TURUN YLIOPISTO

Uhkan ja riskin rajamailla: Kyberturvallisuuden politiikka Suomessa

Valtio-oppi

pro gradu -tutkielma

Laatija(t):

Tuovi Helin

30.4.2025

Turku

Pro gradu -tutkielma

Oppiaine: Valtio-oppi
Tekijä(t): Tuovi Helin
Otsikko: Uhkan ja riskin rajamailla: Kyberturvallisuuden politiikka Suomessa
Ohjaaja(t): Professori Henri Vogt
Sivumäärä: 68 sivua
Päivämäärä: 30.4.2025

Tutkielma tarkastelee, miten kybertoimintaympäristön uhkia ja riskejä käsitellään Suomen turvallisuuspoliittisissa dokumenteissa. Tutkimuksen kohteena ovat Suomen kansalliset riskiarviot ja kyberturvallisuusstrategiat vuosilta 2013–2023. Tutkielma pyrkii selvittämään, millaisia kyberuhkia ja -riskejä dokumenteissa nostetaan esiin, miten niitä jäsennetään turvallistamisen ja riskiyttämisen kautta, ja millaisia merkityksiä tällä on Suomen kyberturvallisuuspolitiikan kehittymiselle. Tavoitteena on ymmärtää, miten uhkien ja riskien käsittely vaikuttaa siihen, miten kybertoimintaympäristöä määritellään ja turvataan osana Suomen turvallisuuspolitiikkaa.

Tutkielman teoreettisena viitekehyksenä toimii Kööpenhaminan koulukunnan turvallistamisteoria, jota täydennetään Olaf Corryn riskiyttämisen käsitteellä. Turvallistamisteoria auttaa tunnistamaan, miten kyberilmiöitä määritellään eksistentiaalisiksi uhkiksi, jotka oikeuttavat poikkeukselliset toimenpiteet. Riskiyttämisen avulla analysoidaan puolestaan sitä, miten ennakoivaa hallintaa ja resilienssiä painotetaan kyberturvallisuustoimissa. Aineistona käytetään Suomen kolmea kansallista riskiarviota vuosilta 2015, 2018 ja 2023 sekä kahta kyberturvallisuusstrategiaa vuosilta 2013 ja 2019.

Analyysissa havaitaan, että Suomen turvallisuuspoliittisissa dokumenteissa kyberuhkia esitetään vakavina uhkina, jotka voivat uhata koko yhteiskunnan toimintaa. Näiden uhkien torjumiseksi painotetaan erityisesti valtion ja yhteiskunnan kykyä selviytyä häiriöistä eli resilienssiä. Samaan aikaan dokumenteissa näkyy myös riskiajattelu, jossa korostetaan tarvetta ennakoida ja hallita erityisesti teknologisia ja sosiaalisia haavoittuvuuksia. Turvallistaminen näkyy siinä, miten kyberuhkat tuodaan osaksi arkipäiväistä turvallisuutta ja liitetään laajempiin yhteiskunnan toimivuuden kysymyksiin. Riskienhallinnassa taas korostuvat jatkuva varautuminen ja ennaltaehkäisy, jotta vakavia häiriöitä voidaan välttää.

Tutkielman johtopäätökset osoittavat, että kyberturvallisuuden uhkia ja riskejä käsitellään Suomen turvallisuuspoliittisissa dokumenteissa toisiaan täydentävinä ilmiöinä. Turvallistaminen nostaa uhkia yhteiskunnallisiksi ja poliittisiksi kysymyksiksi, kun taas riskiyttäminen painottuu konkreettiseen haavoittuvuuksien hallintaan ja resilienssin vahvistamiseen. Uhkien ja riskien rinnakkainen tarkastelu on tärkeää, sillä se auttaa tunnistamaan sekä akuutit, ulkoisista toimijoista johtuvat uhat että järjestelmien sisäiset, hitaammin vaikuttavat riskit. Tutkimus osoittaa, että kyberturvallisuus kytkeytyy tiiviisti yhteiskunnallisiin rakenteisiin ja vaatii kokonaisvaltaista lähestymistapaa, jossa tekniset, sosiaaliset ja poliittiset näkökulmat huomioidaan yhdessä. Tulevaisuudessa on tärkeää kehittää sekä ennaltaehkäiseviä että reagoivia hallintakeinoja ja vahvistaa yhteiskunnallista resilienssiä, jotta kybertoimintaympäristön monimutkaisiin ja jatkuvasti muuttuviin uhkiin ja riskeihin voidaan vastata kestävästi.

Avainsanat: kyberturvallisuus, turvallistaminen, riskiyttäminen, turvallisuuspolitiikka, uhkat, riskit

Sisällysluettelo

1 Johdanto

Digitalisaation kiihtyminen on muuttanut yhteiskunnan toimintaa perustavanlaatuisesti. Tietoverkot ja digitaaliset palvelut ovat läsnä lähes kaikilla elämänalueilla, mikä lisää riippuvuutta teknologisista järjestelmistä ja kasvattaa yhteiskunnan haavoittuvuutta erityisesti kybertoimintaympäristön häiriöille. (Sisäministeriö 2023, 23-24.) Kyberturvallisuus ei ole enää ainoastaan teknologinen kysymys, vaan osa kansallista kokonaisturvallisuutta, jonka merkitys on korostunut entisestään muuttuneessa geopoliittisessa toimintaympäristössä. (Valtioneuvoston kanslia 2024, 8-10.)

Nykyisessä tilanteessa kybertoimintaympäristöä haastavat muun muassa vihamielinen valtiollinen vaikuttaminen, hybridisodankäynti, disinformaatio sekä teknologian, kuten tekoälyn, nopea kehitys. Nämä ilmiöt haastavat perinteiset käsitykset turvallisuudesta ja vaativat uudenlaista lähestymistapaa kyberuhkien ymmärtämiseen ja hallintaan. (Valtioneuvoston kanslia 2024, 13-14.)

Perinteisesti kyberturvallisuutta on tarkasteltu teknisestä näkökulmasta, mutta yhä useammin nousee esiin tarve ymmärtää myös sosiaalisia ja yhteiskunnallisia ulottuvuuksia. Kathleen M. Carleyn (2020, 366-367) mukaan kyberturvallisuuden kokonaisvaltainen ymmärtäminen edellyttää, että teknisten haavoittuvuuksien lisäksi huomioidaan myös sosiaaliset verkostot ja informaation leviämisen vaikutukset. Sosiaalinen media ja disinformaatio voivat heikentää yhteiskunnan resilienssiä, polarisoida kansalaisia ja heikentää luottamusta instituutioihin.

Suomessa on tunnistettu, että digitaalinen haavoittuvuus koskee paitsi teknisiä järjestelmiä myös kansalaisten hyvinvointia ja yhteiskunnan toimivuuteen kohdistuvaa luottamusta. (Valtioneuvoston kanslia 2024, 18.) Tästä syystä Suomen kyberturvallisuusstrategiassa painotetaan resilienssin vahvistamista ja kansalaisten valmiuksien kehittämistä osana laajempaa turvallisuusajattelua.

Sekä Carley (2020, 366–367) että Limnéll, Majewski ja Salminen (2015, 16–18) korostavat, että kyberturvallisuuden haasteet ulottuvat teknisten kysymysten ulkopuolelle. Carleyn mukaan sosiaalisten verkostojen manipulointi ja informaatiovaikuttaminen ovat keskeisiä kyberuhkia, joihin perinteinen tekninen suojaus ei riitä. Vastaavasti Limnéll ym. painottavat, että kyberturvallisuus on nähtävä osana laajempaa yhteiskunnallista kehitystä ja kansallista

turvallisuutta. Tämän vuoksi tässä tutkimuksessa tarkastellaan, millaisia kyberturvallisuuden uhkia ja riskejä Suomessa turvallistetaan ja riskiytetään kansallisissa riskiarvioissa sekä kyberturvallisuusstrategioissa.

1.1 Tutkimuskysymys ja tutkielman rakenne

Tarkastelen pro gradu -työssäni sitä, minkälaisia kyberturvallisuuden uhkia ja riskejä turvallistetaan ja riskiytetään Suomen turvallisuuspoliittisissa dokumenteissa, joissa kyberturvallisuus on nostettu keskeiseksi tekijäksi. Valitsin kolme Suomen kansallista riskiarviota ja kaksi Suomen kyberturvallisuusstrategiaa tutkimukseni aineistoksi, koska ne antavat kattavan kuvan siitä, miten Suomi suhtautuu kyberturvallisuuteen osana kansallista turvallisuuspolitiikkaa ja miten sen haasteisiin pyritään vastaamaan.

Kyberturvallisuusstrategioden tarkoituksena on määritellä keskeiset tavoitteet ja toimenpiteet kybertoimintaympäristön turvaamiseksi, mukaan lukien kyberuhkien ennakoiminen ja niihin varautuminen (Turvallisuuskomitea 2013, 1-2). Kansallisissa riskiarvioissa pyritään käsittelemään taas laajasti niitä riskejä, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja, ja jotka voivat vaatia poikkeuksellisia toimenpiteitä viranomaisilta. Kyberturvallisuus on yksi olennainen turvallisuuden osa-alue näissä riskiarvioissa. (Sisäministeriö 2015, 9.) Valitsin aikajanan, joka kattaa Suomen ensimmäiset kyberturvallisuusstrategiat ja riskiarviot sekä niiden myöhemmät päivitykset, koska se tarjoaa kattavan kuvan kyberturvallisuuspolitiikan ja riskiarvioinnin kehittymisestä. Ensimmäinen kyberturvallisuusstrategia (2013) ja riskiarvio (2015) toivat kyberturvallisuuden entistä näkyvämmin osaksi kansallista turvallisuuspolitiikkaa ja alkoivat määritellä keinoja siihen varautumiseksi.

Tutkimuskysymykseni tässä tutkielmassa on:

1. *Miten kybermaailman uhkia ja riskejä turvallistetaan tai riskiytetään Suomen kansallisissa riskiarvioissa ja kyberturvallisuusstrategioissa?*

Tämän tutkimuskysymyksen avulla pyrin selvittämään, miten Suomen kyberturvallisuuspolitiikka kehystää kybertoimintaympäristön ilmiöitä turvallisuuskysymyksinä ja miten näitä ilmiöitä käsitellään osana kansallista turvallisuutta. Hyödynnän tutkielmassa Kööpenhaminan koulukunnan turvallistamisteoriaa, jonka avulla

analysoin, miten tietyt ilmiöt määritellään eksistentiaalisiksi uhkiksi ja mitä seurauksia tällä on. Turvallistamisen rinnalla käytän riskiyttämisen käsitettä, jonka kautta tarkastelen, miten asiakirjat käsittelevät ennakoivaa hallintaa ja todennäköisyyksiä liittyen kyberriskeihin. Näiden käsitteiden ja aineiston analyysin avulla selvitän, miten kyberuhkia ja -riskejä kehystetään ja miksi tietyt ilmiöt saavat erityistä huomiota osana kansallista turvallisuuspolitiikkaa. Tämä tarkastelu tuo esiin, millä tavoin turvallistaminen ja riskiyttäminen vaikuttavat kyberturvallisuuden hallintaan ja poliittisiin päätöksiin Suomessa.

Analyysissa tarkastelen, miten turvallistaminen ja riskiyttäminen ilmenevät konkreettisesti kansallisissa riskiarvioissa ja kyberturvallisuusstrategioissa. Etsin erityisesti kohtia, joissa kyberuhkia ja -riskejä kehystetään eksistentiaalisina uhkina tai hallittavina riskeinä, ja pohdin, millaisia poliittisia ja turvallisuuspoliittisia vaikutuksia näillä kehystyksillä on. Näin tutkimus tuo esiin, miten kyberturvallisuus on muotoutunut osaksi Suomen kansallista turvallisuuspolitiikkaa.

Tutkielman rakenne on jaettu siten, että johdannon jälkeen tulee luku 2 eli taustoitus, jossa avaan kyberturvallisuuden käsitteen laajemmin ja pohdin, millä lähestymistavalla sitä tulisi tarkastella. Tämän jälkeen tarkastelen uhkien ja riskien roolia osana kyberturvallisuutta, ja syvennyn erityisesti kyberriskeihin turvallisuuspoliittisina riskeinä. Tässä osiossa tuon esiin myös aiempaa tutkimusta kyberturvallisuudesta sekä käsittelen resilienssin merkitystä osana kyberturvallisuuden kokonaisuutta.

Taustoistuksen jälkeen esittelen luvussa 3 tutkimukseni teoreettisen viitekehyksen, joka muodostuu turvallistamisteoriasta sekä riskiyttämisestä. Käytän tutkimuksessani erityisesti Kööpenhaminan koulukunnan turvallistamisteoriaa, jota esittelen tarkemmin tässä luvussa. Tutkimuksessani turvallistamisteoria toimii myös metodisena lähestymistapana, sillä hyödynnän diskurssiivista analyysia selvittääkseni uhkia ja riskejä turvallisuuspoliittisista dokumenteista. Tässä luvussa on oma alaluku, jossa avaan tarkemmin, kuinka teoria toimii tutkimuksen työkaluna. Luvun lopussa esittelen vielä riskiyttämisen, jota käytän tutkimukseni toisena teoreettisena viitekehyksenä.

Luvuissa 4–6 esittelen ensin analyysissä käytetyn aineiston tarkemmin, ja sen jälkeen luvuissa 5–6 käsittelen erikseen aineistostani löytämiä uhka -ja riskitekijöitä. Ensin luvussa 5 käsittelen kyberturvallisuuden uhkia, ja olen jakanut käsittelyn kahteen eri osa-alueeseen:

kyberympäristön teknologisiin ja infrastruktuurisiin uhkiin sekä kyberympäristön strategisiin ja geopoliittisiin uhkiin. Luvussa 6 syvennyn käsittelemään taas kyberturvallisuuden riskejä, ja olen jakanut tekijät kahteen eri osa-alueeseen: kyberympäristön teknologisiin riippuvuuksiin, haavoittuvuuksiin ja infrastruktuurien riskeihin sekä sosiaalisiin tekijöihin ja hybridivaikuttamisen riskeihin kyberympäristössä.

Viimeisessä aineistoanalyysiluvussa 8 analysoin ja vertailen aineistosta löytyviä uhka- ja riskitekijöitä, joita on turvallistettu ja riskiytetty dokumenteissa. Vertailen ensin aiemmista kappaleistani löytämiäni uhka ja riskitekijöitä enemmän ylätasolla, ja sen jälkeen käsittelen vielä niitä yksityiskohtaisemmin kahdessa alaluvussa. Ensimmäinen alaluku käsittelee teknologisia ja infrastruktuurisia tekijöitä ja toinen alaluku käsittelee moninaisia vaikuttavia tekijöitä.

Johtopäätöksissä kokoan analyysistäni tehdyt keskeiset havainnot ja tarkastelen, miten turvallistamisen ja riskiyttämisen prosessit ilmenevät Suomen kyberturvallisuuspolitiikassa. Pohdin myös tutkimuksen tulkintaan liittyviä haasteita, kuten aineiston rajaukseen liittyviä kysymyksiä, sekä esitän jatkotutkimuskysymyksiä, jotka liittyvät esimerkiksi yksilön oikeuksien ja tietosuojan syvempään analyysiin kyberuhkien hallinnassa.

2 Aiempi tutkimus kyberturvallisuudesta

Kyberturvallisuusuhat ja -riskit tuovat turvallisuuspoliittiseen kenttään uusia piirteitä, mikä edellyttää niiden huomioimista laajemmin verrattuna perinteisiin turvallisuushaasteisiin. Vaikka kyberturvallisuuden uhkia ja riskejä on tutkittu jonkin verran, erityisesti Suomen kontekstissa tehty tutkimus on edelleen rajallista. Laajemmassa mittakaavassa kuitenkin kyberturvallisuuden tutkimusta on saatavilla enemmän, ja nämä tutkimukset auttavat ymmärtämään riskien ja uhkien eroja sekä niiden vaikutuksia. Seuraavaksi tarkastelen, miten kyberturvallisuutta on määritelty aikaisemmissa tutkimuksissa.

2.1 Kyberturvallisuus käsitteenä

Kyberturvallisuus on noussut kahdessa vuosikymmenessä pienestä asiantuntijoiden johtamasta turvallisuushuolesta valtioiden, kansallisten ja ylikansallisten järjestöjen yhdeksi suurimmista turvallisuuspoliittisista ongelmista. Harvat turvallisuuspolitiikkaan liittyvät alat ovat kehittyneet niin nopeasti kuin kyberturvallisuusala, jonka takia se eroaa merkittävästi muista

turvallisuuspolitiikan aloista. (Backman 2022, 85). Nykyään maailmantalous, yhteiskuntien turvallisuus, yritysten toiminta ja lähes jokainen elämämme osa-alue ovat riippuvaisia kybermaailman toimivuudesta. Riippuvuus digitaaliseen maailmaan kasvaa todella nopeasti, ja tämä avaa uusia mahdollisuuksia hyödyntää rajatonta kybermaailmaa, joka ei ole riippuvainen maantieteellisesti tai ajallisesti. Riippuvuuden kasvaessa tulee kiinnittää erityistä huomiota myös kybermaailman turvallisuuteen. (Limnéll ym. 2015, 13.)

Merkittävimmät epäonnistumiset kyberturvallisuudessa liittyvät siihen, että se on nähty pelkästään teknisenä ongelmana, vaikka nykypäivän digitaalisessa maailmassa se on ennen kaikkea strateginen ja poliittinen kysymys. Kyberturvallisuuden kokonaiskuvan hahmottamisessa ja suunnan määrittämisessä on vielä puutteita, mikä tarkoittaa sitä, että monilla poliittisilla tahoilla ei ole täyttä ymmärrystä kyberturvallisuuden laajuudesta ja monimutkaisuudesta. Tämä taas johtaa siihen, että poliittisilla tahoilla ei ole selkeää suuntaa siitä, miten kyberturvallisuutta tulisi hallita ja käsitellä tehokkaasti. (Limnéll ym. 2015, 13.)

Kyberturvallisuutta voidaan tutkia monen tieteenalan näkökulmasta. Tämä on tehnyt kyberturvallisuuden määrittelystä käsitteenä entistä hankalampaa, sillä eri tieteenalat saattavat määritellä kyberturvallisuutta hieman eri tavoilla. Ne saattavat tutkia kyberturvallisuutta erilaisista näkökulmista, ja sen kautta ottaa eri aspekteja sen käsittelyssä huomioon. Tämä saattaa vaikeuttaa myös eri tieteenalojen välistä dialogia, koska heillä on erilainen näkemys esimerkiksi kyberturvallisuuden ja kyberturvallisuusriskien merkityksestä. (Cains, Flora, Taber, King & Henshel 2022, 1643–1644.) Kyberturvallisuuden hallintaan osallistuvien toimijoiden määrä ja sen hallitsemiseksi omaksuttujen institutionaalisten ja oikeudellisten lähestymistapojen moninaisuus onkin aiheuttanut käsitteellistä sekaannusta siitä, mitä kyberturvallisuus todellisuudessa on, mitä sen pitäisi olla ja miten sitä tulisi hallita (Backman 2022, 85-86).

Kyberturvallisuutta voidaan määritellä esimerkiksi seuraavilla tavoilla. Ensimmäisenä on kyberturvallisuuden määritelmä Merriam–Webster-sanakirjassa, jossa se on ”toimenpiteitä, joilla suojataan tietokonetta tai tietokonejärjestelmää luvattomalta käytöltä tai hyökkäyksiltä. Toisena on Kansainvälisen televiestintäliiton määritelmä, jossa kyberturvallisuutta kuvaillaan taas kokoelmaksi työkaluja, käytäntöjä, turvallisuuskonsepteja, turvatakeita, ohjeita, riskinhallintamenetelmiä, toimia, koulutuksia, parhaita käytäntöjä, takeita ja teknologioita, joita voidaan käyttää työkaluina kyberympäristön turvaamisessa. Kolmantena yhdysvaltalainen

”The Department of Homeland Security’s National Initiative for Cybersecurity Careers and Studies” määrittelee kyberturvallisuuden toiminnaksi tai prosessiksi, joka suojaa tai puolustaa tietoja ja järjestelmiä luvattomalta käytöltä, muokkaukselta, hyödyntämiseltä tai vahingoittumiselta. (Cains, Flora, Taber, King & Henshel 2022, 1644–1645.) Neljäntenä on vielä määritelmä Suomen kyberturvallisuusstrategian 2013 mukaan, joka kuvailee kyberturvallisuutta tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristö koostuu teknologiasta, informaatiosta ja ihmistoimijoista, ja kyberturvallisuuden tavoitteena on varmistaa näiden kolmen tekijän turvallisuus vaaroilta ja häiriöiltä. (Jansson & Sihvonen 2018, 3.) Kybertoimintaympäristöön luottaminen perustuu siihen, että sen toimijat noudattavat asianmukaisia tietoturvallisuuskäytäntöjä. Nämä käytännöt auttavat tietoturvauhkien ennaltaehkäisyssä ja vähentävät niiden haitallisia vaikutuksia, jos niitä kuitenkin ilmenee. Kyberturvallisuus pitää sisällään toimenpiteitä, joilla pyritään hallitsemaan ja tarvittaessa kestämään kyberuhkia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle. (Turvallisuuskomitea 2013, 13.)

Suomen kyberturvallisuusstrategian määritelmä oli ainoa näistä neljästä määritelmästä, joka toi sen esille, että ihmiset ovat myös osana kyberturvallisuutta. Muut määritelmät korostivat kyberturvallisuuden olevan laitteisto- ja ohjelmistokeskeinen eikä niissä otettu huomioon ihmisten ja sosiaalisen vuorovaikutuksen merkitystä. Tämä saattaa nousta ongelmaksi siinä kohtaa, kun arvioidaan kyberturvallisuuden riskejä, koska riskejä on vaikea arvioida kattavasti ilman ihmisten toiminnan näkökulman huomioimista. Kyberturvallisuuden riskimalleihin on alettu sisällyttämään kuitenkin entistä enemmän ihmillisiä tekijöitä eli ihmisten käyttäytymistä, koska se voi aiheuttaa tai lieventää kyberturvallisuusrikkomuksia. Konekeskeistä kyberturvallisuutta on siis haastettu tällaisella ihmisiä osallistavalla lähestymistavalla tutkimuksissa, joita on tehty esimerkiksi sosiologian ja psykologian näkökulmasta. (Cains, Flora, Taber, King & Henshel 2022, 1643–1645.)

Kyberturvallisuus käsitetään yksinkertaistettuna niin, että siinä on kyse vain teknologiasta ja sen toiminnan turvaamisesta. Kyberturvallisuuteen liittyy teknologian lisäksi myös monia poliittisia kysymyksiä. Ilmiö voidaan laajentaa koskettamaan myös valtiollisia tai kansainvälisen tason kysymyksiä, jos kyberiskut ovat esimerkiksi poliittisesti motivoituneita haittaohjelmia, tietovuotoja tai tiedustelutiedon väärinkäyttöä. Kyberriskejä ja -uhkia tarkasteltaessa onkin hyvä huomata, että ne voivat olla moniulotteisia, ja sen takia ison kuvan

hahmottamisessa tulee ottaa useita eri aspekteja huomioon. Kyberturvallisuus voi pahimmillaan olla todella strategista ja poliittista, joka osaltaan aiheuttaa valtioille merkittäviä uhkia. (Jansson & Sihvonen 2018, 4.)

Kybertoimintaympäristö on myös olennainen osa kyberturvallisuutta. Kybertoimintaympäristö muodostuu useista toisiinsa yhdistyneistä tietoverkoista, joissa tietoa siirretään digitaalisessa muodossa käyttäjältä ja koneelta toiselle, tietoliikennetekniikasta, tietokoneista sekä eri tehtäviä hoitavista datasäiliöistä, reitittimistä ja palvelimista. (Jansson & Sihvonen 2018, 2.) Kybertoimintaympäristö on käytännössä siis sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Informaation käsittely sisältää tiedon keräämisen, tallentamisen, järjestämisen, käytön, siirtämisen, luovuttamisen, säilyttämisen, muuttamisen, yhdistämisen, suojaamisen, poistamisen, tuhoamisen ja muita siihen liittyviä toimenpiteitä. (Turvallisuuskomitea 2013, 12.) Näiden tekijöiden lisäksi ihminen on myös osana tätä toimintaympäristöä, koska se vastaa verkon ylläpidosta ja sen toiminnasta. Kybertoimintaympäristöstä spesiaalin tekee se, että siinä ihmisillä on erilaisia toiminnan mahdollisuuksia ja sellaisia uhkia, joita fyysisessä maailmassa ei ole. Kybertoimintaympäristö ei rajoitu minkään tietyn valtion tai alueen rajojen sisäpuolelle, vaan se on kaikkialla siellä, missä verkko on toiminnassa. Kybertoimintaympäristö laajenee ja muuttuu myös koko ajan ja entistä enemmän vielä digitalisaation kehittyessä. (Jansson & Sihvonen 2018, 3–5.) IT-järjestelmien laajeneminen ja uudet laajalti levitetyt sovellukset avaavat joka päivä uusia väyliä kyberhyökkäyksille (Dacorogna & Kratz 2022).

Kyberturvallisuuden kokonaistilan parantamisen tarvetta ovat lisänneet merkittävät muutokset yhteiskunnan toimintaympäristössä, jatkuvasti muuttuvat kyberturvallisuusuhkat, ICT-ympäristöjen kasvava monimutkaisuus, sulautettujen ja perinteisten ICT-järjestelmien yhdistyminen sekä tunnistetut kehitystarpeet kansallisella tasolla. Kyberturvallisuuden integroiminen kaikkeen toimintaan, prosesseihin ja järjestelmiin, joita uhkatekijät koskevat, on välttämätöntä. Kyberturvallisuuden tulisi olla olennainen osa jokaisen organisaation ja yksilön yhteiskuntavastuuta ja on olennainen osa yhteiskunnan häiriötöntä toimintaa. (Sisäministeriö 2023, 24.)

Kyberturvallisuuden voidaan tulkita olevan monimutkainen, mutta tärkeä osa nykyajan yhteiskuntaa, mikä vaatii kokonaisvaltaista lähestymistapaa. Teknologian suojaaminen ei

pelkästään riitä, vaan sen lisäksi on huomioitava myös poliittiset ja yhteiskunnalliset näkökulmat. Kyberuhat ja -riskit eivät ole pelkästään teknisiä haasteita, vaan niillä on syvempiä vaikutuksia valtioiden turvallisuuteen ja vakauteen. Yhteiskunnan toimintaympäristön jatkuva muutos ja digitalisaation nopea kehitys edellyttävät, että kyberturvallisuutta arvioidaan ja kehitetään jatkuvasti. Siksi kyberturvallisuuden tulisi olla keskeinen osa kaikkien organisaatioiden ja yksilöiden vastuullista toimintaa. Kyberuhat ja -riskit eivät siis koske vain tietotekniikkaa, vaan ne vaikuttavat koko yhteiskuntaan ja sen toimintaan.

2.2 Miten kyberturvallisuutta tulisi käsitellä?

Toimintaympäristö ja siihen liittyvät riskit ovat muuttuneet viime vuosina koronapandemian ja Ukrainan sodan myötä. Ne ovat osoittaneet, kuinka tärkeä rooli kyberturvallisuudella on yhteiskunnan kestävyyden kannalta. Yhteiskunta on riippuvainen IT-järjestelmistä ja sen takia kyberhyökkäyksiä vastaan on kunnolla suojauduttava. (Dacorogna & Kratz 2022). Kyberturvallisuus onkin tullut viime aikoina entistä tärkeämmäksi kansallisten ja kansainvälisten turvallisuuskeskustelujen keskiöön. Keskustelut kyberturvallisuudesta ovat yhä enemmän sotilaallistuneita ja kytköksissä strategisiin uhkiin. Sen korostuminen on saanut useat tutkijat pohtimaan, onko kyberturvallisuus turvallistettu eli toisin sanoen, onko se nostettu pois tavallisesta politiikasta ja käsitelty hätätilanteena, mikä oikeuttaa erityistoimenpiteitä turvallisuuden varmistamiseksi. Tämä on herättänyt keskustelua siitä, miten kyberturvallisuutta tulisi käsitellä ja mitä seurauksia sillä voi olla yhteiskunnalle. (Friis & Reichborn- Kjennerud 2016, 27-28.)

Vaikka turvallistaminen onkin yleinen lähestymistapa monien turvallisuuden osa-alueiden tutkimuksessa, sen soveltaminen kyberturvallisuuteen ei välttämättä ole yhtä tehokasta tai soveltuvaa. Kyberturvallisuuden näkökulmasta turvallistamisen soveltaminen voi välillä olla hankalaa, koska perinteinen turvallistamisen malli ei välttämättä sovi hyvin monimutkaisiin kyberuhkiin. Perinteisessä turvallistamisen mallissa korostetaan äkillisiä muutoksia politiikassa ja kiireellisiä vastauksia, johon taas kyberuhkien luonne ja niiden vakavuus eivät aina sovi. Turvallistamisteorian soveltaminen voi olla vaikeaa, kun "normaalien" ja "poikkeuksellisten" toimenpiteiden rajat eivät ole selviä. Lisäksi turvallistamisen soveltaminen ei aina ota huomioon kyberavaruuden käytännön haasteita ja päivittäistä työtä turvallisuuden ylläpitämiseksi. Kyberturvallisuudessa on oltava jatkuva valmius reagoida ja sopeutua uusiin uhkiin ja haasteisiin. (Friis & Reichborn- Kjennerud 2016, 32-33.)

Karsten Friis ja Erik Reichborn- Kjennerud ehdottavat teoksessaan ”Conflict in Cyber Space” uudenlaista viitekehystä turvallistamisteorian puutteiden korjaamiseksi, jotta sen käyttöä ei tarvitse täysin hylätä. Tämän viitekehyksen avulla tehdään selkeä ero "virallisen" turvallistamisen ja muiden, vähemmän dramaattisten mutta silti vakavien turvallisuushaasteiden välillä. Tämä lähestymistapa auttaa meitä tutkimaan, miten materiaaliset ominaisuudet ja asiantuntijoiden toiminta kyberavaruudessa vaikuttavat kyberturvallisuuteen. Tämän uuden viitekehyksen avulla voimme erottaa uhkat ja riskit toisistaan. Uhkat ja riskit ovat molemmat tapoja tulkita ja edustaa tiettyjä vaaroja, mutta tämän viitekehyksen mukaan vain uhkat voidaan todella turvallistaa. Uhkat ovat kuvaus vaarallisista tilanteista, joissa joku taho tarkoituksella ja kyvykkäästi pyrkii aiheuttamaan haittaa. Riskit puolestaan liittyvät todennäköisyyksiin, ennaltaehkäisyyn, tulevaisuuden skenaarioihin ja hallintaan. Tämä lähestymistapa auttaa ymmärtämään paremmin, miten kyberturvallisuutta voidaan hallita erilaisissa tilanteissa ja miten soveltaa turvallisuuskäytäntöjä niiden mukaan. (Friis & Reichborn- Kjennerud 2016, 33.) Tällainen lähestymistapa, jossa uhkia ja riskejä käsitellään erillisinä ilmiöinä, tarjoaa uudenlaista näkökulmaa kyberturvallisuuden tutkimukseen. Se mahdollistaa syvemmän ymmärryksen siitä, miten nämä käsitteet vaikuttavat kyberturvallisuuteen käytännössä. Seuraavassa luvussa käsittelen vielä riskin ja uhkan määritelmää ja niiden keskinäistä suhdetta paremmin.

2.3 Uhka ja riski osana kyberturvallisuutta

Kokonaisturvallisuuden sanastossa kyberturvallisuutta kuvataan tilaksi, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille siitä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa (Sisäministeriö 2023, 23). Tämä määritelmä korostaa, miten kyberturvallisuuteen liittyy olennaisesti myös kyky hallita kybertoimintaympäristöstä aiheutuvia uhkia ja riskejä. On hyvä vielä tarkemmin eritellä, mitä tarkoitetaan käsitteillä uhka ja riski kyberturvallisuuden kontekstissa, ja mikä on niiden keskinäinen suhde.

Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan. (Turvallisuuskomitea 2013, 13.) Uhka voi olla jokin, mikä konkreettisesti vahingoittaa tai vaarantaa tietyn toimijan, kuten organisaation tai järjestelmän. Uhka perustuu siihen, mitä voisi

tapahtua ja siihen, mitä ihmiset pelkäävät tai uskovat voivan tapahtua. Kuinka vakavana uhkaa pidetään ja kuinka uskottavana se nähdään, riippuu siitä, kuinka kyvykäs ja halukas hyökkääjä on, ja kuinka tärkeä kohde on hyökkääjälle. Joissakin tapauksissa, erityisesti kun kyseessä ovat abstraktimmat ja vähemmän tunnetut uhkat, uhkaa saatetaan liioitella. Lisäämällä tietämystä kybermaailmasta voidaan hillitä liioittelua ja lisätä ymmärrystä. (Limnéll ym. 2015, 103-104.)

Kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta, joka toteutuessaan tai jota hyväksi käyttäen kybertoimintaympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä. (Turvallisuuskomitea 2013, 12.) Riskiä ei voi estää, koska se on osa kaikkea toimintaa, myös digitaalisessa maailmassa. Se ei myöskään ole ongelma, koska ongelmat ovat seurausta jo tapahtuneesta. Riski on normaali osa elämää, joka ottaa huomioon mahdolliset uhat, niiden todennäköisyyden ja vaikutuksen. Se ei ole varsinaisesti hyvä eikä huono asia, vaan se muuttuu ajan myötä. Riskejä ei kuitenkaan tule jättää huomiotta, vaan niihin voidaan suhtautua eri tavoin, kuten välttämällä niitä, hyväksymällä ne, vähentämällä niitä tai siirtämällä ne. (Limnéll ym. 2015, 105.) Riskit ovat subjektiivisempia kuin uhat, koska niiden arviointi perustuu usein yksilöiden omiin käsityksiin, arvioihin ja asenteisiin. (Friis & Reichborn- Kjennerud 2016, 34).

Kyberturvallisuuteen liittyvät riskit ja uhat pystytään erottamaan toisistaan. Näitä kahta voidaan tarkastella esimerkiksi aiemmin mainitun turvallistamisteorian kautta, ja vielä erityisesti Kööpenhaminan koulukunnan näkökulmasta. Kööpenhaminan koulukunnan käsitys turvallistamisesta on puheakti, jonka kautta jostain luodaan turvallisuusongelma. Uhista ja riskeistä puhuttaessa pystytään tunnistamaan puhetoimien eri logiikka. Uhkien turvallistaminen keskittyy yleensä vastapuolten toimintaan ja aikomuksiin, ulkoisiin uhkiin kohteena olevaa toimijaa kohtaan sekä näihin uhkiin puolustautumiseen. Sen sijaan riskien turvallistaminen painottaa järjestelmien haavoittuvuuksia ja niiden kykyä selviytyä turvallisuuspolitiikkaan kohdistuvista uhista ja riskeistä. (Backman 2022, 88–89).

Kyberturvallisuutta käsittelevissä diskursseissa voidaan erottaa uhkien ja riskien väliset eroavaisuudet. Kyberturvallisuuden uhkaperustainen diskurssi keskittyy tunnistettavissa oleviin ja akuutteihin kyberuhkiin, kun taas riskeihin perustuva diskurssi tarkastelee kyberavaruuden pitkäaikaisia, pysyviä tai tulevia vaaroja, jotka voivat vaikuttaa yhteiskuntiin. Sen sijaan, että keskityttäisiin poikkeukselliseen politiikkaan tai militarisointiin

eksistentiaalisten uhkien torjumiseksi, riskeihin perustuva turvallisuuslogiikka keskittyy yleensä pitkän aikavälin yhteiskunnalliseen suunnitteluun ja haittojen syiden hallintaan. (Backman 2022, 88–89).

Riskejä tarkasteltaessa riskiyttämismallin hyödyntäminen turvallistamisteorian ohella on perusteltua, koska se tarjoaa näkökulman, joka keskittyy politiikan rakentamiseen riskien näkökulmasta. Se auttaa ymmärtämään, miten tulevaisuuden skenaariot ja niihin liittyvät politiikat voivat vaikuttaa turvallisuuteen. Tämä on tärkeää, koska monimutkaiset yhteiskunnalliset haasteet eivät aina ilmene dramaattisina uhkina, vaan pikemminkin jatkuvina riskeinä. Riskiyttäminen auttaa hahmottamaan, miten riskit voivat muuttua uhkiksi ja päinvastoin eri tilanteissa. (Friis & Reichborn- Kjennerud 2016, 35.)

Vaikka riskit ja uhat pystytään erottamaan toisistaan, niiden ei tarvitse poissulkea toisiaan. Ne voivat esiintyä tutkimuksissa rinnakkain ja sen kautta voidaan saada uudenlaista näkökulmaa turvallisuustutkimukseen. Tällainen lähestymistapa voi olla toimiva juuri sellaisten poliittisten kysymysten suhteen, jotka ovat monimutkaisia ja rajoja ylittäviä. Kyberturvallisuuteen liittyvissä kysymyksissä tällainen tarkastelutapa voi olla toimiva, koska kybertoimintaympäristö ei rajoitu minkään tietyn valtion tai alueen rajojen sisäpuolelle, vaan se on joka puolella, missä verkko toimii. (Backman 2022, 88–89).
Kyberturvallisuuden monimutkaisuus korostaa tarvetta erotella uhkat ja riskit sekä tarkastella niitä eri näkökulmista. Uhkien painottaminen auttaa reagoimaan nopeasti tunnistettaviin vaaratilanteisiin, kun taas riskien analysointi tarjoaa pitkän aikavälin ymmärryksen yhteiskuntaa mahdollisesti uhkaavista ongelmista. Tämä erottelu on erityisen hyödyllinen poliittisessa päätöksenteossa, jossa tarvitaan sekä välittömiä että pitkäjänteisiä toimenpiteitä. Kybertoimintaympäristön globaali ja rajaton luonne tekee uhka- ja riskiajattelun yhdistämisestä entistä tärkeämpää. Tämä näkökulma voi edistää kyberturvallisuustutkimusta ja auttaa luomaan kestävämpiä turvallisuusratkaisuja.

2.4 Kyberriskien kasvu ja niiden vaikutus turvallisuuspolitiikkaan

Aikaisempi tutkimus kyberturvallisuudesta on painottunut enemmän teknisen tietoturvan näkökulmaan, ja miten kyberhyökkäykset pystytään havaitsemaan tietokonejärjestelmien näkökulmasta. Tutkimusta kyberturvallisuuden riskeistä on tehty huomattavasti vähemmän, vaikka kyberriskit ovatkin kasvava ilmiö. Kyberriskeihin liittyviä tutkimuksia löytyy jonkun verran, mutta niitä löytyy liian vähän siihen nähden, että niiden avulla osattaisiin tehdä

kyberriskeistä tarkkoja ennustuksia. Saatavissa olevan tutkimustiedon puute on muodostunut ongelmaksi sellaisille sidosryhmille, jotka pyrkivät hallitsemaan kyberriskejä niihin varautumalla ja niitä estämällä. Tutkimusdataa tarvitaan enemmän kyberriskeistä, jotta sidosryhmät osaavat tarkemmin ennustaa niitä tulevaisuudessa. (Cremer, Sheehan, Fortmann, Kia, Mullins, Murphy & Materne 2022, 718).

Kyberturvallisuuteen liittyvät riskit eroavat luonteeltaan muista turvallisuuspoliittisista riskeistä. Niihin ei voida soveltaa samoja riskimalleja kuin muihin turvallisuuspoliittisiin riskeihin, sillä niiden riskiskenaariot eroavat sen verran muista riskiskenaarioista. Niitä varten on hyvä luoda omat riskimallinnukset, jotta niihin liittyviin riskeihin pystytään varautumaan ja niitä pystytään hallinnoimaan. (Eling & Wirfs 2018, 1117). Kyberriskit eivät kohdistu pelkästään valtioihin, vaan ne aiheuttavat haasteita myös organisaatioille. Kyberriskit ovat varsinkin nykyään merkittävä osa organisaatioiden kokonaisriskiä, ja ne voivat aiheuttaa merkittäviä kustannuksia niiden liiketoiminnalle. Organisaatioiden liiketoiminta voi pysähtyä muun muassa kiristysohjelmahyökkäysten, teknisten vikojen tai toimitusketjun teknisten ongelmien takia. Kyberturvallisuuteen liittyvät riskit voivat organisaatiossa olla joko ulkoisia tai sisäisiä. Joka tapauksessa molemmat kyberhyökkäykset aiheuttavat ylimääräisiä kustannuksia organisaatioille, mikäli niitä ei pystytä estämään tarpeeksi ajoissa. Siksi organisaatioiden riskinhallintamalleissa on hyvä huomioida myös äärimmäiset riskiskenaariot. (Orlando 2021).

Riskienhallinta on keskeinen toimenpide sekä valtioille että erilaisille organisaatioille, jotta liiketoiminnan jatkuvuus voidaan turvata. Riskienhallinnan tavoitteena on luoda ja suojata organisaation arvoa. Tämä tavoite voidaan toteuttaa parantamalla organisaation suorituskykyä, rohkaisemalla innovaatioita ja tukemalla asetettujen tavoitteiden saavuttamista. Nimenomaan kyberriskeihin varautuessa tulee ottaa huomioon, että kyberhyökkäyksiä voidaan suorittaa helposti ja melko halvalla. Niihin varautuminen on koko ajan yhä haastavampaa, sillä isot tietomurrot tai yrityssähköpostien vaarantaminen erilaisten kiristysohjelmien kautta voi tulla kalliiksi yritykselle. Turvallisuusriskien hallinnassa onkin hyvä ottaa huomioon riskien tunnistaminen, arviointi ja käsittely. Sen lisäksi on hyvä tiedostaa organisaation omaisuuden saatavuus ja luottamuksellisuus. Varautumisesta huolimatta on hyväksyttävä, että aina on olemassa riski siihen, että organisaatioon kohdistuva kyberhyökkäys pystytään tekemään. Organisaatioiden tulisi kuitenkin vahvistaa kyberresilienssiään, eli niiden kykyä sietää

kyberhyökkäyksiä ja palautua niistä nopeasti sekä minimoida niistä aiheutuvat kustannukset. (Orlando 2021).

Kyberturvallisuusriskien kasvaessa tarve sen tutkimukselle on myös kasvanut entistä enemmän. Ilmiöstä tarvitaan tutkimusta, jotta siihen osataan paremmin varautua. Vaikka kyberturvallisuuden tutkimuksen tarve on suuri, kyberriskeihin liittyvää tietoa on edelleen rajoitetusti saatavilla. Ilmiön vähäinen tutkimus johtuu siitä, että kyberturvallisuus on noussut turvallisuuspoliittiseksi ongelmaksi kunnolla vasta viime vuosina. Lisäksi siihen liittyvät riskit ovat suhteellisen uusia ja kehittyvät jatkuvasti, mikä tuo jatkuvasti uusia näkökulmia tutkimukseen. Toinen syy voi olla se, että kyberhyökkäysten kohteeksi joutuneet instituutiot eivät anna tapauksista tietoja julkisesti, joten niitä ei voida käyttää tutkimusaineistona. (Cremer ym. 2022, 698-699).

Yksi ratkaisu tutkimusdatan saatavuuden parantamiseksi voisi olla, että tapahtuneet kyberhyökkäykset olisi jatkossa ilmoitettava yhteiselle taholle, joka vastaisi tietojen keräämisestä ja tallentamisesta. Tämän ansiosta tutkijat voisivat analysoida riskejä helpommin ja perusteellisemmin, mikä johtaisi kattavampiin määritelmiin kyberriskeistä. Uuden datan avulla kyberturvallisuuden tutkimuskenttä voisi muodostua yhtenäisemmäksi kokonaisuudeksi. (Cremer ym. 2022, 719).

Kyberhyökkäysten keskitetty ilmoittaminen ja tietojen kerääminen voisi merkittävästi parantaa kyberturvallisuustutkimusta Suomessa. Esimerkiksi kyberturvallisuuskeskus voisi luoda järjestelmän, joka kerää ja analysoi kyberhyökkäyksiä, jolloin tutkijat saisivat tärkeää tietoa käytettäväkseen. Tämä ei vain syventäisi tietämystä kyberriskeistä, vaan vahvistaisi kansallista ja mahdollisesti myös kansainvälistä yhteistyötä niiden torjumisessa. Kun tiedot ovat helpommin saatavilla ja vertailtavissa, saadaan tarkempaa tietoa kyberriskeistä. On kuitenkin tärkeää varmistaa, että tietoja käsitellään turvallisesti, jotta tähän järjestelmään säilyy luottamus ja riskit pysyvät hallinnassa. Tällainen lähestymistapa voisi olla yksi tehokas tapa parantaa kyberriskien arviointia Suomessa ja edistää parempaa valmiutta sekä kyberriskien että -uhkien hallintaan.

2.5 Resilienssi

Turvallisuuden kannalta on olennaista ymmärtää, että resilienssi eli kyky selviytyä erilaisista häiriöistä muodostaa keskeisen osan kokonaisturvallisuutta. Resilienssi on tärkeä tekijä, sillä

sen avulla pystytään sopeutumaan helpommin erilaisiin tilanteisiin tai yllättäviin muutoksiin. Kun resilienssi on vahva, pienet tai suuremmatkin häiriöt eivät horjuta toimintaa liikaa eivätkä aiheuta paniikkia. Tässä suhteessa on tärkeää huomioida, miten resilienssi kehittyy ajan kuluessa ja miten digitalisaation laajentuminen vaikuttaa siihen. Resilienssi on olennainen osa myös, kun puhutaan kyberturvallisuudesta, sen riskeistä ja niiden hallinnasta. (Limnéll ym. 2015, 35.)

Alkaen vuodesta 2012 Maailman talousfoorumin kokouksessa Davosissa, kyberresilienssi on noussut merkittäväksi aiheeksi yksilöiden, yritysten ja yhteiskuntien keskuudessa (Björck 2015, 311). Resilienssillä tarkoitetaan kykyä pysyä vahvana ja sopeutua, kun asiat eivät mene suunnitellusti tai normaalista poikkeavissa tilanteissa. Se tarkoittaa, että toimintaa pystytään jatkamaan, vaikka paine olisi suuri tai osa toiminnasta olisi vaikeuksissa. Lisäksi resilienssi tarkoittaa sitä, että osataan aloittaa toimenpiteitä tilanteen palautumiseksi häiriön sattuessa, vaikka tilanne olisi erityisen haastava. (Limnéll ym. 2015, 234.) Voidaan tarkastella vielä spesifisti kyberresilienssin merkitystä. Kyberresilienssillä tarkoitetaan sitä, että haluttu lopputulos säilyy jatkuvasti, vaikka tapahtuisi haitallisia kybertapahtumia. Tämä voi koskea esimerkiksi koko maata, organisaatiota tai tiettyä tietojärjestelmää. Jokainen näistä tasoista tuo omat haasteensa ja vaatii erilaisia keinoja ja valvontaa kyberresilienssin varmistamiseksi. On tärkeää käsitellä kyberkestävyyttä kokonaisvaltaisesti ja useilla tasoilla samanaikaisesti, jotta se olisi tehokasta. (Björck 2015, 312).

Kyberresilienssi näkee haitalliset kybertapahtumat osana normaalia toimintaa, kun taas perinteisempi turvallisuusajattelu saattaa nähdä ne poikkeuksellisina ja odottamattomina tapahtumina. Tämä ero antaa mahdollisuuden suunnitella vastatoimia ja hätäsuunnitelmia osaksi jokapäiväistä toimintaa sen sijaan, että ne otettaisiin käyttöön vain hätätilanteissa. Tällä tavalla esimerkiksi organisaatiot ja valtiot voivat sopeutua kyberriskeihin ja integroida niiden torjunnan osaksi normaalia toimintaa. Kun yhteinen ymmärrys kyberresilienssin merkityksestä vakiintuu, se auttaa yksilöitä, yrityksiä ja yhteiskuntia kehittämään tehokkaampia kyberresilienssin käytäntöjä. (Björck 2015, 312-315.).

Esimerkiksi monet yritykset ovat haluavat vahvistaa kyberresilienssiä erilaisten riskien varalta, ja se on keskeinen osa liiketoiminnan riskienhallintaa. Tämä näkyy niiden pyrkimyksissä kehittää monimutkaisia kontrollimekanismeja suojatakseen kriittiset liiketoimintaomaisuutensa. (Orlando 2021.) Tietoturvaan sijoitetaan yhä enemmän rahaa, kun

yritykset kehittävät parempia tapoja suojata tärkeitä asioitaan verkossa. Samalla voidaan huomata kehitys, jossa kyberhyökkäysten määrä ja niistä aiheutuvat kustannukset kasvavat. Lisäksi tutkimusten mukaan hakkerit voivat olla keskimäärin yli 200 päivää tietojärjestelmässä ennen kuin heidän tietomurtonsa havaitaan. Kaikkien kyberriskien eliminointi on mahdotonta, kyberhyökkäyksen havaitsemis- ja reagointikyvyllä sekä palautumiskyvyllä on tärkeä merkitys. Kyberturvallisuuden testaus auttaa organisaatioita valmistautumaan hyökkäyksiin ja antaa tärkeää tietoa siitä, miten hyvin järjestelmä pystyy vastaamaan uhkiin. Tämä auttaa organisaatiota arvioimaan, kuinka hyvin se on suojattu kyberuhkilta. (Caron 2021, 193-194.)

Vahva kyberresilienssi auttaa vähentämään häiriöiden vaikutuksia ja varmistaa, että toiminta jatkuu mahdollisimman sujuvasti. Tämä osoittaa, että pelkkä uhkien ja riskien estäminen ei riitä, vaan myös toipumiskyky on keskeistä. Resilienssin tutkiminen ja kehittäminen on tärkeää, jotta löydetään vahvempia ja turvallisempia ratkaisuja nykypäivän digitaalisessa ympäristössä. Tämä ei vain paranna yksittäisten organisaatioiden valmiutta, vaan vahvistaa myös koko yhteiskunnan kykyä kohdata kyberuhkia ja -riskejä. Panostamalla resilienssiin organisaatiot voivat vastata tehokkaammin uhkiin ja riskeihin sekä varmistaa toimintansa jatkuvuuden. Tällainen kokonaisvaltainen lähestymistapa vahvistaa sekä yksilöiden että yhteiskunnan kykyä kohdata ja selviytyä kyberhyökkäyksistä.

3 Teoreettinen viitekehys

Tässä tutkielmassa hyödynnän Kööpenhaminan koulukunnan turvallistamisteoriaa, joka on keskeinen lähestymistapa turvallisuuden tutkimuksessa, sekä Olaf Corryn kehittämää riskiyttämismallia täydentävänä teoriana. Aluksi esittelen turvallistamisteorian taustan ja merkityksen yhteiskuntatieteellisessä tutkimuksessa. Tämän jälkeen tarkastelen, miten turvallistamisteoriaa voidaan käyttää metodina tai työkaluna turvallisuustutkimuksissa. Lopuksi käsittelen riskiyttämismallia, joka täydentää turvallistamisteoriaa keskittymällä riskien hallintaan ja ennaltaehkäisyyn nykyajan turvallisuuspolitiikassa.

3.1 Turvallistamisteoria

Alun perin turvallisuustutkimus keskittyi pääasiassa sotilaallisiin ja valtioon liittyviin kysymyksiin, jolloin turvallisuusongelmat oli helpompi tunnistaa, kun ne liittyivät suoraan sotilassektoriin tai voimankäyttöön. Turvallisuus ja maanpuolustus yhdistettiin vahvasti näihin alueisiin. Nykyään on kuitenkin tärkeää ymmärtää, että turvallisuusongelmia voi esiintyä myös

sotilas- ja valtiotason ulkopuolella. Tällaisia ongelmia on usein vaikea tunnistaa, koska ne eivät ole aiemmin olleet perinteisen turvallisuustutkimuksen kohteena. (Buzan ym. 1998, 1-2.)

Turvallistamisteoria kehittyi 1980- ja 1990-lukujen vaihteessa kylmän sodan päättymisen ja kansainvälisen turvallisuuspolitiikan muutosten seurauksena. Tämä ajanjakso nosti esiin uusia turvallisuuskysymyksiä, kuten ilmastonmuutoksen ja terrorismiin liittyvät uhat, jotka kyseenalaistivat perinteisen käsityksen turvallisuusuhista, jotka oli aiemmin rajattu sotilaalliseen sektoriin. (Wæver 1995, 73.) Turvallisuuden käsite laajentui koskemaan sotilaallisen sektorin lisäksi muun muassa taloudellista, yhteiskunnallista ja ympäristöön liittyviä sektoreita (Buzan ym. 1998, 1).

Monet tahot, kuten rauhantutkimuksen, feministisen tutkimuksen ja turvallisuustutkimuksen alat sekä erilaiset organisaatiot, pitivät turvallisuuden käsitettä liian kapeana. Nämä näkemykset ehdottavat, että turvallisuustutkimusta voidaan tarkastella joko perinteisen sotilas- ja valtiokeskeisen näkemyksen kautta tai laajemman lähestymistavan kautta, joka huomioi myös muut turvallisuuteen vaikuttavat osa-alueet. Laajempi näkökulma voi tuoda esille turvallisuuskysymyksiä, jotka eivät ole heti näkyvillä, kuten älylliset tai poliittiset uhat, ja näiden tunnistaminen on usein haastavampaa. (Buzan ym. 1998, 1-2.)

Turvallistamisteorian lähtökohtana on turvallisuustutkija Ole Wæverin havainto siitä, että turvallisuusuhkien määrittely ja mittaaminen eivät ole täysin objektiivisia. Wæverin mukaan tärkeämpää on se, miten turvallisuudesta puhutaan. Hän esitti vuonna 1995, kun valtion edustaja käyttää termiä 'turvallisuus', hän siirtää kyseisen ongelman erityiseen kategoriaan, mikä oikeuttaa erityisten keinojen käyttöön ongelman ratkaisemiseksi. (Wæver 1995, 73.)

Kyberturvallisuus erityisesti on nykyaikainen turvallisuuskysymys, joka ei sovi perinteiseen sotilaallisen turvallisuuden käsitteeseen, mutta on silti merkittävä uhka valtiolle ja yhteiskunnalle. Turvallistamisteorian näkökulmasta kyberuhat voivat jäädä helposti huomaamatta tai niitä voidaan aliarvioida, jos niitä ei selkeästi esitellä vakavina uhkina. Koska kyberuhat ovat usein vaikeasti havaittavia ja abstrakteja, niiden tunnistaminen ja torjuminen vaatii, että niiden merkityksellisyyttä erikseen korostetaan kansalliselle ja kansainväliselle turvallisuudelle. Tämä osoittaa, että turvallisuuden käsitettä olisi tarpeellista laajentaa perinteisten sotilaallisten uhkien lisäksi myös moderneihin, digitaalisiin uhkiin, kuten esimerkiksi kyberhyökkäyksiin ja tietojärjestelmien haavoittuvuuksiin.

3.1.1 Kööpenhaminan koulukunnan turvallistamisteoria

Kööpenhaminan koulukunnan teoreetikot Barry Buzan, Ole Wæver ja Jaap de Wilde ovat kehittäneet turvallistamisteorian alkuperäisen version. Turvallistamisen käsite on esitetty ensimmäistä kertaa Barry Buzanin, Ole Wæverin ja Jaap de Wilden teoksessa ”Security: A New Framework For Analysis” vuonna 1998. Tämän teorian pohjalta turvallistamisen käsitettä on laajennettu, ja eri tutkijat ovat esittäneet siitä erilaisia tulkintoja. (Stritzel 2014, 11.)

Buzanin ja hänen kollegoidensa tulkinnan mukaan turvallisuus liittyy olennaisesti selviytymiseen. Turvallistamista tarvitaan, kun jokin kohde, kuten valtio, kokee suuren ja eksistentiaalisen vaaran. Näitä kohteita, joita kutsutaan referenttiobjekteiksi, pidetään niin tärkeinä, että niiden eloonjääminen on ensisijaista. Perinteisesti valtiota on pidetty tällaisena referenttiobjektina, jolla on oikeus ryhtyä voimakkaisiin toimiin eksistentiaalisia uhkia vastaan. Turvallisuuden käsitteen käyttö on tärkeää, koska se antaa valtioille mahdollisuuden perustella voimankäyttöä ja reagoida suuriin uhkiin. Kun valtion johtaja puhuu "turvallisuudesta", se tarkoittaa usein, että tilanne on niin vakava, että valtio voi julistaa hätätilan ja käyttää kaikkia tarvittavia toimenpiteitä uhan torjumiseksi. Eksistentiaalinen uhka tarkoittaa tilannetta, jossa jotain tärkeää, kuten valtio, on vaarassa. Tämä uhka ei ole sama kaikilla alueilla tai tasoilla, vaan se vaihtelee sen mukaan, mistä on kyse. Turvallisuuden käsite toimii poliittisena välineenä, joka voi muuttaa sääntöjä ja vaikuttaa siihen, miten politiikkaa toteutetaan. (Buzan ym. 1998, 21-22.)

Turvallistamista voidaan lähtökohtaisesti verrata politisoimiseen. Eroavaisuus näiden kahden välillä on kuitenkin se, että turvallistamisessa jokin asia ei esiinny vain poliittisena ongelmana, vaan erityisesti turvallisuuspoliittisena ongelmana. Turvallistamisen kautta jokin asia saatetaan esittää merkittävänä turvallisuusuhkana kansallisesti tai kansainvälisesti, ja tämän vuoksi sen ratkaisemista tulisi pitää ensisijaisena muihin uhkiin nähden. Turvallistamisen kautta uhka voidaan esittää suurempana kuin se todellisuudessa on. Todellinen uhka ei välttämättä ole niin vakava kuin turvallistamisen yhteydessä annetaan ymmärtää. (Buzan ym. 1998, 23-24.)

Välillä saattaa olla vaikeaa erottaa onko jokin julkinen asia pelkästään politisoitunut vai onko se myös turvallistettu. Tämä yhteys politisoinnin ja turvallistamisen välillä viittaa siihen, että turvallistaminen ei aina ole valtion harjoittamaa, vaan myös muut toimijat voivat esittää asioita turvallisuusuhkina. Julkisesta asiasta tulee turvallisuusuhka, koska se esitetään sellaisena. Turvallistamisen tarkka määrittely ja kriteerit perustuvat siihen, että tunnistetaan yhteisesti

koettu eksistentiaalinen uhka, jonka katsotaan olevan riittävän merkittävä vaikuttaakseen politiikkaan. Kun jokin asia esitetään keskustelussa eksistentiaalisena uhkana jollekin viitekohteelle, tämä yksinään ei vielä johda turvallistamiseen. Sen sijaan kyseessä on turvallistava liike, ja asiaa pidetään turvallistettuna vasta, kun yleisö hyväksyy sen uhkana. Turvallistava lähestymistapa ei painota välittömien hätätoimien käyttöönottoa. Sen sijaan se korostaa, että ennen kuin voidaan oikeuttaa hätätoimenpiteitä tai muita toimia, eksistentiaalisen uhka on ensin perusteltava selkeästi ja saatava riittävä tuki sen tunnustamiselle. (Buzan ym. 1998, 24-25.)

Kööpenhaminan koulukuntaan kuuluvat tutkijat näkevät turvallistamisen pääosin puheaktina. Heidän mukaansa puheen avulla voidaan luoda jostain asiasta tai ilmiöstä turvallisuusuhka. (Stritzel 2014, 13.) Tällä tarkoitetaan sitä, että kun jostain asiasta aletaan puhumaan turvallisuusuhkana, siitä tulee sellainen. Käytännössä joku voi ilmoittaa, että tietylle asialle on muodostunut uhka, ja tämän perusteella voidaan toteuttaa poikkeuksellisia toimenpiteitä sen suojelemiseksi. Tällaisessa tilanteessa turvallisuuskysymys siirtyy normaalin politiikan alueelta niin kutsutun hätäpolitiikan alueelle. Hätäpolitiikan alueella turvallisuuskysymykseen reagoidaan nopeammin ja siinä ei välttämättä sovelleta normaaleja demokratian toimintamalleja. Turvallisuus ei ole tällaisessa tilanteessa etukäteen määritelty, vaan sen merkitys määräytyy sen mukaan, miten uhka esitetään. Kööpenhaminan koulukunnan tutkijoiden mukaan turvallisuuden merkitys määrittyy ihmisten välisessä vuorovaikutuksessa. (Taureck 2006, 54-55.) Tätä puheaktin ilmiötä tarkastellaan tarkemmin seuraavassa luvussa.

Turvallistamisen kautta pyritään suojaamaan tiettyjä kohteita turvallisuusuhkilta. Suojaamisen kohteina on yleensä valtio, väestö, jokin yhteisö tai alue. Suojaamisen kohteina voi olla näiden asioiden lisäksi myös esimerkiksi identiteetti, kulttuuri, ympäristö, organisaation vakaus tai sosiaalinen järjestys sekä rahoitusjärjestelmä tai markkinat. (Stritzel 2014, 15.)

Osa tutkijoista on rakentanut tutkimuksensa Kööpenhaminan koulukunnan turvallistamisnäkemyksen pohjalta, vaikka ne eivät ole täysin rekonstruoitavissa. Toiset tutkijat ovat sen sijaan päättäneet hakea uusia lähestymistapoja turvallistamisteoriaan Kööpenhaminan koulun ulkopuolelta, ja lähteneet rakentamaan vaihtoehtoista toisen sukupolven näkemystä turvallistamisteoriasta. (Stritzel 2014, 11-12.) Turvallistamisteoria onkin alkuperäisen muodostumisensa jälkeen jakautunut erilaisiksi teoreettisiksi alasuuntauksiksi. Keskeisimmät kaksi alasuuntausta ovat filosofinen koulukunta ja sosiologinen koulukunta. Kööpenhaminan

koulukunnan käsitys turvallistamisteoriasta kuuluu filosofiseen koulukuntaan. (Balzacq 2011, 1-3.)

Turvallistamisteorian vaikutus näkyy laajasti kansainvälisessä turvallisuustutkimuksessa, ja sen rooli on ollut merkittävä etenkin siinä, miten turvallisuusuhat esitetään ja miten niihin reagoidaan. Teorian laajeneminen ja jakautuminen eri suuntauksiin, kuten filosofiseen ja sosiologiseen lähestymistapaan, korostaa sen monipuolisuutta ja soveltuvuutta erilaisiin tilanteisiin. Tämä kehitys herättää kysymyksiä turvallistamisteorian soveltamisesta nykypäivän turvallisuusuhkiin, kuten ilmastonmuutokseen, kyberturvallisuuteen tai pandemioihin, joissa uhkat ovat monitasoisia ja monesti epätarkasti määriteltyjä. Keskeiseksi pohdittavaksi asiaksi nousee, missä määrin turvallistamisteorian viitekehys mahdollistaa näiden uusien uhkien ymmärtämisen ja kuinka se voi toimia politiikan välineenä näiden uhkien hallinnassa.

3.1.2 Puheakti, toimija ja yleisö

Kööpenhaminan koulukunnan mukaan turvallistamiseen tarvitaan kolme keskeistä tekijää: puheakti, turvallistava toimija ja yleisö (Barthwal-Datta 2012, 6). Ensin voidaan tarkastella yksityiskohtaisemmin puheaktia, joka on Kööpenhaminan koulukunnan turvallistamisen teorian ytimessä. Tämä lähestymistapa korostaa, että pelkkä turvallisuudesta puhuminen ja sen määritteleminen on jo itsessään merkittävä turvallisuustoimi. Se, miten turvallisuusongelmat ilmaistaan, vaikuttaa suoraan siihen, miten niihin suhtaudutaan ja millaisia sosiaalisia käytäntöjä ja vuorovaikutusta niiden ympärille muodostuu. Turvallisuuden artikulointi viittaa siihen, että tietty asia nähdään uhkana arvokkaalle kohteelle, mikä oikeuttaa normaalista politiikasta poikkeavien turvallisuustoimien käytön. Tämä antaa turvallistavalle toimijalle valta-aseman määritellä, miten kyseistä uhkaa käsitellään. Wæverin mukaan valtion 'turvallisuus'-termin käyttö nostaa esille asian vakavuuden ja oikeuttaa poikkeustoimenpiteiden käytön sen torjumiseksi. (Stritzel 2007, 360.)

Turvallistamisteorian puheakti pohjautuu John L. Austinin käsitykseen "performatiivisista lausunnoista". Austinin mukaan performatiiviset lausunnot eivät pelkästään kuvaa todellisuutta, vaan niillä on kyky luoda ”uutta” todellisuutta. Performatiiviset lausunnot eivät toimi perinteisen totuus/väärä-ajattelun mukaisesti, vaan vaan ne edellyttävät tiettyjä "onnistumisolosuhteita". Tämä tarkoittaa sitä, että vaikka puheakti ei olisikaan totta, se voi silti tapahtua onnistuneesti, jos tietyt ehdot täyttyvät. Turvallisuustutkimuksessa tämä siirtää huomion pois perinteisestä uhka–todellisuus -suhteesta siihen, mitä puheakti saa aikaan. Wæver

väittää soveltaen Austinin ajatuksia, että pelkkä "turvallisuus"-termin käyttö ei ole pelkästään jonkin asian sanallista ilmaisemista tai kuvailemista, vaan itse asiassa konkreettinen teko. Kööpenhaminan koulun näkökulmasta tämä merkitsee poikkeuksellista tapaa käsitellä turvallisuutta. Heidän mukaansa, kun turvallisuus nostetaan esiin puheessa, se voi johtaa siihen, että yleisö hyväksyy sääntöjen rikkomisen, jota ei normaalisti hyväksyttäisi. (Stritzel 2007, 361.)

Toinen merkittävä tekijä puheaktin lisäksi on turvallistava toimija, joka toteuttaa turvallistamisen puheaktin kautta. Turvallistava toimija voi olla henkilö tai taho, joka aloittaa keskustelun jonkun asian turvallisuudesta. Usein tämä henkilö tai taho edustaa laajempaa ryhmää tai organisaatiota, joka lopulta päättää tarvittavista toimenpiteistä. Useimmiten turvallistavat toimijat ovat virkamiehiä, poliittisia johtajia, lobbareita tai painostusryhmiä. He pyrkivät usein perustelemaan toimenpiteitänsä väittämällä, että valtion, kansakunnan tai sivilisaation, turvallisuuden puolustaminen on välttämätöntä. Kööpenhaminan koulukunnan tutkijat suosittelevat, että silloin kun turvallistavat toimijat ovat vahvasti sidoksissa tiettyihin rooleihin, niiden tarkastelu kollektiivisina edustajina – kuten puolueina, valtioina tai painostusryhminä – on hyödyllisempää kuin keskittyminen yksittäisiin henkilöihin. (Barthwal-Datta 2012, 6.)

Turvallistavien toimijoiden roolia tutkiessa on tärkeää ymmärtää, miten nämä toimijat tunnistetaan ja millaisia tekijöitä vaikuttaa heidän toimintaansa. Ensinnäkin turvallistavan toimijan tunnistaminen liittyy enemmän siihen, millainen logiikka ohjaa toimintaa kuin siihen, kuka esittää puheen. Tämä tarkoittaa, että keskeistä on ymmärtää, onko toimintaa ohjaava logiikka yksilön vai organisaation, ja miten vastuuta jaetaan eri toimijoiden kesken. Puheaktin organisaatiologiikkaan keskittyminen on useimmiten tehokkain tapa selvittää, kuka tai mikä edistää turvallisuutta. Turvallistavan toimijan ja viitekohteen erillisyys merkitsee sitä, että on olemassa "yleisö", eli ne, jotka pyritään saamaan hyväksymään ennennäkemättömät toimenpiteet tietyn turvallisuusongelman vuoksi. (Buzan ym, 1998, 41–42.) On tärkeää huomata, että turvallistava toimija ei automaattisesti ole valtio tai sen virkamies. Toimijat voivat olla erityyppisiä, mukaan lukien kansalaisjärjestöt, yritykset tai kansainväliset organisaatiot, jotka vaikuttavat turvallisuuskysymyksiin. Tämä monimuotoisuus tuo esiin kysymyksen siitä, miten erilaiset toimijat ja heidän logiikkansa vaikuttavat turvallisuuskäytänteisiin ja -päätöksiin.

Kolmas keskeinen tekijä turvallistamisteoriassa on yleisö. Kööpenhaminan koulukunta käsittelee turvallistamista prosessina, jossa keskeistä on turvallisuudesta puhuvan toimijan ja merkittävän yleisön välinen vuorovaikutus. (Stritzel 2007, 363.) Teorian perusajatuksena on, että turvallistaminen on intersubjektiivinen prosessi, joka perustuu yleisön hyväksyntään. Kööpenhaminan koulukunnan tutkijoiden mukaan turvallistaminen voi tapahtua vasta, kun yleisö on hyväksynyt sen. (Balzacq ym. 2016, 499.) Tämä tarkoittaa, että kun jokin asia nähdään uhkana, sen tulkinta ja esittäminen ei ole pelkästään yhden toimijan tekemä päätös, vaan siitä käydään vuorovaikutteista keskustelua ja neuvottelua toimijan ja siihen liittyvän yleisön välillä. Vaikka toimija voi esittää oman tulkintansa ja näkemyksensä uhasta, lopullinen ratkaisu, eli se hyväksytäänkö tämä tulkinta yhteiseksi käsitykseksi, on yleisön päätettävissä. (Stritzel 2007, 363.)

Yleisön rooli turvallistamisessa ei ole aina yksiselitteinen, ja empiirisissä tutkimuksissa saattaa herätä erilaisia kysymyksiä. Tutkimuksissa ei ole aina selvää, mikä yleisö on milloinkin merkittävin ja miksi. Lisäksi ei ole aina helppo määritellä, milloin yleisö voidaan katsoa "vakuuttuneeksi" jostain asiasta. (Stritzel 2007, 363.) Tutkijat ovat pyrkineet myös ymmärtämään, millaisia ominaisuuksia ja kriteerejä yleisön hyväksyntään liittyy. He ovat pohtineet myös, miten useiden eri yleisöjen olemassaolo vaikuttaa teorian soveltamiseen ja miten yleisön hyväksyntä voi ilmetä eri tavoin ja erilaisissa tarkoituksissa. (Balzacq ym. 2016, 499.) Kysymyksiä herättää myös ajatus siitä, onko jokin turvallistettu asia ”hyväksytty intersubjektiivisesti" eli hyväksytty vapaaehtoisesti ilman ulkoista pakkoa tai sortoa. (Stritzel 2007, 363.)

Turvallistamisteoria tuo esiin, kuinka tärkeää on ymmärtää puheakti, toimija ja yleisö kokonaisuutena. Teoria korostaa, että turvallisuuden rakentaminen ei ole vain yksittäisen toimijan käsissä, vaan edellyttää yleisön hyväksyntää. Tämä on erityisen ajankohtaista kyberturvallisuuden kohdalla, jossa uhat eivät yleensä ole näkyvissä ja niitä voi olla vaikea hahmottaa. Toimijat, kuten hallitukset ja asiantuntijat, joutuvat vakuuttamaan yleisön näiden uhkien vakavuudesta ilman konkreettisia todisteita, mikä korostaa puheaktin merkitystä. Tapa, jolla kyberuhat esitetään, vaikuttaa suoraan siihen, miten yleisö ne hyväksyy ja millaisia toimenpiteitä ryhdytään toteuttamaan. Tämä tekee yleisön roolista ratkaisevan tärkeän kyberturvallisuuden turvallistamisessa.

3.1.3 Turvallistamisen oikeuttaminen

Kaikkia asioita ei kuitenkaan pysty muuttamaan turvallisuuskysymyksiksi, vaan onnistunut turvallistaminen muodostuu kolmesta vaiheesta. Ensimmäinen vaihe on olemassa olevien uhkien tunnistaminen. Toinen vaihe on hätätoimenpiteet ja niiden toteuttaminen. Kolmas vaihe keskittyy tarkastelemaan, miten nämä poikkeustoimet vaikuttavat eri yksiköiden välisiin suhteisiin. Tämä tarkoittaa käytännössä sitä, miten eri ryhmät ja organisaatiot sopeutuvat tilanteisiin, joissa normaaleja sääntöjä ei noudateta hätätilanteiden vuoksi. (Taureck 2006, 55.)

Ensimmäinen vaihe vaatii tilanteen, jossa jokin uhkaa olemassaoloa. Tämän tilanteen seurauksena on tarpeen asettaa kyseinen uhka turvallisuuskysymykseksi. Turvallisuuskysymys on yleensä kiireellinen ja vakava, ja sen laiminlyöminen voi vaarantaa yksilöiden tai yhteiskunnan olemassaolon tai kyvyn. Tämä korostaa kyseisen turvallisuusuhkan priorisointia muiden asioiden yli ja osoittaa sen merkityksen. Teoriassa mikä tahansa ryhmä tai organisaatio voi turvallistaa jonkun asian, kunhan se saa yleisön hyväksynnän sille, että tietyn turvallisuuskysymyksen kohdalla on tarve soveltaa normaaleja sääntöjä tai toimintatapoja. Käytännössä valtion hallinto kuitenkin useimmiten luo turvallisuuskysymykset, mikä osaltaan taas monimutkaistaa turvallisuuden tutkimusta, koska se rajoittaa sitä, kuka voi määritellä turvallisuuden ja millä perusteilla. (Taureck 2006, 55.)

Turvallistamista tutkinut Ole Wæver suhtautuu kriittisesti asioiden turvallistamiseen ja siihen, miten turvallisuuskysymykset määritellään tai esitetään tietyssä viitekehyksessä. Hänen mukaansa turvallisuusnäkemykset eivät saisi olla liian rajoittuneita tai vääristyneitä, sillä ne voivat ohjata poliittisia päätöksiä tiettyyn suuntaan. Tämän takia Wæver on tuonut esille kannattavansa turvallisuuden ”purkustrategiaa”, joka pyrkii vähentämään turvallisuuskysymysten liiallista korostamista ja siirtämään ne normaalin poliittisen päätöksenteon piiriin. Tämä on kuitenkin Wæverin normatiivinen käsitys turvallistamisesta. (Taureck 2006, 55.)

Kööpenhaminan koulukunnan teoreetikot ovat laajasti pohtineet turvallistamisen oikeuttamista, erityisesti sitä, kuka voi turvallistaa asioita ja millä perustein. He ovat myös pohtineet, kuinka painava syy tarvitsee esimerkiksi olla, että jokin asia turvallistetaan. Teoreetikot käyttävät tästä teoksessaan ”Security: A New Framework For Analysis” esimerkkinä toisen maailmansodan aikaista tilannetta: Iso-Britannian pääministeri Churchill olisi voinut painottaa Saksan ja natsismin olevan vakava turvallisuusuhka Euroopalle. Saksan valtakunnankansleri Hitler taas

olisi voinut turvallistaa Iso-Britannian sen vuoksi, että tämä näki Saksan uhkana. Turvallistaminen ei kuitenkaan edellytä vastavuoroista reaktiota; Hitler olisi voinut pitää Britanniaa uhkana riippumatta sen toimista. Turvallistaminen on aina jollain tavalla yhteydessä turvallistavaan toimijaan eli siihen henkilöön, joka on puheaktin kautta tehnyt jostain asiasta turvallisuusongelman. Uhka voi näyttäytyä eri tavalla eri toimijoille, mikä tekee tärkeäksi sen, kuka puheen pitää ja kenelle se on suunnattu. (Buzan, Wæver & de Wilde 1998, 44-45.)

Turvallistamisen oikeuttaminen nostaa esiin kysymyksen siitä, kuka saa määritellä turvallisuusuhat ja millä perusteilla. Vaikka teoriassa kuka tahansa voi turvallistaa asian, käytännössä valtioilla ja muilla vaikutusvaltaisilla toimijoilla on suurin valta tässä keskustelussa. Tämä vallan keskittyminen voi rajoittaa avointa keskustelua ja politisoida turvallisuuskysymykset. Wæverin kriittinen näkemys korostaa, että liiallinen turvallistaminen voi rajoittaa normaalia poliittista päätöksentekoa ja legitimoida tarpeettomia poikkeustoimia. Tämä herättää kysymyksen siitä, käytetäänkö turvallisuuspuhetta joskus tarpeettomien toimenpiteiden perustelemiseen, jotka eivät ole hyödyllisiä yhteisen edun kannalta. On tärkeää miettiä, miten turvallisuuskysymyksiä arvioidaan ja miten voidaan estää turvallisuuspuheen liiallinen käyttö vallan välineenä. Voidaanko turvallisuusprosesseja tehdä avoimemmiksi, jotta demokratia ja avoin keskustelu säilyvät tärkeinä?

3.2 Turvallistamisteoria metodina

Tässä tutkimuksessa turvallistamisteoria toimii sekä teoreettisena viitekehyksenä että metodologisena työkaluna. Sen avulla voidaan analysoida, miten Suomen kansallisissa riskiarvioissa ja kyberturvallisuusstrategioissa rakennetaan kyberturvallisuuden uhkia ja riskejä diskursiivisesti. Turvallistamisteoria tarjoaa keinoja ymmärtää, miten tietyt asiat esitetään turvallisuusuhkina ja miten nämä uhkakuvat johtavat poikkeuksellisiin toimenpiteisiin. Keskeistä tässä on diskursiivinen lähestymistapa, jonka avulla tarkastellaan, miten uhkakuvia luodaan ja vahvistetaan eri yhteyksissä. (Balzacq 2011, 32-33, 39.) Turvallistamisteoria ei ainoastaan paljasta, miten uhkakuvat rakentuvat, vaan myös sen, miten nämä rakennetut uhkat muokkaavat yhteiskunnallisia ja poliittisia päätöksiä. Se auttaa ymmärtämään, miksi tietyt asiat nostetaan keskeisiksi uhkatekijöiksi ja miten tämä vaikuttaa poliittiseen ja sosiaaliseen toimintakenttään.

Diskurssianalyysi on olennainen osa turvallistamisteoriaa, koska se tutkii, miten kielen ja merkitysten avulla luodaan uhkia. Tämä menetelmä auttaa ymmärtämään, miten sosiaalista

todellisuutta rakennetaan poliittisissa keskusteluissa ja miksi tietyt asiat esitetään uhkina tietyissä konteksteissa. (Jokinen, Juhila & Suoninen 2004, 9–10.) Tässä tutkimuksessa analysoin Suomen riskiarvioita ja kyberturvallisuusstrategioita tunnistaakseni ne uhkat ja riskit, jotka on esitetty keskeisinä turvallisuusongelmina kyberturvallisuuden näkökulmasta. Turvallistamisteorian avulla analysoin, miten nämä tekijät on esitetty eksistentiaalisina uhkina, jotka oikeuttavat poikkeuksellisia toimenpiteitä. Analyysi keskittyy erityisesti dokumenttien kielellisiin ja retorisiin keinoihin, kuten uhkien kuvaamiseen, esittämiseen ja perusteluun.

Kyberuhkat ovat usein abstrakteja ja vaikeasti havaittavia, minkä vuoksi niiden turvallistaminen perustuu vahvasti diskursseihin. Turvallistaminen onnistuu, kun diskursseissa korostetaan uhkien kiireellisyyttä ja vakavuutta (Balzacq 2011, 46–47.) Näiden diskurssien tarkastelu kielen ja merkitysten kautta on mahdollista diskurssianalyysin avulla, joka tutkii, miten sosiaalista todellisuutta ja uhkakuvia rakennetaan eri konteksteissa (Jokinen ym. 2004, 10.) Tämän vuoksi turvallistamisteorian ja diskurssianalyysin yhdistelmä on keskeinen työkalu kyberturvallisuuden uhkien ja riskien tutkimuksessa.

3.3 Riskiyttäminen

Olaf Corry on kehittänyt käsitteen "riskiyttäminen", joka viittaa sosiaaliseen prosessiin, jossa poliittisia kysymyksiä käsitellään riskien, ei pelkkien uhkien kautta. Tämä käsite täydentää turvallistamisteoriaa, ja se voidaan sijoittaa oikeastaan turvallistamisen ja politisoinnin väliin. Se tuo esille näkökulman, joka korostaa tulevaisuuden skenaarioiden ja riskien hallinnan merkitystä nykyaikaisissa yhteiskunnissa. (Friis & Reichborn- Kjennerud 2016, 35.) Riskiyttäminen nähdään turvallisuustutkimuksessa uutena turvallisuuden mallina, jossa korostetaan ennaltaehkäisyä, riskien arviointia ja hallintaa pikemminkin kuin akuuttien uhkien torjumista. Nykyajan turvallisuuskäytännöissä painotetaan todennäköisyyksien arviointia ja hajautettujen riskien hallintaa, eikä niinkään vastustajien pelottelua tai välittömiä toimenpiteitä. Tähän liittyvät pitkäaikaiset turvallisuushankkeet sekä varovaisuusperiaatteen laajeneminen turvallisuuskysymyksiin. Lisäksi on otettu käyttöön monipuolisia riskinhallintatekniikoita, kuten rekisteröinti, seulonta ja profilointi. (Corry 2012, 236.)

Riskiarviot ja riskien hallinta eivät kosketa vain perinteisiä turvallisuusuhkia, vaan ne ulottuvat laajasti eri elämänalueisiin. Riskiyttämisen ydin on siinä, että riskejä tarkastellaan laajasti eri yhteiskunnallisissa konteksteissa. Riskien arvioinnista ja hallinnasta on tullut olennainen osa monia tilanteita ja päätöksentekoprosesseja, mikä korostaa riskiyttämisen laajaa vaikutusta

yhteiskunnassa. (Hardy & Maguire 2016, 95.) Lisäksi yhteiskunnat varautuvat jatkuvasti erilaisiin katastrofaalisiin skenaarioihin, kuten ilmastonmuutokseen tai ydinsotaan. (Corry 2012, 236).

Riskiyttäminen laajentaa turvallisuuden käsitettä ja sen soveltamista uusiin huolenaiheisiin, mikä tarkoittaa kokonaisuudessaan turvallisuuden käsityksen monipuolistumista (Estève 2021, 602). Tällainen muutos turvallisuusalalla ja turvallisuuden tutkimuksissa on merkittävä. Huomionarvoista kuitenkin on se, ettei ”riskiä” vielä näy niin paljon turvallisuuden peruskäsitteissä, kuten Kööpenhaminan koulun turvallistamisen käsitteessä. Kööpenhaminan koulukunta painottaa omassa turvallisuuskäsitteessään enemmänkin sitä, kuinka turvallistavat puheaktit oikeuttavat poikkeukselliset poliittiset toimenpiteet, jotka tehdään turvallisuutta uhkaavan vaaran takia. Riskin huomioiminen osana turvallisuutta on lisääntynyt, mutta siitä huolimatta sen vaikutus ”perinteiseen” turvallisuuteen on edelleen hieman epäselvää. Riskien tunnistamisen on ainakin kuvailtu johtavan turvallisuustoimenpiteiden laajentamiseen tai uusien turvallisuuskäytäntöjen kehittämiseen. Tällä tavoin voidaan parantaa yleistä turvallisuutta ja valmistautumista mahdollisiin uhkiin tai vaaratilanteisiin. (Corry 2012, 236).

Corryn mukaan mikään asia ei ole itsessään välttämättä uhka tai riski, koska erilaiset vaarat voivat vaihdella tulkinnaltaan riskin ja uhan välillä eri aikoina. Erottamalla uhkaturvallisuuspolitiikat ja riskiturvallisuuspolitiikat toisistaan ei siis voi suoraan päätellä, että jälkimmäinen olisi vakavampi tai vaarallisempi kuin edellinen. Sen sijaan Corry esittää, että riskiturvallisuus voidaan erottaa uhkaturvallisuudesta kolmen keskeisen ominaisuuden avulla. Ensinnäkin riskiyttäminen korostaa haitan perustavia syitä toisin kuin haitan suoria aiheuttajia (kuten uhkia). Tämä avaa mahdollisuuden tarkastella taustatekijöitä ja rakenteita, jotka mahdollistavat haitallisten tapahtumien syntymisen. Toiseksi se muuttaa turvallisuustoiminnan painopistettä ulkoisesta uhkasta sisäisten haavoittuvuuksien hallintaan. Kolmanneksi riskiyttäminen edistää pitkän aikavälin strategista ajattelua ja ennaltaehkäiseviä toimia pikaisen puolustuksen sijaan. Nämä tekijät yhdessä luovat pohjan riskipolitiikan kehittämiselle, joka pyrkii hallitsemaan ja vähentämään mahdollisia tulevia haittoja. (Friis & Reichborn- Kjennerud 2016, 35-36.)

Turvallisuustutkijat ovat kuitenkin havainneet, että riskipuhe voi joskus aiheuttaa tarpeetonta paniikkia ja liioitella turvallisuusuhkia, vaikka riski olisi todellisuudessa pieni. Esimerkiksi sotilaat saattavat perustella tiukkojen toimenpiteiden käyttöönottoa riskin vuoksi, vaikka

todellinen uhka olisi vähäinen. Tämä voi johtaa siihen, että he toimivat ilman selkeää käsitystä tilanteen todellisesta vaarallisuudesta. Tällainen lähestymistapa korostaa varovaisuutta ja ennaltaehkäisyä, vaikka riski olisi vähäinen, mikä voi ohjata turvallisuuspolitiikkaa liialliseen varovaisuuteen. (Estève 2021, 606.)

Turvallisuuskeskustelussa käsitteet riski ja uhka esiintyvät usein rinnakkain, vaikka ne eroavat merkittävästi toisistaan. Riskin ja uhan välinen ero on keskeinen tekijä nykyaikaisen turvallisuuspolitiikan muotoutumisessa. On tärkeää ymmärtää, ettei riskipolitiikka suoraan korvaa turvallistamista, vaan edustaa erilaista lähestymistapaa turvallisuuskysymyksiin. Jos kaikki uhat ja riskit luetaan turvallistamiseksi, voidaan tehdä virheellisiä päätelmiä ja esimerkiksi käyttää turvallistamisen purkustrategiaa tilanteissa, joissa se ei ole tarkoituksenmukaista. (Corry 2012, 237.)

Voidaan tarkastella tarkemmin uhkakeskeisen ja riskikeskeisen turvallistamisen määritelmiä sekä niiden keskeisiä eroavaisuuksia. Uhkakeskeinen turvallistaminen perustuu ajatukseen välittömästä uhasta tai suorasta vahingosta, joka vaatii poikkeuksellisia toimenpiteitä. Tällainen uhka esitetään kiireellisenä ja vakavana, mikä oikeuttaa nopean reagoinnin ja voi lisätä tiettyjen yhteiskunnallisten toimijoiden, kuten viranomaisten, päätösvaltaa. Riskikeskeinen turvallistaminen puolestaan käsittelee uhkia laajempina ja hajanaisina riskeinä, jotka liittyvät erilaisiin skenaarioihin ja vaativat pitkäaikaista hallintaa. Tämä lähestymistapa painottaa riskien arviointia ja hallintaa pikemminkin kuin välittömiä, poikkeuksellisia toimia. Riskikeskeinen turvallistaminen johtaa usein siihen, että vastuu jakautuu useiden toimijoiden kesken ja hallintastrategiat rakennetaan yhteistyössä monien viranomaisten ja asiantuntijoiden kanssa. Nämä kaksi lähestymistapaa eroavat siinä, että uhkakeskeinen turvallistaminen painottaa välittömän vahingon uhkaa, kun taas riskikeskeisessä turvallistamisessa keskitytään hajautettuihin riskeihin ja niiden hallintaan. (Rhinard ym. 2024, 679–681.)

Riskiyhteiskuntaa tutkineen Ulrich Beckin mukaan kapitalistinen moderni yhteiskunta synnyttää jatkuvasti uusia turvattomuuden muotoja. Vaikka poliittiset toimijat pyrkivät lieventämään turvallisuusuhkia uusilla strategioilla ja sääntelyillä, täydellistä turvallisuutta ei voida saavuttaa. Yhteiskunta käyttää riskien käsitettä keinona hallita systemaattisesti epävarmuuksia ja turvallisuusriskejä. Riskien hallinnan pyrkimykset voivat paradoksaalisesti lisätä turvattomuutta, kun moderni yhteiskunta synnyttää jatkuvasti uusia riskejä ja tiedon puutteet vaikeuttavat niiden hallintaa. Sotilaallisen turvallisuuden alalla riskit ovat keskeisiä

konfliktien hallinnassa, mikä korostaa siirtymistä kohti globaaleja turvallisuusnäkökulmia, jotka eivät enää rajoitu alueellisiin tai kansallisiin ulottuvuuksiin. Riskiyttämisessä "tulevaisuuden läsnäolo" on erityisen tärkeä käsite: se tarkoittaa, että tulevaisuuden mahdolliset tapahtumat alkavat ohjata politiikkaa, kun perinteinen syy-seuraus-ajattelu ei enää päde monimutkaisten riskien keskellä. (Estève 2021, 605.)

Riskiyttäminen tuo uudenlaisen ulottuvuuden turvallisuustutkimukseen, jossa uhat nähdään laajemmin monimutkaisina ja ennakoimattomina riskeinä. Sen sijaan, että keskityttäisiin vain välittömien uhkien torjumiseen, riskiyttämisessä korostetaan ennakointia ja varautumista tulevaisuuden epävarmuuksiin. Tämä lähestymistapa painottaa riskien hallintaa pitkällä aikavälillä, eikä pelkästään välittömiä toimenpiteitä. Riskiyttäminen ajatuksena on hyödyllinen, kun tarkastellaan nykyaikaisia turvallisuusuhkia, kuten kyberturvallisuutta, jossa uhat eivät ole suoraan näkyviä tai välittömiä, mutta voivat silti aiheuttaa merkittäviä ongelmia. Kyberuhat vaativat jatkuvaa riskien arviointia ja ennakoivia toimia, koska ne muuttuvat jatkuvasti ja niiden vaikutukset voivat olla laajoja.

Kööpenhaminan koulukunnan turvallistamisteoria ja riskiyttämisen käsite toimivat tutkimuksen perustana kyberuhkien ja -riskien käsittelyn tarkastelussa. Niiden avulla selvitän, miten kansallisissa riskiarvioissa ja kyberturvallisuusstrategioissa rakennetaan uhkia ja riskejä turvallisuuskysymyksiksi sekä miten näiden prosessien kautta muokataan Suomen turvallisuuspoliittista toimintaympäristöä. Tämän teoreettisen viitekehyksen kautta tarkastelen erityisesti sitä, miten turvallistaminen ja riskiyttäminen vaikuttavat poliittisiin valintoihin ja päätöksentekoon.

4 Aineiston esittely

4.1 Tutkielman aineisto

Tutkielman aineisto koostuu Suomen kansallisista riskiarvioista ja kyberturvallisuusstrategioista, joissa käsitellään kyberuhkia ja -riskejä osana kansallista turvallisuutta. Näissä dokumenteissa tuodaan esille, millaisia kybertoimintaympäristöön liittyviä haasteita pidetään merkityksellisinä ja miten niitä tulisi hallita. Tarkastelen aineistoa turvallistamisen ja riskiyttämisen näkökulmista, jotta voidaan ymmärtää, miten kyberuhat ja -riskit rakentuvat osaksi kansallista turvallisuuspolitiikkaa.

Ennen ensimmäistä kansallista kyberturvallisuusstrategiaa (2013) kyberuhkia ja -riskejä käsiteltiin pääasiassa tietoturvan näkökulmasta. Keskeinen dokumentti tässä kehityksessä oli vuoden 2008 kansallinen tietoturvastrategia, joka laadittiin osana Suomen tietoyhteiskuntapolitiikkaa. Strategian tavoitteena oli luoda turvallinen arki digitaalisessa ympäristössä varmistamalla luottamus sähköisiin palveluihin ja tietoverkkoihin. Se painotti tietoturvaosaamisen merkitystä ja korosti yhteiskunnan eri toimijoiden yhteistyötä uhkien hallinnassa. (Liikenne- ja viestintäministeriö 2009, 1.)

Tietoturvastrategiassa tunnistettiin yhteiskunnan kasvava riippuvuus tietoverkoista ja tietojärjestelmistä, minkä vuoksi haavoittuvuudet verkkorikollisuudelle ja kyberuhille nähtiin kriittisinä riskeinä. Strategia myös linjasi, että tietoturva ei ole vain tekninen kysymys, vaan se liittyy laajemmin luottamukseen ja palveluiden käytettävyyteen. (Liikenne- ja viestintäministeriö 2009, 5.) Tämä dokumentti osoittaa, että ennen vuotta 2013 kyberturvallisuus ei ollut erillinen politiikan alue, vaan se nähtiin osana laajempaa tietoyhteiskuntakehitystä.

Kun vuoden 2009 tietoturvastrategiassa korostettiin tietoturvaa osana arjen palveluita ja yhteiskunnan digitaalista toimintavarmuutta, vuoden 2012 turvallisuus- ja puolustuspoliittinen selonteko nostaa kyberuhkat selvästi osaksi kansallista turvallisuutta. Selonteossa kyberhyökkäykset rinnastetaan perinteisiin uhkiin, kuten terrorismiin, mikä osoittaa, miten kybertoimintaympäristö on noussut laajemman turvallisuuspoliittisen tarkastelun kohteeksi. Lisäksi selonteossa painotetaan ennakoivaa hallintaa ja kansainvälistä yhteistyötä, mikä korostaa kyberuhkien hallinnan ennakoivaa lähestymistapaa. (Valtioneuvosto 2012, 21–22.)

Selonteko toimi myös tärkeänä pohjana alkuvuonna 2013 valmistuneelle kansalliselle kyberturvallisuusstrategialle, jossa painotettiin kyberuhkien ennakoivaa hallintaa ja Suomen kykyä suojautua niiltä. Tämä kehys heijastuu myös kansallisissa riskiarvioissa, jotka ovat keskeinen osa Suomen kokonaisvaltaista turvallisuuspolitiikkaa ja joissa kyberriskien erittelyä pidetään yhä tärkeämpänä osana kansallista varautumista. Kyberriskien käsittely näissä arvioissa tarjoaa konkreettisen kuvan siitä, miten valtion tasolla pyritään ennakoimaan ja hallitsemaan kyberuhkia, ja miten tämä kehys on muotoutunut kyberturvallisuusstrategian ja muiden turvallisuuspoliittisten asiakirjojen vaikutuksesta.

Kansalliset riskiarviot ovat keskeisiä analyysin kannalta, koska ne tarjoavat kokonaisvaltaisen kuvan niistä uhkista ja riskeistä, joita Suomi pitää merkityksellisenä osana kansallista turvallisuutta. Näissä asiakirjoissa kyberturvallisuus on tunnistettu yhdeksi keskeiseksi teemaksi, mikä mahdollistaa sen tarkastelun turvallistamisen ja riskiyttämisen näkökulmista. Alun perin riskiarviot on laadittu osana Euroopan unionin pelastuspalvelumekanismin vaatimuksia. Euroopan parlamentin ja neuvoston päätöksen mukaan jokaisen EU-maan tulee kehittää riskiarvioita kansallisella tai paikallisella tasolla ja toimittaa niiden keskeiset osat komissiolle säännöllisin väliajoin. Suomessa kansallisten riskiarvioiden laatimisesta vastaa sisäministeriö, mutta niiden valmistelu on toteutettu poikkihallinnollisesti varautumisen laaja-alaisuuden vuoksi. Riskiarvioiden kautta on mahdollista tarkastella, miten kybertoimintaympäristön uhkia käsitellään osana ennakoivaa hallintaa ja kansallista varautumista.

Kolmen riskiarvion lisäksi hyödynnän aineistossa kahta Suomen kyberturvallisuusstrategiaa, jotka on julkaistu vuosina 2013 ja 2019. Strategiat on laatinut poikkihallinnollinen työryhmä, ja niiden valmistelu käynnistettiin tasavallan presidentin ja valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan päätöksellä vuonna 2011. Tavoitteena on ollut luoda yhtenäinen käsitys kyberturvallisuuden merkityksestä sekä linjata konkreettisia toimenpiteitä kybertoimintaympäristön hallintaan. Ne keskittyvät sekä haitallisten vaikutusten ennaltaehkäisyyn että elintärkeiden toimintojen suojaamiseen kybertoimintaympäristössä.

Aineiston dokumentit kattavat vuosikymmenen ajanjakson, 2013–2023, mikä mahdollistaa kyberuhkien ja -riskien kehityksen sekä Suomen niihin vastaamisen tarkastelun pitkällä aikavälillä. Tämän ajallisen ulottuvuuden kautta voidaan tarkastella, millä tavoin

turvallisuuspoliittiset asiakirjat määrittelevät kybertoimintaympäristön ilmiöt ja minkälaisia turvallisuuskysymyksiä niiden yhteyteen liitetään.

Dokumenttien tarkastelu Kööpenhaminan koulukunnan turvallistamisteorian ja riskiyttämisen käsitteen kautta mahdollistaa sen analysoinnin, miten kyberuhkia ja -riskejä kehystetään kansallisina turvallisuuskysymyksinä. Kansalliset riskiarviot ja kyberturvallisuusstrategiat eivät ainoastaan kuvaa kybertoimintaympäristöön liittyviä uhkia ja riskejä, vaan myös ohjaavat niiden hallintaa ja resurssien kohdentamista. Tässä tutkimuksessa tarkastelen, miten näissä asiakirjoissa rakennetaan turvallisuuteen liittyvää narratiivia, ja millaisia seurauksia turvallistamisella ja riskiyttämisellä on Suomen turvallisuuspolitiikassa. Seuraavaksi esittelen yksityiskohtaisemmin aineiston dokumentit ja niiden keskeiset sisällöt.

4.1.1 Suomen kansallinen riskiarvio vuodelta 2015

Suomen kansallinen riskiarvio 2015 on kattava tarkastelu Suomen turvallisuusympäristön tilasta ja sen haavoittuvuuksista. Arvio on laadittu monipuolisesti huomioiden erilaisia uhkia ja riskejä sekä kansallisen turvallisuuden parantamiseksi. Siinä tarkastellaan laajasti eri turvallisuusnäkökulmia, kuten sotilaallisia, poliittisia, taloudellisia ja ympäristöllisiä tekijöitä (Sisäministeriö 2016, 12).

Riskiarvio jakautuu useisiin skenaarioihin, joissa käsitellään erilaisia uhkia, riskejä ja haasteita. Tässä tutkimuksessa keskityn erityisesti kybertoimintaympäristöön ja sen keskeisiin tekijöihin, vaikka saatan sivuta myös muita riskiarvion skenaarioita, koska kyberturvallisuus saattaa olla kytköksissä myös niihin jossain määrin.

Kybertoimintaympäristöä käsittelevässä skenaariossa tarkastellaan erityisesti kyberrikollisuutta, informaatiovaikuttamista ja kyberhyökkäyksiä sekä niiden mahdollisia vaikutuksia. Riskiarvio painottaa kyberuhkia ennen kaikkea teknisinä ja taloudellisina haasteina, jotka voivat vaikuttaa yhteiskunnan toimintavarmuuteen ja taloudelliseen vakauteen. Erityisesti kriittisen infrastruktuurin suojaaminen nousee esiin keskeisenä tavoitteena, mutta sitä käsitellään pääasiassa teknisen varautumisen ja riskienhallinnan näkökulmasta. Resilienssi ei nouse tässä dokumentissa keskeiseksi teemaksi, vaan kyberturvallisuutta lähestytään ennen kaikkea suojautumisen ja torjunnan kautta.

4.1.2 Suomen kansallinen riskiarvio vuodelta 2018

Suomen kansallinen riskiarvio vuodelta 2018 tarjoaa päivitetyn katsauksen maan turvallisuusympäristöön ja siihen liittyviin riskeihin. Tämä riskiarvio antaa päivitetyn version Suomen kyberturvallisuuden tilasta verrattuna vuoden 2015 riskiarvioon. Riskiarvion tarkoituksena on tunnistaa keskeiset uhat ja riskit, joita Suomi saattaa kohdata tulevaisuudessa, ja tarjota suuntaviivoja niiden hallintaan. (Sisäministeriö 2019, 9-11.)

Riskiarviossa tarkastellaan laajasti turvallisuuden eri ulottuvuuksia, mukaan lukien kyberuhkia, digitaalista turvallisuutta sekä perinteisiä turvallisuusuhkia ja yhteiskunnan kriisivalmiutta. Arvio sisältää myös laajempia kansainvälisiä ja alueellisia turvallisuuskysymyksiä, jotka voivat vaikuttaa Suomen turvallisuustilanteeseen.

Kyberuhat saavat tässä riskiarviossa aiempaa enemmän huomiota. Kyberuhkia ei käsitellä enää pelkästään teknisinä tai taloudellisina haasteina, vaan osana laajempaa turvallisuusympäristöä, jossa informaatiovaikuttaminen ja hybridivaikuttaminen ovat merkittävässä roolissa. Riskiarviossa nostetaan esiin myös yhteiskunnan kasvava riippuvuus digitaalisista järjestelmistä ja tietoverkoista, mikä lisää kyberuhkien merkittävyyttä. Kyberuhkat ja hybridivaikuttaminen ovat yhä enemmän yhteenkietoutuneita, mikä tekee uhkien torjumisesta monimutkaisempaa. (Sisäministeriö 2019, 14-16.) Resilienssin merkitys on kasvanut vuoden 2015 riskiarvioon verrattuna. Riskiarviossa korostetaan tarvetta vahvistaa kyberturvallisuuden hallintaa sekä lisätä yhteiskunnan ja kriittisten järjestelmien kestokykyä kyberuhkia vastaan. (Sisäministeriö 2019, 9.)

4.1.3 Suomen kansallinen riskiarvio vuodelta 2023

Suomen kansallinen riskiarvio vuodelta 2023 tarjoaa jälleen päivitetyn katsauksen maan turvallisuustilanteeseen ja tunnistettuihin riskeihin. Se perustuu aiempien vuosien riskiarvioihin, mutta sisältää päivityksiä, jotka huomioivat muuttuneen kansainvälisen toimintaympäristön sekä kehittyneet uhkamallit. Riskiarviossa tarkastellaan monipuolisesti turvallisuuden eri ulottuvuuksia, mukaan lukien hybridivaikuttaminen, kyberuhkat ja yhteiskunnan kriisinsietokyky. (Sisäministeriö 2023, 9–11.)

Tässä riskiarviossa on havaittavissa, kuinka kyberturvallisuuden merkitys on entisestään kasvanut osana kansallista turvallisuusstrategiaa. Kyberuhat eivät ole enää ainoastaan teknisiä tai taloudellisia riskejä, vaan ne kytkeytyvät laajasti myös hybridivaikuttamiseen,

informaatiosodankäyntiin ja yhteiskunnalliseen vakauteen. Vuoden 2023 riskiarviossa tieto- ja viestintäverkkojen ja palveluiden häiriöt tunnistetaan omaksi uhkamallikseen (Sisäministeriö 2023, 59–60). Kyberuhkat liittyvät myös laajemmin hybridivaikuttamiseen, informaatiovaikuttamiseen ja digitalisoituneen yhteiskunnan haavoittuvuuksiin (Sisäministeriö 2023, 23–25, 31). Tämä osoittaa, että kyberuhkia ei tarkastella vain erillisinä teknisinä riskeinä, vaan osana kansallisen turvallisuuden kokonaisuutta. Dokumentissa todetaan, että kyberuhkat voivat vaikuttaa yhteiskunnan elintärkeisiin toimintoihin, kuten infrastruktuuriin, puolustukseen ja talouteen.

Vuoden 2023 riskiarvio nostaa esiin myös resilienssin keskeisen roolin kyberturvallisuuden hallinnassa. Resilienssi nähdään nyt tärkeänä osana varautumisstrategiaa, ja raportissa korostetaan sekä ennaltaehkäisyä että kykyä sopeutua ja palautua kyberuhista ja häiriötilanteista. Kyberturvallisuuteen liittyvät riskit kytketään yhä vahvemmin yhteiskunnan elintärkeisiin toimintoihin, kuten talouteen, infrastruktuuriin, huoltovarmuuteen ja puolustuskykyyn. Lisäksi kansainvälisen yhteistyön merkitys kyberuhkien torjumisessa ja hallinnassa on riskiarviossa aiempaa korostetumpi. (Sisäministeriö 2023, 23-24.)

4.1.4 Suomen kyberturvallisuusstrategia vuodelta 2013

Vuoden 2013 kyberturvallisuusstrategia korostaa kansallisen kyberturvallisuuden merkitystä ja esittelee keskeiset strategiset linjaukset sen vahvistamiseksi. Se tuo esiin Suomen riippuvuuden tietoverkoista ja järjestelmistä sekä niihin kohdistuvat uhat, mukaan lukien valtiolliset toimijat ja kyberrikolliset. Strategiassa määritellään myös kyberturvallisuuden visio ja toimintamalli, joissa korostetaan yhteistyötä eri toimijoiden välillä sekä kansainvälisen yhteistyön merkitystä. Lisäksi strategiassa nostetaan esiin kansallisen kyberresilienssin kehittäminen ja kyberuhkien torjunnan vahvistaminen. Strategiassa painotetaan erityisesti kokonaisturvallisuuden periaatetta, jossa kyberturvallisuus nähdään osana laajempaa yhteiskunnallista varautumista. (Turvallisuuskomitea 2013, 1-6.)

Tarkastelen strategiassa erityisesti sen määrittelemiä kyberuhkia ja riskejä sekä niiden hallintaan liittyviä toimenpiteitä. Lisäksi analysoin strategian vaikutusta Suomen kyberturvallisuuden kehitykseen. Tämä strategia on keskeinen, koska se on Suomen ensimmäinen kyberturvallisuusstrategia ja toimii pohjana myöhemmille kehityssuunnille. Se ohjaa digitaalisen ympäristön toimijoita ennaltaehkäisemään uhkia ja lisäämään luottamusta kyberturvallisuuden ylläpitämisessä. Strategia toimii lähtökohtana myös kansalliselle

päätöksenteolle ja ohjaa lainsäädännön sekä viranomaisten toimintamallien kehittämistä kyberuhkien torjunnassa.

4.1.5 Suomen kyberturvallisuusstrategia vuodelta 2019

Vuoden 2019 kyberturvallisuusstrategia rakentuu vuoden 2013 strategian pohjalle, mutta se on päivitetty vastaamaan toimintaympäristön muutoksia ja kansallisen toiminnan kehittämistarpeita. Strategia on erityisesti päivitetty huomioimaan uudet uhkakuvat ja kehittyneet riskit, joita digitalisoituminen sekä muut globaaliin turvallisuustilanteeseen liittyvät muutokset ovat tuoneet mukanaan. (Turvallisuuskomitea 2019, 4.)

Strategiassa määritellään kolme keskeistä strategista linjausta: 1) kansainvälisen yhteistyön kehittäminen, 2) kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä 3) kyberturvallisuuden osaamisen kehittäminen. Kansainvälisellä tasolla painotetaan yhteistyötä EU:n ja muiden toimijoiden kanssa, kun taas kansallisesti strategia korostaa kyberturvallisuusjohtajan roolia, tilannekuvan kehittämistä ja elinkeinoelämän osallistamista varautumiseen. Lisäksi strategiassa käynnistetään kansallinen kehittämisohjelma, jonka tavoitteena on vahvistaa kyberuhkien torjuntaa ja resilienssiä. (Turvallisuuskomitea 2019, 5–8.)

Strategia tuo uusia painotuksia vuoden 2013 linjauksiin, erityisesti kansainvälisen yhteistyön, varautumisen ja kyberosaamisen kehittämisen osalta. Se laajentaa aiempaa lähestymistapaa korostamalla entistä enemmän elinkeinoelämän roolia kyberturvallisuuden edistämisessä sekä kyberuhkien ennakoivaa hallintaa. Tarkastelen, miten nämä linjaukset vaikuttavat Suomen kyberturvallisuuspolitiikkaan ja millaisia keinoja strategiassa esitetään kyberuhkien ja riskien hallintaan sekä niiden vaikutusten lieventämiseen.

Edellä esitellyt viisi dokumenttia tarjoavat kokonaiskuvan siitä, miten kyberuhkia ja riskejä on käsitelty Suomen kansallisissa riskiarvioissa ja kyberturvallisuusstrategioissa eri aikoina. Seuraavaksi tarkastelen ensin kyberuhkia ja niiden käsittelyä dokumenteissa, minkä jälkeen siirryn kyberriskien analyysiin. Lopuksi vertailen eri dokumenttien lähestymistapoja ja niiden vaikutuksia Suomen kyberturvallisuuspolitiikkaan. Tässä analyysissä sovellan turvallistamisen ja riskiyttämisen käsitteitä, joiden avulla tarkastelen, miten tietyt kyberuhat ja -riskit määritellään osaksi kansallista turvallisuutta ja miten niiden hallintaa perustellaan.

5 Kyberturvallisuuden uhkat ja reagoiva hallinta

Molemmissa kyberturvallisuusstrategioissa ja kolmessa riskiarviossa nostetaan esille keskeisiä teemoja, jotka liittyvät kyberturvallisuusuhkiin. Vaikka dokumenteissa on useita samankaltaisia teemoja, niiden välillä on myös merkittäviä eroavaisuuksia. Tässä luvussa tarkastelen, miten keskeisiä kyberturvallisuusuhkia on kuvattu ja millaisista uhkista muodostuu turvallisuusongelmia näissä dokumenteissa. Aloitan käsittelemällä niitä kyberuhkia, jotka nousevat esiin useissa dokumenteissa ja joita pidetään keskeisinä uhkakuvina.

Suomen kyberturvallisuusstrategian (2013) mukaan kyberuhka määritellään mahdollisuutena sellaiseen kybertoimintaympäristöön kohdistuvaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan. (Turvallisuuskomitea 2013, 13.)

Turvallistamisen näkökulmasta kyberuhat on kehystetty poliittisissa dokumenteissa eksistentiaalisina turvallisuusuhkina, jotka oikeuttavat poikkeuksellisia vastatoimia. Buzanin ym. (1998, 21–22) mukaan turvallistaminen tapahtuu, kun poliittinen toimija esittää tietyn ilmiön niin vakavana uhkana, että sen torjuminen vaatii välittömiä toimenpiteitä. Tämä prosessi on selvästi nähtävissä Suomen kyberturvallisuusstrategioissa, joissa uhkia ei kuvata vain teknisinä haasteina, vaan myös laajemmin yhteiskunnallista vakautta uhkaavina tekijöinä.

5.1 Kyberympäristön teknologiset ja infrastruktuuriset uhkat

Jokaisessa näistä dokumenteista kriittiseen infrastruktuuriin kohdistuvat kyberhyökkäykset ja sen haavoittuvuudet mainitaan keskeisinä turvallisuusuhkina. Kriittinen infrastruktuuri määritellään Suomen kyberturvallisuusstrategiassa seuraavasti: *"Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja."* (Turvallisuuskomitea 2013, 12.) Tämä määritelmä osoittaa, että kriittinen infrastruktuuri ei koostu vain fyysisistä rakenteista, vaan myös digitaalisista järjestelmistä, jotka ovat yhtä haavoittuvaisia kyberuhkille.

Hyökkäysten tavoitteena voi olla tiedon muuttaminen, varastaminen tai tuhoaminen, mikä voi heikentää kansallista turvallisuutta. Esimerkkejä tästä ovat valtiollisiin tietojärjestelmiin kohdistuva vakoilu tai sabotaasi sekä yritysmaailmaan kohdistuvat uhkat, kuten yritysvakoilu, petokset tai vahingonteot (Sisäministeriö 2016, 21). Kybertoimintaympäristön laajeneminen ja yhteiskunnan digitalisoituminen ovat lisänneet tällaisia uhkia. Backmanin (2022, 85) mukaan kyberturvallisuus on noussut nopeasti yhdeksi valtioiden ja ylikansallisten järjestöjen suurimmista turvallisuuspoliittisista kysymyksistä. Jansson ym. (2018, 2) määrittelevät kybertoimintaympäristön muodostuvan tietoverkoista ja tietojärjestelmistä, joissa tieto siirtyy digitaalisesti käyttäjältä toiselle. Tämä infrastruktuuri on altis hyökkäyksille, sillä sen toiminta on yhä enemmän riippuvainen globaalisti verkottuneista järjestelmistä.

Digitalisoituminen on lisännyt tietoverkkovakoilun riskejä. Dokumenteissa nämä uhat turvallistetaan osaksi digitaalisen infrastruktuurin haavoittuvuuksia, sillä niiden kautta voidaan uhata yhteiskunnan toimivuutta. Rikolliset ja valtiolliset toimijat voivat hyödyntää laittomia keinoja saadakseen arkaluonteista tietoa, mikä voi vaikuttaa yritysten kilpailukykyyn ja kriittisen infrastruktuurin turvallisuuteen. Vuoden 2023 riskiarviossa todetaan, että *"Digitalisoitunut yhteiskunta lisää riskejä myös valtionhallintoon ja yritysmaailmaan kohdistuvalle tietoverkkovakoilulle, jota kohdistetaan vähäisessä määrin myös kriittiseen infrastruktuuriimme. Sekä rikollisryhmittymät että autoritääriset valtiot käyttävät oikeudetonta tiedonhankintaa yritysten aineettoman pääoman anastamiseen ja kilpailuedun luomiseen."* (Sisäministeriö 2023, 25). Tämä osoittaa, että tietoverkkovakoilu ei ole ainoastaan tekninen uhka, vaan sillä voi olla myös laajempia taloudellisia ja poliittisia vaikutuksia.

Limnéll ym. (2015, 13) huomauttavat, että kyberturvallisuutta käsitellään usein vain teknisenä kysymyksenä, vaikka se on ennen kaikkea strateginen ja poliittinen ilmiö. Tämä tukee ajatusta, että tietoverkkovakoilulla voi olla laajempia yhteiskunnallisia seurauksia, kuten tiedon manipulointia tai yritysten toiminnan vaarantamista.

Viime vuosina kyberhyökkäykset ovat myös nousseet osaksi sotilaallista toimintaa. Esimerkiksi Ukrainan sodassa Venäjä on käyttänyt sotilaallisen voiman ohella kyberhyökkäyksiä osana hybridioperaatioitaan, kohdistuen yhteiskunnan keskeisiin toimintoihin ja infrastruktuureihin. (Sisäministeriö 2023, 38.) Tämä osoittaa, että kriittisen infrastruktuurin haavoittuvuuksien hyväksikäyttö on tullut keskeiseksi osaksi nykyaikaista sodankäyntiä. Friis ja Reichborn-Kjennerud (2016, 27–28) tuovat esiin, että kyberturvallisuuden sotilaallistuminen on herättänyt

kysymyksiä siitä, missä määrin kyberuhkia tulisi turvallistaa eli käsitellä poikkeuksellisina uhkina, jotka oikeuttavat erityistoimenpiteitä. Dokumenteissa tällaiset kyberuhat turvallistetaan uhkina, jotka eivät uhkaa vain yksittäisiä toimijoita, vaan koko yhteiskunnan resilienssiä ja kansallista turvallisuutta.

Näiden haavoittuvuuksien ohella palvelunestohyökkäykset nousevat esiin yhtenä keskeisimmistä uhkamuodoista, ja ne mainitaan merkittävänä uhkana kolmessa viidestä tarkastelemastani dokumentista. Palvelunestohyökkäykset muodostavat merkittävän osan kyberrikollisuudesta. Niistä on tullut merkittävä uhka, joka kohdistuu laajasti eri tahoihin - valtioihin, yrityksiin ja yksityisiin kansalaisiin. Tietoverkkoympäristöstä on tullut rikollisille houkutteleva toimintakenttä taloudellisten ja terroristisen hyötyjen tavoittelussa. (Turvallisuuskomitea 2013, 27.)

Palvelunestohyökkäykset ovat erityinen muoto tietoverkkohyökkäyksistä, joissa pyritään estämään palvelujen normaali toiminta. Tällaiset hyökkäykset voivat lamaannuttaa kriittisiä palveluja, kuten terveydenhuoltoa tai viestintäjärjestelmiä, ja niitä käytetään myös laajemmissa kyberhyökkäyskampanjoissa. (Turvallisuuskomitea 2013, 27.) Palvelunestohyökkäykset voivat olla osa laajempia kyberoperaatioita, joilla pyritään vaikuttamaan valtion tai yhteiskunnan toimintaan. Ne ovat usein strategisesti suunniteltuja ja voivat liittyä pitkän aikavälin tavoitteisiin, joita valtiolliset tai ei-valtiolliset toimijat pyrkivät saavuttamaan. Palvelunestohyökkäykset voidaan toteuttaa samanaikaisesti muiden kyberoperaatioiden kanssa, mikä lisää niiden tehokkuutta. (Sisäministeriö 2015, 20.) Dokumenteissa palvelunestohyökkäykset turvallistetaan keskeisinä kyberturvallisuusuhkina, joiden tehokkuus perustuu niiden kykyyn häiritä kriittisiä yhteiskunnallisia toimintoja nopeasti ja laajasti.

Palvelunestohyökkäysten ohella tietomurrot ovat toinen merkittävä kyberuhka. Niiden tavoitteena on hankkia luvattomasti tietoa ja käyttää sitä vahingollisesti. Suomessa tietomurrot on esitetty konkreettisena esimerkkinä kyberoperaatioista, jotka voivat vaarantaa kansallisen turvallisuuden. Tämä korostaa niiden mahdollisia vaikutuksia yhteiskunnan vakauteen ja digitaaliseen infrastruktuuriin. Vuoden 2023 riskiarvio toteaa: *"Tietoverkkorikollisuus, kuten tietomurrot tai laajamittaiset yksityisyyden suojan loukkaukset uhkaavat väestön perusoikeuksia, ja valtiollisten toimijoiden oikeudeton toiminta verkossa tai tietojärjestelmissä luo uhkia kansalliselle turvallisuudelle. Lisäksi ne voivat aiheuttaa luottamuspulaa palveluiden*

käyttäjien parissa. Tämä voi johtaa yleisesti luottamuksen rapautumiseen yhteiskunnan palveluita ja viranomaistoimintaa kohtaan." (Sisäministeriö 2023, 25.)

Tämä osoittaa, että tietomurrot eivät ole pelkästään tekninen riski, vaan ne voivat vaikuttaa laajemmin kansalaisten luottamukseen sekä yhteiskunnallisiin instituutioihin. Friis ja Reichborn-Kjennerud (2016, 33) tuovat esiin, että tällaiset kyberuhkat on usein turvallistettu niin, että ne oikeuttavat poikkeuksellisia toimenpiteitä, kuten lisääntyvää valvontaa ja kansallisten puolustusmekanismien vahvistamista.

Tietomurrot eivät aina ole pelkästään yksittäisiä rikoksia, vaan ne voivat olla osa laajempaa poliittista strategiaa. Kyberrikollisuutta ja tietomurtoja voidaan käyttää painostuksen välineinä, jos perinteiset vaikutusyritykset eivät tuota haluttua tulosta. (Sisäministeriö 2015, 20.) Tietomurrot liittyvät yleensä suurempiin, järjestäytyneisiin kyberuhkiin, joita voivat toteuttaa valtiot, rikollisjärjestöt tai terroristiryhmät (Sisäministeriö 2018, 49). Tämä tuo esiin turvallistamisen ja riskiyttämisen eron: turvallistamisessa uhka esitetään välittömänä vaarana, kun taas riskiyttämisessä painopiste on todennäköisyyksissä ja ennakoivassa hallinnassa (Friis & Reichborn-Kjennerud 2016, 32–33).

Tietojärjestelmien haavoittuvuudet mainitaan Suomen kansallisissa riskiarvioissa sekä vuosilta 2018 että 2023. Digitalisaation kehittyessä ja järjestelmien keskittämisen myötä on syntynyt uusia riskejä, joissa yhden järjestelmän vika voi aiheuttaa laajoja häiriöitä useilla eri sektoreilla. (Sisäministeriö 2018, 18). Dacorogna ja Kratz (2022) huomauttavat, että kyberuhkien hallinta vaatii jatkuvaa sopeutumista, sillä teknologian kehittyessä myös hyökkäyskeinot muuttuvat.

Tietoteknisten järjestelmien haavoittuvuudet voivat vaarantaa useiden organisaatioiden toimivuuden sekä tietojen luottamuksellisuuden ja eheyden. Tämä on erityisen vakava uhka, kun on kyse kriittisistä tiedoista, kuten esimerkiksi henkilötiedoista tai taloustiedoista. Näiden vaarantuminen voi heikentää sekä organisaatioiden että niiden asiakkaiden luottamusta ja toimintakykyä. (Sisäministeriö 2018, 18). Haavoittuvuuksien vuoksi on tärkeää kehittää resilienssiä, jotta järjestelmät voivat palautua nopeasti häiriöistä. *"Ilman toimivia viestintäpalveluja ja -verkkoja monet elinkeinoelämän ja yhteiskunnan palvelut eivät ole joko käytettävissä tai niiden käyttö ainakin vaikeutuu merkittävästi. Myös monet kansalaisten*

arkipäiväiset palvelut ja rutiinit ovat riippuvaisia viestintäpalveluiden ja -verkkojen luotettavasta toiminnasta." (Sisäministeriö 2018, 48). Tämä korostaa, kuinka riippuvaisuus digitaalisista järjestelmistä tekee yhteiskunnasta haavoittuvan ja lisää tarvetta tehokkaille kyberturvallisuustoimenpiteille.

Vaikka tietoteknisten järjestelmien haavoittuvuudet voivat heikentää yksittäisten organisaatioiden toimintaa ja tietoturvaa, niiden vaikutukset ulottuvat laajemmalle kuin vain organisaatiotasolle. Haavoittuvuudet voivat vaikuttaa myös koko yhteiskuntaan ja sen kriittisiin toimintoihin, kuten esimerkiksi energia-, vesi- ja liikennejärjestelmien ylläpitämiseen. Yhteiskunnan normaalin toiminnan kannalta on tärkeää, että nämä järjestelmät toimivat ilman häiriöitä. (Sisäministeriö 2016, 18-20.)

Tietoverkkojen häiriöt mainitaan yhtenä keskeisenä kyberturvallisuuden haasteena Suomen kansallisissa riskiarvioissa vuosilta 2015 ja 2018. Rikolliset ja muut haitalliset toimijat voivat yrittää manipuloida kriittisiä ohjausjärjestelmiä, kuten liikenne- ja energiainfrastruktuuria, syöttämällä niihin vääriä tietoja. Tämä voi aiheuttaa sellaisia sellaisia vaaratilanteita, joilla on suoria vaikutuksia yhteiskunnan turvallisuuteen. Myös terroristit voivat käyttää tietoverkkoja esimerkiksi propagandan levittämiseen ja väkivallan lietsontaan. Tämä taas aiheuttaa sen, että viranomaisilta vaaditaan valvontaa ja turvatoimia näiden varalta. (Sisäministeriö 2016, 21-22.)

Pilvipalveluiden ja järjestelmien keskittäminen voi johtaa siihen, että yhden järjestelmän häiriö vaikuttaa useisiin muihin järjestelmiin. *"Pilvipalveluiden ja järjestelmien keskittämisen yleistyessä yksittäisten järjestelmähäiriöiden kerrannaisvaikutukset voivat olla merkittäviä vikojen ja häiriöiden ketjuuntumisen vuoksi."* (Sisäministeriö 2018, 18.) Tämä alleviivaa järjestelmien keskinäisriippuvuuden merkitystä: kyberhyökkäykset voivat vaikuttaa useisiin toimialoihin samanaikaisesti ja aiheuttaa laajoja yhteiskunnallisia seurauksia.

Suomi on tietoyhteiskuntana erityisen riippuvainen tietoverkkojen ja -järjestelmien toiminnasta, mikä tekee siitä haavoittuvan kyberuhille. Tämä on tunnistettu Suomen kyberturvallisuusstrategiassa jo vuonna 2013, jossa korostettiin keskinäisriippuvuuden mukanaan tuomia turvallisuusriskejä. (Turvallisuuskomitea 2013, 1.) Keskinäisriippuvuuden vuoksi Suomella ei ole täyttä kontrollia kaikista digitaalisista järjestelmistään, mikä tekee siitä alttiin ulkoisille vaikutusyrityksille. Vuoden 2023 riskiarviossa täsmennetään: *"EU:n sisällä*

rajat ylittävät digitaaliset palvelut ovat yleistyneet ja jäsenvaltioiden keskinäinen riippuvuus toistensa digitaalisesta infrastruktuurista on lisääntynyt. Yhdessä jäsenmaassa tapahtuvilla kyberhäiriöillä saattaa olla merkittäviä vaikutuksia muihin jäsenmaihin" (Sisäministeriö 2023, 25). Tämä korostaa, että kyberuhkien vaikutukset eivät rajoitu kansallisiin rajoihin, vaan voivat laajentua muihin valtioihin digitaalisten verkkojen kautta.

Keskinäisriippuvuutta on lisännyt myös yhä useampien laitteiden kytkeytyminen internettiin, mitä voidaan kutsua esineiden internetiksi. Yhä useampia toimintoja pystytään ohjaamaan digitaalisesti, ja tämä on johdosta sähköisten palveluiden häiriöt voivat aiheuttaa häiriöitä myös fyysisiin palveluihin. Esimerkiksi vedenjakelu voi olla erityisen herkkä tällaisille häiriöille. (Sisäministeriö 2018, 18.) Lisäksi digitaalisten järjestelmien sekä niiden tarjoajien ja käyttäjien välinen keskinäinen riippuvuus voi olla huomattavaa (Sisäministeriö 2023, 24).

Kyberturvallisuuteen liittyvissä häiriötilanteissa voi samaan aikaan ilmetä useita uhkia, mikä johtuu verkottuneen yhteiskunnan, eri toimintojen keskinäisriippuvuuksien sekä tahattomien ja tahallisten tekojen vaikutuksesta. Tällainen häiriötilanteiden ketjuuntuminen tarkoittaa, että yhden ongelman esiintyminen voi aiheuttaa laajasti vaikutuksia myös muissa toiminnoissa. Sen takia yksittäisellä häiriötilanteella voi olla laajempia seurauksia keskinäisriippuvaisessa toimintaympäristössä. Pitkään jatkuvat laajat häiriötilanteet voivat myös lisätä yhteiskunnan alttiutta uusille häiriöille. Riskienhallinnan kannalta on tärkeää tunnistaa nämä ketjuuntumiset ja keskinäisriippuvuudet, jotta niihin voidaan varautua paremmin. (Sisäministeriö 2023, 12.)

Kyberturvallisuus on noussut yhdeksi keskeisimmistä turvallisuuskysymyksistä, ja sitä käsittelevät dokumentit korostavat erityisesti kriittisen infrastruktuurin haavoittuvuutta sekä kyberuhkien monimuotoisuutta. Tietoverkkovakoilu, palvelunestohyökkäykset ja tietomurrot nähdään paitsi teknisinä haasteina, myös laajempina poliittisina ja taloudellisina uhkina, jotka voivat vaikuttaa yhteiskunnan vakauteen ja kansalliseen turvallisuuteen.

Dokumenteissa kyberuhkat turvallistetaan vakavina haasteina, mikä perustelee tarvetta laajoille suojautumistoimenpiteille. Keskinäisriippuvuuden kasvu lisää haavoittuvuutta: kyberhyökkäykset eivät enää vaikuta vain yksittäisiin järjestelmiin, vaan voivat heikentää kriittisiä yhteiskunnallisia toimintoja laajemminkin. Tämän vuoksi varautuminen ja ennakoiva riskienhallinta ovat olennaisia keinoja torjua kyberuhkia ja turvata yhteiskunnan keskeiset palvelut.

Tämä analyysi tukee Friisin ja Reichborn-Kjennerudin (2016, 33) ajatusta siitä, että kyberturvallisuus ei ole yksiselitteisesti turvallistettu tai riskiytetty ilmiö, vaan eri uhkatyyppejä käsitellään eri tavoin riippuen niiden luonteesta ja vaikutuksista. Esimerkiksi järjestelmien haavoittuvuudet on esitetty pitkän aikavälin riskinä, jota voidaan hallita varautumisella ja teknisin ratkaisuin, kun taas palvelunestohyökkäykset ja tietomurrot on turvallistettu välittöminä uhkina, jotka oikeuttavat aktiivisia vastatoimia.

5.2 Kyberympäristön strategiset ja geopoliittiset uhkat

Nykymaailmassa kyberturvallisuusuhkat eivät rajoitu vain teknisiin haasteisiin, vaan ne liittyvät yhä tiiviimmin myös strategisiin ja geopoliittisiin konteksteihin. Limnéll ym. (2015, 13) korostavat, että kyberturvallisuutta tarkastellaan usein pelkästään teknisenä kysymyksenä, vaikka se on ensisijaisesti strateginen ja poliittinen ilmiö. Tämä vahvistaa näkemystä, että valtiollisten toimijoiden kyberoperaatiot eivät ole pelkkiä teknisiä haasteita, vaan ne toimivat myös kansainvälisen politiikan välineinä. Yksi keskeinen strateginen ja geopoliittinen uhka kyberturvallisuudelle on valtiolliset toimijat ja niihin liittyvät kyberuhat. Nämä tekijät on turvallistettu uhkana Suomen kyberturvallisuusstrategiassa vuonna 2013 ja kaikissa tarkastelemissani riskiarvioissa.

Nykyisessä kybertoimintaympäristössä uhkien luonne on paljon muuttunut ja monipuolistunut, sillä uhkat eivät kosketa vain yksittäisiä ihmisiä tai yrityksiä. Kyberturvallisuusuhkia muodostavat toimijat ovat ammattimaisempia kuin ennen, ja heidän toimillaan on laajempia yhteiskunnallisia vaikutuksia. Vuoden 2015 riskiarviossa sanotaan: *”Suomen valtioon tai yhteiskuntaan kohdistuva, valtiollisen toimijan tai siihen verrattavan ryhmän, esim. terroristijärjestön tahallisesti aiheuttama kyberhyökkäys on usein osa laajempaa kriisiä tai konfliktia Euroopassa. Todennäköisesti kyse on tällöin valtiollisen tai muun toimijan laajemmasta operaatiosta, jonka taustalla on kuukausia jopa vuosia kestänyt suunnittelu ja kehityskulku.”* Valtiolliset toimijat ovat vahvasti osa tätä ilmiötä, sillä ne käyttävät kyberhyökkäyksiä usein poliittisen ja taloudellisen painostuksen välineinä. Kyberhyökkäykset ovat valtiollisille toimijoille yksi vaikuttamiskeino perinteisten sotilaallisten voimakeinojen lisäksi. (Turvallisuuskomitea 2013, 1.) Pahimmillaan valtiollinen kyberhyökkäys voi olla todella tuhoisa, sillä se voi kohdistua sekä kriittisen infrastruktuurin kohteisiin, että muihin elintärkeisiin toimintoihin (Sisäministeriö 2016, 21). Tällaiset uhkat on turvallistettu osaksi kansallisen turvallisuuspolitiikan keskiötä, jotta niiden vaikutuksiin voidaan varautua tehokkaasti. Kybertoimintaympäristö on myös muuttanut kansainvälisiä suhteita, koska se

tarjoaa esimerkiksi pienille valtioille mahdollisuuden vaikuttaa maailmanpolitiikkaan kyberhyökkäysten avulla. Sillä kybertoimintaympäristössä merkitsee enemmänkin tekninen osaaminen eikä valtion koko tai sotilaalliset resurssit. (Turvallisuuskomitea 2013, 17.) Tällainen kehitys on määritelty merkittäväksi uhkaksi erityisesti globaalien valtasuhteiden kannalta, joissa perinteiset resurssipohjaiset valta-asemat voivat heikentyä teknologisen osaamisen vuoksi.

Kyberhyökkäysten tunnistamisessa on ongelmakohtia sen suhteen, milloin ne tunnistetaan yksittäiseen toimijaan kohdistuvaksi rikollisuudeksi ja milloin taas valtiota vastaan kohdistuvaksi teoksi. Valtiolliset kyberuhkat ovat yleensä myös valtioiden rajat ylittäviä, mutta samaan aikaan kansallisilla viranomaisilla on toimivaltaa vain omien maidensa rajojen sisällä. (Sisäministeriö 2016, 21.) Näiden lisäksi kybertoimintaympäristössä sodan ja painostuksen rajat ovat vaikeasti tunnistettavia (Sisäministeriö 2016, 27). Turvallistaminen on tässä yhteydessä keskeistä, koska sen avulla määritellään, milloin kyberuhka tulkitaan kansalliseksi turvallisuuskysymykseksi ja milloin sen käsittely kuuluu muille tahoille.

Suomen valtioon tai yhteiskuntaan kohdistuva kyberhyökkäys, jonka tekee valtiollinen toimija tai vastaava ryhmä, kuten terroristijärjestö, on usein osa laajempaa kriisiä. Tällaiset konfliktit voivat vaikuttaa Euroopassa laajemmin ja sitä on saatettu suunnitella kuukausia tai jopa vuosia. Kyberhyökkäys voi mahdollisesti olla seuraus eri osapuolten välisistä erimielisyyksistä tai kulttuurisista vastakkainasetteluista, joilla on vaikutusta Suomeenkin. Suomen valtionjohtoon voidaan pyrkiä vaikuttamaan, jotta saadaan tiettyjä tavoitteita läpi. Tällaista voidaan tehdä erityisesti siinä tilanteessa, jos Suomi ei toimi hyökkääjän intressien mukaisesti. (Sisäministeriö 2016, 20.) Tällaiset tilanteet on turvallistettu osaksi Suomen ulko- ja turvallisuuspolitiikkaa, jotta ne voidaan ennakoida ja torjua tehokkaasti.

Toinen merkittävä uhka kybertoimintaympäristössä sen muutoksen ja monipuolistumisen myötä on hybridivaikuttamisen lisääntyminen. Sisäministeriön (2018, 16) mukaan hybridivaikuttaminen tarkoittaa erilaisten, toisiaan täydentävien keinojen käyttöä, joissa hyödynnetään kohteen heikkouksia tavoitteiden saavuttamiseksi. Tämä ilmiö on turvallistettu osaksi kansainvälistä hybridisodankäynnin uhkakeskustelua, mikä korostaa sen keskeistä roolia nykypäivän turvallisuusympäristössä. Vuoden 2023 riskiarviossa kuvaillaan hybridivaikuttamista näin: *”Hybridivaikuttaminen voi kohdistua kaikkiin yhteiskunnan elintärkeisiin toimintoihin. Vaikuttaminen voi kohdistua suorasti tai epäsuorasti esimerkiksi*

poliittiseen päätöksentekoon, yhteiskunnan tärkeiden palveluiden tai kriittisen infrastruktuurin toimivuuteen, väestön mielipiteisiin, viranomaisia kohtaan tunnettuun luottamukseen tai Suomen kantoihin kansainvälisillä foorumeilla." (Sisäministeriö 2023, 26.) Kyberhyökkäykset ovat keskeinen osa tätä vaikuttamista, ja toimintaympäristön muuttuessa sen seuraukset voivat olla entistä vakavampia, kuten yhteiskunnan vakauden horjuminen ja sisäisen turvallisuuden vaarantuminen (Sisäministeriö 2016, 18). Esimerkkejä tällaisista keinoista ovat taloudellinen painostus, kyberhyökkäykset ja informaatiovaikuttaminen. Tämä ilmiö on turvallistettu osaksi kansainvälistä hybridisodankäynnin uhkakeskustelua, mikä korostaa sen merkitystä nykyajan turvallisuudessa.

Informaatio-operaatiot, kuten tietoverkkojen häirintä ja psykologiset operaatiot, voidaan turvallistaa osaksi hybridivaikuttamista, koska ne yhdistävät sotilaallisia ja ei-sotilaallisia keinoja. Tämä tekee hybridivaikuttamisesta erityisen riskialtista. (Sisäministeriö 2016, 28.) Vaikka Suomea koskevat hybridiuhat ovat olleet vielä melko vähäisiä, on silti tärkeää huomioida informaatio-operaatioiden ja kyberoperaatioiden, kuten trollauksen, lisääntyminen. Turvallistamisen näkökulmasta tällaiset ilmiöt voivat uhata Suomen yhteiskunnan vakautta merkittävästi. (Sisäministeriö 2016, 29.)

Kyberturvallisuusympäristön muutokset ovat myös lyhentäneet uhkien ennakkovaroitusaikoja, mikä vaikeuttaa taas päätöksentekoa ja viranomaisten toimintavalmiutta. Hybridivaikuttamisen turvallistaminen kansalliseksi turvallisuuskysymykseksi onkin tärkeää, sillä se voi vaikuttaa poliittiseen päätöksentekoon ja yhteiskunnan sisäisiin asioihin yllättävillä tavoilla (Sisäministeriö 2018, 14-16). Näiden muutosten vuoksi hybridivaikuttaminen muodostaa merkittävän uhan kyberturvallisuudelle, sillä se voi aiheuttaa häiriöitä keskeisissä palveluissa ja heikentää kansalaisten luottamusta viranomaisiin (Turvallisuuskomitea 2019, 4).

Hybridivaikuttamisen ohella disinformaatio ja informaatiovaikuttaminen ovat nousseet keskeisiksi haasteiksi osana nykypäivän kyberturvallisuutta. Turvallistaminen näiden ilmiöiden osalta on välttämätöntä, sillä niiden vaikutukset voivat ulottua yhteiskunnallisen vakauden heikentämiseen. Informaatioteknologioiden käytön yleistyminen on tehnyt vaikuttavia muutoksia yhteiskuntaamme. Näiden informaatioteknologioiden käyttö on tuonut monia hyviä asioita yhteiskuntaan, sillä ne ovat muun muassa lisänneet avoimuutta ja mahdollistaneet aktiivisen osallistumisen yhteiskunnalliseen keskusteluun. Niiden käyttö ei kuitenkaan ole tuonut pelkästään hyviä asioita, vaan ne ovat tuoneet esille myös uudenlaisia uhkia. Näitä uhkia

ovat muun muassa vihamielinen informaatiovaikuttaminen, vaalihäirintä, disinformaation levittäminen, vihapuhe ja verkossa tapahtuva häirintä. (Sisäministeriö 2023, 31.)

Vuoden 2018 riskiarviossa todetaan, että *"Informaatiovaikuttamisen yleistyminen on paljolti seurausta tiedonvälityksen muutoksesta ja nopeudesta, sosiaalisen median synnystä sekä informaatiokanavien moninaistumisesta. Uudessa globaalissa viestintäympäristössä voi tavoittaa reaaliajassa suurempia ihmismassoja kuin koskaan aikaisemmin ja vaikuttaa yleiseen mielipiteeseen. Toinen syy informaatiovaikuttamisen yleistymiseen on se, että on olemassa valtioita, jotka hyödyntävät uusia teknologian keinoja ja tekevät systemaattisia informaatio-operaatioita tavoitteenaan kohteen heikentäminen."* (Sisäministeriö 2018, 23.)

Kyberympäristö ja sosiaalinen media muodostavat sellaisen alustan, jonka kautta voidaan pyrkiä vaikuttamaan jonkun tietyn maan sisäisiin asioihin, kuten yhteiskunnan vakauteen tai kansalaisten mielipiteisiin. Trollauksen ja disinformaation levittämisen avulla voidaan pyrkiä jakamaan kansalaisten mielipiteitä, aiheuttaa erimielisyyksiä ja vähentää luottamusta viranomaisiin. (Sisäministeriö 2018, 16.) Näiden ilmiöiden turvallistaminen kyberturvallisuuden uhkiksi on tarpeen, jotta niiden vaikutuksia voidaan ymmärtää ja torjua tehokkaasti. Esimerkiksi koronaviruspandemian aikana Suomessa nähtiin koronavirukseen ja rokotteisiin liittyvää disinformaatiota sekä viranomaisten, tutkijoiden, toimittajien ja päättäjien häirintää ja uhkailua. Tällaista toimintaa tehtiin niin sosiaalisessa mediassa kuin sen ulkopuolellakin. Tällaisten disinformaatiokampanjoiden tarkoituksena oli vääristellä tietoja hallituksen päätöksistä ja kansalaisten oloista sekä hyväksikäyttää yhteiskunnallista tyytymättömyyttä. Muita Suomeen kohdistuneita disinformaatiovaikuttamisen keinoja on ollut Suomen historiaa koskevien faktojen ja tapahtumien vääristely sekä erinäisten tietojen käyttäminen tarkoituksenhakoisesti irrottamalla ne kontekstista. (Sisäministeriö 2023, 32-33.)

Informaatiovaikuttaminen ei rajoitu pelkästään digitaalisiin ympäristöihin, se voidaan turvallistaa uhkatekijäksi, joka vaikuttaa myös fyysisen ympäristön tapahtumiin. Esimerkiksi palvelunestohyökkäysten, tietomurtojen ja kriittiseen infrastruktuuriin kohdistuvalla häirinnällä voidaan vaikuttaa sekä fyysiseen ympäristöön että informaatioympäristöön. Tällaisilla kyberhyökkäyksillä pyritään vaikuttamaan yhteiskunnan elintärkeisiin toimintoihin ja toimintakykyyn. (Sisäministeriö 2023, 31.) Ne eivät vaikuta vain tietoverkkoihin, vaan niillä voi olla merkittäviä seurauksia myös ihmisten ja kriittisten palveluiden toimintaan. Turvallistamisen kautta informaatio- ja kyberuhkien keskeinen merkitys

hybridivaikuttamisessa korostuu, sillä niissä yhdistetään fyysisiä ja digitaaliseen ympäristöön kohdistuvia vaikuttamisen keinoja tavoitteen saavuttamiseksi. (Sisäministeriö 2018, 49.)

Samalla kun informaatiovaikuttaminen ja disinformaatio haastavat yhteiskuntien vakauden, teknologian nopea kehitys tuo mukanaan monia muita kyberturvallisuusuhkia. Vuoden 2013 kyberturvallisuusstrategiassa sanotaan: ”*Tietotekniikan levittäytyminen yhä laajemmin teollisuustuotanto- ja ohjausjärjestelmiin on luonut uusia haavoittuvuuksia ja mahdollisia hyökkäyskohteita kybertoimintaympäristössä.”* (Turvallisuuskomitea 2013, 18.) Teknologinen kehitys on muokannut yhteiskuntia ja niiden valtarakenteita merkittävällä tavalla. Turvallistaminen teknologian kehityksen luomien haavoittuvuuksien osalta on keskeistä, sillä tieto- ja viestintäteknologia sekä niihin liittyvät palvelut ovat muuttaneet niin yksilöiden arkea kuin globaalien instituutioiden toimintaa. Teknologian kehitys on helpottanut elämäämme erilaisten innovaatioiden kautta, jotka ovat parantaneet tehokkuutta, turvallisuutta ja ekologisuutta. Esimerkiksi tekoäly, robotiikka, esineiden internet ja liikenteen älykäs automaatio ovat sellaisia innovaatioita, joilla on ollut merkittävä vaikutus yhteiskunnankin kehityksen kannalta. Samalla yhteiskunnat ovat tulleet entistä riippuvaisemmiksi viestintäpalveluiden ja -verkkojen toimivuudesta, ja mahdolliset häiriöt näissä järjestelmissä voivat aiheuttaa vakavia häiriöitä keskeisiin toimintoihin. (Sisäministeriö 2018, 17.)

Teknologian kehityksen mukana on tullut paljon hyviä asioita, mutta samalla se on lisännyt haavoittuvuuksia. Kehitys on kytkenyt keskeisiä järjestelmiä, kuten energiaverkkoja ja terveydenhuoltoa, internetiin, mikä lisää niiden alttiutta kyberhyökkäyksille. (Sisäministeriö 2018, 17.) Uudet teknologiat ovat lisänneet järjestelmien kompleksisuutta, mikä voi taas vaikeuttaa niiden suojaamista. Dokumenteissa kyberhyökkäysten monipuolistuminen ja tehokkuus on tunnistettu merkittäväksi uhkatekijäksi, sillä ne voivat vahingoittaa laajoja kohteita kerralla. (Sisäministeriö 2023, 25.) Teknologian kehitys asettaa haasteita kyberturvallisuudelle sen puolesta, että turvatoimet sitä vastaan eivät aina ehdi kehittyä samassa tahdissa (Turvallisuuskomitea 2019, 4). Tämän takia kansallisen ja kansainvälisen yhteistyön merkitys korostuu entistä enemmän kyberuhkien torjunnassa (Sisäministeriö 2023, 25).

Voidaan nähdä, että kyberturvallisuusuhkien kenttä on laajentunut merkittävästi viime vuosina, ja nykyään ne ulottuvat teknisten ongelmien lisäksi myös strategisiin ja geopoliittisiin kysymyksiin. Valtiolliset toimijat ovat keskeisiä tekijöitä kyberuhkien maailmassa, ja ne käyttävät kyberhyökkäyksiä saadakseen muun muassa poliittista ja taloudellista valtaa.

Turvallistamisen näkökulmasta hybridivaikuttaminen, disinformaatio ja informaatiovaikuttaminen ovat olennainen osa kyberturvallisuusuhkien määrittelyä, sillä ne voivat heikentää yhteiskunnan vakautta ja kansalaisten luottamusta viranomaisiin. Teknologian kehityksen kautta kyberhyökkäyksistä on tullut entistä monipuolisempia ja tehokkaampia, mikä tekee kyberturvallisuudesta yhä haasteellisempaa. Kyberuhkien monimuotoistuminen ja lisääntyminen edellyttää tiivistä yhteistyötä eri toimijoiden välillä yhteiskunnan resilienssin vahvistamiseksi. Kansallisen ja kansainvälisen varautumisen merkitys korostuu, kun teknologiset, geopoliittiset ja hybridivaikuttamiseen liittyvät uhkat limittyvät yhä tiiviimmin toisiinsa.

6 Kyberturvallisuuden riskit ja ennakoiva hallinta

Sekä kyberturvallisuusstrategioissa että riskiarvioissa tuodaan esille tiettyjä keskeisiä teemoja kyberriskeihin liittyen. Tässä luvussa tarkastelen piirteittäin, miten keskeisiä kyberturvallisuusriskejä on kuvattu ja millä tavalla ne näyttäytyvät turvallisuusongelmina näissä dokumenteissa. Tarkastelen jälleen ensimmäisenä niitä kyberturvallisuusriskejä, joita on eniten nostettu esille näissä dokumenteissa.

Suomen kyberturvallisuusstrategian (2013) mukaan kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta. Toteutuessaan tai hyödyntämällä tätä haavoittuvuutta voidaan aiheuttaa vahinkoa, haittaa tai häiriötä toiminnalle, joka on riippuvainen kybertoimintaympäristön toiminnasta. (Turvallisuuskomitea 2013, 12.)

6.1 Kyberympäristön teknologiset riippuvuudet, haavoittuvuudet ja infrastruktuurien riskit

Kaikissa viidessä näistä kyberturvallisuutta käsittelevistä dokumenteista tuodaan esille yhteiskunnan riippuvuus tietoverkoista esille yhtenä keskeisenä kyberriskinä. Tämä ilmiö on kasvanut merkittävästi viime vuosina, ja sen myötä aiheuttanut uusia haasteita kyberturvallisuudelle. Yhteiskunnan turvallisuuden varmistaminen kuuluu valtion tärkeimpiin tehtäviin, ja elintärkeiden toimintojen toimivuus on turvattava kaikissa olosuhteissa. Vuoden 2013 kyberturvallisuusstrategiassa todetaan, että *”Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille.”* (Turvallisuuskomitea 2013, 1.) Digitaalisiin palveluihin kohdistuva riippuvuus on turvallistettu korostamalla niiden toimintakyvyn turvaamisen tärkeyttä, mutta samalla riskiytetty, koska järjestelmien häiriöt voivat uhata yhteiskunnan keskeisiä toimintoja. Tämä riippuvuus tietoverkoista ja järjestelmistä luo merkittävän riskin, sillä häiriöt näissä kriittisissä järjestelmissä voivat heijastua laajasti koko yhteiskunnan toimintakykyyn. (Turvallisuuskomitea 2013, 1.)

Yhteiskunnan lisääntynyt tietointensiivisyys, ulkomaisen omistuksen kasvu sekä tietoliikennejärjestelmien keskinäinen integraatio luovat uusia vaatimuksia elintärkeiden toimintojen turvaamiselle normaalioloissa ja poikkeusoloissa (Turvallisuuskomitea 2013, 1).

Vuoden 2015 riskiarvion mukaan *”Esimerkiksi Suomessa tapahtuva maksuliikenne on täysin riippuvainen toimivista tietoliikenneyhteyksistä Eurooppaan.”* (Sisäministeriö 2016, 18.) Tämä antaa Euroopan muille maille mahdollisuuden vaikuttaa Suomen maksuliikenteeseen tämän keskinäisriippuvaisen järjestelmän kautta. Tämä muodostaa Suomelle merkittävän riskin, johon on jo hyvä varautua etukäteen. Tämän järjestelmän turvallistaminen edellyttää varautumista ulkoisiin häiriöihin, mutta samalla sen riskiyttäminen voi heijastua laajemmin kansainvälisiin suhteisiin.

Digitalisaation laajeneminen on tuonut uusia riskejä ja toiminnot, kuten maksuliikenne ja viestintäjärjestelmät, ovat kytkeytyneet vahvasti digitaalisiin palveluihin. Jos yksi järjestelmä kärsii häiriöstä, vaikutukset voivat näkyä myös muissa tärkeissä toiminnoissa. Tämä keskinäisriippuvuus tekee yhteiskunnan alttiiksi laajoille ja samanaikaisille häiriöille, jolloin kyberhyökkäykset voivat lamauttaa useita elintärkeitä palveluita, mikä vaarantaa näin yhteiskunnan toimintakyvyn. (Sisäministeriö 2018, 17-18.) Tämä keskinäisriippuvuus on turvallistettu, mikä tarkoittaa, että sen hallinta edellyttää vahvaa kyberturvallisuutta. Samalla se kuitenkin riskiyttää yhteiskunnan, sillä järjestelmien keskinäinen riippuvuus altistaa laajoille häiriöille.

Kun digitalisaatio lisääntyy ja järjestelmät ovat yhä enemmän riippuvaisia toisistaan, tietojärjestelmien suojauspuutteiden riskit kasvavat. Vuoden 2018 riskiarvion mukaan *”Yhteiskäyttöisten sähköisten alustojen vikaantuminen, häiriöt tai haavoittuvuudet saattavat vaikuttaa kerralla useiden eri organisaatioiden palvelujen käytettävyyteen, tietojen luottamuksellisuuteen tai eheyteen.”* (Sisäministeriö 2018, 18.) Tämä voi tuoda vakavia riskejä kybertuvallisuuteen. Kyberturvallisuuden hallinnan haasteita lisää se, että sitä voidaan tarkastella monista eri tieteenalojen näkökulmista, mikä on tehnyt sen määrittelystä monimutkaisempaa. Tämä saattaa vaikeuttaa eri asiantuntijatahojen välistä yhteistyötä ja vaikuttaa siihen, miten kyberuhkia ja -riskejä tunnistetaan ja arvioidaan. (Cains ym. 2022, 1643–1644.)

Tietojärjestelmien suojaamisen puutteet voivat luoda monenlaisia riskejä kyberturvallisuuteen liittyen. Kaikissa kolmessa riskiarviossa sekä molemmissa kyberturvallisuusstrategioissa nostetaan tietojärjestelmien suojaamisen puutteet yhdeksi keskeiseksi riskiksi kyberturvallisuudessa. Puutteiden käsittely strategioissa osoittaa, kuinka nämä riskit on riskiytetty osaksi kansallisen riskienhallinnan keskeisiä tavoitteita. Puutteet voivat vakavasti

heikentää sähkönjakelun, tietoliikenteen ja maksujärjestelmien toimintavarmuutta. Ne voivat vaikuttaa merkittävästi esimerkiksi elintarvikkeisiin ja ruokapalveluihin sekä lamaannuttaa tuotantolaitoksia ja kauppoja samanaikaisesti. Lyhyellä aikavälillä näistä häiriöistä ei koidu riskejä elintarvikehuollolle, mutta pidemmällä aikavälillä elintarvikehuolto voi pysähtyä hetkeksi kokonaan. Tämän vuoksi suojauspuutteiden riskit on turvallistettu merkittäväksi yhteiskunnalliseksi kysymykseksi, jonka ratkaiseminen vaatii jatkuvaa kehitystä. (Sisäministeriö 2023, 80.)

Vuoden 2015 riskiarviossa todetaan, että *”Globaali kybertoimintaympäristö muodostuu monimutkaisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansalaisten, viranomaisten ja yritysmaailman tietoverkkoja sekä kriittisen infrastruktuurin ohjaus- ja valvontajärjestelmiä.”* (Sisäministeriö 2016, 18.) Erityisesti tässä alleviivataan riskitekijänä sitä, että tekniset komponentit ja tietovarastot sijaitsevat usein kansainvälisillä palvelimilla, joiden kyberturvallisuus ei välttämättä vastaa Suomen kansallisiin tarpeisiin. Tämä kuvaa, miten kybertoimintaympäristön globaalit riippuvuudet ovat riskiytetty Suomen kansallisen turvallisuuden näkökulmasta. Monet suomalaiset IT-alan yritykset ja tekniset palvelut saattavat olla ulkomaisessa omistuksessa, mikä osaltaan lisää myös riskiä, etteivät nämä yritykset huomioi riittävästi Suomen kansallisia turvallisuustarpeita. (Sisäministeriö 2016, 18.) Riippuvuus kansainvälisistä tietoyhteyksistä vaikuttaa myös kriittisen infrastruktuurin toimivuuteen, sillä sen häiriöt voisivat vaikuttaa nopeasti yhteiskunnan elintärkeisiin toimintoihin. Koko yhteiskunta on näin ollen riippuvainen tietoliikenneyhteyksistä ja niiden infrastruktuurin toimivuudesta. (Sisäministeriö 2018, 17.) Tämä riippuvuus on turvallistettu välttämättömänä turvattavana osana kansallista kriittistä infrastruktuuria.

Jotta yhteiskunnan elintärkeät toiminnot saadaan turvattua, on tärkeää määritellä, mitkä osat infrastruktuuria ovat välttämättömiä niiden toiminnalle. Riskienhallinnan osalta on järkevää asettaa muun muassa kriittiselle infrastruktuurille tavoitetasot, jotta se täyttää kansalliset vaatimukset yhteiskunnan toiminnan jatkuvuudelle turvallistaminen voi varmistaa, että se on resilienssin kannalta riittävän suojattu. Näiden tasojen avulla voidaan varmistaa, että yhteiskunnan keskeiset palvelut ja infrastruktuuri kestävät häiriöitä ja ovat toimintakykyisiä kaikissa tilanteissa. (Turvallisuuskomitea 2019, 7.)

Valtiolliset toimijat muodostavat konkreettisia kyberturvallisuuteen liitettäviä uhkia, joita käsiteltiin edellisessä luvussa. Valtiolliset toimijat luovat kuitenkin myös riskejä

kyberturvallisuuteen. Kyberhyökkäykset ovat valtiollisten toimijoiden keino heikentää yhteiskunnan resilienssiä, mikä korostaa kyberturvallisuuden merkitystä yhteiskunnan turvallistamisessa. (Turvallisuuskomitea 2013, 1.) Vuoden 2013 kyberturvallisuustrategian mukaan *”Kyberoperaatiot on tulkittu niin sanotuiksi pehmeiksi toimiksi, minkä vuoksi niiden käyttökynnyksen voidaan arvella olevan alempi kuin perinteisten sotilasoperaatioiden.”* (Turvallisuuskomitea 2013, 17.) Matalamman kynnyksen takia kyberympäristö on arvaamattomampi ja valtiolliset toimijat voivat tehdä kyberoperaatioita kevyemmin perustein. Tämä voi aiheuttaa riskin äkillisistä ja vaikeasti ennakoitavista hyökkäyksistä, joihin ei pysty valmistautumaan samalla tavalla kuin sotilaallisiin operaatioihin. Kybertoimintaympäristö antaa pienille valtioille mahdollisuuden tehdä kyberhyökkäyksiä, koska niiden tekemiseen ei tarvitse niin paljon resursseja. Tämä heikentää turvallisuusjärjestelmää, joka nojaa perinteisiin resursseihin. (Turvallisuuskomitea 2013, 17.)

Valtiollisten toimijoiden hybridivaikuttaminen tekee kyberhyökkäysten ja perinteisten voimakeinojen erottelusta vaikeampaa. Tämä riski liittyy siihen, että kriisitilanteessa voi olla vaikeaa erottaa sotilaallisia toimia edellyttävät toimet ja kyberoperaatioiksi jäävät toimet. Tämä hidastaa paljon vastatoimien aloittamista. Valtiollisten toimijoiden tietomurrot ja yksityisyyden loukkaukset voivat heikentää kansalaisten luottamusta turvallisuustoimiin, mikä tekee yhteiskunnasta haavoittuvamman niin sisäisille jännitteille kuin ulkoisillekin kyberhyökkäyksille. (Sisäministeriö 2023, 25;35.)

Teknologian kehitys nostetaan myös esille yhdeksi riskitekijäksi kyberturvallisuudessa. Teknologian kehittyminen on lisännyt yhteiskunnan riippuvuutta viestintäverkoista, radiotaajuuksista ja tietojärjestelmistä, jotka ovat kriittisiä peruspalveluiden ja yhteiskunnan toiminnan kannalta. Vuoden 2018 riskiarviossa sanotaan, että *”yhä useammat palvelut ovat aiempaa riippuvaisempia viestintäpalveluiden, viestintäverkkojen, radiotaajuuksien ja tietojärjestelmien häiriöttömästä toiminnasta. Mahdolliset häiriöt voivat vaikuttaa myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan.”* (Sisäministeriö 2018, 17.) Yhä useamman palvelun ja infrastruktuurin digitalisoituminen ja verkkoon kytkeytyminen lisäävät niiden haavoittuvuutta kyberhyökkäyksille, mikä uhkaa palveluiden jatkuvuutta ja turvallisuutta. Teknologian kehityksen myötä järjestelmät ja organisaatiot ovat yhä tiiviimmin yhteydessä toisiinsa, mikä kasvattaa häiriöiden kerrannaisvaikutusten riskiä. (Sisäministeriö 2018, 17-18.) Jatkuvasti kehittyvät teknologiat edellyttävät myös kyberturvallisuuden toimien vahvistamista ja näiden riskien turvallistamista.

Uudet teknologiat, kuten tekoäly ja esineiden internet, tarjoavat alustan kyberhyökkäyksille. Digitalisaation mukanaan tuomat uudet teknologiat tarjoavat paitsi mahdollisuuksia myös uusia riskejä, mutta ne voivat myös edistää kyberympäristön turvallistamista ja hyökkäysten ennakoinnin kehittämistä. Teknologian kehitys on myös lisännyt kykyjä erilaisille toimijoille kyberrikollisuuteen, valtiolliseen vakoiluun, tiedusteluun ja hybridivaikuttamiseen liittyen, jotka taas voivat mahdollisesti uhata yhteiskunnan kriittisiä toimintoja. Digitalisaation kehitys lisää myös perinteisten riskien, kuten inhimillisten virheiden, vakavuutta, sillä ne voivat aiheuttaa laajamittaisia ongelmia yhä keskeisemmässä digitaalisessa ympäristössä. (Turvallisuuskomitea 2019, 4.)

Kaikissa tarkastelemissani dokumenteissa nostetaan keskeiseksi riskiksi yhteiskunnan kasvava riippuvuus digitaalisista palveluista ja kriittisistä tietojärjestelmistä, sillä niiden häiriöt voivat aiheuttaa merkittäviä kerrannaisvaikutuksia laajasti eri sektoreilla. Kyberuhkien ja -riskien erottaminen toisistaan on keskeistä, sillä ne edellyttävät erilaisia hallintakeinoja: uhkia voidaan pitää tahallisina ja kohdennettuina haitallisina tekoina, kun taas riskit liittyvät todennäköisyyksiin, ennaltaehkäisyyn ja hallintaan. (Friis & Reichborn-Kjennerud 2016, 33.) Dokumenteissa korostetaan erityisesti sitä, miten keskinäisriippuvuudet lisäävät häiriöiden riskiä ja kansainvälisiin ulottuvuuksiin liittyviä epävarmuuksia, joiden myötä esimerkiksi ulkomainen omistus ja globaalit tietoliikenneyhteydet voivat osaltaan muodostaa turvallisuusriskin. Uuden teknologian kehitys on myös luonut merkittäviä riskejä ja lisännyt kyberturvallisuuden monimutkaisuutta esimerkiksi tekoälyn ja esineiden internetin yleistymisen myötä. Näiden riskitekijöiden hallinta edellyttää tietojärjestelmien suojauksen vahvistamista ja kansallisen resilienssin kehittämistä, jotta riskejä voidaan ennaltaehkäistä, riskiyttää ja torjua mahdollisimman tehokkaasti.

6.2 Sosiaaliset tekijät ja hybridivaikuttamisen riskit kyberympäristössä

Nyky-yhteiskunta on vahvasti riippuvainen digitalisaatiosta, mikä tekee kyberturvallisuudesta ja siihen liittyvistä riskeistä yhä merkittävämpiä. Sen takia on tärkeää, että kyberriskejä kartoitetaan tarpeeksi, jotta niihin osataan suojautua ja turvallistamisen avulla varmistaa kriittisten toimintojen jatkuvuus. Koska osaamisvaje kyberturvallisuusriskien tunnistamisessa voi kasvattaa haavoittuvuutta kriittisissä toiminnoissa tai mahdollistaa kyberhyökkäyksen onnistumisen. (Turvallisuuskomitea 2013, 31-32.)

Vuoden 2019 kyberturvallisuusstrategiassa painotetaan, kuinka *”suomalainen yhteiskunta tarvitsee kyberturvallisuuden osaamista sekä julkisessa hallinnossa että elinkeinoelämässä. Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, ja jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme.”* (Turvallisuuskomitea 2019, 8.) Kansallisella tasolla on erityisen tärkeää varmistaa, että kaikilla on riittävät valmiudet toimia turvallisesti digitaalisessa ympäristössä. Koulutuksella ja tutkimuksella on keskeinen rooli kyberturvallisuuden osaamisvajeen täyttämisessä, mikä osaltaan riskiyttää kyberuhkien vaikutuksia ja edistää niiden ennakoimista, jotta kaikilla oppilailla olisi perustaidot toimia turvallisesti digitaalisessa ympäristössä ja ymmärrys kyberuhkien tunnistamisesta. Tämä tukisi laajamittaisten riskien ehkäisyä ja parantaisi yhteiskunnan resilienssiä kyberuhkia vastaan. (Turvallisuuskomitea 2013, 31-32.) Pitkällä aikavälillä kustannustehokkain tapa parantaa kansallista kyberturvallisuutta on myös panostaa osaamisen kehittämiseen. Tätä tukevia toimia voisi olla esimerkiksi tietoturva-alan koulutuspaikkojen lisääminen ja jatkuvan koulutuksen tarjoaminen alan ammattilaisille. (Turvallisuuskomitea 2019, 8.)

Vaikka osaamisen kehittäminen ja koulutus vahvistavat kyberturvallisuutta, on tärkeää huomioida myös yksityisyyden suojan merkitys digitaalisessa ympäristössä. Yksityisyyden suoja on tärkeä osa kyberturvallisuutta, sillä henkilötietojen ja viestinnän turvaaminen lisää kansalaisten luottamusta digitaalisiin palveluihin. Turvallistamisen näkökulmasta yksityisyyden suoja voi kuitenkin edellyttää tasapainottelua tiedon jakamisen ja suojelun välillä, mikä vaikuttaa riskien hallintaan. Yksityisyyden suojalla viitataan yksilöiden henkilötietojen ja luottamuksellisen viestinnän suojaan. Tämä nostetaan käsittelemissäni dokumenteissa kyberturvallisuuden riskiksi, sillä erilaisten kyberhyökkäysten avulla voidaan rikkoa yksityisyyden suojaa. (Turvallisuuskomitea 2013, 10.)

Yksityisyyden suoja ja siihen liittyvä lainsäädäntö luo haasteita kyberturvallisuudelle. Kansainväliset sopimukset ja EU-lainsäädäntö asettavat tiukat vaatimukset henkilötietojen käsittelylle ja viestinnän luottamuksellisuudelle, mikä voi estää kyberturvallisuustiedon tehokkaan siirron viranomaisille. Tämä hidastaa kyberhyökkäysten torjuntaa ja heikentää Suomen kyberturvallisuutta, sillä viranomaisten välinen tiedonvaihto on keskeistä tehokkaan reagoinnin kannalta. (Sisäministeriö 2016, 24.) Riskiyttämisen avulla voitaisiin kuitenkin priorisoida, mitkä tiedonvaihdon osa-alueet ovat olennaisimpia kriittisten uhkien torjunnassa.

Viestinnän luottamuksellisuuden suoja, joka on osa yksityisyyden suojaa, koskee myös digitaalisten laitteiden välistä tiedonvaihtoa. Tämä tekee kyberhyökkäysten ehkäisemisestä entistä vaikeampaa, koska tietoa ei voida vapaasti jakaa, vaikka se olisi tarpeellista turvallisuuden kannalta. Tietoturvan puutteet ja lainsäädännön rajoitteet voivat estää toimenpiteet, lisätä tietovuotojen riskiä ja heikentää kyberturvallisuutta sekä luottamusta digitaalisiin palveluihin, mikä tekee yksityisyyden suojasta riskin kyberturvallisuudelle. (Sisäministeriö 2016, 23.)

Kybertoimintaympäristöön kohdistuvat riskit eivät rajoitu pelkästään osaamisen puutteeseen tai yksityisyyden suojaan, sillä riskit voivat olla myös laajempia ja monimuotoisempia riskejä. Vuoden 2015 riskiarvion mukaan *”turvallisuusympäristön muutoksen myötä hybridivaikuttaminen, kyberhyökkäykset ja terrorismi ovat lisääntyneet.”* (Sisäministeriö 2016, 18.) Tässä yhteydessä turvallisuusympäristön muutos viittaa erityisesti teknologian nopeaan kehitykseen ja sen mukanaan tuomiin haavoittuvuuksiin. Erityisesti hybridivaikuttaminen on lisääntynyt viime vuosina ja samalla luonut monitasoisen riskin, sillä ne kohdistuvat paitsi teknisiin järjestelmiin myös kansalaisten luottamukseen ja yhteiskunnan vakauteen. Hybridivaikuttamisen turvallistaminen voisi edellyttää kohdennettuja toimia, jotka vahvistavat kansalaisten ja instituutioiden luottamusta kriisitilanteissa. (Sisäministeriö 2016, 27-28.)

Hybridivaikuttamisessa olennaista on se, että kyberturvallisuuteen voidaan pyrkiä vaikuttamaan monen eri kanavan kautta. Esimerkiksi vihamielisellä informaatiovaikuttamisella ja disinformaation levittämisellä voidaan pyrkiä fyysisen ympäristön lisäksi vaikuttamaan informaatioympäristöön, ja tätä kautta yhteiskunnan elintärkeisiin toimintoihin. Tämä informaatiovaikuttaminen muodostaa riskin kyberturvallisuudelle, sillä yhteiskunnan vakauden heikentyessä myös kybertoimintaympäristön hallinta vaikeutuu. (Sisäministeriö 2023, 31.) Teknologian kehittyessä kyberhyökkäyksille altistuvien laitteiden ja järjestelmien määrä on kasvanut, ja niiden haavoittuvuuksia voidaan hyödyntää hybridioperaatioissa, mikä osaltaan lisää kyberrikosten määrää. Kyberrikosten määrän kasvu Suomessa taas kuormittaa poliisin resursseja. (Sisäministeriö 2016, 27-28.)

Hybridivaikuttaminen sodankäynnin muotona on yleistynyt Euroopassa, mikä on lisännyt informaatio- ja kyberoperaatioiden riskiä myös Suomessa. Tällainen toiminta tekee Suomesta potentiaalisen kohteen kyber- ja hybridivaikuttamiselle, jonka takia Suomen on panostettava entistä enemmän kyberturvallisuuteen ja vahvistettava kansainvälisiä

turvallisuusyhteistyöverkkoja. Tämä turvallistaminen parantaa kansallista turvallisuutta ja kykyä kohdata hybridiuhkien luomia riskejä. (Sisäministeriö 2016, 29.)

Erityisen suuri riski hybridivaikuttamisessa liittyy sosiaalisen median käyttöön kyberympäristössä. Vuoden 2018 riskiarvion mukaan *”kyberympäristö ja sosiaalinen media tarjoavat valtiollisille ja ei-valtiollisille tahoille toimintaympäristön, jossa tiedonhankinnan ohella pyritään vaikuttamaan kohdemaan sisäisiin asioihin kuten yhteiskunnan vakauteen, kansalaismielipiteisiin, poliittisiin voimasuhteisiin ja liittolaissuhteisiin. Trollaamisella ja disinformaation levittämisellä pyritään keinotekoisesti jakamaan kohdemaan kansalaismielipidettä, lisäämään eripuraa ja vähentämään luottamusta viranomaisiin.* (Sisäministeriö 2018, 16.) Sosiaalinen media on kehittynyt merkittäväksi kanavaksi disinformaation levittämiselle ja kansalaisten mielipiteisiin vaikuttamiselle, mikä aiheuttaa merkittäviä kyberturvallisuusriskejä yhteiskunnalle. Tällainen käyttö riskiyttää yhteiskunnan kyvyn suojautua tehokkaasti, sillä sen kautta voidaan pyrkiä jakamaan mielipiteitä, luomaan epäluottamusta viranomaisia kohtaan ja yleisesti lisäämään epävakautta yhteiskunnassa. (Sisäministeriö 2018, 16.)

Sosiaalisessa mediassa käytetään esimerkiksi trollaamista ja valetilejä vaikuttamisen keinoina, joiden avulla pyritään luomaan erimielisyyksiä kansalaisten mielipiteiden välille. Tällä tavalla voidaan luoda yleistä epäluottamuksen ilmapiiriä, joka vähentää kansalaisten yhteenkuuluvuutta ja vaikuttaa yhteiskunnallisten instituutioiden toimintaa. Tällaiset toimintatavat voivat riskiyttää yhteiskunnan vakauden ja kyberturvallisuuden, sillä ne voivat heikentää instituutioiden toimintakykyä ja kansalaisten luottamusta viranomaisiin. (Sisäministeriö 2018, 16.) Tällaisilla kyberhyökkäyksillä voidaan myös pyrkiä vaikuttamaan vaaleihin esimerkiksi siten, että vaalien luotettavuudesta ja rehellisyydestä levitetään huhuja sosiaalisessa mediassa. Tällainen riskiyttäminen on todella vaarallista, sillä se voi uhata koko länsimaisen demokratiajärjestelmän uskottavuutta. (Sisäministeriö 2018, 24.)

Sosiaalisessa mediassa voi esiintyä myös strategista ja pitkäkestoista vaikuttamiskampanjoita, joissa teknologisten keinojen avulla pyritään levittämään harhaanjohtavaa tietoa mahdollisimman uskottavasti. Kuvamanipulaatiot ja valheelliset uutisvideot voivat olla osa sitä, miten eri tilanteista voidaan luoda tahallaan vääristynyt kuva. Näiden menetelmien kautta tuotettua väärää tietoa voidaan taas jakaa sosiaalisen median eri kanavissa ja valeuutissivustoilla. Tällaisen vaikuttamisen kautta pyritään turvallistamaan valheellinen

narratiivi, joka heikentää yhteiskunnan kykyä puolustautua disinformaatiota vastaan ja horjuttaa kansalaisten luottamusta perinteiseen mediaan. (Sisäministeriö 2018, 25-26.)

Suomen yhteiskunnan resilienssi disinformaatiota vastaan perustuu kansalaisten vahvaan luottamukseen instituutioihin, mediaan ja oikeusjärjestelmään (Sisäministeriö 2023, 33). Tämän vuoksi turvallistamisen näkökulmasta on tärkeää, että kansalaisilla on vahva kriittinen medialukutaito ja että media säilyttää sekä vastuullisuutensa että riippumattomuutensa. Suomen koulutusjärjestelmällä on vahva rooli tässä, sillä se tukee tätä resilienssiä kehittämällä kriittistä medialukutaitoa, joka auttaa kansalaisia tunnistamaan esimerkiksi valheelliset uutiset. (Sisäministeriö 2018, 26.) Näiden lisäksi vahva ja totuuteen perustuva kansallinen tarina on keskeinen keino torjua ulkopuolista vaikuttamista. Se luo yhteiskunnalle yhtenäisen arvopohjan ja identiteetin, joka taas auttaa vastustamaan disinformaatiota ja vääristelyä. Tämä turvallistaminen on tärkeää yhteiskunnan yhtenäisyyden ja kykyjen säilyttämiseksi kriisitilanteissa, sillä se vahvistaa kansalaisten luottamusta toisiinsa sekä yhteisiin instituutioihin. (Sisäministeriö 2023, 33.)

Tarkastelemissani dokumenteissa korostetaan kyberosaamisen ja yksityisyyden suojan esille nostamista oleellisena osana kyberturvallisuuden riskien ehkäisemisessä. Riittävä kyberosaaminen kaikilla yhteiskunnan tasoilla tukee digitaalisen ympäristön turvallisuutta ja vähentää haavoittuvuuksia. Yksityisyyden suojan ylläpito luo taas omat haasteensa kyberturvallisuudelle, koska se voi rajoittaa tiedon jakamista viranomaisten välillä, hidastaa kyberuhkien torjuntaa ja vaikeuttaa nopeaa reagointia kriittisiin tilanteisiin. Hybridivaikuttaminen nostetaan myös yhdeksi suureksi riskiksi kyberturvallisuudessa ja erityisesti sosiaalisen median kautta tapahtuva disinformaatio on merkittävä riski, joka voi riskiyttää kansalaisten luottamusta yhteiskunnallisiin instituutioihin ja lisätä epävakautta. Näiden riskien ennaltaehkäiseminen ja torjuminen vaatii dokumenttien mukaan koulutusta, kriittistä medialukutaitoa ja kansainvälisen yhteistyön kehittämistä, jotta Suomen resilienssi paranee näitä vastaan.

7 Suomen kyberturvallisuuden uhkien ja riskien muotoutuminen

Seuraavaksi käsittelen tarkastelemissani dokumenteissa esiin tuotuja uhkia ja riskejä yksityiskohtaisemmin ja vertailen niitä keskenään. Pyrin syventymään tarkemmin siihen, minkälaisista asioista dokumenteissa on turvallistamisen avulla luotu turvallisuusongelmia ja mistä vuorostaan riskiyttämisen avulla riskejä.

Aloitan tarkastelemalla aineistostani löytämiäni keskeisiä uhkia, jotka toin esille luvussa 5. Luvun 5 kyberturvallisuutteen liittyvät uhat jaoin kahteen eri osa-alueeseen, joista ensimmäinen käsitteli kyberympäristön teknologisia ja infrastruktuurisia uhkia. Turvallistamisen näkökulmasta nämä uhkat keskittyivät pääosin tekniikan aiheuttamiin uhkiin, kuten kriittiseen infrastruktuuriin kohdistuviin hyökkäyksiin, palvelunestohyökkäyksiin, tietomurtoihin, tietoteknisten järjestelmien haavoittuvuuksiin, tietoverkkojen häiriöihin ja tietoteknisten järjestelmien keskinäiseen riippuvuuteen. Nämä uhkat korostavat, kuinka riippuvuus teknologisista järjestelmistä tekee infrastruktuurista haavoittuvaisen ja kuinka kriittistä on varautua niiden suojaamiseen sekä häiriöiden vaikutusten minimoimiseen.

Toinen kyberturvallisuuteen liittyvien uhkien osa-alue käsitteli kyberympäristön strategisia ja geopoliittisia uhkia. Nämä uhkat ulottuvat taas teknologian ulkopuolelle, sillä ne liittyvät erilaisiin laajempiin toimintaympäristöihin, kuten kansainvälisiin suhteisiin ja politiikkaan laajemmin. Turvallistamisen avulla dokumenteissa korostetaan valtiollisia toimijoita ja niihin liittyviä kyberuhkia, hybridivaikuttamista, disinformaatiota ja informaatiovaikuttamista sekä teknologian nopeaa kehitystä. Tämä korostaa, kuinka kyberympäristö liittyy yhä tiiviimmin kansainväliseen politiikkaan ja valtakamppailuihin, joissa teknologian kehitys ja informaation hallinta luovat uusia haasteita.

Voidaan nähdä, että aineiston perusteella esiin nousseet uhat kytkeytyvät laajempiin ilmiöihin, kuten hybridivaikuttamiseen, disinformaatioon, teknologisiin haavoittuvuuksiin ja geopoliittisiin jännitteisiin. Turvallistaminen ilmiönä tekee näistä uhkista moniulotteisia ja vaikeasti hallittavia. Teknologiset uhat, kuten infrastruktuurin haavoittuvuudet ja tietomurrot, tuovat taas esille, kuinka riippuvainen yhteiskunta on teknisistä järjestelmistä. Strategiset ja geopoliittiset uhat, kuten valtiollisten toimijoiden kybertoimet ja kansainvälinen voimapolitiikka, tuovat esiin kyberympäristön keskeisen roolin globaalissa politiikassa. Näiden uhkien välinen yhteys osoittaa, että kyberturvallisuus on niin yhteiskunnallinen ja poliittinen kuin tekninen kysymys. Se kuvastaa samaan aikaan teknologia kehityksen luomia haasteita sekä kansainvälisten suhteiden muutoksista tulevia haasteita.

Seuraavaksi tarkastelen vuorostaan aineistostani löytämiäni riskejä, joita erittelin luvussa 6. Luvun 6 kyberturvallisuuteen liittyvät riskit jaoin myös kahteen eri osa-alueeseen, joista ensimmäinen käsitteli kybertoimintaympäristön teknologisia riippuvuuksia, haavoittuvuuksia ja infrastruktuurien riskejä. Riskiyttämisen avulla näihin riskeihin kuuluivat riippuvuus

tietoverkoista, tietojärjestelmien suojaamisen puutteet, kybertoimintaympäristön globaalisuus, valtiolliset toimijat ja niiden aiheuttamat riskit sekä teknologian kehitys. Näiden riskien erittely havainnollistaa, kuinka kybertoimintaympäristön riskit syntyvät teknologian ja järjestelmien keskinäisistä riippuvuuksista, jotka voivat tehdä järjestelmistä haavoittuvia ja alttiita häiriöille.

Toinen kyberturvallisuuteen liittyvien riskien osa-alue käsitteli sosiaalisia tekijöitä ja hybridivaikuttamisen riskejä kyberympäristössä, tuoden esiin kyberturvallisuuden moninaisuuden. Näissä riskeissä painottuivat osaamisvaje, yksityisyyden suoja, hybridivaikuttaminen, sosiaalinen media ja disinformaatio. Riskiyttäminen tässä yhteydessä mahdollistaa tarkastelun siitä, kuinka kyberturvallisuus ulottuu teknisten kysymysten lisäksi myös yhteiskunnallisiin ja sosiaalisiin haasteisiin, tehden siitä moniulotteisen ilmiön.

Aineiston perusteella kyberturvallisuuteen liittyvät riskit ovat moninaisia ja liittyvät sekä teknologisiin että sosiaalisiin tekijöihin. Teknologiset riskit, kuten järjestelmien keskinäiset riippuvuudet ja suojauspuutteet, korostavat infrastruktuurien haavoittuvuutta ja yhteiskunnan vahvaa riippuvuutta tietoverkoista. Sosiaalisiin tekijöihin liittyvät riskit, kuten osaamisvaje ja disinformaatio, kuvastavat kybertoimintaympäristön kytkeytymistä laajempiin yhteiskunnallisiin haasteisiin. Tämä osoittaa, että kyberturvallisuuden riskit ovat sekä teknisiä että inhimillisiä, ja niiden hallinta edellyttää monipuolista ymmärrystä niin teknologiasta kuin yhteiskunnallisista tekijöistä. Turvallistamisen näkökulmasta riskien hallinta on osa prosessia, jossa näistä teknisistä ja inhimillisistä haasteista tehdään keskeisiä turvallisuusongelmia.

Kyberturvallisuuden uhkien ja riskien tarkastelu nostaa esiin niiden erojen sekä yhteisten tekijöiden pohdinnan. Aineistoni perusteella voidaan todeta, että uhat ja riskit näyttäytyvät toisistaan poikkeavina ilmiöinä, mutta samalla ne kytkeytyvät tiiviisti toisiinsa. Uhkat ja riskit eroavat toisistaan ylätasolla siten, että uhkat ovat usein laajempia ja liittyvät abstraktimpiin ilmiöihin, kuten hybridivaikuttamiseen, disinformaatioon ja teknologian haavoittuvuuksiin. Riskit ovat taas enemmän konkreettisempia, ja niiden vaikutukset näkyvät esimerkiksi luottamuksen heikkenemisenä instituutioihin, yksityisyyden suojan heikentymisenä tai yhteiskunnan vakauden horjumisena. Riskit voivat myös ilmetä uhkien mahdollisina seurauksina. Tämä ero osoittaa, miten turvallistaminen ja riskiyttäminen täydentävät toisiaan kyberuhkien ja -riskien ymmärtämisessä: turvallistaminen painottaa uhkien vakavuutta, kun taas riskiyttäminen keskittyy niiden käytännön vaikutuksiin. Tämä on merkityksellistä

kyberturvallisuuden hallinnan kannalta, sillä se auttaa kohdentamaan resursseja oikean määrän eri kohteisiin ja arvioimaan, miten uhkia hallitaan ja riskejä ehkäistään.

Aiemmin käsiteltyjen havaintojeni perusteella uhkat luovat perustan riskien toteutumiselle, mikä tekee uhkien torjunnasta ensisijaista. Esimerkiksi teknisten järjestelmien haavoittuvuudet eivät itsessään aiheuta vahinkoa, mutta niiden hyödyntäminen voi mahdollistaa hyökkäyksiä, joissa tietoja varastetaan tai tuhotaan. Haavoittuvuuksien esittäminen uhkina turvallistamisen kautta rakentaa pohjaa riskiyttämiselle, jossa huomio keskittyy näiden uhkien mahdollisiin seurauksiin. Tällaiset riskit voivat pahimmillaan vaarantaa yhteiskunnan toiminnan perusedellytykset. (Sisäministeriö 2016, 21). Voidaan nähdä, että uhat ovat yleensä abstraktimpia, kuten järjestelmien haavoittuvuudet, kun taas niiden mahdollistamat riskit konkretisoituvat yhteiskunnan toiminnan vaarantamisena.

Tällainen uhkien abstraktisuus voi tehdä niihin reagoimisesta haastavampaa, koska niiden mahdollinen vaikutus on vaikea ennakoida. Esimerkiksi kriittisten järjestelmien haavoittuvuudet voivat mahdollistaa kyberhyökkäysten ketjureaktion, jossa yksi palvelunestohyökkäys voi lamauttaa useita keskinäisriippuvaisia sektoreita, kuten terveydenhuollon ja energiatuotannon (Sisäministeriö 2018, 48-49). Tämä uhka on näkynyt muun muassa Ukrainan sodassa, jossa Venäjä on kohdistanut kyberhyökkäyksiä infrastruktuuriin osana laajempia hybridioperaatioita (Sisäministeriö 2023, 39). Tällaiset esimerkit osoittavat, kuinka abstrakti uhka, kuten teknologinen haavoittuvuus, voi muuttua konkreettiseksi riskiksi, jolla on laajoja yhteiskunnallisia vaikutuksia.

Kyberturvallisuuden uhkista ja riskeistä tekemieni havaintojen perusteella voidaan huomata, että niiden hallintaan ehdotetaan hieman erilaisia toimintatapoja. Uhkien hallinta on tyypillisemmin ennaltaehkäisevää ja laajempaa, kun taas riskien hallinta keskittyy niiden konkreettisten vaikutusten lieventämiseen. Esimerkiksi uhkien hallinnassa teknologisten haavoittuvuuksien torjunta on keskeistä. Tietojärjestelmien suojauspuutteet voivat aiheuttaa merkittäviä riskejä erityisesti kriittisille infrastruktuureille, kuten sähkönjakelulle, tietoliikenteelle ja maksujärjestelmille. Näiden järjestelmien haavoittuvuudet voivat vahvasti heikentää yhteiskunnan toimintavarmuutta, esimerkiksi lamaannuttamalla tuotantolaitoksia ja kauppoja samanaikaisesti. Vaikka lyhyellä aikavälillä nämä haavoittuvuudet eivät vaikuttaisi elintarvikehuoltoon, pitkällä aikavälillä ne voivat jopa pysäyttää elintarvikehuollon kokonaan.

Tämän takia ennaltaehkäisevä uhkien hallinta, kuten järjestelmien säännöllinen suojaus ja päivitykset, on todella tärkeää näiden uhkien ennaltaehkäisemiseksi ja riskien lieventämiseksi. (Sisäministeriö 2023, 80).

Riskien hallinnassa taas korostuu kyberosaamisen ja yksityisyyden suojan merkitys. Riittävä kyberosaaminen yhteiskunnan eri tasoilla parantaa digitaalisen ympäristön turvallisuutta ja vähentää haavoittuvuuksia. Samalla yksityisyyden suoja voi luoda omia haasteitaan kyberturvallisuudelle, sillä se voi hidastaa tiedon jakamista viranomaisten välillä ja vaikeuttaa nopeaa reagointia kyberriskeihin. Esimerkiksi hybridivaikuttamien, kuten sosiaalisen median kautta tapahtuva disinformaatio, on merkittävä riski, joka voi heikentää kansalaisten luottamusta yhteiskunnallisiin instituutioihin ja lisätä epävakautta. Tällaisten riskien torjuminen edellyttää koulutusta, kriittistä medialukutaitoa ja kansainvälistä yhteistyötä, mikä puolestaan parantaa Suomen resilienssiä kyberuhkia vastaan. (Sisäministeriö 2023, 12).

Riskien hallinnan kannalta on myös tärkeää kehittää varajärjestelmiä ja suorittaa säännöllisiä turvallisuustestejä, jotta voidaan ennakoida ja minimoida mahdollisia uhkia ja riskejä. Tällaiset toimet eivät ole ainoastaan teknisiä ratkaisuja, vaan myös osa turvallistamisen prosessia, jossa tietyt uhkat nostetaan hallinnan prioriteeteiksi ja niille luodaan riskinhallintamalleja. Tällaisten toimenpiteiden avulla voidaan vähentää vahinkojen laajuutta ja parantaa yhteiskunnan valmiuksia reagoida kyberhyökkäyksiin, jotka voivat aiheuttaa laajoja vaikutuksia. (Sisäministeriö 2023, 24.) Varautuminen ja ennakoivat toimet ovat välttämättömiä kyberturvallisuuden ja yhteiskunnan toiminnan turvaamiseksi.

Havainnoissani korostuu, kuinka tärkeää on yhdistää pitkäjänteinen suunnittelu ja konkreettiset toimenpiteet kyberturvallisuuden ylläpitämisessä. Uhkien ennaltaehkäisy luo vakautta, kun taas riskien hallinta varmistaa, että uhkiin voidaan reagoida nopeasti ja tehokkaasti. Tällainen tasapaino on olennaista, sillä kybertoimintaympäristö muuttuu jatkuvasti. Ilman tätä tasapainoa kyberturvallisuuden hallinta voi jäädä puutteelliseksi, mikä altistaa yhteiskunnan yllättäville ja vakaville häiriöille. Kyberturvallisuuden hallinta vaatii kokonaisvaltaista lähestymistapaa, jossa ymmärretään sekä uhkien että riskien luonne. Tämä mahdollistaa ennakoivien strategioiden ja tehokkaiden reagointikeinojen yhdistämisen, jotka auttavat suojaamaan yhteiskunnan toimintakykyä nopeasti muuttuvassa kybertoimintaympäristössä.

Aiemman perusteella voidaan todeta, että uhkat ja riskit ovat toisiinsa kytkeytyneitä. Yksi uhka voi muuttua riskiksi, ja samalla se voi synnyttää uusia uhkia. Näiden ilmiöiden keskinäinen riippuvuus tekee kyberturvallisuuden hallinnasta monimutkaisen haasteen. Esimerkiksi sosiaalisen median kautta leviävä väärä tieto (riski) voi vahingoittaa organisaation mainetta ja houkutella hyökkääjiä kohdistamaan tarkempia iskuja organisaation tietojärjestelmiin, mikä taas voi johtaa uusiin hyökkäyksiin (uhka). Tämä korostaa kokonaisvaltaisen lähestymistavan tarvetta, jossa ymmärretään ja hallitaan uhkien ja riskien välisiä yhteyksiä osana laajempaa turvallisuussuunnitelmaa.

Tässä yhteydessä on tärkeää, että Suomi kehittää kyberturvallisuuspolitiikkaa, joka painottaa uhkien ja riskien yhteyksien ymmärtämistä ja hallintaa. Turvallistamisen ja riskiyttämisen käsitteet tarjoavat kehyksen, jonka avulla voidaan hahmottaa, miten nämä ilmiöt kytkeytyvät toisiinsa ja luovat kybertoimintaympäristön turvallisuuspoliittista kehystä.

Uhkiin ja riskeihin liittyvien ilmiöiden keskinäinen riippuvuus tarkoittaa, että pelkkä yksittäisiin riskeihin reagoiminen ei riitä, eikä pelkkä uhkien torjunta voi poistaa kaikkia riskejä. Tämä korostaa kokonaisvaltaisen ajattelun merkitystä, sillä kyberympäristössä tarvitaan kykyä hallita sekä laajoja uhkia että niiden konkreettisia seurauksia. Suomen tulisi panostaa kyberresilienssin kehittämiseen siten, että otetaan huomioon uhkien ja riskien mahdolliset ketjut sekä niiden laajemmat vaikutukset. Lisäksi organisaatioiden tulisi osata ennakoida mahdollisia uhkaketjuja ja valmistautua niihin etukäteen.

7.1 Teknologiset ja infrastruktuuriset tekijät

Edellisessä luvussa esitellyt uhkien ja riskien erot ja yhtäläisyydet osoittavat, että kybertoimintaympäristön ilmiöt ovat monimutkaisia ja toisiinsa kytkeytyneitä. Seuraavaksi syvennyn tarkastelemaan, miten erityisesti teknologiset ja infrastruktuuriset tekijät vaikuttavat riskien ja uhkien muodostumiseen ja hallintaan. Teknologisten ja infrastruktuuristen uhkien ja riskien välillä on eroja, mutta ne ovat samankaltaisia erityisesti siinä, miten ne vaikuttavat yhteiskunnan kriittisiin toimintoihin.

Uhat, kuten valtiollisten toimijoiden tekemät kyberoperaatiot tai hyökkäykset kriittiseen infrastruktuuriin, ovat tahallisia tekoja, joiden tavoitteena on heikentää yhteiskunnan toimintakykyä (Turvallisuuskomitea 2013, 17). Esimerkiksi sellaiset kyberhyökkäykset, joiden avulla pyritään lamauttamaan elintärkeitä palveluita, kuten maksuliikennettä tai sähkönjakelua, ovat keskeisiä teknologisia uhkia. Näiden uhkien turvallistaminen vaatii arviointia siitä, miten

ne vaarantavat yhteiskunnan perustoiminnot ja miten ne tunnistetaan poliittisesti merkittäviksi turvallisuusuhkiksi. On tärkeää, että Suomi kehittäisi entistä tiiviimpää yhteistyötä EU:n ja muiden kansainvälisten toimijoiden kanssa, erityisesti kriittisten infrastruktuurien suojaamiseksi, ja vahvistaisi kyberpuolustuksen resursseja näiden uhkien torjumiseksi.

Riskit sen sijaan liittyvät enemmän teknologian ja infrastruktuurin luonteeseen. Esimerkiksi riippuvuus tietojärjestelmistä, niiden keskinäisriippuvuudet ja suojauspuutteet ovat ilmiöitä, jotka eivät ole seurausta välttämättä tahallisesta toiminnasta, mutta voivat aiheuttaa yhtä laajoja seurauksia yhteiskunnalle. (Sisäministeriö 2018, 17-18.) Tällaiset tekijät ovat osa riskiyttämistä, jossa teknologian ja infrastruktuurin haavoittuvuudet voivat altistaa yhteiskunnan suurille ongelmille. Tässä yhteydessä olisi tärkeää, että Suomi ottaisi käyttöön tiukempia sääntöjä ja velvoitteita kriittisten infrastruktuurien toimijoille kyberresilienssin parantamiseksi. Tämä voisi sisältää esimerkiksi sääntelyn, joka velvoittaisi toimijat toteuttamaan säännöllisiä kyberturvallisuusarviointeja ja varautumissuunnitelmia.

Keskeinen yhtäläisyys uhkien ja riskien välillä on niiden vaikutus yhteiskunnan toiminnan jatkuvuuteen. Molemmat voivat häiritä yhteiskunnan kriittisiä toimintoja, kuten tietoliikennettä, maksujärjestelmiä tai ruokahuoltoa (Sisäministeriö 2023, 80). Näiden vaikutukset voivat laajasti aiheuttaa kerrannaisvaikutuksia, jotka johtavat turvallistamiseen ja heikentävät yhteiskunnan toimintakykyä riskiyttämisen seurauksena (Sisäministeriö 2018, 17–18). Uhkat korostuvat erityisesti poikkeusoloissa tai tilanteissa, joissa esimerkiksi joku ulkopuolinen toimija käyttää kyberhyökkäyksiä painostuskeinona jotain maata tai yhteiskuntaa kohtaan. Tällainen toimintatapa tekee juuri uhkien ennakoimisesta ja torjumisesta vaikeaa (Turvallisuuskomitea 2013, 1). Olisi tärkeää, että Suomi osallistuisi aktiivisesti kansainvälisiin keskusteluihin ja sopimuksiin, jotka tähtäävät globaalien kyberuhkien ennakoimiseen ja torjuntaan.

Riskit ovat taas läsnä enemmän normaalioloissa, sillä ne liittyvät enemmän infrastruktuurien ja teknologioiden sisäisiin tekijöihin, kuten digitaalisten järjestelmien haavoittuvuuksiin ja teknologian nopeaan kehitykseen. Riskiyttäminen tässä kontekstissa tarkoittaa sitä, että nämä haavoittuvuudet voivat vähitellen tulla osaksi laajempaa turvallisuusnarratiivia, jolloin niistä tulee kansallisia turvallisuuskysymyksiä. Esimerkiksi tekoäly ja esineiden internet voivat luoda uusia uhkakuvia ja riskejä. Tällaiset kehityskulut onkin tärkeää ymmärtää sekä riskien että uhkien turvallistamisessa ja riskiyttämisessä. Suomi voisi myös luoda foorumeita ja työryhmiä,

joissa eri sidosryhmät, kuten valtionhallinto, yritykset ja tutkimuslaitokset, voisivat yhdessä kehittää ennakoivia ratkaisuja näiden uusien teknologioiden tuomiin haasteisiin.

Merkittävin ero uhkien ja riskien välillä liittyy niiden luonteeseen: uhat ovat aktiivisia ja usein ulkoisten toimijoiden tahallisesti aiheuttamia, kun taas riskit ovat usein syntyvät usein järjestelmien sisäisistä haavoittuvuuksista tai keskinäisriippuvuuksista. Turvallistamisen näkökulmasta uhkien tahallisuus ja ulkoinen alkuperä korostavat niiden merkitystä politiikassa, sillä niiden torjunta vaatii aktiivisia toimia ja oikeuttaa esimerkiksi kyberpuolustuksen vahvistamisen. Riskiyttämisen kautta taas teknologisten haavoittuvuuksien ja keskinäisriippuvuuksien esiin nostaminen voi korostaa infrastruktuurin suojauspuutteiden merkitystä ja kiinnittää huomion entistä enemmän resilienssin kehittämiseen. Suomen tulisi panostaa entistä enemmän ennakoivaan sääntelyyn ja infrastruktuurien suojaamisen varautumissuunnitelmien kehittämiseen. Molempia yhdistää kuitenkin se, että ne vaativat huolellista ennakointia ja varautumista. Esimerkiksi riskien hallinnassa korostetaan infrastruktuurin suojauspuutteiden parantamista ja resilienssin vahvistamista, kun taas uhkien torjunta edellyttää kansallista kyberpuolustuskykyä ja kansainvälistä yhteistyötä. (Sisäministeriö 2018, 17; Turvallisuuskomitea 2019, 7). Tämän vuoksi on tärkeää, että Suomi jatkaa kyberpuolustuskyvyn kehittämistä ja varmistaa tehokkaan kansainvälisen yhteistyön erityisesti kyberuhkien torjumisessa. Tämä tekee sekä uhkien että riskien hallinnasta keskeisen osan kyberturvallisuusstrategiaa, jossa molempiin ilmiöihin vastataan samanaikaisesti ja toisiaan täydentävillä keinoilla. Turvallistaminen ja riskiyttäminen ovat keskeisiä prosesseja, joiden avulla uhkia ja riskejä tarkastellaan ja liitetään osaksi kansallisen turvallisuuden kokonaisuutta.

7.2 Moninaiset vaikuttavat tekijät

Kyberturvallisuus ei rajoitu pelkästään teknologisiin ja infrastruktuurisiin kysymyksiin, vaan siihen vaikuttavat myös sosiaaliset ja poliittiset tekijät, jotka luovat merkittäviä uhkia ja riskejä. Esimerkiksi valtiollisten toimijoiden hybridivaikuttaminen, disinformaatio ja informaatiovaikuttaminen osoittavat, kuinka teknologinen kehitys ei pelkästään mahdollistaa uusia hyökkäyksiä, vaan myös tuo esiin sosiaalisia ja rakenteellisia haavoittuvuuksia. Seuraavaksi tarkastelen laajemmin sellaisia uhkia ja riskejä, jotka ulottuvat teknologian ulkopuolelle.

Kyberturvallisuuden uhkia ja riskejä tarkastellessa voidaan nähdä, että ne ovat monitahoisia, koska niihin vaikuttavat erilaiset sosiaaliset, strategiset ja geopoliittiset tekijät sekä hybridivaikuttaminen. Monitahoisia uhkia ovat esimerkiksi valtiollisten toimijoiden hybridivaikuttaminen, disinformaatio ja informaatiovaikuttaminen, joiden tavoitteena on heikentää yhteiskunnan vakaata toimintaa ja kansalaisten luottamusta instituutioihin. Näiden uhkien turvallistaminen vaatii erityistä huomiota, koska ne eivät ole pelkästään teknologisia, vaan ne hyödyntävät myös yhteiskunnan rakenteellisia heikkouksia, kuten kansalaisten poliittista jakautuneisuutta ja media roolia tiedon levittämisessä. Esimerkiksi disinformaation torjumiseen ei riitä pelkästään tekniset ratkaisut, vaan siihen tarvitaan myös lainsäädännön kehittämistä, joka selkeyttää ja vahvistaa viranomaisten roolia disinformaation torjunnassa sekä kansalaisten kriittisen ajattelun edistämistä kouluissa ja mediassa. Informaatiovaikuttamisen ehkäisemisessä on tärkeää, että kansalaisilla on luottamus viranomaisiin ja että yhteiskunnalla on valmius puuttua siihen nopeasti, jos se uhkaa heikentää yhteiskunnan vakaata toimintaa. Tällaisessa tilanteessa turvallistaminen ja riskiyttäminen voidaan nähdä toisiaan kytkeytyvänä, sillä turvallistaminen tuo esiin ne osat, jotka ovat enemmän alttiita näille uhkille, kun taas riskiyttäminen tunnistaa rakenteelliset heikkoudet, jotka voivat tehdä yhteiskunnasta haavoittuvamman.

Monitahoisia riskejä taas ovat esimerkiksi osaamisvaje kyberturvallisuudessa, joka osaltaan voi lisätä riskiä siitä, että disinformaatio ja hybridivaikuttaminen onnistuvat odotettua tehokkaammin. Kyberturvallisuuden riskiyttämisen näkökulmasta on tärkeää tuoda esiin osaamisvajeet ja yhteiskunnan heikkoudet, jotka voivat mahdollistaa manipuloinnin ja epäluottamuksen lisääntymiseen. Sosiaalinen media toimii myös merkittävänä alustana disinformaation leviämiselle, mikä on nostettu merkittävänä riskinä kyberturvallisuuden kannalta dokumenteissa. Tässä yhteydessä riskiyttäminen näkyy, koska heikot valvontajärjestelmät ja muut teknologiset rakenteet voivat helpottaa disinformaation leviämistä ja ajan myötä vaikuttaa laajemmin yhteiskunnan turvallisuuteen. Riskiyttäminen auttaa tunnistamaan rakenteelliset heikkoudet ja tuomaan ne osaksi yhteiskunnan turvallisuuskeskustelua. Nämä rakenteelliset riskit eivät ole tarkoituksella luotuja uhkia, mutta ne voivat pahentaa muiden uhkien vaikutuksia ja heikentää yhteiskunnan resilienssiä. Suomi voisi kehittää ja laajentaa kyberturvallisuuden koulutusta ja osaamisen vahvistamista erityisesti julkiselle sektorille ja kriittisille toimijoille, jotta kyberuhkiin pystytään reagoimaan tehokkaammin.

Näiden monitahoisten uhkien ja riskien keskeisenä yhtäläisyytenä on niiden kyky horjuttaa yhteiskunnan perustoimintoja ja luottamusta instituutioihin. Disinformaatiokampanjat ja osaamisvajeet voivat pahimmillaan johtaa siihen, että päätöksentekijät, kansalaiset ja organisaatiot perustamaan toimintansa virheelliseen tietoon, mikä taas heikentää kriisinhallintaa ja valmiutta. Turvallistamisen näkökulmasta voidaan nähdä, että tällaiset uhkat voivat heikentää yhteiskunnan turvallisuutta. Ennaltaehkäisy näitä uhkia vastaan vaatii sekä teknologisten suojausten että sosiaalisten ja institutionaalisten rakenteiden vahvistamista. Esimerkiksi disinformaation leviämisen ehkäiseminen ei ole pelkästään teknologinen, vaan myös sosiaalinen haaste, jossa yhteiskunnan täytyy pystyä käsittelemään ja kyseenalaistamaan väärää tietoa. Suomi voisi investoida ohjelmiin, jotka edistävät kansalaisten medianlukutaitoa ja kykyä erottaa luotettavat tiedonlähteet epäluotettavista.

Uhkat ja riskit vaikuttavat myös merkittävästi julkiseen keskusteluun ja sen jakautumiseen. Esimerkiksi hybridivaikuttamisessa voidaan hyödyntää yhteiskunnan sisäisiä heikkouksia, kuten avointa mediaympäristöä ja kansalaisten kriittisen ajattelun puutetta. Tällöin turvallistaminen edellyttää sellaisia toimia, joilla pyritään lisäämään tiedon luotettavuutta ja vahvistamaan kansalaisten kykyä tunnistaa väärää tietoa. Suomi voisi myös kehittää lainsäädäntöä, joka säätelee väärän tiedon levittämistä erityisesti sosiaalisessa mediassa ja varmistaa tehokkaan valvonnan ja valvontakäytännöt näiden alustoilla.

Monitahoisten uhkien ja riskien luonteessa voidaan nähdä taas eroavaisuuksia. Uhat ovat usein tahallisia ja suunniteltuja tekoja, joita aiheuttavat esimerkiksi valtiolliset tai muut ulkopuoliset toimijat. Näiden uhkien hallinnassa turvallistaminen on keskeistä, ja se vaatii ennakoivaa reagointia sekä vahvoja poliittisia päätöksiä, kuten lainsäädännön kehittämistä ja kansainvälisen yhteistyön lisäämistä. Suomi voisi tiivistää yhteistyötä muiden maiden kanssa kehittääkseen globaaleja sääntöjä kyberhyökkäyksistä ja disinformaation torjumisesta. Riskit puolestaan ovat rakenteellisia ja kehittyvät pidemmän ajan kuluessa yhteiskunnan teknologisten tai sosiaalisten ongelmien seurauksena. Esimerkiksi valtiollisen toimijan tarkoituksella levittämä disinformaatio voidaan nähdä uhkana, kun puolestaan sosiaalisessa mediassa leviävä disinformaatio voidaan nähdä enemmän riskinä, joka voi johtua alustan rakenteellisista puutteista, kuten puutteellisista valvontajärjestelmistä. Riskien hallinnassa korostuu resilienssin kehittäminen ja rakenteellisten haavoittuvuuksien tunnistaminen, jotta yhteiskunta voisi paremmin sopeutua ja palautua tällaisista häiriöistä. Resilienssi ei ole vain kykyä vastustaa uhkia, vaan myös kykyä sopeutua ja toipua rakenteellisista ongelmista.

8 Johtopäätökset

8.1 Uhkat ja riskit Suomen kybertoimintaympäristössä

Tässä tutkielmassa olen tarkastellut, minkälaisia kyberturvallisuuden uhkia ja riskejä turvallistetaan ja riskiytetään Suomen riskiarvioissa ja kyberturvallisuusstrategioissa. Analysoin Suomen kansallisia riskiarvioita vuosilta 2015, 2018 ja 2023 sekä kyberturvallisuusstrategioita vuosilta 2013 ja 2019. Tavoitteenani oli muodostaa kattava kuva siitä, millaisista kyberturvallisuuteen liittyvistä uhkista ja riskeistä on rakennettu turvallisuusongelmia Suomessa noin kymmenen vuoden aikana.

Aluksi käsittelin kyberturvallisuuden käsitettä ja sen merkitystä, minkä jälkeen tarkastelin, miten kyberturvallisuutta tulisi käsitellä. Tämän jälkeen syvennyin uhkien ja riskien tarkasteluun osana kyberturvallisuuden tutkimusta sekä kyberresilienssin näkökulmasta. Taustoituksen jälkeen käsittelin tutkielman teoreettista viitekehystä, turvallistamisteoriaa ja riskiyttämistä, sekä esittelin, miten hyödynnän turvallistamisteoriaa myös metodina. Tämän jälkeen analysoin tutkimusaineiston ja esittelin löytämäni uhkat ja riskit erikseen. Lopuksi vertailin ja erittelin havaintojani siitä, miten kyberturvallisuuteen liittyvät uhat ja riskit on tutkimassani aineistossa määritelty.

Tutkimistani riskiarvioista ja kyberturvallisuusstrategioista käy ilmi, että kyberturvallisuuden uhat ja riskit muodostavat monimutkaisen kokonaisuuden, jossa eri tekijät kytkeytyvät vahvasti toisiinsa. Uhat ovat usein abstrakteja ja liittyvät ulkoisten toimijoiden tahallisiin toimenpiteisiin, kuten valtiollisten toimijoiden toteuttamiin kyberhyökkäyksiin. Riskit puolestaan ovat konkreettisempia ja johtuvat järjestelmien sisäisistä tekijöistä, kuten teknologisista riippuvuuksista ja suojauspuutteista. Uhkien ja riskien välillä on jatkuva vuorovaikutus: uhkat voivat synnyttää riskejä, kuten haavoittuvuuksia tai resurssien menetyksiä, ja heikko riskinhallinta voi puolestaan lisätä uhkien vaikutuksia.

Kyberturvallisuuden uhkia ja riskejä tarkasteltaessa on tärkeää huomioida, että ne eivät rajoitu ainoastaan teknologisiin ja infrastruktuurisiin tekijöihin, vaan sisältävät myös sosiaalisia ja poliittisia ulottuvuuksia. Esimerkiksi disinformaation leviäminen osoittaa, että kyberturvallisuutta ei voida tarkastella erillään laajemmista yhteiskunnallisista kysymyksistä. Teknologian kehitys, kuten tekoälyn kehittyminen, tuo mukanaan uusia kyberturvallisuusriskejä, mutta samalla haastaa perinteisen turvallisuusajattelun, joka voi

keskittyä liikaa yksittäisiin teknisiin uhkiin. Tämä korostaa tarvetta tarkastella riskienhallintaa ja uhkiin varautumista kokonaisvaltaisesti – sekä teknologisen kehityksen että ihmisten toiminnan näkökulmasta, jotta kyetään vastaamaan nopeasti muuttuvan kybertoimintaympäristön haasteisiin.

Turvallistamisella ja riskiyttämisellä on erilaiset, mutta toisiaan täydentävät näkökulmat kyberturvallisuuden käsittelyyn. Turvallistaminen nostaa uhkia yhteiskunnallisiksi ja poliittisiksi kysymyksiksi, mutta samalla se saattaa antaa niille liikaa painoarvoa keskittymällä niiden näennäiseen merkitykseen enemmän kuin niiden todelliseen todennäköisyyteen. Tämä puolestaan herättää kysymyksen siitä, miten turvallistaminen voisi ohjata resursseja tarkoituksenmukaisesti niin, ettei se samalla aiheuta tarpeetonta pelon lietsomista.

Riskiyttäminen keskittyy puolestaan enemmän haavoittuvuuksiin ja niiden hallintaan, mikä tuottaa konkreettisempia ratkaisuja. Riskiyttämisessä voidaan kuitenkin helposti unohtaa laajemmat yhteiskunnalliset seuraukset, kuten luottamuksen heikkeneminen. On tärkeää, että riskiyttämisessä huomioidaan myös sen vaikutukset yhteiskunnalliseen resilienssiin eikä keskitytä vain teknisten järjestelmien haavoittuvuuksiin. Turvallistaminen ja riskiyttäminen yhdessä muodostavat monipuolisemman kehyksen kyberturvallisuuden tarkastelulle. On kuitenkin arvioitava, kuinka paljon näitä lähestymistapoja tulisi yhdistää. Voiko esimerkiksi liiallinen turvallistaminen haitata riskiyttämisen käytännön hyötyjä?

Uhkien ja riskien hallintakeinoilla on myös merkittävä rooli kyberturvallisuudessa. Uhkien hallinnassa painotetaan ennaltaehkäisyä, jonka avulla pyritään estämään kyberhyökkäyksiä. Ennaltaehkäisy voi tarkoittaa esimerkiksi kriittisten järjestelmien parempaa suojaamista tai tiiviimpää kansainvälistä yhteistyötä. Näiden keinojen avulla pyritään estämään uhkien toteutumista. Tulevaisuudessa on kuitenkin syytä tarkastella, onko ennaltaehkäisy yksinään riittävä keino torjumaan kyberuhkia vai tulisiko sen rinnalle kehittää myös muita hallintakeinoja niiden tehokkaammaksi ehkäisemiseksi.

Riskien hallinnassa painotetaan puolestaan järjestelmien heikkouksien tunnistamista ja vähentämistä, mikä vaatii jatkuvaa varautumista ja kykyä sopeutua muutoksiin. Tällaisia hallintakeinoja ovat esimerkiksi varajärjestelmien luominen ja kyberturvallisuustietoisuuden lisääminen. Sosiaalisten riskien, kuten disinformaation ja osaamisvajeiden, hallinta myös osoittaa, kuinka tiiviisti kyberturvallisuus liittyy yhteiskunnan rakenteisiin. Tästä syystä sitä

tulisi käsitellä sekä teknisenä että yhteiskunnallisena ilmiönä. Uhkien ja riskien hallintakeinojen voidaan nähdä täydentävän toisiaan, kun niitä tarkastellaan kokonaisuutena. Niiden välistä suhdetta voitaisiin merkittävästi yhtenäistää, jotta kyberturvallisuuden hallinta olisi kokonaisvaltaisempaa.

Yhteiskunnallisen resilienssin vahvistamisella on keskeinen merkitys kyberturvallisuuden hallinnassa. Teknologisten suojauskeinojen lisäksi on tärkeää vahvistaa ihmisten kykyä tunnistaa ja varautua kybertoimintaympäristön haasteisiin. Esimerkiksi kansalaisten kriittisellä medialukutaidolla on merkittävä vaikutus disinformaation ja hybridivaikuttamisen torjumisessa. Ihmisten vahva kyky arvioida tietojen todenmukaisuutta tukee yhteiskunnan resilienssiä. Tämä kyky on riippuvainen kansalaisten osaamisesta, mikä puolestaan edellyttää vahvaa kyberosaamista ja mediakriittisyyttä. Koulutusjärjestelmän rooli on keskeinen, sillä se tukee kansalaisten valmiuksia toimia turvallisesti digitaalisessa ympäristössä ja kehittää kriittistä medialukutaitoa. Kyberosaamisen vahvistaminen on myös keskeinen kyberturvallisuuden hallintakeino, joka vahvistaa yhteiskunnan resilienssiä. Se voi myös merkittävästi pienentää ihmisten ja organisaatioiden alttiutta kyberriskeille.

Yhteiskunnallisen resilienssin kehittäminen on erityisen tärkeää, koska monet kyberuhat ja riskit kytkeytyvät yhteiskunnallisiin ilmiöihin. Resilienssin kehittämisessä tulee ottaa entistä vahvemmin huomioon se, että kyberturvallisuus ei ole vain tekninen ongelma, vaan osa laajempaa sosiaalista ja poliittista kokonaisuutta. Tässä korostuu tarve rakentaa resilienssiä kestävällä ja kokonaisvaltaisella tavalla. Resilienssi ei ole tärkeä vain siksi, että se ehkäisee uhkien ja riskien toteutumista, vaan myös siksi, että se tukee yhteiskunnan kykyä toipua nopeasti niiden vaikutuksista. Tämä palautumiskyky on keskeinen tekijä nykypäivän yhteiskunnassa, sillä kyberturvallisuusympäristö on monimutkainen ja siihen liittyvät uhkat ja riskit kasvavat jatkuvasti.

Kyberturvallisuudessa on tärkeää löytää tasapaino sekä ennakoivien että reagoivien lähestymistapojen välillä. Ennakoivat toimet, kuten järjestelmien suojaaminen ja kansainvälisen yhteistyön vahvistaminen, voivat estää uhkien toteutumisen, mutta ne eivät yksinään riitä kyberhyökkäysten torjumiseen. Reagoivat toimet ovat olennainen lisä ennakoiviin toimiin, sillä ne auttavat lieventämään riskien vaikutuksia tilanteissa, joissa ennaltaehkäisy ei ole ollut riittävää. Tulevaisuudessa on tärkeää arvioida, milloin ennakoivien toimien painottaminen on tarpeellista ja milloin taas reagoivat toimet on otettava käyttöön. Kyberturvallisuus ei saisi keskittyä vain uhkien torjumiseen, vaan riskien hallintaan on

kiinnitettävä entistä enemmän huomiota päätöksenteossa. Tämä edellyttää, että poliittisessa päätöksenteossa otetaan huomioon kyberturvallisuuden kokonaisvaltainen hallinta ja sen moninaiset näkökulmat.

Kyberturvallisuus ei ole pelkästään tekninen ongelma, vaan se on myös yhteiskunnallinen ja poliittinen kysymys, joka vaatii kokonaisvaltaista lähestymistapaa. Se on vahvasti sidoksissa yhteiskunnan rakenteisiin ja yleisesti kansalliseen turvallisuuteen. Tästä syystä turvallistaminen ja riskiyttäminen tarjoavat hyödylliset kehykset kybertoimintaympäristön ilmiöiden ymmärtämiseksi ja hallitsemiseksi. Nämä teoriat auttavat ymmärtämään, kuinka kyberuhkat ja -riskit kytkeytyvät laajempiin yhteiskunnallisiin ja poliittisiin kysymyksiin ja miten niitä tulisi käsitellä osana kansallista ja kansainvälistä turvallisuutta. Tällainen kokonaisvaltainen lähestymistapa on tulevaisuudessa välttämätön, jotta kyberturvallisuus voidaan ottaa osaksi laajempaa turvallisuuden hallintaa ja yhteiskunnallista kehitystä.

8.2 Tulevia tutkimusaiheita

Tarkastelun tulokset osoittavat tässä tutkimuksessa, kuinka kyberturvallisuus on paitsi tekninen, myös vahvasti yhteiskunnallinen ja poliittinen kysymys, joka kytkeytyy laajasti yhteiskunnan rakenteisiin ja kansalliseen turvallisuuteen. Turvallistaminen ja riskiyttäminen tarjoavat tässä tutkimuksessa hyvän kehyksen kyberuhkien ja -riskien ymmärtämiseen ja hallintaan, korostaen kokonaisvaltaisen lähestymistavan merkitystä muuttuvassa toimintaympäristössä. Luvussa 2 toin esille, kuinka aiempi kyberturvallisuuden tutkimus on painottunut teknisen tietoturvan näkökulmasta tehtyyn tutkimukseen ja erityisesti siihen, miten kyberhyökkäyksiä voidaan havaita ja estää tietojärjestelmissä. Vaikka kyberriskejä on selkeästi tutkittu vähemmän, niiden merkitys kasvaa jatkuvasti. Tutkimustiedon puute taas vaikeuttaa kyberriskien tehokasta ennustamista ja hallintaa. Tästä syystä kyberriskien vähäinen tutkimus ja niiden kasvava merkitys korostavat tämän tutkimuksen ajankohtaisuutta, sillä se tarjoaa uusia näkökulmia kyberturvallisuuden yhteiskunnallisten ja kansallisten vaikutusten ymmärtämiseen ja hallintaan Suomessa.

On kuitenkin huomioitava, että vaikka tämä tutkimus tarjoaa kattavaa tietoa kyberturvallisuuden yhteiskunnallisista vaikutuksista, analyysissa käytetyt Suomen kansalliset riskiarviot ja kyberturvallisuusstrategiat rajoittavat tutkimuksen laajuutta. Sisäministeriön työryhmät ovat laatineet riskiarviot vuosilta 2015, 2018 ja 2023 ja turvallisuuskomitean työryhmät ovat laatineet kyberturvallisuusstrategiat vuosilta 2013 ja 2019. Koska kyseiset

asiakirjat ovat valtionhallinnon laatimia, ne edustavat ensisijaisesti viranomaisten näkökulmaa kyberturvallisuuteen. Tämän vuoksi voidaan jättää huomioimatta muiden toimijoiden, kuten yritysten tai kansalaisten, näkemyksiä tai tarpeita. Lisäksi aineisto kattaa ajallisesti vain rajatun tarkastelujakson noin kymmenen vuoden ajalta, mikä saattaa heikentää johtopäätösten yleistettävyyttä jatkuvasti muuttuvassa kyberuhkien ja riskien toimintaympäristössä.

Tutkimuksessani tuli esille monia tärkeitä kyberturvallisuuden uhkiin ja riskeihin liittyviä tekijöitä. Tulevissa tutkimuksissa voitaisiin syventyä tarkastelemaan näitä yksittäisiä tekijöitä vielä syvällisemmin ja selvittää, miten ne vaikuttavat kyberturvallisuuteen. Erityisesti kyberturvallisuuden yhteiskunnallisia ja eettisiä ulottuvuuksia olisi tärkeää tutkia syvällisemmin, kuten yksilön oikeuksia, tietosuojaa ja valtion roolia kansalaisten digitaalisen turvallisuuden turvaajana. Kyberuhkien kasvaessa yhteiskunnassa on myös tärkeää pohtia, kuinka turvallisuus ja yksilönvapaudet voidaan tasapainottaa. Miten valtiot voivat estää kyberhyökkäykset ilman, että ne loukkaavat kansalaisten perusoikeuksia, kuten sananvapautta tai yksityisyyttä? Tällainen tutkimus voisi aloittaa tärkeän keskustelun siitä, kuinka kyberturvallisuus voidaan sisällyttää osaksi laajempaa yhteiskunnallista ja poliittista diskurssia, jossa otetaan huomioon niin turvallisuusnäkökulmat kuin eettiset ja oikeudelliset rajat. Tämä puolestaan avaisi uusia näkökulmia siihen, kuinka kyberturvallisuus on paitsi tekninen myös yhteiskunnallinen ja inhimillinen kysymys, joka vaikuttaa syvällisesti yksilöiden ja yhteisöjen hyvinvointiin.

9 Aineistolähteet

Sisäministeriö. 2016. *Suomen kansallinen riskiarvio 2015.* Sisäministeriön julkaisu 3/2016. Sisäinen turvallisuus. Helsinki: Sisäministeriö.

Sisäministeriö. 2019. *Kansallinen riskiarvio 2018.* Sisäministeriön julkaisuja 2019/5. Sisäinen turvallisuus. Helsinki: Sisäministeriö.

Sisäministeriö. 2023. *Kansallinen riskiarvio 2023.* Sisäministeriön julkaisuja 2023/4. Sisäinen turvallisuus. Helsinki: Sisäministeriö.

Turvallisuuskomitea. 2013. *Suomen kyberturvallisuusstrategia.* Valtioneuvoston periaatepäätös. Helsinki: Turvallisuuskomitea.

Turvallisuuskomitea. 2019. *Suomen kyberturvallisuusstrategia 2019.* Valtioneuvoston periaatepäätös. Helsinki: Turvallisuuskomitea.

10 Tutkimuskirjallisuus

Backman, Sarah. 2022. Risk vs. threat-based cybersecurity: the case of the EU. *European security* 32:1, 85-103.

Balzacq, Thierry. 2011. *Securitization Theory. How security problems emerge and dissolve.* Oxon: Routledge.

Balzacq, Thierry; Léonard, Sarah & Ruzicka, Jan. 2016. 'Securitization' revisited: theory and cases. *International Relations* 30:4, 494–531.

Barthwal-Datta, Monika. 2012. *Understanding security practices in South-Asia securitization theory and the role of non-state actors.* Oxon: Routledge.

Björck, Fredrik ym. 2015. Cyber Resilience – Fundamentals for a Definition. Teoksessa Rocha, Alvaro ym. *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353. New York: Springer Cham.

Buzan, Barry ym. 1998. *Security. A New Framework For Analysis.* Boulder-London: Lynne Rienner Publishers.

Cains, Mariana; Flora, Liberty; Taber, Danica; King, Zoe & Henshel Diane. 2022. Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis* 42:8, 1643-1669.

Carley, Kathleen M. 2020. Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory* 26, 365–381.

Caron, Filip. 2021. Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal* 36:2, 193-217.

Corry, Olaf. 2012. Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change. *Millennium: Journal of International Studies* 40:2, 235–258.

Cremer, Frank; Sheehan, Barry; Fortmann, Michael; Kia, Arash N. Kia; Mullins, Martin; Murphy, Finbarr & Materne, Stefan. 2022. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice* 47:3, 698–736.

Dacorogna, Michel & Kratz, Marie. 2022. Special Issue “Cyber Risk and Security”. *Risks* 10:6.

Eling, Martin & Wirfs, Jan. 2018. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272:3, 1109-1119.

Estève, Adrien. 2021. Preparing the French military to a warming world: climatization through riskifcation. *International Politics* 58, 600–618.

Friis, Karsten & Ringsmose, Jens. 2016. *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives.* London: Routledge.

Hansen, Lene & Nissenbaum, Helen. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53, 1155–1175.

Hardy, Cynthia & Maguire, Steve. 2016. Organizing risk: Discourse, power, and "riskification". *The Academy of Management review* 41:1, 80-108.

Jansson, Saara & Sihvonen, Tanja. 2018. Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä* 41:1, 1-28.

Jokinen, Arja; Juhila, Kirsi & Suoninen Eero. 2004. *Diskurssianalyysin aakkoset.* Tampere: Vastapaino.

Liikenne- ja viestintäministeriö. 2008. *Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi.* Liikenne- ja viestintäministeriön julkaisuja 62/2008. Helsinki: Liikenne- ja viestintäministeriö.

Limnéll, Jarno; Majewski, Klaus & Salminen, Mirva. 2014. *Cyber Security for Decision Makers*. Helsinki: Docendo Oy.

Orlando, Albina. 2021. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. *Risks* 9:10.

Rhinard, Mark ym. 2024. Understanding variation in national climate change adaptation: Securitization in focus. *Politics and Space* 42:4, 676–696.

Stritzel, Holger. 2007. Towards a Theory of Securitization:Copenhagen and Beyond. *European Journal of International Relations* 13:3, 357–383.

Stritzel, Holger. 2014. *Security in Translation: Securitization Theory and the Localization of Threat.* Basingstoke: Palgrave Macmillan.

Taureck, Rita. 2006. Securitization theory and securitization studies. *Journal of international relations and development* 9:1, 53-61.

Valtioneuvoston kanslia. 2012. *Suomen turvallisuus- ja puolustuspolitiikka 2012: Valtioneuvoston selonteko.* Valtioneuvoston kanslian julkaisusarja 5/2012. Helsinki: Valtioneuvoston kanslia.

Valtioneuvoston kanslia. 2024. *Suomen kyberturvallisuusstrategia 2024–2035.* Valtioneuvoston kanslian julkaisuja 2024/11. Helsinki: Valtioneuvoston kanslia.

Wæver, Ole. 1995. “Securitization and Desecuritization”. Teoksessa Ronnie D. Lipschutz (toim.): On security. New York: Columbia University Press.