VAASAN YLIOPISTO
TEKNIIKAN JA INNNOVAATIOJOHTAMISEN YKSIKKÖ
TIETOTEKNIIKKA

Matti Laukkanen

KYBERTURVALLISUUS SUOMESSA

Tietotekniikan
pro gradu -tutkielma

VAASA 2018

SISÄLLYSLUETTELO

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Matti Laukkanen
Tutkielman nimi: Kyberturvallisuus Suomessa
Ohjaajan nimi: Tero Vartiainen
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2010
Tutkielman valmistumisvuosi: 2018 **Sivumäärä:** 60

TIIVISTELMÄ

Tutkielman tavoitteena on tutkia kyberturvallisuutta Suomessa valtion ja kansalaisen näkökulmista. Kyberturvallisuus on olennainen osa kansalaisten jokapäiväistä elämää ja digitalisaation myötä turvallisuus korostuu etenkin verkossa. Ihmiset käyttävät paljon internetiä ja jakavat siellä henkilökohtaisia tietoja, jotka voivat vaarantaa henkilön turvallisuutta joutuessaan vääränlaiseen käsittelyyn. Turvallisuus kyberympäristössä korostuu tulevaisuudessa vielä enemmän maailman verkostoitumisen myötä.

Tutkimusongelmana on selvittää mitä on kyberturvallisuus, mitä siihen kuuluu ja miten kyberturvallisuuteen panostetaan Suomessa. Tutkielman tarkoitus on tutkia kyberturvallisuutta yleisesti Suomessa ja lähestyä aihetta valtion sekä kansalaisen näkökulmista. Aihe on rajattu näihin kahteen näkökulmaan sekä maantieteellisesti Suomeen. Työn ulkopuolelle jätettiin yritysten kyberturvallisuus ja pidemmälle viety tekninen tarkastelu.

Tutkielma toteutettiin narratiivisena kirjallisuuskatsauksena ja osaltaan myös tapaustutkimuksena. Tutkimusmenetelmä mahdollisti monipuolisen lähdeaineiston käyttämisen, joten aineistona on käytetty kyberturvallisuusalan kirjallisuutta, tieteellisiä artikkeleita ja aihetta käsitteleviä internetsivuja. Tutkimusongelma ratkaistaan selvittämällä kyberturvallisuuteen liittyvät yleiset asiat, miten ne liittyvät yleisesti turvallisuuteen ja käsittelemällä kyberturvallisuutta Suomessa valtion sekä kansalaisen näkökulmista.

Aineiston perusteella kyberturvallisuuteen panostetaan Suomessa sekä valtion, että kansalaisten toimesta. Suomen valtio on laatinut selkeän kyberturvallisuusstrategian, jonka mukaan tavoitteena on olla maailman osaavin valtio kyberturvallisuudessa. Suomessa järjestetään kansalaisille erilaisia koulutuksia kyberturvallisuuteen liittyen ja muun muassa Puolustusvoimien koulutusohjelmaan kuuluu perustason kyberturvallisuusasiat. Kansalaisille aiheen tärkeys kasvaa digitalisoitumisen myötä. Älylaitteet ja sosiaalisen median yleistyminen ovat lisänneet huomattavasti kyberturvallisuusuhkia, joihin kaikkien on varauduttava. Kyberturvallisuusuhkista on tullut tavallisten turvallisuusuhkien kaltaisia ja internetin yleistymisen vuoksi verkostoituminen näkyy selkeästi kansalaisten elämässä.

AVAINSANAT: kyberturvallisuus, tietoturvallisuus, kyberympäristö, kyberturvallisuusstrategia, esineiden internet

VAASAN YLIOPISTO
School of Technology and Innovations
Author: Matti Laukkanen
Topic of the Master's Thesis: Cybersecurity in Finland
Instructor: Tero Vartiainen
Degree: Master of Science in Economics and Business Administration
Major: Computer Science
Year of Entering the University: 2010
Year of Completing the Master's Thesis: 2018 **Pages:** 60

ABSTRACT

The purpose of this thesis was to study cybersecurity in a perspective of citizens and Finnish government point of view. Cybersecurity is a relatively important part of a citizen's daily life and the growth of the digitalization has recently highlighted the user security and privacy in the internet. Use of the internet as a communication tool increases the risk of personal data losses which might lead to the lack of privacy security. Security and privacy issues will get more attention along the quick expand of global networking in the future.

The research problem was to clarify the term of cybersecurity, what matters are related to the term and how the cybersecurity is invested in Finland. The aim of the study was to research cybersecurity generally in Finland and get closer the topic in two aspects, individual and Finnish government. This thesis focuses on those two aspects and geographically in Finland. The following topics were not included, corporate and technical overview of the cybersecurity.

This thesis was completed as a narrative literature overview and case study method was partly used as well. Research method enabled wide use of the various reference sources. Reference studies included literature, scientific articles and internet sources of the cybersecurity related material. The research problem is solved by clarifying general issues related to the cybersecurity, how these are connected to the common security and processing cybersecurity in the point of view individual and government.

According to the results achieves in this thesis, cybersecurity is well invested in Finland and as well at individual perspective. Finnish government has published strategy of cybersecurity, which goal is to be world´s leading country in cybersecurity. Educational courses are held in Finland to proof and share the knowledge of cybersecurity. The Finnish Defense Forces is one example of where common cybersecurity education is held. Importance of this topic increases for the individuals as the digitalization growth in the future. Risks of the cybersecurity are widely increased due to smart devices and social media expand which are available for every citizen. Threats has become alike to the common security threats and networking through internet is seen clearly in daily life.

KEYWORDS: cybersecurity, informaton security, cyberspace, strategy of cybersecurity, the Internet of Things

1 JOHDANTO

Turvallisuus on aina keskeinen ja tärkeä aihe yhteiskunnalle. Nopea teknologian kehittyminen sekä älylaitteiden ja erilaisten sovellusten yleistyminen ovat lisänneet jaettavan informaation määrää ja näin informaation määrä on nykyajan yhteiskunnassa kasvavassa roolissa. Informaatio on yksi yhteiskunnan tärkeimmistä arvoista, joten sen suojelu ja puolustaminen ovat yhteiskunnan kannalta tärkeää. Informaatioteknologian turvallisuus, kyberturvallisuus ja digitaalinen turvallisuus ovat kaikki turvallisuutta, jotka koskevat digitaalisen tiedon turvallisuutta verkottuneessa maailmassa. Hallitusten, organisaatioiden ja yksittäisen ihmisen maailmanlaajuisesti täytyy kohdata kyberturvallisuuden haasteet. Kyberturvallisuus koskee valtioiden ja kriittisten infrastruktuurien turvallisuutta sekä yleistä turvallisuutta, ihmishenkien turvallisuutta ja organisaatioiden taloudellista turvallisuutta. (Ghernouti-Helie 2010.)

Maailmassa yhä useampi asia toimii bittien varassa ja kyberturvallisuuden merkitys kasvaa. Digitaalisen toimintaympäristön hyväksikäyttö muuttaa maailman valtasuhteita ja antaa pienemmillekin valtioille mahdollisuuden menestyä. Virtuaalimaailmassa koko ja määrät eivät ole niinkään ratkaisevia tekijöitä, vaan osaaminen ja kekseliäisyys kun ajatellaan kilpailuetua. Digitaalisen toimintaympäristön vaikutuksen lisääntyminen tarjoaa pienille valtioille mahdollisuuksia tasoittaa valta- ja resurssieroja. Kybermaailmassa välimatkojen merkitys on olematon ja taloudelliset sekä poliittiset kumppanit voivat sijaita missä päin maailmaa tahansa. Suomessa hyvä kansallinen osaaminen on mittava taloudellinen pääoma ja suomalaiseen tietoturvaosaamiseen luotetaan maailmalla. Tällä alalla Suomella on hyvä mahdollisuus lähteä profiloitumaan digitaalisen maailman normiston rakentajana. (Haukkala & Limnell 2012.)

1.1 Tutkimuksen tavoitteet ja rajaus

Tämä pro gradu -tutkielma tutkii kyberturvallisuutta Suomessa. Tutkielman alkukappaleissa käsitellään turvallisuutta, selvitetään mitä kyberturvallisuudella tarkoitetaan ja käydään läpi kyberturvallisuuden uhat, riskit ja haavoittuvuus sekä kybersota, kyberhyökkäys- ja – puolustusnäkökulmat.

Turvallisuuden liittäminen kyberympäristöön on aihe, joka nykyään on paljon esillä erilaisissa medioissa. Aihetta tutkitaan juuri sen vuoksi, koska kyberturvallisuus yleistyy teknologioiden kehityksen myötä ja se on tärkeä osa kansalaisten arkielämää. Pro gradu – tutkielman tavoitteena on luoda kattava käsitys kyberturvallisuudesta Suomessa eri näkökulmista katsottuna. Tutkielma on rakennettu seuraavan tutkimuskysymyksen ympärille:

- Miten kyberturvallisuus näkyy Suomessa valtion ja kansalaisen näkökulmasta katsottuna?

Valitsin edellä mainitut valtion ja kansalaisen näkökulmat aiheen tutkimiseen, koska niiden perusteella saa hyvän yleistiedollisen käsityksen aiheesta. Työn alkupuolella käydään läpi turvallisuuteen liittyviä asioita ja niiden liittyminen kyberympäristöön. Tutkielman toisessa luvussa on tarkoitus avata käsitteitä aiheeseen liittyen, joita sitten käsitellään myöhemmin tapaustutkimuksen muodossa. Aihe on rajattu kybertuvallisuuden peruskäsitteisiin ja niiden käsittelyyn Suomessa. Kyberturvallisuutta avataan valtion ja kansalaisen näkökulmista, mutta tarkka teknisten asioiden yksityiskohtainen käsittely jää tämän tutkielman ulkopuolelle.

1.2 Tutkimusmenetelmä

Tutkielma toteutetaan tapaustutkimuksena, jossa kohteena on Suomi. Varsinainen tutkimusmenetelmä on narratiivinen kirjallisuuskatsaus, joten teoria pohjautuu tieteellisiin artikkeleihin ja alan kirjallisuuteen. Erityistä esitutkimusta ei tehdä, vaan käytettävä tieto haetaan kirjoista ja internetistä löytyvästä sähköisestä materiaalista. Tutkimuksessa käytetään aiheeseen liittyvää julkaistua kirjallisuutta, elektronisia tietokantoja sekä kyberturvallisuusaihetta käsitteleviä internetsivuja ja julkaisuja. Narratiivinen kirjallisuuskatsaus valikoitui tutkimusmenetelmäksi, koska sen luonteeseen kuuluu, että tutkittava ilmiö kuvataan laaja-alaisesti, ja kuvailevan kirjallisuuskatsauksen alalajina myös tutkimuskysymykset ovat yleisesti väljempiä kuin esimerkiksi systemaattisessa kirjallisuuskatsauksessa (Salminen 2011: 6).

1.3 Tutkimuksen rakenne

Tutkielman toisessa luvussa käydään läpi turvallisuuteen liittyviä asioita yleisesti, avataan kyber – sanan merkitystä ja selitetään mitä on kyberympäristö. Luvussa avataan termejä kyberturvallisuuteen liittyen ja kerrotaan turvallisuudessa kybermaailmassa. Kolmannen luvun tarkoitus on esitellä peruskäsitteitä ja teoriaa kyberturvallisuuteen liittyen, joita sitten tapaustutkimuksen muodossa käsitellään myöhemmin. Neljännessä luvussa esitellään tutkielman muoto ja tutkimusmenetelmä. Neljäs luku pitää sisällään teoriaa tapaustutkimukseen ja tutkimusmenetelmään liittyen. Luvun tarkoitus on avata käsitys tutkielman tavoista käsitellä aihetta ja perehdyttää lukija tutkimusmenetelmään.

Viides luku käsittelee kyberturvallisuutta Suomen valtion näkökulmasta. Tässä luvussa esitellään valtion toimenpiteitä kybertuvallisuuden ylläpitämiseksi sekä strategisia linjauksia. Kuudes luku käsittelee aihetta kansalaisen näkökulmasta. Luvun tarkoitus on avata käsiteltävää aihetta ja sen tärkeyttä kansalaisille. Kansalaisten kannalta esitellään keskeisimmät asiat kyberturvallisuuteen liittyen. Tutkielman viimeisessä luvussa keskustellaan aiheesta ja tuloksista, esitetään jatkotutkimusehdotuksia sekä tehdään johtopäätöksiä kirjallisuuskatsauksen muodossa tehdystä tutkimuksesta. Tämä viimeinen eli diskussio -luku kokoaa tutkielman aiheen ja tulokset päättäen tehdyn tutkimustyön.

2 TURVALLISUUS JA KYBERYMPÄRISTÖ

Tämä luku sisältää aiheen pohjustukseksi peruskäsitteitä turvallisuuteen ja kyberturvallisuuteen liittyen. Luvussa lähetään syventymään aiheeseen perusasioita esittämällä aikaisempien tutkimusten ja muiden tieteellisten lähteiden pohjalta. Ensin käydään läpi mitä on turvallisuus ja sitten avataan kyber – termistöä. Kyberturvallisuus pitää sisällään turvallisuuteen ja kyberympäristöön olennaisesti liittyviä asioita, joten on hyvä lähteä perehtymään aiheeseen perusasiat läpikäymällä.

2.1 Turvallisuus

Turvallisuus tarkoittaa vaaran poissa olemista, ja sitä esiintyy ilmiönä kaikkialla missä on jonkinlaista vaaraa. Maailman verkottuessa turvallisuuden piirteet uudistuvat ja täydellinen turvallisuus on usein absoluuttisesti mahdotonta. Turvallisuutta uhkaavaa vaaraa ei voida koskaan poistaa kokonaan, vaan kyse on vaaran vähentämisestä ja siitä kuinka paljon sen eteen ollaan valmiita panostamaan. Näin on erityisesti toiminnoissa, joissa ihminen ja tekniikka ovat mukana. (Oulun yliopisto 2015.)

Terminä turvallisuutta käytetään monien eri asioiden yhteydessä. Esimerkiksi sodassa (sotilaallinen turvallisuus), rikollisuudessa, onnettomuuksissa, työssä (työturvallisuus), elintarvikkeissa, liikenteessä ja tiedossa (tietoturvallisuus) tulee turvallisuus esille. Täydellisen turvallisuuden tavoitteleminen on mahdotonta, eikä siitä kannata edes haaveilla. Oma ja yhteinen turvallisuus on mitoitettava resurssien ja arvostusten mukaisesti ja jäljelle jäänyt riski on huomioitava. Ihmisten pitää osata elää turvallisuuden ulkopuolelle jäävän epävarmuuden kanssa. (Oulun yliopisto 2015.)

Turvallisuus on sitä, mitä ihminen tuntee, kuten hallinnan tunne, osallisuuden tunne ja yksilönä pärjäämisen tunne. Yksilön ympäriltä löytyy yhteiskunnan ja sen eri yksilöiden punoma turvaverkko, josta saa apua turvallisuuden tuntemiseen. Perinteiset turvallisuustoimijat, kuten pelastuslaitos ja poliisi kuuluvat tähän turvaverkkoon. Turvallisuuden tunne on peräisin kansalaisesta itsestään ja jokainen yhteisön yksilö luo turvallisuutta ympärilleen. (Sitra 2014.)

Perinteisesti ajateltuna turvallisuus on tuotu jostain muualta, erillisenä osana tarpeiden mukaan. Nykyään nopeasti muuttuvassa maailmassa turvallisuusuhat tulevat niin yllättävistä paikoista, ettei varautuminen aina riitä. Juuri tämän takia yhteiskunnalta vaaditaan ennakointia ja joustavuutta, jotta turvallisuus otetaan huomioon kaikessa yhteiskunnan toiminnassa. (Sitra 2014.)

Perinteisessä turvallisuuskäsityksessä on kyse valtion tehtävästä suojella kansakuntaa viholliselta. Turvallisuuskäsite rajataan usein turvallisuuspolitiikkaan, jota valtiot harjoittavat. Siihen liittyen keskeisimmät toimijat ovat Puolustusvoimat, puolustusliitot ja Yhdistyneet kansakunnat. Tämä turvallisuus käsitetään ulko- ja puolustuspoliittisena turvallisuutena tarkoituksenaan kansallisen vapauden ja itsenäisyyden turvaaminen. Maailmanlaajuinen tavoite on maailmanrauha. Valtion tehtävänä on sisäisen järjestyksen ylläpitäminen ja kansalaisten koskemattomuuden ja oikeuksien suojaaminen. Tätä sisäpolitiikan piiriin kuuluvaa turvallisuuspolitiikkaa hoitavat poliisi ja oikeuslaitos. (Niemelä ja Lahikainen 2000: 25–26.)

2.2 Sisäinen turvallisuus

Sisäinen turvallisuus on sisäministeriön piiriin kuuluva vastuualue. Sisäisen turvallisuuden keskeisimmät toimet ovat poliisitoimi, pelastuslaitos, rajavaltiolaitos ja hätäkeskuslaitos. Turvallisuusviranomaisten vastuulla on suuria tehtäväkokonaisuuksia, jotka liittyvät oleellisesti yhteiskunnan turvallisuuteen. (Sisäministeriö 2015.)

Sisäiseen turvallisuuteen Suomessa on luotu strategia, jonka valtioneuvosto on hyväksynyt 5.10.2017. Strategian tavoitteena on tehdä Suomesta maailman turvallisin maa. Sisäisen turvallisuuden strategia kostuu megatrendeistä, muutosvoimista, päämääristä ja toimenpiteistä. Näistä neljästä osa-alueesta kolme viimeisintä sisältävät erilaisia tekijöitä, jotka strategiassa erotellaan seuraavanlaisesti:

Päämäärät:

- turvallisuusympäristön analysointi ja sen muutoksien ennakointi
- syrjäytymisen aiheuttaman turvattomuuden torjunta ennalta ehkäisevästi
- turvallisuusrakenteiden ja -prosessien tehostaminen ja vaikuttavuus
- yksilön ja yhteiskunnan kriisinkestokyvyn ylläpito ja parantaminen

Muutosvoimat:

- ääriliikkeet ja -ideologiat
- monimuotoinen polarisaatio (ryhmän vaikutus yksilön toimintaan)
- arvojen sirpaloituminen
- julkinen talous
- maahanmuuton turvallisuusvaikutukset
- globaali turvallisuusympäristö
- teknologia

Sisäisen turvallisuuden toimintaympäristö on todella monimuotoinen ja siihen vaikuttaa kasvavissa määrin Suomen ulkopuoliset tekijät. Tulevaisuudessa muutoksia on odotettavissa enemmän ja niihin on vaikeampi varautua etukäteen.

Toimenpiteet:

- analysointi ja varautuminen
- toimivaltuudet ja kapasiteetti
- turvallisuus arki elämässä
- asiantuntemus ja kriisinkestokyky
- turvallisuuden uudistukset
- turvallisuuden valvominen
- maakuntien ja kuntien työ
- tarkkailu

(Sisäministeriö 2017.)

Strategia keskittyy ilmiöihin, joissa turvallisuusriskit ovat viime vuosina kasvaneet ja joiden arvioidaan aiheuttavan eniten haittaa yhteiskunnan turvallisuudelle lähitulevaisuudessa. Strategian toimeenpanoon on nimetty ohjaus- ja seurantaryhmä, jonka keskeisimpiä tehtäviä ovat toimeenpanosuunnitelman vahvistaminen ja seuraaminen sekä toimenpiteiden toteuttamisesta raportoiminen turvallisuuden ja oikeudenhoidon ministeriryhmille. (Sisäministeriö 2017.)

Sisäisen turvallisuuden tarkoitus on luoda yhteiskunnalle turvallinen olotila. Siihen kuuluu kansalaisten oikeus nauttia oikeusjärjestelmän eduista ja vapauksista ilman rikollisuutta sekä ylimääräisiä häiriöitä. Sisäinen turvallisuus varmistaa sellaisten toimintamallien käyttöönoton, joiden avulla viranomaiset ja järjestöt voivat sekaantua yhteiskunnan,

yhteisöjen ja niihin kuuluvien yksilöiden turvallisuutta vaarantaviin tilanteisiin. (Sisäasiainministeriö 2012.)

2.3 Tietoturva

Tietoturvalla tarkoitetaan tietojen, järjestelmien, tietoliikenteen ja palveluiden suojaamista hallinnollisilla, teknisillä ja muilla toimenpiteillä olosuhteista riippumatta (Pietikäinen 2013). Tietoturva on laaja aihe, jolla on pyrkimys kolmeen tavoitteeseen. Näitä tietoturvan kannalta keskeisiä asioita ovat luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa, että tiedon pitää säilyä luottamuksellisena eli henkilökohtainen ja salassa pidettävä tieto pitää olla vain oikeiden ihmisten saatavilla. Tietoja suojataan lukoilla, salasanoilla, käyttäjäoikeuksien rajoituksilla ja salausalgoritmeilla. Eheys tarkoittaa, että tiedon käsittelyn ja käytön aikana siihen saa kohdistua vain oikeutettuja muutoksia. Saatavuus puolestaan tarkoittaa sitä, että tieto pitää olla saatavilla ja käytettävissä. Saatavuutta vaikeuttaa koneiden rikkoutuminen, nettiyhteyksien katkeaminen ja sovellusten kaatuminen. Tietoturvan tarkoitus on suojata itse tietoja ja tietojärjestelmiä. Tietojärjestelmien toiminta halutaan varmistaa kaikissa olosuhteissa, ja niiden käytön turvallisuus edellä mainittujen kolmen tavoitteen toteuttamiseksi. (Järvinen 2012: 10–12.)

Tietoturvan varmistaminen ja saavuttaminen edellyttävät todentamista. Todentaminen on osapuolten henkilöllisyyden varmistamista ja se on käytännön tilanteissa vaikeaa. On hankala löytää toimintatapoja, joilla ihmisten henkilöllisyys ja laitteiden sekä verkkopalvelujen aitous voidaan aukottomasti varmistaa. Tämän takia useat tietoturvaongelmat johtuvat todentamisen ongelmista eikä huonosta salauksesta tai epäluotettavista laitteista. (Järvinen 2012: 12.)

Ihmiset ovat tekemisissä tietoturvan kanssa kolmella eri tasolla. Nämä kolme tasoa ovat henkilökohtainen, työ ja kansallinen. Henkilökohtaiseen tasoon kuuluvat nettipalvelut, sähköinen asiointi, matkapuhelin ja kodintekniikan laitteet. Esimerkkejä asioista, joihin liittyy tietotekniikkaa ja sen myötä tietoturvakysymyksiä henkilökohtaisella tasolla, ovat harrastukset, liikkuminen, tiedonhankinta ja viestintä. Näissä asioissa omalla toiminnalla on suuri merkitys tietoturvan toteutumiseksi. Nykyään lähes jokaisessa työssä ja ammatissa on hallittava tietotekniikan perusteet. Työelämässä on käytössä tietokoneita ja älypuhelimia, joiden mukana työt siirtyvät työpaikoilta muuallekin. Tulee muistaa, että työpaikalla annetut tietoturvaohjeet koskevat myös muualla kuin työpaikalla tehtyjä työasioita. (Järvinen 2012: 13–14.)

Organisaatiotasolla tietoturva muodostuu teknisistä ja hallinnollisista asioista sekä niiden suunnittelusta, toteutuksesta ja seurannasta organisaation tavoitteiden mukaisesti (Laaksonen, Nevasalo & Tomula 2006: 17). Tietoturvallisen ympäristön toteutumisen kannalta on tärkeää, että tietoturvaasiat huomioidaan organisaation jokaisessa yksikössä ja niiden mukainen toiminta pitää olla osana työntekijöiden päivittäisiä toimia (Laaksonen ym. 2006: 116).

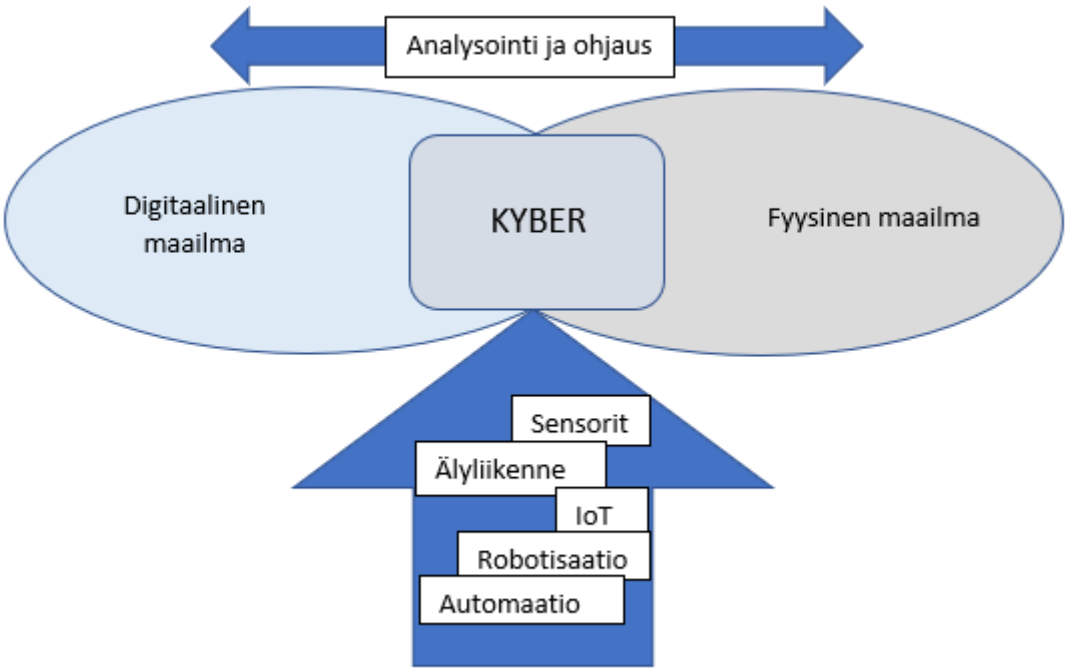
Kuva 1. Viisi askelta tietojen turvaamiseen (Kotisalo & Järvinen 2017).

Kuvassa 1 esitellään viisi askelta tietoturvan parantamiseksi. Tietoturvauhkilta suojaudutaan parhaiten varautumalla niihin. Suojattavien kohteiden ja riskien tunnistaminen ovat tärkeimpiä asioita, jotta voidaan säätää asetukset sekä tilata suojauspalvelut niiden mukaan. Suojauspalveluja ovat palomuurien lisäksi salasanat sekä virustentorjuntaohjelmat. Kuvassa esitetyt viisi askelta muodostavat syklin, joka toimii parhaiten, kun sitä toistaa mahdollisimman säännöllisesti. (Kotisalo & Järvinen 2017.)

Kansallisella tasolla tietoturva on Suomessa ylpeyden aihe. Kansainvälisissä vertailuissa suomalaisten koti- ja työkoneiden on havaittu olevan maailman puhtaimpia. Tietoturva kuuluu koulujen opetukseen ja se on muutenkin kansallisesti esillä. Kansallisella tasolla tietoturvassa on kyse koko maan turvallisuudesta. (Järvinen 2012: 14.)

2.4 Kyber

Sana ”kyber” juontaa juurensa kybernetiikasta, jonka Wiener määritteli vuonna 1948 omaksi tieteekseen. Kybernetiikalla tarkoitetaan tiedettä, missä elollisen olennon ja koneen välistä kommunikointia ja viestintää toteutetaan (Ashby 1957,1). Sanaa käytetään yleensä yhdyssanan määriteosana ja sen merkitys viittaa sähköisessä muodossa olevan tiedon käsittelyyn, eli tietotekniikkaan, tiedonsiirtoon ja tietojärjestelmiin (Rautiainen 2013). Kyber-sana on liitetty digitaaliseen ympäristöön vanhan tieteiskirjallisuuden perusteella. 1940 -luvulta lähtien biologian, insinööri- ja sosiaalitieteiden toimijat käyttivät sanaa ”cyborg” kuvaamaan elävien organismien ja koneiden hallintaa. Koneiden ja organismien yhdistelmä viittasi älyllä varustettuihin laitteisiin (Kantola 2017).



Kuva 2. Kyber on bittien ja atomien vuorovaikutusta (Kasvi 2016).

Kuva 2 esittää ”kyberin” muodostumista digitaalisen ja fyysisen maailman väliin. Aiemmin bitit ja atomit ovat olleet ”erillään”, mutta teknologian kehityksen myötä niiden väliin on muodostunut ”kyber”, jonka kautta ne yhdistyvät. Perinteiset tietoturvauhat kohdistuvat lähinnä tietoon, mutta kyber:n välityksellä uhkatekijät saavuttavat fyysisen maailman. Tämän johdosta digitaalinen maailma ja fyysinen maailma ovat vuorovaikutuksessa keskenään, ja digitaalinen analysoi ja ohjaa fyysistä maailmaa. (Kasvi 2016.)

2.5 Kyberympäristö

Kyberympäristö muodostuu ympäristöstä, jossa toimii yksi tai useampi sähköisen informaation käsittelyyn tarkoitettu järjestelmä. Tällaisessa ympäristössä voidaan käsitellä, muokata, varastoida ja siirtää tietoa. Kyberympäristöön kuuluvat fyysiset rakenteet eli tietokoneet, kaapelit, viestirakenteet, mutta myös ohjelmistot sekä käyttäjät käyttäjäprofiiliensa kautta. Kyberympäristöstä käytetään myös sanaa kybertoimintaympäristö. (Kantola 2017.)

Kybertoimintaympäristö on kuin ihmisten luoma digitaalinen rinnakkaistodellisuus, jossa yhdistyvät ihmiset ja laitteet toisiinsa informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta. Kybertoimintaympäristö ulottuu yli valtioiden rajojen. Kybertoimintaympäristössä toimii paljon haavoittuvaisia digitaalisia verkkoja, joten on ensisijaisen tärkeää varmistaa verkkojen turvallinen sekä luotettava toiminta. Tällainen ympäristö tuo paljon mahdollisuuksia valtioille, yrityksille ja kansalaisille, kuten esimerkiksi uusien liiketoimintojen harjoittaminen sekä sosialisoituminen. (Ulkoministeriö 2018.)

Kyberympäristö rakentuu monisyisestä ja -kerroksisesta globaalista informaatioverkostosta, johon kuuluu eri tahojen kommunikaatioverkkoja. Tällaisia tahoja ovat turvallisuusviranomainen, julkishallinto ja yritysorganisaatiot. Lisäksi verkostoon kuuluu teollisuuden ja infrastruktuurin ohjaus- ja valvontajärjestelmiä. Kyseinen ympäristö toimii reaaliaikaisena yhdistävänä tekijänä valtioiden, yrityksien ja kansalaisten välillä. Ympäristön kehitys on tuonut mukanaan uusia riskejä, mutta se on myös lisännyt hyvinvointia sekä muokannut valta-asetelmia eri maiden välillä. Kyberympäristö luo myös pienille valtioille sekä yksityisille toimijoille mahdollisuudet tehokkaaseen toimintaan, koska siinä ympäristössä osaaminen on hallitsevaa. Kyberympäristössä laitteiden ja järjestelmien ongelmat sekä kyberhyökkäykset saavat aikaan negatiivisia seurauksia hallintoon,

palveluihin ja yrityselämään sekä toimintaan yhteiskunnassa. (Suomen kyberturvallisuusstrategian taustamuistio 2013: 17.)

Kyberympäristö on voimavara, joka luo runsaasti uudenlaisia mahdollisuuksia. Turvallinen kyberympäristö auttaa yksilöiden sekä yritysten toimintaa, ja helpottaa niiden toimimista. Turvallinen toimintaympäristö myötävaikuttaa valtioiden houkuttelevuutta kansainvälisinä investointikohteina. Uutena ja vahvistuvana alueena kyberympäristö antaa valtioille ja yrityksille mahdollisuuksia menestymiseen myös liiketoiminnan kannalta. (Suomen kyberturvallisuusstrategia 2013: 1.)

Informaation muokkaamiseen, varastointiin ja siirtoon kyberympäristössä on ominaista datan ja viestintäverkkojen tuella sähkömagneettisen spektrin ja elektroniikan käyttö. Kyberympäristöön lasketaan kuuluviksi kaiken muun lisäksi fyysiset rakenteet, jotka liittyvät informaation käsittelyyn. (Suomen kyberturvallisuusstrategia 2013: 12.)

2.6 Kybermaailma

Kybermaailma määritellään globaaliksi ja moniulotteiseksi tieto- ja kommunikaatioverkoksi, johon kytkeydytään kiinteän tai liikkuvan päätelaitteen avulla. Se on internetin, muiden fyysisten verkkojen, digitaalisten palveluiden sekä virtuaalitodellisuuden yhteen sulautuma tai useiden käyttäjien virtuaaliympäristö, jossa toiminta on virtuaalista. (Lehto 2013: 10.)

Nykymaailma on muuttunut niin paljon tekniikan osalta, että on alettu yhä enemmän kiinnittämään huomioita edellä mainittuun kybermaailmaan. Muutoksen ovat tehneet aika, data, verkko ja äly. Nykyään internetissä jaetaan tietoa valtavia määriä ja esimerkiksi jokaisen minuutin aikana jaetaan 216000 valokuvaa Instagram -palvelussa. Informaatioteknologian räjähdysmäinen kasvu on muodostanut globaalin verkoston verkottuneiden laitteiden avulla. Koneiden älykkyys kasvaa koko ajan ja niillä korvataan ihmisten osaamista. Kybermaailma kasvaa koko ajan ja toiminta siirtyy yhä enemmän koneiden ja sovellusten väliseksi toiminnaksi. (Lehto 2013: 10.)

Kybermaailma muodostuu neljästä eri kerroksesta. Nämä kerrokset ovat fyysinen, syntaktinen, semanttinen ja pragmaattinen kerros. Fyysinen kerros pitää sisällään verkkolait-

teet, kytkimet, reitittimet, langalliset ja langattomat yhteydet. Syntaktinen kerros muodostuu järjestelmän ohjaus- ja hallintaohjelmista, verkkoprotokollista ja virheenkorjauksesta. Semanttiseen kerrokseen tulee käyttäjän informaatio- ja tietosisältö sekä toimintojen ohjaus. Pragmaattisessa kerroksessa puolestaan tapahtuu informaation merkityssisällön ymmärtäminen ja tulkinta. Kybermaailma siis syntyy näiden kerrosten yhteistoiminnasta eli laitteelta lähtevän informaation kulkemisesta aina sisällön ymmärtämiseen ja tulkintaan. (Lehto 2013: 9-10.)

3 KYBERTURVALLISUUDEN KÄSITTEET

Turvallisuus kyberympäristössä on asia, joka korostuu koko ajan enemmän, kun verkostoituminen maailmassa kasvaa. Käytettävien verkottuneiden laitteiden ja sovellusten varjopuolena on haavoittuvuus ja erilaisiin uhkiin varautuminen lisää huomattavasti niiden turvallisuutta. Tietoyhteiskunnan kehittymisen myötä erilaisia toimintoja ja palveluita käytetään sähköisessä toimintaympäristössä, mikä lisää yhteiskunnan haavoittuvuutta. Sähköiseen toimintaympäristöön ilmestyy eri tahoilta palveluille haitallisia ohjelmia, joita kutsutaan haittaohjelmiksi. Näillä haittaohjelmilla voidaan estää pääsy palvelimelle tai lamauttaa tietojärjestelmä (Pekander 2016: 4).

Tulevaisuudessa valtaosa palveluistamme ovat tieto- ja viestintätekniikan avulla tuotettuja digitalisoituja kokonaisuuksia. Digitalisoitumisen myötä myös kyberturvallisuus on merkittävä kehityksen edellytys ja mahdollistaja. Olemme tälläkin hetkellä pelottavan riippuvaisia teknologiasta ja esimerkiksi sähkö- ja tietoliikenneverkkojen toiminnasta. Riippuvuus kasvaa koko ajan, joten on ensisijaisen tärkeää, että riskienhallinta, tietoturvallisuus, yksityisyydensuoja ja kyberturvallisuus paranevat jatkoa ajatellen. Kimmo Rousku artikkelissaan sanookin: ”Mitä laaja-alaisemmin digitalisaatio iskee yhteiskuntaan, sitä tärkeämpää on varmistaa kyberturvallisuuden osa-alueiden toteutuminen osana palvelukokonaisuutta”. (Rousku 2015.)

3.1 Kyberturvallisuus

Haavoittuvuus järjestelmissä on yleensä tulos tahallisesta tai tahattomasta laiminlyönnistä tai suunnittelussa on tapahtunut virhe, joka suoraan tai välillisesti vahingoittaa järjestelmän käytettävyyttä, eheyttä tai luottamuksellisuutta. Haavoittuvuuksia on kybertoimintaympäristön turvallisuudessa monenlaisia. Turvallisuus on olennainen asia elämässä ja siihen liittyy kyberavaruudessa monenlaisia asioita, kuten tiedon turvallisuus, tietokoneen ja varastoinnin turvallisuus, kommunikaation turvallisuus sekä toiminnallinen ja fyysinen turvallisuus. Käsiteltäessä tietojärjestelmää, turvallisuuden tärkeimmät osatekijät ovat ihmiset, laitteisto ja ohjelmisto. Kyberturvallisuuteen liittyen tietojärjestelmässä on kolme osa-aluetta, jotka vastaavat kyberavaruuden tiedon saatavuudesta, eheydestä ja luottamuksellisuudesta. Nämä ovat ihmisten ammattitaito, ohjelmistojen luotettavuus ja

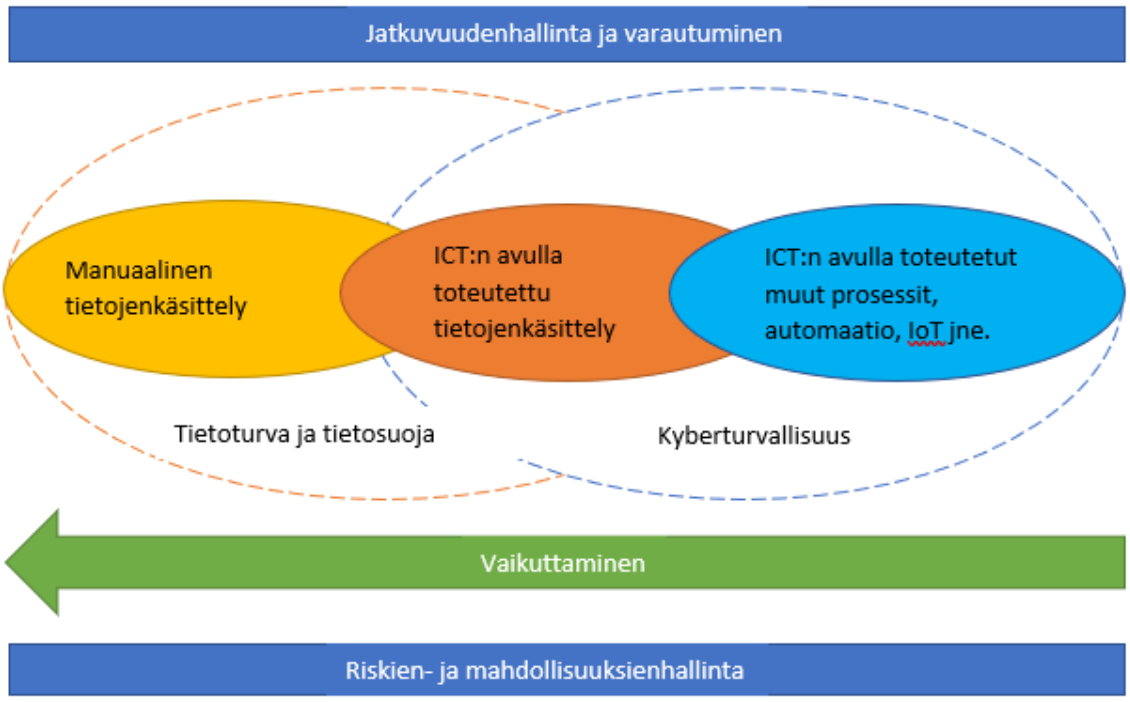
laitteiston toimintavarmuus. Näihin kolmeen asiaan panostaen pyritään kyberturvallisuuteen kyberavaruudessa. (Kostopoulos 2013: 1-2.)

Kyberturvallisuudella tarkoitetaan toimintoja ja toimenpiteitä kyberympäristön järjestelmien, prosessien ja toimijoiden turvaamiseksi. Se voidaan myös mieltää tilaksi, jossa kyberympäristössä toiminta on luottavaista ja turvattua. Kyberturvallisuuden tarkoitus on turvata järjestelmien lisäksi niihin liittyvä infrastruktuuri, prosessit ja käyttäjien toiminta. (Kantola 2017.)

Kybermaailmasta ja kyberturvallisuudesta on tullut teknologian kehityksen myötä tärkeä osa arkipäivää. Maailmantalous, yhteiskuntien turvallisuus, yritysten toiminta ja arkipäiväinen elämämme ovat pitkälti riippuvaisia bittien toimivuudesta. Riippuvuus bittien turvallisesta toiminnasta lisääntyy koko ajan digitaalisen maailman kasvaessa. Kehittyvän teknologian mukana tuomat mahdollisuudet sekä niiden mukana tullut haavoittuvuus lisääntyy. Digitalisoituvassa maailmassa kyberturvallisuuden takaavien perustaitojen osaaminen tulee olla yhtä lailla kansalaistaito, kuten lukeminen, laskeminen ja kirjoittaminen. Kyberturvallisuus kuuluu kaikille, koska kybermaailma on älypuhelinten ja muiden älylaitteiden ansiosta kaikkialla läsnä ja se läpäisee kaikki turvallisuuden tasot ja ulottuvuudet. (Limnell, Majewski & Salminen 2014: 13.)

Kybermaailman tapahtumilla on suoria vaikutuksia fyysiseen maailmaan ja arkipäivän toimivuus on riippuvainen bittien toimivuudesta. Toimiva ja paras kyberturvallisuus luodaan siten, että se rakennetaan suoraan käytettäviin järjestelmiin, tuotteisiin ja ratkaisuihin. Siinä tulee ottaa huomioon kaksi erityisen tärkeää asiaa. Ensimmäisenä kyberuhat, jotka ovat todellisia ja pahimmillaan vaikutuksiltaan todella vakavia. Välinpitämättömyydestä joutuu helposti maksamaan moninkertaisen hinnan. Toisena asiana on kyberturvallisuuden positiivinen puoli, nimittäin mahdollisuudet. Kyberturvallisuudesta puhuttaessa keskitytään monesti kyberuhkiin ja sen mahdollisuudet jäävät pienemmälle huomiolle. Kybermaailma tarjoaa kuitenkin suuria mahdollisuuksia, kuten esimerkiksi yritysten toiminnan laajentaminen, palveluiden kehittäminen ja kustannusten alentaminen. Tärkeää on löytää tasapaino mahdollisuuksien ja uhkien välille ja huomioida siinä kunkin organisaation erityispiirteet ja tilanne. Kyberturvallisuudesta sanotaankin, että se on tasapainottelua mahdollisuuksien ja uhkien välillä. (Limnell, Majewski & Salminen 2014: 14–15.)

Useasti kyberturvallisuus liitetään internetverkon sekä tieto- ja viestintätekniikan(ICT) -toimintojen yhteyteen, mutta todellisuudessa ne ovat vain pieni osa-alue, jota kyberympäristössä hyödynnetään. Kyberturvallisuus on laaja kokonaisuus, jonka yhtenä osa-alueena on tiedon turvaaminen ja organisaation jatkuvuuden takaaminen erilaisissa häiriötilanteissa. Sillä pyritään huolehtimaan yhteiskunnan toimimisesta ja elintärkeiden, kriittisten toimintojen turvaamisesta kaikenlaisissa olosuhteissa. Tällaisia toimintoja ovat sähkönjakelu, pankkien maksuliikenne ja yhteiskunnan johtaminen. Kyberturvallisuudessa suojataan laajasti kaikkea infrastruktuuria ja siihen kuuluu olennaisesti kyberpuolustus, -hyökkäys ja -sodankäynti. Sille on olennaista myös kyberuhat, jotka tulevat esille myöhemmin. (Rousku 2012.)



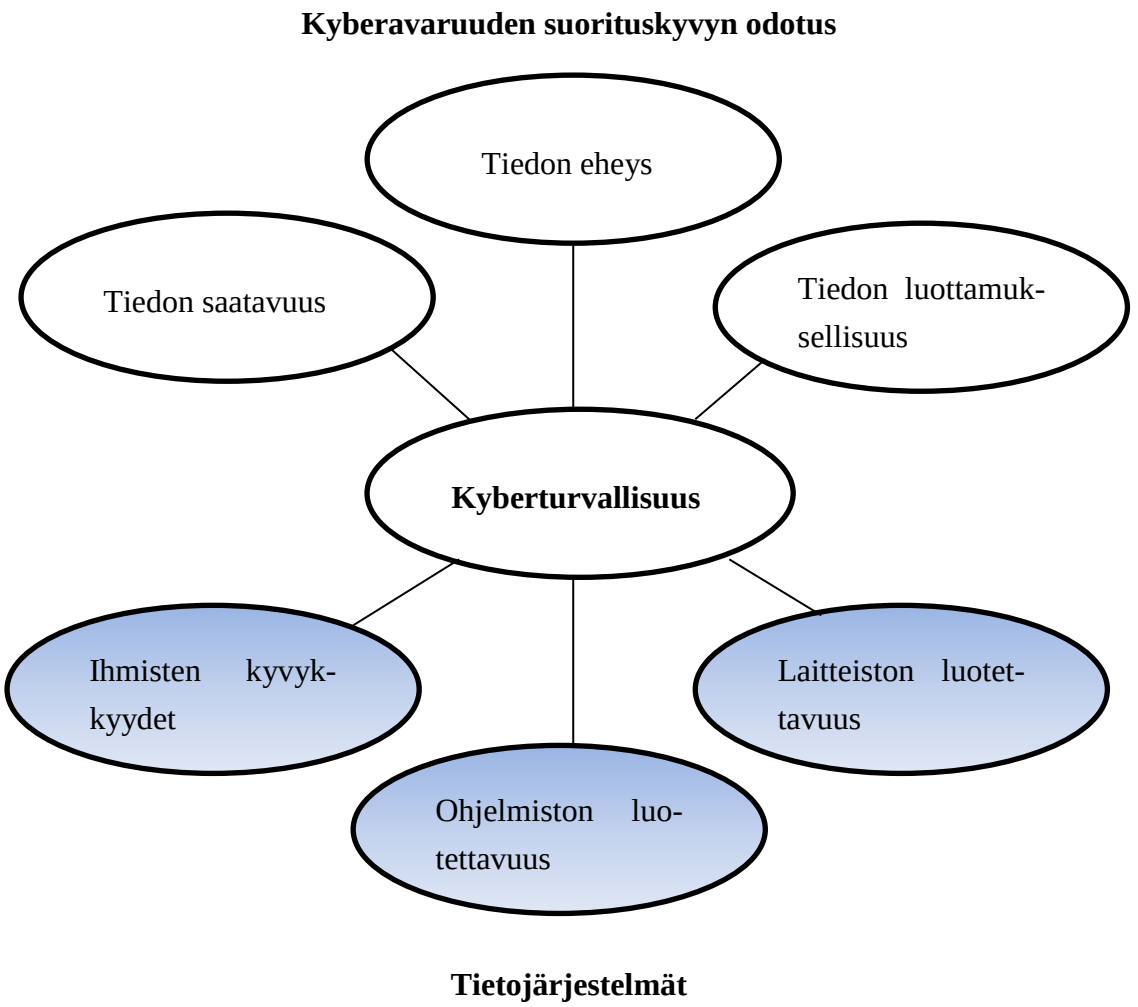
Kuva 3. Kyberturvallisuus ja ICT -toiminta (Rousku 2015).

Kyberturvallisuuden keskeisiä osa-alueita Kimmo Rouskun (2015) mukaan ovat tietoturva fyysisine rakenteineen, tietosuoja, jatkuvuudenhallinta ja varautuminen sekä riskien- ja mahdollisuuksienhallinta. Tämä on esitetty kuvassa 3, jossa näkyy myös tietoturvan kolme fyysistä rakennetta.

Tietoja käsitellään edelleen myös manuaalisesti, koska ICT ei ulotu vielä kaikkialle. Leviävä digitalisoituminen korostaa tietoturvallisuutta, joka turvaa tietoa sekä kyberturvallisuutta, joka turvaa toimintaa. Keskeinen rooli ICT:n turvallisuuden toteuttamisessa on nimenomaan kyberturvallisuudella. Keskittymällä kyberturvallisuuteen huolehditaan siitä, ettei ICT -palveluista aiheudu haittaa, häiriötä tai vaaraa sähköisen informaation käsittelystä riippuvaiselle toiminnalle. Kyberturvallisuus osana digitaalista turvallisuutta keskittyy ICT -toiminnan teknisen puolen turvaamiseen. Jotta voidaan puhua digitaalisesta turvallisuudesta, tarvitaan siihen lisäksi käyttäjän eli kansalaisen tai organisaation näkökulma. Nämä näkökulmat sisältävät tietosuojan ja yksityisyydensuojan, joten kyberturvallisuus liitettynä näihin saadaan aikaan digitaalinen turvallisuus. Ilman kyberturvallisuutta ja digitaalista turvallisuutta ei voida organisaatiotasolla hallita kokonaisuuteen liittyviä riskejä ja uhkia. (Rousku 2015.)

Jokainen valtio vastaa turvallisuudesta kyberavaruudessa ja keskittyy turvallisuuden sosiaalisiin, taloudellisiin, teknologisiin ja poliittisiin osa-alueisiin. Yhteiskunta odottaa viranomaisten hoitavan turvallisuutta läpinäkyvällä, tehokkaalla ja vaikuttavalla tavalla. Yksityisyysoikeuksia ja omien mielipiteiden ilmaisun vapautta pidetään tärkeinä. Lainsäätäjillä ja sosiologeilla on ollut monia haasteita tasapainon löytämiseksi kansalaisoikeuksien ja turvallisuuden välillä ja tasapaino edellyttää sosiaalista kanssakäymistä, jonka seurauksena toiminta kehittyy. Kyberturvallisuuspolitiikka on parhaimmillaan silloin, kun se vastaa ihmisten yksityiskohtaisesta turvallisuudesta. Kyberturvallisuus on paljolti kiinni siihen käytettävistä resursseista. Mitä enemmän resursseja käytetään, sitä tehokkaampaa se on. Vastuulliset johtajat kuitenkin jakavat resursseja kyberturvallisuuden eri osa-alueille maksimoidakseen yleistä turvallisuutta. Kyberturvallisuus vaatii korkeasti koulutettuja henkilöitä, joiden jatkokoulutusta pidetään menestyksen kulmakivenä. Tärkeä haaste kybertaloudessa on kyberturvallisuuden mittaaminen. (Kostopoulos 2013: 187.)

Kuvassa 4 esitetään kybertuvallisuuden syntymiseen edellytettävät tekijät. Kyberturvallisuuden edistäminen lähtee kyberavaruuden suorituskyvystä, joka pitää sisällään tiedon saatavuuden, eheyden ja luottamuksellisuuden. Nämä ovat kaikki oikeanlaiseen tietoon liittyviä ominaisuuksia. Tietojärjestelmiin ja niiden käyttöön liittyen tarvittavia vaatimuksia ovat ihmisten kyvykkyys, ohjelmiston luotettavuus sekä laitteiston luotettavuus. Kyberturvallisuus rakentuu kyberavaruuden suorituskyvyn ja tietojärjestelmien välisten tekijöiden seurauksena. (Kostopoulos 2013: 2.)



Kuva 4. Kyberavaruuden ja tietojärjestelmien vaatimukset kyberturvallisuuden edistämiseksi (Kostopoulos 2013: 2).

3.2 Kyberuhat, riskit ja haavoittuvuudet

Kybermaailman negatiivinen puoli on sen mukanaan tuomat uhat ja erilaiset epävarmuudet. Kyberturvallisuuden tarkoitus on taistella kybermaailman uhkia vastaan, ennaltaehkäistä, torjua ja lieventää niiden vaikutuksia. Uhat, riskit ja haavoittuvuudet vaikuttavat toinen toisiinsa ja ne ovat luonteeltaan suhteellisia ja rajallisia (resurssit, aika, kyky ja vahingoittavuus). Uhat, riskit ja haavoittuvuudet ovat aina toimija- ja tilannekohtaisia. (Limnell ym. 2014: 105.)

Uhka on käytännössä pakottavaa toimintaa, ja uhkailulla pyritään tekemään negatiivinen vaikutus hyökättävään kohteeseen ja sen toimintaan. Uhkailun tarkoitus on saada hyökkäyksen uhri toimimaan uhkaajan haluamalla tavalla ja viestimään uhan aiheuttajalle sekä sen toimintaympäristöön. Kyseessä ei ole vahingoittava toiminta vaan sillä uhkaaminen. Kyberuhkan käytäntö on täysin samanlainen. Kyberuhan torjumiseen voidaan käyttää fyysisen maailman resursseja, kuten poliittista ja taloudellista vaikutusvaltaa. Paras keino kyberuhkien torjumiseen on kyberturvallisuuden perusasioista huolehtiminen ja lisätty tietoisuus sekä toimintakyky. Myös tietoturvan ajantasaisuus, kybertuvallisuuden haasteiden tunnistaminen ja niihin reagoiminen vähentävät kyberuhkien riskiä. (Limnell ym. 2014: 106.)

Kybertilan häiriöt ovat turvallisuusuhka ja Suomikin on joutunut sisäisten sekä ulkoisten kyberoperaatioiden kohteeksi. Tietoverkkoturvallisuus liittyy kansalaisten arkipäiväisiin toimintoihin, jotka kyberhyökkäyksellä voidaan lamauttaa. Sisäiset heikkoudet, vahinkoa aiheuttavat ja laittomasti toimivat ulkoiset tekijät luovat kyberuhkaa. Vapaata tietojärjestelmää käytetään hyväksi ammattirikollisten ja terroristien tahoilta ja kyberuhkissa piilee uudenlaisen sodankäynnin mahdollisuus. Kyberturvallisuuden uhkiin tulee varautua monipuolisesti ja ajoissa. (Lohela 2013.)

Kybermaailman nopea kehitys vaikeuttaa ajan tasalla pysymistä, joten tietoisuus ja toimintakyvyn säilyminen kyberhyökkäyksen kohdatessa on tärkeää. Kyberuhat voivat olla organisaation sisäisiä tai ulkopuolisia. Sisäiset uhat liittyvät organisaation talouteen, maineeseen ja tietopääomaan. Niiden lähteinä ovat pääasiassa ”sisäpiiriläiset”, jotka ovat katkeroituneet tai muuten haluavat tehdä vahinkoa organisaatiolle. Usein heillä on tarvittavat käyttöoikeudet tai pystyvät hankkimaan sellaiset varastaakseen tietoa tai vahingoittaakseen kohdetta. Sisäinen uhka liittyy myös vahingossa tuotuun haittaohjelmaan järjestelmässä, mutta yleensä järjestelmän vahingoittaminen on tarkoituksellista. Ulkoiset uhat puolestaan ovat organisaation ulkopuolelta tulevia uhkia, joilla ulkopuolinen haluaa vahingoittaa tai vaikeuttaa organisaation toimintaa. Kybermaailmassakaan ei kaikkia uhkia voida torjua, sillä täydellistä kyberturvallisuutta ei ole olemassa. (Limnell ym. 2014: 106–107.)

Kyberuhat on jaettu viiteen eri kategoriaan niiden vakavuuden perusteella. Ensimmäinen ja lievin uhka on kyberaktivismi, johon kuuluu vandalismi, hakkerointi ja haktivismi eli palveluihin murtautuminen ja niiden sotkeminen. Seuraavana on kyberrikollisuus eli ri-

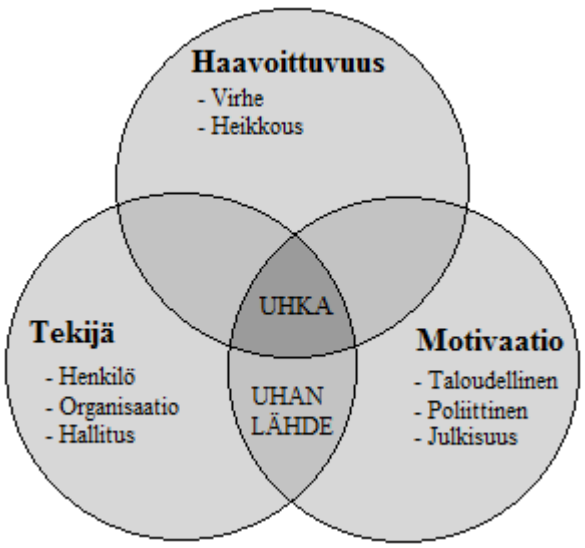
koksien tekeminen tietoverkkoja hyväksi käyttäen, esimerkiksi laittoman sisällön julkaiseminen verkossa. Kolmas kategoria on kybervakoilu, jolla pyritään salassa pidettävien tietojen hankintaan yksityisiltä ihmisiltä, yrityksiltä tai julkisilta yhteisöiltä. Sitten tulee kyberterrorismi, jossa hyökätään kriittistä infrastruktuuria vastaan ja pyritään aiheuttamaan aineellista tuhoa ja pelkoa. Viimeinen ja kriittisin kyberuhka on kybersodankäynti, joka pitää sisällään valtiollisten toimijoiden operaatioita kybermaailmassa ja se edellyttää valtioiden välistä sotatilaa. Kybersodankäynti muodostuu kolmesta kokonaisuudesta: strategisesta, taktisoperatiivisesta kybersodankäynnistä ja kybersodankäynnistä sotaa alemmissa kriiseissä. (Lehto 2013: 12.)

Digitaalisessa maailmassa on uhkien tavoin myös riskejä. Riskejä ei voida uhkien tapaan torjua, vaan niitä sisältyy väistämättä toimintaan kybermaailmassa. Riskeihin suhtaudutaan välttämällä niitä, rajaamalla tai lieventämällä niitä, siirtämällä ja oppimalla elämään niiden kanssa. Riskienhallinta on tärkeä osa kyberturvallisuutta. Viime vuosikymmeninä riskit ja riskitietoisuus ovat läpikäyneet yksityisen ja julkisen hallinnon. Kybermaailman lainalaisuudet heijastavat riskiajattelua ja riskienhallinnasta on tullut myös hallinnolle tärkeä osa turvallisuutta. Riskienhallinta koostuu suunnittelusta, riskien tunnistamisesta ja analysoinnista, riskien kehityksen seuraamisesta, korjaavien toimien suorittamisesta, viestinnästä, raportoinnista ja muusta dokumentaatiosta. Riskistä puhuttaessa tila ei ole rajoite vaan se ylittää organisatoriset ja kansalliset rajat. Kaikki toimijat kohtaavat riskejä normaalielämässä ja kybermaailmassa. Kyberturvallisuus vaatii riskien kannalta toimijoilta joustavuutta, ketteryyttä ja riskien sietokykyä. (Limnell ym. 2014: 108–110.)

Henkilökohtainen tietokone on ensimmäinen väline, joka kannattaa suojata kyberavaruuden riskeiltä. Mitä tehokkaammin noudatetaan riskeihin liittyviä turvatoimia, sitä tehokkaampaa on digitaalisten resurssien suojelu. Haittaohjelmilta suojautumiseen voidaan käyttää seuraavia sääntöjä, jotka vähentävät riskejä: ohjelmistopäivitykset, sisällön minimointi, järjestelmävalvojatili sekä sääntöjen ja lakien noudattaminen. Ohjelmistojen päivitys on tärkeää, koska kehittäjät tekevät uudempiin ohjelmistoversioihin paremman suojan haittaohjelmia vastaan. Ohjelmistojen päivitys voi olla kallista, mutta se maksaa itsensä takaisin pitkällä aikavälillä. Arkaluontoisen sisällön minimointi tietokoneessa vähentää riskiä sen leviämisestä internetiin ja näin myös salattavan tiedon määrä vähenee. Jos olet käyttäjänä tietokoneella, niin vältä järjestelmänvalvojana olemista samaan aikaan, koska vartioimaton tietokone ylläpitäjän oikeuksilla on täysin suojaamaton. Kuka tahansa pääsee tekemään muutoksia tietokoneeseen, jos siihen pääsee järjestelmävalvojan oikeuksilla sisään ja siitä syystä järjestelmävalvojan tiliä tulee käyttää vain ohjelmistojen

päivitykseen ja asentamiseen. Lakien ja erilaisten sääntöjen noudattaminen kyberympäristössä on huomioitava, koska niitä noudattamalla riskit hyökkäyksen kohteeksi valikoitumisesta vähenee. (Kostopoulos 2013: 54–55.)

Haavoittuvuus antaa hyökkääjälle mahdollisuuden heikentää järjestelmän tieto- tai toimintavarmuutta. Se muodostuu, kun järjestelmään on tullut vika tai heikkous, jota hyökkääjä pääsee käyttämään hyväksi. Pelkkä haavoittuvuus ei vielä johda järjestelmän virheelliseen toimintaan, vaan hyökkääjällä pitää olla myös kyky käyttää vikaa hyväkseen. Haavoittuvuuksia pystytään vähentämään niiden hallinnalla järjestelmän omistajan toimesta. Hallintaan kuuluvat haavoittuvuuksien tunnistaminen, luokitteleminen, korjaaminen ja lieventäminen. Käytännössä haavoittuvuus on uhkasta jäljelle jäänyt osuus sen jälkeen, kun siitä on vähennetty kohteen sieto- ja palautumiskyky. Eli järjestelmän parempi sieto- ja palautumiskyky vähentää haavoittuvuutta tietyn uhan edessä. Nykyisen yhteiskunnan suurimmat haavoittuvuudet ovat tietojärjestelmissä ja -verkoissa, joita ohjataan kybermaailmasta käsin. Materiaalisia tekijöitä suurempi haavoittuvuus johtuu naiivista luottamuksesta tietojärjestelmiin ja luottamuksen puutteesta kybermaailman toimivuuteen. (Limnell ym. 2014: 110–111.)



Kuva 5. Uhkien ja riskien muodostuminen kyberavaruudessa (Maniscalchi 2009).

Kuvassa 5 esitellään kyberuhkien ja – riskien muodostuminen ja niihin liittyvät tekijät. Kyberuhka muodostuu kolmen asian yhteensulautumisesta: tekijä, haavoittuvuus ja motiivi. Tekijä voi olla yksittäinen henkilö, organisaatio tai hallitus. Haavoittuvuus altistaa kyberuhille, joka muodostuu järjestelmän virheistä ja heikkouksista. Motiivi on syy hyökkäykselle ja se voi olla taloudellinen, poliittinen tai julkisuuden edun tavoitteleminen. (Maniscalchi 2009.)

3.3 Kyberhyökkäys

Kyberhyökkäys on yksilön tai organisaation tekemää vahingoittavaa toimintaa, joka kohdistuu tietojärjestelmiin, infrastruktuuriin, tietoverkkoihin tai henkilökohtaisiin tietokoneisiin. Hyökkääjä pyrkii varastamaan kohteesta tietoa tai muuttamaan ja tuhoamaan valitsemansa kohteen tietoja murtautumalla siihen. (Karnouskos 2011.)

Hyökkäyksillä voidaan aiheuttaa suuria häiriöitä tai lamauttaa osia kriittisestä infrastruktuurista ja yhteiskunnan kannalta tärkeistä toiminnoista. Valtio tai organisaatio voidaan hyökkäyksien ja häirinnän avulla painostaa poliittisiin, sotilaallisiin ja taloudellisiin myönnytyksiin. Kyberhyökkäykset on rinnastettu sotilaallisiin toimiin, joihin voidaan käyttää kaikkia mahdollisia keinoja. (Suomen kyberturvallisuusstrategian taustamuistio 2013: 17.)

Ensimmäiset 1980- ja 1990-luvulla tehdyt tietojärjestelmähyökkäykset olivat poikkeuksetta asiantuntijoiden suorittamia. Nykyään hyökkäyksiä voi tehdä kuka tahansa valmisohjelmistojen avulla ja useasti niitä käyttävät nuoret tietokoneharrastajat huvikseen sekä rikolliset taloudellisten intressien vuoksi. Hienostuneemmat räätälöidyt ohjelmistot ovat suunniteltu tiettyyn käyttötarkoitukseen sopiviksi ja niiden taustalta löytyvät useasti valtiolliset toimijat tai kyberterroristit. (Janczwewski & Colarik 2008: 262–263.)

Hyökkäys käynnistyy tiedustelulla. Hyökkääjä kerää tietoa kohdeorganisaatiosta käyttämällä teknisiä menetelmiä. Menetelmiä käytetään organisaation internetsivuille tai muihin avoimiin lähteisiin. Tiedustelua voidaan tehdä myös sosiaalisilla menetelmillä, esimerkiksi lähettämällä organisaation tietohallinnolle kysymyksiä. (Valtiovarainministeriö 2009: 18.) Seuraavassa vaiheessa alkaa hyökkäyksen suunnittelu analysoitujen tietojen perusteella ja samalla valitaan tarvittavat työkalut sekä hyökkäysmenetelmä (Valtiovarainministeriö 2009: 18).

Kolmannessa vaiheessa tehdään verkkolaitteiden, työasemien ja palvelimien tietojen skannaus eli lukeminen ja pyritään löytämään haavoittuvuudet. Verkkoskannauksella selvitetään verkon rakennetta ja porttiskannauksella etsitään avoimia portteja, joiden kautta murtaudutaan. Porttiskannauksella voidaan lisäksi selvittää mitä ohjelmia ja protokollia kohdejärjestelmässä käytetään. Ohjelmistojen haavoittuvuusskannauksen tarkoitus on selvittää käyttöjärjestelmä- ja sovellus-versiotietoja sekä vertailla niitä. Tämän vaiheen tuloksena on luettelo järjestelmän murtautumiseen johtavista keinoista. (Heinonen 2003: 12–15.)

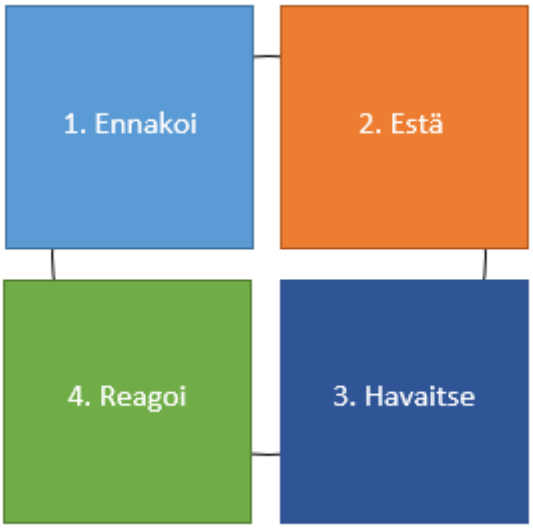
Hyökkäyksissä käytettävät haittaohjelmat jakautuvat kahteen osaan: lataajaan ja haittakoodiin. Lataaja on pieni ja huomaamaton, tehtävänään noutaa haittakoodia sisältävä ohjelma verkosta. Lataaja voidaan ohjelmoida käynnistymään ajastimella, jonka avulla saadaan peitettyä jälkiä. (Valtiovarainministeriö 2009: 18.)

Neljännessä vaiheessa lataaja aktivoituu ja noutaa haittaohjelman määrätystä osoitteesta tai palvelimella olevan konfiguraatiotiedoston tietojen perusteella. Viides eli murtautumisvaihe käynnistyy haittaohjelman aktivoiduttua. Haittaohjelma pyrkii kaappaamaan järjestelmänvalvojan oikeudet tai muut murtautumisen kannalta riittävät oikeudet. Hyökkäyksen tavoitteena voi olla tuhon aiheuttaminen kohdejärjestelmälle, kohdejärjestelmän hyödyntäminen jatkohyökkäyksiä ajatellen tai tiedon varastaminen kohteesta. Viimeisessä vaiheessa tehdään hyökkäyksen jälkien hävittäminen. Hävittäminen tapahtuu sotkemalla lokitiedostot tai tuhoamalla tiedot käyttöjärjestelmien, sovellusten ja verkkolaitteiden lokeista. (Valtiovarainministeriö 2009: 18–19.)

3.4 Kyberpuolustus

Kyberpuolustukseen kuuluu tiedustelu, puolustaminen ja valittuihin kohteisiin vaikuttaminen kyberympäristössä. Puolustuksen yksi tärkeä osa alue on vastahyökkäykset, jotka tukevat puolustusta (Kantola 2017). Kyberpuolustus on rinnastettavissa ilma-, maa- ja meripuolustukseen, jossa voidaan käyttää sotilaallista suorituskykyä myös kyberavaruudessa, valtion lain sallimissa puitteissa. Puolustuksessa on omat haasteensa, jotta voidaan aiheuttaa tarkoituksenmukainen vaikutus ilman yllättäviä sivuseurauksia. Tällaisia sivuseurauksia voi tapahtua, koska verkot ja järjestelmät ovat riippuvaisia toisistaan. Muutokset yhdessä verkoston kohdassa saattaa tehdä muutoksia myös toiseen verkoston kohtaan aiheuttaen ei-toivottuja tapahtumia. (Candolin 2011.)

Kyberpuolustuskyky syntyy tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä ja se mitoitetaan mahdollisimman tehokkaasti alueellisen koskemattomuuden turvaamiseksi ja maan puolustamiseksi. Puolustus on uhkien hallintaa ja niihin varautumista ylläpitämällä erilaisia suojaus- ja vaikuttamiskeinoja sekä luomalla tarvittava toipumiskyky kyberhyökkäykselle. Uhkien syntyminen on kyettävä havaitsemaan ajoissa ja sitä varten pitää pystyä reaaliaikaiseen kybermaailman ilmiöiden ja tapahtumien seuraamiseen. Seuraamisen edellytyksenä on kybertilannekuvan muodostaminen ennakkovaroituksen sekä valmistautumisajan mukaisesti. Tiedusteluun liittyvällä toiminnalla tuotetaan tietoa kybertoimintaympäristön toimijoiden, järjestelmien ja verkkojen kokoonpanoista sekä haavoittuvuuksista. Kybertiedustelulla pyritään luomaan suojautumisen ja vaikuttamisen edellyttämä tilannetietoisuus ja tiedustelutieto. Kyberpuolustuskykyä kehitetään yhteistyössä viranomaisten, elinkeinoelämän, tiedeyhteisön ja muiden toimijoiden kanssa kansallisella tasolla. (Suomen kyberturvallisuusstrategian taustamuistio 2013: 28–29.)



Kuva 6. Suojautuminen kyberhyökkäyksiltä (Salonaho 2015).

Mikael Salonaho (2015) on jaotellut kyberhyökkäyksiltä puolustautumisen neljään vaiheeseen, kuten kuvassa 6 esitetään. Ennakointivaiheessa pyritään seuraamaan hyökkääjien viestintää ja tutkimaan käytössä olevia työkaluja sekä selvittämään seuraava kohde. Toisessa vaiheessa hyökkäys pyritään estämään eri teknologioita käyttäen. Tunkeutumisenestojärjestelmät ovat tätä varten, ne on suunniteltu havaitsemaan ja estämään vahin-

gollinen verkkotoiminta ennen syntyneitä vahinkoja. Kolmas vaihe on uhkien havaitseminen esimerkiksi virustentorjuntaohjelmiston avulla. Havaintotyökalut usein hälyttävät vasta, kun hyökkäys on ohittanut puolustuksen ja aiheuttanut esimerkiksi haittaohjelmatartunnan. Neljännessä vaiheessa tulee reagoida nopeasti tilanteeseen, kun puolustus on murrettu. Nopealla reagoimisella voidaan pienentää toipumisaikaa ja selvitä pienemmillä palveluhäiriöillä. Reagointivaiheeseen tulee laatia toimintasuunnitelma, jotta osataan toimia tilanteen vaatimalla tavalla. (Salonaho 2015.)

3.5 Kybersota

Kybersota on internetliikenteen häirintää ja vakoilua, joihin paras puolustautuminen on kansalaisen, yhtiön tai viranomaisen suojelu. Kybersotaan liittyvät oleellisina asioina häirintä ja vakoilu, jotka tapahtuvat kyberavaruuden kautta. Häirinnässä hyökkääjä pyrkii lähettämään kohdetietokoneelle suuria tiedostoja tai suuria määriä yhteydenottopyyntöjä, jolloin tietokoneen rasituksensietokyky katoaa ja sen yhteys ulkomaailmaan katkeaa. Tällä tavalla voidaan poistaa käytöstä tärkeitä tiedotuskanavia yrityksiltä, ministeriöiltä ja eri tiedotusvälineiltä. (Helsingin Sanomat 2013.)

Vakoilussa puolestaan on kysymys vakoiluohjelmien käyttämisestä johonkin tiettyyn yhtiöön tai organisaatioon, jolloin hyökkääjä pääsee seuraamaan niiden tietoliikennettä tai muuta tärkeää toimintaa. Vakoiluohjelmien avulla hyökkääjä pääsee tietoa salaavien suojausten ohi kohteen siitä tietämättä. Pyrkimyksenä on päästä käsiksi kohteen tietojärjestelmiin ja saada sieltä arvokasta tietoa. (Helsingin sanomat 2013.)

Sodankäynnin oleellinen asia on vastustajan viestiyhteyksien tuhoaminen ja vaikeuttaminen sekä psykologinen vaikuttaminen. Rauhan aikana kyberhyökkäyksellä voidaan aiheuttaa suuria mediakohuja, jotka voidaan laskea lieväksi kybersodankäynniksi. Psykologinen vaikuttaminen voi olla esimerkiksi kuvien lähettelyä kuvanjakopalveluiden kautta. Näin pyritään vaikuttamaan kohteeseen. Propagandan käyttö nettitiedotusvälineissä on samanlaista kuin sensuuri. (Helsingin sanomat 2013.)

Uutisissa käsitellään kybersotaa nykyään lähes päivittäin. Palvelunestohyökkäyksillä kaadetaan internetsivuja, murtaudutaan ministeriöiden tietojärjestelmiin ja vakoillaan yksityishenkilöiden älypuhelimia. Kybersota-aiheen käsittely mediassa nopeuttaa varuste-

lukilpaa kyberturvallisuuteen liittyen ja luo pelon ilmapiiriä yhteiskuntiin. Kaikki kybermaailman tapahtumat eivät ole sodankäyntiä, mutta edellä mainittujen toimintojen voimallinen käyttö digitaalisessa maailmassa ja yhteiskuntien riippuvuus kybermaailman toimivuudesta luovat monenlaisia mielikuvia kybersodankäynnin ulottuvuudesta. Useissa valtioissa kybermaailma on nostettu sodankäynnin viidenneksi ulottuvuudeksi maan, meren, ilman ja avaruuden rinnalle. Esimerkiksi Yhdysvallat ja venäjä ovat perustaneet erilliset joukot sotilaallista kyberkykyä ja oppijärjestelmää ajatellen. (Limnell ym. 2014: 138.)

Käsite kybersodankäynti juontaa juurensa aiemmin käytettyyn informaatiosodankäynnin käsitteeseen. Tom Rona julkaisi vuonna 1976 konseptin informaatiosodankäynnistä, joka poikkeaa yksityiskohdiltaan jonkun verran kybersodankäynnistä. Kybersodankäynnin taistelukenttä voi rajoittua yhteen laitteeseen tai sen osaan tai kattaa maailmanlaajuisia verkkoja (Kramer, Starr & Wentz 2009: 30–34). Sodasta puhuttaessa sotilas- ja tiedustelujohtajat ovat sitä mieltä, että seuraavan suuren sodan taistelukenttänä toimii kyberavaruus (Stiennon 2010: 173).

4 TUTKIMUKSEN TOTEUTUS

Tutkielman tutkimusosa toteutetaan tapaustutkimuksena, jossa kyberturvallisuutta käsitellään Suomeen liittyen. Tutkimuksen ”tapaus” on Suomi. Tapaustutkimus valikoitui sopivaksi tutkimustavaksi, koska kyberturvallisuus on erityinen asia nimenomaan Suomessa.

Tutkimuksen tutkimusmenetelmä on narratiivinen kirjallisuuskatsaus, ja tässä työssä aiheeseen liittyen esitetään tietoa käyttäen kehyksenä tai rajana Suomea. Aiheen käsittely rajoittuu Suomen sisälle. Tutkittavaa aihetta käsitellään valtion ja kansalaisen näkökulmasta. Narratiivinen kirjallisuuskatsaus kuvailevan kirjallisuuskatsauksen alatyyppinä sopii hyvin tähän tutkimukseen, koska kuvailevaan kirjallisuuskatsaukseen kuuluu yleisluontoinen asioiden esittely ilman tarkempia sääntöjä (Salminen 2011: 6). Seuraavaksi käydään tarkemmin läpi tapaustutkimus ja narratiivinen kirjallisuuskatsaus.

4.1 Tapaustutkimus

Tapaus- eli case-tutkimuksessa on oleellista tutkittavan tapauksen valitseminen. Tapaustutkimuksessa tutkitaan yhtä tai useampaa tapausta, joiden määrittely, analysointi ja ratkaisu on tutkimuksen päämäärä. Alustuksena tapauksen tutkimiselle on tutkimuskysymys. Tapaus voidaan määrittää ennen tai jälkeen aineiston keruun aloittamista ja tyypillisesti rinnakkain käytetään laadullista sekä määrällistä aineistoa. Tapaustutkimukset perustuvat erilaisiin lähtökohtiin, näkökulmiin ja valintoihin, jonka vuoksi tutkimuksen tavoitteita voi olla monia. Tyypillisiä tavoitteita ovat ilmiöiden ja tapahtumien selittäminen, kuvauksen tuottaminen, tapauksen ymmärtäminen ja hypoteesien tuottaminen sekä uusien teoreettisten ideoiden synnyttäminen. (Eriksson & Koistinen 2005: 1-4.)

Tapaustutkimukset jakautuvat intensiivisiin ja ekstensiivisiin tutkimuksiin. Intensiivinen tapaustutkimus tarkoittaa ainutlaatuisen ja teoreettisesti mielenkiintoisen tapauksen tarkkaa kuvausta, tulkintaa ja ymmärtämistä. Ekstensiivinen tapaustutkimuksessa tapauksia käytetään välineinä ilmiöiden tutkimisessa ja etsitään yhteisiä malleja sekä käsitteitä usean tapauksen vertailun avulla. Tapaustutkimus yleisellä tasolla on tutkimuksellinen lähestymistapa eikä niinkään aineiston keruu- ja analyysimenetelmä. (Eriksson & Koistinen 2005: 1-4.)

Mikäli seuraavat ehdot täyttyvät, on suotavaa valita tutkimuksen lähestymistavaksi tapaustutkimus:

- *'Mitä-', 'miten-' ja 'miksi-'kysymykset ovat keskeisellä sijalla.*
- *Tutkijalla on vähän kontrollia tapahtumiin.*
- *Aiheesta on tehty vain vähän empiiristä tutkimusta.*
- *Tutkimuskohteena on jokin tämän ajan elävässä elämässä oleva ilmiö.*

(Eriksson & Koistinen 2005: 4.)

Tapaustutkimuksessa voidaan käyttää erilaisia aineiston analyysimenetelmiä eli metodeita, jonka vuoksi tapaustutkimus on koko tutkimusprosessia ohjaava strategia (Eriksson & Koistinen 2005: 4).

Tapaus voi olla yksilö tai ihmisryhmä, tapahtuma, toiminto, prosessi, episodi, instituutio tai maantieteellinen paikka. Oleellisinta on, että tapaus voidaan ymmärtää kokonaisuutena, kuten tässä tutkimuksessa kokonaisuus/tapaus on Suomi. Tapausta tutkitaan kokonaisuutena eri näkökulmista ja tutkimus on kokonaisvaltaista kuvausta ilmiöstä. Tutkimus tapahtuu nykyhetkessä ja todellisessa tilanteessa, ilmiötä tutkitaan ilman keinotekoisia järjestelyitä ja pakotteita. Tutkijan oma arvomaailma vaikuttaa näkemykseen ja tutkimustulokseen. (Kajaanin ammattikorkeakoulu 2018.)

4.2 Narratiivinen kirjallisuuskatsaus

Kirjallisuuskatsauksen tavoite on arvioida ja kerätä yhteen saatavissa oleva tieto aihetta käsittelevistä tutkimuksista (Hovi, Saranto, Korhonen, Korhonen & Holopainen 2011: 37). Kirjallisuuskatsauksia on erilaisia, vaikka se yleisesti ymmärretään melko suppeasti. Erilaisuus tulee niiden metodisesta monipuolisuudesta ja menetelmällisistä erityispiirteistä. Yksi esimerkki kirjallisuuskatsauksien jakamisesta on jako kolmeen perustyyppiin: kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus ja meta-analyysi. Kirjallisuuskatsauksen päämääränä voi olla olemassa olevan teorian arvioiminen ja kehittäminen sekä tai uuden teorian rakentaminen, mutta se voi olla myös kattavan kokonaiskuvan muodostaminen valitusta aihealueesta. Kirjallisuuskatsauksen tyyppi valikoituu aihepiirin, tutkimuskysymysten ja käytettävän aineiston perusteella. (Salminen 2011: 6.)

Narratiivinen kirjallisuuskatsaus on kuvailevan kirjallisuuskatsauksen alatyyppi yhdessä integroivan katsauksen kanssa ja samalla yksi yleisimmin käytetyistä kirjallisuuskatsauksen tyypeistä. Kuvailevaa kirjallisuuskatsausta voidaan luonnehtia yleiskatsaukseksi ilman tiukkoja ja tarkkoja sääntöjä. Tälle tyypillistä on käytettävän aineiston laajuus ja aineiston valinta ilman tiukkoja metodisia sääntöjä. Tutkittava ilmiö kuvataan laaja-alaisesti ja voidaan tarvittaessa luokitella tutkittavan ilmiön ominaisuuksia. Jos verrataan tutkimuskysymyksiä niin ne ovat yleisesti väljempiä kuin systemaattisessa kirjallisuuskatsauksessa tai meta-analyysissä. (Salminen 2011: 6.)

Narratiivinen kirjallisuuskatsaus on metodisesti kaikista kevyin ja se antaa laajan kuvan käsiteltävästä aiheesta. Tämän tyyppisiä katsauksia on eroteltu kolmeen toteuttamistapaan: toimituksellinen, kommentoiva ja yleiskatsaus. Toimituksellisissa katsauksissa julkaisun päätoimittaja tai muu kirjoittaja tekee lyhyehkön kirjallisuuskatsauksen, joka tulee lehdessä tai muussa julkaisussa käsiteltävää aihetta. Kommentoivat katsaukset herättävät keskustelua ja niiden tekijälle kirjallisuuskatsaus ei ole tiukka metodi. Kommentoivan katsauksen idea on herättää keskustelua. Laajin näistä kolmesta toteuttamistavasta on yleiskatsaus. Yleensä narratiivinen kirjallisuuskatsaus mielletäänkin yleiskatsaukseksi ja tämän tyyppisen katsauksen tutkimusaineisto ei ole erityisen tarkkaan seulottua. Narratiivinen katsaus helpottaa tutkimustiedon päivittämistä, mutta ei välttämättä tarjoa analyyttisia tuloksia. Tutkimustietoa voidaan käyttää aiheen opettamisessa, kun siihen ei välttämättä muun tieteellisen kirjallisuuden avulla pystytä. (Salminen 2011: 6-7.)

4.2.1 Aineiston kerääminen

Tutkielman aiheeseen liittyvää aineistoa löytyi melko laajasti, mutta luotettavien ja asiapitoisten aineistojen kerääminen osoittautui osittain melko hankalaksi. Aihe on sen verran uusi, että aiheesta tehtyjä tutkimuksia on rajallinen määrä ja suurimmassa osassa tutkimuksista on käytetty paljon samaa lähdeaineistoa. Aineistona käytin pääasiassa internetistä löytyviä sähköisiä materiaaleja, mutta hyödynsin myös painettuja kirjoja ja artikkeleita. Hahmottelin tutkimuksen alkuvaiheessa tutkimukselle alustavan rakenteen, jonka mukaan aloin kerätä aineistoa.

Teoriataustaisen aineiston hakemisen aloitin kartoittamalla aiheesta tehtyä painettua kirjallisuutta tutkimuskysymykseen liittyen. Tutkimuskysymys ohjasi aineiston keräämistä

alusta asti, ja toimi samalla tutkimuksen tärkeimpänä ”punaisena lankana”. Tutkimus aineiston hakemiseen käytin internetissä toimivia tietokantoja: Melinda, Arto ja Finna. Melinda on Suomen korkeakoulukirjastojen yhteistietokanta, Arto puolestaan kotimainen artikkeliviitetietokanta ja Finna on Suomen kirjastojen, arkistojen ja museoiden yhteinen hakupalvelu. Käytin lisäksi theseus.fi -palvelua, josta löytyy Suomen ammattikorkeakoulujen opinnäytetöitä ja julkaisuja. Tietokantahakujen lisäksi käytin manuaalihaussa Googlea ja Google Scholar -palvelua, joka on Googlen tuottama maksuton hakupalvelu tieteellisille julkaisuille.

Tietokantahakuihin sekä manuaalihakuun käytetiin samoja hakusanoja. Hakusanoiksi valittiin ”turvallisuus”, ”Suomen turvallisuus”, ”kyberturvallisuus”, ”Suomen kyberturvallisuusstrategia”, ”kyberturvallisuuden nykytilanne”, ”puolustusvoimat ja kyberturvallisuus”, ”kansalaisen kyberturvallisuus”, ”esineiden internet”, ”esineiden internetin kyberturvallisuus”, ”sosiaalinen media”, ”sosiaalisen median tietoturvallisuus”, ”kyberturvallisuus koulutus”, ”älylaitteet ja tietoturva”, ”älylaitteiden kyberturvallisuus” ja ”älypuhelimien kyberturvallisuus”. Osa hakusanoista käännettiin englanniksi MOT -sanakirjaa käyttäen. Englanniksi käännetyistä hakusanoista käytettiin: ”cybersecurity”, ”cybersecurity in Finland”, ”Internet of Things”, ”Internet of Things and cybersecurity”, ”social media and information security” ja ”intelligent device and information security”.

Aineistohaulle asetin narratiiviselle kirjallisuuskatsaukselle tyypilliset, kohtuullisen sallivat sisäänotto- ja poissulkukriteerit (Salminen 2011: 6-7). Tässä tutkimuksessa valituille aineistoille asetetut kriteerit näkyvät alla.

	Sisäänottokriteerit	**Poissulkukriteerit**
Julkaisuvuosi:	2000 - 2018	Ennen vuotta 2000
Julkaisukieli:	suomi ja englanti	Muut kielet
Hinta:	Maksuton tai kirjastokortilla saatava	Maksullinen julkaisu
Muut:	Valtion näkökulma, kansalaisen näkökulma, lähdeluettelo saatavissa, nimetty organisaatio tai henkilö lähde	Yritysten näkökulma, lähteetön julkaisu, keskustelupalstat

Tutkimukseen käytettävä aineisto on julkaistu viimeisten kahdeksantoista vuoden aikana. Käytettävien julkaisujen kieleksi valittiin suomi ja englanti, jotta aineistosta saatiin mahdollisimman kelvollista ilman mahdollisia käännösvirheitä. Kielten valinta osaltaan myös rajaa käytettävän aineiston laajuutta. Käytetty materiaali on ollut maksutonta ja näkökulmat aineistoon on valittu tutkimuskysymyksen mukaisesti. Tutkimuksen lähdeaineisto on luotu organisaatioiden tai nimettyjen henkilöiden toimesta.

4.2.2 Aineiston arviointi

Tutkimusaineiston haun yhteydessä hakutuloksista hylättiin sellaiset lähteet, joiden luotettavuus oli selkeästi huono. Tutkimukseen valittiin vain sellaiset aineistot, joista oli saatavana asiantuntija- tai organisaatioperäinen lähdemerkintä. Aineiston luotettavuutta arvioitiin esitettyjen väitteiden ja niihin esitettyjen perustelujen kannalta.

Aineiston piti täyttää aiemmin esitetyt sisäänottokriteerit. Eniten käytettiin aineistoa, joka oli julkaistu vuoden 2010 jälkeen. Kyberturvallisuus on sen verran uusi aihe, että tutkimuksessa suosittiin tuoreinta julkaistua aineistoa. Tutkimusperäisen aineiston saatavuus oli haastavaa, koska aiheesta ja valitsemistani näkökulmista julkaistua aineistoa ei ole paljoa saatavilla. Aineistosta suurin osa oli suomenkielellä julkaistua, mutta myös englanninkielistä aineistoa käytettiin. Suomessa on paljon kyberturvallisuusalan asiantuntijoita, joten heidän julkaisema aineisto on varmasti luotettavaa.

Aineisto arvioitiin laadultaan kohtalaiseksi lähteiden monipuolisen alkuperän vuoksi. Tutkimukseen hyväksyttyä aineistoa on käytetty myös muissa aiheeseen liittyvissä tutkimuksissa. Tutkimukseen pyrittiin hyödyntämään kaikki saatavilla oleva julkisesti esitetty aineisto. Maksullisia aineistoja tutkimuksessa ei käytetty.

5 KYBERTURVALLISUUS VALTION NÄKÖKULMASTA

Tietoyhteiskuntana Suomi on riippuvainen tietoverkkojen ja -järjestelmien toiminnasta. Yhteiskunnan tietointensiivisyys, ulkomaisen omistuksen kasvu ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan kannalta tärkeiden toimintojen turvaamiseksi normaalioloissa ja vakavissa häiriö- tai poikkeustiloissa. Kybertoimintaympäristöön kohdistuneita hyökkäyksiä voidaan käyttää välineinä poliittisessa ja taloudellisessa painostuksessa sekä kriisitilanteissa normaalien sotilaallisten voimakeinojen ohella. Huolehtiminen toimintaympäristöstä parantaa Suomen kansainvälistä asemaa investointikohteena. Kyberturvallisuus on uusi ja koko ajan vahvistuva liiketoiminnan alue, ja kansallinen kyberturvallisuus sekä suomalaisten yritysten menestys ovat sidoksissa toisiinsa. (Suomen kyberturvallisuusstrategia 2013: 1.)

5.1 Suomen kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategia on kuvattu valtioneuvoston 24.1.2013 antamassa periaatepäätöksessä. Strategian tarkoitus on määritellä keskeiset tavoitteet ja toiminnat, joilla vastataan kybertoimintaympäristön haasteisiin sekä taataan sen toimivuus. Linjaukset ja niiden saavuttamiseen tarvittavat toimenpiteet auttavat Suomea hallitsemaan toimintaympäristön haittavaikutuksia sekä vastaamaan ja toipumaan niistä. Strategia noudattaa samoja periaatteita ja määritelmiä kuin yhteiskunnan turvallisuusstrategia, ja siinä on otettu huomioon periaatepäätös kokonaisturvallisuuden järjestelyistä. Eriteltyinä asioina siinä ovat kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset, jotka esitellään seuraavaksi. (Suomen kyberturvallisuusstrategia 2013: 1-2.)

5.1.1 Visio

Suomella on katsottu olevan hyvät mahdollisuudet kyberturvallisuuden kärkimaaksi osaamisen ja yhteistyökykynsä ansiosta. Yhteistyökyky rakentuu tiiviistä ja luottamuksellisesta vuorovaikutuksesta yksityisen ja julkisen sektorin välillä sekä hallinnon alojen välillä. Visio muodostuu seuraavista asioista:

- *Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.*

- *Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.*

- *Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.*
  (Suomen kyberturvallisuusstrategia 2013: 3.)

5.1.2 Toimintamalli

Kyberympäristön muutokset ovat nopeita ja vaikeasti ennakoitavissa. Informaatioteknologian, kyberhyökkäysmuotojen ja haittaohjelmien kehityssykli on lyhyt, joten se asettaa kasvavan haasteen yhteiskunnalle kyberuhkiin varautumisessa. Varautuminen ja kyberuhkien torjuminen pitää olla koordinoitua toimintaa, jotta se on tehokasta. (Suomen kyberturvallisuusstrategia 2013: 4.)

Valtioneuvosto muodostaa ylimmän tason kyberturvallisuuden johtamisessa. Sen tehtävänä ovat poliittinen ohjaus ja strategiset linjaukset sekä voimavaroista ja toimintaedellytyksistä päättäminen. Johtaminen ja häiriötilanteiden hallinta edellyttävät valtioneuvostolta ja eri toimijoilta luotettavaa ja ajantasaista kyberturvallisuuden tilannekuvaa. Häiriötilanteiden hallinnasta vastaa kukin ministeriö ja hallinnonala. Strategiset tehtävät ja kehittämistarpeet perustuvat uhkien analysointiin ja hallintaan. Ministeriöiden ja hallinnonalojen tulee huolehtia, että tavoitteiden mukaiset tehtävät toteutetaan. Uhkien sietokyky sovelletaan niin, että varautumis- ja ennakointikyky, toimintakyky häiriötilanteissa sekä niiden jälkeinen toipumis- ja palautumiskyky ovat kokonaisturvallisuuden päämäärien mukaisia. (Suomen kyberturvallisuusstrategia 2013: 4.)

Periaatteet Suomen kyberturvallisuudelle ovat:

1. *Kyberturvallisuuteen kuuluvat asiat ovat pääasiassa valtioneuvoston toimivaltaan kuuluvia. Ministeriöt vastaavat toimialallaan valtioneuvostolle hallinnon asianmukaisesta järjestämisestä, ja kyberturvallisuuteen liittyvien asioiden valmistelusta.*

2. *Kyberturvallisuuden toimintamalli noudattaa periaatteita ja toimintatapoja, jotka on määritelty Yhteiskunnan turvallisuusstrategiassa (YTS).*

3. *Kyberturvallisuus perustuu yhteiskunnan tietoturvallisuuden järjestelyihin ja edellytyksenä on jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut. Ratkaisujen toteuttamista tuetaan ja helpotetaan moninaisten yhteistoimintaan perustuvien harjoitusten ja rakenteiden avulla.*

4. *Kyberturvallisuuden toimintamalli pohjautuu laaja-alaiseen ja tehokkaaseen tiedon keruu-, analysointi- ja hankintajärjestelmään, jaettuun yhteiseen tilannetietoisuuteen sekä kansainväliseen ja kansalliseen yhteistoimintaan varautumisessa. Edellytyksenä on kansallisen Kyberturvallisuuskeskuksen perustaminen sekä koko yhteiskunnan kokoaikaisen tietoturvallisuustoiminnan kehittäminen.*

5. *Kyberturvallisuuden jäsentelyssä noudatetaan vastuunjakoa yritysten, järjestöjen ja viranomaisten välillä. Vastuunjaon perusteena on erilaiset säädökset ja ennalta sovittu yhteistyö. Nopeat muutokset, uudet mahdollisuudet ja kyky nopeaan reagointiin yllättävissä tilanteissa vaatii toimijoilta strategisen ketteryyden periaatteiden noudattamista ja ymmärtämistä.*

6. *Kyberturvallisuutta kehitetään teknisten ja toiminnallisten edellytyksien mukaan. Kyberturvallisuudessa panostetaan kansainväliseen yhteistoimintaan sekä kansallisiin toimenpiteisiin osallistumalla maailmanlaajuiseen kehittämis-, tutkimus- ja harjoitustoimintaan. Koulutuksen, kehittämisen ja tutkimuksen toteuttaminen lisää kansallista taidokkuutta sekä parantaa Suomea tietoyhteiskuntana.*

7. *Kyberturvallisuuden kehitystyössä keskitytään kybertoimintaympäristön koulutukseen, tuotekehitykseen, tutkimukseen ja työllistymiseen. Päämääränä on kehittää Suomi kyberturvallisuuden johtavaksi maaksi.*

8. *Suomen lainsäädäntö ja kannustimet tulee olla alan yritystoimintaa ja kehittymistä tukevia, jotta voidaan varmistaa kyberturvallisuuden kehittyminen. Kyberturvallisuusala kehittyy pääosin yritystoiminnan kautta.* (Suomen kyberturvallisuusstrategia 2013: 5.)

5.1.3 Strategiset linjaukset

Suomen kyberturvallisuuden kehittämiseen on laadittu strategiset linjaukset. Ne luovat edellytykset vision toteutumiselle ja niiden toimeenpano vahvistaa julkisen ja yksityisen sektorin välistä yhteistoimintaa. Yhteistyön avulla palvellaan koko yhteiskuntaa ja tuetaan tärkeitä toimintoja tuottavia toimijoita huolehtimalla eri toimintojen häiriöttömästä jatkumisesta arkielämässä ja häiriötilanteissa. (Suomen kyberturvallisuusstrategia 2013: 6.)

Kyberturvallisuuden suorituskykyä parannetaan ministeriöiden johdolla, muun muassa määrittelemällä strategiset tehtävät. Tehtävien ja niiden vaatiman suorituskyvyn kehittäminen vaatii eri ministeriöiden, alue- ja paikallishallinnon, elinkeinoelämän sekä järjestöjen toimenpiteitä ja resursointia. Kehittämisessä otetaan huomioon hallinnon eri tasot ja elinkeinoelämän sekä järjestöjen rooli. (Suomen kyberturvallisuusstrategia 2013: 6.)

Periaatepäätöksen mukaiset strategiset linjaukset:

1. Toimivan yhteistoimintamallin avulla varmistetaan kansallisten kyberuhkien torjunta ja kyberturvallisuuden edistyminen viranomaisten ja muiden toimijoiden kanssa.

2. Kyberturvallisuuden tilannetietoisuuden ja tilanneymmärryksen opettaminen yhteiskunnalle tärkeiden toimintojen turvaamiseen osallistuville toimijoille.

3. Kehitetään ja säilytetään yhteiskunnan kannalta tärkeiden organisaatioiden ja yrityksien kykyä torjua ja havaita tärkeisiin toimintoihin kohdistuvat kyberuhkat ja häiriötilanteet. Panostetaan myös häiriötilanteista toipumiseen elinkeinoelämän jatkuvuuden hallinnan vuoksi.

4. Pidetään huolta poliisin käytössä olevista edellytyksistä selvittää, paljastaa ja ennalta ehkäistä rikoksia, jotka ovat kybertoimintaympäristöön kohdistuvia tai sitä hyödyntäviä.

5. Lakisääteisissä tehtävissä kokonaisvaltaisen kyberpuolustuskyvyn luominen Puolustusvoimien toimesta.

6. Kansallisen kyberturvallisuuden vahvistaminen ottamalla osaa aktiivisesti kyberturvallisuuden kannalta merkittävien ulkomaisten yhteistyöfoorumeiden ja organisaatioiden toimintaan.

7. Kehitetään yhteiskunnan eri toimijoiden kyberosaamista.

8. Tehokkaan kyberturvallisuuden toteuttamisen edellytyksien varmistaminen lainsäädäntöä muokkaamalla.

9. Kyberturvallisuutta koskevat tehtävät, palvelumallit ja yhteiset perusteet kyberturvallisuuden vaatimusten hallinnasta tarkennetaan viranomaisille ja elinkeinoelämän toimijoille.

10. Strategian toteuttamista ja tuloksia seurataan.
    (Suomen kyberturvallisuusstrategia 2013: 7-11.)

5.2 Suomi kyberturvallisuuden kärkimaa

Suomen tavoite oli olla kyberturvallisuuden maailmanlaajuinen edelläkävijä vuonna 2016. Joillakin kybertuvallisuuteen varautumisen alueilla maa on kärkijoukkoa, mutta eri osa-alueilla on vielä paljon tehtävää. Tärkeimmät haasteet liittyvät kolmeen asiaan: lainsäädäntöön, resursseihin ja johtamiseen. Lainsäädäntöön tulee tehdä muutoksia, jotta voidaan kehittää valmiutta digitaalisen maailman uhkia vastaan ja kertoa maan ulkopuolelle millaisessa ympäristössä kyberturvallisuutta kehitetään. Resursseja pitää saada lisää ja johtajuuden puutteeseen täytyy vastata. Vahvin voimavara näihin on osaava ihminen, kuten koodarit ja yhteiskunnan päättäjät. Heidän avullaan Suomesta saadaan luotua kyberturvallisuuden mallimaa. (Limnell 2015.)

Henkisen ja fyysisen sietokyvyn parantaminen häiriötilanteita vastaan on tärkeää suomalaisen yhteiskunnan ja yrityselämän turvallisuuden kannalta ja juuri näitä osa-alueita on vahvistettava. Digitaalinen maailma on nykyään erottamaton osa arkea, kuten kansalaisten elämää, liiketoimintaa ja sodankäyntiä. Kansallisen kyberstrategian mukaisilla linjauksilla ja niiden toimeenpanolla Suomi pääsee hyvin alkuun kyberturvallisuuteen asettamiensa tavoitteiden saavuttamiseksi. (Limnell 2015.)

Kyberturvallisuustutkimus on Suomessa maailman parhaimmistoa ja se on noteerattu Eurooppaa ja Yhdysvaltoja myöten. Merkittävä henkilö Suomen kyberturvallisuuden takana on Aalto-yliopiston kyberturvallisuuden professori Jarno Limnell. Limnell korostaa yhteistyön merkitystä eurooppalaisten yliopistojen välillä kyberturvallisuustutkimuksessa ja hän on erityisen tyytyväinen siitä, että ilmiönä kyberturvallisuus on laaja ja nykyään paljon esillä myös tiedotusvälineissä. Ilmiön leviämiseen on vaikuttanut luottamus teknologiaan ja digitaalisiin palveluihin. (Pajunen 2017.)

Jopa Yhdysvaltojen presidentti Donald Trump on kehunut Suomen kyberturvallisuusosaamista presidenttimme Sauli Niinistön vierailulla Valkoisessa talossa. Pian vierailun jälkeen uutisoitiin, että Ouluun perustetaan kyberturvallisuuden tutkimuskeskus Suomen ja Yhdysvaltojen toimin. Tämän uuden Cyber Security and Software Engineering Research Site -yksikön taustalla on 13 yliopistoa ja yli 20 teollista ja julkishallinnollista kumppania ja se on keskittynyt julkishallintoa ja yrityksiä koskeviin uhkiin sekä nettikiusaamiseen ja verkkomaksamisen ongelmiin. (Pajunen 2017.)

Maailmalla ollaan erityisen kiinnostuneita suomalaisten mallista varautua erilaisiin uhkatekijöihin, olivat ne sitten fyysisiä tai kybermaailman puolella. Kyberturvallisuudessa ei pelkkiin uhkiin varautuminen riitä vaan on tärkeää varautua myös sen tuleviin vaikuttamiskeinoihin. Suomessa kaikki turvallisuusasiat otetaan vakavasti ja Limnell:n mukaan mikään maa ei voi hoitaa kyberturvallisuuttaan yksin, vaan painottaa nimenomaan eurooppalaista yhteistyötä. (Pajunen 2017.)

Suomi on yksi eurooppalaisista menestyjämaista kyberturvallisuudessa ja meillä on merkittävä kyberturvateollisuus, jolla voimme kilpailla kansainvälisten jättiyritysten rinnalla. Digitaalisuus on ei tunne fyysisiä rajoja ja kansallinen itsenäisyytemme on muutakin kuin valtion fyysiset rajat. Kansallinen kyberturvateollisuutemme on yksi tulevaisuuden kilpailuvalteista, koska tulevaisuudessakin jokainen maa joutuu ottamaan vastuun omasta turvallisuudestaan, kyvyistä ja osaamisesta myös kyberturvallisuuden osalta. (Remes 2017.)

5.3 Puolustusvoimat ja kyberturvallisuus

Puolustusvoimat kehittää kykyjä tiedustella, suojautua sekä vaikuttaa kyberympäristössä. Suomen kyberturvallisuusstrategiassa Puolustusvoimien rooli on kokonaisvaltaisen puolustuskyvyn luonti. ”*Jos käytetään puolustuskykyjä maalla, merellä ja ilmassa, on nykyään mahdollista käyttää puolustuskykyjä myös kyberavaruudessa”* sanoo Puolustusvoimien tietoverkkopuolustussektorin johtaja, Catharina Candolin. Kyberpuolustuksen merkityksen kasvaessa uudelle puolustushaaralle maa-, meri- ja ilmavoimien lisäksi ei ole varsinaista tarvetta vaan kyberpuolustus nähdään yhteiskäyttöisenä suorituskykynä. Puolustusvoimat kehittää kykyjä kyberympäristössä vaikuttamiseen strategian mukaisesti. Vaikuttamiskyvyn kehittäminen tarkoittaa myös hyökkäyskyvyn kehittämistä. (Kontiainen 2013.)

Puolustusvoimat varautuu nykyajan hybridisodankäyntiin parantamalla tietoverkkojen suojausta, ja aikomuksissa on perustaa kybersotaan erikoistuva yksikkö Puolustusvoimien tietoverkkojen ja -järjestelmien suojaksi. Tietojen mukaan kyberosaston tarkoitus on kehittää kyberpuolustuksen suorituskykyä, osallistua järjestelmien ylläpitoon ja luoda valtakunnallista kyberpuolustuksen tilannekuvaa. Kyberpuolustukseen kuuluu myös kyky hyökätä ja omia tietojärjestelmiä testataan juuri harjoitushyökkäysten avulla. Informaatiosotaan liittyen Puolustusvoimien rooli on oikaista julkisuudessa esitettyä virheellistä tietoa ja uutisointia Suomeen liittyvistä asioista. (Koistinen 2014.)

Erilaisiin uhkiin varaudutaan Puolustusvoimissa jatkuvasti. Varusmiesten kyberkoulutukseen keskitytään enemmän ja palveluksen aikana tietotekniikan, matkapuhelimen sekä sosiaalisenmedian käyttöön annetaan koulutusta. Koko maailma on internetissä, jonka kautta voidaan lamauttaa eri maiden tietotekniikkajärjestelmät. Asevelvollisen kyberkoulutus liittyy operaatioturvallisuuteen, paikkatietoon ja palvelusturvallisuuteen. Operaatioturvallisuus tarkoittaa sitä, ettei sotilas omalla toiminnallaan jaa sellaista tietoa verkkoon, mikä vaarantaa joukkojen turvallisuutta. Paikkatieto liittyy matkapuhelimiin, jonka avulla voidaan selvittää henkilön sijainti. Palvelusturvallisuuteen liittyvät sosiaalisen median ja matkapuhelimen vääräaikainen käyttö, mikä voi vaarantaa varusmiespalveluksessa olevien turvallisuutta. Koulutusta annetaan kolmella eri kaudella palveluksen aikana: peruskoulutus-, erikoiskoulutus- ja joukkueharjoituskaudella. (Kettumäki 2015.)

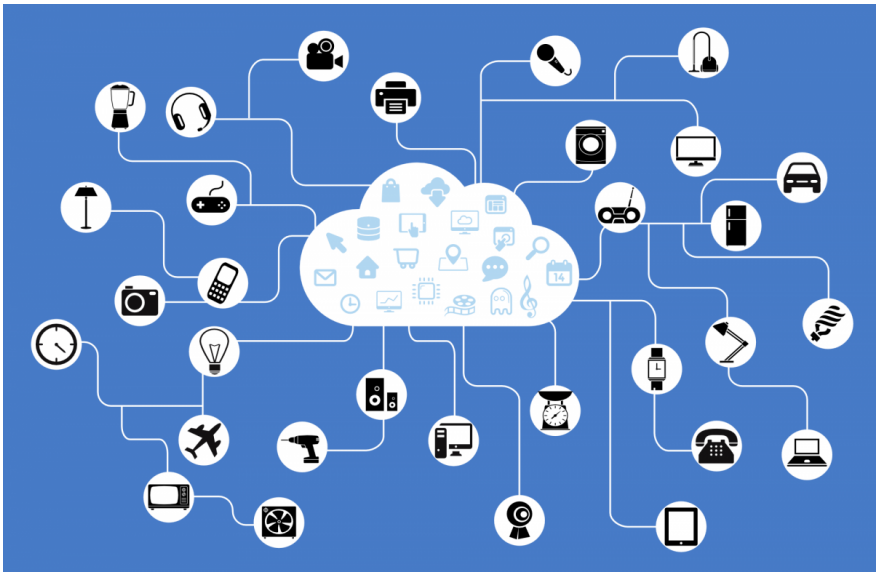
Puolustusvoimat lisäävät kyberkoulutustaan jatkuvasti. Tietoverkkojen ja kyberuhkien tunnistamiseen sekä torjuntaan erikoistuvia varusmiehiä koulutetaan jokaisesta saapumiserästä. Kybervarusmiesten tarkkaa määrää ei paljasteta, eivätkä he saa palvelusaikana näyttäytyä mediassa tunnistettavina. Tarkoituksena on saada reserviin kymmeniä kyberkouluttautuneita varusmiehiä, ja lisäksi heille tarjotaan mahdollisuutta jäädä töihin Puolustusvoimiin kyberasiantuntijaksi. Palvelusajaltaan kyberkoulutuksen käynyt varusmies saa kyberturvallisuusalan kokemuksen lisäksi työtodistuksen. (Suihkonen 2016.)

6 KYBERTURVALLISUUS KANSALAISEN NÄKÖKULMASTA

Kyberturvallisuus on ollut keskeinen puheenaihe uutisoinnissa ja lehtien palstoilla jo pidemmän aikaa. Usein siitä puhutaan sotien yhteydessä tai muuten isojen suurvaltojen välisissä konflikteissa. Tästä huolimatta kyberturvallisuus on yhä enemmän ja suurempi osa tavallisten kansalaisten elämää. (Moilanen 2017.)

Kansalaisten tavallisessa arjessa automatisointi on edennyt niin pitkälle, ettei palaaminen vanhanaikaisiin manuaalisiin järjestelyihin ole välttämättä mahdollista. Nykyään yhteiskunnalle ominainen piirre on riippuvuus erilaisten informaatioteknologian sovelluksista ja toimivista tietoliikenneyhteyksistä. Tästä Moilanen blogissaan sanookin, ”että elämme arkeamme kybermaailmassa – halusimme sitä tai emme”. Luottamus monimutkaisiin, verkostomaiseen toimintatapaan perustuviin järjestelmiin on keskeinen osa arkea, vaikka tieto niiden rakenteesta, häiriönsietokyvystä ja toipumisvalmiudesta voi olla hyvinkin vähäistä. Muun muassa tämän vuoksi kansalaisille tieto kyberturvallisuudesta on ensisijaisen tärkeää. (Moilanen 2017.)

Uuden askeleen kansalaisten jokapäiväiseen kyberturvallisuuteen tuo esineiden internet. Koteihimme asennetaan yhä enemmän sähköisiä verkottuneita laitteita ja verkossa kaikki ovat alttiina monenlaisille tietoturvauhkille (Moilanen 2017).



Kuva 7. Esineiden internet (Clark 2015).

Kuvassa 7 on havainnollistettu internetiin kytkettyjä arkielämän laitteita, joista muodostuu esineiden internet. Jeff Clark (2015) kirjoittaa internetin rajoittamattomasta käytöstä sekä internetin kysynnän ja tarjonnan riippuvuudesta. Clark:n (2015) mukaan kysyntä hidastuu tarjonnan rajoissa, ja tämän voi aiheuttaa internetiin liitettyjen laitteiden tulva. Hänen mukaan internet -vero voisi olla tarpeellinen.

Esineiden internet (internet of things) on jatkuvasti muuttuva ja kehittyvä maailmanlaajuinen verkon rakenne, jossa fyysisillä ja virtuaalisilla esineillä on henkilöllisyys, fyysisiä ominaisuuksia ja virtuaalinen persoona. Esineiden ja verkon välisestä tiedon välittämisestä vastaavat käyttöliittymät, jotka voivat mukautua eri käyttäjien tarpeisiin tai jopa käyttäjien toimintaa ennakoivaksi. Esineiden internetin avulla ihmisten ja laitteiden yhteys lisääntyy. (Grahn 2017.) Muutamia arkisia esimerkkejä esineiden internetistä ovat kotien lämmitys- ja valaistusjärjestelmien säätäminen etänä matkapuhelimella, saunan tai kahvinkeittimen ohjaaminen matkapuhelimella ja vauvan itkuhälytin. Kaikki nämä ottavat yhteyden internetiin ja ovat näin alttiita tietoturvauhkille. Useimmiten tai melkein poikkeuksetta aina tällaisten jo valmiiksi verkkoon kytkettyjen laitteiden tietoturva jää kuitenkin kuluttajan vastuulle. (Partanen 2018.)

Laitteiden ja ihmisten verkostoituminen tuo kansalaisille isoja hyötyjä ja älykäs seuranta tehostaa palveluja sekä mahdollistaa etätoiminnan. Se tuo myös turvaa, koska koneet osaavat monesti laskea ja ennakoida paremmin kuin ihmiset, joten viat saadaan nopeasti esille ja erilaisia arvoja optimoitua paremmin. Ajatuksena laitteiden ja ihmisten verkostoituminen on mahtava, mutta se tuo myös ison huolen tietoturvaongelmaa ajatellen. Varsinkin verkkoon kytketyt kodin laitteet ovat varsin heikosti suojattuja ja niiden tietoturvaa ei ole välttämättä testattu loppuun saakka, joten ne tarjoavat hyökkääjälle usein heikosti suojatun maalin. Tämän vuoksi kansalaisilla tulee olla hyvä tuntemus laitteiden kyberturvallisuudesta, koska verkkoon kytkettyjä laitteita on kohta kaikkialla. (Tapanainen 2017.)

F-Securen tutkimusjohtajan Mikko Hyppösen mukaan kansalaisen kyberturvallisuudessa on kysymys ihmisten vastuusta omien tietojensa luovuttamisesta. Pitää miettiä mitä tietoja laittaa nettiin ja mihin tämä tieto menee, sekä haluaako tiedon pysyvän verkossa vuosikymmenien ajan. Yhteiskunnan tulee myös osaltaan kantaa huolta kansalaisten tiedoista, joita kansalaiset eivät voi itse suojata. Kansalaisen vastuulle jää kuitenkin suodatus omien tietojen luovuttamisesta. (Sitra 2013.)

6.1 Sosiaalinen media

Sosiaalinen media tarkoittaa internetin palveluja ja sovelluksia, joissa käyttäjien keskinäinen kommunikaatio ja oma sisällöntuotanto yhdistyvät. Ominaista sosiaaliselle medialle on sen helppokäyttöisyys, maksuttomuus ja mahdollisuus yhteisölliseen tuotantoon. Erona perinteiseen joukkoviestintään on se, että käyttäjät voivat tehdä asioita kuten kommentoida, tutustua toisiinsa ja jakaa erilaisia sisältöjä. Nykyään paljon käytettyjä sosiaalisen median kanavia ovat esimerkiksi: Facebook, YouTube, Twitter ja Instagram. (Hintikka 2008.)

Sosiaalisen median kasvu on tuonut mukanaan myös huolia, liittyen kansalaisten kyberturvallisuuteen. Sosiaalisen median rikoksista on tullut arkipäivää ja yhä useammin yleisestikin tehdyt rikokset liittyvät jollakin tavalla sosiaaliseen mediaan. Tavanomaista rikollisuutta sosiaalisessa mediassa ovat: kiusaaminen, koulu-uhkaukset, viharikokset, petokset, identiteettivarkaudet, seksuaalirikokset, tekijänoikeusrikokset ja huumausainerikokset. (Viestintävirasto 2015.)

Kyberkriminaalit saavat paljon arvokasta tietoa sosiaalisen median kautta. Ihmiset jakavat paljon tietoa itsestään, perheistään työstään ja kaikesta normaali kansalaiset elämään liittyvistä asioista. Hyökkääjät käyttävät näitä tietoja hyväkseen ja voivat edellä mainittujen tietojen avulla tutustua huolellisesti valittuun kohteeseen. Rikoksen tekijät käyttävät metodinaan manipulointia ja pyrkivät näin saamaan käyttäjän tekemään jotain normaalista poikkeavaa. Yleisin tapa käyttäjän manipulointiin on tietojenkalasteluhyökkäys. Tällaisessa hyökkäyksessä sosiaalisen median käyttäjä saa sähköpostin, jossa on linkki haittaohjelman sisältävään liitetiedostoon. Hyökkääjän tarkoitus on saada käyttäjä avaamaan liitetiedosto. Monet yritykset ovat tällaisen toiminnan uhreina kärsineet suuria rahallisia menetyksiä, kun hyökkääjät ovat saaneet työntekijät tekemään valheellisia rahansiirtoja. Järjestäytyneet rikollisryhmät ja valtioihin kytköksissä olevat toimijat tekevät yleisimmin tietojenkalasteluhyökkäyksiä. (Lehto, Limnell, Innola, Pöyhönen, Rusi & Salminen 2017: 15-16.)

Monelle sosiaalisen median käyttäjälle tietojenkalastelu tulee yllätyksenä. Hyökkääjien intressit vaihtelevat ja heillä on monenlaisia keinoja. Tavanomainen kohde on käyttäjätunnukset ja salasanat, joiden avulla hyökkääjät kaappaavat käyttäjän tilin, jota he voivat

vahingoittaa tai käyttää osana uutta kalasteluhyökkäystä. Jos motiivina on raha, he pyrkivät varastamaan käyttäjän luottokorttitiedot tai erilaisten maksutilien (esimerkiksi PayPal) tunnukset. (Ahlberg 2017.)

Tietojenkalastelusivustot eivät voi varastaa tietoja automaattisesti, joten yksinkertaisin tapa välttää tietojen saaminen on sulkea selain. Vahvojen salasanojen käyttö, eri salasanojen käyttäminen jokaisessa palvelussa ja hyökkäysten olemassaolon tiedostaminen ovat tärkeitä keinoja suojautumiseen. Kriittinen suhtautuminen erilaisiin kyselyihin ja sivustoihin estävät myös usein tietojen leviämisen väärille tahoille. Uhkien tiedostaminen ja halutessaan erilaisten koulutuksien käyminen lisäävät varmasti tietoisuutta tietojenkalasteluhyökkäyksistä sekä sosiaalisen median kyberturvallisuudesta. (Ahlberg 2017.)

6.2 Kyberturvallisuus koulutukset

Median kautta kansalaisille levinnyt tietoisuus kyberturvallisuudesta on saanut kansalaiset aktivoitumaan. Aiheesta kiinnostuneet suomalaiset ovat innostuneet kyberturvallisuuden ja informaatiovaikuttamisen koulutuksista. Maanpuolustusyhdistyksen järjestämille kursseille on koko ajan enemmän tulijoita kuin kursseja keretään järjestämään. Vapaaehtoisten kurssien suosio on yllättänyt kurssien järjestäjät ja kyberturvallisuus kiinnostaa paljon muitakin ihmisiä kuin niitä, joita maanpuolustuskoulutus innostaa. (Koljonen 2017.)

Kyberturvallisuus koetaan niin tärkeänä asiana, että kansalaiset ovat halukkaita omalla kustannuksellaan ja ajallaan opiskelemaan aiheeseen liittyviä asioita. Monien kurssien kouluttaja Jarno Limnell Aalto -yliopistosta sanoo, että ”mitä paremmin kansalaiset tunnistavat vaikuttamisyritykset, sitä vaikeampi heidän luottamustaan yhteiskuntaan on horjuttaa”. Maanpuolustuskoulutusyhdistyksen(MPK) kursseja on sekä tavallisille kansalaisille että Puolustusvoimissa palveleville. Kyseisen yhdistyksen kaikki toiminta perustuu vapaaehtoistyöhön, myös kouluttaminen. MPK on saanut vuonna 2016 ICT -Suomi ry:ltä 100 000 euroa kansalaisten kyberturvallisuustaitojen kehittämistä varten. (Koljonen 2017.)

Kyberkoulutuksien kysyntä on kasvanut hurjasti viime vuosina. MPK järjestää kansalaisille suunnattuja yleisluontoisia tieto- ja kyberturvakursseja, mutta myös kohdennettuja

ja teknisempiä erikoiskursseja. Koulutuksien taustalla on kansallisen kyberstrategian suositukset sekä halu valmentaa kansalaisia torjumaan heihin kohdennettuja tietoturva- ja kyberuhkia. Peruskurssien tarkoituksena on yleiskuvan muodostaminen tietoturva- ja kyberasioista, joten osallistujilta ei odoteta ennakkotietoutta aiheesta. Erikoikurssit on suunnattu reserviläisille, opiskelijoille ja asiantuntijoille, ja kurssit ovat avoimia kaikille aiheen perusosaamisen omaaville. Opettajat ovat vapaaehtoisia kyberturvan ammattilaisia ja opetukseen kuuluu tietoteknisten asioiden lisäksi myös esimerkiksi informaatiosodankäyntiä. (Aukia 2015.)

Kansalaisten kyberturvallisuustaidot ovat nykyään osa yhteiskunnan turvallisuutta ja ne ovat muodostuneet kansalaistaidoksi. Suomessa vallitseva vahva maanpuolustustahto, erinomainen kyberosaaminen ja oppimisen halu edesauttavat kansalaistaitojen kehittymistä. Puolustusvoimissa koulutetaan varusmiehiä kybersodankäyntiin keskittyvässä yksikössä, ja varusmiehet saavat koulutuksen kyberpuolustuksen tehtäviin. Maanpuolustuskoulutusyhdistys järjestää kaikille kansalaisille suunnattuja kyberturvakursseja. Aaltoyliopiston professori Jarno Limnell on luennoinut useita kursseja ja havainnut kurssilaisten osaamisen tason olevan korkea. Limnell kannustaa kansalaisia osallistumaan kyberperustaitojen kehittämiseen suunnatuille kursseille, koska aihe on jatkossa entistäkin tärkeämpi digitalisoituvassa maailmassamme. (Limnell 2016.)

Vapaaehtoisten lyhyempien koulutuksien lisäksi kansalaisilla on nykyään mahdollisuus opiskella kyberturvallisuutta korkeakouluissa ja yliopistoissa. Korkeakoulut järjestävät kyberturvallisuuteen erikoistumiskoulutuksia ja esimerkiksi Jyväskylän yliopistossa informaatioteknologian tiedekunnassa voi valita kyberturvallisuuden maisteriopinnot, joiden laajuus on 120 opintopistettä. Tällaisesta maisteriohjelmasta valmistuneilla on mahdollisuus toimia vaativissa asiantuntijatehtävissä, joissa kehitetään julkisen sekä yksityisen sektorin kyberturvallisuutta. Kyberturvallisuuden lisääntyminen luo kansalaisille työpaikkoja erityisesti puolustusvoimien, poliisin ja yritysten tehtäviin asiantuntijoiksi ja johtajiksi. (Jyväskylän yliopisto 2017.)

6.3 Älylaitteiden kyberturvallisuus

Lisääntyvä teknologian määrä ja älylaitteiden räjähdysmäinen kasvu kansalaisten keskuudessa huolestuttavat ihmisten omien tietojen turvaamisen kannalta. Laitteisiin asennettavat sovellukset ja ohjelmistot käyttävät sekä säilyttävät paljon käyttäjän tietoja, jotka ovat

kyberturvallisuuden kannalta monien uhkien kohteena. Älylaitteita käytetään paljon pankkiasioiden, henkilökohtaisten ja työasioiden hoitamiseen, jonka seurauksena laitteille tallentuu paljon tietoja käyttäjästä ja yrityksistä. Nämä tiedot ovat jatkuvasti hyökkääjille alttiina ja sen vuoksi ne tulisi suojata mahdollisimman monimutkaisilla salasanoilla ja tietoturvaohjelmilla. Kaspersky Lab:n vuonna 2013 teettämästä tutkimuksesta selviää, että vain 56 prosenttia suomailaisista suojaa älylaitteensa salasanoilla. (Mobiiliasiantuntijat 2017.)

Monesti puhutaan älylaitteiden tietoturvallisuudesta, mutta voidaan puhua myös kyberturvallisuudesta. Harry Kantolan (2017) mukaan tietoturvallisuudella tavoitellaan tietyn järjestelmän toiminnan turvaamista ja kyberturvallisuudella puolestaan turvataan järjestelmän lisäksi siihen liittyvien käyttäjien toimintaa synnyttäen turvaamisen kokonaiskonseptin. Älylaitteiden tietojen turvaaminen on käyttäjien ja heidän peruselämänsä turvaamista. Tietojen turvaamista varten on tarjolla paljon erilaisia tietoturvaohjelmia, ilmaisia sekä maksullisia. Yleensä maksullisien ohjelmien käyttäjä saa enemmän työkaluja laitteensa turvaamiseen ja apua ohjelmien käyttämiseen. Osaan ilmaisista ohjelmista saa myös palveluntarjoajalta tukea, mutta mainokset tulevat mukana eli ohjelmissa näkyvät jatkuvat ilmoitukset ja kausialennukset maksulliseen versioon liittyen häiriten ohjelman käyttäjää. (Graziano 2014.)

Älypuhelimet ovat todella suuri kyberturvallisuusuhka käyttäjilleen. Käyttäjien on tiedettävä suojattavat kohteet, jotta ne voivat varautua uhkiin. Älypuhelimien suojattavat kohteet voidaan jakaa kolmeen osa-alueeseen:

1. Henkilökohtaiset tiedot
2. Laite
3. Sovellukset

Henkilökohtaisiin tietoihin kuuluvat osoitekirja, puheluhistoria, sijaintitieto, kalenteri, salasanat, sähköposti ja sen liitteet sekä muu vain käyttäjän tiedossa oleva informaatio. Laitteeseen liittyen suojattavia kohteita ovat älypuhelin itsessään ja järjestelmät resurssit (järjestelmän muisti, suoritin, akku ym.). Käyttäjän asentamat sovellukset ovat myös tärkeä suojattava kohde, koska ne yleensä sisältävät tietoja käyttäjästä. Henkilökohtaisia tietoja voidaan hallita sovellusten kautta ja näin sovellukset ovat yhteydessä käyttäjän tietoihin. Käyttäjien tulee olla tarkkana puhelimeen tallennettujen tietojen kanssa ja käyttäjätun-

nuksien ja salasanojen tallentamista sovelluksen muistiin on vältettävä. Laitteen joutuminen vääriin käsiin voi aiheuttaa mittavat vahingot laitteen omistajalle, varsinkin jos laitteeseen ja sovelluksiin on valmiiksi tallennettu käyttäjätiedot ja salasanat. (Jeon, Kim, Lee & Won 2011: 313.)

7 DISKUSSIO

Tutkimuksen tarkoituksena oli selvittää mitä kyberturvallisuus on Suomessa, valtion ja kansalaisen näkökulmista katsottuna. Narratiivisen kirjallisuuskatsauksen avulla etsittiin vastauksia aiemmin tehdyistä tutkimuksista ja muista julkisista materiaaleista aiheeseen liittyen. Narratiivinen kirjallisuuskatsaus sopi tähän tutkimukseen tutkimusmenetelmäksi todella hyvin, koska sen avulla oli mahdollista luoda yleiskuva aiheesta. Jaottelin tutkimusaineiston kahden edellä mainitun näkökulman mukaan ja pyrin nostamaan esille näkökulmien kannalta keskeisimmät asiat kyberturvallisuuteen liittyen.

Suomen valtion näkökulmasta keskeisintä on maan ja valtioelinten puolustaminen kyberturvallisuusuhkilta sekä kyky suojata elintärkeät toiminnot kaikissa tilanteissa kyberuhkaa vastaan. Valtion laatima kyberturvallisuusstrategia ohjaa toimintaa ja sen mukaisia strategisia linjauksia pyritään ensisijaisesti noudattamaan. Strategia muodostuu visiosta, periaatepäätöksistä ja strategisista linjauksista. Maan puolustamisen kannalta tärkeää on varusmieskoulutukseen sisällytetty kyberturvallisuuskoulutus, Puolustusvoimat ovat kehittäneet oman koulutusohjelman, jonka varusmiehet voivat palveluksessaan valita.

Kyberturvallisuusstrategiaan liittyen Suomi valtiona halusi olla maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa vuonna 2016. Suomessa osaaminen on todella hyvällä tasolla, ja se on huomioitu maailmalla. Erityisesti Suomen malli varautua erilaisiin uhkatekijöihin on kiinnostanut muita maita. Remeksen (2017) mukaan Suomi on yksi eurooppalaisista menestyjämaista kyberturvallisuudessa eli tavoite jollakin tavalla täyttynyt.

Kansalaisten näkökulmasta hurja teknologian kehittyminen ja lisääntyvät älylaitteet ovat lisänneet kiinnostusta kyberturvallisuusasioissa. Kotien sähköiset järjestelmät ja sosiaalisen median yleistyminen ovat luoneet uudenlaisia turvallisuusuhkia. Älypuhelimien ja erilaisten sovellusten kautta tietoa joutuu useasti vääränlaiseen käsittelyyn. Tutkimuksen mukaan tärkein puolustautuminen on käyttäjän omien tietojen suojaaminen sekä tiedostaminen omien henkilökohtaisten tietojen levittämisessä. Ihmiset ovat hiljalleen alkaneet ymmärtämään kyberturvallisuuteen liittyviä uhkia ja halukkuus kyberturvallisuuskoulutuksiin on ollut kova. Nopeasti kehittynyt digitalisaatio ja sen myötä tulleisiin uhkatekijöihin suhtaudutaan vakavasti. Kyberturvallisuus on liitetty osaksi kansalaisten turvallisuutta.

Tutkimuksen mukaan kyberturvallisuus on Suomessa hyvällä pohjalla. Valtio kehittää kyberturvallisuutta lisääntyvissä määrin, ja Suomen osaaminen alalla on huomioitu Yhdysvaltoja myöten. Halu kyberturvallisuuden kehittämiseen on kova ja erilaisia koulutuksia järjestetään toistuvasti. Kehitysideana olisi rohkeamman yhteistyön tekeminen useampien valtioiden kanssa, ja määrärahojen keskittäminen tähän digitalisaation mukana kasvavaan kyberturvallisuuden puolustamiseen. Median kautta leviävää tiedottamista kyberturvallisuudesta tulisi lisätä, ja keskittyä perinteisiin kyberturvallisuusuhkiin. Tällä tavalla kansalaisille saatettaisiin paremmin tietoa aiheesta.

Kansalaisten näkökulmasta kyberturvallisuusuhkiin tulisi suhtautua kriittisemmin. Pitäisi miettiä enemmän internetiin jaettavan tiedon seurauksia, ja mitä yleensäkin itsestä kannattaa julkaista. Tiedon jakaminen on tehty liian helpoksi ja monesti ihmiset ymmärtävät jakamisen seuraukset liian myöhään. Voisi sanoa, että teknologian kehitys on saanut ihmiset julkaisemaan itsestään poikkeuksellisen paljon henkilökohtaisia tietoja internetiin näkyviksi. Sovelluksissa käytettävät käyttäjä- ja salasanatietojen tallentamisominaisuuksien poistaminen vähentäisi varmasti niiden väärin käyttöä.

Tutkimus rakennettiin tutkimuskysymyksen ympärille ja rajattiin Suomen kannalta valtion ja kansalaisen näkökulmiin. Tutkimuksen aihepiiri oli melko laaja ja tarkoituksena oli esitellä keskeisimmät asiat näihin näkökulmiin liittyen. Lähdeaineisto oli myös melko monipuolinen ja hyvien lähteiden löytäminen osoittautui haasteelliseksi. Tutkimuksessa käytettiin pääasiassa alan asiantuntijoiden julkaisemia aineistoja, sekä painettuja julkaisuja. Tutkimusta voidaan pitää luotettava, koska käsiteltäviä aiheita löytyi useista eri lähteistä. Tutkimukseen valittiin eniten pinnalla olevat aiheet kyberturvallisuuteen liittyen.

Tätä tutkimusta voisi hyödyntää kyberturvallisuuden opetustarkoitukseen, erityisesti tavallisille ei niin paljoa aiheeseen perehtyneille ihmisille. Tutkimuksen perusteella saa kohtalaisen kokonaiskuvan valtion sekä kansalaisen kyberturvallisuudesta. Jatkotutkimusta voisi tehdä valitsemalla uusia näkökulmia aiheeseen, ja käsittelemällä kyberturvallisuutta maailmanlaajuisesti. Kyberturvallisuus on olennainen osa yritysten toimintaa, joten yrityksien näkökulmasta voisi tehdä laajempaakin tutkimusta. Maailmalla ollaan todella kiinnostuneita Suomen mallista kyberuhkiin varautumisessa, joten tutkimusta voisi tehdä Suomen mallin eroista muiden valtioiden malleihin verrattuna. Kyberturvallisuuden korostuminen teknologian kehityksen myötä lisää tarpeita aiheesta tehtäville tutkimuksille.

LÄHTEET

Ahlberg, Janne (2017). Instadefsec; Ajankohtaista: *Tietojenkalastelu sosiaalisessa mediassa tulee monelle yllätyksenä.* 25.4.2017. Saatavilla: https://www.instadefsec.fi/ajankohtaista/blogi/2017/04/tietojenkalastelu-sosiaalisessa-mediassa-tulee-monelle-yllatyksena.html?tagged=sosiaalinen+media

Ashby, W. Ross (1957). *An introduction to cybernetics*. Saatavilla: http://www.science-lib.net/files/Introduction%20to%20Cybernetics%20%20W.%20 Ashby%20%281957%29%20WW.pdf

Aukia, Jussi-Pekka (2015). Huoltovarmuuskeskus; Varmuuden vuoksi; Kansalaisen varautuminen: *Kyberturvallisuus kiinnostaa.* 29.12.2015. Saatavilla: https://www.varmuudenvuoksi.fi/aihe/kansalaisen_varautuminen/280/kyberturvallisuus_kiinnostaa

Candolin, Catharina (2011). *Tietoverkkopuolustus osana maanpuolustusta*. Kyberturvallisuus/kyberpuolustus blogi. 6.12.2011. Saatavilla: http://kyberturvallisuus. blogspot.fi/

Clark, Jeff (2015). *Supply, demand and internet taxation*. Datacenterjournal. 25.11.2015. Saatavilla: http://www.datacenterjournal.com/supply-demand-internet-taxation/

Eriksson, Päivi & Koistinen, Katri (2005). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus 3/2005. Kerava: Savion Kirjanpaino Oy. 49s. ISBN 951-698-123-2.

Ghernouti-Helie, Solange (2010). 2010 International Conference on Availability, Reliability and Security: *A national strategy for an effective cybersecurity approach and culture.* Saatavilla: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5438067

Grahn, Hilkka (2017). Jyväskylän yliopisto; ITKP0002 Johdatus kyberturvallisuusteen; Kyberuhkien vaikutukset ja verkottuneen tietoyhteiskunnan tulevaisuus; Tietoyhteiskunnan tulevaisuuden haasteita; Internet of Things (IoT) eli esineiden internet. Saatavilla: https://peda.net/jyu/it/do/kkv/6kvjvtt/6tth/iotieei2

Graziano, Dan (2014). *Protect your Android device from malware*. C|net. 25.6.2014. Saatavilla: https://www.cnet.com/how-to/protect-your-android-device-from-malware/

Haukkala, Hiski & Limnell, Jarno (2012). Helsingin Sanomat: *Kyberturvallisuus on Suomen valttikortti*. Pääkirjoitus 16.12.2012. Saatavilla: http://www.hs.fi/ paakirjoitukset /a1355545998241

Heinonen, Arsi (2003). *Verkkohyökkäysinformaation keskitetty analysointi*. Tekninen korkeakoulu. Espoo. Diplomityö.

Helsingin Sanomat (2013). Kotimaa: *Mitä Kybersota on?* 24.1.2013. Saatavilla: http://www.hs.fi/kotimaa/Mit%C3%A4+kybersota+on/a1305641261197

Hintikka, Kari (2008). Jyväskylän yliopisto; sanasto; sanat-kansio; sosiaalinen media. Saatavilla: http://kans.jyu.fi/sanasto/sanat-kansio/sosiaalinen-media

Hovi, Sirpa-Liisa; Saranto Kaija; Korhonen, Teija; Korhonen, Anne; Holopainen, Arja (2011). Järjestelmällinen katsaus on paljon muutakin kuin tiedonhakua. Tutkiva Hoitotyö Vol. 9 (2). Fioca. 37.

Janczewski, Lech J. & Colarik, Andrew M. (2008). *Cyberwarfare and Cyber Terrorism*. 2. painos. Herheys, Yhdysvallat: IGI Global. 532 s. ISBN 978-1-59140-991-5.

Jeon, Woongryul; Kim, Jeeyeon; Lee, Yuongsook & Won, Dongho (2011). *A Practical Analysis of Smartphone Security*. 7/2011. Saatavilla: https://www.researchgate.net/publication/221095013_A_Practical_Analysis_of_Smartphone_Security

Jyväskylän yliopisto (2018). Opiskelu; Maisteriohjelmat; Kyberturvallisuus: *Kyberturvallisuuden maisteriopinnot*. 18.4.2018. Saatavilla: https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus

Järvinen, Petteri (2012). *Arjen tietoturva*. Jyväskylä: Docendo. 323s. ISBN 978-951-0-38948-5.

Kajaanin ammattikorkeakoulu (2018). Opinnäytetyöpakki; tukimateriaali; tutkimustyypit. Saatavilla: http://www.kamk.fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Tutkimustyypit/Kuvaileva/Tapaus

Kantola, Harry (2017). Rannikon puolustaja 4/2017; artikkeli: *Mikä ihmeen kyber-?* Saatavilla: http://www.rannikonpuolustaja.fi/archive/2017_4.pdf

Karnouskos, Stamatis (2011). Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In:*37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia*, 7-10 Nov 2011. Retrieved 20 Apr 2014.

Kasvi, Jyrki (2016). Aalto-yliopisto; Kyberturvallisuus koskee meitä jokaista – yleisöluentosarja: *Digitalisaation mahdollisuudet ja turvallisuus*. 19.1.2016. Saatavilla: https://www.slideshare.net/JyrkiKasvi/kyberturvallisuus-koskettaa-meit-jokaista

Kettumäki, Antti (2015). Yle; uutiset, kotimaa: *Suomessa varaudutaan uudenlaiseen sodankäyntiin: kyberpuolustus sotilaan perustaidoksi*. 19.3.2015. Saatavilla: http://yle.fi/uutiset/suomessa_varaudutaan_uudenlaiseen_sodankayntiin_kyberpuolustus_sotilaan_perustaidoksi/7874214

Koistinen, Antti (2014). Yle; uutiset, kotimaa: *Puolustusvoimat perustaa uuden kyberyksikön – hybridisotiin varaudutaan vahvistamalla verkkopuolustusta.* 25.9.2014. Saatavilla: http://yle.fi/uutiset/puolustusvoimat_perustaa_uuden_kyberyksikon__hybridisotiin_varaudutaan_vahvistamalla_verkkopuolustusta/7491555

Koljonen, Tarja (2017). Keskisuomalainen; kotimaa: *Kyberturvallisuus ja informaatiosota vetävät maanpuolustuskurssit täyteen.* 17.5.2017. Saatavilla: https://www.ksml.fi/kotimaa/Kyberturvallisuus-ja-informaatiosota-vet%C3%A4v%C3%A4t-maanpuolustuskurssit-t%C3%A4yteen/987056

Kontiainen, Taneli (2013). Ruotuväki-lehti; uutiset: *Kyberpuolustukseen kehitetään suorituskykyjä.* 10.10.2013. Saatavilla: http://www.puolustusvoimat.fi/portal/ puolustusvoimat.fi/!ut/p/c5/04

Kostopoulos, George K. (2013). *Cyberspace and cybersecurity.* United States of America: Taylor & Francis Group. 218 s. ISBN 978-1-4665-0133-1.

Kotisalo, Janne & Järvinen, Markku (2017). E-Karjalan ICT-Palvelut.net Oy: *5 askelta tietojen turvaamiseen.* 30.6.2017. Saatavilla: http://www.ictpalvelut.net/news/show/title/-5-askelta-tietojen-turvaamiseen/src/@random558851f68a148

Kramer, D. & Starr, S. Wentz, L. (2009). *Cyberpower and National Security*. Virginia, Yhdysvallat: Potomac Books. ISBN 978-1-59797-423-3.

Laaksonen, Mika; Nevasalo, Terho & Tomula, Karri (2006). *Yrityksen tietoturvakäsikirja: ohjeistus, toteutus ja lainsäädäntö.* 324s. Helsinki: Edita Publishing Oy. ISBN 951-37-4701-8.

Lehto, Martti (2013). Sotilasaikakauslehti 12/2013: *Kybermaailman määrittelyä*. 88.vuosikerta. Mikkeli: AO-Paino. Saatavilla: http://www.upseeriliitto.fi/files/4020/SAL_12_2013.pdf.

Lehto, Martti; Limnell, Jarno; Innola, Eeva; Pöyhönen, Jouni; Rusi, Tarja & Salminen, Mirva (2017). Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017: *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Valtioneuvoston kanslia. 17.2.2017. Saatavilla: http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykyti-la%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Limnell, Jarno (2015). Aamulehti; Kotimaa: *Puheenaihe: Kyberturvallisuuden tärkeyttä ei ole vielä täysin tiedostettu.* 2.3.2015. Saatavilla: http://www.aamulehti.fi/ Kotimaa/1194964564012/artikkeli/puheenaihe+kyberturvallisuuden+tarkeytta+ei+ole+viela+taysin+tiedostettu.html

Limnell, Jarno (2016). Iltalehti; Blogit: *Tärkeää maanpuolustustyötä kyberturvallisuudessa.* 1.1.2016. Saatavilla: https://blogit.iltalehti.fi/jarno-limnell/2016/01/01/tarkeaa-maanpuolustustyota-kyberturvallisuudessa/

Limnell, Jarno, Majewski, Klaus & Salminen, Mirva (2014). *Kyberturvallisuus*. 1. painos. Jyväskylä: Docendo Oy. 246 s. ISBN 978-952-291-047-9.

Lohela, Maria (2013). Ryhmäpuheenvuoro: Liittoutumana muuttuvassa maailmassa. *Turvallisuus- ja puolustuspoliittinen selonteko*. 7.5.2013. Saatavilla: https://www.perussuomalaiset.fi/news/ryhmapuheenvuoro-liittoutumattomana-muuttuvassa-maailmassa/

Maniscalchi, Jago (2009). Digitalthreat: *Threat vs Vulnerability vs Risk*. 26.6.2009. Saatavilla: http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/#

Mobiiliasiantuntijat (2017). *Mobiilitietoturvavinkkejä kuluttajille ja pienille organisaatioille.* Saatavilla: http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html

Moilanen, Panu (2017). Jyväskylän yliopisto; tiedeblogi: *Arjen kyberturvallisuus on uusi tutkimushaaste.* 5.10.2017. Saatavilla: https://www.jyu.fi/fi/blogit/tiedeblogi/moilanen_p

Niemelä, Pauli & Lahikainen, Anja Riitta (2000). *Inhimillinen turvallisuus*. Tallinna: Kirjakas/Tallprint. 377s. ISBN 951-768-064-3.

Oulun yliopisto (2015). Opiskelijan terveys- ja voimavarat. Turvallisuus. Saatavilla: http://www.oulu.fi/hyvinvointi/opiskelijan_terveys__ja_voimavarat/turvallisuus.htm

Pajunen, Ilpo (2017). Yle; uutiset: *Kyberturvallisuus Suomen valtti maailmalla – esillä myös EU:n huippukokouksessa Tallinnassa.* 28.9.2017. Saatavilla: https://yle.fi/uutiset/3-9855517

Partanen, Minttu-Maaria (2018). Helsingin Sanomat; Koti: *Kodinkoneet on nykyään kytketty verkkoon, mutta niiden tietoturva on jätetty kuluttajan vastuulle – onko se reilua?* 25.1.2018. Saatavilla: https://www.hs.fi/koti/art-2000005537878.html

Pekander, Heidi (2016). Helsingin yliopisto; Pro gradu -tutkielma: *Kyberturvallisuuden keskeiset käsitteet.* Saatavilla: https://helda.helsinki.fi/bitstream/handle/10138/162869/Pekander_Heidi_ProGradu_2016.pdf?sequence=2

Pietikäinen, Suvi (2013). Valtiovarainministeriö; Vahti-ohjeet: *Tietoturvallisuus – mitä se on?* 27.11.2013. Saatavilla: https://www.vahtiohje.fi/web/guest/691

Rautiainen, Juha (2013). *Kyber sitä, kyber tätä – muutamia kyberkäsitteitä*. Juhan IT-blogi. 1.11.2013. Saatavilla: https://juhanit.wordpress.com/2013/11/01/kyber-sita-kyber -tata-muutamia-kyberkasitteita

Remes, Juha (2017). Tietoturvallinen Suomi; *Suomi on kyberturvallisuuden kärkimaa Euroopassa.* 27.3.2017. Saatavilla: https://tietoturvallinensuomi.fi/suomi-on-kyberturvallisuuden-karkimaa-euroopassa/

Rousku, Kimmo (2012). Tietoviikko; Turvasatama. *Kyberturvallisuus – mitä se oikeastaan on?* 6.9.2012. Saatavilla: http://www.tietoviikko.fi/blogit/turvasatama/ kyberturvallisuus++mita+se+oikeastaan+on/a836007

Rousku, Kimmo (2015). Tietoviikko; Turvasatama. *Kyberturvallisuus on digitalisaation edellytys ja mahdollistaja* 11.8.2015. Saatavilla: https://www.tivi.fi/blogit/kyberturvallisuus-on-digitalisaation-edellytys-ja-mahdollistaja-3327790

Rousku, Kimmo (2015). Elisa; Yrityksille. *Digitalisaatio edellyttää myös digitaalista turvallisuutta.* 30.10.2015. Saatavilla: https://hub.elisa.fi/digitalisaatio-edellyttaa-myos-digitaalista-turvallisuutta/

Salminen, Ari (2011). Vaasan yliopisto; Vaasan yliopiston julkaisuja; *Mikä kirjallisuuskatsaus?* 5/2011. Saatavilla: https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Salonaho, Mikael (2015). Tietoviikko; Kumppaniblogi; Tieto. *Neljä askelta kyberhyökkäysten torjumiseksi, osa2.* 4.5.2015. Saatavilla: https://www.tivi.fi/Kumppaniblogit/tieto/2015-05-04/Nelj%C3%A4-askelta-kyberhy%C3%B6kk%C3%A4ysten-torjumiseksi-osa-2-3220967.html

Siren, Torsti (2011). *Strateginen kommunikaatio ja informaatio-operaatiot 2030*. Helsinki: Juvenes Print Oy. 314s. ISBN 978-951-25-2253-8.

Sisäasiainministeriö (2012). Sisäisen turvallisuuden ohjelma: *Turvallisempi huominen*. 14.6.2012. ISBN 978-952-491-760-5 Saatavilla: http://www.intermin.fi/ download/34893_262012_STO_III_fi.pdf?856e9e241c05d188

Sisäministeriö (2015). *Sisäinen turvallisuus on ministeriön suurin vastuualue*. Turvallisuus. Saatavilla: http://www.intermin.fi/fi/turvallisuus

Sisäministeriö (2017). Ministeriö; Sisäisen turvallisuuden strategia: *Sisäisen turvallisuuden strategia rakentaa maailman turvallisinta maata.* Saatavilla: http://intermin.fi/sisaisen-turvallisuuden-strategia

Sitra (2013). Artikkelit; Uusi turvallisuus; Haastattelu: *Yksilön kyberturvallisuus – mitä se on, Mikko Hyppönen?* 26.11.2013. Saatavilla: https://www.sitra.fi/artikkelit/yksilon-kyberturvallisuus-mita-se-mikko-hypponen/

Sitra (2014). Artikkelit; Uusi turvallisuus: *Tulevaisuuden turvallisuus on kuin kananmuna kakkutaikinassa*. 18.3.2014. Saatavilla: http://www.sitra.fi/artikkelit/uusi-turvallisuus/tulevaisuuden-turvallisuus-kuin-kananmuna-kakkutaikinassa

Stiennon, Richard (2010). *Surviving Cyberwar*. Plymouth, Iso-Britannia: Government Institutes. 168 s. ISBN 978-1-60590-674-4.

Suihkonen, Rai (2016). Keskisuomalainen; kotimaa: *Puolustusvoimat lisää salamyhkäistä koulutusta: ”Olemme kiinnostuneet palkkaamaan taitonsa näyttäviä”.* 14.2.2016. Saatavilla: https://www.ksml.fi/kotimaa/Puolustusvoimat-lis%C3%A4%C3%A4-tuntuvasti-kyberkoulutusta/729592?pwbi=f8a85c2d4f827e9f0e39e1a848fbe190

Suomen kyberturvallisuusstrategia ja taustamuistio (2013). Valtioneuvoston periaatepäätös 24.1.2013. Saatavilla: http://www.yhteiskunnanturvallisuus.fi/fi/ materiaalit

Tapanainen, Tero (2017). ECraft: *Esineiden internet (IoT) ja tietoturva: riskit ja ratkaisut.* 13.11.2017. Saatavilla: https://www.ecraft.com/fin/blog/2017/11/13/esineiden-internet-ja-tietoturva-riskit-ja-ratkaisut

Ulkoministeriö (2018). Ulkoministeriö; Toiminta ja tavoitteet; Ulko- ja turvallisuuspolitiikka: *Kyberturvallisuus ja kybertoimintaympäristö.* 15.1.2018. Saatavilla: http://formin.finland.fi/public/default.aspx?nodeid=49571

Viestintävirasto (2015). Kyberturvallisuus; tietoturva nyt!: *[Teema] Vieraskynänä Marko Forss: Sosiaalisen median rikoksista on tullut arkipäivän rikollisuutta*. 16.6.2015. Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/ 06 /ttn201506160914.html

Valtiovarainministeriö (2009). Kohdistetut hyökkäykset, VAHTI 6/2009. Helsinki: VM-julkaisutiimi. Saatavilla: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091117Kohdis/kohdistetut_hyoekkaeykset_netti_kannet.pdf