustaa internetin käyttäjiä ennalta ehkäisevissä toimenpiteissä ja turvallisuusuhkiin vastaamisessa. Se julkaisee tietoturvavaroituksia, pyrkii lisäämään kyberturvallisuustietoisuutta ja tukee teknisiä asiantuntijoita, joihin asiakkaat ovat todennäköisesti yhteydessä tietoturvatapausten yhteydessä. Tuen määrä ja sisältö riippuvat kyberturvallisuustapauksen vakavuudesta. CERT-EE hallinnoi virtuaalista tilannehuonetta, jolla pyritään kriisien ennaltaehkäisemiseen tarjoamalla tehokas yhteistyöympäristö palveluntarjoajille ja hallinnon organisaatioille. Hallinnon organisaatioiden on lain velvoittamina ilmoitettava kaikki merkittävät kyberturvallisuustapaukset CERT-EE:lle.

RIA:n alla myös kriittisen tietoliikenneinfrastruktuurin suojaamisosasto. Kriittisen tietoliikenneinfrastruktuurin suojaamisen komitean tehtävänä on edistää julkinen-yksityinen yhteistyötä, tuoda yhteen kyberturvallisuus- ja ICT-johtajat kriittisten palveluiden organisaatioista vaihtamaan operatiivista tietoa, tunnistamaan ongelmia ja laatimaan ehdotuksia valtion kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi.

Viron Puolustusministeriö koordinoi kansallista puolustusta. Sen alaisuuteen on järjestetty erillinen osasto, jolla työskentelee niin teknisiä kuin politiikka-asiantuntijoita. Se keskittyy kyberpuolustuspolitiikkoihin ja koordinoi hallinnonalan tietojärjestelmien kehittämistä, suunnittelee politiikkoja ja ohjaa niiden toimeenpanoa. Kyberpuolustus mainitaan yhdeksi keskeiseksi kehitettäväksi kyvyksi. Lisäksi, Viron kyberpuolustusharjoitusympäristöä ollaan laajentamassa NATO:n harjoitustoimintaan sopivaksi. Valtio rakentaakin kyberpuolustustaan yhteistyössä NATO:n kyberturvallisuuskeskuksen ja kyberyksikön (The Defence League's Cyber Defence Unit) kanssa. Jälkimmäinen on vapaaehtoisten muodostama kyberpuolustusorganisaatio, jota kehitetään julkisen, yksityisen ja kolmannen sektorin yhteistyönä. Sen osaamista hyödynnetään mm. harjoituksissa, valmennuksessa ja järjestelmätestauksessa. Sitä voidaan käyttää myös siviiliviranomaisten tukemiseen ja kriittisen infrastruktuurin suojaamiseen kriisiaikoina[137].

Asevoimien henkilöstö- ja viestipataljoonan tehtävänä on varmistaa strategisen tieto- ja kommunikaatioteknologian käytettävyys kaikissa tilanteissa. Toimintaa koordinoi Strategisen kommunikaation keskus, jonka tehtävänä on mm. käytössä olevan ICT:n suojaaminen; digitaalisten palveluiden tuottaminen Puolustusministeriön alaisille yksiköille; sähköisen, puolustuskeskeisen sodankäynnin kehittäminen; kyberpuolustuksen suunnitteleminen; ja Kyberlaboratorion[138] toiminnan järjestäminen. Poliisi- ja rajavartiolaitosneuvoston kyberrikosten tutkinta-osaaminen on koottu yhteen osastoon ja Viron sisäinen turvallisuuspalvelu (KAPO) on lisännyt kyberturvallisuuden tutkinta- ja tiedustelukykyään.

Viro panostaa näkyvyyteen ja toimintaan kansainvälisissä järjestöissä ja foorumeilla. Osa sen kyberdiplomatiaa ovat myös virtuaaliset edustustot[139], joiden tarkoituksena on varmistaa valtion olemassa olon jatkuminen, vaikka sen digitaaliset toiminnot saataisiin alas tai se

[136] Oikeudet ovat tuore lisä RIA:n toimivaltuuksiin, joten niiden käytännön merkitystä on vielä vaikea arvioida.

[137] Haasteeksi on osoittautunut mm. organisaation asema tilanteissa, joissa kybertoiminta on kohdennettavissa organisaatioon: Onko kyse Viron valtiollisesta toiminnasta vai jostain muusta?

[138] Harjoitusympäristö, jota on hyödynnetty mm. Naton harjoituksissa.

[139] Ensimmäinen tällainen edustusto avattiin Luxemburgiin vuonna 2017.

vallattaisiin. Kriittisen tiedon varastoimisella ulkomaille pyritään varmistamaan, että autentikointi- ja auktorisointipalvelut jatkuvat myös em. tilanteissa. Se on tutkimuksen valtioista ainoa, jolla on merkittävää kokemusta laajamittaisen kyberhyökkäyksen kohteeksi joutumisesta.

4.3 Analyysi vertailumaista

Kyberturvallisuuden strategisen johtamisen keskiössä ovat kansainvälisen referenssiarvioinnin perusteella **ennakointi ja aikainen havainnointi, uhkien torjuminen ennakoivasti, uhkatilanteisiin vastaaminen, sekä yhteiskunnan sietokyvyn parantaminen.** Kaikissa vertailuun valituissa valtioissa **kyberturvallisuutta tuotetaan kokonaisvaltaisesti**, kansainvälisistä kumppanuuksista yksityisiin kansalaisiin. Kyberturvallisuusjohtaminen on tavalla tai toisella organisoitua (keskitettyä: Israel ja Singapore; hajautettua keskitetyllä johdolla: Alankomaat ja Australia; hajautettua: Ruotsi ja Viro) ja **organisaatiorakenteita pyritään virtaviivaistamaan.** Johtaminen tapahtuu eri ministeriön alaisuudessa (useimmiten suoraan pääministerin alaisuudessa) ja asevoimien rooli vaihtelee valtioittain (täysin integroidusta lähes erilliseen toimijuuteen). Kyberturvallisuustapahtumiin varaudutaan yhdessä (kansainvälisten kumppaneiden kanssa, poikkihallinnollisesti ja yksityinen-julkinen yhteistyössä) ja erikseen (hallinnonala- ja organisaatiokohtaisesti) harjoittelemalla. Strategioiden toimeenpanoa seurataan vuosittaisella raportoinnilla.

Hajautettuja strategisen kyberturvallisuusjohtamisen malleja on kritisoitu toimijoiden vaikeudesta tunnistaa oma vastuunsa, mikä aiheuttaa muun muassa sitoutumisen puutetta, ongelmia tiedonkulussa ja toiminnan koordinoinnissa sekä aloitteellisuuden puuttumista. Toisaalta sektorikohtaiset viranomaiset tuntevat oman toimialansa ja sen toimijat parhaiten, mikä edesauttaa yhteistyössä onnistumista. Lisäksi **kokonaistoimintaa koordinoivilla toimijoilla pitää olla selkeä käsitys omasta tehtävästään ja riittävät valtuudet.** Keskitettyjä strategisen johtamisen malleja taas leimaa perustamisvaiheessa toimialojen kiistely kyberturvallisuuden omistajuudesta, tarve löytää resurssit uusien tai uusia valtuuksia saavien organisaatioiden järjestämiseen ja toiminnan toteuttamiseen sekä siirtymävaiheen epävarmuudet ja organisatorinen kitka. Järjestämisvaiheen jälkeen riittävällä valtuutuksella ja resursseilla (ml. osaaminen) toimivan keskitetyn johdon voi kuitenkin olettaa selkeyttävän kokonaiskyberturvallisuuden tuottamista.

Valittava strategisen johtamisen perusmalli ohjaa sitä, mitä käytäntöjä muista valtioista kannattaa harkita Suomessa sovellettaviksi. Kyberturvallisuuskeskuksen rooliin, resursointiin, hallinnolliseen sijoittamiseen ja valtuuksiin ulkomailta on löydettävissä erilaisia vaihtoehtoja (tiedottamiskeskuksesta operatiiviseen toimijuuteen), mutta vertailluista valtioista useimmissa vastaava keskus on olemassa. Alueelliset, paikallistakin osaamista hyödyntävät ”kyberturvallisuuskeskukset” voisivat parantaa alueellista tiedonkulkua ja paikallista sitoutumista. Vastaavasti voitaisiin harkita toimialakohtaisia keskuksia. Kyberrikostorjuntaan ja/tai kyberpuolustukseen on useimmissa valtioissa järjestetty omat keskuksensa.

Yritysten ja kolmannen sektorin toimijoiden tuominen mukaan strategisen kyberturvallisuuden suunnitteluun, toteuttamiseen ja johtamiseen lisäisi kokonaisvaltaisuutta ja helpottaisi varautumisvelvoitteiden perustelua. Lisäksi paras mahdollinen tieto olisi hyödynnettävissä ennakointiin, varautumiseen ja tilannejohtamisen tukemiseen. Ekosysteemiajattelun (jossa digitalisaation ja kyberturvallisuuden mahdollisuuksia ja riskejä arvioidaan yhdessä kaikilla yhteiskunnan osa-alueilla) tuominen mukaan strategiseen johtamiseen vahvistaisi valtion roolia, mutta voisi samalla kasvattaa sen roolia esimerkiksi kyberturvallisuustutkimuksen rahoittamisessa ja/tai yksityisen rahoituksen houkuttelemisen tukemisessa.

Kansallisten strategioiden ohella Suomessa voitaisiin harkita julkista strategiaa valtion rajojen ulkopuolella tapahtuvan kyberturvallisuustyön ohjenuoraksi. Myös valtion ”virtuaalisen olemassaolon” varmistamista laaja-alaisen yhteiskunnallisen häiriö- tai poikkeustilan aikana voisi miettiä digitalisaation ulottuessa yhä syvemmälle yhteiskunnan rakenteisiin.

5. KANSAINVÄLISET JA KANSALLISET KYBERTURVALLISUUDEN MITTAAMISEN KEHIKOT JA MENETELMÄT

5.1 Tutkimuksen lähtökohta

Kyberturvallisuuden mittaaminen ja ymmärtäminen ovat osa ylimmän johdon johtamista ja päätöksentekoa sekä käytännön toimintatapoja. Kyberturvallisuus on kiinteä osa kansallista kokonaisturvallisuuden mittaamista, raportointia ja johtamista. Kansallisella tasolla tulee keskittyä sellaisen mittariston kehittämiseen, joka kuvaa kybersuorituskyvykkyyttä strategisella tasolla.

Suomen kyberturvallisuusstrategiassa esitetty linjaus strategian toimeenpanon valvonnan ja toteutumisen seurannasta ei ole onnistunut parhaalla mahdollisella tavalla. On tärkeää, että määritettyjen toimenpiteiden ja hankkeiden etenemistä seurataan ja mitataan säännöllisesti, jolloin saadaan parempi kokonaiskuva kyberturvallisuuden sen hetkisestä kehittämisen tilasta. Mittaamisen keinoja on jatkuvasti kyettävä kehittämään erityisesti toimenpiteiden laadun seurannassa. Tavoitteena tulisi kypsyysmallin ja mittariston avulla toteutettava vuosittainen arviointi Suomen kyberturvallisuuden tilasta. Tuloksena syntyisi siis vuosittainen kyberturvallisuus-arvio, jossa tarkastellaan tässäkin tutkimuskokonaisuudessa esillä olevia kyberturvallisuuden eri osa-alueita ja niiden senhetkistä tilaa.

Suomeen on tärkeä muodostaa kyberturvallisuusarvioinnin malli, jolla esimerkiksi yritykset ja organisaatiot voivat arvioida kyberturvallisuutensa tasoa, tulla tietoisiksi heikkouksistaan ja puutteellista varautumistoimistaan sekä huolehtia vähintään perusasioiden kuntoon laittamisesta. Yhteiskunnan kriittisten toimintojen osalta vuosittaiset kyberturvallisuuden tason arvioinnit on tarvittaessa tehtävä pakollisiksi. Tällä hetkellä Suomessa ei ole olemassa selkeitä kyberturvallisuuden tason mittareita, mikä hankaloittaa alueen kehityksen kokonaisvaltaista arviointia.[140]

5.2 Kyberturvallisuuskyvykkyyden mittaaminen

5.2.1 Perusteita

Kyberturvallisuuden mittariston määrittelyn pääasiallisena tarkoituksena on antaa tarvitsijalleen yleiskatsaus siitä, miten kansallisen kyberturvallisuuden toimeenpano-ohjelman edellyttämät tehtävät ovat edenneet ja miten jatkossa eri toimenpiteitä tulisi kehittää.

Yhteiskunnan tietotekniset palvelut kehittyvät jatkuvasti, jolloin sen riippuvuus palvelujen sisältämistä tekniikoista ja verkostoista kasvaa. Näin muodostuva kansallinen kybertoimintaympäristö on monimutkainen ja jatkuvasti dynaamisesti muuttuva. Kansallisen kyberturvallisuuden kehittämiseen ja mittaamiseen on aloitettu kiinnittämään yhä enemmän huomiota. Niinpä viime vuosina on käyttöön ilmestynyt useita mittaristoja, mutta niiden käyttö on vasta alkuvaiheessa.[141]

[140] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017

[141] Rikk Raul, Analytical Article How to Measure National Cyber Security: the development of national cyber security index, 2017

Kuten edellä on todettu, kyberkyvykkyyden mittaamiseen ei ole käytettävissä kansainvälisesti vakiintunutta yhtä menetelmää. Mittareiden vertaamiseksi ja kansallisen mittarin valinnalle onkin aluksi syytä asettaa ensisijaisia vaatimuksia. Vaatimukset voidaan johtaa tarkasteltavan mittauskohteen osalta yleisiä mittaamiseen liittyviä näkökulmia noudattamalla.

Daniel Miessler on listannut organisaation pääasialliset näkökulmat mittariston kehittämiselle seuraavasti:[142]

1. Päätöksenteko (Tarina): Mittariston tulisi tukea päätöksentekoa. Jos näin ei tapahdu, todennäköisesti organisaatiossa tuhlataan resursseja.

2. Kouriintuntuva (Ymmärrettävä): Mittariston tulisi olla määritettävissä käyttäen numeroita, jolloin voidaan käyttää luokittelua, kuten korkeaa, keskikokoista tai matalaa (tai muuta laadullista merkintää) ja näin estää turha hienosäätö.

3. Kehitystä tukeva: Mittariston tulisi vastata tavoiteltavia strategisia turvallisuustekijöitä. Tämä ei tarkoita lyhytaikaista kehitystä, vaan pikemminkin se huomioi kohteen kokonaisstrategian ja tiedon suunniteltujen tavoitteiden saavuttamisesta.

4. Data-perusteinen: Mittaristolla tulee olla taustalla luotettava data.

5. Toistettava: Mittaristolla pitäisi olla helppo kerätä tietoja ja päivittää niitä säännöllisesti. Hyvät (toistettavissa olevat) tiedot ja automaatio voivat auttaa kääntämään tarvittavat toimenpiteet oikeaan suuntaan.

6. Resurssiin sopeutettu: Koko mittariston on oltava organisaation resurssien mukaan ylläpidettävissä.

7. Diskreetti: Mittaristo on yleensä jaoteltava osiin siten, että se kohdentuu oikein mitattaviin suureisiin. Tämä tavoite palvelee mittariston läpinäkyvyyttä ja siitä saatavien tietojen käytettävyyttä.

8. Merkittäviin seikkoihin kohdentuva: Mittariston tule kohdentua asioihin, joita halutaan seurata eikä ohjautua helposti saatavien tietojen mittaamiseen.

9. Arviointikohteiltaan optimaalinen: Mittariston laajuus tulee harkita tarkoin. Suuri määrä mitattavia suureita saattaa johtaa tarpeettoman mittaamiseen ja johtaa tavoitetilan kannalta katsottuna harhaan.

Luettelossa esitettyjä organisaation toiminnan mittaamisen pääasiallisia näkökulmia on tässä tutkimuksessa käytetty arviointiperusteena myös kansallisen mittariston valinnan osalta.

5.2.2 Mitattavat asiat

Suomen kansallista kyberstrategian toimeenpano-ohjelmaa on päivitetty. Uusi ohjelma käsittää vuodet 2017-2020. Siinä tarkastellaan kyberturvallisuuden kehittämistä valtion, maakuntien, kuntien, yritystoiminnan ja kolmannen sektorin muodostamassa palvelukokonaisuudessa, jossa kansalainen on asiakkaana. Digitaalisista palveluista ja niiden

[142] Miessler, Daniel, An Information Security Metrics Primer

kyberturvallisuudesta valtaosa tuotetaan elinkeinoelämän toimesta kansallisissa ja kansainvälisissä palvelukokonaisuuksissa ja verkostoissa.[143]

Toimeenpano-ohjelman 2017-2020 toimenpiteet on valittu siten, että ne edistävät vision saavuttamista ja ovat strategisten linjausten mukaisia. Toimenpiteiden valinnassa on painotettu vaikuttavuuden näkökulmaa korostaen kansalaista julkisen hallinnon palveluiden asiakkaana, elintärkeiden toimintojen turvaamista sekä julkisen hallinnon että elinkeinoelämän, tiede- ja tutkimusmaailman välistä yhteistyötä. Toimeenpano-ohjelma kokoaa julkisen hallinnon sisäiset ja yhdessä elinkeinoelämän sekä järjestöjen kanssa toteutettavat laaja-alaiset ja merkittävät tieto- ja kyberturvallisuutta parantavat hankkeet ja toimenpiteet yhteen ja tuo ne näkyville yhdenmukaisesti jäsennettynä ja vastuutettuina. Toimeenpano-ohjelmaan sisällytettynä hankkeiden ja toimenpiteiden etenemistä on mahdollista säännöllisesti seurata ja mitata, jolloin on myös mahdollista saada parempi kokonaiskuva kyberturvallisuuden kehittämisen tilanteesta. Mittaamisen keinoja on jatkuvasti kehitettävä erityisesti toimenpiteiden laadun seurannassa. Toimeenpano-ohjelmaan valittujen laajasti vaikuttavien toimenpiteiden lisäksi kyberturvallisuutta parannetaan jatkuvasti myös muilla hallinnonalakohtaisilla toimenpiteillä sekä kyber- ja tietoturvallisuuden ja toiminnan jatkuvuuden hallinnan kehittämiseen liittyvällä työllä. Kun toimeenpano-ohjelmaa tarkastellaan ja mitataan vuosittain, voidaan siinä yhteydessä toimenpiteitä muuttaa, lisätä tai poistaa.[144]

Kyberturvallisuusstrategian strategiset linjaukset ovat:

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

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

3. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisenkannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennaltaehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.

7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.

8. Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.

[143] Turvallisuuskomitea, Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017

[144] Ibid.

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

10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Toimeenpano-ohjelma jakaantuu kolmeen kokonaisuuteen, joissa vastataan seuraaviin kysymyksiin: [145]

1. Johtamisella on varmistettu kyberturvallisuuden vision saavuttaminen
   Mitä johtamisen ja ohjauksen rakenteita, malleja ja lainsäädäntöä tulisi luoda kyberturvallisuuden vision saavuttamiseksi? Mitä hallinnon ja elinkeinoelämän sekä järjestöjen yhteisiä tilanneymmärryksen keräämisen ja jakamisen malleja tulisi luoda ja kehittää?

2. Yhteiskunnan digitalisoidut elintärkeät toiminnot ovat turvatut
   Mitä laaja-alaisesti vaikuttavia hallinnollisia ja teknisiä toimenpiteitä tarvitaan, jotta kybertoimintaympäristöön voidaan luottaa normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa?

3. Kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä
   Mitä osaamisen kehittämisen kokonaisuuksia tulisi olla saatavilla kansalaisille, elinkeinoelämälle ja hallinnolle? Kuka tarjoaa osaamisen kehittämisen kokonaisuuksia ja tuottaa tutkittua tietoa?

Suomen kansallinen kyberstrategian toimeenpano-ohjelma painottaa myös elinkeinoelämän keskeistä merkitystä kansalaisten digitaalisten palveluiden tuottamisessa. Niissä on mukana laaja joukko yrityksiä, joiden kyberturvallisuudesta valtaosa tuotetaan kansallisissa ja kansainvälisissä palvelukokonaisuuksissa ja verkostoissa. Yrityksillä onkin yhä kasvava tarve oman kyberturvallisuutensa mittaamiseen.

Kansallisen kyberturvallisuuden mittaamiseen liittyykin useita eri näkökulmia. Valittavan mittarin tulee ensisijaisesti soveltua kyberstrategian toimeenpano-ohjelman ja siten kansallisen kyberturvallisuuden kyvykkyyden kehittymisen mittaamiseen. Toisaalta kansallista kyvykkyyttä on syytä arvioida myös verrokkimaita vasten, jolloin mittarin tulisi olla kansainväliseen vertailuun soveltuva. Lisäksi valittavalle mittarille olisi eduksi, jos elinkeinoelämän yritykset voisivat soveltaa sitä edes joiltakin osiltaan käyttöönsä.

5.3 Kyberturvallisuusmittareita

5.3.1 Global Cybersecurity Index, GCI[146]

International Telecommunication Union (ITU) on kehittänyt vuonna 2014 kansalliseen kyberturvallisuuden arvioimiseen mittariston, jonka nimi on Global Cybersecurity Index, (GCI). Se mittaa kehitystä viidellä alueella:[147]

1. Oikeudelliset toimenpiteet,

[145] Turvallisuuskomitea, Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017

[146] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[147] ITU, Global Cybersecurity Index 2017

2. Tekniset toimenpiteet,
3. Organisoituminen,
4. Valmiuksien kehittäminen,
5. Yhteistyö.

Mitattavia alueita voidaan kuvata seuraavasti:[148]

- Lainsäädäntö mittarina kuvaa yhtenäisten kyberturvallisuuteen liittyvien oikeudellisten puitteiden luomista yhteiskunnassa. Se mittaa rikosten tutkinnan ja syytteeseenpanon sekä seuraamusten määräämisen toteutumista.

- Teknologia on keskeisessä roolissa kyberturvallisuuden toteutumisessa. Ilman riittäviä teknisiä toimenpiteitä ja kykyä havaita ja reagoida kyberturvallisuutta uhkaaviin tapahtumiin kasallinen kyberturvallisuus on haavoittuva. Teknisiä toimenpiteitä voidaan mitata alan toimintaan hyväksyttyjen laitosten olemassaololla ja kattavuudella (lukumäärällä).

- Organisaatio ja menettelytavat ovat välttämättömiä kaikkien kansallisten aloitteiden asianmukaisen täytäntöönpanon kannalta. Se sisältää strategiset tavoitteet, johon sisältyy kattava suunnitelma tavoitteista, toteutuneista toimenpiteistä ja niiden mittaamisesta. Mittaaminen kohdistuu kyberturvallisuuteen liittyvien strategioiden olemassaoloon ja toimijoiden lukumäärään.

- Kapasiteetin rakentaminen on olennaista kolmelle ensimmäiselle toimenpiteelle (oikeudellinen, tekninen ja organisatorinen). Teknologian, riskien ja niiden vaikutusten ymmärtäminen auttaa kehittämään strategioita, niihin liittyviä toimintatapoja ja lainsäädäntöä. Kapasiteetin rakentamista voidaan mitata tutkimus- ja kehitystoiminnan, koulutusohjelmien ja sertifioitujen ammattilaisten ja julkisen sektorin toimijoiden olemassaololla ja lukumäärällä.

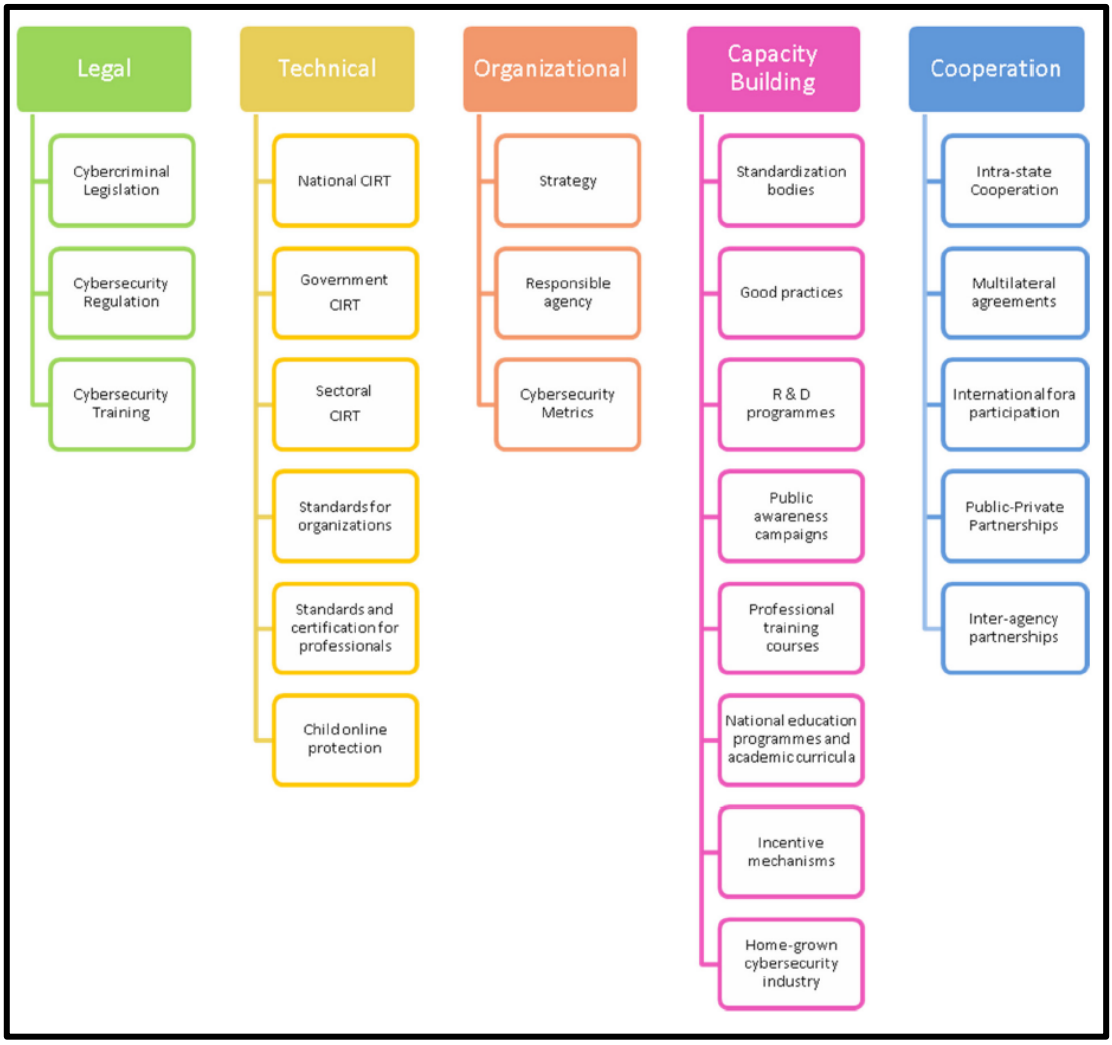
- Kyberturvallisuus edellyttää kaikkien yhteiskunnan sektorien ja tieteenalojen panostusta sen huomioimiseen laajasti koko yhteiskunnan toimintaympäristössä. Yhteistyö lisää vuoropuhelua ja koordinointia, mikä puolestaan mahdollistaa kattavien kyberturvallisuutta lisäävien toimenpiteiden soveltamista yhteiskunnassa. Kansallista ja kansainvälistä yhteistyötä voidaan mitata kumppanuuksien, yhteistyötä edistävien toimenpiteiden ja tiedon jakamisen toteutumisen ja määrän perusteella.

Kyselylomake koostuu kuvan 3 alakohdista. Näiden 25 indikaattorin arvot perustuvat 157 kysymykseen. Näin kyselytutkimukselle saavutetaan tarvittava laajuus ja varmistetaan vastausten tarkkuus ja laatu.

Mittarin metodologiassa on tapahtunut kehitystä vuosien 2014 ja 2017 aikana suoritettujen tutkimusten välillä. Kunkin kohteen arvioinnissa on siirrytty kolmen tason arvioinnista ns. binäärijärjestelmään, jossa arvioidaan jonkin tietyn toiminnan, osaston tai toimenpiteen olemassaoloa tai puuttumista. Toisin sanoen "osittaisia" toimenpiteitä ei oteta huomioon kuten aiemmin on tehty. Toisaalta jälkimmäiseen tutkimukseen on sen jokaiseen viiteen pilariin lisätty useita uusia kysymyksiä tutkimuksen syvyyden tarkentamiseksi.

Kuvaan 3 on havainnollistettu mittariston rakenne ja sisältö.

[148] ABI Research, Global Cybersecurity Index & Cyberwellness Profiles April 2015



Kuva 3. GCA:n osa-alueet ja niiden sisällöt[149]

Mittaristo ei pyri määrittämään tietyn toimenpiteen tehokkuutta tai jonkin toimenpiteen toteutumisen tilaa, vaan kansallisten rakenteiden olemassaoloa. Mittariston tulosten vertailussa monet maat jakavat saman sijoituksen, mikä osoittaa, että niillä on sama mittariston antama indeksilukema.

Uusimmassa vuoden 2017 indeksissä Euroopan maiden joukossa Suomi oli sijalla kuusi edellään Viro (1), Ranska (2), Norja (3), Iso-Britannia (4) ja Alankomaat (5). Aikaisemmasta vertailusta Suomen sijoitus on pudonnut yhdellä. Kuitenkin kokonaisindeksi oli noussut edellisestä 0.6176 arvoon 0.741, mikä tarkoittaa Suomen kehittyneen edellisestä arvioinnista, mutta osassa maita kehitys on ollut vieläkin voimakkaampaa. Kansainvälisessä vertailussa Suomen sijoitus oli kuudestoista, kun edellisessä indeksissä sijoitus oli kahdeksas. Kansainvälisessä vertailussa Singapore oli noussut sijalle yksi ohi Yhdysvaltain, joka oli sijalla kaksi. Sijalla kolme oli Malesia ja sijalla neljä Oman ja Viro sijalla viisi. [150]

5.3.2 EU Cybersecurity Dashboard

Tämä eurooppalainen mittaristo on tarkoitettu jäsenvaltioissa kybertuvallisuuden kartoittamiseen EU: n tasolla. Business Software Alliance -raportti vuoden 2015 aineiston perusteella

[149] ITU, Global Cybersecurity Index 2017

[150] Ibid.

tarjoaa kattavan yleiskuvan mittarista. Raportissa tarkastellaan kutakin EU: n jäsenvaltion tietotekniikkavarmuuspolitiikan viittä keskeistä osa-aluetta:[151]

1. Tietoverkkoturvan oikeudelliset perusteet
2. Toiminnalliset valmiudet
3. Julkisen ja yksityisen sektorin kumppanuudet
4. Alakohtaiset kyberturvallisuussuunnitelmat
5. Koulutus

Kuvasta 4 ilmenee luettelo osa-alueiden kysymyksistä ja niiden mitta-asteikko. Kysymyksiä on yhteensä kaksikymmentä viisi. Ne kuvaavat samalla osa-alueiden sisältöjä. Mittaristo mittaa kansallisten kyberturvallisuuden rakenteiden olemassaoloa. Kuvasta ilmenee myös Suomen tilanne vuoden 2015 aineiston perusteella.[152]

[151] BSA The Software Alliance (2017), EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

[152] BSA The Software Alliance (2017), EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

EU Cybersecurity Maturity Dashboard 2015

✔ Yes ✖ No ◑ Partial Exit Fullscreen

#	Question	Cyprus	Czech Republic	Denmark	Estonia	Finland
	LEGAL FOUNDATIONS					
1.	Is there a national cybersecurity strategy in place?	✔	✔	✖	✔	✔
2.	What year was the national cybersecurity strategy adopted?	2013	2011	—	2014	2013
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	✔	✖	✔	✔
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	✔	◑	✔	◑
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	◑	✔	✔	✔	✔
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✖	✔	✔	✔	✔
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	◑	✖	✔	✔
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	✔	✖	✔	✔
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	✖	✖	✖	✖
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	✔	✖	✔	✖
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	✔	✔	✔	✔
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	N/A	◑	✔	✔	✔
	OPERATIONAL ENTITIES					
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✖	✔	✔	✔	✔
2.	What year was the computer emergency response team (CERT) established?	—	2011	2009	2008	2014
3.	Is there a national competent authority for network and information security (NIS)?	◑	✔	✔	✔	✔
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✖	✔	✔	✔	✔
5.	Are national cybersecurity exercises conducted?	◑	◑	✔	✔	✔
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	✔	◑	◑	✖
	PUBLIC PRIVATE PARTNERSHIPS					
1.	Is there a defined public private partnership (PPP) for cybersecurity?	◑	✖	✖	◑	◑
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	✖	✔	◑	✔
3.	Are new public private partnerships in planning or underway (if so, which focus area)?	✖	◑	✖	✖	✖
	SECTOR SPECIFIC CYBERSECURITY PLANS					
1.	Is there a joint public private sector plan that addresses cybersecurity?	◑	✖	✖	✖	◑
2.	Have sector specific security priorities been defined?	✖	✖	✖	✖	✖
3.	Have any sector cybersecurity risk assessments been conducted?	✖	✔	✖	✖	✖
	EDUCATION					
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✖	✔	✖	✔	✔

Kuva 4. EU Cybersecurity Dashboard-mittarin rakenne.[153]

5.3.3 Viron National Cyber Security Index[154]

Viron e-Governance Akatemian yhteistyössä Viron ulkoasiainministeriön kanssa kehittämä kansallinen tietoturvaindeksi mittaa kansallista valmiutta estää keskeisten kyberturvallisuus-riskien toteutuminen ja kykyä hallita omia toimenpiteitään niihin liittyvissä rikoksissa ja

[153] BSA The Software Alliance (2017), EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

[154] http://ncsi.ega.ee/methodology/

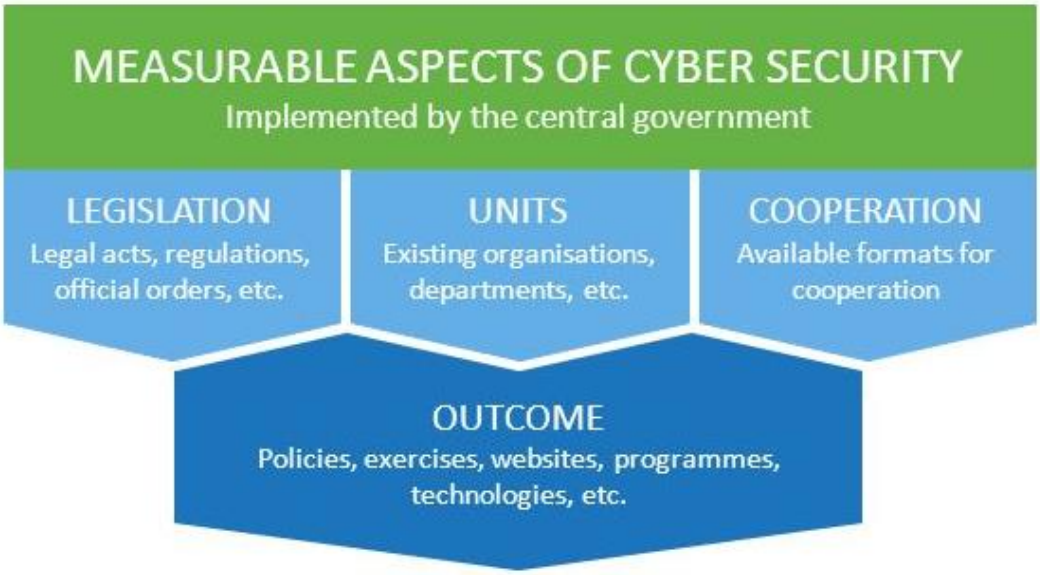
laajoissa verkkohyökkäyksissä. Mittaria voidaan käyttää kansallisen kyberturvallisuuskapasiteetin rakentamisen mittarina. Indeksi mittaa erityisesti kansallista varautumista kyberhyökkäyksiin, joiden kohteena voi olla sähköisten palvelujen estyminen, tietojen eheyden rikkoutuminen tai tietojen luottamuksellisuuden vaarantuminen.[155]

Indeksi perustuu kahteentoista kansallista kapasiteettia kartoittavaan osa-alueeseen (kts. kuvat 5 ja 6), jotka ovat järjestetty neljään ryhmään seuraavasti:

- Yleiset kyberturvallisuusindikaattorit
- Kyberturvallisuuden perusindikaattorit
- Tapahtumien ja kriisinhallinnan indikaattorit
- Kansainväliset tapahtumaindikaattorit

Jokaista kahtatoista osa-aluetta kohti mittarissa on neljä kyberturvallisuuden näkökulmaa. Nämä ovat voimassa oleva lainsäädäntö, toimivat yksiköt, yhteistyöjärjestelyt ja erilaisten prosessien tulokset. Mittarin toiminta perustuu asiantuntijaryhmän arvoihin, jotka muodostuvat eri kyberturvallisuusnäkökulmista seuraavasti: [156]

- Lainsäädäntö: 1 piste, jos lainsäädäntöä on olemassa.
- Toimivat yksiköt: 2-4 pistettä, jos alueella on vastuuyksikkö.
- Yhteistyöjärjestelyt: 2 pistettä, jos alueella on käytössä jokin yhteistyömalli (neuvosto, komitea jne.)
- Prosessien tulokset: 1-3 pistettä, jos alueella on esittää toimintaprosessistaan tuloksia tulos (asiakirja, toimenpide, tekniikka jne.)

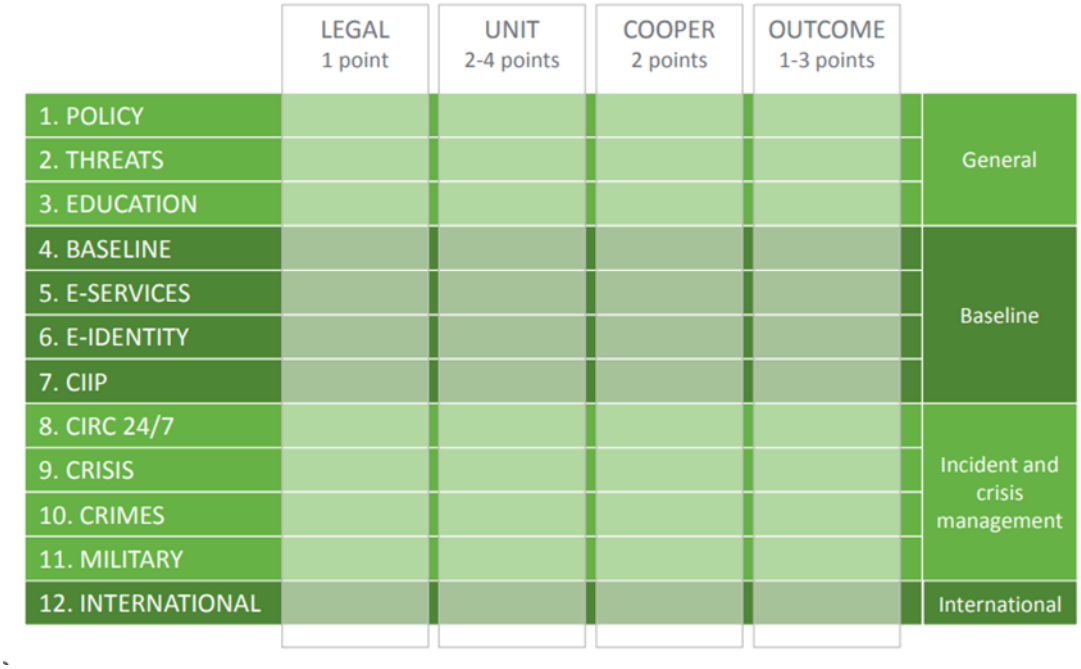


Kuva 5. NCSI-mittarin mitattavat osa-alueet.[157]

[155] EGA. e-Governance Academy. (2017) National Cyber Security Index (NCSI). Methodology description

[156] Ibid.

[157] Ibid.



Kuva 6. NCSI-mittarin rakenne[158]

Liitteessä 1 on kuvattu taulukossa 4 NCSI-mittarin rakenne alakriteereineen ja kansallisen kyberturvallisuuden toimeenpano-ohjelman eri kohtien vastaavuus.

Mittarin käytöstä on referenssejä useista eri maista (yli 30 maata arvioitu). Suomi toteuttaa parhaillaan mittarin mukaista arviointia.

5.3.4 Cyber Security Capability Maturity Model (CMM)[159]

The Global Cyber Security Capacity Centre at the University of Oxford (2014) on kehittänyt mittausmallin, jolla voidaan arvioida kansallista kyberturvallisuuden kypsyystilaa hyödyntäen viittä arviointialuetta (ulottuvuutta). Malli mahdollistaa tutkimuskohteen itsearvioinnin sekä lisäksi mahdollisuuden vertailla ja suunnitella kyberturvallisuuden investointeja, strategioita ja asettaa prioriteetit kapasiteettinsa ja kyvykkyyksiensä kehittämiseen.

Mallissa kyberturvallisuutta tarkastellaan siis viidellä ulottuvuudella, jotka kattavat:

- Laaditun kyberturvallisuuden politiikan ja puolustuksen (kuusi arviointikohdetta)
- Kannustavan ja vastuullisen yhteiskunnan kyberturvallisuuskulttuurin (neljä arviointikohdetta)
- Työvoiman ja johtamisen kyberturvallisuustaitojen rakentamisen (neljä arviointikohdetta)
- Tehokkaiden laillisuus- ja säätelymekanismien luomisen (kolme arviointikohdetta)
- Riskikontrollien kattavuuden läpi tekniikan ja toimintaprosessien (kolme arviointikohdetta).

Kussakin ulottuvuudessa on useita tekijöitä, jotka kuvaavat kyberturvallisuuden hallintaa tutkimuskohteessa huomioiden sen erilaiset kyvykkyys- ja kapasiteettitekijä jokaisen ulottuvuuden osalta. Tavoitteenamme on tunnistaa ulottuvuuksista eri tasot aina alimmasta kyvykkyyden ja

[158] EGA. e-Governance Academy. (2017) National Cyber Security Index (NCSI). Methodology description

[159] Global Cyber Security Capacity Centre University of Oxford (2014). Cyber Security Capability Maturity Model (CMM) – V1.2

kapasiteetin tasosta aina korkeimman tason strategiseen lähestymistapaan asti sekä kykyyn optimoida toimintaympäristön näkökohdat (toiminta, uhka, sosioekonominen ja poliittinen). Mittaristoa pitää sisällään kyvykkyyden kypsyysasteen arviointiin viisi tasoa kutakin arviointikohdetta kohden:

1. Aloitustaso: Arviointikohteesta ei ole tunnistettavissa oleellisia kehitysaskeleita. Se voi pitää sisällään alustavia aikeita kybervalmiuksien kehittämisestä, mutta konkreettisia toimia ei ole tehty. Konkreettista toimenpiteistä ei ole todisteita.

2. Kehittyvä taso: Arviointikohteesta voidaan tunnistaa kybervalmiuksien toimenpiteitä, jotka ovat alkaneet hahmottua, mutta voivat vielä olla ”ad hoc” tyyppisiä ja vielä vasta alustavasti määriteltyjä. Todisteita toiminnasta voidaan selvästi osoittaa.

3. Vakiintunut taso: Arviointikohteesta on tunnistettavissa kybervalmiuteen liittyviä toimenpiteitä ja ne ovat käytössä. Resurssien kohdentamisessa on vielä kehitettävää. Toiminnan arviointi on käytössä.

4. Strateginen taso: Arviointikohteen osalta on tehty valintoja siitä, mitkä toiminnat ovat kybervalmiuden osalta tärkeitä ja mitkä ovat vähemmän tärkeitä kyseiselle arviointikohteelle. Resurssien käytön suhteen on tehty valintoja (priorisoitu). Strateginen taso heijastaa pitkälti toiminnan ja sen resursoinnin valintojen priorisointeja. Niiden pitäisi huomioida kansakunnan / organisaation erityiset olosuhteet.

5. Dynaaminen taso: Dynaamisella tasolla arviointikohteessa on olemassa selkeät mekanismit strategian muuttamiseksi riippuen vallitsevista olosuhteista: esimerkiksi uhkaympäristö, globaali konflikti tai merkittävä muutos yhdellä ongelma-alueella kyberrikollisuus. Dynaamiset organisaatiot ovat kehittäneet menetelmiä strategioiden muuttamiseksi harppauksin, "sense-and-respond" tavalla. Toimintaympäristön jatkuva huomioiminen, nopea päätöksenteko ja resurssien kohdentaminen ovat tällä tasolla tyypillisiä ominaisuuksia.

Mittaristo mukainen arviointityö sisältää neljä peruskomponenttia:

- Ulottuvuus
- Arviointikohde
- Mittari (arviointikohteen osatekijä)
- Arviointitulos viisiasteisella arviointiasteikolla

Esimerkiksi arviointiulottuvuus ”laaditun kyberturvallisuuden politiikan ja puolustuksen” sisältää kuusi arviointikohdetta, yhteensä neljäkymmentäneljä arviointialuetta. Mittaristossa näitä arviointikohteita on yhteensä kaksikymmentä, joita arvioidaan edellä kuvatulla viisiasteisella arviointiasteikolla.

Liitteen 2 taulukossa 6 on esitetty CMM-mittarin rakenne ja kansallisen kyberturvallisuuden toimeenpano-ohjelman vastaavuus.

Taulukossa 1 on esimerkki CCM-mittarista dimension 1 (Cyber Security Policy and Strategy), osan DI-1 (National Cyber Security Strategy) kategorian Strategy Development osalta. [160]

[160] Global Cyber Security Capacity Centre University of Oxford (2014). Cyber Security Capability Maturity Model (CMM) – V1.2

Taulukko 1 CCM-mittari

D1-1: National Cyber Security Strategy					
Categories	Start-Up	Formative	Established	Strategic	Dynamic
Strategy Development	Little or no evidence exists of a cyber security national strategy, although some cyber component may be the responsibility of one or more departments of government. This will have been developed without broad, cross-governmental consultation. Cyber security strategy development may acknowledge societal values, traditions, and legal principles but will not be the result of wide consultation with stakeholders. Advice may have been sought from international partners.	An outline national cyber security strategy has been articulated built on a foundation of government consultation. Some relevant departments have contributed. Processes for strategy formation and renewal have been initiated. Consultation processes will have been established for key stakeholder groups, including international partners.	A national cyber security strategy has been established. Agreement has been reached on the content of, and responsibility for a specific mandate to consult across public and private sectors and civic society. Consultation processes will have been followed and observations fed back to the identified strategy 'owners'. Data and historic trends are used to predict, identify and plan. An understanding of national cyber security risks and threats drives capacity building at a national level.	Representation of the overarching national cyber strategy can be made with authority and confidence by multiple stakeholders across government. Wider stakeholders feel they understand how their interests are represented and are confident of the processes by which they can influence strategy. Strategy review and renewal processes are confirmed. Regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience are conducted. Metrics and measurement processes are implemented and inform decision making. Cyber security strategic plans, aligned with national strategic plans, drive capacity building and investments in security.	Continual revision and refinement of cyber security strategy is conducted responsively to adapt to changing socio-political, threat and technology environments. Promotion of trust and confidence building measures (TCBMs) is undertaken to ensure the continued inclusion and contribution of all stakeholders including the private sector and international partners. Wide and continuous societal participation in cyber security issues.

Mittariston käytöstä on olemassa referenssi Oxfordin yliopiston, Kosovon valtion ja Maailman pankin yhteistyössä toteutetusta arviointitapahtumasta vuodelta 2015.[161]

5.3.5 Cyber Readiness Index 2.0 (CRI)

Potomac Institute for Policy Studies tutkimuslaitoksen mittariston pääasiallisena tavoitteena on kansallisen kyberturvallisuuden kypsyyden tilan osoittaminen perustaksi kehitystyön edellyttämille jatkotoimenpiteille. Mittariston rakenne määrittää kybervalmiuden tavoitetilan ja mittaa sen toteutumista kolmessa valmiustasossa: riittämätön, osittain toiminnassa tai täysin toiminnassa. Menetelmän julkaisemisen jälkeen sillä on profiloitu ja julkaistu yhdeksän maakohtaista tulosta. Maat ovat Ranska, Saksa, Intia, Italia, Japani, Alankomaat, Saudi-Arabia, Iso-Britannia ja Yhdysvallat.[162]

Analyysi sisältää yli seitsemänkymmentä arviointikohdetta seuraavissa seitsemässä kyberturvallisuuteen vaikuttavassa osa-alueessa:

1. Kansallinen strategia
2. Tapahtumiin reagointi
3. Rikollisuus ja lainvalvonta

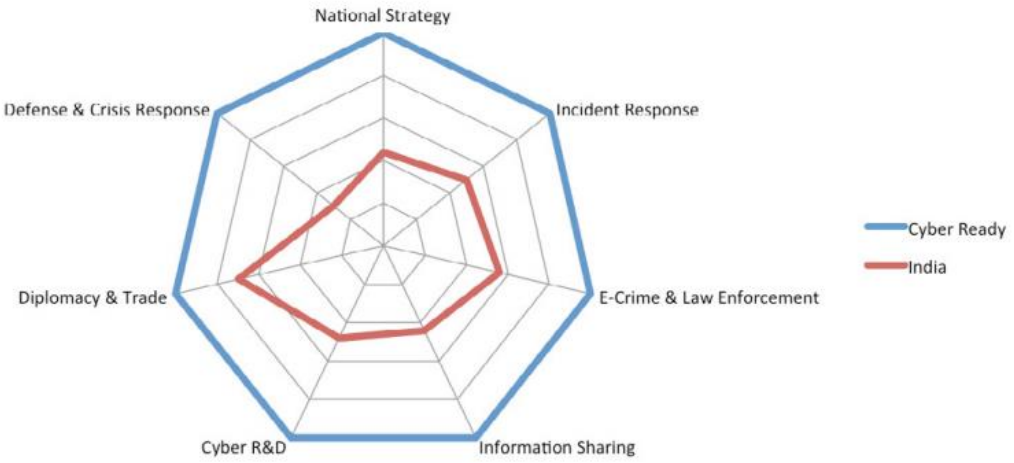
[161] The World Bank (2015). The World Bank Supports the Strengthening of Cyber Security in Kosovo

[162] Hathaway Melissa, Demchak Chris, Kerben Jason, McArdle Jennifer, Spidalieri Francesca, Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index, 2015

4. Tietojen jakaminen
5. Investoinnit tutkimukseen ja kehittäminen
6. Diplomatia ja kauppa
7. Puolustus ja kriisinhallinta

Edellä mainittuja osa-alueita arvioidaan neljän näkökulman mukaisesti, jolloin saadaan arviointiin muodostettua seitsemänkymmentä kohdetta. Otsikot ovat julistus, organisoituminen, resurssit ja toteutus. Kunkin arviointikohde (sanallisesti kuvattu) arvioidaan kolmessa kyberturvallisuuden valmiustilassa: riittämätön näyttö/todiste, osittain toiminnassa tai täysin toiminnassa.

Vuonna 2016 mittaristolla on arvioitu mm. Intian kyberturvallisuuden tilaa, jota voidaan käyttää esimerkkinä mittariston käytöstä. Sen tuloksista on julkaistu raportti joulukuussa 2016, missä tulokset on esitetty yhteenvetona graafisella asteikolla kuvan 7 mukaisesti.



Kuva 7. Esimerkki Intian kyberturvallisuuden mittaustuloksista.[163]

5.4 Mittaristojen analyysi

Edellä esitetyt kansallista kyberkyvykkyyttä mittaavat mittaristot eroavat toisistaan niin mitattavien kohteiden kuin mittausasteikkojenkin osalta. Mittareita voidaan kuitenkin vertailla kohtuullisesti keskenään niistä käytössä olevien kuvausten perusteella. Kaikista niistä löytyy keskeisiä indikaattoreita kansallisen kyberturvallisuuden tilan arvioimiseksi. Mittareiden vertailu on suoritettava osin suhteellisena vertailuna, mutta asetettuihin tavoitteisiin nähden sen voi arvioida olevan riittävällä tarkkuudella tarkoituksenmukaisen. Laadukkaan mittarin näkökulmista (kts. luku 5.2.2) voidaan muodostaa oheinen vertailutaulukko 2, johon kansallisen kyberturvallisuuden mittaamiseen tarkoitetut edellä kuvatut mittarit on asetettu.

[163] Hathaway Melissa, Demchak Chris, Kerben Jason, McArdle Jennifer, Spidalieri Francesca, India Cyber Readiness at a Glance, 2016

Taulukko 2 Mittareiden vertailu

NÄKÖ-KULMA	GCI	EU Dash-board	NCSI	CMM	CRI
Päätöksenteko			X	X	
Ymmärrettävä			X	X	
Kehitystä tukeva			X	X	
Data-perusteinen	X	X	X	X	X
Toistettava	X	X	X	X	X
Resursoitu					
Diskreetti	X	X	X	X	X
Merkittävyys	X	X	X	X	X
Laajuusperiaate	X	X	X	X	X

Vertailutaulukkoa koskevat perustelut ovat:

A. Päätöksenteko (Tarina): Mittaristot NCSI ja CMM tukevat päätöksentekoa muita kattavammin mitattavien kohteiden osilta.

B. Kouriintuntuva (Ymmärrettävä): Mittaristot NCSI ja CMM sisältävät luokitteluasteikkoja muita laajemmin ja ovat siten tarkastelukohteen osalta kouriintuntuvampia.

C. Kehitystä tukeva: Mittaristot NCSI ja CMM mahdollistavat mm. luokitteluasteikkojensa perusteella tavoitteiden kehityksen seuraamisen.

D. Data-perusteinen: Jokaisen mittarin osalta on käytettävissä dataa, joka voidaan todentaa.

E. Toistettava: Tarkasteltavana olevien mittareiden mittaustapahtumat ovat toistettavissa. Kaikkien osalta tietoja kerääminen ja päivittämien on suoritettava manuaalisesti ryhmätyönä. Automaatiota ei voida luontevasti käyttää.

F. Resurssiin sopeutettu: Koko mittariston on oltava organisaation resurssien mukaan ylläpidettävissä. Resurssien tarvearviointia ei ole suoritettu.

G. Diskreetti: Mittaristot ovat rakenteiltaan erilaisia tarkastelunäkökulmiltaan, silti jokainen niistä mittaa laajasti kansallisen kyberturvallisuuden kehittymistä. Kaikki mittaristot ovat kutenkin olleet käytössä. Mittareiden voi arvioida siten kohdentuvan oikein

mitattaviin suureisiin. Mittaristot ovat läpinäkyviä, mikä palvelee niistä saatavien tietojen käytettävyyttä.

H. Merkittäviin seikkoihin kohdentuva: Mittaristojen erilaisista tarkastelunäkökulmista huolimatta niiden voi arvioida kohdentuvan riittävällä tarkkuudella asioihin, joita halutaan seurata, eivätkä ne ohjaa pelkästään helposti saatavien toissijaisten tietojen mittaamiseen.

I. Periaate vähemmän on yleensä enemmän: Mittaristot on kehitetty kansallisen kyberturvallisuuden kyvykkyyden tilannekuvan mittaamiseen ja niitä on siihen myös jo käytetty, joten niiden laajuudet ovat tarkoin harkittuja. Mittarit sisältävät erilaisista näkökulmistaan huolimatta tarkoituksenmukaisen lähestymistavan mittauskohteeseen.

6. KYBERTURVALLISUUDEN STRATEGISEN JOHTAMISEN JA TILANNETIETOISUUDEN SEKÄ KYVYKKYYDEN MITTAAMISEN MALLIT

6.1 Kyberturvallisuuden strateginen johtaminen

Tässä tutkimuksessa tavoitteena oli määritellä, mitä kyberturvallisuuden strateginen johtajuus on ja miten sitä toteutetaan kokonaisturvallisuuden vastuumallissa, miten yleinen häiriötilanteiden hallintamalli toteutetaan laajoissa kyberturvallisuuden häiriötilanteissa, miten kyberturvallisuuden strateginen johtaminen on organisoitava ja millainen on valtionhallinnon kyberturvallisuuden johtamisen rakenne. Tutkimuksessa määriteltiin kyberturvallisuuden strategista johtamista ja luotiin strategisen johtamisen malleja ottaen huomioon kyberturvallisuusvarautumisen ja laajamittaisten kyberhäiriötilanteiden johtamisen.

Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista.

Kyberturvallisuus on keskeinen osa suomalaisen yhteiskunnan turvallisuutta sekä kilpailukykyä. Teknologisen kehityksen ja digitalisoitumisen syvenemisen myötä kyberturvallisuuden merkitys kasvaa. Samalla korostuu johtaminen, niin operatiivinen kuin strateginen kyberturvallisuuden johtaminen. **Strategisen ja operatiivisen johtamisen rajat eivät kaikissa tilanteissa ole kyberturvallisuuden johtamisessa aina selkeät** vaan ajoittain vaikeasti erotettavissa toisistaan. On kuitenkin huomioitava *kyberturvallisuuden strategisen johtamisen erityispiirteet*, jotka on tarkemmin esitetty luvussa 2.6.2.

Kybertoimintaympäristöön yhdistyvässä strategisessa johtamisessa on yhteisiä piirteitä yleisen strategisen johtamisen ja sen toimintatapojen kanssa. Kybertoimintaympäristö kuitenkin asettaa strategiselle johtamiselle erityispiirteitä, erityisesti häiriötilanteiden nopeuden (aikatekijä) osalta. Toisaalta kyberturvallisuuden strateginen johtaminen yhteiskunnassa käsittää jo tänä päivänä hyvin laajan tehtäväkentän aina kyberomavaraisuuden kehittämisen ymmärtämisestä poliittisen päätöksenteon tukemiseen. *Kyberturvallisuuden kehittämisen tehtäväkenttä on suomalaisessa yhteiskunnassa laaja ja kyberturvallisuudessa on kyse yhteiskunnallisesti hyvin merkittävästä asiasta*. Tämä korostaa kyberturvallisuuden strategisen johtamisen tarvetta suomalaisessa yhteiskunnassa. **Strategisen johtajuuden tulee ilmentyä niin normaalioloissa kuin häiriö- ja poikkeustilanteissa.** Erityisenä haasteena strategisessa johtamisessa on tässä tutkimuksessa noussut esille kokonaisvaltaisen strategisen johtajuuden puute.

Kyberturvallisuutta voi pitää malliesimerkkinä kokonaisturvallisuuden tarpeellisuudesta, sillä kyberturvallisuudessa menestyäkseen on **yhteiskunnan eri toimijat kyettävä osallistamaan sekä voimavarat ja toimintatavat yhteensovittamaan mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi.** Kyse on koko yhteiskunnan kyberkyvykkyyden kehittämisestä. Tämä edellyttää strategista yhteensovittamista ja johtamista sekä **vahvaa osaamista, strategista analyysikyvykkyyttä ja toimeenpanokykyä.**

Tutkimuksessa kyberturvallisuuden strategisen johtamisen vaatimuksina ovat lisäksi korostuneet **toimiva lainsäädäntö, johtajuuteen yhdistyvät riittävät toimivaltuudet ja**

johtamisen mahdollistavat taloudelliset resurssit. Tilannetietoisuus ja **uhkatilanteiden ennakointi** nousivat esille tutkimuksessa keskeisinä asioina. Kybertoimintaympäristön jatkuva ja nopea muutos edellyttää puolestaan johtamiselta strategista **ketteryyttä.**

Tämän tutkimuksen kansainvälisessä referenssiarvioinnissa kyberturvallisuuden strategisen johtamiseen yhdistyy läheisesti **kyberturvallisuuden tuottaminen kokonaisvaltaisesti, organisaatiorakenteiden virtaviivaistaminen sekä vaatimus strategisen johtajuuden läheisestä yhteydestä poliittiseen päätöksentekoon.**

Kyberturvallisuuden strategisessa johtamisessa oleellista on digitaalisesta toimintaympäristöstä ja sen arvioidusta kehityksestä johdettujen **tavoitteiden tunnistaminen ja asettaminen**. Tutkimuksessa on korostunut vision selkeys ja sen viestintä vision toimeenpanon perustana kyberturvallisuuden strategisessa johtamisessa. Selkeä tavoitetila on edellytys myös pitkän tähtäimen toimeenpanolle sekä **toimeenpanon jatkuvalle seuraamiselle** määriteltyjen mittareiden avulla. Kyberturvallisuuden strategiseen johtamiseen kuuluu myös tietoinen **kansallisen kyberturvallisuusidentiteetin rakentaminen** ja vahvistaminen niin yhteiskunnan sisällä kuin kansainvälisesti.

Yksityisellä sektorilla on merkittävä osa kyberosaamisesta ja infrastruktuurista. Valtionhallinnon, yksityisen sektorin ja kolmannen sektorin yhdessä tekemisen perustana on vahva luottamus. Kyberturvallisuuden strategisen tavoitteisiin kuuluu **luottamukseen perustuvan yhteistyön ilmapiirin ylläpitäminen ja vahvistaminen.** Eri toimijoiden välille on jo nykyisin muodostunut tarpeeseen ja yhdessä tekemiseen perustuvia rakenteita. Prosessit ja johtamisrakenteet ovat kuitenkin ajoittain epäselviä niin strategisella kuin operatiivisella tasolla.

Strategisen johtamisen yhtenä päämääränä on kehittää valtionhallinnon, yksityisen sektorin ja kolmannen sektorin välistä yhteistoimintaa ja kehittää sitä asetettujen tavoitteiden mukaisesti. Strategisen johtajuuden sekä muodostettujen **johtamisrakenteiden tulisi olla mahdollisimman selkeitä ja kaikkien toimijatahojen tunnistettavissa kaikissa tilanteissa** – niin normaaliajan varautumisessa kuin laajasti yhteiskuntaan vaikuttavien häiriötilanteiden aikana.

Alla olevassa taulukossa 3 on esitetty kyberturvallisuuden strategiseen johtamiseen yhdistyvien keskeisten osatekijöiden nykytilaa ja tavoitetilaa sekä tarvittavia muutoksia tavoitetilan saavuttamiseksi. Oleellista on huomioida, että esitetyt osatekijät ovat vuorovaikutuksessa toisiinsa ja niitä on yhteensovitettava.

Taulukko 3 Kyberturvallisuuden strategisen johtamisen keskeisiä osatekijöitä

OSATEKIJÄ	NYKYTILA	TARVITTAVA MUUTOS	TAVOITETILA
Pitkän aikavälin tavoitteet	Kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmassa määritellään pitkän aikavälin tavoitteet. Tavoitteet on saavutettu osittain.	Tavoitteiden kirkastaminen ja toimeenpano. Kyberturvallisuustyöhön osallistuvien toiminnan koordinoinnin tehostaminen sekä tavoitteiden saavuttamiseen yhdistyvä poliittinen sitoutuminen ja resurssointi.	Pitkän aikavälin tavoite on asetettu, viety toteutettavaksi poliittisesti sitoutettuna riittävin resurssein ja kyberturvallisuudessa on saavutettu asetetut tavoitteet.
Johtajuus	Kyberturvallisuuden strategista johtajuutta ei ole. Operatiivisen johtamisen prosessit eivät ole kaikilta osin selkeät.	Johtajuus on a) määriteltävä strategisella tasolla ja b) selkeytettävä käytännön toimenpitein.	Johtajuus on määritelty ja yksiselitteisesti osoitettavissa niin normaalioloissa kuin häiriö- ja poikkeustilanteissa.

Tilannetietoisuus/-ymmärrys	Kyberturvallisuuden tilannekuva on osin pirstaleinen. Historiatiedon puutteen ja tiedon heikon vertailtavuuden vuoksi päätökset perustuvat hajanaiseen tietoon. Strateginen kyberanalyysi on heikkoa.	Tilanneymmärryksen yhtenäistäminen ja kokoaminen. Yhteisen tietovarannon luominen. Strategisen analyysikyvykkyyden kehittäminen.	Kybertoimintaympäristössä tehdyt havainnot sekä niin operatiivinen kuin strateginen tilanneymmärrys tukee kokonaisturvallisuuden strategisen tason päätöksentekoa.
Toimenpiteiden vaikutus ja seuraaminen	Toimintaympäristö muuttuu nopeasti ja osin hallitsemattomasti. Edellyttää niin strategisen kuin operatiivisen johtamisen ketteryyttä. Nykyiset prosessit ovat ajoittain hitaita ja kankeita.	Edellyttää niin strategisen kuin operatiivisen analyysin sekä tilanneymmärryksen kehittämistä. Tehtävien toimenpiteiden vaikuttavuutta on kyettävä seuraamaan kokonaisvaltaisesti ja mittamaan.	Toimenpiteitä kyetään jatkuvasti kehittämään strategisen johtamisen ohjatessa toimenpiteitä. Toimenpiteitä seurataan määritellyillä mittareilla.
Kyberomavaraisuus	Kyberturvallisuuden kehittämisen kokonaisvaltainen koordinaatio puuttuu.	Suomen kyberomavaraisuuden vahvistaminen asetettujen tavoitteiden mukaisesti.	Suomella on tavoitteiden mukainen kyberomavaraisuus.

6.2 Kyberturvallisuuden strategisen johtamisen mallit

Tutkimukseen tuotettiin vaihtoehtoisia malleja kyberturvallisuuden strategisen johtamisen toteuttamiseksi Suomessa. Esitettävät viisi mallia perustuvat johtotason henkilöiden ja alan asiantuntijoiden tutkimushaastatteluissa, kansainvälisessä referenssimaiden arvioinneissa sekä tutkimuskirjallisuudessa/-dokumenteissa esiintyneisiin ja esitettyihin näkemyksiin sekä tutkimuksen tekijöiden arvioihin.[164]

Yhteiskunnan turvallisuusstrategian mukaan ”kokonaisturvallisuus on suomalaisen varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä.”[165]

Kyberturvallisuuden strategisen johtamisen mallien muodostamista on ohjannut Suomen kyberturvallisuusstrategiassa määritetty ja vuoden 2017 toimeenpano-ohjelmassa tarkennettu visio, jonka mukaan:

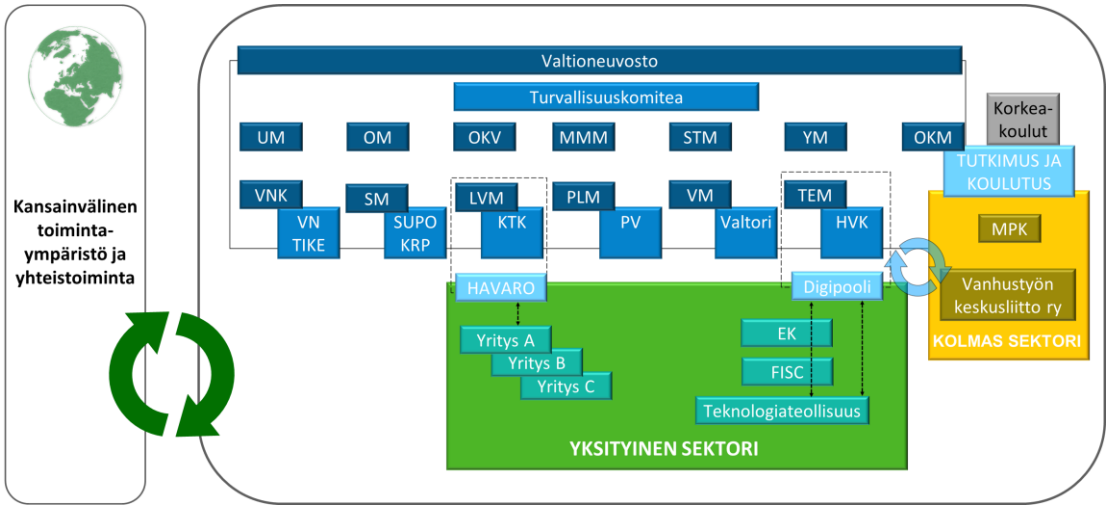
1. Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.
2. Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.
3. Suomi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

Myös tutkimushaastatteluissa tuotiin esille useita vaihtoehtoisia malleja kyberturvallisuuden strategisen johtamisen toteuttamiseksi. Esitetyt näkemykset ilmenevät esitettävistä vaihtoehtoisista malleista. Esitetyt mallit eivät ole prioriteettijärjestyksessä, eikä niiden yhteydessä tuoda esille sitä, miten ”suosittu” juuri kyseinen malli oli haastateltavien keskuudessa. Malleilla ei siten ole ”painokertoimia”, eikä tässä tutkimuksessa erityisesti suositella mitään mallia vaan kunkin mallin osalta tuodaan esille kyseisen mallin vahvuuksia ja heikkouksia kyberturvallisuuden strategisen johtamisen vaatimusten perusteella.

[164] Suomen kyberturvallisuusstrategia, s.3,
Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, s. 7.

[165] Yhteiskunnan turvallisuusstrategia, 2.11.2017, s.7

Oheisella kuvalla 8 havainnollistetaan johtamismallien arvioinnin perustana sitä toimintaympäristöä, johon kyberturvallisuuden strategisen johtamisen malli eri vaihtoehdoissa voi sijoittua. Julkisen sektorin, yksityisen sektorin ja kolmannen sektorin toimijoiksi on sijoitettu Suomen kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmissa tunnistettuja organisaatioita, toimintoja ja yhdistyksiä.



Kuva 8. Nykytila kyberturvallisuuden tuottamiseen osallistuvista toimijoista.

Kyberturvallisuuden strategisen johtamisen malleja esitetään viisi:

1. Nykymalli
2. Kansallinen kyberturvallisuusjohtaja
3. Kansallinen kyberturvallisuusyksikkö
4. Vahvennettu Kyberturvallisuuskeskus
5. Kyberturvallisuusvirasto

6.2.1 Nykymalli

Nykytilamallissa kyberturvallisuutta johdetaan osana yhteiskunnan elintärkeiden toimintojen turvaamista, eikä sille luoda erillistä strategista johtajuutta tai johtamisprosessia.

Normaalioloissa ennakointi ja varautuminen hoidetaan hallinnonaloittain ja yksityisen/kolmannen sektorin kanssa tehdyin sopimusjärjestelyin ja yhteistyöperiaattein kyberturvallisuusstrategian toimeenpano-ohjelman mukaisesti. Hallinnonalojen budjettien ulkopuolisia resursseja kyberturvallisuustyöhön ei ohjata. Turvallisuuskomitea koordinoi kokonaisturvallisuuden tuottamista, avustaa Valtioneuvostoa ja ministeriöitä sekä toimii tarvittaessa konsultoivana asiantuntijaelimenä. Se vastaa yhteiskunnan turvallisuusstrategiasta (mukaan lukien strategian toimeenpanon seuraaminen) sovittaen yhteen valtionhallinnon (mukaan lukien aluehallinto), kuntien, elinkeinoelämän ja järjestöjen kybervarautumista eri turvallisuustilanteisiin.

Häiriötilanteissa toimivaltainen viranomainen johtaa toimintaa ja vastaa viestinnästä. Laajamittaisten kyberturvallisuuden häiriötilanteiden hallinnassa toimivaltainen ministeriö tai Valtioneuvoston kanslia kutsuu tarvittaessa koolle ylimääräisen valmiuspäällikkökokouksen. Samoin Valtioneuvoston tilannekeskuksen toimintaa tarvittaessa vahvennetaan, jotta voidaan muodostaa kokonaisvaltainen ja ajanmukainen tilannetietoisuus päätöksenteon tueksi. Toiminnan valmistelua ja koordinointia varten voidaan kutsua myös koolle erikseen nimitettävä kokoonpano, jota johtaa vastuunalainen valmiuspäällikkö. Kokoonpanon tehtävänä on

valmistella häiriötilanteen koordinointiin liittyviä asioita kansliapäällikkökokouksia varten. Viranomaiset ja muut kyberturvallisuuden toimijat säilyttävät normaaliolojen tehtävänsä ja vastuunsa, joskin jokaisen toimintaa ja yhteistyötä tehostetaan. Tiedusteluvaltuudet eri tilanteissa määräytyvät alkuvuodesta 2018 eduskuntakäsittelyyn tuodussa tiedustelulainsäädännössä.

Mallin vahvuuksia ovat muun muassa sen tuttuus (kyberturvallisuuden johtaminen on sulautettu jo olemassa oleviin häiriötilanteiden hallintajärjestelyihin) ja vähäinen hallinnon uudelleen järjestämisen tarve. Suomessa (kyber)turvallisuuden toimijat tuntevat toisensa verrattain hyvin, mikä edesauttaa tiedonvaihtoa ja yhteistyön sujumista, vaikkei yksiselitteisiä kyberturvallisuuden johtamissuhteita olisikaan määritelty. Mallin pohjalla on nykyinen lainsäädäntö

Mallin heikkoutena on epävarma kyky reagoida riittävän nopeasti laajamittaiseen kyberhyökkäykseen tai häiriötilanteeseen sekä tuottaa alati muuttuviin kyberuhkiin varautumisen kannalta välttämätöntä ennakoivaa strategista analyysitietoa. Nykyistä johtamisrakennetta ei voi pitää varautumisen yhteensovittamisen, strategisten tavoitteiden tunnistamisen tai kansallisen kyberturvallisuusidentiteetin vahvistamisen kannalta optimaalisena. Nykymalli ei ohjaa riittävästi hallinnonalojen, elinkeinoelämän ja kolmannen sektorin kyberturvallisuusvarautumista eikä muodosta riittävän keskitettyä strategista analysointikykyä tilannetietoisuuden tuottamisen tueksi. Kyberturvallisuuden kansallisen omavaraisuuden tunnistaminen ja kehittäminen jäävät nykymallissa puutteelliseksi. Kansainvälisissä vertailuissa korostunut kyberturvallisuuden strategisen johtamisen läheisen yhteyden tarpeellisuus poliittiseen päätöksentekoon ei näyttäydy selkeänä.

6.2.2 Kansallinen kyberturvallisuusjohtaja

Tässä mallissa perustetaan **kyberturvallisuuden ylimmän johtajan tehtävä, joka sijoitetaan Valtioneuvoston kansliaan tai vaihtoehtoisesti johonkin kyberturvallisuuden kannalta keskeiseen ministeriöön tai organisaatioon**.

Olemassa olevien yhteiskunnan kokonaisturvallisuuden johtamissuhteiden kannalta kyberturvallisuusjohtajan sijoittaminen Valtioneuvoston kansliaan olisi selkeä ja poliittisesti neutraali vaihtoehto, mistä on esimerkkejä kansainvälisistä referenssimaista. Kanslian nykyiset tehtävät tukevat kyberturvallisuustyössä tarvittavia toiminnallisuuksia, esimerkiksi tilannekuvan tuottamiseen sekä valtioneuvoston ja pääministerin tukemiseen liittyvät tehtävät. Kyberturvallisuusjohtajan toimenkuva yhteen sovitetaan kokonaisturvallisuuden strategiseen johtamiseen sen sijaan, että luotaisiin erillinen kyberturvallisuusjohtamisen toimintalinja. Johtaja ohjaa kyberomavaraisuuden kehittämistä poikkihallinnollisesti. Kohdeorganisaation budjettiin lisätään henkilön palkkaus- ja toimintakustannukset.

Kansallisen kyberturvallisuusjohtajan nimittäminen muuttaa valtionhallinnon johtamisrakenteita eri tasoilla lainsäädännöstä aina toiminnallisuuksiin asti. Johtajan toimenkuva voi olla joko 1) sektoreittain tehtävän kyberturvallisuustyön yhteensovittamista ja koordinoimista Turvallisuuskomitean kokonaisturvallisuuden yhteensovittamistyöhön tai 2) rajoitetulla toimeenpanovallalla varustettua kyberturvallisuuden ylintä kansallista päätöksentekoa, joka on sovitettu kokonaisturvallisuuden kehikkoon.

Häiriötilanteisiin varautuminen tapahtuu hallinnonaloittain, mutta kyberturvallisuusjohtajalla on yleisymmärrys siitä, mitä toimenpiteitä hallinnonaloilla tehdään. Tarpeen mukaan hän lisäohjeistaa, yhteensovittaa ja osallistaa uusia toimijoita varautumiseen. Kyberturvallisuusjohtaja saa käyttöönsä tarvittavat tiedot kybertoimintaympäristön tapahtumista. Kyberturvallisuusjohtajan toimenkuva voi olla myös liikkuva, jolloin tehtävänä normaalioloissa on tukea hallinnonalojen kyberturvallisuustyötä, varautumista ja kyberomavaraisuuden ylläpitämistä.

Asiantuntijaroolissa kyberturvallisuusjohtaja arvioi kyberturvallisuuden strategista kokonaiskuvaa osana sektorikohtaista kokonaisturvallisuuden varautumista.

Laajamittaisissa kyberhäiriötilanteissa johtaja koordinoi tilannetietoisuutta ja toimivaltuuksiensa rajoissa päättää yksittäisistä strategisista toimenpiteistä. Tarvittaessa hän asiantuntijuudellaan tukee toimien toteuttamista ja ennakoi niiden vaikutuksia. Liikkuvalla tehtävänkuvalla varustettu kyberturvallisuusjohtaja siirtyy häiriötilanteissa tukemaan toimivaltaisen viranomaisen toimintaa, toisin sanoen häiriötilanteissa substanssijohtaminen hoidetaan hallinnonaloittain, mutta kyberturvallisuusjohtaja asiantuntijuudellaan ja toimivallallaan tukee tehtäviä toimenpiteitä. Riippumatta siitä, millaiseksi kyberturvallisuusjohtajan toimenkuva määritellään, tulee toimivaltuuksien jaon johtajan ja hallinnonalojen operatiivisten johtajien välillä olla selkeä ja yksiselitteinen.

Mallin keskeinen vahvuus on johtosuhteiden selkeys kyberturvallisuudessa: nimitetty kyberturvallisuusjohtaja koordinoi, johtaa tai tukee kyberturvallisuustyötä kaikissa tilanteissa. Johtajan toimenkuva perustuu tämän tutkimuksen luvuissa 2.6.2 ja 6.1 esitettyihin strategisen johtamisen vaatimuksiin ja tavoitteisiin. Johtaminen on myös lähellä poliittista päätöksentekoa ja poliittista ohjausta. Tässä mallissa yksittäinen henkilö saa kuitenkin johdettavakseen asiakokonaisuuden, johon ei ole suunnattu erillisiä resursseja.

Tilanteessa hallinnonalat rajat ylittävä johtaminen on haasteellista, koska resurssit ja johtamisjärjestelmät on kohdennettu hallinnonalojen sisällä. Mallin heikkoutena voi myös pitää yhtäältä suhteettoman laajan vallan ja vastuun keskittymistä yhdelle henkilölle. Tehtäväkentän ollessa strategisessa johtamisessa laaja, voidaan kyseenalaistaa yksittäisen henkilön mahdollisuudet toteuttaa kaikki määritetyt tehtävät. Mikäli kyberturvallisuusjohtajan rooli on löyhästi koordinoiva, jää niin varautumisen kuin häiriötilanteiden johtaminen kevyeksi. Nopeasti eskaloituvassa häiriötilanteessa tulee strategisen johdon ja operatiivisten toimijoiden välillä olla nopea ja toimiva yhteys sekä selkeät toimivaltuudet kullekin osapuolelle.

6.2.3 Kansallinen kyberturvallisuusyksikkö

Kansallisen kyberturvallisuusyksikön malli mukailee kansallisen kyberturvallisuusjohtajan mallia. **Kyberturvallisuusjohtajan alaisuuteen perustetaan erillinen kyberturvallisuusyksikkö, jolla on kykyä johtaa, kehittää ja tukea kansallista kybervarautumista ja laajemminkin edistää kyberturvallisuuden kansallisen vision toteutumista.**

Yksikkö sijoitetaan Valtioneuvoston kansliaan tai vaihtoehtoisesti johonkin kyberturvallisuuden kannalta keskeiseen ministeriöön tai organisaatioon. Sijoituspaikka osoittaa myös kansallisen kyberturvallisuusjohtajan tehtävän sijainnin. Sijoittamista Valtioneuvoston kansliaan puoltaa se, että mallissa kyberturvallisuusyksikkö vastaa strategisen tason analyysista ja toimii strategisen johdon esikuntana laajavaikutteisten häiriötilanteiden hallinnassa. Kansainvälisissä vertailuissa nousee esille tämän päivänä kybertoimintaympäristön haasteisiin vastaamisessa strateginen analyysikyvykkyys, joka on Suomessa vielä suhteellisen pientä. Kyberturvallisuusyksikkömallin osaratkaisuna voidaan nähdä kyberturvallisuusjohtajan sijoittaminen Valtioneuvoston kansliaan ja olemassa olevan tilannekeskuksen resurssien vahvistaminen kyberturvallisuuden osalta. Kyberturvallisuusyksikön tarvitsemat toimintaresurssit lisätään sen sijoitusorganisaation budjettiin.

Kyberturvallisuusyksikköön rekrytoidaan riittävä määrä asiantuntijoita, joiden tehtävänä on kerätä ja analysoida päätöksenteon perustaksi tarvittavaa tietoa sekä ennakoida kybertoimien vaikutuksia kokonaisturvallisuusympäristössä. Analyysituotteet suunnataan ensisijaisesti kansallisen päätöksenteon tueksi. Strategisen tason tuotteet toimivat operatiivisella

tasolla tehtyjen havaintojen palautteena ja oppimisvälineinä. Mallissa korostuu tilannetietoisuus ja päätöksenteko strategisen ja operatiivisen rajapinnassa – varsinkin häiriötilanteissa. Siten mallin voi arvioida olevan malleista ”ketterin” ja kykenevin mukauttamaan strategisia toimenpiteitä toimintaympäristön muuttuessa.

Normaalioloissa kyberturvallisuusjohtaja vastaa hallinnonalojen ja yksityisen/kolmannen sektorin välisen kyberturvallisuustyön yhteensovittamisesta sekä kyberomavaraisuuden kehittämisestä ja ylläpitämisestä poikkihallinnollisesti. Asiantuntijat tuottavat yksikön johdon alaisuudessa strategisen tason analyysia kybertoimintaympäristön muutoksista, skenaarioita eri strategisten liikkeiden vaikutuksista kokonaisturvallisuusympäristöön ja päätösehdotuksia. Hallinnonalojen omat strategisen analyysin toimijat tukevat perustettavan yksikön toimintaa. Yksikkö vastaanottaa myös laajennetusti tilannetietoa, jolla on merkitystä koko yhteiskunnan kyberturvallisuuden kannalta. Kyberturvallisuusyksikön analyysituotteiden pohjalta päätökset tekee joko kyberturvallisuusjohtaja, hallinnonaloittaisen varautumisen johtajat tai kokonaisturvallisuuden toimintamallin mukaisesti toimivaltainen taho (viranomainen/ministeriö).

Häiriötilanteissa kyberturvallisuusyksikön toimintaa tehostetaan. Se saa analyysinsä tueksi kohdennettua tilannetietoa (myös ulkomailta) sekä tietoa kehittämistä vaativista suorituskyvyistä kyeten siten reagoimaan ja toimivaltuuksiensa puitteissa edistämään valmiutta. Päätöksenteko-oikeudet normaaliolojen tai poikkeusolojen häiriötilanteissa on rakennettava siten, että johtosuhteet ovat selkeitä ja toimivia nopeaa päätöksentekoa vaativissa tilanteissa, joissa selkeää etukäteisjärjestelyä ei ole luotu. Kyberturvallisuusjohtaja toimii ensisijaisena tiedottajana laajamittaisissa kyberhäiriötilanteissa.

Kyberturvallisuusyksikön vahvuutena on sijoittuminen lähelle poliittista päätöksentekoa sekä kyky johtaa ja kehittää kyberturvallisuustoimintaa poikkihallinnollisesti. Mallia voi johtamisen näkökulmasta pitää varsin ketteränä ja keskitettynä johtamisen mallina, jossa johtajalla on oma yksikkönsä johtamisen tueksi laajassa tehtäväkentässä. Kansainvälisessä vertailussa vastaava yksikkö on sijoitettu joko pääministerin toimistoon, yleisesti turvallisuudesta ja oikeudesta vastaavaan ministeriöön tai samankaltaisia tehtäviä hoitaa yleisesti kansallisen turvallisuustoiminnan yhteensovittamisesta vastaava organisaatio. Mallissa kyberturvallisuuden johtaminen on osittain sulautettu jo olemassa oleviin häiriötilanteiden hallintajärjestelyihin, joten siihen siirtymisestä seuraisi rajallinen hallinnon uudelleen järjestämisen tarve. Tämä vähentää rasitetta ja epäselvyyksiä, joita kokonaisturvallisuuden järjestelyjen muuttaminen aiheuttaisi.

6.2.4 Vahvennettu Kyberturvallisuuskeskus

Tässä mallissa **kyberturvallisuusjohtajan ohjaukseen sijoitetaan Kyberturvallisuuskeskus, jonka operatiivista osaamista ja toimintavaltuuksia täydennetään strategisella analysointikyvyllä**. Keskuksen tilannekuvatoimintoa vahvennetaan strategisella analyysikyvyllä, millä tavoitellaan tilannetietoisuuden tuottamista strategisen päätöksenteon tueksi. Keskus sijoitettaisiin kyberturvallisuusjohtajan sijoituspaikan mukaisesti ja se toimisi läheisessä yhteistyössä Valtioneuvoston tilannekeskuksen kanssa. VN-TIKE:n tehtävänä säilyy kokonaisturvallisuuden tilannekuvan tuottaminen koko hallitukselle ja kaikille hallinnonaloille.

Kyberturvallisuuskeskuksen vahvistamisella ja siirtämisellä kyberturvallisuusjohtajan ohjaukseen tavoitellaan poikkihallinnollista integraatiota kyberturvallisuuden johtamisessa. Malli tuo strategisen ja operatiivisen kyberturvallisuustoiminnan lähemmäs toisiaan, jolloin tiedonkulku sekä tehtyjen päätösten ja toiminnan yhdensuuntaisuus paranevat. Kyberturvallisuustyö hallinnonaloilla tapahtuu Kyberturvallisuuskeskuksen koordinoimana eikä muita

kyberturvallisuustoimintojen siirtoja hallinnonalojen välillä tehdä. Kyberturvallisuuskeskuksen vahvennettuun toimintaan ohjataan tarvittavat resurssit.

Normaalioloissa Kyberturvallisuuskeskus toimii pääsääntöisesti kuten nykyään tuottaen strategista tilannetietoisuutta VN-TIKE:n sovittamana kokonaisturvallisuuden tilannekuvaan, tulevaisuuden arvioita havaittujen kehityskulkujenpohjalta sekä ehdotuksia päätöksentekoon. Tällaiset tehtävät ovat korostuneet myös kansainvälisessä vertailussa. Käytettävissään sillä on oman tiedontuotantonsa ohella muiden tilannekuvia, joilla on merkitystä koko yhteiskunnan kyberturvallisuuden kannalta. Tässä mallissa varautumista johtaa kyberturvallisuusjohtaja apunaan Kyberturvallisuuskeskus. Se arvioi ja kehittää kyberomavaraisuuden tasoa ja antaa ehdotuksia toimintatavoista, joilla omavaraisuutta parannetaan.

Laaja-alaisissa kyberhäiriötilanteissa Kyberturvallisuuskeskus toimii kyberturvallisuusjohtajan ohjauksessa ja tukee operatiivisia toimijoita tehtäviensä mukaisesti. Strategisen ja operatiivisen kybertoiminnan läheisyyden ansiosta strategista tavoitetta pystytään sovittamaan nopeasti tilanteenmukaiseen operatiiviseen toimintaan. Kyberturvallisuuskeskuksen ja VN-TIKE:n tiivistetty yhteistyö taas auttaa ennakoimaan eri toimintavaihtoehtojen vaikutuksia kokonaisturvallisuuteen.

Mallin vahvuuksia ovat strategisen ja operatiivisen toiminnan läheisyys, johtosuhteiden selkeys ja suoraviivaisuus, jolloin saavutetaan ketteryys suorituskykyjen käytössä, mikä palvelee niin strategisen vakauden ylläpitämistä kuin yllätyksellisen toiminnan mahdollistamista. Malliin siirtyminen vaatii rajallisia muutoksia olemassa oleviin kokonaisturvallisuuden järjestelyihin, mm. poikkihallinnollisia yhteistyön järjestelyjä tulee tarkentaa Kyberturvallisuuskeskuksen uuden roolin myötä. Myös Kyberturvallisuuskeskuksen resursointia täytyy merkittävästi lisätä.

Heikkoutena on kyberturvallisuustoimintojen hajautuneisuus ja eri toimintojen jääminen hallinnonaloille. Vienee myös aikaa ennen kuin Kyberturvallisuuskeskuksen viiteryhmät (nykyiset ja tulevat) omaksuvat sen uuden roolin.

6.2.5 Kyberturvallisuusvirasto

Tässä mallissa **muodostetaan Kyberturvallisuusvirasto, jonne sijoitetaan kyberturvallisuuden strateginen johto ja kyberturvallisuustoiminnot.**

Tähän virastoon kootaan kaikki keskeiset valtionhallinnon kyberturvallisuustoiminnot ja näin luodaan erillinen kyberturvallisuusjohtamisen toimintalinja. Eri hallinnonaloille jäävät välttämättömät kontaktipinnat kokonaisturvallisuuden koordinoimiseksi ja mm. kansainvälisten vastuiden hoitamiseksi. Poikkihallinnollisena viranomaistoimijana Kyberturvallisuusvirastoa ei sijoiteta minkään ministeriön vaan suoraan Valtioneuvoston kanslian ohjaukseen. Kansainvälisessä vertailussa vastaava virasto tai toimisto on useimmiten sijoitettu Pääministerin kansliaan.

Kyberturvallisuusvirastolle osoitetaan oma budjetti ja hallinnonaloilta turvallisuustoimintojen mukana siirtyvät niihin osoitetut resurssit, minkä ohella virastolle allokoidaan riittävät resurssit toimia keskitettynä yhteiskunnan kyberturvallisuuden ylläpitäjänä. Sen toimiala on varsin laaja sisältäen mm. turvallisuusstandardoinnin ja -auditoinnin, valtion- (ml. maakuntien) ja kunnallishallinnon tietojärjestelmien ja -verkkojen ylläpitämisen ja turvallisuuden, yksityisen sektorin kyberturvallisuuden varautumisjärjestelyjen ohjaamisen, Kyberturvallisuuskeskuksen ja kansainvälisen yhteistyön tukemisen eri hallinnonaloilla.

Kyberturvallisuusvirastosta ei luoda julkisorganisaatiota, joka vastaisi koko kansallisen kybertoimintaympäristön turvaamisesta vaan julkinen-yksityinen kumppanuudet ovat tärkeä osa kyberturvallisuustyötä. Varautuminen tapahtuu hallinnonaloittain, mutta Kyberturvallisuusvirasto ohjeistaa, koordinoi, tukee ja seuraa sitä sekä vastaa kansallisten ja alueellisten harjoitusten pitämisestä (niin kybertoimintaympäristöön keskittyvät harjoitukset kuin kyberelementin sisällyttäminen kokonaisturvallisuuden häiriötilanneharjoituksiin). Normaalioloissa Kyberturvallisuusvirasto kokoaa yhteen ja ylläpitää kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja ennakoi digitaalisen ympäristön tulevia kehityskulkuja. Sen vastuulle tulisi myös julkisten tietojärjestelmien ja -verkkojen kehittäminen sekä toiminnan ja ylläpidon johtaminen. Kyberomavaraisuutta kehitetään poikkisektorisessa yhteistyössä Kyberturvallisuusviraston johtamana. Viraston osaksi liitettävä Kybertuvallisuuskeskus säilyttää pääosin nykyiset tehtävänsä.

Häiriötilanteissa virasto pystyy ylläpitämänsä ajanmukaisen tilannetietoisuuden avulla ohjeistamaan tehokkaasti toimijoita valtionhallinnon eri tasoilla, yksityisellä ja kolmannella sektorilla sekä tarvittaessa myös maakunnissa. Se kykenee nopeasti reagoimaan tapahtumiin ja luomaan strategista etua yllätystä hyödyntämällä. Viraston kyberturvallisuusjohtajalla on mahdollisuus tehokkaasti johtaa ja koordinoida toimenpiteitä vakavien ja laajamittaisten kyberhyökkäysten torjunnassa. Virasto pitää valtion ylimmän johdon tilanteen tasalla, jotta kokonaisturvallisuuden strategiset tavoitteet tulevat huomioon otetuksi riittävän nopeasti. Tehokkaan toiminnan varmistamiseksi virastossa tarvitaan kansallisen puolustuksen ja sisäisen turvallisuuden asiantuntijuutta. Laajamittaisissa kyberhäiriötilanteissa virasto hoitaa myös tilanteesta tiedottamisen yhdessä VNK:n kanssa.

Malli tehostaa parhaiten julkishallinnon kyberturvallisuuden varautumista ja häiriötilanteiden hallintaa keskittämällä strategisen johtajuuden ja toiminnallisuudet yhteen paikkaan. Poikkihallinnollisuutensa ansiosta se poistaa esille tulleiden siiloratkaisuiden haasteita, joskin virastoa luotaessa on tarkkaan selvitettävä sen ja eri hallinnonalojen väliset suhteet. Kyberturvallisuusvirastomallissa voidaan luoda tehokas kyberturvallisuuden strateginen analyysikyvykkyys ja varmistaa tuotetun tiedon nopea siirtyminen päätöksentekoon ja johtamiseen.

Virastomallissa voidaan yhdistää valtionhallinnon keskeiset kyberresurssit tehokkaaksi kokonaisuudeksi, jonka avulla voidaan tehostaa sekä poikkihallinnollista yhteistyötä että yhteistyötä elinkeinoelämän kanssa. Tämä malli parantaa kykyä vastata asiakastarpeiden ja toimintaympäristön muutoksiin, kehittää ja vahvistaa kyberturvallisuuden strategista ohjausta sekä sillä saavutetaan synergiaetuja. Sen avulla voidaan myös parantaa hallinnon tuottavuutta ja erityisesti **vaikuttavuutta** resurssien monipuolisemmalla ja tehokkaammalla käytöllä.

Mallin heikkoutena on kyberturvallisuustoimintojen osittainen siirtyminen pois hallinnonaloilta, jolloin saatetaan menettää tietoa ja osaamista eri hallinnonalojen erityispiirteistä. Viraston luominen vaatii laaja-alaisia uudistuksia olemassa oleviin hallintorakenteisiin, johtamis- ja vastuusuhteiden uudelleen muotoilemista ja riittävää resursointia. Siirtymäajanjaksolla hallinnollinen kitka vie osan toiminnan tehokkuudesta kunnes uusi toimintamalli vakiinnuttaa paikkansa.

6.2.6 Mallien tarkastelussa huomioitavaa

Tässä selvityshankkeessa esitetyt johtamismallit on kuvattu periaatteellisella tasolla. Jonkin tässä esitetyn tai jonkin muun johtamismallin valmistelun jatkaminen edellyttää virkamiesvalmistelua. Tällöin on selvitettävä tarvittavat toiminnalliset ja organisatoriset muutokset sekä tarvittavat säädösmuutokset, tehtävä taloudelliset tarkastelut sekä laadittava vaikutuksista laaja-alainen arviointi lausuntoineen ja aikataulu uudistuksen toteuttamiseksi.

Esitetyt mallit sisältävät riskejä, joiden määrä ja vaikuttavuus ovat verrannollisia muutoksen laajuuteen. Riskit saattavat johtaa epätarkoituksenmukaisiin ratkaisuihin toiminnan järjestämisessä. Siksi jatkovalmistelussa tulee kiinnittää erityistä huomiota siihen, että toiminnan ja palvelutason laadukkuus, luotettavuus sekä häiriötön jatkuminen varmistetaan mahdollisen muutoksen aikana ja sen jälkeen.

Tämän tutkimushankkeen aikana on ollut käynnissä Liikenne- ja viestintäministeriön virastouudistus, johon liittyviä päätöksiä ei tutkimuksen päättyessä ole vielä tehty. Hallinnonalan virastot ovat uudistuksen esiselvitysvaiheessa pitäneet tärkeänä, että virastoratkaisun tarkoituksenmukaisuutta arvioitaisiin ainakin Viestintäviraston kyberturvallisuuskeskuksen osalta huolellisesti laajemmasta näkökulmasta ennen sen toimeenpanoa.

6.3 Tilannekuva, -tietoisuus ja -ymmärrys

Tutkimuksella selvitettiin kybertilannekuvan kehittäminen, kyberhäiriötilanneymmärryksen ja analysoinnin toimintamalli.

Jokainen organisaatio tarvitsee toimiakseen tietoa ympäristöstään ja sen tapahtumista sekä niiden vaikutuksesta omaan toimintaansa. Tarkoituksenmukainen ja nopea, oikeisiin tietoihin ja arvioihin perustuva tilannetietoisuus korostuu häiriötilanteissa, jolloin joudutaan nopeasti tekemään hyvinkin laaja-alaisesti vaikuttavia päätöksiä. Voidakseen tehdä oikeita ratkaisuja päätöksentekijöiden on tiedettävä toiminnan perusteet, seuraukset, miten muut päätöksiin reagoivat ja mitä riskejä päätöksiin sisältyy. Tästä syystä kaikilla päätöksentekijöillä tulee olla riittävä tilannetietoisuus ja -ymmärrys, joka on väline oikea-aikaiseen päätöksentekoon ja toimintaan. Tilannetietoisuus ja -ymmärrys edellyttävät yhteistoimintaa ja osaamista, jotka mahdollistavat kokonaisvaltaisen toimintaympäristön seurannan, informaation analysoinnin ja kokoamisen, tiedon jakamisen, tutkimustarpeiden tunnistamisen sekä verkostojen hallinnan.

Kybertoimintaympäristö on dynaaminen ympäristö, jolloin häiriötilanteisiin varautumisessa tarvitaan erityisesti strategista ketteryyttä. Nykyinen johtamisen malli yhteiskuntaan kohdistuvissa vaarallisissa ja laaja-alaisissa häiriötilanteissa ja niihin yhdistyvissä toimivaltuuksissa on haasteellinen kybertoimintaympäristön edellyttämän kriittisen reagointinopeuden osalta. Lisäksi yhteiskunnassa ei ole päätetty, kenellä on päätäntävalta ja mandaatti kertoa, mihin resurssit tällöin ensisijaisesti ohjataan tai kenen järjestelmät palautetaan toimintaan ensiksi tai mitä vastatoimia tarvitaan. Kenelläkään ei siis ole mandaattia määritellä sitä, mikä on kriittistä ja miten tilanteisiin reagoidaan.

Kansallinen kyberturvallisuuden tilannekuva ja -tietoisuus muodostaa kolmitasoisen kokonaisuuden. Alimmalla tasolla on eri toimijoiden teknis-taktinen tilannekuva ja siihen liittyvä analysointi. Keskeisiä viranomaistoimijoita ovat KRP, SUPO, Puolustusvoimat, Kyberturvallisuuskeskus ja Valtori. Yksityisellä sektorilla eri yritykset kokoavat omaa kybertilannekuvaansa tai ovat ulkoistaneet toiminnan alan toimijoille.

Kyberturvallisuuskeskus tuottaa yhdistetyn kyberturvallisuuden tilannekuvan. Kyberturvallisuuskeskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille sekä muodostaa ja jakaa kyberturvallisuuden yhdistettyä tilannekuvaa. Eri viranomaistoimijat, yksityinen sektori ja kansainväliset yhteistyöverkostot tuottavat havainto- ja analyysitietoja tähän tilannekuvaan.

Strategisella tasolla VN-TIKE huolehtii valtioneuvoston yhteisen tilannekuvan tuottamisesta. Se tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista

koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille.

Kybersuojauksessa työn- ja vastuunjako valtionhallinnon toimijoiden välillä ei ole ongelmaton reagointinopeuden, vastatoimien koordinoinnin ja rahoituksen näkökulmasta. Pitkälle kehittyneet ja perinteisille suojaustavoille vieraat kyberhyökkäykset (Advanced Persistent Threat -hyökkäykset, APT) voivat edetä niin nopeasti, että valtioneuvoston voi olla vaikeaa vastaavalla nopeudella päättää ohjesääntönsä mukaisesti häiriötilanteen hallinnasta. Pahimmassa tapauksessa vastuuttaminen pitäisi pystyä tekemään muutamissa minuuteissa, käynnistää vastatoimet viivytyksettä ja ottaa käyttöön kyvyt ja välineet.[166]

Yhteiskunnan turvallisuusstrategiasta, edellä mainitusta Valtion tarkastusviraston tarkastuskertomuksen vaatimuksesta ja tämän tutkimuksen asiantuntijaorganisaatioiden haastatteluiden perusteella kansallisen kyberturvallisuuden johtamisen normaali- ja poikkeusoloissa kriittiset menestystekijät ovat hyvä tilannetietoisuus, riittävät toimintavaltuudet, nopea reagointikyky, selkeä toimintamalli ja toiminnan resursointi.

Strategisessa johtamisessa tarvittavan tilannekuvan, -tietoisuuden ja -ymmärryksen kehittämiseksi tarvitaan nykyisen toimintamallin tehostamista sekä datavarannon ja yhteistoimintaverkoston kehittämistä. Strategisen johtamisen keskittäminen tehostaa myös tilannetietoisuutta ja -ymmärrystä. Johtamisen vaikuttavuutta edustavat mm. seuraavat ominaisuudet; toiminnan yhdenmukaisuus tilanteesta toiseen, toiminnan siiloutumisen estäminen, keskinäisriippuvaisuuden huomioiminen ja toiminnan koordinointi. Tutkimuksessa on usein asiantuntijoiden arvioinneissa tunnistettu tilannetietoisuuden ja strategisen johtamistoiminnan resursoinnin kapeikot, joten keskittämisellä voidaan optimoida rajallisia resursseja.

Kansallisten kyberturvallisuuden häiriötilanteiden hallinnan tavoitteiden saavuttamiseksi tarvitaan seuraavia toimenpiteitä:

- Kehitetään keskitettyä tilannekuvaympäristöä Kyberturvallisuuskeskuksen pohjalta, joka on tukena valtion virastoille, kriittisille infrastruktuurin toimijoille ja kumppaneille 24 tuntia vuorokaudessa.

- Tiivistetään yhteistyötä Kyberturvallisuuskeskuksen ja Valtioneuvoston tilannekeskuksen kanssa (yhteistyön malli riippuu valittavasta kyberturvallisuuden strategisen johtamisen mallista)

- Tukeudutaan käytössä oleviin kansallisiin perusrakenteisiin, joilla seurataan valtakunnallisia verkkoja ja kriittisen infrastruktuurin kumppanuusverkostoja.

- Tehostetaan Kyberturvallisuuskeskuksen kykyä saada käyttöönsä kaikki kyberturvallisuuspoikkeamat. Sen yhteyteen tulisi rakentaa kansallinen kyberturvallisuushavaintojen tietovaranto kaikkien toimijoiden käyttöön.

- Käytetään avoimia ja luottamuksellisia lähteitä kybertilanteen analysoimiseksi. Hyödynnetään tässä työssä erityisesti yhteistoimintaverkostoja (luodaan virtuaalinen kansallinen kyberturvallisuuden analysointikeskus)

- Kootaan tärkeät tiedot ja asiantuntija-analyysit, joiden perusteella voidaan ohjata kansallisen häiriötilanteen eri johto-organisaatiota.

[166] VTV. Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus, Valtiontalouden tarkastusviraston tarkastuskertomukset, 16/2017.

- Ylläpidetään läheistä yhteyttä kansallisiin ja kansainvälisiin kumppaneihin.

- Vahvistetaan kykyä vastata kriittisen infrastruktuurin häiriöihin ripeästi ja tehokkaasti luomalla valmius välittömästi koota kyberturvallisuuskriittisissä tapauksissa reagointiyksikkö (Cyber Response Task Force)

Haastatteluissa asiantuntijat totesivat, että tiedossa oleva Kyberturvallisuuskeskuksen kehittäminen edistää operatiivisen tason kyberturvallisuuden tilannekuvaa ja -tietoisuutta, kun keskus saa siihen riittävät resurssit. Sama resurssilisäys tarvitaan VN-TIKE:n kybertilannekuva ja -ymmärryksen kehittämiseksi.

Analysointikyvykkyyden kehittämiseksi tarvitaan tietovaranto/tietoallas, josta muodostuisi suuria tietomassoja sisältävä paikka kyberhavaintotiedon tallentamiseen ja prosessointiin. Tämän tietovarannon ympärille muodostuisi usean toimijan ekosysteemi, jossa kukin voisi omilla analyysityökaluillaan hyödyntää koottua tietoa. Ratkaisu mahdollistaisi analysoinnin toteuttamisen toiminnan eri tasoilla virtuaaliyhteisössä. Strategiselle tasolle muodostettaisiin kyky koota saadusta informaatiosta ylimmälle johdolle tarkoitettu strateginen kybertilannetietoisuus. Strateginen analyysi toimisi kiinteässä yhteistyössä VN-TIKE:n kanssa.

6.4 Kyberturvallisuuden kyvykkyyden seuraaminen ja kypsyysmalli

Suomen kansallisen kyberturvallisuuden toimeenpano-ohjelma 2017 -2020 kokoaa yhteen julkisen hallinnon, elinkeinoelämän ja järjestöjen toteutettavat laaja-alaiset ja merkittävät tieto- ja kyberturvallisuutta parantavat hankkeet ja toimenpiteet vastuineen. Toimeenpano-ohjelman etenemisen seuraaminen siihen sisältyvien hankkeiden ja toimenpiteiden osalta edellyttää niiden kehityksen mittaamista, mistä muodostuu kansallisen kyberturvallisuuden eri kyvykkyyksien kehittymisen seuraaminen kyseisellä tarkastelujaksolla. Mittaamisen tulee tukea myös toteutettujen toimenpiteiden laadun seuraamista. Toimeenpano-ohjelma sisältää laajasti vaikuttavia toimenpiteitä, joita kehitetään hallinnonalakohtaisilla muilla toimenpiteillä sekä kyber- ja tietoturvallisuuden ja toiminnan jatkuvuuden hallinnan kehittämiseen liittyvällä työllä. Toimeenpano-ohjelman etenemisen mittaamista tarkasteltaessa ja mittaria valittaessa nämä vaatimukset on otettava huomioon.

Tutkimuksessa keskityttiin löytämään kansallisen kyberturvallisuusstrategian linjausten mukaisten toimenpiteiden edistystä mittaava ja kansalliseen toimintaympäristöön parhaiten soveltuva mittaristo unohtamatta kuitenkaan mittariston mukautuvuutta ja käytettävyyttä eri organisaatioiden käyttöön. Edellä kuvatun laadukkaan mittarin näkökulmista arvioituna jatkotarkasteluun valittiin kaksi mittaria, joita seuraavaksi arvioidaan toimeenpano-ohjelman mittaamisen tarpeita vasten ja arvioidaan kansalliseen käyttöön esitettävän mittariston mukauttamista eri organisaatioiden omaan käyttöön.

Luvussa 5 esitettyjen perusteiden perusteella mittarin valinta johti tarkasteluun kahden vaihtoehdon kesken. Ne ovat *National Cyber Security Index (NCSI)* ja *Cyber Security Capability Maturity Model (CMM)*. Nämä mittarit tukevat parhaiten tarkasteluissa olleiden mittareiden osalta kansallisen kyberturvallisuuden toimeenpano-ohjelman edistymiseen liittyvää päätöksentekoa ja tarinaa sen etenemisestä. Ne pitävät sisällään muita kattavammat luokitteluasteikot ja ovat siten tarkastelukohteen osalta tarkoituksenmukaisimpia.

Liitteessä 1 on esitetty taulukkona A National Cyber Security Index (NCSI) mittarin rakenne. Mittariin on hahmoteltu Suomen kansallisen kyberturvallisuuden toimeenpano-ohjelman

kohdat, joita sillä voidaan arvioida seurattavan. Mittarilla voidaan seurata toimeenpano-ohjelman toteutumista laajasti eikä mittari toisaalta sisällä mittaustarpeiden osalta ylimääräisiä muuttujia. Siitä puuttuvat ainoastaan sähköenergian toimitusvarmuuteen ja yhteiskunnan keskeisten kohteiden sähkönjakelun varmistamiseen (kohta 16) sekä huoltovarmuuskriittisten yritysten kyberturvallisuuden edistämisen seuraamiseen (kohta 17) liittyvät kohdat. Arvioinnissa on oletettu, että kohta 7, toimeenpano-ohjelman seurantamittaristo on luotu ja otettu käyttöön.

Liitteessä 2 on esitetty taulukkona Cyber Security Capability Maturity Model (CMM) mittarin rakenne. Mittariin on hahmoteltu samoin kuin edellisen mittarin tapauksessa Suomen kansallisen kyberturvallisuuden toimeenpano-ohjelman kohdat, joita sillä voidaan arvioida seurattavan. Tälläkin mittarilla voidaan seurata toimeenpano-ohjelman toteutumista laajasti, mutta sen rakenne on huomattavasti monipuolisempi kuin NCSI-mittarin rakenne, joten se sisältää merkittävästi enemmän arvioitavia muuttujia. Siitä puuttuvat myös sekä sähköenergian toimitusvarmuuteen ja yhteiskunnan keskeisten kohteiden sähkönjakelun varmistamiseen, että huoltovarmuuskriittisten yritysten kyberturvallisuuden edistämisen seuraamiseen liittyvät kohdat. Lisäksi siitä puuttuu merkittävä kansainvälisen yhteistoiminnan seuraamiseen liittyvä muuttuja. Tässäkin arvioinnissa on oletettu, että kohta 7, toimeenpano-ohjelman seurantamittaristo on luotu ja otettu käyttöön.

Yhteenvetona em. mittareista voidaan todeta, että molemmat niistä ovat mittauskohteen osalta kattavia ja siten niiden voidaan arvioida olevan käyttöön sopivia. *NCSI-mittari kohdentuu CMM-mittaria täsmällisemmin Suomen kansallisen toimenpano-ohjelman seuraamiseen.* Se ei sisällä mittauskohteen osalta ylimääräisiä osia, joten sen toteuttamisen ja ylläpitämisen voidaan katsoa olevan CMM-mittaria resurssitehokkaampi. Koska Viro käyttää mittaria, siitä syntyisi lisäksi synergiaetuja maittemme välillä. Mittarin kansainvälinen käyttö laajenee koko ajan, joten sen antamien tulosten voi arvioida olevan riittäviä myös kahdenvälistä arviointia laajempaan kansainväliseen Suomen kyberturvallisuuden kyvykkyyden vertailuun. **Edellä mainituista syistä johtuen NCSI-mittarin arvioidaan soveltuvan parhaiten Suomen kansalliseksi kyberturvallisuuden kyvykkyyttä osoittavaksi mittariksi.**

Tärkeimmät jatkotoimenpiteet liittyvät mittarin käyttöönottoon. Lähtökohtana on parhaillaan käynnissä oleva arviointi. Tarvittavat jatkotoimenpiteet ovat hyvä päättää arviointiprosessin kokemusten perusteella.

Liitteen 1 taulukossa 5 on hahmoteltu NCSI-mittarin pohjalta yritysten ja muiden organisaatioiden käyttöön soveltuva mittari. Tämän mittarin käyttöönoton voi katsoa kohdistuvan toimeenpano-ohjelman kohdan 20 tavoitteeseen ”Kansallinen kevyt kyberturvallisuusarviointi, jonka avulla organisaatiot voivat huolehtia minimitason saavuttamisesta turvallisuuden osalta, on laadittu”. Mittarin käyttöönotolla voitaisiin vastata siis kohdan 20 tavoitteeseen, mutta sen käyttö esimerkiksi kriittisen infrastruktuurin organisaatioissa mahdollistaisi koko alueen kyberturvallisuuden kehityksen seuraamisen yhtä hyvin kuin se palvelisi myös muidenkin yksittäisten organisaatioiden omia tarpeita.

LIITE 1 NCSI-MITTARI

Taulukossa 4 on esitetty NCSI-mittarin rakenne ja kansallisen kyberturvallisuuden toimeenpano-ohjelman (TPO 2017-2020) eri kohtien vastaavuus.

Taulukko 4 NCSI-mittari ja kansallisen TPO:n vertailu

	INDICATORS	LEGAL	UNITS	COOPR	OUT-COME
	GENERAL CYBER SECURITY INDICATORS				
1	Capacity to develop national security policies	1,2,4	1,2,4	1,2,4	1,2,4
2	Capacity to analyze national level cyber threats	3,20	3,20	3,20	3,20
3	Capacity to provide cyber security education	6,22	6,22	6,22	6,22
	BASELINE CYBER SECURITY INDICATORS				
4	Capacity to ensure baseline cyber security	11,21	11,21	11,21	11,21
5	Capacity to provide secure environment for e-services	13,18	13,18	13,18	13,18
6	Capacity to provide e-identification and e-signature	15	15	15	15
7	Capacity to protect essential e-services /CII	12,19	12,19	12,19	12,19
	INCIDENT AND CRISES MANAGEMENT INDICATORS				
8	Capacity to detect and respond to cyber incidents 24/7	9	9	9	9
9	Capacity to manage large-scale crises	14	14	14	14
10	Capacity to fight against cybercrime	10	10	10	10
11	Capacity to conduct military cyber operations	8	8	8	8
	INTERNATIONAL INFLUENCE INDICATORS				
12	Capacity to provide international cyber security	5	5	5	5

Taulukossa 5 on esitetty NCSI-mittarin modifioitu rakenne organisaatiokohtaiseen hyödyntämiseen.

Taulukko 5 NCSI-mittari organisaatiokäyttöön

	INDICATORS	QUIDE	UNITS	COOPR	OUT-COME
	GENERAL CYBER SECURITY INDICATORS				
1	Capacity to develop organization security policies				
2	Capacity to analyze organization level cyber threats				
3	Capacity to provide cyber security education				
	BASELINE CYBER SECURITY INDICATORS				
4	Capacity to ensure baseline cyber security				
5	Capacity to provide secure environment for e-services				
6	Capacity to provide e-identification and e-signature				
7	Capacity to protect essential e-services				
	INCIDENT AND CRISES MANAGEMENT INDICATORS				
8	Capacity to detect and respond to cyber incidents 24/7				
9	Capacity to manage large-scale crises				
10	Capacity to fight against cyberattacks				
11	Capacity to conduct defensive cyber operations				
	INTERNATIONAL INFLUENCE INDICATORS				
12	Capacity to provide international cyber security				

LIITE 2 CCM-MITTARI

Taulukossa 6 on esitetty CMM-mittarin rakenne ja kansallisen kyberturvallisuuden toimeenpano-ohjelman (TPO 2017-2020) vastaavuus.

Taulukko 6 CMM-mittarin rakenne ja kansallisen TPO:n vastaavuus

DIMENSIONS	CATEGORIES	TPO-KOHTA
Dimension 1: Cyber Security Policy and Strategy		
	D1-1: National Cyber Security Strategy	**1,2,3,4,5**
	• Strategy Development	1
	• Organization	2
	• Content	3,4,5
	D1-2: Incident Response	**8**
	• Identification of incidents	
	• Organization	
	• Coordination	
	D1-3: Critical National Infrastructure (CNI) Protection	
	• Identification	
	• Organization	
	• Response planning	
	• Coordination	
	D1-4: Crisis Management	**14,20**
	• Planning	14
	• Evaluation	20
	D1-5: Cyber Defence Consideration	
	• Strategy	
	• Organization	
	• Coordination	
	D1-6: Digital Redundancy	
	• Planning	
	• Organization	
Dimension 2: Cyber culture and society		
	D2-1: Cyber Security Mind-set	
	• Government	
	• Private sector	
	• Society at-large	
	D2-2: Cyber security Awareness	**9**
	• Awareness raising	9
	D2-3: Confidence and trust on the Internet	**12,15,18,19,21**
	• Trust in use of on-line services	15
	• Trust in e-government	12,18,19
	• Trust in e-commerce	21
	D2-4: Privacy online	
	• Privacy standards	
	• Employee privacy	
Dimension 3 - Cyber security education, training and skills		
	D3-1: National availability of cyber education and training	**22**
	• Cyber Education	22
	• Training	22

	D3-2: National Development of cyber security education	
	• National development of cyber security education	
	D3-3: Corporate training & educational initiatives within companies	
	• Training employees in cyber security	
	D3-4: Corporate Governance, Knowledge and Standards	
	• Boardroom Understanding of Cybersecurity	
Dimension 4 - Legal and regulatory frameworks		
	D4-1: Cyber security legal frameworks	**10,11**
	• Legislative framework for ICT Security	11
	• Privacy, data protection & other human rights	
	• Substantive cybercrime law	10
	• Procedural cybercrime law	
	D4-2: Legal Investigation	
	• Law Enforcement	
	• Courts	
	D4-3: Responsible Disclosure	
	• Responsible Disclosure	
Dimension 5: Standards, organizations and technologies		
	D5-1: Adherence to standards	
	• Implementation of standards and minimal acceptable practices	
	• Procurement	
	• Software Development	
	D5-2: National Infrastructure Resilience	**13**
	• Infrastructure Technology	
	• National Resilience	13
	D5-3: Cyber Security marketplace	**6**
	• Cyber security Technologies	
	• Cyber Insurance	6

LÄHTEITÄ JA TAUSTA-AINEISTOJA

1. Kirjallisuus, katsaukset

Aaltola, M., Käpylä, J., Mikkola, H. & Behr, T. *Towards the Geopolitics of Flows: Implications for Finland.* Ulkopoliittisen instituutin raportti 40. Ulkopoliittinen instituutti, 2014. Haettu osoitteesta: https://storage.googleapis.com/upi-live/2017/01/fiia_report_40_web.pdf

ABI Research. Global Cybersecurity Index & Cyberwellness Profiles April 2015

Accenture. *Aplifyyou. Technology for People. The Era of the Intelligent Enterprise*. Technology Vision 2017, 2016

BSA The Software Alliance. EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace, 2017. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

BSI, German Federal Office for Information Security. haettu osoitteesta: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

EGA. e-Governance Academy. National Cyber Security Index (NCSI). Methodology description, 2017. Haettu osoitteesta: http://ncsi.ega.ee/methodology-description

Eisenhardt, K. Making Fast Strategic Decisions in High-Velocity Environments, 1989. The Academy of Management Journal, 32(3), 543-576

Erillisselvitys kyberturvallisuusasioiden järjestämisestä

Euroopan komissio. Pohdinta-asiakirja Euroopan puolustuksen tulevaisuudesta, 23.7.2017. Haettu osoitteesta: https://www.eduskunta.fi/FI/tiedotteet/Sivut/komission-pohdinta-euroopan-puolutuksen-tulevaisuudesta.aspx,
Euroopan komissio, Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentami-nen EU:lle, JOIN(2017) 450 final, 13.9.2017,

Euroopan komissio, Tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle, Kahdestoista raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia, COM(2017) 779 final/2, Bryssel 18.1.2018

Euroopan parlamentin päätöslauselma Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö, 6.9.2013

Euroopan parlamentin ja neuvoston asetus 2016/679, Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), 27 päivänä huhtikuuta 2016

Euroopan unionin kyberturvallisuusstrategia - Avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013) 1 final, 7.2.2013

Euroopan unionin verkko- ja tietoturvadirektiivi (NIS-direktiivi), 17.6.2016

Global Cyber Security Capacity Centre University of Oxford. Cyber Security Capability Maturity Model (CMM) – V1.2, 2014. Haettu osoitteesta: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, HE 192/2017 vp

Hanén, Tom. Yllätysten edessä. Kompleksisuusteoreettinen tulkinta yllättävien ja dynaamisten tilanteiden johtamisesta, 2017. Julkaisusarja 1: Tutkimuksia nro 11. Maanpuolustuskorkeakoulu. Helsinki.

Hathaway Melissa, Demchak Chris, Kerben Jason, McArdle Jennifer, Spidalieri Francesca, Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index, 2015. Haettu osoitteesta: www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cyber-Readiness_EN.pdf

Hathaway Melissa, Demchak Chris, Kerben Jason, McArdle Jennifer, Spidalieri Francesca, India Cyber Readiness at a Glance, 2016. Haettu osoitteesta: http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf

Horsmanheimo S., Kokkoniemi-Tarkkanen H., Kuusela P., Tuomimäki L., Puuska S., Vankka J. Kriittisen infrastruktuurin tilannetietoisuus. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 19/2017

Huoltovarmuuskeskus. Huoltovarmuuskeskuksen verkkosivut, 2017. Haettu osoitteesta:https://www.huoltovarmuuskeskus.fi/organisaatio/sektorit-ja-poolit/

Huoltovarmuuskeskus. Kyberturvallisuuden tilannekuva energia-alalla, Huoltovarmuuskeskuksen verkkosivut, https://www.huoltovarmuuskeskus.fi/kyberturvallisuuden-tilannekuva-energia-alalla/

International Telecommunication Union & ABI Researc. Global Cybersecurity Index and Cyberwellness Profiles, report 2015

ITU. Global Cybersecurity Index 2017. Haettu osoitteesta: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Janhunen Kirsi. Valtionhallinnon häiriötilanteiden hallinta – miten VIRT-toimintaa kehitetään? Valtionvarainministeriö. VAHTI-päivä 10.12.2015. Haettu osoitteesta: http://vm.fi/documents/10623/1942650/VAHTI_p%C3%A4iv%C3%A4_1210_2015_VIRT-toiminta.pdf/7cf270bb-77cb-419c-aa0a-825007508aa2

Juuti Pauli, Luoma Mikko, Strateginen johtaminen, Kustannusyhtiö Otava, Keuruu 2009

Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, Turvallisuuskomitea, 2017

Kuusisto Rauno, Tilannekuvasta täsmäjohtamiseen, - Johtamisen tietovirrat kriisihallinnan verkostossa, Liikenne- ja viestintäministeriö, Helsinki 2005

Kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia

Laki sähköisen viestinnän palveluista, 7.11.2014/917

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, 1406/2011

Lehto Martti, Limnéll Jarno, Innola Eeva, Pöyhönen Jouni, Rusi Tarja, Salminen Mirva, Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, helmikuu 2017, ISBN 978-952-287-368-2 (verkkoj.)

Leppänen, A., Linderborg, K. & Saarimäki, J. Tietoverkkorikollisuuden tilannekuva, 2016. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, 17/2016. Haettu osoitteesta: http://tietokayttoon.fi/documents/10616/2009122/17_Tietoverkkorikollisuuden+tilannekuva.pdf/6ef911d2-cbe8-43bd-aafa-e10ed573f28a?version=1.0

Liikenne- ja viestintäministeriö. Maailman luotetuinta digitaalista liiketoimintaa, Suomen tietoturvallisuusstrategia, 7/2016, 19.4.2016

Liikenne- ja viestintäministeriö. Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti, 20.4.2017

Liikenne- ja viestintäministeriö, Virastouudistus, 19.1.2018. Haettu osoitteesta; https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0246e40f-4e8a-46d4-81fb-6b255600b34b

Miessler, Daniel. An Information Security Metrics Primer, 28.12.2014. Haettu osoitteesta: https://danielmiessler.com/study/information-security-metrics/#good

Ministeriöiden kyberturvallisuustehtävät, 10.2.2014, http://www.turvallisuuskomitea.fi/index.php/fi/component/k2/16-ministerioiden-kyberturvallisuustehtavat

NATO Strategic Foresight Analysis. 2017 Report. Haettu osoitteesta: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf

Rantala Jonna. NIS-direktiivin kahdet kasvot – riskit ja riskienhallinta, Jyväskylän yliopisto, Tietotekniikan pro gradu -tutkielma 24.9.2017

Rikk Raul. Analytical Article How to Measure National Cyber Security: the development of national cyber security index, 2017

Räsänen Erkki. Varautuminen sopimuksin kyberturvallisuusuhkiin, 14.4.2016

Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö, 14.1.2015

Turvallisuuskomitea. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017. Haettu osoitteesta: https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/126-suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020

Valmiuslaki, 29.12.2011/1552

Valtioneuvoston asetus valtioneuvoston ohjesäännön muuttamisesta, 333/2017, 1.6.2017

Valtioneuvoston asetus valtiovarainministeriöstä, 26.6.2003/610

Valtioneuvoston ohjesääntö, 3.4.2003/262

Valtioneuvoston päätös huoltovarmuuden tavoitteista, 857/2013, Helsinki 5.12.2013

Valtiovarainministeriö. Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet. Valtiovarainministeriön julkaisuja 2016.

Viestintävirasto. HAVARO havainnoi ja varoittaa tietoturvaloukkauksista. Viestintäviraston verkkosivut, 2016. Haettu osoitteesta: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605241520.html

Virrantaus Kirsi, Seppänen Hannes. Yhteiskunnan kriittisen infran dynaaminen haavoittuvuusmalli. MATINE: Tiivistelmäraportti 2013/841. Haettu osoitteesta: https://www.defmin.fi/files/2728/841_Virrantaus_tiivistelmaraportti_2013.pdf

VNK. Varautuminen ja kokonaisturvallisuus. Komiteamietintö. Valtioneuvoston kanslian julkaisusarja, 21/2010. Haettu osoitteesta: http://vnk.fi/documents/10616/622962/J2110_Varautuminen+ja+kokonaisturvallisuus.pdf/da689ade-30ad-4c1e-8221-90ecd62c4cad?version=1.0

VTT. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015, haettu osoitteesta: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79562/Kyberosaaminen%20Suomessa.pdf?sequence=1&isAllowed=y

VTV. Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus, Valtiontalouden tarkastusviraston tarkastuskertomukset, 16/2017. Haettu osoitteesta: https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

World Bank. The World Bank Supports the Strengthening of Cyber Security in Kosovo, 2015. Haettu osoitteesta: http://www.oxfordmartin.ox.ac.uk/downloads/cybersecurity/WB-GCSCC%20Kosovo%20press%20release.pdf

Yhteiskunnan turvallisuusstrategia, Yhteiskunnan turvallisuusstrategia ja sen liitteet. Valtioneuvoston periaatepäätös, 2.11.2017

2. Maakatsaukset

Alankomaat

2011 The National Cyber Security Strategy (NCSS): Strength through cooperation

2012 The Defence Cyber Strategy.

2013 National Manual on Decision-making in Crisis Situations – The Netherlands.

2014 National Cyber Security Strategy 2 (NCSS 2): From awareness to capability

2017 'Building Digital Bridges' - International Cyber Strategy: Towards an integrated international cyber policy

Kansallisen turvallisuus- ja vastaterrorismin koordinaattorin julkaisemat vuosittaiset kyberturvallisuusarviot 2015, 2016 ja 2017. Saatavilla: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands

Keskeisten kyberturvallisuusorganisaatioiden internet-sivut:

- National Cyber Security Centre (https://www.ncsc.nl/english)
- Dutch Cyber Security Council (https://www.cybersecurityraad.nl/index-english.aspx)
- National Coordinator for Security and Counterterrorism (https://english.nctv.nl/)

Melissa Hathaway ja Francesca Spidalieri (2017) The Netherlands Cyber Readiness at Glance. Potomac Institute for Policy Studies.

Kadri Kaska (2015) National Cyber Security Organization: the Netherlands. Sarjan toimittaja Kadri Kaska. Nato DDC COE.

Eric Luiijf (2016) National Cyber Security Organisation, Part 1: The Netherlands. Teoksessa Lech J. Janczewski ja William Caelli (toim.) Cyber Conflicts and Small States. Ashgate, Farnham. Pp. 71-102.

Australia

2016 Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity

2016 Defence White Paper.

2017 Australia's Cyber Security Strategy: First Annual Update

2017 Strategies to Mitigate Cyber Security Incidents. A New Cyber Security Baseline.

Kyberturvallisuuskeskuksen vuosittaiset uhkaraportit 2015, 2016 ja 2017. Saatavilla: https://www.acsc.gov.au/publications.html

Keskeisten kyberturvallisuusorganisaatioiden internet-sivut:

CERT Australia (https://www.cert.gov.au/)

Australian Cyber Security Centre (https://www.acsc.gov.au/index.html)

Australian Signals Directorate (https://www.asd.gov.au/)

AusCERT (https://www.auscert.org.au/)

William Caelli (2016) National Cyber Security Organisation, Part 1: Australia. Teoksessa Lech J. Janczewski ja William Caelli (toim.) Cyber Conflicts and Small States. Ashgate, Farnham. Pp. 123- 162.

Frank Smith & Graham Ingram (2017) Organising cyber security in Australia and beyond. Australian Journal of International Affairs 71(6), pp. 642-660.

Igor Mikolic-Torreira, Don Snyder, Michelle Price, David Shlapak, Sina Beaghley, Megan Bishop, Sarah Harting, Jenny Oberholtzer, Stacie Pettyjohn, Cortney Weinbaum & Emma Westerman (2016) Exploring Cyber Security Policy Options in Australia. RAND Corporation and Australian National University, National Security College. Available at: https://www.rand.org/pubs/research_reports/RR2008.html [16.9.2017]

Israel

Dmitry Adamsky (2017) “The Israeli Odyssey toward its National Cyber Security Strategy” The Washington Quarterly 40(2), Summer 2017, pp. 113-127.

Advancing National Cyberspace Capabilities. Resolution No. 3611 of the Government of August 7, 2011 (http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/ Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf) [29.8.2016]

Elran, Meir & Gabi Siboni (2015) “Establishing an IDF Cyber Command” INSS Insight No. 719, July 8, 2015 (http://www.inss.org.il/index.aspx?id=4538&articleid=10007)

Even, Shmuel (2015) “The Strategy for Integrating the Private Sector in National Cyber Defense in Israel” Military and Strategic Affairs 7(2), pp. 103—124 (http://www.inss.org.il/ uploadImages/system-Files/MASA7-2Eng%20Final_Even.pdf)

Michael Herzog (2015) “New IDF Strategy Goes Public” The Washington Institute Policy Analysis, Policy Watch 2479, August 28, 2015. Available at: http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public [19.11.2017]

Deborah Housen-Couriel (2017) National Cyber Security Organisation: Israel. Sarjan toimittaja Kadri Kaska. Nato DDC COE.

Grzegorz Małecki (2017) Summary – a path forward – comparing Israeli and Polish experiences. Teoksessa Buildig cybersecurity system in Poland: Israeli experience. Fundacja im. Kazimierza Pułaskiego, Warsaw, pp. 21-24.

Eviatar Matani; Lior Yoffe & Michael Mashkautsan (2016) A Three-Layer Framework for a Comprehensive National Cybersecurity Strategy. Georgetown Journal of International Affairs 17(3), pp. 77-84.

Eviatar Matani; Lior Yoffe & Tal Goldstein (2017) “Structuring the national cyber defence: in evolution towards a Central Cyber Authority” Journal of Cyber Policy 2(1), pp. 16-25.

National Cyber Bureaun internet-sivut (http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx)

National Cyber Bureaun strategiaesitys (http://scirex.grips.ac.jp/center/wp-content/uploads/2015/12/151110_matania.pdf)

National Cyber Bureaun taustapaperi (https://ccdcoe.org/sites/default/files/documents/ Background_for_the_Government_Resolutions_Regarding_Cyber_Security-February_2015.pdf)

Lior Tabansky & Isaac Ben Israel (2017) Cybersecuriy in Israel: Why the Success? Teoksessa Buildig cybersecurity system in Poland: Israeli experience. Fundacja im. Kazimierza Pułaskiego, Warsaw, pp. 6-14.

Lior Tabansky & Isaac Ben Israel (2015) Cybersecurity in Israel. Springer Briefs in Cybersecurity.

Ruotsi

2009 Strategi för samhällets informationssäkerhet 2010–2015. MSB.

2011 Förutsättningar för krisberedskap och totalförsvar i Sverige. Försvarshögskolan.

2012 Samhällets informationssäkerhet: Nationell handlingsplan. MSB.

2014 Regeringens proposition 2014/15:109. Försvarspolitisk inriktning – Sveriges försvar 2016–2020.

2015 Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. SOU 2015:23.

2015 En ny säkerhetsskyddslag. SOU 2015:25.

2016 Nationell handlingsplan för samhällets informationssäkerhet. Slutrapport. MSB.

2017 Nationell säkerhetsstrategi.

2017 Nationell strategi för samhällets informations- och cybersäkerhet Skr. 2016/17:213.

Brå:n tutkimusraportti (https://www.bra.se/download/18.62fc8fb415c2ea1069322f02/ 1499074273136/2017_17_It-inslag_i_brottsligheten_kortv_webb.pdf)

MSB:n tiedote (https://www.msb.se/Upload/Forebyggande/Informationssakerhet/ Fakta-bad%20SAMFI.pdf)

Oikeusministeriön tiedote (http://www.government.se/49edf4/contentassets/ b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf)

Keskeisten kyberturvallisuusorganisaatioiden internet-sivut:

MSB (https://www.msb.se/)

CERT-SE (https://www.cert.se/)

Singapore

2013 National Cyber Security Masterplan 2018

2016 Singapore's Cyber Security Strategy

2017 Singapore Cyber Landscape

2017 Cybersecurity Bill (laki viedään parlamentin käsittelyyn 2018)

Keskeisten kyberturvallisuusorganisaatioiden internet-sivut:

Cyber Security Agency of Singapore (https://www.csa.gov.sg/)

SingCERT (https://www.csa.gov.sg/singcert)

Chung Vu (2016) Cyber Security in Singapore. Policy Report. RSiS Nanyang Technological University. S. Rajaratnam School of International Studies. Available at: https://www.rsis.edu.sg/ wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singa-pore.pdf [5.11.2017]

Viro

2008 National Cyber Security Strategy 2008-2013

2010 National Security Concept of Estonia (vuoden 2017 päivitys ei ollut saatavilla)

2011 National Defence Strategy Estonia

2014 Cyber Security Strategy 2014-2017

Tietojärjestelmäviranomaisen vuosittaiset kyberuhka-arviot 2015 ja 2017. Saatavilla: https://www.ria.ee/en/publications.html [9.11.2017]

Keskeisten kyberturvallisuusorganisaatioiden internet-sivut:

Tietojärjestelmäviranomainen (https://www.ria.ee/en/about-estonian-information-system-authority.html)

CERT-Estonia (https://www.ria.ee/en/cert-estonia.html)

Osula, Anna-Maria (2015) National Cyber Security Organisation: Estonia. Sarjan toimittaja Kadri Kaska. Nato CCD COE.

Pernik, Piret & Emmet Tuohy (2013) Cyber Space in Estonia: Greater Security, Greater Challenges. Report. International Centre for Defence Studies.

Pernik, Piret & Emmet Tuohy (cccc) Interagency Cooperation on Cyber Security: The Estonian Model. Paper. International Centre for Defence Studies.

Lisäksi: Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, VNK 30/2017 -selvitystä varten kerätty haastattelumateriaali.

VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

tietokayttoon.fi

ISSN 2342-6799 (pdf)
ISBN 978-952-287-532-7 (pdf)