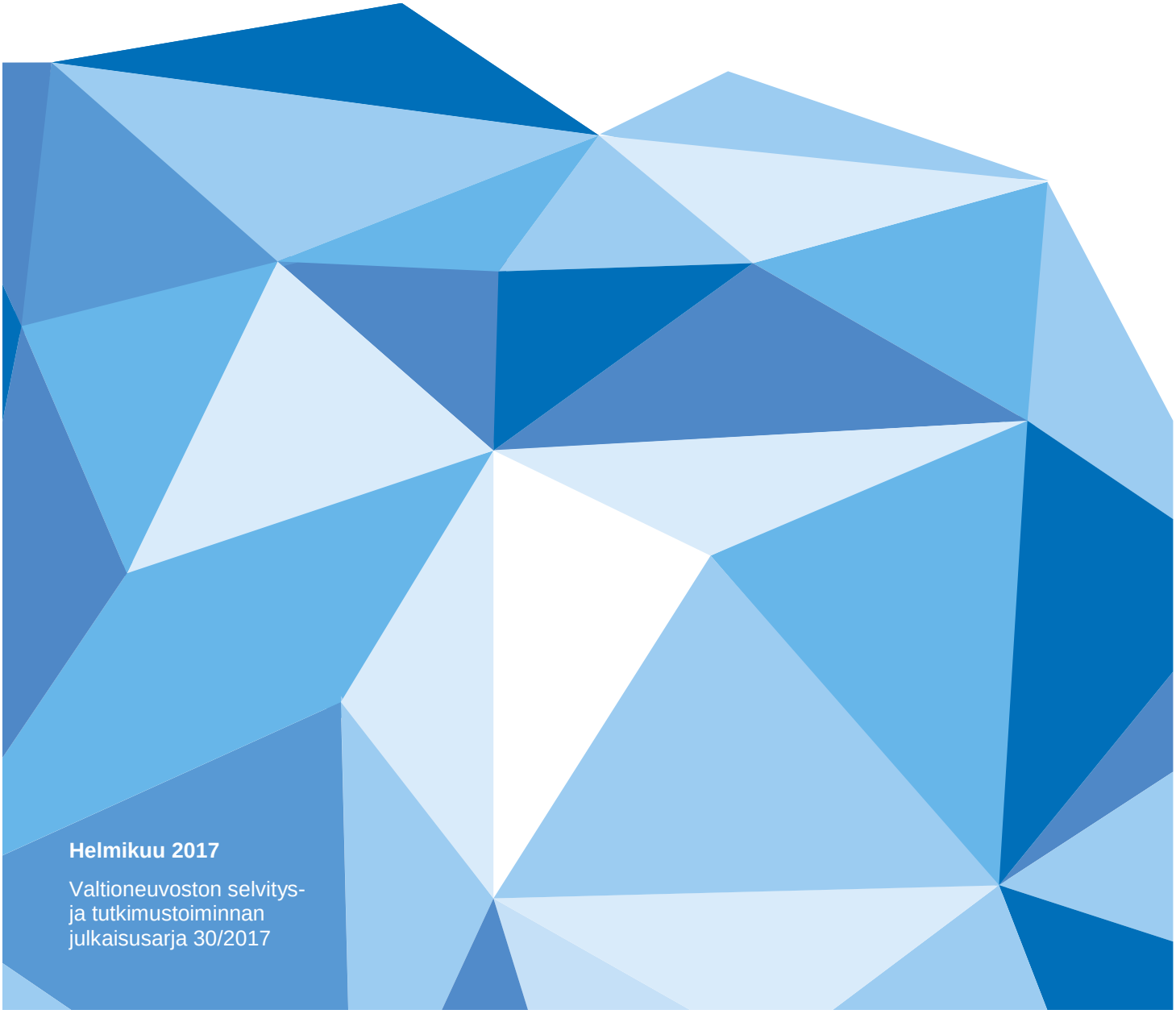
VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

Martti Lehto, Jarno Limnéll, Eeva Innola,
Jouni Pöyhönen, Tarja Rusi, Mirva Salminen

# Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi



**Helmikuu 2017**

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017

# KUVAILULEHTI

| | | | |
|---|---|---|---|
| **Julkaisija ja julkaisuaika** | Valtioneuvoston kanslia, 17.2.2017 | | |
| **Tekijät** | Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, Mirva Salminen | | |
| **Julkaisun nimi** | Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi | | |
| **Julkaisusarjan nimi ja numero** | Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017 | | |
| **Asiasanat** | Kyberturvallisuus, kyberturvallisuusstrategia, turvallisuus, Suomi | | |
| **Julkaisuaika** | Helmikuu, 2017 | **Sivuja** 79 | **Kieli** Suomi |


**Tiivistelmä**

Tämän tutkimushankkeen tavoitteena oli selvittää kokonaisvaltaisesti, kuinka vuoden 2013 kyberturvallisuusstrategiassa asetettu tavoite ”Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” on saavutettu ja millainen Suomen kyberturvallisuuden tavoitetilan tulisi olla vuonna 2020. Tutkimushankkeessa tehtiin turvallisuustilanneanalyysi kyberturvallisuuden megatrendeistä, selvitettiin kyberturvallisuuden nykytila ja kehittämistarpeet julkisella ja yksityisellä sektorilla, analysoitiin kuuden maan kyberturvallisuuden nykytilaa ja sen kehittämistä. Tutkimuksen yhteenvetona esitetään tunnistetut puutteet ja kehityskohteet kyberturvallisuuden tavoitetilan 2020 saavuttamiseksi. Tutkimuksen perusteella Suomi ei ole edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa, mutta kuuluu kansainväliseen kärkikymmenikköön. Suomen kyberturvallisuuden edelläkävijyys on kuitenkin omissa käsissämme.

Tutkimuksessa määriteltiin tavoitetila, jonka mukaan **vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaa kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti.**

Kyberturvallisuus on kehittynyt viime vuosina kyberturvallisuusstrategian strategisten linjausten ja laaditun toimeenpanosuunnitelman perusteella. Tutkimus osoitti, että tarvitaan merkittäviä kehittämistoimia, jotta voimme saavuttaa edelläkävijyyden aseman kyberturvallisuudessa. Tunnistettuja kehittämiskohteita ovat strategisen johtamisen kehittäminen, poliittisen sitoutumisen vahvistaminen, kansainvälisen toiminnan tehostaminen, tilannetietoisuuden ja havaintokyvyn parantaminen, elintärkeiden toimintojen turvaamisen edistäminen, lainsäädännön kehittäminen, resurssien lisääminen, kyberturvallisuuden vahvistaminen kansallisena kilpailuetuna, osaamisen, tutkimuksen ja yleisen tietoisuuden vahvistaminen, kyberturvallisuuden kehittäminen osana kokonaisturvallisuutta sekä toimenpiteiden tehokas seuraaminen ja kypsyysmallin luominen.

Kehittämisen toteuttamiseksi tarvitaan jatkotutkimusta ainakin aiheista: kyberturvallisuuden strateginen johtaminen Suomessa, kybertilannekuvan ja analysointikyvykkyyden kehittäminen sekä yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin ja kyberomavaraisuuden määrittely osana kansallista kyberresilienssiä.



Tämä julkaisu on toteutettu osana valtioneuvoston vuoden 2016 selvitys- ja tutkimussuunnitelman toimeenpanoa (tietokayttoon.fi).

# PRESENTATIONSBLAD

| | |
|---|---|
| **Utgivare & utgivningsdatum** | Statsrådets kansli, 17.2.2017 |
| **Författare** | Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, Mirva Salminen |
| **Publikationens namn** | Cybersäkerheten i Finland - nuläge, måltillstånd och nödvändiga åtgärder för att uppnå måltillståndet |
| **Publikationsseriens namn och nummer** | Publikationsserie för statsrådets utrednings- och forskningsverksamhet 30/2017 |
| **Nyckelord** | Cybersäkerheten, cybersäkerhetsstrategin, säkerheten, Finland |
| **Utgivningsdatum** | Februari, 2017 **Sidantal** 79 **Språk** Finska |


**Sammandrag**

Syftet med forskningsprojektet var att genomföra en övergripande utredning om hur målet i cybersäkerhetsstrategin från 2013 ”Finland ska vara en global föregångare inom beredskapen för cyberhot och i hanteringen av störningar i samband med sådana” har uppnåtts och hurdant Finlands måltillstånd borde vara vad gäller cybersäkerhet år 2020. I forskningsprojektet genomfördes en säkerhetssituationsanalys av megatrenderna inom cybersäkerheten, undersöktes cybersäkerhetens nuläge och utvecklingsbehov på den offentliga respektive privata sektorn, analyserades cybersäkerhetens nuläge och dess utveckling i sex länder. Forskningssammandraget belyser uppfunna brister och utvecklingsmål för att uppnå måltillståndet för cybersäkerheten 2020. Utgående från undersökningen är Finland inte en föregångare inom beredskapen för cyberhot och i hanteringen i samband med sådana, men hör internationellt sett till de tio toppländerna.  Att Finland skulle vara en föregångare inom beredskapen för cyberhot ligger i våra egna händer.

I undersökningen definieras ett måltillstånd, enligt **vilket cybersäkerheten i Finland 2020 är en inbyggd egenskap i det digitala samhället, vilket möjliggör att aktörerna kan förlita sig på alla digitala lösningar och använda sig av dem på ett tryggt sätt.**

Cybersäkerheten har utvecklats under senare år utgående från de strategiska linjedragningarna och den utarbetade verkställighetsplanen för cybersäkerhet. Undersökningen visade att det behövs betydande utvecklingsåtgärder för att Finland ska bli en föregångare inom cybersäkerheten. Utvecklingsmål som identifierats: att utveckla strategisk ledning, att förstärka det politiska engagemanget, att effektivera den internationella verksamheten, att förbättra lägesmedvetenheten och observationsförmågan, att främja betryggandet av livsviktiga funktioner, att utveckla lagstiftningen, att öka resurserna, att förstärka cybersäkerheten som nationell konkurrensfördel, att förstärka kunnandet, forskningen och den allmänna medvetenheten, att utveckla cybersäkerheten som en del av den totala säkerheten samt att effektivt följa upp åtgärderna och att skapa en mognadsplan. För att realisera utvecklingen behövs fortsatt forskning åtminstone om följande teman: strategisk ledning av cybersäkerheten i Finland, utveckling av cyberlägesbeskrivningen och analysförmågan samt definiering av samhällets livsviktiga funktioner, den kritiska infrastrukturen och cybersjälvförsörjningen som en del av den nationella cyberresiliensen.



Den här publikationen är en del i genomförandet av statsrådets utrednings- och forskningsplan för 2016 (tietokayttoon.fi/sv).

# DESCRIPTION


| | |
|---|---|
| **Publisher and release date** | Prime Minister´s Office, 17.2.2017 |
| **Authors** | Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, Mirva Salminen |
| **Title of publication** | Finland's cyber security: the present state, vision and the actions needed to achieve the vision |
| **Name of series and number of publication** | Publications of the Government´s analysis, assessment and research activities 30/2017 |
| **Keywords** | Cyber security, cyber security strategy, security, Finland |
| **Release date** | February, 2017 **Pages** 79 **Language** Finnish |



**Abstract**

The aim of this research project was to clarify comprehensively how the following vision, defined in Finland's Cyber Security Strategy 2013, has been achieved: 'By 2016, Finland will be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats'. A further aim was to clarify what Finland's Cyber Security Vision for 2020 should be. In the project, we performed a security situation analysis on the megatrends of cyber security, surveyed the present state and development needs of cyber security in the public and private sectors, and analysed the present state and development of cyber security in six countries. As a conclusion of the study, we present the identified shortages and the actions needed to achieve the cyber security vision for 2020. Based on the study, Finland is not a global forerunner in cyber threat preparedness and in managing the disturbances caused by them, but it does rank among the ten best countries in this field. However, it is in our own hands whether we will be forerunners in cyber security.

A vision was defined in the study, according to **which in the Finland of 2020, cyber security will be integrated within the digital society, enabling all actors to utilise all the digital solutions of society reliably and safely.**

Cyber security has advanced over the past few years based on the strategic guidelines of the Cyber Security Strategy and its action plan. The study demonstrated that significant measures are needed for Finland to establish a global forerunner position in cyber security. The following development actions were identified: developing strategic management, strengthening political commitment, enhancing international activities, improving situation awareness and observation, promoting the safeguarding of vital functions, developing legislation, increasing resources, strengthening cyber security as a national competitive advantage and as part of overall security, monitoring the actions efficiently, creating a capability maturity model, and enhancing competence, research and general awareness.

In order to promote cyber security, further research is needed at least on the strategic management of cyber security in Finland, the development of a cybersecurity situation picture and analysis skills, and the definition of the vital functions of society, critical infrastructure and cyber self-sufficiency as part of national cyber resilience.



This publication is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2016 (tietokayttoon.fi/en).

# SISÄLLYS

# 1. JOHDANTO

## 1.1 Tutkimuksen tausta ja tavoitteet

### 1.1.1 Tutkimuksen tausta

Kansallisessa kyberturvallisuusstrategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joilla vastataan kybertoimintaympäristöön liittyviin haasteisiin ja varmistetaan kybertoimintaympäristön toimivuus. Kyberturvallisuusstrategia julkaistiin vuonna 2013 ja sitä täydentää vuonna 2014 julkaistu toimeenpano-ohjelma. Strategia esittää yleisen vision kyberturvallisuuden tavoitetilasta ja toimeenpano-ohjelmassa määritetään käytännön toimenpiteitä tavoitteen saavuttamiseksi ja kyberturvallisuuden parantamiseksi. Toimeenpano-ohjelman yhteensä 74 määritettyä toimenpidettä koottiin hallinnonalojen ja huoltovarmuusorganisaation kanssa yhteistyössä. Toimenpiteissä painottuvat yritysten kyberturvallisuuden ja liiketoimintamahdollisuuksien parantaminen sekä julkinen-yksityinen -yhteistyön tehostaminen.

Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja -kerroksisista informaatioverkostoista, joihin kuuluu kansallisia julkishallinnon, yritysmaailman ja turvallisuusviranomaisten tiedonsiirtoverkkoja, informaatiojärjestelmiä ja digitaalisia palveluita ja palvelualustoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta ja ohjausjärjestelmiä, mitkä internetin välityksellä muodostavat maailmanlaajuisen verkoston.

Tämä kybertoimintaympäristön kehitys vaikuttaa myös Suomeen. Suomi on yksi kehittyneimmistä digitaalisista tietoyhteiskunnista, jonka toiminnat ovat riippuvaisia erilaisista digitaalisista verkoista ja niiden antamista palveluista. Tietoteknisten laitteiden ja järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen tai vakavat kyberhyökkäykset voivat aiheuttaa kielteisiä vaikutuksia julkisiin palveluihin, liike-elämään ja hallintoon ja siten koko yhteiskunnan toimintaan.

Kansallisella itsenäisellä kyberkyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Kansallisen kehittämisen perustaksi tarvitaan ajantasainen tilannekuva Suomen kyberturvallisuuden nykytilasta sekä analyysi tavoitetilasta ja tarvittavista toimenpiteistä sen saavuttamiseksi.

### 1.1.2 Tutkimuksen tavoitteet

Tutkimushankkeen tavoitteena oli selvittää kokonaisvaltaisesti, kuinka vuoden 2013 kyberturvallisuusstrategiassa asetettu tavoite ”Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” on saavutettu ja millainen Suomen kyberturvallisuuden tavoitetilan tulisi olla vuonna 2020.

Hankkeen osatavoitteita olivat:

- Kyberturvallisuustilanneanalyysin laatiminen
- Suomen kyberturvallisuustilanne ja strategian toimeenpanon toteutuminen julkisella ja yksityisellä sektorilla
- Kansainvälinen kyberturvallisuuden benchmarking ja Suomen vertautuminen verrokkimaihin

- Suomen kyberturvallisuuden tavoitetila vuonna 2020 ja tarvittavat linjaukset

Tutkimushanke jakautui viiteen työpakettiin, jotka on esitetty taulukossa 1:

Taulukko 1. Tutkimushankkeen työpaketit

| **Työpaketit** | **Tutkimuskysymykset** | **Tavoitteet** |
|---|---|---|
| **WP1**<br><br>**Turvallisuustilanneanalyysi** | Mikä on kybertoimintaympäristön turvallisuustilanne nyt, kuinka tilanne on muuttunut vuodesta 2013 ja mitkä ovat keskeiset tunnistettavissa olevat kybertoimintaympäristön turvallisuuteen vaikuttavat trendit vuoteen 2020 mennessä? | Työpaketin tavoitteena oli tuottaa kuva globaalista kyberturvallisuustilanteesta erityisesti vuoden 2013 jälkeen. |
| **WP2**<br><br>**Suomen kyberturvallisuuden nykytila julkisella sektorilla** | - Onko Kyberturvallisuusstrategian visiona esitetty tavoitetila saavutettu?<br>- Onko suunniteltu toimintamalli toteutunut ja onko kyberturvallisuutta onnistuttu kehittämään strategiassa esitettyjen linjausten mukaisesti?<br>- Ovatko toimijat sitoutuneita toteuttamaan Kyberturvallisuusstrategian toimeenpano-ohjelman listaamia toimenpiteitä ja ovatko tunnistetut toimenpiteet edistäneet strategisten linjausten toteutumista?<br>- Mitkä ovat tunnistetut haasteet Kyberturvallisuusstrategian vision ja strategisten linjausten täysimääräiselle toteutumiselle?<br>- Mitkä toimenpiteet ovat olleet erityisen onnistuneita kansallisen kyberturvallisuuden edistämisessä?<br>- Onko nykyisellä järjestelmällä edellytyksiä estää, rajoittaa ja toipua vakavista kohdistetuista kyberhyökkäyksistä niin, että yhteiskunnan elintärkeät toiminnot kyetään ylläpitämään?<br>- Onko kyberhäiriötilanteisiin varautuminen tai häiriötilanteiden hallinta tarkoituksenmukaisesti organisoitu ja resursoitu? | Työpaketin tavoitteena oli tuottaa tilannekuva kansallisesta kybersuorituskyvystä julkisella sektorilla ja kuinka kyberturvallisuusstrategian tavoitteet ovat toteutuneet. |
| **WP3**<br><br>**Suomen kyberturvallisuuden nykytila yksityisellä sektorilla** | - Onko Kyberturvallisuusstrategian visiona esitetty tavoitetila saavutettu?<br>- Onko suunniteltu toimintamalli toteutunut ja onko kyberturvallisuutta onnistuttu kehittämään strategiassa esitettyjen linjausten mukaisesti?<br>- Ovatko toimijat sitoutuneita toteuttamaan Kyberturvallisuusstrategian toimeenpano-ohjelman listaamia toimenpiteitä ja ovatko tunnistetut toimenpiteet edistäneet strategisten linjausten toteutumista?<br>- Mitkä ovat tunnistetut haasteet Kyberturvallisuusstrategian vision ja strategisten linjausten täysimääräiselle toteutumiselle?<br>- Mitkä toimenpiteet ovat olleet erityisen onnistuneita kansallisen kyberturvallisuuden edistämisessä?<br>- Onko nykyisellä järjestelmällä edellytyksiä estää, rajoittaa ja toipua vakavista kohdistetuista kyberhyökkäyksistä niin, että yhteiskunnan elintärkeät toiminnot kyetään ylläpitämään?<br>- Onko kyberhäiriötilanteisiin varautuminen tai häiriötilanteiden hallinta tarkoituksenmukaisesti | Työpaketin tavoitteena oli tuottaa tilannekuva kansallisesta kybersuorituskyvystä yksityisellä sektorilla ja kuinka kyberturvallisuusstrategian tavoitteet ovat toteutuneet. |

| | | |
|---|---|---|
| | organisoitu ja resursoitu? | |
| **WP4**<br><br>**Kansainvälinen suorituskykyanalyysi** | Kuinka Suomen kyberturvallisuuden nykytila suhteutuu keskeisiin vertailumaihin verrattuna? | Työpaketin tavoitteena oli tuottaa analyysi valittujen maiden kybersuorituskyvystä ja sen kehittämisestä. |
| **WP5**<br><br>**Kyberturvallisuuden tavoitetila 2020** | Toimintaympäristö- ja nykytila-analyysi, tunnistetut puutteet ja kehityskohteet sekä kansainvälinen vertailu huomioiden, millainen Suomen kyberturvallisuuden tavoitetilan tulisi olla vuonna 2020?<br>Millaisia vaihtoehtoisia, myös negatiivisia, kehityskulkuja asetetulle tavoitetilalle on mahdollista tunnistaa?<br>Millaisille taustaolettamuksille eri vaihtoehtoiset kehityskulut perustuvat?<br>Kuinka varmistetaan turvallinen kybertoimintaympäristö yhteiskunnan eri toimijoiden käyttöön ja yritysten toiminnan sekä kasvun takaajaksi?<br>Millaisin strategisin linjauksin, lainsäädäntötoimin, toiminnan organisoinnein, käytännön toimenpitein ja resurssein esitetty tavoitetila vuonna 2020 olisi mahdollista saavuttaa? | Työpaketin tavoitteena oli tuottaa koottu toimintaympäristö- ja nykytila-analyysi, tunnistetut puutteet ja kehityskohteet sekä kansainvälinen vertailu huomioiden, millainen Suomen kyberturvallisuuden tavoitetilan tulisi olla vuonna 2020. |

## 1.2 Aineistot ja menetelmät

Tutkimushankkeessa kerättiin hyvin monipuolinen ja laaja-alainen aineisto. Keskeisimmät aineistokokonaisuudet ovat tärkeimpien kriittisen infrastruktuurin ja julkisen sektorin toimijoiden sekä alan asiantuntijoiden haastattelut, 19 eri organisaatioiden tuottamaa kyberturvallisuuskatsausta, ja käyttöön saadut harjoituskertomukset.

Tutkimushankkeessa haastateltiin yhteensä 31 yksityisten yrityksien ja julkisten organisaatioiden tieto/kyberturvallisuudesta vastaavaa henkilöä. Yksityisten yritysten haastattelujen teemat käsittelivät yritysten kyberturvallisuuden vahvuuksia, heikkouksia, uhkia ja mahdollisuuksia. Lisäksi haastattelussa kartoitettiin laajemmin kunkin toimialan kyberturvallisuuden tilaa ja kehittämistarpeita. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville luvattiin täysi anonymiteetti.

Kansainvälistä vertailutietoa kerättiin kuudesta maasta: Alankomaat, Iso-Britannia, Israel, Ruotsi, Singapore ja Viro. Tutkimusaineisto käsitti kunkin maan kyberturvallisuusstrategian ja vastaavat turvallisuusdokumentit. Lisäksi kustakin maasta pl. Iso-Britannia haastateltiin 2–3 keskeisissä kyberturvallisuustehtävissä toimivaa henkilöä. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville luvattiin täysi anonymiteetti.

Lisäksi tutkimuksessa on hyödynnetty soveltuvin osin Suomen kyberturvallisuusstrategiaa ja sen toimeenpanosuunnitelmaa, Kyberturvallisuusstrategian toimeenpano-ohjelman päivityksen kuulemistilaisuuksien ja haastattelujen pohjalta tehtyä muistiota. Lisäksi keskeistä dokumenttiaineistoa ovat olleet mm. valtionhallinnon strategiat (Yhteiskunnan turvallisuusstrategia, 2010 jne.), aiemmat tutkimukset ja selvitykset (esim. Jyväskylän yliopiston selvitys alan tutkimus- ja koulutustarjonnasta, 2015, VTT:n selvitys Kyberosaaminen Suomessa – Nykytila

ja tiekartta tulevaisuuteen, 2016) ja osin esimerkiksi erilaiset kansainväliset vertailut (esim. Global Cyber Security Index).

Hankkeen eri työpaketeissa käytettiin työmenetelmiä, jotka esitetty taulukossa 2:

Taulukko 2. Hankkeen tutkimusmenetelmät

| **Työpaketti** | **Tutkimusmenetelmä** |
|---|---|
| **WP1** | Aineistolähtöinen sisällönanalyysi |
| **WP2** | Puolistrukturoitu teemahaastattelu |
| **WP3** | SWOT-analyysi |
| **WP4** | Aineistolähtöinen sisällönanalyysi, puolistrukturoitu teemahaastattelu |
| **WP5** | Kvalitatiivinen sisältöanalyysi, jossa käytetään aineistopohjaisen teorian näkökulmaa |

# 2. TURVALLISUUSTILANNEANALYYSI

## 2.1 Kyberturvallisuuden megatrendit vuonna 2016

Kyberuhkaksi kutsutaan tässä tutkimuksessa pahantahtoista tarkoitusta vahingoittaa tai tuhota tietoverkkoa, -järjestelmää tai päätelaitetta. Tutkimuksessa käytössä olleiden raporttien mukaan kyberuhkien merkittävimmät trendit olivat kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhkat, yrityksen sisäpiiri hyökkäyskanavana, liiketoiminnan tuhoamiseen tähtäävät hyökkäykset sekä henkilötietojen varastamiseen tähtäävät hyökkäykset. Myös huijaukset ja tietojen kalastelut, palvelunestohyökkäykset, kohdistetut hyökkäykset sekä jatkuvat hyökkäykset mainittiin useassa raportissa.

Useat tutkimukset mainitsivat yhdeksi suurimmista trendeistä kiristyshaittaohjelmat sekä niiden määrän nopean kasvun myös vuonna 2016. Kiristyshaittaohjelmista syntyy jatkuvasti uusia kehittyneempiä muotoja, ja tämän lisäksi kiristyshaittaohjelma-palveluna -konsepti on hyvin suosittu mustilla markkinoilla. Kiristyshaittaohjelmat tulevat kohdistumaan myös uusille toimialoille, kuten pankki- ja rahoitustoimialalle sekä julkishallintoon. Kiristyshaittaohjelmia kehitetään yhä enemmän myös päätelaitteisiin, erityisesti älypuhelimiin, koska päätelaitteiden ja älypuhelinten käyttö on lisääntynyt edelleen. Kiristyshaittaohjelmat kohdistuvat yhä enenevässä määrin myös yrityksiin. Kiristyshaittaohjelma voi levitä koko yrityksen sisäverkkoon, jolloin se voi pahimmillaan salata kaikki verkkolevyt sekä pilvipalvelujen tiedostot.

Cisco on vuoden 2016 kyberuhkaraportissaan nostanut haavoittuvuudet edelleen yhdeksi päätrendiksi kyberuhkien alueella. Haavoittuvuudet antavat rikollisille mahdollisuuden aikaikkunan toimia. Tätä rikolliset osaavat hyödyntää; hyökkäyskampanjoita ehditään käynnistää ennen kuin sovelluksen heikot kohdat löydetään. Rikolliset hyödyntävät mm. hyökkäystyökalupakkeja, kiristys- ja muita haittaohjelmia, käyttäjän manipulointia yms. Vaikka palvelun tarjoajat uudistavat ja hienosäätävät sovelluskehityksen prosesseja, kehittävät kyberhyökkääjät kuitenkin jatkuvasti uusia taitoja, jotta tietoturva-aukot löydettäisiin nopeasti ja pystyttäisiin hyödyntämään hyökkäyksissä. Kyberhyökkääjät tekevät yhä enemmän hyökkäyksiä, jotka ovat yhä monimutkaisempia sekä haasteellisempia puolustaa. Tietoturva-asiantuntijoiden on jatkuvasti pidettävä yllä ymmärrystä ja tietoa haavoittuvuuksista sekä käytettävä vahvaa ja huolellista korjaustiedostojen päivitysrutiinia. Rikollisten hyödyntämää aikaikkunaa on siis mahdollista lyhentää - ja näin ollen madaltaa tätä riskiä - omaksumalla nopea ja huolellinen korjaustiedostojen päivitysrutiini.

Hyökkääjät etsivät sisäänpääsyä yritysten järjestelmiin yhä alempaa, laitteistojen ytimestä. Hyökkäyksiä on tehty levyasemien laiteohjelmiin sekä grafiikan prosessointiyksiköihin[1]. Hyökkäykset, jotka hyödyntävät BIOS tai muita laiteohjelmien haavoittuvuuksia, osoittavat, että kontrollia saavutetaan sitä enemmän, mitä alemmaksi mennään. Onnistuneiden laitteistohyökkäyksien avulla hyökkääjä pääsee koko fyysiseen koneeseen ilman hälytyksiä. Virtuaalikoneet, koko muistialue, kaikki levyasemat jatkavat toimintaa normaalisti jopa uudelleenkäynnistyksen ja uudelleenasennuksen jälkeen.

Useat tutkimuksessa mukana olevat raportit ilmoittavat, että yrityksen sisäpiiriläiset ovat merkittävä kyberuhka. IBM:n mukaan sisäpiiriläiset tekivät jopa 60% kaikista hyökkäyksistä. Kaspersky puolestaan arvioi, että 21% organisaatioista oli menettänyt luottamuksellista tietoa sisäpiiriuhkan vuoksi vuoden 2014 aikana. Tämän lisäksi Kasperskyn tutkimus osoitti, että

[1] Eng. graphics processing unit

73%:ssa organisaatioista oli ollut sisäpiirin aiheuttama tietoturvatapahtuma vuonna 2015. Sekä IBM että ENISA lukevat tähän ryhmään tahattomat ja tahalliset tekijät. IBM ilmoitti lisäksi, että kokonaismäärä oli kasvanut edellisen vuoden lukemista (55%, vuonna 2014). Verizonin tutkimissa tapauksissa 77% käyttöoikeuksien väärinkäytöstä oli sisäpiiriläisten tekemiä. Verizon tutki vielä tarkemmin näiden sisäpiiriläisten roolia yrityksessä ja totesi, että kolmasosa oli loppukäyttäjiä, joilla oli käyttöoikeudet luottamukselliseen tietoon. Ainoastaan 14% oli esimiesroolissa tai rooleissa, jossa suuremmat käyttöoikeudet johtuivat erityisroolista (esim. järjestelmähallinta tai kehittäjä). Verizonin tutkimus suosittaa, että ”tervehenkistä epäilyä on syytä harrastaa kaikista työntekijöistä”. Motivaationa hyökkääjillä oli joko taloudellinen hyöty (34%) tai vakoilu (25%).

Yksi merkittävistä kybertoimintaympäristön trendeistä on eri tavoin liiketoiminnan tuhoamiseen tähtäävät hyökkäykset. Mandiant raportoi tutkimuksessaan, kuinka hyökkääjät tuhosivat kriittisiä liiketoiminnan järjestelmiä, julkaisivat luottamuksellista tietoa, kiristivät yrityksiä ja pilkkasivat yritysten johtoa. Joidenkin hyökkääjien motiivina oli raha, jotkut kostivat, jotkut kostivat poliittisista syistä ja jotkut halusivat häväistä. Mandiant myös mainitsee, että tuhoamiseen tähtäävät hyökkäykset eroavat perinteisistä ”hitaista ja hiljaisista” hyökkäyksistä, joissa verkkoon on tunkeuduttu ja tietoa varastettu ilman, että on jääty kiinni. Tuhoamiseen tähtäävillä hyökkäyksillä halutaan tuoda julkisuutta hyökkääjälle tai hyökkääjän ajamalle asialle. Lisäksi tuhoamiseen tähtäävät hyökkäykset johtivat usein luottamuksellisen tiedon julkistamiseen – sen seurauksena häväistykseen sekä maineen pilaamiseen. Joissakin tapauksissa yritykset eivät enää pystyneet jatkamaan liiketoimintaa. Hyökkäyksen seurauksena yritysten johtohenkilöitä joutui eroamaan, suuria lunnassummia jouduttiin maksamaan sekä kalliita järjestelmän uusimisia jouduttiin tekemään. Mandiant arvioi, että liiketoiminnan tuhoamiseen tähtäävät hyökkäykset ovat kasvussa. Tämä johtuu siitä, että hyökkäyksellä saadaan korkea vaikutus alhaisella kustannuksella. Tuhoamiseen tähtäävää ”kyberkyvykkyyttä” kutsutaan asymmetriseksi, koska se voi aiheuttaa hyvin merkittävää ja suhteetonta tuhoa ilman, että hyökkääjillä tarvitsee olla suuria resurssimääriä tai teknistä edistyksellisyyttä.

Mandiant on myös tutkimuksissaan havainnut, että henkilötietojen varastamiseen tähtäävät hyökkäykset lisääntyivät erityisesti vuoden 2015 aikana. Tutkituissa tapauksissa näytti siltä, että varastettu tietomäärä oli niin suuri, että tavoitteena oli kerätä mahdollisimman paljon henkilötietoja eikä niinkään saada käsiin yksittäisten ihmisten tietoja. Mandiantin tutkimusten mukaan nämä toimijat voidaan jäljittää Kiinaan. Hyökkäykset kohdentuivat usealle eri toimialalle: terveystoimialaan, matkustamiseen, rahoitusalaan sekä julkishallintoon. Hyökkääjät tähtäsivät erityisesti sellaiseen tietoon, jota he voisivat käyttää todentaakseen henkilöllisyyden, esimerkiksi sosiaaliturvavakuutustietoihin, syntymäpäiviin, työnantajahistoriatietoihin ja kysymys/vastaus -tietoihin.

## 2.2 Merkittävimmät kyberuhat

Uhkien kategorisointi perustuu tutkimusdatan perusteella tehtyyn analyysiin. Jotkut kyberuhkat esiintyvät kuitenkin myös muiden uhkien kanssa. Esimerkiksi, kohdistetut hyökkäykset sekä APT-hyökkäykset (Advanced Persistent Threat) ovat haasteellisia kategorisoida sopimaan vain yhteen uhka-alueeseen, koska niissä käytetään useita hyökkäysmetodeja. Toisaalta, palvelunestohyökkäykset sekä hajautetut palvelunestohyökkäykset on tässä tutkimuksessa sijoitettu pilvipalveluiden alle; ne voisivat olla aivan yhtä hyvin erillään tai osana kohdistettuja hyökkäyksiä.

### 2.2.1 Älypuhelimet ja esineiden Internet

Älypuhelimet sekä esineiden internet ovat houkutteleva kohde kyberrikollisille. Älypuhelimiin sekä esineiden internetiin syntyy yhä kehittyneempiä haittaohjelmia, jotka voivat varastaa arvokasta henkilökohtaista tietoa, kiristää rahaa uhreilta sekä olla osana laajoja palvelunestohyökkäyksiä. Symantecin arvioiden mukaan älypuhelinten haavoittuvuuksien määrä on kasvanut joka vuosi viimeisten kolmen vuoden aikana. Saatamme pian nähdä kännyköihin suunnattujen PC-tyyppisten hyökkäystyökalujen kasvun mustilla markkinoilla.

AT&T puolestaan raportoi, että haavoittuvuuksien etsimiseen tähtäävät skannaukset[2] päätelaitteissa ovat kasvaneet 458% edellisistä vuosista. Dell arvioi raportissaan seuraavien neljän trendin voimistuvan vuoden 2016 aikana. Ensimmäisenä trendinä Dell mainitsee HTTPS-kryptauksen ja uhkien skannauksen välisen taistelun jatkuvan; yritykset eivät halua joutua tinkimään suorituskyvystä. Toisena trendinä Dell mainitsee Flash-plugineissa olevien ns. nollapäivävirusten vähenemisen. Tämä johtuu siitä, että suuret yritykset kuten Mozilla ja Google eivät enää tue Flash-plugineja. Kolmantena, ennustetaan, että NFC-tunnistuksen kautta tulevat haittaohjelmahyökkäykset uhkaavat Android Pay -sovellusta. Hyökkäykset voivat hyödyntää Android-sovelluksissa olevia haittaohjelmia sekä maksupäätejärjestelmä. Neljäntenä arvellaan, että Android Auto -sovellus tulee yleistymään uusissa autoissa. Tämä saattaa johtaa tiettyjen autojen hallintaan liittyvien etähallintana toteutettujen kiristyshaitta-hyökkäysten kasvuun. Näin voitaisiin estää esimerkiksi autosta ulospääsy. Google tekee kuitenkin jatkuvasti parannuksia ja kehitystyötä Androidin turvallisuuden parantamiseksi. Tietoturvaan liittyvää parannus- ja kehitystyötä tehdään sekä päätelaitteeseen että pilvipalveluihin.

Internetiin liittyneiden laitteiden määrä on kasvanut nopeasti. Gartnerin ennusteiden mukaan vuonna 2016 internetiin on liitetty 6,4 miljardia laitetta, vuoteen 2015 verrattuna 30% enemmän. Vuonna 2020 laitteita olisi jo noin 20,8 miljardia. Vuonna 2016 5,5 miljoonaa laitetta liitetään internetiin joka päivä. Vuonna 2015 tapahtui useita IoT-hyökkäyksiä, joissa löydettiin vakavia haavoittuvuuksia autoista, sairaanhoitolaitteista, digitaalisista videonauhureista sekä CCTV-kameroista. Vuonna 2016 tapahtui kaksi suurta IoT-hyökkäystä; syyskuussa KrebsOnSecurity.com blogiin sekä lokakuussa internet-yritys Dyniin – molemmat todettiin aiheutuneen Mirai-haittaohjelmasta. Syyskuun hyökkäys oli ennätyssuuri, 620 Gbps. Mirai hakee internetistä suojaamattomia IoT-laitteita. Näissä laitteissa on oletuskäyttäjänimet sekä salasanat. Tämän jälkeen haittaohjelma valjastaa laitteet palvelunestohyökkäyksiin. Tyypillisten haittaohjelmien lisäksi kyberkriminaalit ovat alkaneet käyttää tietojenkalasteluohjelmia, joiden avulla saadaan esimerkiksi käyttäjien pankkitunnukset haltuun. Lisäksi kiristyshaittaohjelmia, jotka salaavat kännyköiden tiedostot, esiintyy paljon. Käyttäjä on asentanut uuden sovelluksen älypuhelimeen ja tämän jälkeen laite on mennyt lukkoon ja näyttöön on ilmestynyt FBI-varoitus.

### 2.2.2 Web

Verizon määrittelee raportissaan web-hyökkäyksen sellaiseksi häiriötilanteeksi, jossa web-sovellus on ollut hyökkäysvektorina.[3] Määritelmä käsittää myös kooditason haavoittuvuuksien hyödyntämisen sovelluksessa sekä todentamismekanismien murtamisen. Web-palveluiden omistajat eivät yhä tänä päivänä päivitä palvelimiaan eivätkä web-sivustojaan tarpeeksi usein. Tämä vertautuu siihen, että jättää ikkunan auki rikollisille, jotka voivat päästä sisään ja käyttää hyväkseen mitä tahansa saatavilla olevaa tietoa. Symantecin arvion mukaan viimeis-

[2] engl. vulnerability scanning

[3] attack vector. Termille ei ole vielä vakiintunutta suomennosta.

ten kolmen vuoden aikana enemmän kuin kolme neljästä skannatusta web-palvelusta sisälsi päivittämättömiä haavoittuvuuksia, joista 15% oli luokiteltu kriittisiksi vuonna 2015. Web-hyökkäysten määrä on tuplaantunut vuonna 2015. Eräs syy on se, että hyökkäysvälineitä on laajalti saatavissa ja hyökkäykset on helppo toteuttaa. Jos web-palvelimet on jätetty haavoittuvaisiksi, ovat myös web-sivustot haavoittuvaisia sekä niitä käyttävät vierailijat. Verizonin mukaan käyttäjät voivat kuitenkin tietyillä toimenpiteillä pienentää web-hyökkäyksistä aiheutuvia riskejä. Ensinnä, käyttäjien pitäisi välttää yksittäiseen tekijään, salasanaan perustuvaa tunnistamista erityisesti kriittisissä järjestelmissä. Toiseksi, web-sovelluksen turvaamisessa ei kannata myöskään luottaa siihen, että käyttäjät eivät joutuisi näppäilyvakoilun uhriksi. Kolmanneksi, kaikkien käyttäjäsyötteiden validointi pitäisi tehdä kaikessa mahdollisessa käyttäjien tuottamissa kentissä, esimerkiksi että kuva on todella kuva eikä web shell tai että käyttäjät eivät pääse antamaan miltään kentiltä komentoja tietokannoille. Neljäntenä, kaikkiin lisäosiin, varsinkin kolmansien osapuolien tuottamiin lisäosiin, pitäisi suhtautua varauksella. Lopuksi, CMS-järjestelmälle (sisällönhallintajärjestelmä) sekä lisäosille pitäisi olla säännöllinen päivitysprosessi. Web-palvelimien haavoittuvuuksia aiheuttavat käyttöjärjestelmien lisäksi sisällönhallintajärjestelmät. Vaikka tietoturvaa on parannettu viime vuosina ja automaattisia päivityksiä otettu käyttöön, lisäosien (plugins) tietoturva on edelleen suuri ongelma. Symantec mainitsee esimerkkinä Wordpress-palvelun lisäosat, joita käytännössä kuka tahansa voi tehdä ja jotka saattavat olla hyvin turvattomia. Sekä Windowsin että Wordpressin lisäosat ovat suosittuja haittaohjelmakohteita, koska käyttäjämäärä on suuri. Symantec ehdottaa kolmea tapaa pienentää lisäosien haittaohjelmahyökkäyksiä. Ensinnä, lisäosia pitäisi päivittää säännöllisesti, koska lisäosat ovat äärimmäisen herkkiä haavoittuvuuksille. Toiseksi, tiedotusvälineitä sekä tietoturvalistoja pitäisi jatkuvasti ja tarkasti seurata haavoittuvuusvaroitusten huomaamiseksi. Kolmantena, ainoastaan tarpeellisia lisäosia pitäisi asentaa. Vuonna 2015 todettiin useita uusia tapauksia haittaohjelman sisältävistä mainoksista. Tämä vaikutti lähes kaikkialla internetissä, jossa on mainoksia. Mainokset ovat helpompi tapa saastuttaa sivuston kävijät kuin saastuneiden linkkien tuominen web-sivustoille. Rikollisten on helppo saada haltuunsa suosittu web-sivusto tai asentaa haittaohjelmamainoksia suosituille sivustoille, joissa kävijämäärä on korkea. Näin rikollisten ei tarvitse tehdä työlästä käyttäjän manipulointiprosessia (social engineering). Haasteena on se, että mainostoimistot pyytävät vain vähän tietoja mainostajilta. Näin rikollisten on helppo tekeytyä laillisiksi yrityksiksi ja ladata haittaohjelmamainoksia sivustoille. Haittaohjelmamainoksia sisältävät sivustot ovat yhä yleisempiä. Evästeiden avulla rikolliset voivat räätälöidä koodin siten, että kohteena voi olla melkein mikä tahansa käyttäjäryhmä profiloituna esimerkiksi maantieteellisen sijainnin, kellonajan, yrityksen, mielenkiinnon tai viimeaikaisen selainkäyttäytymisen mukaan.

Rikollisille on syntynyt mainostoimistojen löysäkätisyyden vuoksi uusi liiketoiminta-alue: malvertising-as-a-service.[4] Koska mainokset ilmestyvät web-sivustolle vain hetkeksi, tekee tämä haittaohjelman jäljittämisen vaikeammaksi. Profiloidessaan asiakaskuntaa mainostoimistot antavat tietämättään hyökkääjille runsaasti arvokasta tietoa esimerkiksi selaintyypeistä, kielestä yms. Yhtenä ratkaisuna on pidetty ad-blockereiden käyttöä. Haasteena on kuitenkin se, että jotkut yritykset kieltävät ad-blockereiden käyttämisen.

### 2.2.3 Sosiaalinen media

Sosiaalinen media on arvokas tietolähde kyberkriminaaleille. Ihmiset jakavat hyvin paljon tietoa sosiaalisessa mediassa itsestään, perheistään, työstään, ystävistään, sukulaisistaan, harrastuksistaan sekä lomamatkoistaan. Sosiaalinen manipulointi edellyttää hyökkääjältä taustatutkimusta sekä huolellista tutustumista kohteeseen. Lähteinä ovat sosiaalisen median profiilit, kaikenlainen uhrin online-aktiviteetti, jonka avulla saadaan selville työ, työkaverit sekä

[4] malvertising-as-a-service –käsitteellä ei ole vakiintunutta suomennosta. Palveluna tarjottava mainoshaittaohjelma

yrityksen organisatorinen rakenne. Hyökkääjät tuntevat erittäin hyvin yrityksen, kollegat, yrityksen johtohenkilöt sekä avainprosessit.

Social engineering (käyttäjän manipulointi) on kyberkriminaalien käyttämä metodi, jonka avulla saadaan joku tekemään jotakin sellaista, mitä hän ei normaalisti tekisi. Social engineering hyödyntää sähköpostikommunikointia, hienovaraista tietojen utelua keskustelun lomassa sekä haittaohjelma-ansoja. Tietojenkalasteluhyökkäys on kaikkein yleisin manipuloinnin tapa. Tietojenkalasteluhyökkäyksessä uhri saa sähköpostin, jossa on haittaohjelman sisältävä liitetiedosto linkkinä. Tarkoitus on saada uhri aukaisemaan liitetiedosto tai linkki. Symantecin mukaan tietojenkalasteluhyökkäyksistä on tullut helppo tapa hyökätä, koska kyberkriminaalien käyttämien työkalujen markkinat ovat kehittyneet. Kriminaalit tekevät myös yhteistyötä toistensa kanssa: toiset kehittelevät hyökkäykseen tarvittavia työkaluja, toiset puolestaan myyvät näitä työkaluja niille rikollisille, jotka haluavat toteuttaa hyökkäyksen. Tällä hetkellä trendinä on hyökätä tiettyihin organisaatioyksiköihin: jotkut hyökkäyksistä ovat hyvin hienovaraisia ja erittäin vaikea huomata huijauksiksi. Yritykset ovat menettäneet miljoonia dollareita, koska työntekijät huijattiin uskomaan tekaistut rahansiirtopyynnöt. Tietojenkalasteluhyökkäykset pyrkivät hyödyntämään nykyisiä liiketoimintakontakteja sekä pääsemään yrityksen tietoihin käsiksi ja rakentamaan luottamusta. Tietojenkalasteluhyökkäyksiä käyttävät järjestäytyneet rikollisryhmät sekä valtioihin läheisissä kytköksissä olevat toimijat.

### 2.2.4 Kohdistetut hyökkäykset

Trend Micron[5] mukaan kohdistetuissa hyökkäyksissä hyökkääjä hyödyntää aktiivisesti löydettyjä kohdeorganisaation palvelujen haavoittuvuuksia ja heikkouksia. Kohdistetut hyökkäykset ovat yleensä ammattimaisesti toteutettuja ja niihin on yleensä varattu osaavat ja hyvät resurssit. Hyökkäykset kohdistetaan kansallisiin salaisuuksiin, aineettomiin pääomiin sekä henkilötietoihin. Hyökkäykset saatetaan toteuttaa pitkän aikavälin kuluessa. Hyökkäyksiä voidaan muuntaa, sovitella sekä kehittää, jotta voidaan hyödyntää kohdeorganisaation heikkouksia mahdollisimman hyvin. Kohdistetut hyökkäykset toteutetaan usein kampanjoina, jolloin ne koostuvat sarjasta epäonnistuneita ja onnistuneita yrityksiä päästä syvemmälle ja syvemmälle kohdeorganisaation verkkoon. Yleensä ne kohdistuvat tiettyihin toimialoihin ja hyökkääjillä on pitkän tähtäimen päämäärä mielessä. Kohdistetuissa hyökkäyksissä hyödynnetään useita erilaisia tekniikoita, esimerkiksi drive-by lataukset, Microsoft SQL injektio, haittaohjelmat, vakoiluohjelmat, tietojenkalastelu sekä roskapostit. On esitetty, että jatkuvien kohdistettujen hyökkäysten takana on usein jokin valtiollinen toimija tai valtion kanssa hyvin läheisesti toimiva rikollisryhmä. Kohdistetuissa hyökkäyksissä hyödynnetään usein ns. nollapäivähaavoittuvuuksia ja nk. watering hole -hyökkäyksiä. Ne ovat hakkereille erityisen arvokkaita. Hakkerit pitävät yleensä hyvin salassa löytämänsä nollapäivähaavoittuvuudet, jotta niitä voisi hyödyntää mahdollisimman pitkään. Watering Hole -hyökkäykset tehdään yleensä saastuneilla websivustoilla; ne aktivoituvat vasta kun vierailija tulee tietystä IP-osoitteesta. Tämä piilottaa hyökkäyksen hyvin. Jopa tietoturvatutkijoilla on haasteellista löytää watering hole -haittaohjelma, koska he tulevat web-sivulle eri IP-osoitteesta. Kun tällainen hyökkäys löydetään, siirtyvät hyökkääjät toiselle sivustolle käyttäen taas jotakin muuta löydettyä nollapäivähaavoittuvuutta.

### 2.2.5 Tietovuodot ja yksityisyyden suoja

Viimeisten vuosien kuluessa on uutisoitu isoista tietovuodoista, joiden seurauksena miljoonia henkilötietoja on joutunut vääriin käsiin. Operaatiot ovat olleet hyvin kohdennettuja ja hyök-

[5] http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks

kääjä on saattanut tutkia useiden kuukausien aikana yrityksen sisäverkkoa ja siellä sijaitsevia tietoja ennen kuin vuoto on havaittu. Monet näistä suurista tietovuotohyökkäyksistä on pystytty kohdentamaan Kiinaan. Tutkimuksissa on pohdittu, kuinka Kiinasta lähtöisin olevat hyökkääjät käyttäisivät varastamiansa henkilötietoja. Vielä ei tutkimusten mukaan ole löytynyt viitteitä siitä, miten hyökkääjät olisivat pystyneet hyödyntämään varastamiansa suuria henkilötietomääriä. Mandiant arvelee Kiinasta lähtöisin olevien toimijoiden motiivien olevan mm. seuraavia: (1) identiteetin verifioinnin sekä pääsynhallinnan ohittaminen, (2) perinteisen vakoilun tukeminen, sisäpiiriläisten ja asiantuntijoiden identifiointi sekä rekrytointi, (3) operaatioiden kohdistaminen tiettyihin kansanosiin. Kiinalaiset hyökkääjät saattavat olla kiinnostuneita vähemmistöistä, toisinajattelijoista, ulkomaisista toimittajista, järjestöjen työntekijöistä sekä muista henkilöistä, joiden saatetaan olevan uhka Kiinan kommunistisen puolueen mielikuvalle ja asemalle.

### 2.2.6 Pilvipalvelut

Pilvipalvelu-termi kattaa laajan kirjon erilaisia teknisiä ratkaisuja ja ympäristöjä mukaan lukien sovelluspalvelut (software as a service, SaaS), sovellusalustat palveluna (platform as a service, PaaS) sekä infrastruktuurit palveluna (infrastructure as a service, IaaS). Yritykset ovat viime aikoina olleet kiinnostuneita erityisesti infrastruktuurista palveluna. Yritykset siirtävät pilveen yhä enemmän dataa sekä palveluja. Pilvipalvelut helpottavat yritysten yhteydenpitoa toisiinsa sekä asiakkaisiin; voidaan olla yhteydessä mistä vain ja milloin vain. Pilvipalvelut tarjoavat myös uudenlaisia konferenssi- ja muita yhteydenpitopalveluita. Lisäksi pilvipalvelut tarjoavat edullista tietojensäilytyskapasiteettia. Yritykset käyttävät tällaista kapasiteettia yhä enemmän; pilvipalveluissa sijaitsee hyvin paljon yrityksen liiketoiminnan kannalta kriittistä dataa: taloudellista tietoa, innovaatioihin liittyvää tietoa, asiakkuuksiin liittyvää tietoa, yritysoperaatioihin liittyviä tietoja, henkilöstön luottamuksellisia tietoja yms. Siksi myös sekä tietoturvatutkijat että kyberkriminaalit ovat alkaneet yhä enemmän kiinnostua pilvipalveluista. Pilvipalvelut ovat myös tavallaan uusi palvelukerros, joka puolestaan kasvattaa hyökkäysalaa.[6] Pilvipalveluissa esiintyy tavallisia haavoittuvuuksia, esimerkiksi SQL-injektiovirheitä, mutta myös muunlaisia haasteita. Virheelliset konfiguroinnit sekä heikko käyttäjien hallinta asettivat pilvipalvelut alttiiksi luvattomalle käytölle. Pilvipalveluihin sekä yritysten ja organisaatioiden infrastruktuuriin kohdistui monenlaisia hyökkäyksiä. Esimerkiksi palvelunestohyökkäysten ja bottiverkkohyökkäysten tarkoituksena on ollut saada palvelu kokonaan pois verkkokäytöstä. Hajautetut palvelunestohyökkäykset[7] ovat viime vuosien aikana kasvaneet lukumäärältään ja intensiteetiltään. Monet niistä kestävät 30 minuuttia tai vähemmän. Kasvun syynä on mm. se, että vuokrattavia bottiverkkoja on hyvin saatavilla. Myös esineiden intenet tuo lisää mahdollisuuksia bottiarmeijoiden hyödyntämiseen hyökkäyksissä. On ennustettu, että rikolliset käyttävät haavoittuvuuksia sisältäviä internetlaitteita yhä enemmän tulevina vuosina suurimittaisiin palvelunestohyökkäyksiin. Vaikka palvelunestohyökkäysten tunnistamiseen ja estämiseen on olemassa ratkaisuja, yrityksille on tulossa haasteita esineiden internetlaitteiden turvallisuuden kanssa. Jos tietoturva ei ole kunnossa, on vaikea tietää, onko tulostin, jääkaappi, lämmönsäädin tai leivänpaahdin osa globaalia bottiverkkoarmeijaa. Hajautettujen palvelunestohyökkäysten tarkoituksena on tuhota kohdeorganisaation tärkeimmät liiketoimintaprosessit sekä organisaation näkyvyys ja saatavuus verkossa. Viime vuosina hyökkäyksistä on tullut yhä vaarallisempia. Samaan aikaan hyökkäyksen toteuttamisen kustannukset ovat alentuneet. Kasperskyn tutkimusten mukaan 50% tutkimuksen organisaatioista oli kokenut jonkinlaista tuhoa osana palvelunestohyökkäystä vuonna 2015. Usein palvelunestohyökkäykseen on liitetty myös tietovuotohyökkäys, jotta hyökkäyksen teho saadaan maksimoitua. Vuonna 2015 45%:ssa palvelunestohyökkäyksistä mukana oli haittaohjelma, 32%:ssa mukana oli

[6] engl. attack surface. Ei vielä vakiintunutta suomennosta.

[7] Distributed denial-of-service (DDoS)

verkkoon tunkeutuminen sekä hakkerointi ja 26%:ssa tietovuoto. Pilvipalvelut eivät välttämättä ole vähemmän turvallisia kuin muut IT-palvelut. Palveluiden hallinnoijien on hyvä tarkistaa, että pilvipalvelut on konfiguroitu oikein ja että kaikki data on suojattu. Erityisesti on myös huomioitava pääsynhallinta pilvipalveluihin; suositeltavaa olisi käyttää kaksiosaista todentamismenetelmää. Symantec suosittaa myös seuraavia toimenpiteitä:

- Uhkatietoisuuden lisääminen,
- Säännöllinen sekä nopea muutostiedostojen ja päivitysten asentaminen,
- Valmiiksi integroitujen tietoturvapalveluiden hyödyntäminen (mukaan lukien antivirusohjelmistot),
- Vahvan palomuurin käyttäminen (päästää läpi ainoastaan tunnetun liikenteen),
- Lokien säännöllinen läpikäyminen epäilyttävän verkkoliikenteen tunnistamiseksi,
- Monikerroksinen suojaus (jos yksi kerros pettää, muut kerrokset suojaavat verkon eri osia),
- Hyvien tietoturvapolitiikoiden käyttöönotto ja henkilöstön säännöllinen koulutus,
- Pääsynhallinnassa ”vähiten oikeuksia”[8] -periaatteen noudattaminen,
- Hyökkäyksenesto- ja tunnistusjärjestelmien käyttöönotto,
- Varmuuskopioiden taltiointi toimitilojen ulkopuolella,
- Kaikkien pilvipalveluiden hallinnoimiseen tarkoitettujen käyttäjätunnusten huolellinen tallessapito ja varmistus (pääsy ainoastaan tarve-tietää[9] -periaatteella),
- Pilvipalveluiden resurssien asetusten ymmärtäminen sekä huolellinen ja ymmärrettävä konfigurointi,
- Tapahtumien lokikirjoituksen päällä pito, jotta nähdään kuka käyttää järjestelmien tietoja,
- Pilvipalveluiden tarjoajan palvelutasosopimukset ja niiden suojausmenetelmien ymmärtäminen,
- Pilvipalveluiden IP-osoitteiden säilyttäminen haavoittuvuuksien hallintaprosesseissa ja kaikkien pilvipalveluiden auditointi.

### 2.2.7 Kyberhyökkäysten top-5 toimialat

IBM Security on tutkimuksessaan selvittänyt, mitkä toimialat joutuivat eniten kyberhyökkäysten kohteeksi vuonna 2015 ja miksi. Raportin mukaan ne ovat: terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne ja kuljetustoimialat. Viisi kahdeksasta suurimmasta vuoden 2010 jälkeen terveystoimialaan kohdistuneesta hyökkäyksestä tapahtui vuoden 2015 ensimmäisten kuuden kuukauden aikana. Raportin mukaan yli 100 miljoonaa potilastietoa varastettiin vuonna 2015. Rikolliset ovat kiinnostuneita potilastiedoista, koska niistä maksetaan pimeillä markkinoilla hyvin; tyypillinen potilastieto sisältää luottokorttinumeroita, sähköpostiosoitteita, sairasvakuutusnumeroita, työnantajatietoja sekä sairaushistoriatietoja. Näillä on rikollisille arvoa, koska ne yleensä ovat voimassa vuosia. Kyberrikolliset käyttävät tietoja tietojenkalasteluhyökkäyksissä, petoksissa sekä identiteettivarkauksissa.

Valmistus- ja tuotantotoimialaan luetaan autonvalmistus, elektroniikan, tekstiilin sekä farmasian alueiden valmistus ja tuotanto. Hyökkäysten määrä kasvoi tässä toimialassa selvästi ja oli vuonna 2015 toiseksi suurin hyökkäysten kohteeksi joutunut toimiala. Autonvalmistukseen kohdistettiin eniten hyökkäyksiä – osuus kaikista hyökkäyksistä oli noin 30% vuonna 2015. Tämän arvellaan johtuvan siitä, että hyökkääjät pystyivät etähyökkäämään verkossa olevaan autoon.

[8] engl. least privilege. Pääsy ainoastaan siihen tietoon, joka on työn tekemisen kannata ehdottoman välttämätöntä. https://en.wikipedia.org/wiki/Principle_of_least_privilege

[9] engl. need-to-know basis

Pankki- ja rahoitustoimialaan kohdistuvat hyökkäykset puolestaan vähenivät vuonna 2015 johtaen siihen, että rahoitustoimiala siirtyi vuonna 2015 toimialalistalla kolmanneksi vuoden 2014 ensimmäisen sijan jälkeen. On myös arveltu, että toimialalla on parannettu huomattavasti kyberturvallisuutta, mikä on osaltaan vaikuttanut hyökkäysten vähentymiseen. On kuitenkin huomattava, että pankkien tarjoamat uudet palvelut, kuten luottokortit, pankkiautomaatit sekä mobiilimaksaminen, ovat tuoneet uudenlaisia mahdollisuuksia myös rikollisille toteuttaa kyberhyökkäyksiä. Monet asiakkaat joutuivatkin mm. Dyren sekä Dridex Troijalaisen uhriksi.

Julkishallinto siirtyi listalla neljänneksi vuonna 2015. Julkisuuteen tuli suuria tietovuotoja, kuten USA:ssa tapahtunut miljoonien työntekijätietojen vuotaminen, jossa oli sosiaaliturvatunnuksia, syntymäpaikkoja sekä digitaalisia sormenjälkiä. Myös Turkissa tuli julkisuuteen vuonna 2015 tietovuoto, jossa miljoonien kansalaisten henkilötiedot varastettiin ja se puolestaan mahdollisti identiteettivarkaudet. Japanissa varastettiin henkilötietoja, kun työntekijät kansaneläketoimistossa huijattiin avaamaan haittaohjelman sisältämä linkki.

Liikenne- ja kuljetustoimiala oli viidenneksi eniten hyökkäysten kohteeksi joutunut toimiala vuonna 2015. Tämä toimiala sisältää mm. lentokoneet, linja-autot, maanalaiset, junat, raitiovaunut sekä laivat. Tämä toimiala on koko maailmankaupan ydin, koska ilman sitä maailmankauppa halvaantuisi. Raportin mukaan poliittisesti motivoituneet kyberrikolliset yrittävät jatkuvasti halvaannuttaa maailmankaupan runkona toimivaa toimialaa, jotta syntyisi massiivinen kaaos. Toisena hyökkäysmotiivina oli edelleen raha ja tämä johti mm. haittaohjelmahyökkäyksiin sekä palvelunestohyökkäyksiin.

## 2.3 Kyberuhkien aiheuttajat

### 2.3.1 Sisäpiiriläiset

Kriminaalien, hakkereiden, kybervakoojien, haktivistien, kybersotilaiden sekä kyberterroristien lisäksi kyberuhkan aiheuttajana voi olla organisaation sisäpiiri. On huomattava, että sisäpiiriin kuuluu ENISA:n määrityksen mukaan laaja joukko toimijoita. Sisäpiiriläisiä voivat olla nykyiset sekä entiset työntekijät, nykyiset sekä entiset palveluntarjoajat, sopimuskumppanit sekä konsultit, nykyiset sekä entiset toimittajakumppanit sekä liiketoimintakumppanit ja asiakkaat. On tunnistettava, kenellä näistä ryhmistä on luottamuksellisia käyttöoikeuksia. ENISA:n mukaan suurin osa väärinkäytöksistä voidaan jäljittää tähän ryhmään. Väärinkäytösten motiivina on myös tilanteen sopivuus ja mukavuus. Oikeuksia väärinkäyttämällä voidaan ohittaa laillisen prosessin rajoittavat tietoturvakontrollit. Muita motiiveja ovat rahastustarkoitus ja kosto. Kenen käyttäjätunnuksia on sitten eniten käytetty väärin? ENISA luettelee seuraavat käyttäjäryhmät: loppukäyttäjät, asiakkaat, kassa, rahoitus sekä johtohenkilöt. Järjestelmän pääkäyttäjät eivät olleet väärinkäytösten luettelon kärkipäässä.

### 2.3.2 Kybervandaalit: hakkerit, haktivistit, script kiddiet, yksinäiset sudet

Hakkeri on henkilö, joka tunkeutuu tietoverkkoon tai tietojärjestelmään tai käyttää luvatta tietoa, ohjelmaa tai palvelua.[10] Haktivistien päämääränä on puolestaan hakkeroida sekä levittää tietoa organisaatioista tai vallassa olevista ihmisistä häväistystarkoituksessa sekä tuoda julkisuuteen oletettuja väärinkäytöksiä. Haktivistit puoltavat sananvapautta sekä internetin avoimuutta. Haktivistit ovat myös protestoineet heidän tuomitsemistaan samoin perustein kuin terroristeja. Joissain tapauksissa haktivistit ovat hyökänneet terroristeja vastaan, esim.

[10] Tekniikan Sanastokeskus, http://www.tsk.fi/tepa/netmot.exe?UI=figr&height=161. Tarkistettu 13.1.2017.

ISISiä sulkemalla jihadistien verkkopalveluita ja paljastamalla 10 000 Twitter ja Facebook-tiliä, joita on käytetty terrorismikampanjointiin sekä rekrytointiin.

Script kiddies -nimitystä käytetään hakkereista, jotka etsivät ja lainaavat tietoja ja koodia internetistä ja tekevät niiden avulla hyökkäyksiä. Script kiddies -ryhmää motivoi pääasiassa hauskanpito. On ennustettu, että tämä ryhmä voi vielä tulevaisuudessa kasvaa ja aiheuttaa vielä enemmän tietoturvatapahtumia. Haasteena on myös se, että script kiddiesit voivat aiheuttaa odottamattomia lopputuloksia toiminnallaan. Erilaisten hakkerointikilpailujen avulla kyberturvallisuusyhteisöt yrittävät johtaa toiminnan positiiviseen suuntaan. Yksi kuuluisista viime vuosien script kiddies -tietomurrosta on ns. Talktalk-tietovuoto, jossa päätekijäksi osoittautuivat 16- ja 15-vuotiaat englantilaiset koulupojat.[11] Sosiaalisen median kanavia käyttävät hakkeroinnit ovat jatkaneet kasvuaan vuonna 2015. Tämä johtuu erityisesti siitä, että kohdennetut tietojenkalasteluhyökkäykset ovat kasvaneet. Sosiaalisen median kanavista saadaan merkittävästi tietoja tällaisille hyökkäystavoille. Lisäksi työkaluja on laajasti saatavissa hyökkäyksiin. Työkaluja käytetään edistyneisiin käyttäjän manipulointihyökkäyksiin.[12]

Yksinäiset sudet ovat henkilöitä, jotka valmistelevat sekä toteuttavat väkivaltaisia tekoja yksinään, ilman minkäänlaista komentorakennetta sekä ilman minkäänlaisten ryhmien apua. ENISA esittää myös tutkimuksessaan, että erityyppisiä kyberagentti-/-toimintaryhmiä perustettaisiin. Ryhmillä olisi aktiivinen rooli kyberhyökkäysten torjunnassa. Tämä ajatus perustuu siihen, että kyberturvallisuusyhteisöjen pitäisi pohtia kuinka vapaaehtoisia ryhmiä saataisiin osallistumaan kansallisiin kyberpuolustusaloitteisiin. Tällaiset ryhmät toimisivat aktiivisesti ja torjuisivat yhteiskuntaan kohdistuvia kyberriskejä.

### 2.3.3 Kybervakoilijat

AT&T mainitsee myös, että USA:n hallitus sanoo kybervakoilun olevan merkittävin ja yhä kasvava uhka valtion turvallisuudelle sekä menestykselle. Kybervakoiluryhmät ovat kiinnostuneet aineettomasta omaisuudesta, liikesalaisuuksista, kansallisista salaisuuksista, sotilaallisesta luottamuksellisesta tiedosta sekä valtioiden poliittisiin prosesseihin vaikuttamisesta.

Kybervakoilua tekevät sekä valtiot että yritykset. Kybervakoilu on jatkanut kasvuaan sekä muuttunut yhä monimuotoisemmaksi. Kybervakoilun takaa löytyy usein valtion tukema ryhmittymä. ENISA mainitsee muutamia tärkeimpiä julkisuuteen tulleita kybervakoilutapauksia: TV5 Monde, Sony, Bundestag-vuoto, Equation Groupin julkitulleet toimintatavat sekä OPM tietomurto. Sony ja TV5Monde -hyökkäyksillä oli tuhoava vaikutus, koska molemmissa tapauksissa kohteet eivät voineet toimia päiviin/viikkoihin kyberhyökkäyksen johdosta. Bundestag-tapaus osoittaa, että fyysisen maailman konflikteilla – tapahtumat Itä-Euroopassa - on myös vaikutus kybermaailmaan. Equation Groupin tapauksessa puolestaan hyökkäys osoitti voimansa myös kyber-fyysisiin alajärjestelmiin (esim. laitteisto). OPM-tietomurto (Office of Personnel Management) johti puolestaan biometristen sekä muiden henkilöiden yksityisten tietojen vuotamiseen. Tällainen tietomurto on korvaamaton, koska henkilöiden tiedot ovat ainutkertaisia.

Raja valtiollisen ja teollisen vakoilun välillä on häilyvä, erityisesti tapauksissa, joissa suuret monikansalliset toimijat ovat mukana, tai kampanjoissa, joissa kansallisten kykyjen lisäksi mukana on vihamielisiä aktivistiryhmiä, kilpailijoita sekä teollisuusvakoilua. Lisäksi valtion tukeman vakoilun (esimerkiksi APT-hyökkäyksissä) ja kohdistettujen kampanjoiden (targeted

[11] https://www.theguardian.com/business/2015/nov/06/nearly-a57000-had-data-breached-in-talktalk-cyber-attack

[12] Social engineering = käyttäjän manipulointi. Toiminta, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä. Tekniikan Sanastokeskus, http://www.tsk.fi/tsk/

attacks/advanced targeted attacks) raja on häilyvä. ENISA ilmoittaa omassa raportissaan lukevansa myös kohdistetut kampanjat osaksi valtion tukemaa vakoilua ymmärtäen kuitenkin, että kaikilla kohdistetuilla kampanjoilla ei välttämättä ole valtion tukemaa vakoilutaustaa. Kybervakoilu laajenee siis osittain kattamaan sellaisiakin aktiviteetteja, joita tässä raportissa on kuvattu muiden kyberuhkien aiheuttajien kohdalla.

Kybervakoojien käyttämä taito- ja keinovalikoima kehittyy jatkuvasti. Tämä näkyy puolestaan myös puolustusstrategioissa. Enenevässä määrin kehitys menee myös kohti kyber-fyysisiä järjestelmiä. Tämä taktiikka vähentää jäljitettävyyttä ja toisaalta lisää hyökkäyksistä toipumisen tarvetta.

### 2.3.4 Kyberterroristit ja -sotilaat

ENISA antaa raportissaan yhden esimerkin kyberterrorismista: ISIS. Kyberasiantuntijat sekä kansallisen turvallisuuden asiantuntijat keräävät ja analysoivat tällä hetkellä ISISin iskuvoimaa kybermaailmassa. ISIS käyttää modernia teknologiaa hyväkseen mm. viestinnässään sekä rekrytoinnissa. ISIS myös kehittää tätä aluetta jatkuvasti. ENISAn mukaan ISISin käyttäytyminen rinnastuu lähinnä online social hackers -ryhmän toimintaan. Lisäksi ISIS yrittää palkata hakkereita ylläpitämään heidän sosiaalisen verkostonsa infrastruktuuria eli hallinnoimaan sosiaalisen median kampanjoita. Kyberterroristit ovat myös kiinnostuneita anonyymeista maksujen siirroista kerätessään sekä jakaessaan rahaa. Kyberterroristit käyttävät myös hyödykseen palveluina saatavia kyberrikoksia. Asiantuntijoiden mukaan ISISillä ei tällä hetkellä uskota olevan merkittäviä kyberterroristikyvykkyyksiä.

Kybersotilaat ovat yleensä kansallisesti motivoituneita ja ryhmittymät voivat toiminnassaan siirtyä kyberterroristien, aktivistien sekä kybervakoilun välimaastoon. Esimerkkinä tästä on Syrian Electronic Army. Tämän ryhmän avainhenkilöillä on tai on ollut läheiset suhteet Syyrian hallitukseen. Muita esimerkkejä tällaisista ryhmittymistä ovat Yemen Cyber Army ja Iranian Cyber Army. Terroristihyökkäys Pariisissa Charlie Hebdo -lehden toimitukseen on myös esimerkki kyberterroristien sekä kybersotilaiden välimaastossa toimivasta ryhmästä.

## 2.4 Vuoteen 2020 ennustettuja uhkia

Aiemmin McAfee on ennustanut, että kyberturvallisuutta eniten muokkaavat voimat ovat: yhä laajeneva kyberhyökkäysala, hakkeroinnin teollistuminen, IT tietoturvamarkkinoiden monimutkaisuus sekä hajautuneisuus. McAfee ennustaa, että tulevaisuudessa nähdään yhä laajeneva kyberhyökkäysala, hyökkääjien kehittyneisyyden lisääntyminen, tietovuotojen kustannusten kasvu, yhteensopivien tietoturvateknologioiden puute sekä taitavien tietoturvaammattilaisten puute. AT&T puolestaan mainitsee neljä suurta aluetta, joissa se arvelee tulevina vuosina syntyvän uusia, vaarallisia mahdollisuuksia kyberhyökkääjille:

1. Esineiden internet,
2. Pilvipalvelut,
3. Big Data,
4. Mobiliteetti,
5. BYOD -filosofia (Bring Your Own Device)

Koska verkkoon liitettävien esineiden määrä tulee suurenemaan valtavasti ja tämän lisäksi pienten sensoreiden turvaaminen tulee olemaan haasteellista, tulevat kyberhyökkääjät saamaan valtavasti uusia hyökkäysmahdollisuuksia esineiden internetin kasvun myötä. Pilvipalveluiden lisääntyminen tulee tarkoittamaan myös uusia mahdollisuuksia kyberhyökkääjille.

Pilvipalvelut ovat usein kolmansien osapuolien toimittamia. Kaikkien linkkien pilvipalveluun sekä pilvisovelluksiin pitäisi käyttää turvallisia sekä valvottuja verkkoyhteyksiä.

McAfee mainitsee virtualisoinnissa uudentyyppisen kehityksen; virtualisointi siirtyy data center -tyyppisestä toiminnasta kohti verkottumista. Tätä kehittyvää teknologiaa kutsutaan Network Function Virtualizationiksi (NFV). Se tulee vaikuttamaan telealalla hyvin paljon tulevina vuosina. Vaikka Virtual Networking on esiintynyt pilvipalveluissa jo jonkun aikaa, uutta on se, että se tulee jatkossa liittämään käyttäjät sekä päätelaitteet pilvipalveluihin. McAfee mainitsee myös containers-käsitteen sekä ”containerization” -käsitteen, joka tulee toteuttamaan virtualisointia nopeammin, tehokkaammin ja kevyemmin. Se korvaa perinteiset ”imaget” pilvipalveluissa. Kolmantena uutena teknologiana McAfee mainitsee ns. software-defined networks (SDN). SDN:ää käytetään yhdessä NFV:n kanssa ja McAfeen mukaan yhdessä nämä teknologiat tulevat luomaan mahdollisuuksia uusille uskomattomille lisäarvopalveluille ja -sovelluksille, jotka ovat on-demand, skaalautuvia sekä täysin automatisoituja. Em. teknologiat ovat avoimeen lähdekoodiin perustuvia uusia sovelluksia ja tulevat luomaan myös uudentyyppisiä riskejä ja uhkia sekä laajentamaan kyberhyökkäyspinta-alaa entisestään.

Big Data -sovelluksia käytetään suurissa yrityksissä jo paljon, mutta ennustetaan, että Big Data -alue tulee kasvamaan lähivuosina runsaasti. AT&T huomauttaa kuitenkin raportissaan, että Big Data -sovellusten turvaamiseen ei kuitenkaan ole rakennettu vielä kovinkaan tehokkaita turvaamisen sovelluksia, näin ollen nämä sovellukset ovat hyvin haavoittuvaisia esimerkiksi yrityksen sisäpiirin tahattomille tai tahallisille väärinkäytöksille. Neljänneksi mobiliteetista sekä uusista päätelaitteista haetaan tehokkaampia tapoja toimia. Lisäksi ihmiset haluavat tuoda omat päätelaitteensa töihin. Tämä synnyttää uusia tietoturva-aukkoja, joita kyberhyökkääjien on helppo hyödyntää.

Ennusteiden mukaan myös valtioiden kybersodankäynnin kyvykkyydet tulevat edelleen kehittymään sekä hyökkäysten laajuudessa että edistyksellisyydessä. Valtioiden tekemät kyberhyökkäykset tulevat vaikuttamaan poliittisiin suhteisiin sekä valtarakennelmiin ympäri maailmaa. Valtioiden käyttämät työkalut valuvat sitten jollakin aikavälillä myös kyberrikollisryhmien käyttöön. Näillä ryhmillä hyökkäyksen motiivina on pahan tekeminen, taloudellinen hyöty tai kaaoksen aiheuttaminen.

Kybertoimintaympäristössä tapahtuu myös positiivista kehitystä. Tietoturvayhtiöt sekä hallinnolliset organisaatiot ovat parantaneet yhteistyötään ja lukuisia yhteistoimintaa parantavia ja tehostavia toimintatapoja, prosesseja sekä järjestelmiä on luotu. Kyberrikosten  sekä kyberuhkien vähentäminen on siis hieman myös helpottunut. Haavoittuvuuksien sekä tietoturvan tutkimukseen panostetaan myös paljon. Suuret tietoturvayritykset panostavat tutkimukseen sekä kehitykseen. Markkinoille syntyy tehokkaita työvälineitä kyberhyökkäysten tunnistamiseen, suojaamiseen, sekä pysäyttämiseen.

## 2.5 Johtopäätökset

Kyberuhkien aiheuttajat kehittävät jatkuvasti uusia tapoja hyökätä organisaatioihin. Kyberrikoksista on tullut mustilla markkinoilla toimiva vahva ja elinvoimainen liiketoiminnan alue. Vaikka uudet palvelut tuovat mukanaan myös uudenlaisia kyberuhkia, organisaatiot eivät voi kääntyä pois verkkopalveluiden, mobiiliuden, Big Datan sekä pilvipalveluiden tuomista hyödyistä. Digitalisaatio on synnyttänyt työtä sekä elämää helpottavia uusia innovaatioita. On sen sijaan lähdettävä aivan uusilla tavoilla hakemaan IT:n, kyberturvan sekä liiketoiminnan liittoa. Kyberrikollisia vastaan toimiminen edellyttää myös uudenlaisia tapoja toimia yritysten ja organisaatioiden välillä. On aktiivisesti jaettava tietoa kyberuhkista, tapahtuneista hyökkä-

yksistä sekä uusista vaaroista. Kyberrikosten torjuminen vaatii avoimuutta, aktiivista viestintää ja opiskelua sekä toimijoiden verkostoitumista.

AT&T esittää raportissaan viittä eri strategista toimintatapaa kyberuhkien torjunnassa: kulttuuri, kyberturva osana liiketoimintaa, työkalut ja sovellukset, kumppanuudet sekä rahoitus. Kyberturvallisuuden pitää olla organisaatioissa kulttuurinen pilari. Kyberturvallisuutta edistetään, harjoitetaan sekä arvostetaan organisaation kaikissa osissa. Koulutuksen tulee olla riittävää, jotta tietoisuus kyberturvallisuuden uhkista tulee osaksi työntekijöiden kulttuuria. Liiketoiminnan tavoitteiden pitää olla linjattuna kyberturvallisuuden tavoitteiden kanssa; kyberturvallisuus on aina osana teknologia- sekä liiketoimintapäätöksissä. Riskien hallinta sekä määräystenmukaisuus ovat oleellinen osa myös päätöksentekoa. Mitä aikaisemmin kyberturvallisuus on osana yrityksen liiketoiminnan suunnittelua, sitä parempaan lopputulokseen päästään. Kolmanneksi, organisaatioilla pitää olla ajan tasalla olevat palvelut sekä ratkaisut kyberhyökkäysten torjunnassa sekä organisaatioiden keskeisten varojen suojaamisessa. Organisaatioiden olisi säännöllisesti myös auditoitava luotettavan kumppanin toimesta koko tietoturvaratkaisu (esim. testaushyökkäykset sekä toimintatapojen testaukset). Neljänneksi, on mietittävä huolellisesti sopivat kumppanit kyberturvallisuudessa; keiden kanssa kyberturvallisuutta voidaan kehittää parhaiten kokonaisuutena, strategisena kumppanuutena ja minkälaisia muita kumppaneita pitäisi olla. Viidenneksi, investoinnit sekä kyberturvallisuuteen että tietoturvallisuuteen tulee turvata. Investoinneissa on otettava huomioon riskit, käytettävät kyberturvallisuusratkaisut, käytettävissä olevat tietolähteet sekä turvattava data/informaatio.

# 3. SUOMEN KYBERTURVALLISUUDEN NYKYTILA JULKISELLA SEKTORILLA

## 3.1 Johdanto

Tässä luvussa käsitellään kansallisen julkisen sektorin näkemystä kyberturvallisuudesta. Osion on tarkoitus vastata kysymykseen: *Onko Kyberturvallisuusstrategian visiona esitetty tavoitetila saavutettu* sekä *onko kyberturvallisuutta onnistuttu kehittämään strategiassa esitettyjen linjausten mukaisesti?* Tämän luvun painopiste on arvioida Suomen kyberturvallisuuden nykytilaa suhteessa strategiassa kuvattuun visioon, toimintamalliin sekä strategisten tavoitteiden toteutumiseen.

Tarkastelussa keskitytään analysoimaan haastatteluaineistoja. Valtionhallinnosta identifioitiin eri hallinnonaloilta 12 keskeistä asiantuntijaa, jotka ovat omilla aloillaan tai yleisemmin mukana kyberturvallisuusstrategian suunnittelu- ja/tai toimeenpanotyössä mukana. Haastattelut tehtiin joulukuussa 2016 ja ne toteutettiin puolistrukturoituina teemahaastatteluina.

Tämä luku rakentuu haastatteluaineiston varaan siten, että aluksi arvioidaan kyberturvallisuusstrategiassa esitettyä visiota ja toimintamallia ja seuraavaksi käsitellään asiantuntijoiden näkemyksiä kyberturvallisuusstrategiassa esitettyyn kymmeneen strategiseen linjaukseen.

## 3.2 Kyberturvallisuusstrategian toteutuminen

Kyberturvallisuus ymmärretään strategiassa tavoitetilana, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvataan[13]. Strategiassa esitetään kolmen kohdan visio, jossa (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” sekä (3) ”vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.”[14]

Kyberturvallisuuden tilaa seurataan valtionhallinnon osalta jatkuvasti. Esimerkiksi valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI laatii vuosittain tietoturvakyselyn julkishallintoon. Sen tulokset ovat useana vuonna osoittaneet, että tieto- ja kyberturvallisuus kehittyy jatkuvasti mutta lisäkehitettävää löytyy aina. Suurimpana haasteena on kybertoimintaympäristön nopea kehitys ja kyberuhkien nopea evoluutiosykli suhteessa valtionhallinnon johtamis- ja päätöksentekoprosessien kestoon.

Tällä hetkellä kenttätasolla on hyvää osaamista ja esimerkiksi VIRT-toiminnan (Virtual Incident Response Team) avulla saadaan tietoa vaihdettua, mutta poikkihallinnollinen ja PPP-yhteistyön kattava johtamisrakenne ja malli puuttuvat.

Liikenne- ja viestintäministeriön ensimmäinen tietoturvastrategia julkaistiin vuonna 2003 ja sitä päivitettiin kertaalleen. Turvallisuus- ja puolustusasiain komitean (nyk. Turvallisuuskomitean) johdolla laadittiin vuosina 2011-2013 kyberturvallisuusstrategia (17. maa Euroopassa, joka tuotti kyberturvallisuusstrategian). Strategiassa on pyritty huomioimaan kaikkien näkö-

[13] Kyberturvallisuusstrategia 2013, s 1.

[14] ibid. s 3.

kulmat (kaikki hallinnonalat toivat oman panoksensa strategiatyöhön), mikä aiheutti jännitteitä jo valmisteluvaiheessa ja sen toteuttaminen jäi hallinnonalasiiloihin. Haastateltavien mukaan strategian suurin arvo on siinä, että se on olemassa ja sen visio on selkeä vaikkakin ylioptimistinen. Epäsopuisa prosessi vaikutti myös lopputulokseen; strategiaa kritisoitiin haastatteluissa liiasta yleisluontoisuudesta ja liiasta valtionhallintokeskeisyydestä. Elinkeinoelämä jäi liiaksi taustalle. Hallinnonalojen riitaisuus ja eri näkemykset ovat tehneet strategiasta liiallisen kompromissin. Tästä huolimatta haastatteluissa oltiin pääosin sitä mieltä, että lopputuloksen kompromissiluonteesta huolimatta sen linjausten mukaisesti on hallinnonaloilla eletty ja toimintaa kehitetty suhteellisen hyvin.

Yksi strategian onnistumisista on ollut Kyberturvallisuuskeskuksen perustaminen. Sille yhdistettiin Viestintäviraston moninaiset tietoturvatehtävät ja sääntelytoiminta, ml. tarkastus ja hyväksyntä. Rakennemallia otettiin vahvimmin Alankomaista, myös Tanskassa on samansuuntainen malli (ilman tarkastusta ja hyväksyntää). Keskuksella on sille säädetyt lakisääteiset tehtävät sekä EU- ja jossain määrin NATO-yhteistyö kuuluvat sen tehtäviin.

Kansallinen kyberturvallisuus on kehittynyt viimeisten parin vuoden aikana. Erityisesti harjoitustoiminta on parantanut tilannetta ja lisännyt tietoisuutta ja ymmärrystä kybermaailman uhkista. Erityisesti mainittiin Aluehallintoviranomaisten (AVI) harjoitustoiminnan tuloksellisuus.

Keskeisin puute on havainnointikyvyssä, tilannekuvassa ja tilanneymmärryksessä sekä laaja-alaisten hyökkäysten torjunnassa. Tällä hetkellä kyetään johtamaan ja hallitsemaan pieniä ja keskisuuria kyberhyökkäyksiä (palvelunestohyökkäys), mutta vakavien ja laaja-alaisten hyökkäysten torjuntakyky on heikko, johtuen em. havainnointikyvyn ja tilannekuvan puutteista ja selkeän kansallisen johtamismallin puutteesta.

Varautumista on hoidettu vaihtelevalla tavalla. Osa hallinnonaloista on ottanut kyberuhat vakavasti, osalla on vielä puutteita varautumisessa.

Suomen tilanne on kohtuullinen verrattuna keskeisiin edelläkävijöihin, kuten Israeliin ja Yhdysvaltoihin. Myös Norja, Ruotsi ja Alankomaat ovat Suomelle hyviä verrokkimaita. Lisäksi Australia, Kanada ja Iso-Britannia ovat maita, joiden kanssa yhteistyötä kannattaa tehdä. Kyberrikollisuuden torjunnassa keskeisiä verrokkimaita ovat Alankomaat ja Iso-Britannia ja myös Saksa.

## 3.3 Visio ja strategiset linjaukset

Asiantuntijahaastatteluiden lähtökohtana oli selvittää sitä, onko kyberturvallisuusstrategian visiona esitetty tavoitetila saavutettu. Aineiston perusteella tavoitteeseen ei kokonaisuudessaan ole päästy; kuitenkin enemmistön mielestä kehityssuunta on oikea. Visio nähdään saavutetuksi siinä mielessä, että näkökulma kyberturvallisuuteen yhteiskunnassa on oikeanlainen, mutta konkreettisten tulosten osalta on paljon tehtävää.

Kyberturvallisuusstrategian vision näkökulmasta Suomi ei ole edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa, mutta kuuluu kärkijoukkoon. Eri toimijoiden mittareilla mitattuna Suomi sijoittuu yleensä kärkikymmenikköön. Myöskään uhkien kannalta Suomi ei ole globaalissa tarkastelussa kyberhyökkäysten pääkohteita – vielä toistaiseksi.

Strategian visiota siitä, että Suomi olisi edelläkävijä kyberturvallisuudessa ei siis sellaisenaan ole saavutettu. Suomi ei ole kyberturvallisuuden huippumaa maailmassa, mutta hyvänä pidettävä asia on, että samalla vakavia puutteita ei myöskään mainittu. Toisaalta eräs haastatelta-

va painotti sitä, mikä tämän tavoitteen kohdalla usein unohdetaan: Suomi ei pyri olemaan kyberturvallisuuden huippumaa sinällään vaan edelläkävijä nimenomaan kyberuhkiin *varautumisessa* ja siinä kehityksessä monien haastateltavien mukaan Suomi on pitkällä. Suomella on pitkä perinne huoltovarmuudesta ja varautumiseen liittyvässä viranomaisyhteistyössä. Viranomaisyhteistyö mainittiin useassa haastattelussa vahvuudeksi. Yleisesti kyberturvallisuudesta oltiin sitä mieltä, että Suomessa ollaan eurooppalaisittain vahvaa keskitasoa. Toisaalta jotkut haastateltavat eivät osanneet arvioida kyberturvallisuuden kokonaistilaa yhteiskunnassa yleisesti, vaan painottivat vastauksissaan edustamaansa hallinnonalaa.

Kyberturvallisuusstrategia toimeenpano-ohjelmineen on vaikuttanut toimintaan kaikilla hallinnonaloilla. Se näyttäytyy esimerkiksi siinä, että kybertietoisuuden koetaan lisääntyneen strategian voimaantulon jälkeen. Haastatteluaineiston perusteella kyberturvallisuuselementti on nykyään integroituna hallinnonalojen jokapäiväiseen työhön. Se tarkoittaa sitä, että kyberturvallisuutta on onnistuttu kehittämään osana muuta työtä ja muuta toimintaa enemmän kuin ”erillisenä” ja itsellisenä kyberturvallisuustyönä. Eli tietoisuuden lisääntymisen kautta kyberelementti on mukana normaalissa kehitystyössä.

Valtionhallinnon varautumistyössä kyberturvallisuus on aiheena keskusteluissa sekä poikkihallinnollisesti että kunkin hallinnonalan sisällä. Hallinnonaloilla on yleensä kaksi päätehtävää kyberturvallisuuteen liittyen: (1) suojata omat järjestelmät ja (2) kyberturvallisuuselementin integroiminen hallinnonalan substanssiasioihin. Ministeriöt ohjaavat kyberturvallisuustyötä omilla toimialoillaan. Kybertietoisuuden lisääntymisestä huolimatta haasteena on, ettei tietoisuus välttämättä kanavoidu toiminnaksi; aiheen tärkeydestä ollaan tietoisia, mutta henkilöstö ei välttämättä tiedä, mitä sen eteen voi ja pitäisi tehdä. Virkatehtävissä keskitytään hallinnonalan substanssiasioihin ja kyberturvallisuus nähdään hallinnollisena asiana tai sen koetaan olevan ”ulkokehällä”. Tämä näkyy muun muassa siinä, että aihe nähdään edelleen vain teknisenä tietoturvallisuuskysymyksenä, jonka hoitaminen koetaan monesti kuuluvaksi vain ministeriöiden ICT-sektorille. Kyberturvallisuus nähdään käytännössä tällä tavoin erikoistuneena, kun taas haastatteluissa painotettiin, että se pitäisi nähdä laajemmin kansallisen turvallisuuden näkökulmaa painottaen. Meiltä puuttuu pitkän aikavälin poliittinen tahtotila ja johtamismalli, kuinka Suomea tulisi rakentaa kyberturvallisena digiyhteiskuntana. Tämän seurauksena hallinnonalat taas toimivat siiloissaan ja määrittelevät tavoitteensa ja toimintatapansa omista lähtökohdistaan. Edelleenkin on niitä, jotka eivät ota kyberturvallisuutta riittävän tosissaan tai eivät ymmärrä sen kokonaismerkitystä. Haastateltavat arvioivat, että syvällinen muutos saadaan aikaan vasta, kun maatamme vastaa kohdistuu laajamittainen kyberhyökkäys ”kybertsunami”. Nykyisen strategian vision selkeydestä huolimatta digitaalista yhteiskuntaa rakennetaan ottamatta riittävästi huomioon kyberturvallisuuden vaatimuksia.

Haasteina strategian vision toteutumiselle on kyberalan nopea evoluutiosykli ja vauhdikas kehittyminen. Virkamiesprosessina tuotetut strategiat ja ohjelmat vanhentuvat nopeasti suhteessa kybertoimintaympäristön kehitykseen. Strategian esittämä visio on edelleen ajankohtainen tavoite, mutta toimeenpanoon tarvitaan ketteryyttä. Haasteena on nopeuttaa suunnittelu- ja toimeenpanotyötä. Hallinnon prosessien hitaus sekä politiikan tekemisen sykli ja näiden epätahtisuus vaikeuttavat kyberturvallisuuden oikea-aikaista kehittämistä. Vision ajankohtaisuuden vuoksi uutta kyberturvallisuusstrategiaa ei kaivattu, mutta hallinnonaloilla odotetaan toimeenpano-ohjelman päivityksen kautta tulevia uusia toimintaohjeita.

Resurssit mainittiin suurena haasteena strategian vision toimeenpanolle. Kyberturvallisuudelle määritetään uusia tehtäviä, muuta niiden tekemiseen ei ole allokoitu erillisiä resursseja. Erityisesti tämän nähtiin koskevan Turvallisuuskomiteaa. Erillistä rahaa kyberturvallisuuden kehittämiselle ei ole hallinnonaloille saatu. Toisaalta haastatteluissa mainittiin, että valtionhallinnossa on tehty valtavasti työtä esimerkiksi taustajärjestelmien uudistamisessa. Viime vuo-

sina on ollut suuria uudistushankkeita, kuten Apotti. Järjestelmien uudistamisessa vanhojen prosessien digitoimisen sijaan palvelut on ajateltava kokonaan uudella tavalla ja näissä töissä kyberturvallisuuselementti on ollut vahvasti ja luontevasti mukana, vaikkei työtä varsinaisesti nähdä erillisenä kyberturvallisuuden kehittämistyönä. Toisaalta tämä mainittiin myös ongelmana; hallinnonaloille on syntynyt toimintakulttuuri, jossa kyberturvallisuutta tehdään muiden virkatehtävien ohessa. Vaikka kybertietoisuus on lisääntynyt, syvällinen kyberturvallisuusymmärryksen puute haittaa alan kehittämistä. Aiheena kyberturvallisuus on pysyväluontoinen, jonka ongelmat eivät ratkea irrallisilla hankkeilla. Toiminnan ja ajattelun pitääkin olla organisoituna jokapäiväiseen virkatyöhön, mutta haastatteluissa peräänkuulutettiin muutamankin henkilötyövuoden lisäresursointia tarpeelliseksi, jotta jatkuvasti uusia ratkaisuja vaativa kyberturvallisuusajattelu pysyy ajankohtaisena.

## 3.4 Toimeenpano-ohjelma

Kyberturvallisuusstrategian toimeenpano-ohjelma julkaistiin vuonna 2014. Se sisältää kullekin hallinnonalalle heidän osin itse määrittämiään tehtäviä ja vastuita strategian tavoitteiden toimeenpanemiseksi. Haastatteluissa toimeenpano-ohjelman ongelmaksi mainittiin, että suunnitelmallisen ohjelman sijaan se on pikemmin kokoelma ajateltuja toimenpiteitä. Ongelma on siinä, että toimeenpano-ohjelmaa kehitettiin hallinnonalalähtöisesti, mutta ilman tietoa kyberturvallisuuden tulevasta rahoituksesta. Toimeenpano-ohjelmassa todettiin siitä syystä olevan myös epärealistisia tavoitteita. Toimeenpano-ohjelmaa laadittaessa ministeriöissä luultiin ylimääräistä rahoitusta allokoitavaksi toimeenpanotyöhön. Toimenpiteiden epärealistisuus vaikeuttaa tulosten mitattavuutta. Haastatteluissa todettiin, että miten mitata ja seurata toimeenpano-ohjelman toteutusta, jos tietyt toimenpiteet ovat jo alun perin niin suuria tai kalliita, että niitä ei ole edes pyritty käynnistämään. Kyberuhkat kuitenkin kehittyvät ja lisääntyvät jatkuvasti, joten kyberturvallisuuden kehittämiseksi ja ennakkovarautumisen parantamiseksi on toimeenpanotyön oltava suunnitelmallista ja toteuttamiskelpoista.

Strategian toimeenpanon onnistumisina nähtiin muun muassa Kyberturvallisuuskeskuksen sekä Keskusrikospoliisin kyberyksikön perustamiset. Nämä tahot ovat onnistuneet tahoillaan kyberturvallisuuden ja tilannetietoisuuden parantamisessa ja yksiköt ovat hyvin verkottuneet niin kansallisesti kuin kansainvälisesti.

Tulevassa toimeenpano-ohjelman uudistuksessa kaivataan selkeämpää linjaa läpi ohjelman. Ohjelmalta toivottiin selkeämmin määriteltyä tavoitetilaa ja sen mukaisesti suunniteltuja toimenpiteitä. Haastattelujen perusteella nykyisellä toimeenpano-ohjelmalla ei ole ollut suurta merkitystä kaikissa ministeriöissä. Tärkeimmiksi ja hallinnonalojen työtä paremmin suuntaaviksi koettiin ministeriöiden kyberturvallisuustehtävien määrittelyt. Niiden kautta ministeriöiden substanssiosastot pohtivat kyberturvallisuuden parantamista tehokkaimmin. Samoin merkitystä koettiin olleen kyberturvallisuusstrategiassa annetuilla tehtäväkuvauksilla. Toimeenpano-ohjelman sijaan työtä on kokonaisuudessaan ohjannut enemmän Yhteiskunnan turvallisuusstrategia (YTS 2010).

## 3.5 Kyberturvallisuusstrategian strategiset linjaukset

### 3.5.1 Toimintamalli ja kybervarautuminen

Strategian tavoitteena on, että luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.

Kyberturvallisuusstrategiassa määriteltiin kybervarautumisen periaatteellinen toimintamalli. Kyberturvallisuutta johtaa valtioneuvosto määrittelemällä poliittis-strategisen tason linjaukset sekä päättämällä voimavarat ja toimintaedellytykset. Ministeriöt vastaavat hallinnonalojensa kyberturvallisuuden kehittämisestä, varautumisesta ja häiriötilanteiden hallinnasta. Tehokas kyberuhkiin varautuminen ja häiriötilanteiden hallinta vaativat tuekseen riittävän tilannetietoisuuden ja toimintamalli perustuu siihen, että valtioneuvostolla on käytössään yhteinen ja jaettu, ajankohtainen ja luotettava tilannekuva.

Strategian haasteeksi useampi haastateltava näki kyberturvallisuuden johtajuuden puutteen, eli sen, ettei toimintaa tällä hetkellä selkeästi johda kukaan. Siiloutunut hallintorakenne ja -kulttuuri estävät kyberjohtajuuden muodostumista hallinnonalojen vartioidessa omia toiminta-alueitaan. Haastateltavat epäilivät, että mikäli jatkossa halutaan selkeää kyberturvallisuuden johtamista, toimintamallin esitteleminen johtanee jälleen kiistoihin ja vahvaan vastustukseen. Osa näki ongelmia, mikäli valtionhallinnon ICT- ja kyberturvallisuustoimintaa siirretään keskitettyyn johtoon, koska tämä rajoittaisi hallinnonalojen itsenäistä toimintaa.

Operatiivisesta toiminnasta häiriötilanteissa ei ole olemassa selkeää toimintamallia. Yhteiskunnassa ei ole päätetty, kenellä on päätäntävalta ja mandaatti kertoa, mihin resurssit häiriötilanteessa ensisijaisesti ohjataan tai mikä/kenen järjestelmät nostetaan ensiksi pystyyn. Kenelläkään ei siis ole mandaattia määritellä, mikä on kriittistä.

Varautuminen ja häiriötilanteiden hallinta vaihtelevat hallinnonaloittain tai toimijan mukaan. Kyberturvallisuuden roolin ja merkityksen nähdään kasvavan tulevaisuudessa, joten on syytä pohtia toimintamallin riittävyyttä ja tulevia tarpeita jatkossa. Kyberturvallisuusteema on haastattelujen mukaan yksi keskeinen asia poikkihallinnollisessa varautumistyössä. Keskusteluyhteys on hyvä ja työhön ollaan sitoutuneita, mutta osa haastateltavista koki silti varautumisen yhteensovittamisen osin puutteelliseksi. Kybervarautumisen näkökulmasta toimintamalli koetaan hyvin organisoiduksi vastuunjaon osalta, mutta varautumisen yhteensovittamisessa on edelleen viivettä erityisesti häiriötilanteissa.

Haastateltavien mielestä turvallisuusviranomaisten keskinäinen sekä Kyberturvallisuuskeskuksen välinen yhteistyö toimii hyvin ja myös näiden viranomaisten välinen vastuujako on toimiva. Myös eri ministeriöiden valmiuspäälliköiden välinen yhteistoiminta on säännöllistä. Kansallinen harjoitustoiminta (TIETO, VALHA, KYHA) on ottanut kyberturvallisuuden kiinteäksi osaksi harjoituksia ja kokemukset ovat hyviä. Puutteena todettiin, ettei harjoituksista saatuja kokemuksia ”lessons learned” ole riittävästi viety käytäntöön.

Kyberturvallisuuden johtamisessa tulee aikaisempaa voimakkaammin ottaa elinkeinoelämä mukaan ja toimia enenevässä määrin julkinen-yksityinen -mallin mukaan. Kyberturvallisuuden toimintamallia halutaan kehittää lisäämällä ja tehostamalla harjoitustoimintaa ja integroimalla elinkeinoelämä harjoitusten kautta tiiviimmin mukaan. Yhteistyö yksityisen ja julkisen sektorin välillä nähtiin toimivan luontevasti osana kyberturvallisuuskokonaisuutta.

Keskeistä toiminnassa on tulevaisuuden kriittisten häiriöiden tai ongelmatilanteiden kriisiytymisen estäminen. Toiminnan tulee perustua varmuuteen ja luottamukseen, niin kansallisesti kuin erityisesti kansainvälisessä kentässä. Koko toiminnan ja sen toimijoiden tulee luoda luottamusverkosto, jossa tietoa voidaan vaihtaa sovitulla tavalla.

Yhteistoimintamallin osalta keskeisenä pidettiin sitä, että jokainen toimija on vastuussa oman alansa kyberturvallisuusasioiden hoitamisesta. Erityisesti painotettiin sitä, että viranomaiset eivät voi olla vastuussa yksityisen sektorin tieto- ja kyberturvallisuudesta. Yksityisellä sektorilla suuremmilla yrityksillä on hyvällä tasolla olevia kyberturvallisuuden järjestelyitä. Kehityskohteena mainittiin pk-yritysten kyber- ja tietoturvallisuusasiat. Suomessa suurin osa yrityk-

sistä kuuluu kooltaan pk-yritysten luokkaan, joissa kyberturvallisuuden osaaminen ja resursointi voivat olla isoja haasteita. Isompien toimijoiden turvallisuus saattaa olla kiinni pienempien alihankkijoiden tilanteesta, joten huomion kohdistaminen pk-yritysten tilanteen parantamiseen on keskeistä myös laajemman yhteiskunnallinen kyberturvallisuuden kehittämisessä.

Nykytilanteen haasteena on kansallisten resurssien vähäisyys. Mikäli tapahtuu useita enemmän tai vähemmän päällekkäisiän häiriötilanteita, osaavista henkilöistä tulee puute. Resurssipula näkyy erityisesti, kun häiriötilanteet muodostuvat pitkäaikaisiksi.

Haastatteluissa kehitysehdotuksina nousi esiin

1) Toimivan johtamisjärjestelyn rakentaminen aina valtionhallinnon ylimmälle tasolle saakka,
2) Eri toimijoiden välisen yhteisen kyberturvallisuusfoorumin luominen, jossa tiedonvaihto tapahtuu vapaasti
3) Ketteryyden luominen toimintaan, ml. yhteistyö hallinnonalojen välillä, mutta myös yritysten ja yliopistojen/tutkimuslaitosten kanssa.

### 3.5.2 Tilannekuva

Strategian tavoitteena on, että parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.

Tilannekuva kybertoimintaympäristöstä on fragmentaarinen ja sen kokonaisuuden hahmottuminen perustuu jaettuun tietoon viranomaisten, yksityisen sektorin, tutkijoiden ja asiantuntijoiden välillä. Kyberturvallisuuskeskus ylläpitää kansallista kyberturvallisuuden tilannekuvaa. Huoltovarmuuskeskus on teettänyt sektorikohtaisia tilannekartoituksia huoltovarmuuskriittisillä aloilla[15]. Valtioneuvoston rahoittama tietoverkkorikollisuuden tilannekuva julkaistiin keväällä 2016[16]. Tietoverkkorikollisuuden osalta tilannekuvaa pitää yllä keskusrikospoliisin vuonna 2015 perustettu kyberrikosten torjuntakeskus.

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. 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.

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

[15] Ks. esim. energiasektorin kyberturvallisuuden tilannekuvasta: https://www.huoltovarmuuskeskus.fi/kyberturvallisuuden-tilannekuva-energia-alalla/

[16] Leppänen ym. 2016 http://tietokayttoon.fi/documents/10616/2009122/17_Tietoverkkorikollisuuden+tilannekuva.pdf/6ef911d2-cbe8-43bd-aafa-e10ed573f28a?version=1.0

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.

Valtionhallinnossa GovSOC-toiminto tuottaa tieto- ja kyberturvallisuustapahtuminen ennaltaehkäisyä, havainnointia, hallinnan tukea ja koordinointia. GovCERT -palvelujen tehtävänä on tukea valtion ympärivuorokautista tietoturvatoimintoa tuottamalla tietoturvaloukkausten ennaltaehkäisyn, havainnoinnin ja selvittämisen tukipalveluja. GovHAVARO -palvelun avulla täydennetään valtionhallinnon internet-tietoliikenteen tieto- ja kyberturvallisuusuhkien havainnointia. HAVARO-järjestelmässä Kyberturvallisuuskeskuksella on käytännössä näkyvyys kaikkeen tulevaan ja lähtevään liikenteeseen (metatieto ja sisältötieto). HAVARO-toimintaan osallistuville yrityksille ja julkishallinnon toimijoille toiminta on vapaaehtoista. Kyberturvallisuuskeskuksen näkökulmasta kysymys ei ole yksittäisten toimijoiden auttamisesta vaan keskiössä on yhteiskunnan varoittaminen ja turvallisuuden ylläpitäminen. Lisäksi tilannetietoisuutta tuottaa valtionhallinnon VIRT-ryhmän toiminta, joka muodostuu eri organisaatioiden kyberturvallisuusuhkien hallinnasta vastaavista henkilöistä, turvallisuusviranomaisista ja valtion ICT-palveluiden tuottajista. Tällä tasolla tiedon vaihto ja yhteistoiminta toimivat hyvin. Ongelmia syntyy, kun kysymys on turvaluokiteltujen tietojen erityisesti suojaustason III ja II tietojenvaihdosta.

Lisäksi joillain hallinnonaloilla on vahvaa yhteistyötä kyberturvallisuuteen liittyen sekä hallinnonalan sisällä että poikkihallinnollisesti. Kyberturvallisuuskeskuksen ja Valtioneuvoston tilannekuvakeskuksen yhteistyötä pidettiin toimivana ja tiedonjakamisen koettiin olevan riittävällä tasolla. Tilannekuvan tuottamiseen liittyvä vapaaehtoisuuden periaate saattaa aiheuttaa sen, että erityisesti yksityiseltä sektorilta ei saada koottua kaikkea tarpeellista tietoa, jolloin tilannetietoisuus ei vastaa yksityisen sektorin tosiasiallista tilaa.

Kysyntää olisi myös sektorikohtaiselle tilannekuvapalvelulle, mutta Kyberturvallisuuskeskus ei tällä hetkellä pysty 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.

Yleisen näkemyksen mukaan Valtioneuvoston tilannekuvakeskusta (VN-TIKE) tulee kehittää kyberturvallisuuden tilannekuvan kansallisena keskuksena, joka kykenee reaaliaikaiseen laajojenkin häiriötilanteiden tilannetietoisuuden muodostamiseen osana hybridivaikuttamisen torjuntaa.

### 3.5.3 Havainnointikyky

Strategiassa esitetään, että ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden toimijoiden kyky havaita ja torjua kyberuhkia ja -häiriötilanteita on keskeinen kyvykkyys. Havainnointikyky mainittiin haastatteluissa myös keskeiseksi haasteeksi kyberturvallisuuden parantamisessa. Suomessa on edellytyksiä ennaltaehkäisyyn ja parempaan havainnointikykyyn uhkien torjumiseksi. Haastatteluissa ei pääosin osattu antaa arviota havainnointikyvystä koko yhteiskunnan

osalta. Kattavia arvioita hallinnonalakohtaisestikin oli vaikea antaa, koska vakaviin tilanteisiin ei ole jouduttu.

Yleisesti todettiin, että kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen toimivaltuuksien puutteiden vuoksi. Siksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on rajallinen. Yrityksillä on entistä vaikeampi havaita kehittyneitä kyberhyökkäyksiä (APT). Tällä hetkellä yritysvakoiluun tähtääviä APT-hyökkäyksiä toteuttavat rikollisisorganisaatioiden lisäksi valtiolliset tiedusteluorganisaatiot. Näiden kyvykkyydet ovat tehokkaita ja yrityssektorilla on vaikeuksia niiden tunnistamisessa ja torjunnassa.

Yksityisen sektorin, erityisesti kriittisten yritysten osalta, ilmoitusvelvollisuudessa ja tiedon jakamisessa koetaan olevan tehostamisen mahdollisuuksia. Tarvittaessa tulee lainsäädännön keinoin lisätä ilmoitusvelvollisuutta. Keinoina tehostamiseen mainittiin myös julkinen-yksityinen -yhteistyön kehittäminen.

### 3.5.4 Poliisin suorituskyvyn kehittäminen

Strategia esitti vaatimuksen, että huolehditaan poliisin tehokkaista edellytyksistä ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen.

Suojelupoliisin ydintoiminta-alueita ovat terrorismintorjunta, turvallisuustyö ja vastatiedustelu. Suojelupoliisin tehtävänä on torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä ja ulkoista turvallisuutta. Kyberulottuvuudesta on tullut SUPO:lle keskeinen elementti terrorismin torjunnassa ja vastatiedustelussa.

Tietoverkkorikoksia (kyberrikoksia) tutkivat poliisilaitokset ja Keskusrikospoliisi. Tietoverkkorikoksia ovat esimerkiksi tietomurrot, palveluksenestohyökkäykset sekä identiteettivarkaudet ja laittomat tietosisällöt. Tietoverkot mahdollistavat myös perinteisten rikosten, kuten petosten ja väärennösten toteuttamisen. Rikollisryhmät hyödyntävät verkkoa myös yhteydenpitoon, rikosten valmisteluun ja taloudellisen hyödyn tavoitteluun sekä terroristisiin tarkoituksiin.

Tämän rikollisuuden muodon keskeisiä piirteitä ovat 1) valtiolliset rajat ylittävä toiminta, 2) toimijoiden näkymättömyys (attribuutio-ongelma) ja 3) piilorikollisuus. Tietoverkkorikoksista ei ole saatavissa täsmällisiä tilastotietoja, koska piilorikollisuuden määrä on suuri. Poliisissa tietoverkkorikollisuuden torjuntaa painotetaan osana järjestäytyneen rikollisuuden torjuntaa.

Poliisin toimivaltuuksista hankkia rikosten estämiseksi ja paljastamiseksi tarvittavaa tietoa säädetään poliisilaissa. Poliisin toimivaltuuksista hankkia rikosten selvittämiseksi tarvittavaa tietoa säädetään puolestaan pakkokeino- ja esitutkintalaeissa. Kyberrikollisuuden torjunnassa poliisi tarvitsee nykyistä laajemmat toimivaltuudet torjuessaan kansallisia ja rajat ylittäviä kyberhyökkäyksiä. Järjestäytynyttä kyberrikollisuutta tulee voida valvoa nykyistä tehokkaammin jo rikosten valmisteluvaiheessa. Kyberrikollisuuden torjunnassa tarvitaan yhteinen ja keskitetty rikosilmoitusjärjestelmä, joka mahdollistaisi tilannetietoisuuden parantumisen ja tutkintatehtävien tehokkaan jakamisen ja sitä kautta rikosten selvittämisen. Järjestelmän tulisi olla kansalaisille ja yrityksille yksinkertainen ja helppo käyttää.

Poliisin suorituskyky on parantunut ja erityisesti Kyberrikosten torjuntakeskuksen perustaminen keväällä 2015 on tehostanut toimintaa. Se osallistuu mm. tietoverkkorikosten torjuntaan, tekee internet-valvontaa ja laatii uhka-arvioita sekä tekee tiivistä yhteistyötä erityisesti Viestintäviraston kyberturvallisuuskeskuksen ja Europolin kyberrikostorjuntakeskuksen kanssa ja lisäksi monien muiden tahojen kanssa. Tehokas toiminta edellyttää, että todistusaineiston ja tietojen saatavuus sekä siirtäminen valtioiden välillä toimii tehokkaasti.

### 3.5.5 Puolustusvoimien suorituskyvyn kehittäminen

Strategia edellytti, että Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Puolustusvoimat suojaa omat järjestelmänsä siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään huolimatta kybertoimintaympäristön uhkista. Suorituskyvyn varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä.

Puolustusvoimien tehtäviin kuuluu Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä osallistuminen sotilaalliseen kriisinhallintaan. Puolustusvoimista annetun lain mukaan Suomen sotilaalliseen puolustamiseen kuuluu maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen. Uutena puolustettavana alueen on kansallinen kybertila. Valtion täysivaltaisuuteen kuuluu sen alueellinen koskemattomuus. Tämän tulisi koskea myös kansallista kyberaluetta. Nykyinen aluevalvontalaki perustuu perinteisten alueiden valvontaan ja siksi tarvitaan välttämättä uusi sotilastiedustelulaki kattamaan tiedonhankinta myös digitaalisessa kybermaailmassa.

Sotilastiedustelun tehtävänä on muodostaa ja ylläpitää sotilaallisen päätöksenteon edellyttämää sotilasstrategista tilannekuvaa. Sen muodostamiseksi sotilastiedustelu seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Sotilastiedustelulla puolustusvoimat ylläpitää ja kehittää puolustusvalmiutta. Sotilastiedustelun kohteena ovat pääosin valtiotoimijat. Sotilastiedustelun tavoitteena on muodostaa ja ylläpitää toimintaympäristötietoisuutta. Keskeistä on ennakkovaroituskyky sotilaallisten uhkien kehittymisestä, jotta Suomen turvallisuutta koskeva ylimmän valtionjohdon päätöksenteko Suomen valtion suvereniteettia vaarantavista uhista perustuu oikea-aikaiselle tilannetiedolle, ja mahdollistaa tarvittaessa oikea-aikaisiin varautumis- ja vastatoimiin ryhtymisen.[17]

Sotilastiedustelun tiedonhankintatoimivaltuuksista ei ole toistaiseksi säädetty laissa, joten valmisteilla oleva lakiesitys on Puolustusvoimille ehdottoman välttämätön. Valmistelussa olevaa lakiesitystä pidettiin hyvänä lähtökohtana toiminnan kehittämisessä, jotta sotilastiedustelu saisi toimintaedellytykset kerätä tilannekuvan muodostamiseen ja ennakkovaroituksen tuottamiseen tarvittavaa tietoa digitalisoituneessa toimintaympäristössä. Tämä tukee samalla kyberalueen valvontaa ja puolustamista.

Haastattelut tukivat *Suomalaisen tiedustelulainsäädännön suuntaviivoja* -raportin esityksiä lainsäädännön aikaansaamisesta. Raportin mukaan ”tietoliikennetiedustelussa olisi kyse tiedustelutoimivaltuudesta, jonka tarkoituksena olisi tuottaa kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtionjohdon päätöksenteon tueksi. Lisäksi tarkoituksena olisi havaita ja tunnistaa kansalliseen turvallisuuteen kohdistuvia vakavia ulkoisia uhkia sekä kerätä niistä sellaista tietoa, joka mahdollis-

[17] Suomalaisen tiedustelulainsäädännön suuntaviivoja

taa tilannekuvan muodostamisen, torjuntatoimiin ryhtymisen sekä sotilasviranomaisten osalta ennakkovaroituksen antamisen."[18]

Puolustusvoimien sotilaallisen kyberpuolustuskyvyn kehittämisessä tulee tiedustelun, vaikuttamisen ja suojautumisen suorituskykyjä edelleen kehittää tasapainoisena kokonaisuutena vastaamaan toimintaympäristön vaatimuksia. Kybersuorituskyvyn kehittämisessä tulee ottaa huomioon sellaisia tekijöitä kuin hyökkäyskynnyksen nostaminen, tehokas havaintokyky ja tilannekuva sekä kybermaailmaan soveltuvat päätöksenteko- ja johtamisprosessit.

Puolustusvoimissa aloitti tammikuussa 2015 Kyberosasto osana Puolustusvoimien johtamisjärjestelmäkeskusta. Kyberosasto suojaa tietoverkkoja ja -palveluita sekä kehittää kyberpuolustusta. Osasto ylläpitää puolustusvoimien kybertilannekuvaa. Puolustusvoimat on kehittänyt kyberpuolustuksen koulutusta kaikilla tasoilla. Varusmiesten pilottiryhmä aloitti asepalveluksen puolustusvoimien johtamisjärjestelmäkeskuksen kyberosastolla syksyllä 2015. Vuosien kuluessa kyberosastolla palvelevista koostuu osa nykyaikaista reserviä, joka tunnistaa modernit kyberuhat ja osaa operoida kaikissa kybertaistelulajeissa.

### 3.5.6 Kansainvälinen yhteistyö

Strategian mukaan vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.

Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa. Varautumisen ja muun kyberturvallisuuden toteuttaminen jää vaillinaiseksi ilman tehokasta ja järjestelmällisesti koordinoitua kansainvälistä yhteistyötä.

Jokainen viranomainen omalla toimialallaan harjoittaa yhteistyötä erityisesti niiden valtioiden ja organisaatioiden kanssa, jotka ovat maailmanlaajuisesti edelläkävijöitä kyberturvallisuuteen liittyvissä asiakokonaisuuksissa. Aktiivista yhteistyötä tehdään tutkimus- ja kehittämistyön, erilaisten sopimusten valmistelutyön, organisaatioiden työryhmätyöskentelyn, sekä kansainväliseen harjoitustoimintaan osallistumisen kautta. Suomi onkin osallistunut kansainvälisiin kyberharjoituksiin, joissa olemme suoriutuneet hyvin.

Kansainvälinen yhteistoiminta on toiminnan perusedellytys. Kansainvälisessä yhteistyössä keskeisiä ovat luottamusverkostot kuten esim. EGC (European Government CERTs group) ja pohjoismainen yhteistyö, missä verkostossa jaetaan luottamuksellistakin tietoa. Toiminta kansainvälisessä yhteisössä edellyttää tiedonvaihtoa. Suomen on rakennettava suorituskykyinen oma järjestelmänsä, jotta se voi toimia aktiivisena toimijana kansainvälisessä yhteisössä.

Kyberrikollisuuden torjunnassa yhteistyö on kehittynyt hyvin ja kaikki maat haluavat tehdä yhteistyötä. Pohjoismaisella tasolla meillä on pitkä yhteistyöperinne ja mukaan ovat tulleet Baltian maat. Europol ja nyt yhä enemmän Interpol ovat keskeisiä yhteistyökumppaneita sekä Yhdysvaltojen kanssa FBI.

Kansainvälinen oikeusapu perustuu yleensä kansainvälisiin yleissopimuksiin, joissa on useita sopimuspuolia. Oikeusapua säännellään myös kahdenvälisin sopimuksin. Kansainvälinen rikosoikeusapu laajassa merkityksessä kattaa keskinäisen oikeusavun, rikoksen johdosta tapahtuvan luovuttamisen ja tuomittujen siirtämisen. Keskinäiseen oikeusapuun rikosasioissa

[18] Ibid.

sisältyy mm. asiakirjojen tiedoksianto ja todistelupyynnöt eli todisteiden hankkiminen rikostutkintaa tai oikeudenkäyntiä varten. Oikeus-apua annetaan vieraan valtion oikeusviranomaisille niiden käsitellessä toimivaltaansa kuuluvaa rikosasiaa.[19] Nämä menettelytavat on luotu pääosin 1970-luvun perinteisen rikollisuuden tarpeisiin. Kyberrikollisuuden tutkinta ja syyteharkintaan saattaminen edellyttää nopeita toimintaprosesseja. Nykyisellään viralliset prosessit saattavat kestää 9-12 kuukautta, mikä hankaloittaa merkittävästi kyberrikostutkintaa ja epäiltyjen luovuttamista.

Kyberturvallisuuden tuottaminen alkaa Suomen ulkopuolelta, joten kansainvälinen yhteistyö on olennaista. Kansainvälistä kyberyhteistyötä tehdään paljon, mutta pääasiassa toimialakohtaisesti. Erityisesti Kyberturvallisuuskeskus CERT-toimintoineen ja poliisin kyberrikostorjuntayksikkö ovat verkottuneet vahvasti kansainvälisiin vastaaviin yksiköihin. Kyberuhkat tulevat lähes yksinomaan Suomen rajojen ulkopuolelta, joten havainnointi ja ennaltaehkäisy ovat kansainvälistä toimintaa. Kansainvälisen yhteistyön kehittämisessä on menty eteenpäin. Keskeisintä on toimialojen oma yhteistyö, EU-viitekehys ja kyberpuolustusasioissa NATO-yhteistyö. Kyberturvallisuuden turvaaminen ei ole mahdollista vain kansallisin toimin. Kansainvälisen sääntelyn näkökulmasta keskeisimpänä mainittiin EU ja sen uusi NIS-direktiivi.

### 3.5.7 Kyberosaamisen ja -ymmärryksen parantaminen

Strategian tavoitteena oli, että parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä. Sen mukaan yhteiskunnan toimijoiden jatkuvan osaamisen ja tietämyksen kehittämisen tukena panostetaan yhteisten kyberturvallisuuden ja tietoturvallisuuden ohjeistojen kehittämiseen, hyödyntämiseen ja kouluttamiseen. Yhteiskunnan kokonaisvaltaisen valmiuden kehittämiseksi harjoitustoimintaan otetaan mukaan myös yhteiskunnan elintärkeiden toimintojen kannalta tärkeät yritykset ja kansalaisjärjestöt.

Lisäksi tavoitteena oli perustaa kyberturvallisuuden strateginen huippuosaamisen keskittymä tarjoamaan tutkimusyksiköille ja tutkimustuloksia hyödyntäville yrityksille tehokkaan tavan tehdä tiivistä ja pitkäjänteistä yhteistyötä keskenään.

Kansallisen kybersuorituskyvyn haasteena mainittiin syvemmän ymmärryksen puuttuminen. Se johtuu muun muassa siitä, että suuria häiriötilanteita ei ole ollut. Kyberharjoituksia kuitenkin järjestetään niin hallinnonalojen sisällä kuin poikkihallinnollisesti, mutta ne ovat jääneet joidenkin vastaajien mielestä pinnalliselle tasolle tai ne eivät vastaa laajoissa häiriötilanteissa toimimista. Kybervarautumisen rinnastaminen muuhun yhteiskunnalliseen varautumiseen ei ole kaikille täysin selkeää.

Kyberturvallisuuden osaaminen tulisi olla kansalaistaito ja ulottua koko koulutusalaan. Turvallisuusviranomaisten koulutuksessa tarvitaan yleinen kyberturvallisuuskoulutus koko henkilöstölle ja lisäksi syväosaamiseen tähtäävää koulutusta alan erityisosaajille. Tutkimuksessa ja osaamisessa tulee kasvattaa osaajien kriittistä massaa, jotta kansallinen osaamisen ja tutkimuskyvykkyyden kansallinen omavaraisuus säilyy.

Kyberturvallisuuden osaaminen ei ole vain erillinen ammatillinen osaamisalue vaan se kattaa kyvykkyyksiä kansalaistaidoista aina huippuosaamiseen saakka. Tämän vuoksi kyberturvallisuus tulisi sisällyttää eri koulutusasteisiin. Yleissivistävässä perusopetuksessa koulutuksella tulee varmistaa, että nuorilla on riittävät taidot toimia kybermaailmassa ja he ymmärtävät sen uhat ja osaavat suojautua niiltä. Lukiokoulutuksessa ja ammatillisessa koulutuksessa syvennetään näitä taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa.

[19] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus, 2001

Ammatilliseen koulutukseen voidaan sisällyttää kyberturvallisuuden alan perusammattitaitoon ja työelämässä tarvittavaan alan ammatilliseen pätevyyteen johtavaa koulutusta.

Yliopistoissa korostuu kyberturvallisuuden tieteellinen tutkimus ja siihen perustuva opetus. Ammattikorkeakoulut tarjoavat käytännönläheistä ja työelämän tarpeita vastaavaa kyberturvallisuuskoulutusta. Laajasti koko korkeakoulusektorilla toteutettu kyberturvallisuuskoulutus tuottaa yhteiskunnan eri tasoille alan huippuosaajia, joiden tiedot ja taidot vastaavat eri tehtäviin sisältyviä osaamisvaatimuksia.

Kyberturvallisuus tulee sisällyttää myös osaksi aikuiskoulutusta. Kyberturvallisuuden aikuiskoulutus voi olla perustutkinto-opetusta, tutkintoon kuuluvia opintoja, näyttötutkintoihin valmentavaa koulutusta, oppisopimuskoulutusta, ammattitaitoa uudistavaa ja laajentavaa lisä- ja täydennyskoulutusta sekä kansalais- ja työelämätaitoihin valmentavia yhteiskunnallisia opintoja.

Kyberturvallisuuden tutkimusta on toteutettu Suomen Akatemian ja Tekesin rahoittamissa hankkeissa vuodesta 2013 lähtien. Kyberturvallisuusosaaminen tarjoaa huomattavan liiketoimintapotentiaalin. Suomella on huippuosaamista tällä alueella, mutta se on hajallaan yksittäisissä yrityksissä, yliopistoissa ja tutkimuslaitoksissa. Kasvupotentiaali on mahdollista saavuttaa vain yhteistyön kautta ja se on ollut perustana myös yritysten ja Tekesin rahoittamissa ohjelmissa, joista Cyber Trust -hanke on merkittävin. Viime vuosina tehdyt kansalliset T&K-toiminnan leikkaukset ovat supistaneet merkittävästi myös kyberturvallisuuden tutkimuksen resursseja. Haastatteluissa tuli esille huoli kansallisen kyvykkyyden kehittymisestä, kun tutkimuksen ja koulutuksen resursseja supistetaan. Suomen tavoite olla globaali edelläkävijä kyberturvallisuusalalla vaarantuu, mikäli osaamisen ja T&K-resurssit eivät ole riittäviä.

Kyberturvallisuusharjoituksia on toteutettu jo usean vuodenajan mutta osa niistä on jäänyt liian pinnalliselle tasolle eikä niissä ole riittävästi päästy harjoittelemaan syvällisesti häiriötilanteissa toimimista. Teknillis-toiminnallisten harjoitusten lisäksi tulisi järjestää harjoituksia, joissa testataan laaja-alaisten ja -vaikutteisten kyberhäiriötilanteiden johtamis- ja raportointiketju aina ylimpään valtionjohtoon saakka. Säännöllisellä harjoittelulla voidaan osaltaan saavuttaa ja ylläpitää kyberturvallisuusstrategian mukainen tavoitetila. Lisäksi tulee kehittää harjoituksissa saatujen kokemusten vientiä käytäntöön, sillä nykyisellään niitä ei hyödynnetä eri organisaatioissa järjestelmällisesti vaan harjoituksissa vuosi toisensa jälkeen ”opitaan” samoja asioita.

### 3.5.8 Lainsäädäntö

Strategian mukaan kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset. Sen mukaan tuli kartoittaa kybertoimintaympäristöön ja -turvallisuuteen vaikuttava ja liittyvä lainsäädäntö sekä sen kehittämistarpeet hallinnonalojen ja elinkeinoelämän yhteistyönä. Kartoituksen yhtenä tarkoituksena on se, että lainsäädäntö antaisi mahdollisuuden sekä riittävät keinot ja toimivaltuudet eri alojen toimivaltaisille viranomaisille sekä muille toimijoille toteuttaa yhteiskunnan elintärkeiden toimintojen ja erityisesti valtion turvallisuuden suojaamista kyberuhkia vastaan.

Tietoturvallisuutta on Suomessa säädetty eri laeilla jo pitkään, joten perusasiat ja toimintatavat ovat hyvällä tasolla. Tämän hetkistä lainsäädäntöä ei pidetty esteenä hallinnonalojen yhteistoiminnalle eikä siinä koettu olevan merkittäviä puutteita. Kyberturvallisuus kuuluu koko yhteiskuntaan poikkileikkaavasti, joten on haastavaa kehittää erillistä lakipakettia vain kyberturvallisuuteen. Mahdollinen kyber-elementti ja esimerkiksi EU-direktiivit pitää sopeuttaa olemassa oleviin substanssilakeihin.

Toimintaa haittaavana tekijä on tiedon luovutusoikeuksien normiston erilaisuus eri hallinnonaloilla. Laajavaikutteisissa häiriötilanteissa syntyvän tietoaineiston käsittelyssä tulisi olla yhdenmukaiset toimintatavat, ohjeet ja normit. Kyberhyökkäystilanteiden hallinta edellyttää nopeaa ja saumatonta tiedonvaihtoa eri toimijoiden kesken.

Lisäksi esille nostettiin ilmoitusvelvollisuus ja yksityisyydensuoja. Haastatteluissa näkyi tasapainoilu havainnointikyvyn ja yksityisyyden suojan välillä. Esiin nousivat myös tietyt eettiset kysymykset liittyen mm. liikenteen automatisointiin ja tiedon keräämiseen sähköisin sensorein. Kyberalan nopean kehittymisen myötä tarvitaan yhteiskunnallista keskustelua automaation ja digitalisaation etiikkaan ja vastuisiin liittyvistä kysymyksistä.

Tarvitaan yritysten yhteiskuntavastuuta myös tilanteissa, joissa pakottavaa lainsäädäntöä tai normistoa ei ole. Mikäli kaikki kybermaailman toimijat ilmoittaisivat havainnoistaan/poikkeamista/hyökkäyksistä niin häiriötilanteiden hallinta, analysointi, selvittäminen ja varautumisen parantaminen tehostuisivat.

Useat haastateltavat korostivat tiedustelulainsäädännön tarvetta. Tiedustelulainsäädännön uudistaminen on välttämätöntä havainnointikyvyn parantamiseksi. Lisäksi se tarvitaan tuomaan selkeyttä toimintaan ja kansainvälisen yhteistyön tasapainottamiseksi, jossa se toimisi kumppanuutta edistävänä ja luottamusta lisäävänä tekijänä. Tiedustelulainsäädännön uusinta parantaa tilannetta, mutta jättää vielä aukkoja toimivaltuuksiin. Lainsäädäntöä tulee kehittää teknologianeutraalina, jossa tehtävät ja toimivaltuudet ovat tasapainossa.

Kybertilannekuvan kehittämiseksi esitettiin harkittavaksi pakottavan raportoinnin laajentamista, jotta kaikki kyberhäiriöt ja niihin liittyvät tapahtumat saadaan koottua osaksi kansallista tilannekuvaa. Lisäksi esitettiin tarve 24/7-toiminnon toteuttamiseen valtionhallinnossa, jotta voidaan reagoida nopeasti ja tehokkaasti ICT-järjestelmän häiriötilanteisiin. Samalla tulee tarkistaa toimivaltuudet häiriötilanteiden hallinnassa ja poikkeusolojen strategisessa johtamisessa ottaen huomioon kybermaailman ominaisuudet.

Koko lainsäädäntökenttä tulisi myös käydä läpi ja tarkistaa se kybertoimintaympäristön näkökulmasta, jotta niissä tulisi otetuksi huomioon digitaalisen kybermaailman luonne, ominaisuudet ja toiminnallisuudet.

Kyberrikollisuuden torjunnassa tulee voida käyttää hyväksi kaikkia poliisin rekisteritietoja ja poliisilla tulee olla oikeus tiedonhankintaan vihjetietojen perusteella, kun kyseessä on järjestäytyneen kyberrikollisuuden torjunta.

### 3.5.9 Tehtävät ja vastuut eri toimijoille

Strategian mukaisena tehtävänä oli määrittää viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.

Kyberturvallisuuden kehittäminen vaatii selkeää vastuiden määrittelyä ja tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää, että kukin hallinnonala tekee riskiarvioinnin ja kypsyysanalyysin, joiden avulla tunnistetaan kyberturvallisuuden kannalta merkittävät haavoittuvuudet ja riskit sekä niiden hallinnan taso. Saatujen tulosten perusteella laaditaan kunkin hallinnonalan toimeenpano-ohjelmat sekä tuetaan elinkeinoelämän toimeenpano-ohjelmien tekemistä yhteistoiminnassa huoltovarmuusorganisaation kanssa.

Kyberturvallisuuden toimijat ovat yleisesti sitoutuneet laadittavan toimeenpano-ohjeen (TPO) toteuttamiseen, mutta kansallisen vision yleisyys ja selkeän poliittisen tuen puute haittaavat käytännön toteuttamista, jolloin kehittämiseltä puuttuu selkeä suunta. Yrityssektorilla on vielä niitä, jotka eivät ole riittävästi tunnistaneet kyberturvallisuuden uhkia ja mahdollisuuksia.

### 3.5.10 Haasteet ja kehityskohteet

Kyberturvallisuuden vision saavuttamiseksi kehityskohteina mainittiin mm. resursointi, havainnointikyvyn kehittäminen ja kehittyneiden hyökkäysten analysointikyky. Jos kybertoimintaympäristössä ei kyetä havainnoimaan haitallista liikennettä tai tunkeutumisyrityksiä, silloin niiden torjunta on mahdotonta. Kehityskohteina tunnistettiin resursointiin liittyvä kyky ja ymmärrys käyttää resursseja oikeasuuntaisesti sekä luotujen rakenteiden ja toimintatapojen tehokas käyttöönotto.

Tulevaisuuteen liittyen haasteena mainittiin tasapaino suojauksen, anonymiteetin ja havainnointikyvyn välille. Tästä voi nousta tulevaisuuden kyberturvallisuustyön keskeinen haaste. Tulevaisuudessa kybertoimintaympäristön rooli tulee kasvamaan niin positiivisessa kuin negatiivisessa mielessä. Järjestäytynyt rikollisuus ja muu rikollisuus siirtyvät vahvemmin verkkoon. Rikollisten toimintaympäristöt, kuten Tor-verkko ja Dark Net tulevat olemaan yhä vaikeammin valvottavissa. Salauksen käyttö tulee olemaan yksi suurimmista haasteista. Erityisenä huolenaiheena on kryptografian hallinta kansallisesti tasolla. Suomessa tarvitaan tämän alan syväosaamista kansallisen omavaraisuuden näkökulmasta.

Uudenlaiset palvelutuotannon mallit muokkaavat ja tehostavat toimintaympäristöä ja vaativat uutta ajattelua kyberturvallisuudelta. Asioinnin siirtyessä enenevässä määrin verkkoon tunnistautuminen ja pilvipalvelut edellyttävät kyberturvallisuusvaatimusten arvioimista uudelleen.

Kyberturvallisuuden alueella sekä laajemmin kokonaisturvallisuudessa ennaltaehkäisy on keskeisintä. Haastatteluissa painotettiin niin sanottua **Security by Design** -ajattelun kehittämistä. Kyberturvallisuuden parantamiseksi järkevin tapa on panostaa ennaltaehkäisyyn ja turvallisuuden rakentamiseen järjestelmien sisään sisäänrakennetuksi ominaisuudeksi, eikä jälkeen päin ”päälle liimatuksi” ominaisuudeksi. Lisäksi ennaltaehkäisyä tehostaa ihmisten tietoisuuden ja järjestelmien kestokyvyn (resilienssin) kehittämiseen.

Riippuvuus infromaatioteknologiasta kasvaa edelleen ja siihen liittyvän huoltovarmuuden kanssa tehdään paljon työtä. Kuitenkin sääntely- ja vaikuttamismahdollisuudet valuvat kansallisten toimien ulottumattomiin, koska kriittinen verkkoinfrastruktuuri on enenevässä määrin ulkomaalaisomisteisilla toimijoilla. Lisäksi yrityskentässä on edelleen puutteita riskienhallinnassa ja kyvykkyydessä ottaa käyttöön olemassa olevia turvallisuusratkaisuja ja -toimintatapoja.

Yleinen tietoisuuden ja osaamisen nostamisen tarve tuli esiin kaikissa keskustelussa. Huolta, erityisesti lähitulevaisuudessa, aiheuttaa osaamisen kapeus sekä osaavan ja ammattitaitoisen henkilöstön saatavuus tulevaisuudessa. Tämän elementin kehittäminen liittyy niin kansalaistaitojen lisäämiseen kuin tutkimus- ja kehitystoimintaan. Suomessa muun muassa Huoltovarmuuskeskus toimii aktiivisesti tutkimuksen, tuotekehityksen ja harjoitusten edistäjänä. Kansalaisten osalta on syytä pohtia sitä, mitkä ovat ne tulevaisuuden osaamistarpeet, jotka pitäisi sisällyttää perusopetuksen opetussuunnitelmatasolle.

Strategian toimeenpanossa tulee nähdä aikaisempaa vahvemmin kybervakoilun laajentuminen ja kehittyminen, mikä edellyttää tehokkaiden vastatoimenpiteiden toteuttamista. Tällä hetkellä kybertiedustelun torjunta on kansallinen sokeapiste. Kybertoimintaympäristön val-

vonnassa tarvitaan tasapaino tehtävien ja toimivaltuuksien välillä sekä riittävät henkilöstövoimavarat ja taloudelliset resurssit.

Kyberturvallisuuden toimeenpanossa tulee kiinnittää huomiota alan nopeaan kehitykseen, mikä tarkoittaa ketteryyttä ja joustavuutta. Laadittavat strategiat ja asiakirjat jäävät nopeasti ajastaan jälkeen, siksi kehittämisen tulisi tapahtua nonstop-periaatteella. Hitauselementti korostuu valtiohallinnon prosesseissa. Koska haitallinen toiminta kybertoimintaympäristössä lisääntyy ja kehittyy nopeasti, täytyy siihen reagoida proaktiivisesti eikä reaktiivisesti. Proaktiivisuutta tulee myös kehittää elinkeinoelämän ja viranomaisten yhteistyössä.

Vaikka kehityskohteita on paljon, suomalaisessa kyberturvallisuustyössä on myös vahvuuksia. Yksi useasti mainittu on viranomaisyhteistyö ja kriisijohtamismallit ja -perinne. Suomessa on vahva kokonaisturvallisuuteen liittyvää viranomaisyhteistyötä ja huoltovarmuuteen liittyvää julkinen-yksityinen-yhteistyötä. Viranomaistyössä vastuut ovat YTS-tasolta alkaen selkeät, vaikka yhteensovittamisessa on edelleen haasteita. Suomessa on vahva huoltovarmuustyön perinne ja kehittynyt yhteiskunta, jossa luotetaan sekä valtiohallintoon että verkkoympäristön toimivuuteen ja luotettavuuteen. Meillä on hyvää teknistä osaamista, vaikka osaamismassa onkin pieni. Etuna on myös innovatiivinen digiyhteiskunta. Lisäksi vahvuutena mainittiin Kyberturvallisuuskeskuksen vahva osaaminen sekä Suomen luotettu ja neutraali, kansainvälisesti verkottunut asema.

# 4. SUOMEN KYBERTURVALLISUUDEN NYKYTILA YKSITYISELLÄ SEKTORILLA

## 4.1 Johdanto

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu lähtökohdiltaan luotettavasta kansallisesta sähkövoimajärjestelmästä. Tämän lisäksi luotettavuus muodostuu organisaatioiden välisistä toimivista tiedonsiirtoverkostoista sekä palvelutason yritysten järjestelmien tiedon käytettävyydestä, luotettavuudesta ja eheydestä kybertoimintaympäristössä, jonka turvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti kasvattavat.

Tämä luku käsittelee tutkimustuloksia, jotka perustuvat tutkimusmenetelmänä käytettyyn SWOT-analyysiin. Tutkimusmenetelmän avulla on pyritty löytämään ne yrityskohtaiset tiedot ja kansallisen kyberturvallisuuden vaikutustekijät, joilla voidaan vastata tutkimukselle asetettuihin kysymyksiin.

Kohdeorganisaatiot (16 organisaatiota, 7 eri toimialaa) valittiin kriittisen infrastruktuurin yrityksistä (vast.) ja niille kyberturvallisuustuotteita ja -palveluja toimittavista tietoturvayrityksistä. Kohteiden valinnalla pyrittiin kaksisuuntaiseen tiedon hankintaan tutkimusalueesta ja siten hyvään tutkimuksen luotettavuuteen.

## 4.2 SWOT-analyysin soveltaminen yrityksen kybertoimintaympäristöön

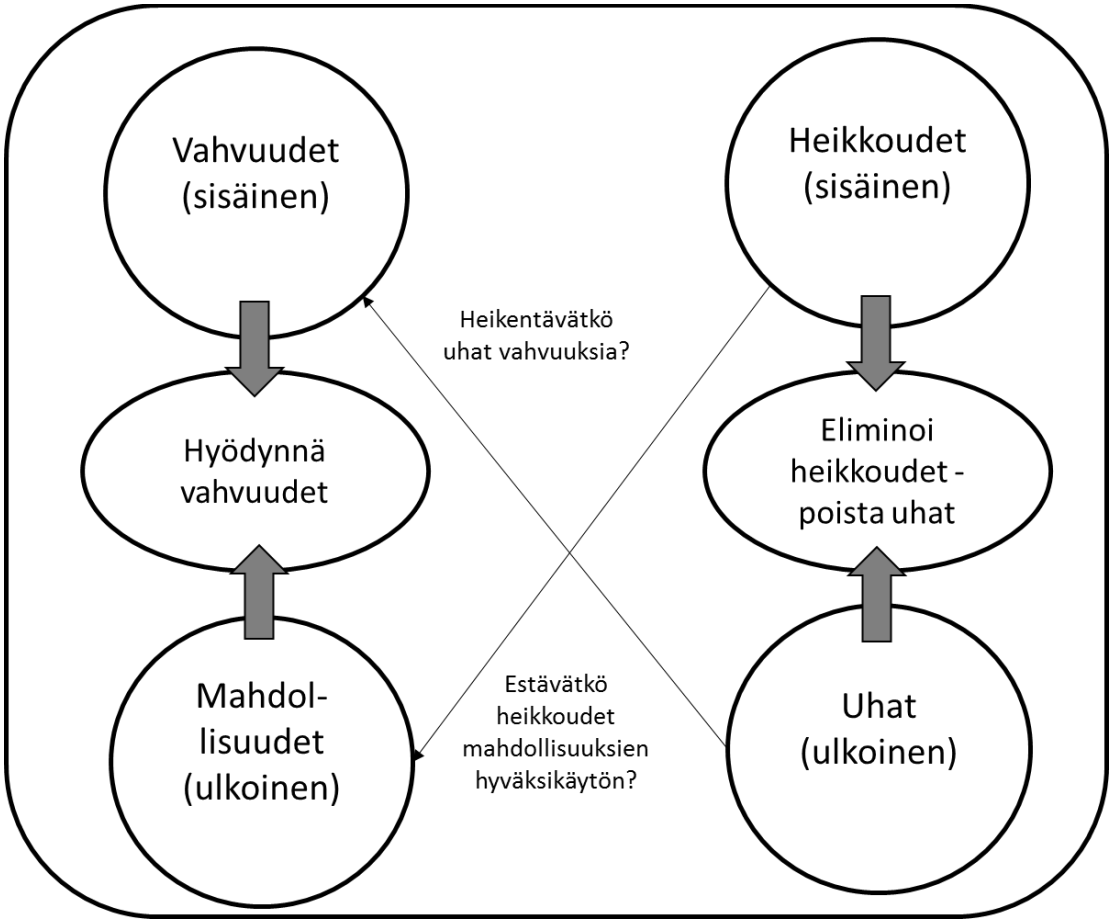
### 4.2.1 SWOT-analyysi

SWOT-lyhenne tulee englannin kielisistä sanoista Strengths (vahvuudet), Weaknesses (heikkoudet), Opportunities (mahdollisuudet) ja Threats (uhat). SWOT-analyysi on tärkeä väline analysoitaessa organisaation toimintakykyä ja sen toimintaympäristöä kokonaisuutena. Se on nelikenttämenetelmä, jota käytetään yleensä yrityksen strategianlaatimisessa, sekä oppimisen tai ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. SWOT-analyysin kohteena voi olla jonkin yrityksen toiminto, organisaatio koko laajuudessaan tai jonkin tuotteen tai palvelun asema ja kilpailukyky tai esimerkiksi kilpailijan toiminta ja kilpailukyky.

SWOT-analyysi on kahden ulottuvuuden kuvaama nelikenttä. Kaavion vasempaan puoliskoon kuvataan myönteiset ja oikeaan puoliskoon negatiiviset asiat. Kaavion yläpuoliskoon kuvataan organisaation sisäiset asiat ja alapuoliskoon ulkoiset asiat. Tämän jälkeen SWOT-analyysin pohjalta voidaan tehdä päätelmiä miten vahvuuksia voidaan käyttää hyväksi, miten heikkoudet muutetaan vahvuuksiksi, miten tulevaisuuden mahdollisuuksia hyödynnetään ja miten uhat vältetään. Tuloksena saadaan toimintasuunnitelma siitä, mitä millekin asialle pitää tehdä.[20]

Kuvassa 1 on esitetty edellä kuvatut nelikenttäanalyysin eri osien riippuvuussuhteet.

[20] Melkman, Simmonds, 2016




Kuva 1. Nelikenttäanalyysin eri osien riippuvuussuhteet[21]

SWOT-analyysin jaoteltu sisäisiin ja ulkoisiin tekijöihin voidaan toteuttaa kybertoimintaympäristössä esimerkiksi seuraavasti:

- Vahvuudet ja heikkoudet ovat sisäisiä tekijöitä. Organisaation vahvuus voi olla esimerkiksi hyvät toimintaedellytykset kybertoimintaympäristössä ja maine luotettavana toimijana toimintaympäristön haasteista huolimatta. Heikkous puolestaan voi olla organisaation kyvyttömyys tunnistaa toimintaansa osana yrityksen verkottunutta toimintaympäristöä tai puutteet toiminnan varmistamisessa toimintaympäristön asettamissa vaateissa.

- Mahdollisuudet ja uhat ovat ulkoisia tekijöitä. Mahdollisuus voi olla esimerkiksi yrityksen vaikutusmahdollisuus kyberluottamusta lisääviin toimenpiteisiin ulkopuolisia resursseja hyväksi käyttäen. Uhka voi puolestaan muodostua siitä, että yritys ei tunnista toimintaympäristönsä kyberturvallisuuden haasteita ja yrityksen ulkopuolelta uhkaavia tietomurtoja.

### 4.2.2 SWOT-analyysi teemat

Kattava yrityksen kyberturvallisuuden analysointi toteutettiin siten, että tarkastelun näkökulmat ulotettiin organisaation strategiaan, operatiivisiin toimiin, teknillis-taktisen tason ratkaisuihin ja kyvykkyystekijöihin huomioiden tutkimuskohteen kyberrakenne ja toiminta osana verkottunutta yhteiskuntaa. Näkökulmat huomioiden kyberturvallisuuden vahvuuksien ja heikko-

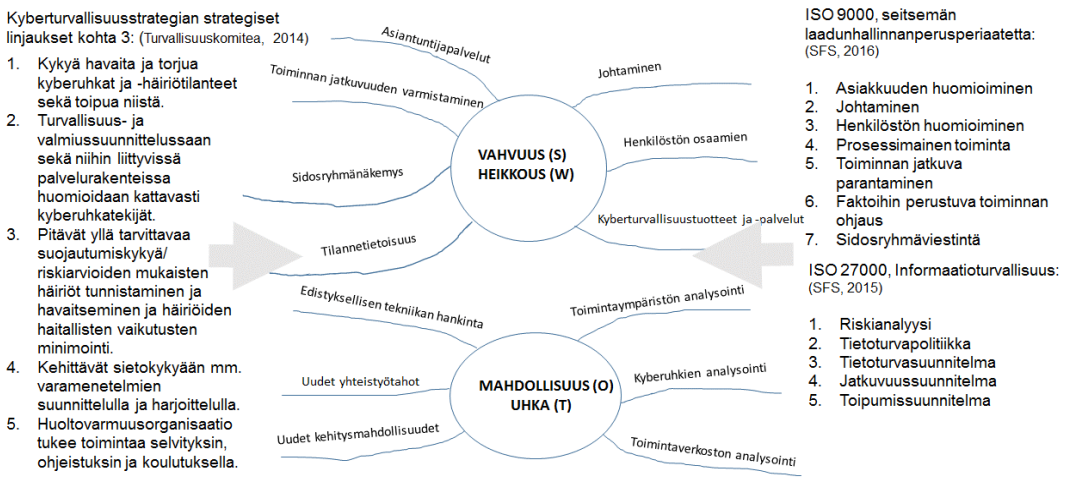
[21] Ibid.

uksien analysointi voidaan suorittaa niiden keskinäistä suhdetta arvioimalla. Mahdollisuuksien ja uhkien arvioinnin keskeisin tekijä on organisaation toimintaympäristön muutos; tässä tutkimuksessa kybertoimintaympäristö. Mahdollisuuksien arviointi liittyy tällöin yrityksen mahdollisuuteen hyödyntää muutosta tukevia toimenpiteitä parantaakseen toimintamahdollisuuksiaan. Uhkien arviointiin puolestaan liittyvät toimintaympäristö- ja uhka-analyysit, joiden perusteella toimenpiteet voidaan kohdistaa niiden pienentämiseen.

Tutkimuksessa kohdeyritys käytettiin hyväksi Huoltovarmuuskeskuksen näkemystä kyberturvallisuuden rakentamista verkottumalla. Viitekehyksessä yritys tai organisaatio sijoittuu toimialalle esim. energia-ala. Yhteistoiminta käsittää yritysten välisen toimialariippumattoman yhteistoiminnan lisäksi yhteistoiminnan Kyberturvallisuuskeskuksen kanssa. Toiminnan tukeen liittyvät kyberturvallisuusyritysten antamat palvelut ja korkeakouluilta saatava tutkimuksellinen ja koulutuksellinen tuki. Normistoon kuuluvat erilaisen sääntelyn lisäksi parhaat käytännöt vast. Kansainvälinen toimintakenttä koostuu kansainvälisen yhteistoiminnan lisäksi mm. globaaleista logistiikkaverkostoista ja maksuliikennejärjestelmistä. Viitekehys on esitetty kuvassa 2.


Kuva 2. Kyberturvallisuutta edistävä verkottunut toimintaympäristö (Huoltovarmuuskeskus)

Tutkimuksen SWOT-analyysin teemat on johdettu Suomen kyberturvallisstrategian strategisten linjausten kohdan 3 yritystoimintaa käsittelevästä kokonaisuudesta. Lisäksi teemojen laadinnassa on hyödynnetty ISO 9000-laatustandardin seitsemää perusperiaatetta ja ISO 27000-informaatioturvallisuuden standardin keskeisimpiä pääkohtia. Kuvassa 3 on esitetty teemojen johtamisen lähtökohdat ja teemat SWOT-analyysin pääkohtiin liittyen.




Kuva 3. Viitetutkimuksen SWOT-analyysin haastattelun teemat.

## 4.3 Tutkimustulokset

Haastattelujen perusteella teemoista on tehty taulukon 3 ja taulukon 4 mukaiset yhteenvedot. Taulukoissa SWOT-analyysin tulokset ovat ryhmiteltyinä haastatteluteemojen mukaisesti.

Taulukko 3. SWOT-analyysin vahvuudet ja heikkoudet

| | **VAHVUUDET**<br>**Positiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** | **HEIKKOUDET**<br>**Negatiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** |
|---|---|---|
| SISÄISET | **Johtaminen:**<br>- kyberturvallisuus huomioitu strategisena tavoitteena, politiikka usein julkaistu<br>- tärkeimmät uhat tunnistettu, riskiperusteinen, osana kokonaisturvallisuutta ja liiketoimintaa<br>- toimenpiteitä priorisoitu<br><br>**Tilannekuva:**<br>- uhkatiedot saadaan usein toimintaverkostosta ja kumppaneilta suoraan<br>- Kyberturvallisuuskeskuksen tiedotteet<br>- joissakin yrityksissä H24/7 valvonta | **Johtaminen:**<br>- politiikan jalkautus läpi organisaation usein haastavaa<br>- vaativimmat uhkakuvat tunnistamatta<br>- toiminta reagoivaa<br>- henkilöstön roolitus usein haastavaa, informaatioturvallisuudesta vastaavan (CISO) edustus puuttuu johtoryhmästä<br>- kuntataustaisten yritysten henkilöresursoinnin puutteet<br><br>**Tilannekuva:**<br>- yleistilanne muodostettava hajallaan olevista tiedoista<br>- toimintaverkoston tilannekuvan muodostaminen vaikeaa<br>- ei reaaliaikaista tilannekuvaa IT-varannoista eikä automaatiosta (ICS) |

| | | |
|---|---|---|
| | **Henkilöstön osaaminen:**<br><br>- IT-henkilöstöllä hyvää osaamista<br>- muulle henkilöstölle annetaan usein koulutusta verkossa<br>- osaamisen todentaminen mm. terveydenhuollossa<br>- web-seminaarit, infokanava tiedon jakelukanavina<br><br>**Tuotteet ja palvelut:**<br><br>- parhaat tuotteet käytössä<br>- palveluissa hyvä osaaminen<br>- ulkoistettuna ostopalveluna, osin hajautettu riskiperusteisesti<br>- työasemat usein omana palveluna, mikä sopii ”tavanomaisiin” uhkiin<br><br>**Sidosryhmät:**<br><br>- ulkoistuksissa parhaat kumppanit<br>- toimialayhteistyö; mm. energiayhtiöt, ERVA-alue<br>- PPP-yhteistyö, mm. HVK-poolit<br>- kansainvälinen yhteistyö<br>- yrityksissä usein hyvä maine sidosryhmien piirissä<br><br>**Asiantuntijapalvelut:**<br><br>- erilaiset auditointikäytänteet käytössä<br>- ongelmatilanteiden selvittämisessä käytetään alan asiantuntijoita<br>- ISO 27000, KATAKRI, HUOVI<br>- parhaat käytänteet käytössä<br>- tutkimusohjelmat, joissa osa yrityksistä mukana<br><br>**Jatkuvuuden varmistaminen:**<br><br>- harjoitustoimintaa, suunnitteluharjoituksia sekä HVK:n ja JAMK:n järjestämiä harjoituksia<br>- varautumissuunnitelmia laadittu | **Henkilöstön osaaminen:**<br><br>- koko henkilöstön kouluttaminen haastavaa<br>- kansallisesti syväosaaminen harvojen käsissä, laajat häiriöt haastavia hoitaa<br>- kuntataustaisissa yrityksissä osaaminen harvojen käsissä (resursointi)<br>- IT/ICS-kokonaisuuden osaaminen<br><br>**Tuotteet ja palvelut:**<br><br>- kumppanuusverkoston toiminnan auditointi haastavaa<br>- puutteellinen näkymä palvelujen suojaukseen (mm. pilvipalvelut)<br>- yrityskeskittymät kriittisessä infrastruktuurissa<br>- kattavan tunnistautumisen puute<br><br>**Sidosryhmät:**<br><br>- osalla toimialoista toimialayhteistyömahdollisuuden puute<br>- liiketoiminnan ja kansallisen huoltovarmuuden yhteensovittaminen (resursointivastuu)<br><br>**Asiantuntijapalvelut:**<br><br>- auditoinnin kattavuus läpi koko toiminnan ja ohjelmistojen toimintaan/palveluun puutteellista<br>- koulutuspalvelujen saatavuudessa haasteita<br>- PPP-yhteydenpito voi olla haastavaa häiriötilanteissa<br>- yritysten omaehtoinen tutkimustoimintaa on vähentynyt |

Taulukko 4. SWOT-analyysin mahdollisuudet ja uhkat

| | **MAHDOLLISUUDET**<br>**Lista mahdollisuuksista, jotka lisäävät kyberluottamusta** | **UHKAT**<br>**Lista uhkatekijöistä, jotka vaikuttavat kyberluottamukseen** |
|---|---|---|
| ULKOISET | **Edistyksellisen tekniikan hankinta:**<br><br>- mahdollisuus investoida uuteen tekniikkaan; erityisesti isoissa yrityksissä<br><br>**Uudet yhteistyötahot:**<br><br>- PPP-toiminnasta kilpailuetua<br>- yhtenäisen tilannekuvan muodostaminen<br>- nykyistä laajemman toimialayhteistyön mahdollisuudet<br><br>**Uudet kehitysmahdollisuudet:**<br><br>- tiedustelulaki ja sen muodostamat toimintaedellytykset<br>- koulutuksen jatkokehittäminen<br>- benchmarking-toiminta<br>- auditointitoiminnan kehittäminen<br>- hallittu regulaatio (toimintojen harmonisointi) | **Toimintaympäristön analysointi:**<br><br>- tuntemattomat uhkatekijät ja tietomurrot<br>- uudet liiketoimintamallit; edellyttävät uusien tekniikoiden käyttöönottoa (esim. IOT, robotiikka), joiden mukanaan tuomaa uhkakuvaa ei tunneta riittävästi<br><br>**Kyberuhkien analysointi:**<br><br>- haasteena teollisuusvakoilu ja valtiollisten toimijoiden kyvykkyys<br>- terrorismi; kyberfyysinen vaikuttaminen sähköverkkoon, vesihuoltoon ja terveydenhuollon järjestelmiin sekä lääkevalmistukseen ja biopankkiin<br>- pysyykö ohjelmistokehitys uhkien mukana; vanhentunutta suojaustekniikka käytössä<br>- henkilöstöriskit, sisäpiiriläiset<br>- avainhenkilöstöön kohdistuvat uhat<br>- kyberuhat keskittyneisiin palveluihin<br><br>**Toimintaverkoston analysointi:**<br><br>- ei näkymää verkostoon ja sen riippuvuussuhteisiin<br>- toimintaverkoston pullonkaulat; kriittisessä infrastruktuurissa samoja yrityksiä merkittävässä asemassa<br>- resurssikapeikot laajojen häiriöiden tilanteessa<br>- osaamisen katoaminen ulkoistetuissa palveluissa; ylikansallinen yhtiö, saneeraukset taloudellisista syistä, joista seuraa osaamisen katoaminen |

## 4.4 Johtopäätökset

### 4.4.1 Yleistä

Yleisten haittaohjelmien aiheuttamien uhkien osalta suojaustoimenpiteet ovat hallinnollisesti ja teknillisesti koko tutkimusalueen osalta kohtalaisen hyvällä tasolla. Sähkövoimajärjestelmän toimintaa valvotaan jatkuvalla seurannalla ja tiedonsiirtoverkkojen puhtauteen luotetaan. Näiltä osin myös teknilliset suojaustoimenpiteet ovat hyvällä tasolla. Kansallinen sähkövoimajärjestelmä ja tiedonsiirtoverkko toimivat perustana koko kriittiselle infrastruktuurille ja sen palveluille.

Kansallinen eri viranomaisten ja kriittisen infrastruktuurin yritysten tiivistä ja toimivaa yhteistyötä pidetään kansallisena vahvuutena. Tutkimuskohteiden kyberturvallisuuden erityisosaaminen on hyvällä tasolla, joskin toiminnan näkökulmasta se on aliresursoitu. Yritykset ovatkin laajasti ulkoistaneet IT-toimintojaan hyödyntääkseen parhaita saatavilla olevia tuotteita ja palveluja sekä varmistaakseen niiden käytettävyyden. Merkittävimmillä kriittisen infrastruktuurin yrityksillä on lisäksi kansainvälistä yhteistoimintaa tilannekuvan muodostamisessa, mitä pidetään ehdottomana edellytyksenä ennakoivalle toiminnalle.

Edistyksellisten haittaohjelmien aiheuttamien kyberuhkien osalta yritysten tilannekuva on yleisten haittaohjelmien uhkakuvaa haastavampi. Varautuminen näiltä osin edellyttää erityisen tiivistä viranomaisten ja yritysten välistä yhteistyötä. Onnistuneen toiminnan edellytyksenä on viranomaisten nykyistä paremmat toimintavaltuudet. Kokonaisturvallisuuden osalta on huomioitava myös terrorismin kyberturvallisuusuhat esimerkiksi vesihuoltoon tai terveydenhuollon järjestelmiin, lääkevalmistukseen tai biopankkiin. Suomi on edelläkävijämaa viranomaisten ja yritysten välisessä yhteistoiminnassa (PPP-toiminta), joka osaltaan parantaa merkittävästi koko yhteiskunnan resilienssiä kybertoimintaympäristössä.

### 4.4.2 Kyberturvallisuusstrategian linjausten toteutuminen

Kyberturvallisuusstrategian linjausten kohta kolme on erityisesti suunnattu yritystoimintaan. Haastattelujen perusteella voidaan todeta, että kohdeyritysten toiminta on edelleen reaktiivista, mutta merkittäviä edistysaskelia kohti proaktiivista toimintaa on otettu kaikilla päätöksentekotasoilla. Johtaminen on laajasti strategia- ja riskiperusteista, asiat huomioidaan melko hyvin yritysten toimintapolitiikoissa. Tilannekuvan luomisessa ja toiminnan kehittämisessä toimitaan verkottuneesti ja erityisesti energia-alalla toimialayhteistyössä. Varautumissuunnitelmia on tehty ja niitä on harjoiteltu. Varautumissuunnittelusta on huolehdittu erityisesti sähkövoimajärjestelmän ja tiedonsiirtoverkkojen osalta. Riskitarkastelua ja varautumissuunnittelua ollaan liittämässä liiketoimintayksiköiden vastuulle ja siten parannetaan toiminnan ja siihen liittyvien uhkatekijöiden yhteyttä. Harjoittelutoimintaa erityisesti Huoltovarmuuskeskuksen johdolla pidetään tärkeänä ja hyvänä toiminnan kehittämismahdollisuutena.

Kyberturvallisuusstrategian toimeenpano-ohjelman listaamista toimenpiteistä kohdat 73 ja 74 kohdistuvat suoranaisesti yritystoimintaan. Toimenpiteitä on kehitetty Cyber Trust ja KYBERTEO-tutkimusohjelmissa, joissa on mukana merkittäviä yrityksiä kriittisen infrastruktuurin osalta. Tutkimustoiminnan ylläpitäminen on tärkeää monestakin näkökulmasta katsottuna. Yritysten taholta siltä edellytetään konkreettisia tuloksia toiminnan kehittämiseen etenkin nykyisessä tilanteessa, jossa yritysten omaehtoinen tutkimustoiminta on vähentynyt aiemmista vuosista. Yritykset ovat myös omalta osaltaan kohtalaisen sitoutuneita osallistumaan tutkimustoimintaan.

Tässä tutkimuksessa tunnistettiin kattavasti yrityksissä toteutettuja strategisia linjauksia edistäviä toimenpiteitä. Niiksi voidaan lukea mm. riskiperusteinen johtaminen, henkilöstön koulutusohjelmat, parhaiten saatavilla olevien tuotteiden ja palvelujen käyttö suojaustoimenpiteinä, yhteistyöverkostot ja asiantuntijapalvelut, kuten auditointipalvelut ja harjoittelu. Lisäksi joillakin organisaatioilla oli käytössä H24/7-valvomoita ja hälytysmenettelyt nopean vasteen aikaan saamiseksi häiriötapahtumiin.

### 4.4.3 Kyberturvallisuusstrategian linjausten toteutumisen haasteet

Yritysten ennakoivien toimenpiteiden suunnittelu perustuu monelta osin toimintaverkostosta saatavan kokonaistilannekuvan hyödyntämiseen. Se on tyypillisesti koottava useista eri lähteistä ja on siten riippuvainen kyseisen yrityksen kyvystä verkottua toimialalla tai laajemmin. Erityisenä haasteena on edistyksellisten uhkien, kuten teollisuusvakoilu ja valtiollisten toimijoiden mahdollisesti aiheuttamien uhkien tunnistaminen.

Myös linjausten toteutumisen osalta merkittäviä haasteita muodostuvat yritysten tai organisaatioiden eritasoiset mahdollisuudet toimintansa kehittämiseen. Isoissa yrityksissä edellytykset kattavaan toiminnan kehittämiseen ja ylläpitämiseen ovat huomattavasti pieniä organisaatioita parempia. Useat tutkimuksen kohdeyritykset olivat tästä toiminnan kehittämisen ja ylläpidon eritasoisesta kehityskulusta huolissaan. Monet pienemmät toimijat voivat olla merkittävässä roolissa isompien yritysten toimitusverkostossa. Osassa kriittisen infrastruktuurin yrityksiä perinteistä tietoturvaa kattavammat suojaustoimenpiteet ovat vasta käynnistymässä. Myös toimenpiteiden resursoinneissa on eroja. Kuntataustaiset organisaatiot ovat tutkimuksessa mukana olleita isoimpia yrityksiä jäljessä kehityksessä.

Edellä esitetty huoli eri toimijoiden epätasaisesta mahdollisuudesta kehittää toimintaansa näkyy myös ketjutetuissa palveluissa, jotka voidaan kokea haasteeksi yrityksissä, vaikka omat toimenpiteet olisivat jo melko hyvin kehittyneet. Näkyvyyttä ketjun eri osiin ei ole helposti saatavilla, jolloin herää kysymys sen osien kyberturvallisuuden kyvykkyydestä. Tätä näkökulmaa tukevat aiemmat tutkimukset mm. pk-yritysten kyberuhkien tunnistamisesta.

Kuten edellä on todettu yritysten ja niiden käyttämien kyberturvallisuuspalvelujen sekä laajemminkin kansallinen erityisosaaminen on hyvää tasoa, mutta se on harvojen käsissä, joten kyberturvallisuuden koulutuksen edelleen kehittämistä ja koulutuspohjan laajentamista kaikilla tasoilla pidetään tutkimuskohteiden osalta erittäin tärkeänä.

### 4.4.4 Kyberturvallisuusstrategian linjausten hyödyt ja toteutuminen jatkossa

Nykyisiä perusjärjestelyjä pidetään tarkoituksenmukaisina ja toimijoiden kyvykkyyksiä hyvinä, joten kansallisella järjestelmällä on hyvät edellytykset estää, rajoittaa ja toipua perinteisistä kyberhyökkäyksistä. Viranomaisyhteistyö ja viranomaisten ja yksityisen sektorin yhteistyö sekä varautuminen kyberturvallisuusriskien ja ennakoimattomien tapahtumien hallintaan muodostavat toiminnan resilienssin. Näistä kyvykkyyksistä huolehtiminen antaa perustan muille toimenpiteille.

Kyberturvallisuuskeskuksen toimintaa pidetiin erityisen merkittävänä, samoin kuin muitakin verkostoitumien muotoja, kuten toimialaverkostot ja kansainvälinen yhteistyö. Kansainvälisiä yhteyksiä kaikilla eri tasoilla pidetään erityisen tärkeinä.

Kyberturvallisuuden tutkimustoiminta ja sen kehittäminen ovat tärkeitä erityisesti siksi, että yritykset ovat vähentäneet omaa tutkimustoimintaansa. Koulutuksen kehittäminen kaikilla sen tasoilla edistää organisaatioiden osaamisen ja kyvykkyyksien kehittymistä. Eri tasoilla tarvi-

taan soveltavaa koulutusta kyberturvallisuuden huomioimiseksi koulutusohjelmissa. Tutkimuksessa tuli esille erityisesti ohjelmistokoulutuksen kehittämistarve. Lisäksi perinteisen IT-osaamisen ja teollisuusautomaatio-osaamisen integraation tarve tulee huomioida yliopisto- ja ammatillisen koulutuksen kehittämisessä.

Huoltovarmuuskeskuksen ja Jyväskylän Ammattikorkeakoulun järjestämät harjoitusmahdollisuudet tulivat positiivisesti esille tutkimuksessa. Niitä pidettiin hyvin tarpeellisina tulevaisuudessa.

Useat keskeiset kriittisen infrastruktuurin yritykset ovat ulkoistaneet tietoliikennettään, IT-palvelujaan ja sitä kautta myös osan oman kyberturvallisuuden hallinnastaan. Tässä verkostossa on sekä kotimaisia että ulkomaalaisia yrityksiä. Kotimaisten yritysten osalta tutkimuksessa tunnistettiin verkoston solmukohtia, joiden merkitystä resursoinnin kannalta tulee jatkossa selvittää.

Kotimaisten tietoturvayritysten osaaminen on haittaohjelmien muodostamien uhkien osalta korkealla tasolla, mutta tutkimuksessa esitettiin epäilyjä kansallisten resurssien riittävyydestä kyberhyökkäysten aiheuttamien laajojen häiriötilanteiden tapauksissa.

### 4.4.5 Jatkotoimenpiteet

Edellä kuvatulla tavalla muodostettu yrityksen kyberturvallisuuden tilannetietoisuuden muodostaminen SWOT-analyysin avulla mahdollistaa strategisten, operatiivisten ja teknillis-taktisen tason toimenpiteiden tarkastelun. Niiden hallinta on keskeisessä roolissa, kun kehitetään koko organisaation toimintaa ja sitä kautta koko kansallisen kriittisen infrastruktuurin toimintakykyä.

Yrityssektorin näkökulmasta esitetään seuraavat jatkotoimenpiteet:

1. Vahvistetaan ja keskitetään kansallista kyberturvallisuuden strategista johtamista ja tilannekuvan kokoamista ja jakamista kriittisen infrastruktuurin toimijoiden käyttöön (myös muut toimijat hyötyvät).

2. Tiedustelulaki tulee saada voimaan (riittävät toimivaltuudet viranomaisille).

3. Vahvistetaan kansallista yhteistyötä viranomaisten kesken ja vahvistetaan verkostoitumista yritysmaailman kanssa (PPP-yhteistyö). Rohkaistaan yrityksiä toimialayhteistyöhön tilannetietoisuuden parantamiseksi (benchmarking-toiminta). Selvitetään mahdollisuudet pk-yritysten osallistumisesta alansa toimialayhteistyöhön ja toimintansa kehittämiseen

4. Pidetään yllä vahvaa kansainvälistä yhteistyötä eri foorumeilla.

5. Edellytetään kriittisen infrastruktuurin yrityksiltä aiempaa proaktiivisempaa kyberturvallisuuden johtamista ja hallintaa. Rohkaistaan toimenpiteisiin kaikilla päätöksentekotasoilla ja kyberturvallisuutta edistävän kyvykkyyden vahvistamiseen. Yrityksen vahvuuksina: strategia, työkalut (politiikka, tuotteet ja palvelut, varautumissuunnitelmat, verkostot), koulutus ja vakuuttaminen.

6. Kehitetään kyberturvallisuuden systeemiajattelua; prosessit ovat verkostossa, tieto keskiöön, verkoston osat huolehtivat omasta osastaan, solmut pitävät itsensä verkoston osina, toiminnassa yhteinen kyberturvallisuuden intressi, resilienssi ydinalueille. Toiminnan avain on jatkuva ja tiivis informaation vaihto.

7. Kehitetään koulutusta ja tutkimustoimintaa; kehitetään yliopisto- ja korkeakouluyhteistyötä ja tutkimusohjelmia, kehitetään koulutusohjelmien sisältöjä mm. ohjelmoinnin osalta ja perinteisen IT-osaamisen ja teollisuusautomaatio-osaamisen integraation osalta, lisätään kohdennettua koulutustarjontaa (mm. päättäjille), lisätään ammatilliseen toisen asteen koulutukseen kyberturvallisuuden edellyttämiä osioita, parannetaan kyberturvallisuuden osaamista kansalaistaitona mm. perusopetuksessa.

8. Kehitetään auditointitoimintaa aiempaa kattavammaksi; toiminta, palvelu tuote. Kehitetään standardointia KATAKRI- ja ISO 27000-standardien pohjalta tukemaan auditointitoimintaa; osaksi yrityksen ja organisaation koko toiminnan johtamista. Selvitetään uuden standardin tarpeellisuus kyberturvallisille kulutushyödykkeille.

9. Kehitetään tuotteita ja palveluja jatkuvasti uhkakuvia vasten. Käytetään tarvittaessa regulaatiota toimenpiteiden harmonisoimiseksi eri organisaatioiden kesken. Selvitetään yrityskohtaisen ja reaaliaikaisen IT-infrastruktuurin tilannekuvajärjestelmän rakentamismahdollisuuksia.

10. Tiivistetään kriittisen infrastruktuurin käsitettä oheisen kuvan 4 mukaiseksi tehokkaiden ja tarkoituksenmukaisimpien toimenpiteiden kohdistamiseksi sen eri tasoille. Kohdistetaan siihen ainakin seuraavat toimenpiteet tavoitteena kansallisen jatkuvuuden hallinnan kehittäminen:

    - Kartoitetaan sähköverkon haavoittuvuudet
    - Selvitetään Kyberturvallisuuskeskuksen mahdollisuudet palvella suoraan kriittisen infrastruktuurin toimijoita
    - Selvitetään TUVE-verkon käyttömahdollisuudet kriittisten toimintojen osalta
    - Selvitetään tiedonsiirto- ja palvelukerrokseen keskittyneiden palveluiden pullonkaulat ja niiden vaikutukset
    - Kehitetään kyberturvallisuuden järjestelyjä ja suojaustekniikoita palveluihin (mm. pilvipalvelut, IoT- ja robotiikkaympäristöt)
    - Kehitetään yritysten IT-tekniikoiden ja teollisuusautomaatiotekniikoiden yhteistoimintaa hallinnollisesti ja teknillisesti


Kuva 4. Kriittisen infrastruktuurin pelkistetty rakenne.

# 5. KANSAINVÄLINEN SUORITUSKYKYANALYYSI

## 5.1 Johdanto

### 5.1.1 Tutkimuskysymys ja -tehtävät

Tutkimusraportin kansainvälisen suorituskykyanalyysin tarkoitus on vastata kysymykseen: *Kuinka Suomen kyberturvallisuuden nykytila suhteutuu keskeisiin vertailumaihin verrattuna?* Tavoitteena on tuottaa analyysi vertaismaiden kybersuorituskyvystä ja sen kehittämisestä, jonka tuloksena syntyy: 1) vertaileva analyysi kansainvälisistä kyberturvallisuusstrategioista ja 2) tarkempi tilannekuva kyberturvallisuuden suorituskyvystä verrokkimaissa. Tämän luvun painopiste on valittujen maiden kyberstrategioiden vertaisanalyysissa.

### 5.1.2 Tutkimuksen viitekehys[22]

Kansainvälisesti ei ole sovittu mittaristoa valtioiden kyberkyvykkyyden arvioimiseksi, mutta eri tutkimuslaitokset sekä kansalliset ja kansainväliset organisaatiot ovat kehittäneet omia analyysityökalujaan. Tutkimusprosessin alkuvaiheessa käytiin läpi jo käytössä olevia suorituskykymittareita sopivan viitekehyksen luomiseksi. Esimerkiksi:

International Institute for Strategic Studies käyttää seitsemää laaja-alaista mittaria Military Balance -julkaisussaan: poliittinen, sotilaallinen, taloudellinen ja sosiaalinen ympäristö, (tieto)tekninen ja infrastruktuurin kehittyneisyys sekä ”muut tekijät”.

Yhdysvaltojen asevoimien puolustushaarojen yhteisoperaatioiden suunnittelussa käytetään DOTMLPF-mallinnusta (sotilasoppi, organisaatio, koulutus, käytettävissä oleva laitteet ja järjestelmät, johtaminen ja koulutus, henkilöstö sekä käytettävissä olevat tilat). Mallinnuksen versio, jossa mittaristoon on lisätty yhteistoimintakyky ja informaatio, on käytössä kybertoimintakyvyn arvioinnissa.

Euroopan Unionin käyttämä mittaristo keskittyy kyberturvallisuuden lainsäädännölliseen perustaan, operatiivisiin kykyihin, julkinen–yksityinen kumppanuuksiin, alakohtaisiin kyberturvallisuussuunnitelmiin ja koulutukseen.

Kansainvälisen televiestintäliiton (ITU) ja ABI Researchin ”globaali kyberturvallisuusindeksi” (GCI) käyttää viittä mittaria: lainsäädäntö, tekninen kyky, organisaatiot, toimintakyvyn rakentaminen ja kansainvälinen yhteistyö. Indeksoinnissa ei oteta kantaa toimenpiteiden onnistuneisuuteen tai vaikuttavuuteen vaan listataan tehdyt toimenpiteet.

ITU:n ja ABI:n indeksointi toimii myös tämän tutkimuksen taustakehyksenä. Maakohtaisten analyysien yhteydessä mainitaan kunkin maan GCI-luku, minkä lisäksi tutkimuksessa käytetty analyysikehys on rakennettu indeksin perustalle. Numeerisen arvioinnin sijaan tutkimuksessa keskitytään kuvailemaan kyberturvallisuuden nykytasoa tutkituissa maissa tehtävän strategiatyön kautta ja nostamaan esiin hyviä käytäntöjä, joita Suomen kyberturvallisuusstrategian toimintaohjelman päivityksessä voisi hyödyntää.

Tutkimuksessa kyberturvallisuutta tarkastellaan kuudella osa-alueella[23].

[22] Kappaleen teksti pohjautuu Martti Lehdon ja Jarno Limnéllin konferenssipaperiin ”Cyber Security Capability and Case Finland”.

1. Lainsäädäntö
2. Tekninen valmius
3. Organisaatiot
4. Yhteistyö (kansallinen ja kansainvälinen)
5. Kybertoimintakyvyn rakentaminen (koulutus ja harjoitukset)
6. Sotilaallisen kyberkyvykkyyden kehittäminen

Tarkastelussa keskitytään ennen kaikkea lainsäädäntöön, organisaatioihin ja johtamiseen, kybertoimintakyvyn rakentamiseen sekä yhteistyöhön. Tekniseen valmiuteen ja sotilaalliseen kyberkykyyn viitataan silloin, kun näistä osa-alueista on ollut tietoa saatavilla ja kun tiedolla on katsottu olevan merkitystä kyberstrategioihin painottuneessa tutkimuksessa.

### 5.1.3 Vertailtavat maat

Kansainväliseen suorituskykyanalyysiin valittiin kuusi vertaismaata: Alankomaat, Iso-Britannia, Israel, Ruotsi, Singapore ja Viro. Valintaan vaikuttivat ensisijaisesti informaatioyhteiskunta-kehityksen vaihe ja arvioitu kyberturvallisuuden taso. Vertailuun haluttiin mukaan maat, jotka suurin piirtein vastaisivat Suomea edellä mainituilla osa-alueilla, vaikka informaatioyhteiskunnan rakentamisen ja sen toiminnan turvaamisen tavat olisivat erilaiset. Lisäksi haluttiin varmistaa, että vertailumaista olisi ”kotiutettavissa” hyviä käytäntöjä kyberturvallisuustoiminnan vahvistamiseksi Suomessa. Huomionarvoista on, että globaalissa kyberturvallisuusindeksissä kaikki vertaismaat sijoittuivat vuonna 2015 Suomen edelle (taulukko 5).

Taulukko 5: ITU:n GCI-indeksi ja sen mukainen järjestys

| **Valtio** | **GCI-indeksi** | **Rank** |
|---|---|---|
| Viro | 0,706 | 5 |
| UK | 0,706 | 5 |
| Israel | 0,676 | 6 |
| Alankomaat | 0,676 | 6 |
| Singapore | 0,676 | 6 |
| Ruotsi | 0,647 | 7 |
| Suomi | 0,618 | 8 |

Tutkimustehtävän mukaisesti ensin käytiin läpi kunkin vertailumaan tämänhetkinen voimassa oleva kyberturvallisuusstrategia (mikäli sellainen on olemassa) edellä mainittuja osa-alueita painottaen. Tämän jälkeen lokakuussa 2016 tehtiin neljä haastattelumatkaa (Alankomaat, Israel, Ruotsi ja Viro), joista kunkin aikana haastateltiin 2–3 keskeisissä kyberturvallisuustehtävissä toimivaa henkilöä. Singaporen osalta tehtiin ryhmähaastattelu Helsingissä. Iso-Britannian osalta keskityttiin vasta julkaistuun kyberturvallisuusstrategiaan, edelliseen strate-

[23] Haastatteluita varten osa-alueet käännettiin englanniksi (1) Regulatory framework (2) Technical capabilities (3) Organization and leadership (4) Capacity building (education and training) (5) National and international cooperation (5) Development of military capabilities.

giaan ja sen toimeenpanon seurantaraportteihin, sekä vuosien 2010 ja 2015 kansallisten turvallisuusstrategioiden kyberturvallisuutta käsitteleviin osioihin. Käytetty lähdemateriaali on listattu liitteessä 1.

## 5.2 Kyberstrategioiden vertaisanalyysi

### 5.2.1 Alankomaat

Alankomaiden GCI-luku on 0,676 ja sijoitus globaalissa vertailussa 6. Alankomaiden voimassa oleva kyberturvallisuusstrategia (NCSS2) on vuodelta 2014[24]. Se tuotettiin laajana julkisen ja yksityisen sektorin välisenä sidosryhmäyhteistyönä. Kyberturvallisuuden tilaa ja strategian toimeenpanoa on arvioitu vuosittaisessa kyberturvallisuusarviossa[25]. Vuonna 2017 julkaistavan NCSS3:n laatiminen on käynnissä.

Kyberturvallisuus kuuluu *Ministerie van Veiligheid en Justitien*[26] hallinnonalaan. Ministeriö tekee strategista suunnittelua ja strategian toimeenpanon hoitaa sen alaisuudessa toimiva *National Cyber Security Center (NCSC*). NCSC:n päävastuisiin kuuluvat CERT-toiminto, kyberuhkiin ja -hyökkäyksiin vastaaminen, kyberuhkien ja -trendien seuraaminen, kyberkriisinhallinta ja julkinen–yksityinen -yhteistyön koordinointi.

Alankomaiden nykyisen kyberstrategian ydin on selkeä visio kyberturvallisuuden tilasta sekä toimenpideohjelma määrittämässä niitä toimia, jolla vision toteuttamiseen pyritään. Strategia on vahvasti vapautta, ihmisoikeuksia, talouskasvua ja kansainvälistä yhteistyötä painottava. Alankomaat pyrkii strategian avulla profiloitumaan avoimena, läpinäkyvänä ja kasvuvetoisena kyberturvallisuuden huippumaana.

Kybertoimintaympäristöön liittyvää lainsäädäntöä on suhteellisen vähän. Yhteiskunnan elintärkeitä toimintoja ylläpitäviä yrityksiä velvoittaa vuonna 2016 voimaan tullut uusi laki tiedonantovelvollisuudesta[27]. Se on osa laajempaa julkinen–yksityinen -yhteistyön kehittämistä valtionhallinnon ja kriittisten yritysten välillä. Kyberturvallisuuden säädöspohjaan suunnitellaan laajennusta, mutta lainkohdat sisällytettäneen jo olemassa oleviin lakeihin. Muilta osin ilmoittaminen digitaalisista uhkista ja mahdollisista hyökkäyksistä perustuu vapaaehtoisuuteen.

Alankomaat on aktiivinen, sitoutunut toimija kansainvälisen yhteistyön ja erilaisten koalitioiden kehittämisessä. Esimerkiksi maan Euroopan neuvoston puheenjohtajuuskaudella 2016 kyberturvallisuus oli agendan tärkeimpiä asioita. Kansainvälistä yhteistyötä tehdään monipuolisesti multilateraalisilla foorumeilla sekä kahdenvälisesti.

Sotilaallinen ulottuvuus on NCSS2:ssa esillä vain mainintana tarpeesta siviili- ja sotilaspuolen yhteistyön parantamiseen. Puolustushallinto ja asevoimat vastaavat sotilaallisen kyberkyvykkyyden kehittämisestä (operatiivinen kyberpuolustus- ja hyökkäyskyky). Verrattuina muihin tutkittuihin maihin, Alankomaat on suhteellisen avoin sotilaallisen kybertoiminnan osalta[28]. Vuoden 2015 kyberpuolustusstrategia määrittelee seitsemän tavoitetta[29], joista yksi on sivii-

[24] Alankomaiden ensimmäinen kyberturvallisuusstrategia (NCSS1) julkaistiin vuonna 2011.

[25] Cyber Security Assessment Netherlands CSAN

[26] Turvallisuus- ja oikeusministeriö

[27] Government of the Netherlands (2016). Laki tiedonantovelvollisuudesta koskien digitaalisia tapahtumia on ensimmäinen puhtaasti kyberturvallisuutta käsittelevä laki.

[28] Alankomaiden puolustusministeriö on tuottanut julkiset hollanninkieliset kyberpuolustusstrategiat vuosina 2012 ja 2015.

[29] Tavoitteet ovat: (1) kyberammattilaisten sitouttaminen, (2) tehokas innovaatio- ja hankintatoiminta, (3) kansallisen ja kansainvälisen yhteistyön kehittäminen, (4) kybertietoisuuden kasvattaminen, (5) digitaalisen resilienssin vahvistaminen, (6) digitaalisen tiedustelun vahvistaminen ja (7) operaatioiden aikaisen kyber-toimintojen vahvistaminen (ml. kyberpuolustusdoktriinin kehittäminen).

liyhteistyön parantaminen. Solmukohtana yhteistyölle toimii NCSC, johon on sijoitettu myös asevoimien henkilöstöä. Asevoimiin perustettiin erillinen *Netherlands Defence Cyber Command* vuonna 2014.

NCSS1:n päätavoitteeksi määriteltiin digitaalisen yhteiskunnan turvallisuuden vahvistaminen. Tarkoitus oli kasvattaa niin kansalaisten kuin hallinnon ja yksityisen sektorin luottamusta ICT-järjestelmiin, luoda rakenteet kyberturvallisuuden kehittämiselle ja kehittää kybertietoisuutta. NCSS2 vie tavoitteet pidemmälle: rakenteet halutaan kehittää verkostomaisiksi ja tietoisuudesta edetään kyvykkyyksiin. Nykyisessä strategiassa on monitahoisempi visio kansainvälisiin kumppanuuksiin perustuvasta turvallisesta ja avoimesta digitaalisesta toimintaympäristöstä. NCSS2-strategia esittää kyberturvallisuuden vision kolme tärkeintä periaatetta niin sanottuna ”kyberturvallisuuden kolmiona”, jossa kolmion sivuille asettuvat turvallisuus, vapaus ja sosio-ekonomiset edut. Strategian tavoitteiden mukaan turvallisuuden, vapauden ja sosio-ekonomisten etujen tasapainon on tarkoitus toteutua eri toimijoiden välisessä kyberturvallisuusdialogissa niin kansallisesti kuin kansainvälisesti. Samaa arvopohjaa ja sääntöjä on seurattava niin fyysisessä kuin digitaalisessa ympäristössä.

Puutteena kyberstrategiassa kuitenkin on se, että nämä läpileikkaavaksi määritellyt pääperiaatteet eli kyberturvallisuuden kolmion -ideaali ei välity toimintasuunnitelmatasolle. Tulevassa strategiassa (NCSC3) kyberturvallisuuden visioon tai päämääriin ei ole tulossa suuria muutoksia. Sen sijaan toimeenpanosuunnitelmaa terävöitetään yleislinjan mukaiseksi, jotta linkki vision, tavoitteiden ja toimeenpanosuunnitelman välillä vahvistuu.

Kyberturvallisuuden kokonaisuutta on tarkoitus parantaa julkinen-yksityinen -yhteistyön kontekstissa. Strategian tavoitteen mukaan kumppanuudesta (*pp-partnership*) edetään pidemmälle, osallistumiseen (*pp-participation*). Esimerkiksi tilannekuvaa parantavat, sektorispesifit ISAC-keskukset[30] ovat yksi yhteistyön toimiva muoto.

Tulevassa strategiatyössä nähdään keskeisenä kaikkien toimijoiden yhteydenotto- ja ilmoituskynnyksen madaltaminen. Tavoitteena on verkostoperustaisen julkinen–yksityinen-yhteistyön kehittäminen luomalla koko maan kattava kyberturvallisuusverkosto. Yhteydenottokynnyksen madaltamista edistetään viemällä verkostoajattelu kaikille tasoille, niin alueelliselle kuin sektorikohtaiselle tasolle. Hajauttamisella uskotaan olevan vaikutus esim. pk-yritysten kyberturvallisuusajattelun aktivoimiseen. NCSC toimii valtakunnallisena pääkeskuksena, jonka alle alueverkosto järjestyy. Muutenkin NCSC:n rooli, koko ja resursointi kasvaa uuden strategian myötä.

Strategiatyössä kehittämisen ydinalueita ovat lisäksi sisäisen koordinaation parantaminen, julkisen rahoituksen kasvattaminen ja kyberturvallisuuden järjestäytymisen parantaminen. Tulevien tavoitteiden toteuttamiseen ei vielä ole korvamerkittyjä julkisia varoja. Alankomaissa tehdäänkin tällä hetkellä kahden eri rahoitusskenaarion mukaista suunnittelutyötä verkostovision toteuttamiseksi: ensimmäisessä skenaariossa julkisen rahoituksen taso on nostettu tarpeiden mukaiselle tasolle ja toisessa ei.

Alankomaiden mallista harkittavia toimintatapoja olisivat: (1) Julkinen-yksityinen -yhteistyön kehittäminen pidemmälle ja tiivistäminen. Alankomaissa toimii esimerkiksi vuonna 2012 perustettu *Cyber Security Raad (CSR*). Se on julkis-yksityinen strateginen neuvonantajaelin, joka ohjeistaa ja neuvoo valtionhallintoa ja arvioi kyberturvallisuuden tilaa tukien yhtä lailla julkisen kuin yksityisen sektorin tavoitteita.

[30] Information Sharing and Analysis Center (ISAC) ovat tiedonvaihtoon ja sektorikohtaisen tilannekuvat parantamiseen tarkoitettuja foorumeita. Niitä toimii mm. satama-, lentoliikenne-, finanssi-, vesihuolto-, ydinenergia-, energia-, terveydenhuoltosektoreilla.

(2) Vision selkeys ja kyberturvallisuustyöhön sitoutuminen. Valtionhallinolla on aktiivinen rooli vision toteuttamisessa samalla kun kyberturvallisuuteen investoidaan monipuolisesti. Kansainvälinen kyberturvallisuuden johtoasema voidaan saavuttaa (a) käyttämällä digitalisaation mahdollisuudet optimaalisesi hyväksi, (b) edistämällä yritysten ja tutkimusyhteisön edelläkävijän asemaa sekä (c) osallistumalla kansainvälisiin, yhtenäiselle arvopohjalle rakentuviin koalitioihin. Myös alue- ja paikallistason toiminnan herättely koetaan tärkeäksi. Sitoutumisen ytimessä on pyrkimys tehdä kyberturvallisuusalasta taloudellisesti kannattavaa ja kilpailukykyistä. Ulkomaisia investointeja pyritään hankkimaan mahdollisimman hyvällä kyberturvallisuusbrändillä.

(3) Vuosittainen kattava (julkinen) kyberturvallisuusarvio. Se mittaa strategian toimeenpanon tasoa ja parantaa kybertilannekuvaa. Arvio tuo ilmi tieto- ja kehittämistarpeita. Tietotarpeiden täyttämisen koordinoimiseksi Alankomaissa on laadittu kyberturvallisuuden kansallinen tutkimusagenda[31] yhdistämään (akateemista) tutkimusmaailmaa ja kansallisia kyberturvallisuustarpeita. Vastaava tutkimus- ja kehitystoiminnan koordinointi hyödyttäisi tutkimuksen ja käytännön tarpeiden kohdentamista.

### 5.2.2 Iso-Britannia

Ison-Britannian GCI-luku on 0,706 ja sijoitus globaalissa vertailussa 5. Iso-Britannia julkaisi uuden kyberturvallisuusstrategian marraskuun 2016[32] alussa tukemaan vuoden 2015 kansallista turvallisuusstrategiaa. Vision mukaan Iso-Britannia on vuonna 2021 turvattu ja sietokykyinen kyberuhkia vastaan sekä menestyksekäs ja itsevarma digitaalinen toimija. Maan tulevaisuus rakentuu digitaaliselle perustalle. Strategian tavoitteena on:

- ”Puolustaa” (defend) kehittyviä kyberuhkia vastaan, vastata häiriöihin tehokkaasti sekä varmistaa, että digitaalinen toimintaympäristö on suojattu ja sietokykyinen. Kansalaiset, yritykset ja julkinen hallinto osaavat puolustaa itseään.
- ”Luoda pelote” (deter) vihamielistä kybertoimintaa vastaan ennalta-ehkäisemällä, keskeyttämällä ja lainvalvonnan keinoin. Iso-Britannia käyttää hyökkäyksellistä kyberkykyä tarpeen mukaan ja vastaa vakavaan kyberhyökkäykseen samoin kuin kineettiseen.
- ”Kehittää” (develop) kasvavaa kyberturvallisuusteollisuutta koulutuksella ja tutkimuksella sekä varmistaa riittävät kyvyt julkisen ja yksityisen sektorin tarpeisiin.

Kyberuhkat nostettiin korkeimman tason uhkiksi kansallisessa turvallisuusstrategiassa 2010, mikä vahvistettiin vuoden 2015 strategiassa. Uusi kyberturvallisuusstrategia rakentuu vuoden 2011 kyberturvallisuusstrategian mukaisen toimintaohjelman perustalle. Viiden viime vuoden aikana Iso-Britanniassa on

- Luotu rakenteita ja toimintatapoja kyberturvallisuustapahtumien raportoimiseksi[33] ja tiedonvaihdon parantamiseksi[34]
- Vahvistettu hallinnon kyberturvallisuutta ja kyberturvallisuustietoisuutta[35]

[31] National Cyber Security Research Agenda on julkaistu vuosina 2012 (NCSRA I) ja 2013 (NCSRA II). Lisäksi vuonna 2015 niitä täydentämään perustettiin Cyber Security Research & Education platform (CSRE) (NWO 2015)

[32] Strategia on laskentatavasta riippuen kolmas tai neljäs Iso-Britannian kyberturvallisuusstrategia. Ensimmäinen julkaistiin vuonna 2009 ja siihen tehtiin laaja päivitys vuonna 2010.

[33] Esim. *Action Fraud* [http://www.actionfraud.police.uk/] [5.11.2016]

[34] Esim. *The Cyber Security Information Sharing Partnership (CISP)* vuodesta 2013 alkaen. Yhteistyöympäristössä jäsenet voivat mm. vaihtaa kyberuhkatietoa reaaliaikaisesti. Nykyisin CERT-UK:n alla.

[35] Esim. hallinnon yhteistyön helpottamiseksi rakennettu *the Public Services Network (PSN)*.

- Vahvistettu kriittisen infrastruktuurin suojaa[36] ja luotu ohjeistusta erikokoisille yrityksille kyberturvallisuuden parantamiseksi[37]
- Nostettu yleistä tietoisuutta mm. nettisivuilla, kampanjoilla, seminaareilla ja kilpailuilla[38]
- Vahvistettu poliisin ja syyttäjän kykyä vastata kyberrikollisuuteen[39]
- Vahvistettu turvallisuuspalveluiden[40] ja asevoimien[41] kykyä toimia kyberavaruudessa
- Lisätty kansainvälistä yhteistyötä ja koulutusta kyberuhkien torjumiseksi
- Rakennettu ammattiasemille ja yrityksille sertifiointi- ja standardointimenettelyjä[42]
- Myönnetty 13 yliopistoille *Academic Centre of Excellence in Cyber Security Research*-status
- Rahoitettu kyberturvallisuuskoulutusta ja -tutkimusta eri organisaatioiden kautta[43]
- Monimuotoistettu kyberturvallisuusalan koulusta ja lisätty opetusta eri koulutusasteilla
- Tuettu kyberturvallisuusalan yritysten vientiponnisteluita ja kotimaista kasvua[44]
- Organisoitu CERT-toiminto vuodesta 2014 alkaen
- Järjestetty lukuisia kyberturvallisuusharjoituksia ja osallistuttu kansainvälisiin harjoituksiin
- Parannettu yksityisyyden suojaa hallinnon digitaalisissa palveluissa[45]

Vuoden 2011 strategiaan verrattuna nykyisessä strategiassa on määritelty ”tarve mennä pidemmälle”. Markkinaehtoinen lähestymistapa ei kykene vastaamaan monimutkaistuviin haasteisiin, joten tarvitaan vahvempaa hallinnollista otetta. Strategiassa kyberturvallisuus määritellään tietojärjestelmien, niissä käsiteltävien tietojen ja niiden tarjoamien palveluiden suojelemiseksi luvattomalta pääsyltä, vahingonteolta ja väärinkäytöltä (tahalliselta tai tahattomalta). Strategian toimenpanoa tuetaan 1.9 miljardilla punnalla viisivuotiskauden aikana[46].

Vastuu kyberturvallisuudesta on jaettu yksilöistä valtionhallintoon, joskin jälkimmäisellä on erityisvastuu koko yhteiskunnan toimivuuden säilymisestä. Hallinnolla on käytettävissä ylivertainen tiedustelutieto ja keinot maan puolustamiseksi kehittyneitä kyberuhkia vastaan sekä mahdollisuus edistää yksityisen ja julkisen sektorin yhteistyötä. Iso-Britannia pyrkiikin vaikuttamaan kyberavaruuden kehitykseen perustavanlaatuisten arvojensa[47] sekä taloudellisten ja turvallisuusintressiensä mukaisesti

- Investoimalla innovatiiviseen kyberturvallisuusteollisuuteen ja tunnistamalla kyvykkäät yksilöt ja start-upit ajoissa

[36] Keskeisin toimija on *The Centre for the Protection of National Infrastructure* (CPNI), jonka tehtävänä on neuvoa ja tukea kriittisen infrastruktuurin organisaatioiden turvallisuustyötä.

[37] Esim. ”10 Steps to Cyber Security” [https://www.ncsc.gov.uk/guidance/10-steps-cyber-security] [5.11.2016]

[38] Esim. Get Safe Online [https://www.getsafeonline.org/], Cyber Aware [https://www.cyberaware.gov.uk/] ja Cyber Security Challenge UK [https://cybersecuritychallenge.org.uk/] [5.11.2016]

[39] Esim. 2013 perustettiin uusi *National Cyber Crime Unit* ja organisoitiin osaksi niin ikään uutta *National Crime Agencyä (NCA)*. 2015 GCHQ ja NCA perustivat *Joint Operations Cellin (JOC)* tuoden yhteen teknisen ja tutkinnallisen osaamisensa.

[40] Erityisesti GCHQ:n kykyä, johon mm. 2013 perustettiin *the Centre for Cyber Assessment (CCA)* tuottamaan tiedustelutietoa hallinnon päätöksenteon tueksi.

[41] GCHQ:n yhteyteen perustettiin aselajien yhteinen *Joint Cyber Unit* kehittämään sotilastaktiikkaa, tekniikkaa ja suunnitelmia asevoimien tueksi. 2013 perustettiin toinen aktiivinen yksikkö ja reserviyksikkö. Yhdessä nämä kolme muodostavat *the Joint Forces Cyber Groupin* (JFCyG). 2013 aloitti myös *the Defence Cyber Protection Partnership (DCPP)*, jonka tavoitteena on parantaa toimitusketjun kokonaisturvallisuutta.

[42] Esim. Cyber Essentials [https://www.cyberessentials.org/] [5.11.2016]

[43] Kahta tohtoriohjelmakeskusta ovat rahoittaneet GCHQ ja *Department of Business, Innovation & Skills (BIS)*.

[44] Hallinnon ja teollisuudenalan yhteistyötä tehdään mm. *Cyber Growth Partnershipin (CPG)* alla.

[45] Esim. turvallista julkispalveluihin tunnistautumista varten rakennettu GOV.UK Verify [https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify] [5.11.2016]

[46] Vuoden 2011 kyberturvallisuusstrategian toimeenpano-ohjelmassa käytettiin £ 860 miljoonaa. Suurin osa rahoituksesta on mennyt ”kansallisen kyvyn kehittämiseen korkean tason kyberturvallisuusuhkiin vastaamiseksi”.

[47] Näitä arvoja ovat demokratia, oikeusvaltioperiaate, vapaus, hallinnon avoimuus ja luotettavuus, ihmisoikeudet ja sananvapaus.

- Parantamalla tiedustelun, turvallisuuspalveluiden, asevoimien, poliisin ja muiden lain toimeenpano-organisaatioiden kykyä ennakoida, estää ennalta, havaita ja keskeyttää kyberhyökkäykset
- Parantamalla kyberuhkien tuntemusta ja kykyä vastata niihin yhteistyössä teollisuudenalan kanssa
- Keskittämällä kyberturvallisuustoiminta GCHQ:n alaisuuteen vuonna 2016 perustettuun *National Cyber Security Centreen (NCSC).*[48]

NCSC:n tehtävänä on: (1) ymmärtää kyberturvallisuusympäristöä, jakaa tietoa ja hyödyntää koottua osaamista järjestelmällisesti (2) vähentää kansallista riskiä yhteistyössä yksityisten ja julkisten organisaatioiden kanssa (erityisesti kriittisen infrastruktuurin aloilla), (3) vastata kyberturvallisuustapahtumiin yhdessä tapahtuman kohteeksi joutuneen organisaation kanssa ja (4) johtaa, ylläpitää ja vahvistaa kansallista kyberturvallisuutta ja -kyvykkyyttä (ml. tilannekuvan ylläpitäminen). Kyberturvallisuutta vahvistetaan kokonaisvaltaisesti[49], monialaisesti ja yhteistyössä kansallisten ja kansainvälisten kumppaneiden kanssa.[50] Tärkeimpiä yhteistyöfoorumeita ovat NATO, EU, YK, OSCE, G20, Kansainyhteisö ja Euroopan neuvosto sekä kahdenkeskiset kumppanuudet.

Iso-Britanniasta kotiutettavia hyviä käytänteitä olisivat pitkäjännitteinen ja riittävästi resursoitu kyberturvallisuustyö, joka perustuu julkisen ja yksityisen kumppanuuteen sekä kybertoimintaympäristön monimutkaistumisen huomioiva toimintatavan uudistaminen. Miten maan ero EU:sta vaikuttaa kansainvälistä yhteistyötä korostavan kyberturvallisuusstrategian toteuttamiseen jää nähtäväksi.

### 5.2.3 Israel

Israelin GCI-luku on 0,676 ja sijoitus globaalissa vertailussa 6. Maalla ei ole julkista kyberturvallisuusstrategiaa, mikä on linjassa maan yleisen toimintatavan kanssa. Nykyinen strategiatyö keskittyy kolmeen kokonaiskyberturvallisuuden tasoon: (1) ”sitkeyteen” (robustness), (2) ”sietokykyyn” (resilience) ja (3) ”puolustukseen” (defence). Näistä ensimmäinen tarkoittaa organisaatioiden kykyä toimia häiriöttömästi; toinen kykyä toimia uhkien suhteen siten, että paluu normaalitilaan tapahtuu nopeasti; ja kolmas valtion toimintaa välittömästi kansallisia etuja koskevissa tilanteissa (ml. aloitteellinen kybertoiminta).[51]

Kyberturvallisuudella tarkoitetaan niitä politiikkoja, turvallisuusjärjestelyitä, toimia, ohjeita, riskienhallintaprotokollia ja teknisiä välineitä, jotka on suunniteltu kyberavaruuden suojaamiseen ja siellä toimimiseen. Kyberturvallisuustyön tavoitteena on edistää kansallista toimintakykyä kyberavaruudessa; parantaa nykyisten ja tulevaisuuden haasteiden hallintaa; vahvistaa kriittistä infrastruktuuria kyberhyökkäyksiä vastaan; edistää Israelin asemaa keskeisenä ICT:n kehittäjänä; ja rohkaista hallintoa, tutkimuslaitoksia, teollisuutta, yksityistä sektoria ja ”erityisorganisaatioita[52]” yhteistyöhön.[53]

[48] National Cyber Security Strategy 2016—2021.

[49] *whole-of-government approach;* vaihtoehtoisesti *comprehensive approach*

[50] Prospectus Introducing the National Cyber Security Centre 2016. Keskus avattiin virallisesti lokakuussa 2016. Se tuo yhteen GCHQ:n tietoturvallisuusyksikön, CPNI:n, CERT-UK:n ja CCA:n kyvyt samalla selkeyttäen kokonaisrakennetta.

[51] Esim. [http://scirex.grips.ac.jp/center/wp-content/uploads/2015/12/151110_matania.pdf] [23.8.2016]

[52] Erityisorganisaatioihin kuuluvat Israelin asevoimat, poliisi, turvallisuuspalvelu ("Shabak"), tiedustelu- ja erikoisjoukkojen organisaatio ("Mossad") sekä puolustussektori *the Head of Security of the Defense Establishmentin (DSDE)* alaisuudessa, joista viimeinen kattaa “the bodies guided by the DSDE as determined in the Law for Organizing Security in Public Bodies of 1998, as well as suppliers and operators developing or manufacturing security equipment for them”.

[53] Advancing National Cyberspace Capabilities. Resolution No. 3611 of the Government of August 7, 2011.

Kyberturvallisuustyötä maassa on tehty 1990-luvulta lähtien; vuodesta 2002 kriittisen infrastruktuurin suojaamista koskevan lain alla. Päävastuun toiminnasta ovat kantaneet keskeiset turvallisuusorganisaatiot. Vuoden 2010 kansallinen kyberaloite laittoi liikkeelle kyberturvallisuuskentän uudelleen organisoinnin. Yhteiskunnan eri aloja edustava asiantuntijatyöryhmä arvioi maan kokonaiskyberturvallisuutta ja antoi ehdotuksensa sitä vahvistaviksi toimenpiteiksi[54]. Ehdotusten mukaisesti vuonna 2011 perustettiin kansallinen kybertoimisto, joka toimii neuvoa-antavana elimenä suoraan pääministerin alaisuudessa ja jolla on kaksi keskeistä tehtävää: (1) kyberpuolustuksen koordinoiminen siviilipuolella ja kriittisen infrastruktuurin suojaamisen integroiminen osaksi sitä (2) kansallinen kyberturvallisuuden ja -kyvykkyyden rakentaminen yhteistyössä teollisuuden ja tutkimuslaitosten kanssa sekä kansainvälinen yhteistyö.[55]

Kybertoimiston rinnalle perustettiin kansallinen kyberviranomainen vuonna 2015. Näistä toimijoista on yhdessä muodostumassa kansallinen direktoraatti. Direktoraatti toimii niin sääntely- kuin toimeenpanevana elimenä, sisältää CERT-toiminnon[56] ja projisoi hallinnon kybervaltaa. Sen tekninen jaosto huolehtii kansallisista tutkimus- ja tuotekehitysprojekteista, joihin on käytettävissä huomattavat taloudelliset varat. Esimerkiksi kuluvalla viisivuotiskaudella koulutusta, tutkimusta ja teollisuudenalaa tuetaan kutakin 75-100 miljoonalla dollarilla[57]. Siviilipuolen kyberpuolustus ei sisällä hyökkäyskykyä, joka on Israelin asevoimilla. Kukin siviiliorganisaatio hoitaa mahdollisen yhteistyön sotilaspuolen kanssa omien yhteyksiensä kautta.

Asevoimilla ja tiedustelupalveluilla on vahva rooli kyberturvallisuudessa. Toiminnasta vastaavia yksiköitä on useita ja sotilaallista kyberpuolustusta ollaan organisoimassa yhden komentokeskuksen alaisuuteen[58]. Koko yhteiskuntaa koskevissa hätätilanteissa kansallinen kyberviranomainen johtaa yhteistyötä, joskin äärimmäisissä tilanteissa vastuu siirtyy asevoimille. Toimialakohtaisissa kybertilanteissa toimialakohtaiset viranomaiset toimivat kansallisen kyberviranomaisen avustuksella. Turvallisuuden tuottamisen painopiste on kansallisessa turvallisuudessa ja ICT-alan tukemisessa[59]. Pyrkimys on toimia mahdollisimman itsenäisesti ja kansainvälinen yhteistyö rajoittuu valikoituun tiedonvaihtoon ja CERT-toimintaan.

Israelissa kyberturvallisuutta lähestytään digitalisaation mahdollistavana ilmiönä ekosysteemi-ajattelun kautta. Uhkiin vastaamisen ohella keskitytään taloudellisiin mahdollisuuksiin. Esimerkiksi Beer Shevaan, mihin asevoimat siirsi osan toiminnoistaan, syntyi kyberturvallisuustutkimuksen ja -teollisuuden keskittymä. Ekosysteemin toimintaa alkoi vuonna 2014 edistää CyberSpark eli toimialan yritysten voittoa tavoittelematon katto-organisaatio, joka tekee yhteistyötä julkishallinnon kanssa. Alueella toimi jo soveltavaan tutkimukseen keskittyvä yliopisto. Fyysisesti läheisillä yhteyksillä hallinnon, asevoimien, teollisuudenalan ja tutkimuksen välillä tavoitellaan kokonaiskyberturvallisuutta vahvistavaa toimintamallia. Asevoimat ja kohdennettu tutkimus- ja kehitysrahoitus tukevat start-up- ja teknologiamyönteistä kulttuuria[60].

Meneillään on uuden kyberlainsäädännön valmistelu, joka kokoaisi yhteen olemassa olevat lait mm. yksityisyydensuojaa ja julkisten instituutioiden turvallisuutta koskien. Muitakin kuin

[54] Tabansky & Ben Israel 2015.

[55] Toimiston internetsivulla tehtävät jaetaan edelleen kolmeen osa-alueeseen (kansallisen kyberpolitiikan yhtenäistäminen, kybertuvallisuuden vahvistaminen ja maan ICT-johtoaseman edistäminen), joiden alle on yhteensä listattu 18 erilaista tehtävää. [http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAnd Authorities/cyber/Pages/default.aspx] [1.11.2016]

[56] CERT-toimintoa kehitetään aiempaa aktiivisempaan suuntaan: se toimii niin hallinnon ja yksityisten organisaatioiden kontaktipintana kuin suorittaa aktiivisia turvallisuustehtäviä. Toiminto monitoroi siviilitoimialoja organisaatioiden vapaaehtoisen osallistumisen pohjalta. Vastineeksi rajoitetusta järjestelmäpääsystä organisaatio saa tukea kyberturvallisuustoimintaansa, mm. tilanne- ja tutkimustukea, ohjausta sekä asiantuntija-apua.

[57] Luvut eivät vielä sisällä asevoimien tai muiden julkisten organisaatioiden itsenäisiä tutkimus- ja tuotekehitysinvestointeja.

[58] Komentokeskuksen on tarkoitus olla toiminnassa vuonna 2017. [https://www.idfblog.com/blog/2015/12/22/idf-cyber-command/] [1.11.2016]

[59] Pääministerin toimiston lukujen mukaan Israelin kyberturvallisuusalan vienti vuonna 2015 oli noin neljän miljardin arvoista, mikä tarkoittaa noin viiden prosentin globaalia markkinaosuutta.

[60] Tabansky ja Ben Israel 2015. Monen ICT-start upin taustalla on asevoimien kouluttama henkilöstö, joka palveluksen jälkeen on hyödyntänyt osaamistaan kaupallisesti. Meneillään olevalla seitsenvuotiskaudella CyberSparkin kehittämiseen ollaan investoimassa noin 100 miljoonaa dollaria.

kriittisen infrastruktuurin yrityksiä (ml. Israelissa toimivat ulkomaiset yritykset) koskeva lainsäädäntö on harkinnassa. Tarkimman (itse-)sääntelyn kohteena ovat puolustus- ja turvallisuus(teollisuuden)alat[61]. Kriittistä infrastruktuuria sääntelevät turvallisuuspalvelut[62], minkä lisäksi tehdään toimialakohtaista sääntelyä (kansallisen kyberviranomaisen ohjeistaessa). Yleisesti organisaatioiden ja kansalaisten suhteen pyritään tietoisuuden nostamiseen.

Nykyiset sertifiointiohjelmat koskevat tiettyjä ammattiasemia ja kriittisen infrastruktuurin yrityksillä on tuotteiden sertifiointimenettely. Vahvaa standardointijärjestelmää ei ole, sillä standardien nähdään ajoittain ”aiheuttavan ongelmia niiden ratkaisemisen sijaan”. Kyberkyvykkyyden rakentamiseksi maassa toimii kuusi hyvin resursoitua yliopistotason tutkimus- ja tuotekehittelykeskusta, jotka tekevät yhteistyötä teollisuuden ja siviili- ja/tai sotilasviranomaisten kanssa. Yläaste-/lukioikäisille on omat koulutusohjelmansa, samoin myöhemmillä koulutusasteilla, asepalveluksessa ja palveluksen suorittamisen jälkeen. Lisäksi järjestetään mm. naisille kohdistettuja koulutuksia ja eri tason kyberturvallisuusharjoituksia. Huippuluokan osaamisen rekrytoiminen on silti haaste.

Israelin mallista harkittavia toimintatapoja olisivat: (1) Ekosysteemiajattelu, jossa hallinto, teollisuus, tutkimuslaitokset ja muut osaamisresurssit tuodaan yhteen ja ne todella tekevät yhteistyötä. Osaaminen ja koulutus ovat keskiössä, samoin kuin innovaatiotoiminnan tukeminen. (2) Vahva poliittinen sitoutuminen kyberturvallisuuden parantamiseen, ml. tietoisuuden, kiinnostuksen ja resurssien lisääminen. (3) Kokonaisvaltainen kyberturvallisuus, ml. tekninen ja operatiivinen kyky, tiedustelu, tietoisuuden lisääminen, fyysinen ulottuvuus ja toimivat organisaatiot. (4) Yksityisen sektorin sääntely velvoittavan lainsäädännön keinoin.

### 5.2.4 Ruotsi

Ruotsin GCI-luku on 0,647 ja sijoitus globaalissa vertailussa 7. Ruotsi valmistelee ensimmäistä kansallista kyberturvallisuusstrategiaansa julkaistavaksi vuoden 2017 aikana. Strategiassa keskitytään julkisen hallinnon organisaatioiden (yhteis)toimintaan ja tehtäviin. Tavoitteena ei ole luoda uusia organisaatioita vaan hyödyntää tehokkaalla tavalla jo olemassa olevia. Yksityinen sektori on ainakin toistaiseksi jätetty valmistelutyön ulkopuolelle, vaikka sen toivotaankin tekevän enemmän kokonaiskyberturvallisuuden eteen.

Strategian valmistelutyön pohjaksi julkaistiin vuonna 2015 ei-sitova raportti *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*, jonka ehdotuksista yksi on jo laitettu käytäntöön: huhtikuun 2016 alussa viranomaisten velvollisuudeksi tuli raportoida kaikki tietoturvatapahtumat yhteiskunnan siviilipuolustusta koordinoivalle *Myndigheten för samhällsskydd och beredska*pille (MSB)[63]. Ruotsissa kyber- ja tietoturvallisuutta ei nähdä erillisiksi konsepteiksi vaan liukumaksi, jossa ”kyber”-etuliitettä käytetään erityisesti kansainvälisissä yhteyksissä ja konfliktitilanteissa[64]. Aiemmassa tietoturva(yhteis)työssä keskityttiin arkipäivän toimivuuteen ja kriisitilanteisiin, mutta nyt kehitetään toimintatapoja myös sodanajan tai sitä vastaaviin olosuhteisiin.

Käytännön tietoturvallisuus(yhteis)työtä viranomaisten välillä on tehty vuosikymmeniä. Yhteistyöfoorumina on toiminut etenkin *Samverkansgruppen för informationssäkerhet* (SAMFI)[65], jonka tehtävänä on edesauttaa tiedon luottamuksellisuuden, oikeellisuuden ja saatavuuden

[61] Puolustusministeriö tarpeen mukaan säätelee ja lisäohjeistaa teollisuudenaloja.

[62] Jatkossa osittain kansallinen kyberviranomainen

[63] Poikkeuksena kansallista turvallisuutta koskevat vakavat tapahtumat, jotka raportoidaan asevoimille tai Säpolle.

[64] SOU 2015:23. Tulevan strategian edeltäjiksi voi siten katsoa mm. MSB:n julkaisemat kansallinen tietoturvallisuusstrategia 2010—15 sekä tietoturvallisuuden kansalliset toimintasuunnitelmat 2008 ja 2012.

[65] MSB:n lisäksi foorumiin osallistuvat Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen (Säpo) ja Rikskriminalpolisen (RKP), Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC) sekä Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST).

varmistamista yhteiskunnassa[66]. SAMFI-yhteistyössä ollaan valmistelemassa kyberturvallisuuden hallintomallia julkiselle sektorille sisältäen mm. standardit, hyvät käytänteet ja uhkakuvat. Julkiselta puolelta käytänteiden oletetaan siirtyvän yksityiselle puolelle, mutta pakottavuutta suunnitelmiin ei sisälly. SAMFI ja toimialakohtaiset viranomaiset vastaavat suurimmasta osasta arkipäivän ja kriisitilanteiden kyberturvallisuustyötä.

SAMFI-yhteistyön ohella kyberturvallisuuden kannalta keskeisiä, meneillään olevia käytännön prosesseja ovat siviilipuolustuksen ”henkiin herättäminen” ja uudelleen organisoiminen MSB:n ympärille[67], Euroopan Unionin verkko- ja tietoturvadirektiivin (NIS-direktiivi) kansallinen toimeenpaneminen sekä *säkerhetsskyddslag*in[68] uudistaminen. Lisäksi EU:ssa meneillään oleva tietosuojaa sähköisen viestinnän alalla koskevan direktiivin uudistaminen vaikuttaa toimintaympäristöön.

Ruotsin hallintomallissa toimialakohtaiset viranomaiset ovat verrattain vahvoja ministeriöihin nähden, itsenäisiä suhteessa toisiinsa (sääntelevät ja valvovat toimialaansa) ja säilyttävät tehtävänsä myös kriisiaikoina. ICT-alaa sääntelee *Post- och Telestyrelsen*. MSB:llä on viranomaistoimintaa koordinoiva rooli asioissa, jotka eivät ole kansallisen turvallisuuden ydintä. Se on mm. järjestänyt kansallisia kyberturvallisuus-harjoituksia[69], joskin pääosa harjoituksista on toimialakohtaisia. Keskeisimpiä kansainvälisiä yhteistyötahoja Ruotsille ovat EU, Nato, OECD ja esim. Pohjoismaiden CERT-yhteistyö sekä yhteistyö Yhdysvaltojen kanssa. Ruotsin CERT on sijoitettu MSB:n yhteyteen.

Ruotsissa kyberpuolustuksen järjestäminen ei ole vain sotilastoimijoiden tehtävä vaan asevoimien ohella keskeisimpiin turvallisuustoimijoihin kuuluvat *Försvarets radionanstalt* (FRA) ja *Säkerhetspolisen* (Säpo). Näillä kolmella on oma yhteistyöelin, jonka toimintaan MSB ajoittain osallistuu. Esimerkiksi FRA voi auttaa muita viranomaisia ja valtionyhtiöitä teknisen tietoturvallisuuden järjestämisessä silloin, kun kyseessä on yhteiskunnan kokonaisturvallisuus. Lisäksi se osallistuu kansallisen tilannekuvan tuottamiseen ja salaustoimintojen järjestämiseen ja voi ohjeistaa toimialakohtaisia viranomaisia kokonaiskyberturvallisuuden tason nostamiseksi.[70]

Kybertoimintakyvyn kehittämisessä on ongelmia mm. rekrytoinnissa, sillä osaavia henkilöitä on vähän ja kilpailu heistä kovaa. Ruotsissa ei ole lähdetty rakentamaan kansallisiin tarpeisiin vastaavia kyberkoulutusohjelmia, sillä koulutusinstituutiot toimivat varsin itsenäisesti. Tutkimusyhteistyötä tehdään jonkin verran, etenkin kyberpuolustuspuolella, mutta ensisijaisesti yhteydet ovat alan yrityksiin, etenkin kriittisen infrastruktuurin suojaamisessa. Myöskään kansallista tutkimus- ja tuotekehitysohjelmaa ei ole, joskin MSB:ltä voi hakea rahoitusta projekteihin, joissa tarkoituksena on kehittää yhteiskunnan kriisinhallintakykyä ja yhteistyötä.

Ruotsista kotiutettavia toimintatapoja olisivat huomion kiinnittäminen siviilikyberpuolustuksen kehittämiseen yhteistyössä kansallisen turvallisuuden keskeisimpien toimijoiden kanssa sekä tieto- ja kyberturvallisuuden näkeminen jatkumona, jossa toiminnan vapaus, vastuut ja sen sisältämät riskit muuttuvat siirtymän mukaisesti.

[66] Myndigheten för samhällsskydd och beredskap (2014) Samverkansgruppen för informationssäkerhet, SAMFI. [https://www.msb.se/Upload/Forebyggande/Informationssakerhet/Faktabad%20SAMFI.pdf] [31.10.2016]

[67] MSB toimii oikeusministeriön sisäasioiden ministerin alaisuudessa, jonka mandaatille kyberturvallisuutta muissa kuin kansallisen turvallisuuden ydintä koskevissa kysymyksissä ollaan keskittämässä.

[68] Ruotsinkielinen *säkerhetsskydd*-käsite kääntyy huonosti suomeksi. Kyse on valtion keskeisimpien turvallisuustoimijoiden toimintakenttää ja -valtuuksia koskevan lainsäädännön uudistamisesta.

[69] Kansainvälisessä harjoitustoiminnassa Försvarshögskolan (FHS) on toiminut kontaktipintana.

[70] Esim. SOU 2015:23.

### 5.2.5 Singapore

Singaporen GCI-luku on 0,676 ja sijoitus globaalissa vertailussa 6. Kooltaan pienen ja luonnonvaroiltaan niukkaresurssisen maan talousmenestys perustuu määrätietoiseen profiloitumiseen alueellisena ja globaalina talouskeskuksena. Kyberturvallisuuden kehittämisessä noudatetaan samaa logiikkaa. Kyberturvallisuuden huippuluokkaisuuteen investoidaan rahallisesti paljon ja toimiala nähdään yhtenä talouden tärkeimmistä kasvusektoreista.

Kyberturvallisuuden vastuuministeriönä toimii tieto- ja viestintäministeriö[71], mutta valtionhallinnossa työskennellään monipuolisesti kyberturvallisuuteen liittyvissä asioissa. Vuonna 2015 perustettiin pääministerin alaisuuteen tieto- ja kyberturvallisuuteen keskittyvä yksikkö, *Cyber Security Agency* (CSA), joka yhdisti aiemmin erillään olleita kyberturvallisuustoimintoja samaan kokonaisuuteen. Virastossa työskentelee noin 150 henkilöä, joista kaksi kolmannesta suoraan kyberturvallisuuden tehtävissä.

CSA kehittää Singaporen hallinnon kyberturvallisuutta sekä strategisella että operatiivisella tasolla. CSA muun muassa valvoo ja kehittää yhteiskunnan kriittisten alojen (10 nimettyä sektoria) operatiivisia kykyjä kyberuhkien torjumiseksi. Myös CERT-toimintoja on siirretty sen alaisuuteen. Operatiivisiin tehtäviin kuuluu lisäksi julkinen–yksityinen-yhteistyön kehittäminen sekä koulutuksen ja tutkimuksen koordinointi. CSA:n tavoitteena on yritysyhteistyön avulla kehittää Singaporeen kyberturvallisuuden ekosysteemi. ”Kyberturvallisuuden ekosysteemi” on konsepti tai tavoitetila, jonka luomiseksi investoidaan huomattavasti sekä julkista että yksityistä rahaa.

Singaporen kyberstrategioissa tavoitetilaa on kuvailtu dynaamisin lausekkein, kuten *vibrant cyber security ecosystem* ja *trusted and robust infocomm hub*. Uusimman strategian visiointi juurruttaa tavoitteita vahvemmin turvallisuusnäkökohtiin: *resilient and trusted cyber environment*.

Singaporessa on tehty kyberturvallisuusstrategian kaltaisia julkaisuja jo vuodesta 2005. Suunnitelmia on julkaistu neljästi hieman eri nimillä: *Infocomm Security Masterplan* (2005–2007), *Infocomm Security Masterplan 2* (2008–2012) ja *National Cyber Security Masterplan 2018*. Viimeisin strategia julkaistiin lokakuussa 2016 nimellä *Singapore’s Cyber Security Strategy*.

Suunnitelmista ensimmäinen keskittyi valtionhallinnon informaatioviestinnän järjestelmien turvallisuuden kehittämiseen. Toinen Masterplan oli päivitys ensimmäisestä versiosta ja se laajeni kriittisen verkkoinfrastruktuurin toiminnan turvallisuuteen ja luotettavuuteen. Tässä strategiapaperissa Singapore alkoi profiloida itseään verkkotoiminnan keskuksena ja solmukohtana. Kolmas Masterplan toi uutena elementtinä yksityisen sektorin sekä kansalaiset mukaan kybervisioon ja laajeni kattavuudeltaan verkkotoiminnan koko ”ekosysteemiin”, millä tarkoitetaan koko yhteiskuntaa.

Strategiapaperit ovat täysin siviilipainotteisia. Sotilaallisten kyvykkyyksien kehittämiseen tai edes siviili-sotilas-yhteistyöhön ei viitata uusimmassa strategiassa lainkaan. Kyberpuolustus on erillään oleva osa-alue, jota kehitetään puolustusministeriön ja asevoimien johdolla. Sotilaallisesta ulottuvuudesta ei ole julkisia asiakirjoja.

Singaporen kyberstrategian suunnittelun yhteydessä toteutettiin laaja konsultaatiokierros. Taustatietoa kerättiin erityisesti yksityiseltä sektorilta. Edellisen Masterplanin edelleen voimassa oleva tavoite on, että Singapore on vuoteen 2018 mennessä ”luotettu ja vakaa tieto-

[71] Ministry of Communications and Information of Singapore

viestinnän solmukohta”. Masterplan esitti tavoitteeseen pääsemisen keinoksi kyberturvallisuuden lisäämisen ja sietokyvyn (resilience) kasvattamisen.

Uusimmassa strategiassa kyberturvallisuuden kokonaisuus rakentuu neljän pilarin varaan: (1) sietokykyinen infrastruktuuri, (2) turvallisempi kyberavaruus, (3) eloisa kyberturvallisuuden ekosysteemi ja (4) kansainvälisten kumppanuuksien vahvistaminen. Erillistä toimintaohjelmaa ei ole, vaan osatavoitteet ja toimintatarpeet esitellään kunkin pilarin sisällä.

Kyberturvallisuusstrategian toimeenpano tuo lähitulevaisuudessa mittavia lainsäädännöllisiä uudistuksia, joista keskeisin on kokonaan uusi *Cyber Security Act*. Tuleva kyberturvallisuuslaki velvoittaa 11 määriteltyä yhteiskunnan kriittistä alaa ilmoitusvastuuseen, standardointiin, riskivarviointeihin ja omien järjestelmien riittävään suojaamiseen. Alkuvuodesta 2017 voimaan astuva laki antaa myös CSA:lle laajemmat toimivaltuudet.

Singaporella on hallituksen johdolla käynnissä laajoja ja kunnianhimoisia tavoitteita kyberturvallisuuden parantamiseksi sekä kyberturvallisuuteen liittyvän hallinnon monipuolistamiseksi ja rakenteen uudistamiseksi. Näitä ovat muun muassa kyberturvallisuuden ekosysteemiajattelu ja Smart Nation -visio. Lisäksi Singapore haluaa olla johtava alueellinen keskus ja solmukohta kybersektorilla sekä kybertoimintaympäristössä kiinteästi toimivilla toimialoilla kuten finanssialalla ja IT-tuotannossa.

Singaporen mallista harkittavia toimintatapoja olisivat: (1) Toimialan näkeminen ja esittäminen kasvusektorina strategiatasolta lähtien. Alan kehittäminen perustuu investointeihin, kumppanuussuhteiden vaalimiseen, osaamispohjan jatkuvaan kehittämiseen sekä innovaatiotoiminnan aktivoimiseen. (2) Osaamisen kehittäminen sekä tutkimus- ja kehitystoiminnan painotus. Osaamista kehitetään koululaisesta, kansalaisesta ja työntekijästä aina huippuosaamiseen saakka yritysten ja valtionhallinnon yhteistyönä.

### 5.2.6 Viro

Viron GCI-luku on 0,706 ja sijoitus globaalissa vertailussa 5. Viroon kohdistui laaja ja lamauttava kyberhyökkäysten sarja vuonna 2007, mikä oli alkusysäys määrätietoiselle kyberturvallisuustyölle. Ensimmäinen kyberturvallisuusstrategia julkaistiin vuonna 2008 ja sen uudistettu versio 2014. Strategisen vision mukaan ”Viron on mahdollista taata kansallinen turvallisuus ja tukea avoimen, osallistavan ja turvallisen yhteiskunnan toimintaa”. Strategia luo pohjan kyberturvallisuuden suunnittelulle ja kehittämiselle. Se on itsenäinen dokumentti osana kansallisen turvallisuuden strategian kenttää.

Kyberturvallisuuden koordinointivastuussa on talous- ja viestintäministeriö. Operatiivisemman työn (ml. strategian toimeenpaneminen) hoitaa ministeriön alainen *Riigi Infosüsteemi Amet* (RIA). RIA:n toiminta jakautuu kahteen päähaaraan: kyberturvallisuuteen ja sähköiseen hallintoon. Kyberturvallisuuden saralla sillä on neljä keskeistä toiminta-aluetta: kriittisen infrastruktuurin suojaaminen, CERT-toiminto, hallinnon ja kriittisten toimijoiden IT-järjestelmien valvonta sekä julkisen sektorin tietoturvastandardisointi (ISKE).

Ensimmäistä strategiaa julkaistaessa kyberturvallisuus kuului puolustusministeriön hallinnonalaan. Vastuuministeriön vaihtuminen kertoo kyberturvallisuuden painopisteiden ja koko käsitteen laajentumisesta. Ensimmäisen strategian painopiste oli kriittisen infrastruktuurin suojaamisessa ja kyberturvallisuuden rakenteellisen pohjan luomisessa. Sen toiminta-ohjelmaan kuului mm. vuonna 2009 perustettu kyberturvallisuusneuvosto. Kyberturvallisuusneuvosto on asianomaisten ministeriöiden ja turvallisuusviranomaisten välinen, korkean ta-

son neuvoa-antava elin. Se on tarkoitettu vain julkisen sektorin luottamuksellisiin keskusteluihin.

Viron hyvän kyberturvallisuusmaineen taustalla on aktiivinen toimijuus. Vaikka kansallinen turvallisuus on Viron strategiassa keskeistä, ei kyberturvallisuus ole Virossa vain kansallisen turvallisuuspolitiikan jatke. Poliittinen johto on ottanut aiheen yhdeksi kärkiteemoikseen myös ulkopolitiikassa. Vuoden 2007 tapahtumat on käännetty politiikassa hyödyksi ja sitä käytetään tehokkaasti kybermaineen edistämisessä.

Kyberturvallisuus on yksi tärkeimmistä kansainvälisen yhteistyön viitekehyksistä[72]. Viro profiloituu vahvana toimijana monilla kyberturvallisuuden multilateraalisilla foorumeilla, erityisesti Natossa. Viron Eurooppa-neuvoston puheenjohtajuuskaudella 2017 kyberturvallisuus on keskeinen aihe ja maa pyrkii EU-yhteistyön laajentamiseen niin strategisella kuin operatiivisella tasolla. Viro on valinnut avoimen lähestymistavan kyberturvallisuuteen ja on valmis jakamaan kokemuksiaan ja saavutuksiaan kansainvälisesti.

Virossa kehitetään kokonaisvaltaista sähköisen hallinnon (*e-State, e-Governance*) mallia. Sen osalta kyberturvallisuutta tai pikemmin digitaalista jatkuvuussuunnittelua varten Virossa on kansallinen digitaalinen strategia. Kyberturvallisuus näyttäytyy myös kansallisessa yrittäjyysstrategiassa, jonka tavoite on tukea toimialan innovaatioita.

Kyberturvallisuudesta säädetään osin osana muita turvallisuuteen liittyviä lakeja[73], mutta selkeä ja nykyaikainen kyberturvallisuuslaki puuttuu[74]. Virossa on käynnissä lainsäädännön puutteita läpikäyvä analyysityö. Lainsäädäntöä ollaan muokkaamassa sekä EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) toimeenpanemiseksi, että keskeisen turvallisuuslain *Emergency Act:*in uudistamiseksi. *Emergency Act* määrittelee elintärkeät toiminnot, jollaiseksi uudessa laissa lisätään sähköinen tunnistautuminen. Lisäksi alakohtaisiin lakeihin sisällytetään tarpeellisia tieto- ja kyberturvallisuutta koskevia elementtejä. Säädöspohjan kehittäminen tapahtuu sisäministeriön alaisuudessa ja sen yhtenä tavoitteena on luoda yksi kokonaisvaltainen kyberturvallisuutta säätelevä laki. Yksityisen sektorin toimijoita konsultoidaan lainsäädännön kehitystyössä.

Viron strategiassa kyberturvallisuus määritetään hyvin selkeästi osaksi kansallista turvallisuutta ja tämä lähtökohta määrittää koko strategian sisältöä ja tyyliä. Strategia on turvallisuus- ja puolustusorientoituneempi kuin esimerkiksi muutamat muut, vertailun talouspainotteisemmat strategiat. Kyberpuolustus on Viron kansainvälistä tunnustusta saanut erikoisosaamisvykkyys.

Strategian yleistavoitteen mukaan kyberkykyjä kasvattamalla ja kansalaisten tietoisuutta lisäämällä varmistetaan luottamus kybertoimintaympäristöön. Osatavoitteiden kautta määritellään tähän yleistavoitteiseen pääsemisen keinot. Niistä tärkeimmiksi on nostettu tietojärjestelmien suojaaminen, kyberrikollisuuden vastainen taistelu, kansallisen kyberpuolustuskyvykkyyden kehittäminen ja osaamispohjan kasvattaminen.

Nykyinen strategia on määritelty vuosille 2014–2017. Sitä ollaan kuitenkin pidentämässä vuodella. Strategia kattaa suhteellisen hyvin sen, mitä Virossa kyberturvallisuuden osalta tehdään ja halutaan tehdä. Pidennyksen syynä on se, että kaikkia asetettuja tavoitteita ei ole halutulla tasolla annetussa ajassa saavutettu. Näin ollen kolmas kansallinen kyberturvallisuusstrategia julkaistaneen vasta vuonna 2019. Nykyisen strategian osatavoitteista Virossa

[72] Ministry of Foreign Affairs

[73] Emergency Act, Public Information Act.

[74] RIA (2015)

on onnistuttu kyberrikollisuuden torjuntaa ja kansainvälistä yhteistyötä koskevin osin suhteellisen hyvin. Lisävuodesta on hyötyä muun muassa koulutuksen ja tutkimuksen sekä puolustussektorin tavoitteiden osalta.

Strategisten linjausten suunnittelutyö kolmannen strategian osalta on jo alkanut. Kyberturvallisuuden rooli taloudessa ja talouskasvun luomisessa korostuu nykyistä enemmän. Vision osalta keskitytään selkeään päätavoitteen määrittelyyn ja sitä kautta koko strategian kirkastamiseen. Toimenpideosiossa keskeistä on tavoitteiden realistisuus, mitattavuus ja niiden esittäminen riittävällä tarkkuudella. Virossa pohditaan esimerkiksi puolivälin tavoitteiden asettamista strategiaan toimeenpanon arvioinnin ja mitattavuuden parantamiseksi.

Viron mallista harkittavia toimintatapoja olisivat: (1) Viro on onnistunut profiloitumaan erityisesti kyberpuolustuksen edelläkävijämaana[75]. Kansainvälisen menestymisen taustalla on asiaosaamisen ohella asialle annettu ulkopoliittinen painoarvo. Määrätietoinen kyberturvallisuusmaaksi profiloituminen on pienen valtion keino merkittävyytensä lisäämiseksi. (2) Kyberturvallisuuden tilaa arvioidaan RIA:n vuosittain julkaisemassa kyberturvallisuuskatsauksessa[76]. Myös Suomessa tulisi pohtia vastaavan vuosittaisen arvion tuottamista julkisena dokumenttina. (3) Virossa pohdittu strategian toimeenpanon arvioinnin ja mitattavuuden parantaminen, johon mahdolliset puolivälin osatavoitteet voisivat olla keino.

## 5.3 Keskeiset havainnot

Vertailluissa maissa tiedostetaan tieto- ja kyberturvallisuuden kasvava merkitys kansallisen turvallisuuden ylläpitämisessä. Osaamista ja kyvykkyyksiä pyritään kehittämään aktiivisesti. **Suurin osa maista tavoittelee globaalia tai alueellista johtoasemaa kyberkyvykkyydessä.** Kaikilla lähtökohtana on olla kyberturvallisuuden huippumaa, vaikka osa strategioista profiloituu vahvemmin taloudellisesti kilpailukykyisenä (Alankomaat, Singapore) ja osa puolustuskykyisenä (Iso-Britannia, Viro). Kaikissa kyberturvallisuusstrategioissa keskeisimpiä tehtäviä on yhteiskunnan kriittisten toimintojen turvaaminen, mutta vaihtelua on siinä, mitä muuta painotetaan ja miten.

Kyberturvallisuustyön johtovastuu on maasta riippuen eri hallinnonaloilla, mikä näkyy strategioiden painotuksissa. Enemmistössä vertailumaita on perustettu uusia organisaatioita tai hallintoelimiä kyberturvallisuuden ympärille. Kansallisia kyberturvallisuuskeskuksia, -virastoja tai -viranomaisia on luotu koordinoimaan kyberturvallisuustyötä. Organisoituminen on tapahtunut kyberturvallisuusstrategioita toimeenpantaessa. Ruotsissa kyberturvallisuutta rakennetaan olemassa olevien rakenteiden varaan ja tietoturvallisuuden jatkeena. Organisoitumisessa kehityskohteena korostuu kokonaisvaltaisuuden lisääminen. Esimerkiksi Israelissa ja Singaporessa painotetaan kyberturvallisuuden ekosysteemiajattelua. Vastaava yhteiskunnan läpileikkaavuus esitetään Alankomaissa verkostoajatteluna, jossa painotetaan alueellisuutta ja klustereita.

Kaikissa maissa on käynnissä lainsäädännön uudistus, jossa joko luodaan kokonaan uutta kyberturvallisuuslainsäädäntöä tai muokataan olemassa olevaa säädöspohjaa nykyaikaisen kybertoimintaympäristön vaatimusten mukaiseksi. Lainsäädäntötyön määrä kertoo siitä, ettei säädöspohjaa nopeasti kehittyvällä alalla ole tai se on vanhentunutta eikä palvele kyberturvallisuuden nykytilanteen tarpeita.

[75] Esimerkiksi Viron rooli Naton kyberkyvykkyyden rakenteissa kasvaa edelleen. Ministry of Defence (2016)

[76] Annual Report of the Estonian Information System Authority's Cyber Security Branch https://www.ria.ee/public/Kuberturvalisus/2015-RIA-Annual-cyber-report.pdf

Kansainvälisen yhteistyön tärkeys korostuu suurimmassa osassa strategioita. Erityisesti Iso-Britanniassa, Virossa ja Alankomaissa kansallisen kyberturvallisuuden rakentaminen alkaa maan rajojen ulkopuolelta: vaikuttamalla kansainvälisillä areenoilla siihen, millaiseksi kybertoimintaympäristö muodostuu. Kansainvälisiin tavoitteisiin pyritään muun muassa kouluttamalla, yhteisellä harjoitustoiminnalla ja tekemällä tiivistä yhteistyötä kansainvälisten kumppaneiden kanssa. Vertailumaista Israelissa kuitenkin pyritään toimimaan mahdollisimman itsenäisesti. Kansainvälisessä yhteistyössä painottuu usein alueellisuus. Esimerkiksi Singaporella on vahva alueellinen painopiste, Virossa nähdään Baltian maat ja Alankomaissa Benelux-maat alueellisena pikemmin kuin kansainvälisenä viitekehyksenä, Ruotsi osallistuu pohjoismaiseen yhteistyöhön ja kaikkien EU-maiden strategioissa unionin merkitys on huomattava.

Kaikissa maissa kyberturvallisuudella on taloudellinen ulottuvuus. Talousnäkökulman painotus kyberstrategioissa vaihtelee. Esimerkiksi Singaporessa ala on keskeinen kasvusektori ja talouspainotus strategiatasolla vahva. Israelissa ekosysteemiajattelun mukaisesti talous ja turvallisuus tukevat vahvasti toinen toisiaan. Kyberturvallisuuden toimiala nähdään kaikissa vertailumaissa digitaalisen yritystoiminnan mahdollistajana ja/tai tärkeänä teollisuudenalana itsessään. Alan innovaatiotoimintaa ja vientiä pyritään tukemaan.

Israel, Iso-Britannia ja Viro painottavat kyberturvallisuustyössään selkeimmin kyberpuolustusta. Singaporessa kansallinen kyberstrategia on täysin siviilipainotteinen. Siviili- ja sotilaspuolen yhteistyön tiiviys vaihtelee maittain: kaikkein läheisintä yhteistyö on Israelissa. Alankomaissa on strategiatyössä mainittu tarve yhteistyön parantamiseen. Siviilipuolustuksen käsite on käytössä Ruotsissa ja Israelissa (osana kokonaispuolustusta).

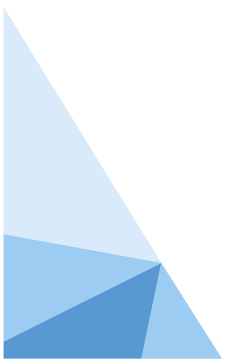
Kyberturvallisuuden ja sen teknisen puolen koulutukseen suuntaudutaan maissa eri tavoin: Israel, Iso-Britannia ja Singapore ovat sisällyttäneet kyberturvallisuuden kaikille koulutuksen tasoille. Melkein kaikissa maissa on perustettu erillisiä kyberturvallisuuteen keskittyviä koulutusohjelmia. Ruotsissa koulutusinstituutiot toimivat verrattain itsenäisesti ja koulutuksen ohella painotetaan kokemusta erilaisista kyberturvallisuuden tehtävistä. Kyberturvallisuuden alan koulutukseen on alettu kiinnittää yhä enemmän huomiota kaikissa vertailumaissa, sillä ne jakavat yhteisen huolen osaamispohjan kapeudesta. Osaavan henkilöstön puute ja rekrytointivaikeudet ovat kyberturvallisuusalan keskeinen haaste.

Jokaisessa maassa järjestetään kyberturvallisuusharjoituksia muodossa tai toisessa. Lisäksi ne osallistuvat aktiivisesti kansainväliseen harjoitustoimintaan. Avoimuus kyberturvallisuustyön ympärillä vaihtelee maittain. Esimerkiksi Viro, Iso-Britannia ja Alankomaat julkaisevat vuosittaisia raportteja kyberturvallisuuden tilasta ja strategian toimeenpanon etenemisestä. Iso-Britanniassa ja Ruotsissa julkaistaan myös hallinnollisia tutkimusraportteja, osastrategioita eri hallinnonaloille ja viranomaiskohtaisia raportteja. Muissa vertailumaissa ei strategian lisäksi tuoteta juurikaan muita virallisia julkisia raportteja. Israelissa ei ole julkista kyberturvallisuusstrategiaa.

Yhteistä kaikille vertailumaille on kyberturvallisuustyön holistisuus. Kyberturvallisuuden parantamiseen tähtäävään työhön pyritään integroimaan kaikki yhteiskunnan tasot (yksilö, yritykset ja organisaatiot, valtio). Inklusiivisuus varsinaisessa strategiatyössä vaihtelee sen tekemisestä tiiviissä vuorovaikutuksessa yksityisen sektorin kanssa (Alankomaat, Singapore) pelkästään valikoituneen hallinnollisen strategiatyöryhmän valmisteluun (Ruotsi).

Vertailumaiden kyberturvallisuusstrategioiden uhkaskenaariot olivat suhteellisen samanlaisia. Ne liittyvät yhteiskunnan ja talouden kriittisten toimintojen yhä kasvavaan digitaaliseen riippuvuuteen. Kyberuhkat, haasteet ja riskit monimutkaistuvat, mutta samalla kybertoimintaympäristöön liittyvät mahdollisuudet myös kasvavat. Kyberturvallisuutta tukevaa toimintaa esite-

tään usein kolmiona. Puolessa vertailumaista kolmiomallilla jäsennettiin joko toiminnan arvoperustaa tai kyberturvallisuustoimintaan osallistuvien organisaatioiden sääntelyn tiukkuutta. Yhtä kaikki, kyberturvallisuus nähdään jokaisessa maassa dynaamisena prosessina, jossa jo tehtyä turvallisuustyötä jatketaan haasteiden moninaistuessa.



# 6. KYBERTURVALLISUUDEN TAVOITETILA 2020

## 6.1 Toimintaympäristö- ja nykytila-analyysi

Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja -kerroksisista informaatioverkostoista, joihin kuuluu kansallisia julkishallinnon, yritysmaailman ja turvallisuusviranomaisten kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta ja ohjausjärjestelmiä, mitkä internetin välityksellä muodostavat maailmanlaajuisen verkoston.

Yhteiskuntaan kohdistuu yhä monimuotoisempia uhkia, joihin on pystyttävä varautumaan entistä tehokkaammin. Hybridiuhkista, informaatio-operaatioista ja kyberhyökkäyksistä on tullut yhä vaikuttavampia ja osaksi kybertoimintaympäristön olemusta. Kyberturvattomassa digiyhteiskunnassa syrjäytyminen, ääriliikkeet ja väkivalta kasvavat, jolloin sisäinen turvallisuus heikkenee, mikä alentaa yhteiskunnan toimintakykyä ja kriisisietoisuutta.

Kybertoimintaympäristö yhdistää valtioita, yrityksiä ja kansalaisia aivan uudella tavalla. Digitaalinen tietoyhteiskunta on merkittävästi lisännyt hyvinvointia, mutta kehityksen kääntöpuolena on riski erilaisista kybertoimintaympäristön uhkista. Tämä kybertoimintaympäristön kehitys vaikuttaa myös Suomeen. Suomi on yksi kehittyneimmistä digitaalisista tietoyhteiskunnista, jonka toiminnat ovat riippuvaisia erilaisista digitaalisista verkoista ja niiden antamista palveluista. Tietoteknisten laitteiden ja järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen tai vakavat kyberhyökkäykset voivat aiheuttaa kielteisiä vaikutuksia julkisiin palveluihin, liike-elämään ja hallintoon ja siten koko yhteiskunnan toimintaan.

Tavaroista ja palveluista tulee jatkuvasti älykkäämpiä. Ne myös liittyvät toisiinsa sekä ihmisiin uusien teknologioiden avulla. Myös yritykset voivat luoda yhä syvempiä reaaliaikaisia suhteita kumppaneihin, asiakkaisiin, palvelun- ja tavarantoimittajiin sekä julkishallintoon. Samaan aikaan digitalisaation seurauksena syntyy yhä uudenlaisia uhkia. Uusi informaatio houkuttelee rikollisia, jotka etsivät uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa.

Työn tekeminen on myös muuttunut. Työtä ei enää tehdä perinteisen luotetun yritysverkon sisäpuolella yhdessä ja samassa toimistossa. Työntekijät haluavat liikkua. Lisäksi heillä voi olla useita erityyppisiä päätelaitteita, joiden tietoturvahallinta voi olla haasteellista. Myös pilvipalveluiden käyttö on lisääntynyt. Sovellukset ja palvelut ovat nykyään internetissä ja pilvessä, kun ne ennen olivat yrityksen omassa sisäverkossa. Yrityksen datakeskukseen on jäänyt vain rajoitettu käsittelykapasiteetti, rajoitettu tietovarasto sekä yrityksen ydinimmateriaaliomaisuus. Työ voi olla tuottavampaa näin, mutta samaan aikaan se asettaa aivan uudenlaisia haasteita kyberturvallisuuden hallinnalle. Kyberturvallisuustoimittajien on kehitettävä parempaa suojaa erilaisille päätelaitteille, pilvipalveluille ja datan käsittelyyn sekä kaikkiin niihin kommunikaatiokanaviin, jotka kytkevät eri palvelut toisiinsa. Uusien päätelaitteiden sekä mielenkiintoisten uusien palveluiden syntyminen on myös johtanut siihen, että henkilökohtaista tietoa jää useisiin palveluihin. On alettu puhua digitaalisesta jalanjäljestä.

Yksityisyydensuojakeskustelua leimaa kaksijakoisuus; toisaalta halutaan olla yhteydessä ulkomaailmaan, jakaa tietoa ja löytää uusia mielenkiintoisia palveluita ja tuttavuuksia – verkostoitua – toisaalta ollaan huolissaan yksityisyydensuojan menettämisestä. Monikansallisille yrityksille koituu myös lisähaastetta siitä, että eri maissa on erilaiset säännökset yksityisyydensuojasta. Tosin 14.4. 2016 hyväksytty EU:n yleinen tietosuoja-asetus luo yhteiset raamit ainakin EU:n alueen toimijoille tietosuojasta. EU:n yleisen tietosuoja-asetuksen tavoitteina ovat yksilön oikeuksien vahvistaminen, sisämarkkinaulottuvuuden lujittaminen, tietosuojan

globaalin ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on luoda Euroopan unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Lisäksi pyritään parantamaan luottamusta verkkopalveluihin ja näin edistämään EU:n digitaalista sisämarkkinoiden kehittämistä.

Kyberhyökkäykset ovat lisääntyneet voimakkaasti viime vuosien aikana. Viiden viime vuoden aikana hyökkäysten määrä on kaksinkertaistunut joka vuosi. Samalla ajanjaksolla kyberturvallisuuteen käytettyjen budjettien koko on samana aikana noussut alle 20 prosenttia. Taloudelliset menetykset yhteiskunnan eri toimijoille on jatkuvassa kasvussa. Huonosti toteutettu kyberturvallisuus vie kaikki ne edut, jotka digitalisaatiolla voidaan saavuttaa.

IoT-uhat tulevat vahvistumaan ja ne tulevat olemaan osa todellisuutta. Tässä suhteessa uhkakuva pahenee tulevaisuudessa. Informaatioteknologiaa sisältävät järjestelmät on rakennettu ja edelleen rakennetaan pääosin liiketoiminta edellä. Tämä aiheuttaa sen, että systeemeitä ja niiden osia paikataan jälkikäteen ja kyberturvallisuudesta tulee päälle rakennettu toiminnallisuus, kun sen tulisi olla sisäänrakennettu toiminallisuus (Security by Design). Muussa tapauksessa kyberturvallisuus jää jälkeen teknologian kehittyessä yhä nopeammin.

Digitaalisen kybermaailman rinnalla on virtuaalinen sosiaalisen median (some) maailma, jossa kyse on osallistumisesta, vuorovaikutuksesta ja jakamisesta. Tässä virtuaalimaailmassa on sekä avoimia että suljettuja yhteisöjä. Some on laajentunut kansalaisten käyttämistä palveluista myös poliittisen johdon välineeksi (erityisesti Twitter, blogit). Sosiaalisessa mediassa ei ole vain kyse teknologiasta vaan siitä miksi ja mitä sosiaalisen median avulla tehdään. Sosiaalinen media ei ole vain verkko vaan myös yhteisö. Siksi vaikuttamisesta sosiaalisen median kautta on tullut merkittävää. Some toimii alustana psykologisille operaatioille ja strategiselle kommunikaatiolle tavoitteena vaikuttaa yksilöiden, yhteisöjen ja hallinnon toimintaan. Virheellisen ja harhaanjohtamiseen tarkoitetun disinformaation välittäminen on kasvava haaste. Nopeassa tiedonvälityksessä väärän tiedon kumoaminen on entistä vaikeampaa. Perinteisestä tunteisiin vetoavasta propagandasta on siirrytty käyttämään näennäisen oikeita ja rationaalisia tietoja tuottamaan ja tukemaan vääriä johtopäätöksiä. Somea ei voi hallita, siksi viranomaiset tarvitsevat uusia työkaluja ja toimintatapoja toimiakseen tehokkaasti somemaailmassa.

Tällä hetkellä kyberhyökkäysten monimutkaisuus, tehokkuus ja kyvykkyys kasvavat nopeammin kuin puolustuskyky. Usein vasta vakavat kyberhyökkäykset antavat sysäyksen turvallisuustoimenpiteiden kehittämiselle.

Kybermaailmassa on tapahtunut pahuuden konvergenssi. Mafia, hakkeriryhmä- ja verkostot, terroristit ja koko järjestäytynyt rikollisuus toimii kybermaailmassa ja käyttää sen palveluita hyväkseen tiedonvaihtoon, viestintään, tilannekuvan muodostamiseen ja johtamiseen. Tällä joukolla ei ole mitään ”toimivaltuusongelmia” vaan ne voivat täysimääräisesti hyödyntää globaalin digimaailman kyvykkyyksiä. Internetin rinnalle tälle pahuuden konvergenssille on muodostunut DarkNet, johon turvallisuusviranomaisilla ei ole riittävää näkymää. Tätä rajoittaa mm. toimivaltuuksien puute.

Kyberturvallisuusuhat tulee nähdä osana hybridivaikuttamista. Tämä edellyttää vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä. Kyberturvallisuuden strategisessa johtamisessa tarvitaan tilanneymmärrystä, selkeitä johtamisvastuita ja -rooleja, saumatonta tiedon kulkua ja -vaihtoa sekä lainsäädännön tulee kaikilta osin tukea koko kansallista kyberturvallisuusprosessia.

## 6.2 Tunnistetut puutteet ja kehityskohteet

Seuraavassa käsitellään tutkimuksessa esille tulleita Suomen kyberturvallisuuden nykytilassa tunnistettuja puutteita ja kehityskohteita. Nämä on luokiteltu 12 kokonaisuuteen, joita määrätietoisesti kehittämällä on mahdollisuus entisestään parantaa Suomen kyberturvallisuusstrategiassa esitetyn vision saavuttamista sekä edistää Suomen kyberturvallisuuden uskottavuutta niin kansallisesti kuin kansainvälisesti. Useat kokonaisuudet kytkeytyvät läheisesti toisiinsa ja siten niitä on syytä käsitellä kokonaisuutena. Samalla on huomioitava, että esille nostettavista puutteista ja kehityskohteista huolimatta Suomessa on tapahtunut paljon myönteistä kehitystä Suomen kyberturvallisuusstrategian julkaisemisen (24.1.2013) jälkeen. Lähtökohtaisesti on tunnistettuja puutteita ja kehityskohteita arvioitaessa huomioitava, että kyberturvallisuuteen yhdistyy sekä kybertoimintaympäristön uhkilta ja riskeiltä suojautuminen että kybertoimintaympäristön ilmentämien mahdollisuuksien hyödyntäminen.

### 6.2.1 Strateginen johtaminen

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. Suomen kyberturvallisuusstrategiassa todetaan, että kyberturvallisuuden johtamisen ylimmän tason muodostaa valtioneuvosto, mutta kukin ministeriö ja hallinnonala vastaavat kyberturvallisuudesta ja siihen liittyvien häiriötilanteiden hallinnasta. On ymmärrettävää, että vastuuta on haluttu hajauttaa, mutta ongelmaksi on muodostunut, ettei kokonaisuutta (koko yhteiskunnan osalta) johdeta riittävän selkeästi. Riittävän voimakkaan ja määrätietoisen strategisen johtamisen puuttuminen on vaikeuttanut kyberturvallisuusstrategian toimeenpano-ohjelman toteutumista. Kyse ei ole pelkästään kyberturvallisuuden johtamisen mallin luomisesta valtionhallinnon osalta, vaan johtajuuden määrittämisestä koko kansallisen kyberturvallisuuden ja sen koordinoinnin kontekstissa. Johtamisen selkeys on asia, mikä on vahvasti esille tullut asia myös kansainvälisten verrokkimaiden osalta, joissa kaikissa on korostettu riittävän toimivaltaista ja selkeää johtamismallia kansallisen kyberturvallisuuden kehittämisessä. Tutkimuksessa nousi esille erityisesti näkemys tarpeellisuudesta keskittää Suomen kyberturvallisuuden johtaminen Valtioneuvoston kansliaan. Lisäksi Turvallisuuskomitean rooli kyberturvallisuuden eri alueita yhteen sovittavana toimijana nousi selkeästi esille.

Strategiseen johtamiseen yhdistyy vuorovaikutteisuuden lisääminen eri toimijoiden (julkinen sektori, yksityinen sektori, tiede- ja tutkimusyhteisö ja järjestöt) välillä. Eri toimijoiden välinen yhteistyö kyberturvallisuuteen liittyvissä kysymyksissä on lisääntynyt, mutta sitä on tarpeellista kehittää entisestään poikkiyhteiskunnallisesti esimerkiksi kyberturvallisuusfoorumin puitteissa. Kehityskohteena on eri toimijoiden yhteistyön toimintamallin / yhteistyöfoorumin luominen, joka näyttäytyisi strategisena neuvonantajaelimenä ja jonka puitteissa eri toimijat voisivat käydä luottamuksellista tiedonvaihtoa ja edistää yhteiskunnallista kyberturvallisuuden kokonaiskoordinaatiota. Kyberturvallisuusfoorumi voisi myös osallistua toimeenpano-ohjelman vuosittaiseen välitarkasteluun ja tarpeen mukaan toimenpiteiden päivittämiseen. Oleellista on, että yhteiskunnan eri avaintoimijoiden välinen yhteistyö on aktiivista, osaamisverkostoa kasvattavaa sekä keskinäistä luottamusta vahvistavaa.

### 6.2.2 Poliittinen sitoutuminen

Vaikka Suomessa on viime vuosina vahvemmin ymmärretty kybertoimintaympäristöön liittyvien asioiden poliittinen luonne ja poliittisen ymmärryksen tarpeellisuus kyberturvallisuusstrategian vision saavuttamisessa, voi poliittisen sitoutumisen vahvistamista pitää edelleen kehityskohteena. Kyse on sekä poliittisen ymmärryksen että poliittisen sitoutumisen vahvistamisesta. Kybertoimintaympäristön muodostuessa niin kansallisen turvallisuuden kuin kansallisen kilpailukyvyn kannalta yhä merkityksellisemmäksi, on tärkeää, että Suomella on vahva poliittinen sitoutuneisuus kyberasioiden edistämiseen sekä poliittinen harkintakyky esimerkiksi vastatoimien osalta kohdattaessa mahdollisia kansallista turvallisuutta uhkaavia kyberhyökkäyksiä. Kybertoimintaympäristöä käytetään yhä aktiivisemmin eri valtioiden toimesta hyväksi poliittisten päämäärien edistämiseen, ja erilaiset kyberoperaatiot ovat keskeisessä asemassa niin sanotussa hybridisodankäynnissä. Kansainvälisessä tutkimuksessa painottuu tänä päivänä kyberasioiden poliittinen luonne (ns. ”cyberpolitics”), mikä kuvaa kybertoimintaympäristön ensisijaista ymmärrystä nimenomaan poliittisena toimintaympäristönä.

Poliittisessa sitoutumisessa on kyse myös kansallisen tahtotilan (kyberturvallisuusstrategian vision) edistämisestä ja viestimisestä kansainvälisesti. Tarkastelluissa verrokkimaissa nousi esille tärkeänä se, että valtion poliittinen johto on valmis esimerkiksi viestimään kansainvälisesti kansallisesta osaamisesta ja koko yhteiskunnan kybervalmiuden kehittämisestä. Edelläkävijyys edellyttää myös sopivissa määrin Suomen ”kyberturvallisuuden brändin” markkinointia ja edistämistä kansainvälisesti.

### 6.2.3 Kansainvälinen toiminta

Kansainvälisessä politiikassa ja yhteistoiminnassa kyberasiat ovat nousseet viime vuosien aikana niin sanotun korkean politiikan asioiden piiriin. Samanaikaisesti kyberturvallisuuden kysymyksiin ollaan kansainvälisesti vasta luomassa yhteisiä pelisääntöjä ja normeja. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä, kuten ETYJ:ssä, EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa. Esimerkiksi Viron tulevan Eurooppa-neuvoston puheenjohtajuuskauden yhtenä pääteemana on kyberturvallisuuden asiat. Kansainvälisillä yhteistyöfoorumeilla sekä valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita. On huomioitava, että kyberturvallisuuden asiat ovat tänä päivänä erottamaton osa Suomen ulko- ja turvallisuuspolitiikkaa ja kansainvälisen profiilin nostaminen myös edesauttaa suomalaisten kyberturvallisuusyritysten kansainvälisiä toimintamahdollisuuksia osana viennin ja kansainvälistymisen edistämistä.

Suomi on etenkin ulkoasiainministeriön ja nimitetyn kybersuurlähettilään toimesta ollut suhteellisen aktiivinen ja tehokas kyberturvallisuusasioissa kansainvälisillä foorumeilla. Toimintaa on kuitenkin tehostettava ja resursoitava nykyisestä, jotta Suomen painoarvo kyberturvallisuuden edelläkävijänä vahvistuu. Tämä on toimintatapa, jota myös muut edelläkävijyyttä tavoittelevat valtiot maailmassa toiminnassaan korostavat. Erityisesti Iso-Britanniassa, Virossa ja Alankomaissa kansallisen kyberturvallisuuden rakentaminen alkaa maan rajojen ulkopuolelta: vaikuttamalla kansainvälisillä areenoilla siihen, millaiseksi kybertoimintaympäristö muodostuu. Suomen on luotava selkeä ”kyber-agenda” eli määritettävä julkisesti tavoitteet, joita Suomi pyrkii kansainvälisessä yhteistoiminnassa edistämään. Kyberturvallisuuden kysymyksissä on havaittavissa tällä hetkellä maailmassa voimakkaitakin ristiriitoja, ja Suomen on mahdollista tavoitella aktiivisella ja luottamusta herättävällä toiminnallaan profiloitumista rauhanvälittäjäksi tai laajaa konsensusta vahvistavaksi toimijaksi. Suomen kyberturvallisuuden uskottavuudenkin näkökulmasta aktiivinen kansainvälinen toiminta on Suomelle tärkeää.

### 6.2.4 Tilannetietoisuus

Kybertoimintaympäristön nopea muutoskehitys sekä erilaisiin uhkiin ja riskeihin vastaaminen edellyttää mahdollisimman reaaliaikaista ja kattavaa tilannetietoisuutta. Päätöksenteon tueksi on kyettävä hankkimaan ja havainnoimaan jatkuvasti päivittyvää uhkatietoa mahdollisimman monista luotettavista kansallisista ja kansainvälisistä lähteistä. Itse tilannekuvan luomisessa korostuu niin tekninen, tilannejohtamisen kuin hallinnollinen tilannekuva. Suomessa on viime vuosien aikana kehitetty kyberturvallisuuden tilannekuvan muodostamista sekä eri toimijoiden keräämien tietojenvaihtoa, mutta tietojenvaihdon sekä havaintokyvyn parantaminen on edelleen Suomessa kehitettävä asia kyberturvallisuudessa. Kansallisen tiedustelulainsäädännön kehittäminen kybertoimintaympäristössä on välttämätöntä. Kyse on niin kansallisen kuin kansainvälisen yhteistoiminnan vahvistamisesta. Tiedonvaihtoon on kyettävä kehittämään tehokkaita menetelmiä ja tapoja sekä vahvistettava ”yhdessä tekemisen” henkeä. On myös tärkeää, että esimerkiksi tietoisuutta havaituista haavoittuvuuksista jaetaan aktiivisesti eri toimijoiden välillä, ja mahdollisista tietomurroista ilmoitetaan luottamuksellisella tavalla, jotta vastaavien tietomurtojen estäminen muualla yhteiskunnassa mahdollistuu. Kyberturvallisuus on joukkuepeliä. Mitä paremmin on mahdollista olla tietoinen kybertoimintaympäristön tapahtumista ja tätä tietoa jaetaan eri toimijoiden välillä, sitä paremmat edellytykset on varautua erilaisiin kyberuhkiin. Kyse on yhteistoimintatapojen kehittämisestä, suomalaisen kokonaisturvallisuuden hengessä.

### 6.2.5 Elintärkeiden toimintojen turvaaminen

Suomen kyberturvallisuusstrategian visiona on, että Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan. Suomi on pitkälle kehittyneenä tietoyhteiskuntana erittäin riippuvainen tietoverkkojen ja -järjestelmien toiminnasta, minkä johdosta kybertoimintaympäristön kautta suuntautuvat uhkat ovat kokonaisturvallisuuden kannalta hyvin merkittävä tekijä. Kasvavan riippuvuuden ohella eri sekä ei-valtiollisten että etenkin valtiollisten toimijoiden kehittynyt kyky vaikuttaa kybertoimintaympäristön kautta Suomen elintärkeisiin toimintoihin muodostaa suomalaiselle yhteiskunnalle yhä vakavammin otettavan uhkatekijän. Elintärkeiden toimintojen kyberturvallisuutta tukevien toimenpiteiden ja viranomaisten kyberturvallisuuden kehittämisen yhteensovittamiseen sekä etenkin energia-, sosiaali- ja terveydenhuolto- ja finanssi-alan kyberturvallisuuteen tulee kiinnittää erityistä huomiota.

Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kyberuhkia vastaan ja myös häiriötilanteiden resilienssi (sietokyky) on edelleen osassa suojattavia kohteita heikolla tasolla. On tärkeää, että varautuminen sekä sen jatkuva kehittäminen tapahtuu kaikilla elintärkeiden toimintojen aloilla, ja varautumista on kyettävä säännöllisesti seuraamaan ja arvioimaan. Suomalaisessa verkottuneessa tietoyhteiskunnassa on nykyistä paremmin tunnistettava elintärkeisiin toimintoihin vaikuttavat ja kriittisen infrastruktuurin kohteet sekä etenkin tunnistettava ne kriittiset palvelut ja toiminnot, joita tarvitaan itsessään ja ne tahot jotka ovat riippuvaisia näiden kriittisten palveluiden ja toimintojen toiminnasta. Kriittisten kybertoimintaympäristön tahojen ja toimintojen tunnistamiseen yhdistyy myös harkinta niin sanotusta kyberomavaraisuudesta eli varmistaa kriittisten infrastruktuurien ylläpidon kannalta riittävä kansallisen omavaraisuuden aste. On tärkeää, että Suomessa muodostetaan selkeä käsitys siitä, että missä määrin ja miltä osin Suomen tulee olla omavarainen kyberturvallisuusosaamisen ja alan yritysten omistuksen suhteen. Tällöin on varmistettava ja kehitettävä keinoja kriittisten yritysten ja osaajien ankkuroimiseksi Suomeen. Tässä kokonaisuudessa on myös huomioitava kriittisten tietovarantojen eheydestä ja saatavuudesta huolehtiminen kaikissa turvallisuustilanteissa.

### 6.2.6 Lainsäädäntö

Suomen kyberturvallisuusstrategian yhtenä strategisena linjauksena todetaan, että ”kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.” Kansainvälisissä eri valtioiden kyberturvallisuuden tasoa mittaavissa indekseissä lainsäädännön ajanmukaisuus on yksi arvioitava ulottuvuus, ja näissä arvioissa Suomi ei saa kovin korkeita arvioita osakseen. Lainsäädännön kehittäminen on yksi tärkeä osakokonaisuus valtiollisen kyberturvallisuuden kehittämisessä ja vahventamisessa. Suomen lainsäädäntöä ei ole kyetty ajanmukaistamaan kyberturvallisuuden vaatimuksia vastaaviksi, joskin tiedustelulainsäädännön osalta on valmistelutyö parhaillaan käynnissä.

Haastattelussa esitettiin harkittavaksi pakottavuuden lisäämistä häiriötilanteiden raportoinnissa. Koska tilannekuva ja tilannetietoisuus perustuvat havaintoihin häiriötilanteista, tarvitaan kansallisen kokonaiskuvan saamiseksi kaikki saatavilla oleva tieto.

Lainsäädännön ajanmukaisuudesta huolehtiminen yhdistyy kyberturvallisuuden ohella laajempaan teknologiseen (kiihtyvään) kehitykseen. Esimerkiksi erilaisten IoT-ratkaisujen, keinoälyn ja pilvipalveluiden kehittyessä on lainsäädännön ajanmukaisuudesta huolehtiminen tulossa aiempaa haastavammaksi, eikä kaikkia kyberuhkia edes pystytä ennakoimaan. Tämä tutkimus osaltaan osoittaa tarpeellisuuden selvittää koko kyberturvallisuuden kentän sekä siihen yhdistyvän teknologisen kehityksen asettamia muutostarpeita lainsäädäntöön kokonaisvaltaisesti, mahdollisesti jo tulevaa kehitystä ennakoiden. Samalla on selvitettävä, että onko erityisesti eri toimijoiden välisen tiedonvaihdon lisäämiselle lainsäädännöllisiä esteitä.

### 6.2.7 Resurssit

Kyberturvallisuuden kehittämisessä on kyse myös resursseista. Suomen kyberturvallisuusstrategian visio ja kohdennetut resurssit eivät ole tasapainossa. Tämän tutkimuksen perusteella voi todeta, että erityisesti kansainvälisesti vertailtuna Suomessa valtion taloudelliset panostukset kyberturvallisuuden kehittämiseen ovat olleet hyvin pieniä. Suomella ei luonnollisesti ole mahdollista samanlaisiin resurssien kohdentamisiin kuin suurvalloilla, mutta kyberturvallisuusstrategian vision saavuttaminen edellyttää merkittävää lisäpanostusta resurssien osalta esimerkiksi Kyberturvallisuuskeskuksen toiminnan vahvistamiseksi.

Resursoinnin lisätarve koskee myös yksityistä sektoria, jossa esiintyy edelleen välinpitämättömyyttä ja ymmärtämättömyyttä kyberturvallisuuden asioita kohtaan. Yritysten ja yhteisöjen ollessa vastuussa omasta kyberturvallisuudestaan, on suomalaisen yhteiskunnan kannalta tärkeää, että kyberturvallisuudesta on yrityksissä ja yhteisöissä huolehdittu määriteltyyn riskitasoon nähden riittävällä tavalla myös resurssien osalta.

### 6.2.8 Kyberturvallisuus kilpailuetuna

Useiden tässä tutkimuksessa vertailtujen maiden kyberturvallisuusstrategioissa painottuu kybertoimintaympäristön ilmentäminen mahdollisuuden ja/tai mahdollistajan näkökulmasta. Kyse on kybertoimintaympäristön kehityksen ymmärtäminen mahdollisuutena, ja kyse on positiivisesta lähestymistavasta turvallisuuteen. Kyberturvallisuus on digitalisaation mahdollistaja. Suomella on vahva kansainvälinen luottamuspääoma ja tätä luottamusta sekä suomalaista kyberturvallisuuden osaamista on oleellista pystyä hyödyntämään. On tärkeää, että niin puhekielessä kuin käytännön toimissa ei kyberturvallisuutta tuoda esille ainoastaan uhkien ja riskien näkökulmasta vaan kybertoimintaympäristö nähdään nykyistä vahvemmin myös nimenomaan mahdollistajana ja voimavarana, jota Suomi haluaa hyödyntää. Kansainvälisesti

Suomella on hyvät mahdollisuudet profiloitua kybertoimintaympäristön osalta turvalliseksi ja luotettavaksi, mikä lisää Suomen houkuttelevuutta investointikohteena. Tällä hetkellä suomalaista kyberturvallisuusdiskurssia ja lähestymistapaa leimaa liiallinen keskittyminen ainoastaan uhkiin ja riskeihin.

Suomen Kyberturvallisuusstrategiassa todetaan hyvin, että ”kansallinen kyberturvallisuus ja suomalaisten yritysten menestys ovat yhteydessä keskenään.” Suomi ei voi olla edelläkävijä kyberturvallisuudessa ilman uskottavaa alan yksityisen sektorin liiketoimintaa. Kyberturvallisuus on itsessään vahvistuva liiketoiminnan alue, ja Suomella on suhteellisesti arvioituna melko laaja kyberturvallisuuteen liittyvä yrityskenttä. Kansainvälisesti useat maat panostavat hyvin vahvasti kansallisten yritystensä liiketoiminnan kehitysedellytyksiin. Niin kansallisen kyberturvallisuuden vahvistamiseksi kuin taloudellisen hyödyn saamiseksi on suomalaista kyberturvallisuuden yrityskenttää kyettävä tukemaan nykyistä vahvemmin nimenomaan kansainvälistymisen, julkisten referenssien hankkimisen, myyntiosaamisen sekä viestiverkostojen luomisen osalta. Kyberturvallisuus on Suomelle mahdollisuus edistää kansainvälistä kilpailukykyä, ja on huomioitava, että kansallinen yritystoiminta on yksi yleisesti arvioitava edelläkävijyyden mittari. Tärkeää on myös luoda uudenlaisia toimintamalleja kyberturvallisuusalan start-up -yritysten tukemiseen ja kannustamiseen.

### 6.2.9 Osaaminen ja tutkimus

Osaamisen taso on yksi keskeinen valtiollisen kyberturvallisuuden tason mittari. Suomella on hyvä kansainvälinen maine kyberturvallisuuden osaamisessa. VTT:n ”Kyberosaaminen Suomessa” -raportin ja tässä tutkimuksessa tehtyjen havaintojen perusteella suomalaisten osaamista on pystyttävä vahvistamaan kyberturvallisuuden edelläkävijyyden saavuttamiseksi. Kyse on myös tarvittavan osaamisen paremmasta tunnistamisesta (minkälaiselle osaamiselle on tarve) varsin nopeasti muuttuvassa teknologian kehityksessä. Tällä hetkellä Suomessa ei ole riittävästi korkeatasoisia kyberturvallisuuden osaajia, joskin trendi on yhteneväinen kansainvälisesti. Esimerkiksi Yhdysvalloissa asiantuntijoiden presidentti Barack Obamalle luovuttama kansallisen kyberturvallisuuden -raportti suosittaa 50 000 uuden kyberturvallisuuden osaajan kouluttamista Yhdysvaltoihin vuoteen 2020 mennessä. Osaavan henkilöstön puute ja rekrytointivaikeudet ovat kyberturvallisuus-alan keskeinen haaste. Kyberturvallisuuden osaajista käydään yhä kovenevaa kilpailua lähivuosina niin Suomessa kuin kansainvälisesti. Osaamisen kehittämisen osalta on tärkeää, että Suomessa toteutetaan viipymättä ”Kyberosaaminen Suomessa” -raportissa esitettyjä osaamisen kehittämisen toimenpide-ehdotuksia, jotka palvelevat niin yritysten kuin julkishallinnon tarpeita. Samalla on päätettävä, että mitä osaamisen alueita Suomessa vahvistetaan ja mitä osaamista kehitetään yhteistyössä ulkomaisten kumppaneiden kanssa. Osaamisen kehittämisen ja vahvistamisen osalta on lisäksi tärkeää, että suomalaiselle nuorisolle pystytään paremmin viestimään kyberturvallisuus-alan eri mahdollisuuksista ja siten houkuteltua tätä ”nukkuvaa osaamista” alan piiriin.

Osaajien kouluttaminen edellyttää hajanaisen koulutuksen ja tutkimuksen nykyistä parempaa koordinaatiota oppilaitosten välillä sekä tutkimustoiminnan monipuolistamista. Samalla on kyettävä ketterään koulutuksen kehittämiseen ja osaamisen vahvistamiseen, sillä alan osaamisvaatimukset muuttuvat varsin nopeasti. Esimerkiksi ihmistieteiden merkitys teknologian kehityksessä sekä poikkitieteellinen strategisiin kysymyksiin keskittyvä kyberturvallisuustutkimus ovat tällä hetkellä tärkeydessään nousevia tutkimustrendejä maailmalla, mutta niiden tutkimus on Suomessa vielä hyvin vähäistä. Huomionarvoista on, ettei Suomessa ole strategista kokoavaa näkemystä alan koulutuksen ja tutkimuksen kehittämisestä. Tärkeää on, että kyberturvallisuuden osaamisen ja tutkimuksen osa-alueita kyetään jakamaan koordinoidusti Suomessa yliopistojen, korkeakoulujen, oppilaitoksien ja tutkimuslaitosten välillä. Tutkimus- ja innovaatiotoiminnassa yhteistyön merkitys korostuu. Kyberturvallisuuden tutkimus ja ope-

tus, alan teknologioiden kehittäminen sekä innovaatiot ovat kansallisia erottautumistekijöitä edelläkävijyyttä tavoiteltaessa. Tutkimus- ja koulutustoiminnassa niin kansallisen kuin kansainvälisen yhteistyön merkitys korostuu, ja erityisen tärkeää se on pienessä maassa, jossa toiminnan volyymilla ja resurssien määrällä ei voida kansainvälisesti kilpailla.

### 6.2.10 Yleinen tietous

Kyberturvallisuus, kuten turvallisuus, on aina myös kulttuurinen asia. Hyvään turvallisuuskulttuuriin liittyy ymmärrys riskeistä, vastuun kokeminen turvallisuuden kehittämisestä ja mahdollisuudesta vaikuttaa turvallisuuden parantamiseen. Kulttuurin muutos vie aikaa ja turvallisuuskulttuuri on vasta hiljalleen vakiintumassa ihmisten toimintaan ja käyttäytymiseen kybertoimintaympäristössä. Yleinen tietous ja osaaminen kyber- ja tietoturvallisuuden perusasioista on arvioitava peruskansalaistaidoksi tämän päivän suomalaisessa digitalisoituneessa tietoyhteiskunnassa. Yleinen tietous kyberturvallisuuden perusasioista ja näiden omaksuminen käyttäytymiseen kaipaa Suomessa aktiivista kehittämistä. Yleisen tietouden lisääntymisestä huolimatta on tietoisuutta kyberturvallisuudesta järjestelmällisesti lisättävä Suomessa niin poliittisten päättäjien, yrityselämän kuin kansalaisten keskuudessa. Kyberturvallisuuden osaaminen ja tietous eivät ole vain erillinen ammatillinen osaamisalue. Suomessa on havaittavissa edelleen varsin paljon tietämättömyyttä ja osaamattomuutta, ja monelle kyberturvallisuus näyttäytyy etäisenä ja vain teknologisena asiana. Kyberturvallisuuden perusosaamisen edistämisen tulee sisällyttää eri koulutusasteisiin ja kohdennettuna myös eri ikäryhmille. On myös huomioitava, että Suomessa on ihmisiä, jotka eivät esimerkiksi ole koskaan käyttäneet internetiä. Yleisen tietouden edistäminen läpi suomalaisen yhteiskunnan lienee helpoin, nopein ja kustannustehokkain tapa vahvistaa Suomen kyberturvallisuuden yleistä tasoa. Myös kansainvälisesti vertailtuna ”yleisen tietouden ja ymmärryksen taso yhteiskunnassa” on yksi kyberturvallisuuden edelläkävijyyden mittari. On ensiarvoisen tärkeää, että yleistä kyberturvallisuuden ymmärrystä, tietoisuutta ja osaamista pystytään Suomessa lisäämään niin valtionhallinnon, yksityisen sektorin kuin järjestökentän toimin.

Yleisen tietouden ja osaamisen edistämisessä on kyse myös vastuullisuuden kulttuurin luomisesta suomalaiseen yhteiskuntaan. Jokaisen suomalaisen on tunnettava vastuunsa ja ymmärrettävä merkityksensä turvallisuustoimijana. Vastuullisuuden kulttuuriin yhdistyy Suomen tietoturvallisuusstrategiassa esitetty tavoite, että Suomessa kehitetään, tarjotaan ja käytetään niin tavaroita, palveluita kuin järjestelmiä, joihin kyber- ja tietoturvallisuus on sisäänrakennettua. Tämän periaatteen toteutuminen lisää Suomen kansainvälistä kilpailukykyä sekä vahvistaa luottamusta Suomen kyberturvallisuutta kohtaan kokonaisuudessaan. Vastuullisen kulttuurin vahventumista on Suomessa kyettävä edistämään niin asenteellisesti kuin käytännön toimin.

### 6.2.11 Erottamaton osa turvallisuutta

Kyberturvallisuus on määritelmällisesti osoittautunut hankalaksi sanaksi suomen kielessä, eikä yhtenäistä määrittelyä kyberturvallisuudelle ole syntynyt. Käsitteen epämääräisyys osaltaan vaikeuttaa käytännön toimenpiteiden aikaansaamista ja sitoutumista kyberturvallisuuden kehittämiseen sekä kaikkinensa yhdistämistä turvallisuuden ymmärrykseen. Ymmärrettävyyden kannalta ”digitaalisen turvallisuuden” ja ”digitaalisen toimintaympäristön” kaltaisten käsitteiden käyttö on suotavaa yleisen ymmärryksen helpottamiseksi mistä kyberturvallisuudessa ja kybertoimintaympäristössä on yksinkertaisten kyse.

Oleellista on ymmärtää digitaalisen ja fyysisen toimintaympäristön yhä tiiviimpi yhteenkietoutuminen. Monilla digitaalisen toimintaympäristön tapahtumilla ja ilmiöillä on vaikutuksena

suoraan tai epäsuorasti fyysiseen toimintaympäristöön, ja päinvastoin. Kehityssuuntauksena on, että digitaalista ja fyysistä turvallisuutta on jatkossa yhä hankalampi erottaa toisistaan. Vaikka kyberturvallisuudessa on luonnollisesti teknisten yksityiskohtien ymmärrys tärkeää, on jatkossa etenkin strategisesti tarkasteltuna tärkeää ymmärtää digitaalisen toimintaympäristön turvallisuus erottamattomaksi osaksi kokonaisturvallisuutta, eikä kyberturvallisuutta tule siten tarpeettomasti erottaa ”omaksi turvallisuudekseen” turvallisuuden kokonaisuudesta. On tärkeää, että turvallisuusympäristöä uhkineen ja mahdollisuuksineen tarkastellaan kokonaisuutena. Kyberturvallisuuden ei tulisi olla oma irrallinen asiansa, vaan se tulee yhdistää osaksi kokonaisturvallisuuden lähestymistapaa. Merkittävä osa kokonaisturvallisuudesta on riippuvaista digitaalisen toimintaympäristön turvallisuudesta ja luotettavuudesta. Tällöin esimerkiksi voi harkita, että missä määrin tarvitaan erillisiä kyberturvallisuusstrategioita vai voisivatko kyberturvallisuuden asiat olla kiinteänä osana turvallisuusstrategioita. Tämä edellyttää vahvaa turvallisuuden strategista ”ison kuvan” kokonaisymmärrystä siitä mitä kybertoimintaympäristö edellyttää toimijoilta, toiminnalta, toimintorakenteilta ja tietojenvaihdolta kokonaisturvallisuuden kentässä. Kyberturvallisuuden asioita käsitellään usein yksinomaan teknologisesta näkökulmasta, minkä vuoksi kokonaisturvallisuuden ja toiminnan turvaamisen merkitys on jäänyt osin vähäiselle huomiolle arvioitaessa turvallisuuden kokonaisuutta.

### 6.2.12 Toimenpiteiden seuraaminen ja kypsyysmalli

Suomen kyberturvallisuusstrategiassa esitetty strateginen 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. Tämän tutkimuksen perusteella suositetaan Kyberturvallisuusstrategian ja sen toimeenpano-ohjelman tavoitteiden ja toimenpiteiden seurantaan käytettävän mittariston ja kypsyysmallin luomista. Tavoitteena tulisi kypsyysmallin ja mittariston avulla toteutettava vuosittainen arviointi Suomen kyberturvallisuuden tilasta. Tuloksena syntyisi vuosittainen kyberturvallisuus-arvio, jossa tarkastellaan tässäkin tutkimuksessa esillä olevia kyberturvallisuuden eri osa-alueita ja niiden sen hetkistä tilaa. Toimeenpanossa ”road map” -tyyppinen toimintatapa voisi olla toimiva ratkaisu.

On tärkeää, että Suomeen muodostuu 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 kyberturvallisuuden tason kokonaisvaltaista arviointia.

### 6.2.13 Suomen kyberturvallisuuden tavoitetila ja jatkotutkimustarpeet

Kansallisen kyberturvallisuuden tavoitteeksi tulisi asettaa, että "Vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaa kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti."

Kehittämisen toteuttamiseksi tarvitaan jatkotutkimusta ainakin aiheista: kyberturvallisuuden strateginen johtaminen Suomessa, kybertilannekuvan ja analysointikyvykkyyden kehittämi-

nen sekä yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin ja kyberomavaraisuuden määrittely osana kansallista kyberresilienssiä.

Jatkotutkimusta tarvitaan kehittämiskohteiden tarkemmaksi analysoimiseksi ja yksityiskohtaisten toimenpiteiden määrittelemiseksi. Kansallisen vision toteuttaminen edellyttää tutkittua tietoa ja eri toimijoiden kiinteässä yhteistyössä toteutettua kehittämistä. Tehokkaan yhteistyön avulla voidaan varmistaa kansallisen kyberturvallisuuden vaikuttavuus ja tuloksellisuus.

# LÄHTEITÄ JA TAUSTA-AINEISTOJA

**1. Kirjallisuus, katsaukset**


Euroopan Neuvoston tietoverkkorikollisuutta koskeva yleissopimus, 2001

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

Heinonen S., Sosiaalinen media, avauksia nettiyhteisöjen maailmaan ja vuorovaikutuksen uusiin muotoihin, TUTU-eJulkaisuja 1/2009

Huoltovarmuuskeskus, Kyberturvallisuuden tilannekuva energia-alalla, Huoltovarmuuskeskuksen verkkosivut, https://www.huoltovarmuuskeskus.fi/kyberturvallisuuden-tilannekuva-energia-alalla/ [16.12.2016].

International Telecommunication Union & ABI Research (2015) Global Cybersecurity Index and Cyberwellness Profiles, report

Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma, Turvallisuuskomitea, 11.3.2014 194/8.1.99/2013

Kyberturvallisuusstrategia (2013), Valtioneuvoston periaatepäätös 24.1.2013. http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia

Lehto M. ja Kähkönen A. (2015), Kyberturvallisuuden kansallinen osaaminen, Jyväskylän yliopiston Informaatioteknologian tiedekunnan julkaisuja No. 20/2015

Lehto M. ja Limnéll J. (2016) "Cyber Security Capability and Case Finland", the 15th European Conference on Cyber Warfare and Security (ECCWS) -konferenssi, 7.-8.7.2016 München, Saksa

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

Liikenne- ja viestintäministeriö, Maailman luotetuinta digitaalista liiketoimintaa, työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi, 10.2.2016

Melkman A. and Simmonds K. Strategic Customer Planning: How to Develop and Implement a Strategic Account Plan. eBook Collection (EBSCOhost) - printed on 8/9/2016

Tiedonhankintalakityöryhmän mietintö, Suomalaisia tiedustelulainsäädännön suuntaviivoja, 14.1.2015

VTT, Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015


**2. Kyberturvallisuusraportit**


AT&T. (2015). Decoding the Adversary. AT&T Cybersecurity Insights, Volume 1.

Cisco. (2016). Midyear Cybersecurity Report.

Dell Security. (2016). Annual Threat Report 2016.

Enisa. (2016). Enisa Threat Landscape 2015. European Union Agency for Network and Information Security.

Europol. (2015). The Internet Organized Crime Threat Assessment. 2015.

FireEye. (2016). 2016 Industrial Control Systems Vulnerability Trend Report. Critical lessons from 15 years of ICS vulnerabilities.

Flexera Software. (2016). Vulnerability Review 2016. Key figures and facts on vulnerabilities from a global information security perspective.

F-Secure (2015). Threat Report 2015.

Gartner. (2015). http://www.gartner.com/newsroom/id/3165317

Google. (2016). Android Security. 2015 Year in Review, April 2016.

Hewlett Packard. (2016). Cyber Risk Report 2016. HPE Security Research.

IBM. (2016). Reviewing a year of serious data breaches, major attacks and new vulnerabilities. IBM Security.

Interpol. (2014). Interpol Annual Report.

Kaspersky Lab. (2015). Global IT Security Risks Survey.

KrebsonSecurity. (2016) https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

Mandiant Consulting (2016). M-Trends 2016.

McAfee Labs. (2016). 2016 Threat Predictions.

PwC. (2016). Turnaround and transformation in cybersecurity. Key findings from the Global State of Information Security Survey, 2016.

Symantec. (2016). Internet Security Threat Report, Vol. 21, April 2016.

Verizon. (2016), Data Breach Investigations Report.

Viestintävirasto. (2015). Viestintäviraston kyberturvallisuuskeskuksen vuosiraportti 2015. Viestintävirasto, Kyberturvallisuuskeskus.

**3. Maakatsaukset**

*Alankomaat*

Cyber Security Assessment Netherlands CSAN 2016, National Cyber Security Center, Ministry for Security and Justice. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html

Cyber Security Assessment Netherlands CSAN 2015, National Cyber Security Center, Ministry for Security and Justice. https://english.nctv.nl/binaries/25760-csan-5-v3.2-web-uk_tcm32-83562.pdf

Government of the Netherlands (2016), First legislative bill on cyber security to the House of Representatives. https://www.government.nl/latest/news/2016/01/21/first-legislative-bill-on-cyber-security-to-the-house-of-representatives [2.10.2016]

Ministry of Defence (2015), Defence Cyber Strategy, Ministry of Defence of the Netherlands. https://www.defensie.nl/english/topics/cyber-security/contents/defence-cyber-strategy [30.10.2015]

National Cyber Security Research Agenda, The Netherlands Organization for Scientific Research. http://www.nwo.nl/documents/ew/cyber-security---nationale-cyber-security-research-agenda-ncsra

National Cyber Security Strategy 2, National Cyber Security Center, Ministry for Security and Justice. https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

National Cyber Security Strategy 1, National Cyber Security Center, Ministry for Security and Justice. https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

NCSC, ISAC's, National Cyber Security Centre -verkkosivut, https://www.ncsc.nl/english/Cooperation/isacs.html [5.11.2016].

NWO (2015), Dutch CyberSecurity Research and Education Platform, The Netherlands Organization for Scientific Research -verkkosivut, http://www.nwo.nl/en/news-and-events/news/2015/ew/new-dutch-cybersecurity-research-and-education-platform.html

Defence Cyber Strategy (2015), Ministry of Defence -verkkosivut, https://www.defensie.nl/english/topics/cyber-security/contents/defence-cyber-strategy

*Iso-Britannia*

(Kaikki asiakirjat saatavilla sivustolta: https://www.gov.uk/government/policies/cyber-security)

Cabinet Office (2011), The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.

Cabinet Office (2012a), Progress against the Objectives of the National Cyber Security Strategy – December 2012.

Cabinet Office (2012b), The UK Cyber Security Strategy Report on progress – December 2012 Forward Plans.

Cabinet Office (2013a), Progress against the Objectives of the National Cyber Security Strategy – December 2013.

Cabinet Office (2013b), The National Cyber Security Strategy Our Forward Plans – December 2013.

Cabinet Office (2014), The UK Cyber Security Strategy Report on Progress and Forward Plans – December 2014.

Cabinet Office (2016), The UK Cyber Security Strategy 2011—2016. Annual Report April 2016.

HM Government (2010a), A Strong Britain in an Age of Uncertainty: The National Security Strategy.

HM Government (2010b), Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.

HM Government (2015), National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom.

HM Government (2016a), National Cyber Security Strategy 2016—2021.

HM Government (2016b), Prospectus Introducing the National Cyber Security Centre.

*Israel*

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/ systemFiles/MASA7-2Eng%20Final_Even.pdf

National Cyber Bureaun internetsivusto, http://www.pmo.gov.il/English/PrimeMinistersOffice/ DivisionsAndAuthorities/cyber/Pages/default.aspx

National Cyber Bureaun strategiaesitys, http://scirex.grips.ac.jp/center/wpcontent/uploads/2015/12/151110_matania.pdf

Tabansky, L. & I. Ben Israel (2015) Cybersecurity in Israel. Springer Briefs in Cybersecurity.

*Ruotsi*

En ny säkerhetsskyddslag. SOU 2015:25. http://www.regeringen.se/contentassets/08d4b02afbc348edad916de817105a9c/en-ny-sakerhetsskyddslag-sou-201525

Euroopan Unionin Neuvosto (2013) Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa. COM(2013) 48 final.

Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. SOU 2015:23. http://www.sou.gov.se/wp-content/uploads/2015/03/SOU-2015_23_webb.pdf

Myndigheten för samhällsskydd och beredskap (2010) Strategy for Information Security in Sweden 2010–2015. https://www.msb.se/RibData/Filer/pdf/25940.PDF

Myndigheten för samhällsskydd och beredskap (2012) Sweden's Information Security. National Action Plan 2012. https://www.msb.se/RibData/Filer/pdf/26419.pdf

Swedish Emergency Management Agency (2008) Information Security in Sweden. Action Plan 2008. https://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/ Information%20Security%20in%20Sweden.pdf

*Singapore*

Singapore's Cyber Security Strategy, Cyber Security Authority Singapore. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en

Cyber Security Masterplan 2018

*Viro*

Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Ministry of Defence (2016), NATO investing in the development of Estonian cyber range. http://www.kmin.ee/en/news/nato-investing-development-estonian-cyber-range [31.10.2016].

Ministry of Foreign Affairs, Estonian Security Policy, Ministry of Foreign Affairs of Estonia. http://www.vm.ee/en/estonian-security-policy [16.10.2016]

RIA (2015), Annual Report of the Estonian Information System Authority's Cyber Security Branch. https://www.ria.ee/public/Kuberturvalisus/2015-RIA-Annual-cyber-report.pdf

VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

tietokayttoon.fi

ISSN 2342-6799 (pdf)
ISBN 978-952-287-368-2 (pdf)