LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

KYBER JA KANSALLINEN DIGITAALINEN TURVALLISUUS -

ONTOLOGISEN TURVALLISUUDEN NÄKÖKULMA SUOMEN KYBERTURVALLISUUSSTRATEGIOIHIN

Arttu Markkanen

Pro gradu -tutkielma

Politiikkatieteet, kansainväliset suhteet

Lapin yliopisto

2025

Lapin yliopisto

Tiedekunta: Yhteiskuntatieteiden tiedekunta

Työn nimi: Kyber ja kansallinen digitaalinen turvallisuus – Ontologisen turvallisuuden näkökulma Suomen kyberturvallisuusstrategioihin

Tekijä: Arttu Markkanen

Koulutusohjelma / opetuskokonaisuus / oppiaine: Politiikkatieteet / Kansainväliset suhteet

Ohjaaja: Yliopistonlehtori Karim Maiche

Työn laji: Pro gradu -tutkielma

Sivumäärä, liitteiden lukumäärä: 61 sivua

Vuosi: 2025

Tiivistelmä:

Tässä pro gradu -tutkielmassa tarkastelen ontologista turvallisuutta vahvistavia tekijöitä Suomen kyberturvallisuusstrategioissa 2013, 2019 ja 2024–2035. Tutkielmassani vastaan siihen kysymykseen, millä keinoilla Suomi vahvistaa omaa ontologista turvallisuuttaan kyseisissä strategioissa. Tutkielman tarkoitus on ymmärtää valtion ontologiseen turvallisuuteen vaikuttavia tekijöitä painottuen kyberturvallisuuteen ja antaa uudenlaisia näkökulmia kyberturvallisuuden tarkasteluun.

Tutkielma on laadullinen tutkimus, jonka aineistona toimivat Suomen kyberturvallisuusstrategiat 2013, 2019 ja 2024–2035. Aineiston analysoimiseksi on käytetty laadullista sisällönanalyysia ja ontologisen turvallisuuden teoreettista kehystä. Ontologinen turvallisuus keskittyy toimijan kokemukseen eksistentiaalisesta varmuudesta, jatkuvuudesta ja ennakoitavuudesta, olemuksen turvallisuuteen. Ontologinen turvallisuus tarjoaa mahdollisuuden tarkastella kyberturvallisuutta uudesta näkökulmasta, joka tarjoaa erilaisia ulottuvuuksia kyberturvallisuuden ilmiöiden ja niiden yhteiskunnallisten vaikutusten ymmärtämiseen.

Tutkielman tulokset koostuvat kolmesta kokonaisuudesta, jotka vahvistavat omilta osiltaan Suomen ontologista turvallisuutta, 1) kansallinen, 2) kansainvälinen ja 3) yksilö. Nämä kolme kokonaisuutta ovat vuorovaikutuksessa keskenään, eivätkä yksin riitä turvaamaan ontologista turvallisuutta. Kyberturvallisuutta ei tule nähdä erillisenä turvallisuuden tai yhteiskunnan ilmiönä. Kyberturvallisuus on yksi kansallisen turvallisuuden ulottuvuus ja osa kansallista kokonaisturvallisuutta mutta sillä on myös kansainvälisiä ja yksilöön vaikuttavia ulottuvuuksia. Kyberturvallisuutta rakentavat yksilöt, yhteisöt ja julkiset instituutiot, eikä kyberturvallisuutta voida sivuuttaa pohdittaessa valtion turvallisuutta. Kyberturvallisuusstrategioissa ilmenevät ontologista turvallisuutta vahvistavat kokonaisuudet eivät kuitenkaan absoluuttisesti yksinomaan ilmennä valtion kokonaisvaltaista turvallisuuden kokemista, turvallisuuden tilaa tai turvallisuuspolitiikkaa.

Avainsanat: Kyberturvallisuus, ontologinen turvallisuus, turvallisuus, identiteetti, valtio, laadullinen tutkimus, sisällönanalyysi

SISÄLLYS

1 JOHDANTO

"We are no longer securing just computers – we are securing the society"

– Mikko Hyppönen

Teknologisen kehityksen myötä tieto- ja viestintätekniikka on kehittynyt viime vuosikymmenien aikana merkittävästi. Digitaaliset laitteet ja järjestelmät hallinnoivat dataa globaalisti, joita käyttävät yksityiset henkilöt, yritykset, järjestöt sekä valtiot. Tämän kehityksen myötä myös turvallisuus ulottuu teknologisiin ratkaisuihin sekä digitaalisiin laitteisiin ja järjestelmiin. Tieto, joka on aikaisemmin sijainnut asiakirjoissa arkistojen uumenissa, sijaitsee nykyään digitaalisissa järjestelmissä ja laitteissa. Tämän tiedon siirtyminen digitaalisiin järjestelmiin on luonut tarpeen turvata digitaaliset laitteet ja järjestelmät, mutta myös muuttanut ihmisten käsitystä ja kokemusta turvallisuudesta.

Digitaalisesta ympäristöstä on tullut yhä tärkeämpi osa yhteiskuntaa. Siellä sijaitsee tieto sekä sen käyttäjät, ihmiset. Digitaalisen maailman kautta on yhä helpompi vaikuttaa myös fyysiseen maailmaan, eikä maantieteelliset valtioiden rajat ole esteenä globaalille vaikuttamiselle. Digitaalisen maailman turvallisuudesta – kyberturvallisuudesta – on tullut yhä kokonaisvaltaisempi turvallisuuden ulottuvuus, joka liittyy läheisesti fyysiseen maailmaan ja yhä läheisemmin yhteiskuntiin. Digitaalisella turvallisuudella on vaikutuksia yksittäisen ihmisen turvallisuuden tunteeseen, mutta se vaikuttaa myös valtioiden turvallisuuspolitiikkaan sekä valtioiden välisiin suhteisiin. Enää ei ole kyse vain tietokoneiden turvaamisesta, vaan laajemmin kokonaisten yhteiskuntien suojaamisesta.

Digitalisoituvissa yhteiskunnissa kyberturvallisuus onkin noussut keskeiseksi osaksi valtioiden kansallista turvallisuutta, kansainvälisiä suhteita, taloudellista tasapainoa ja kansalaisten elämää. Yhteiskunnat digitalisoituvat kiihtyvällä tahdilla ja kyberturvallisuuden tarkoituksena on turvata yhteiskuntaa sekä sen toimintakykyä vihamieliseltä kybervaikuttamiselta ja tietoverkoissa tapahtuvalta tiedustelulta (Sisäministeriö, kyberturvallisuus, intermin.fi). Myös Suomessa yhteiskunnan kriittisten toimintojen jatkuvuus, valtiollinen suvereniteetti ja kansalaisten arjen turvallisuus ovat yhä enemmän riippuvaisia digitaalisista järjestelmistä ja niiden toimivuudesta. Tämän kehityksen myötä myös Suomen kyberturvallisuusstrategiat osana valtion muita turvallisuusstrategioita ovat tulleet keskeisiksi dokumenteiksi, joissa hallitaan erilaisia kybertoimintaympäristöön liittyviä uhkia ja rakennetaan kansallista turvallisuuden tunnetta.

Kyberturvallisuudella on myös vaikutuksia valtioiden välisiin suhteisiin. Kybertoimintaympäristö vaikuttaa globaalisti, eikä toimijoilla ole maantieteellisiä rajoitteita toiminnalleen. Kybertoimintaympäristön epävarmuus on valtioille huolenaihe, joka vaikuttaa kansainvälisessä politiikassa. Ennustettavuus, jatkuvuus ja eksistentiaalinen varmuus on valtioille edellytys selviytymiselle kansainvälisessä järjestelmässä. Kybertoimintaympäristö haastaa valtioiden kykyä hallita tätä ennustettavuutta, jatkuvuutta ja eksistentiaalista varmuutta. Siksi valtioiden turvallisuustarpeiden ymmärtäminen on tärkeää, jotta voidaan ymmärtää myös kansainvälisen järjestelmän dynamiikkoja.

Tässä tutkielmassa tutkin miten ontologinen turvallisuus – yksilöiden ja yhteisöjen kokemus jatkuvuudesta, ennakoitavuudesta ja eksistentiaalisesta varmuudesta – rakentuu ja ilmenee Suomen kyberturvallisuusstrategioissa. Tutkielmassa perehdyn suomalaiseen yhteiskuntaan vaikuttaviin kybertoimintaympäristön ilmiöihin ja kuinka ne vaikuttavat suomalaisen yhteiskunnan turvallisuuden tunteeseen. Tarkastelen, miten nämä kyberympäristössä ilmenevät ilmiöt vaikuttavat Suomen kokemaan ja määrittelemään turvallisuuteen sekä millä keinoilla Suomi valtiona vahvistaa ja ylläpitää sen kokemaa turvallisuuden tunnetta.

Turvallisuutta ja turvallisuuden tunnetta hahmottamaan, käytän tutkielmassa ontologisen turvallisuuden teoriaa, joka syventyy turvallisuuden olemukseen ja turvallisuuden tunteelliseen kokemiseen, perinteisen fyysisen turvallisuuden kokemisen sijaan. Ontologinen turvallisuus keskittyy toimijan kokemukseen eksistentiaalisesta varmuudesta, jatkuvuudesta ja ennakoitavuudesta. Ontologinen turvallisuus perinteisesti keskittyy yksilön kokemaan turvallisuuden tunteeseen psykologisesta näkökulmasta. Tässä tutkielmassa sovellan tätä turvallisuuden kokemista valtiotasolle. Ontologisen turvallisuuden teorian avulla tämä tutkielma keskittyy valtion kokemaan turvallisuuteen ja niiden tarpeeseen kokea turvallisuutta sekä ylläpitää turvallisuutta. Ontologisen turvallisuuden teoria mahdollistaa kyberturvallisuusstrategioiden tarkastelun osana laajempaa pyrkimystä ylläpitää yhteiskunnallista jatkuvuuden tunnetta nopeasti muuttuvassa digitaalisessa maailmassa sekä ymmärryksen valtion tarpeista kokea turvallisuutta.

Perinteisessä turvallisuustutkimuksessa ja kansainvälisessä politiikassa valtioita pidetään pääasiallisina turvallisuuden tuottajina ja ylläpitäjinä omalla maantieteellisellä alueellaan, jotka pyrkivät turvaamaan oman suvereniteettinsa (Mearsheimer 2009, 242). Nykypäivänä, etenkin digitaalisessa toimintaympäristössä, valtion keinoja tarjota turvallisuutta haastetaan jatkuvasti erinäisin keinoin ja eri toimijoiden toimesta. Ontologisen turvallisuuden teoria pyrkii tutkimaan, miten valtio pystyy ylläpitämään perinteisen roolinsa pääasiallisena turvallisuuden ja yleisen järjestyksen tuottajana yksilöille ja kansalle (Lupovici 2023, 155). Tämän teoreettisen näkökulman

soveltaminen kyberturvallisuusstrategioiden tarkasteluun avaa uudenlaisen tulkinnan siitä, miten valtio pyrkii paitsi suojelemaan infrastruktuureja ja tietojärjestelmiä, mutta myös luomaan ja ylläpitämään tietynlaista yhteiskunnallista tunnetilaa ja maailmankatsomusta sekä näkemystä valtion paikasta maailmassa.

Tutkielmani tutkimuskysymys on; millä tavoin Suomi vahvistaa ontologista turvallisuutta kyberturvallisuusstrategioissa? Tutkimuskysymyksen avulla on tarkoitus tutkia millä eri keinoilla Suomi rakentaa ja vahvistaa omaa ontologista turvallisuuttaan kyberturvallisuusstrategioissa. Tarkoitus on myös tarkastella mitkä erilaiset kyberympäristössä esiintyvät ilmiöt koetaan uhkaavan tätä turvallisuutta, sekä miten Suomi niihin varautuu. Kybertoimintaympäristössä esiintyviä ilmiöitä ovat muun muassa kybervakoilu, tekoäly, kyberrikollisuus, informaatiovaikuttaminen, tietomurrot, palvelunestohyökkäykset ja kybersodankäynti. Tutkimuskysymyksen ympärille olen koostanut pienempiä avustavia kysymyksiä, jotka auttavat hahmottamaan tutkittavaa ilmiötä ja kokonaisuutta. Näitä kysymyksiä ovat: minkälainen on Suomen kyberturvallisuuden tila? Minkälainen on Suomen identiteetti ja mihin Suomi identifioituu? Ketkä ovat Suomen poliittisia ystäviä ja vastustajia?

Kyberuhkien hahmottamiseksi ja konkretisoimiseksi tutkielmassa käytän konkreettisia esimerkkejä kyberuhkista, kuten kybervakoilua tai kyberrikollisuutta. Näitä esimerkkejä käsitellään muun muassa uutisartikkeleiden muodossa. Tarkoitus ei ole analysoida tapauksia sen syvällisemmin, vaan käyttää niitä apuna hahmottamaan kyberuhkien moniulotteisuutta ja konkreettisia vaikutuksia fyysiseen maailmaan. Näiden esimerkkien on tarkoitus ilmentää kyberuhkien käytännön konkreettisia seurauksia turvallisuuden tunteeseen, niin yksilöille kuin valtiollekin.

Tutkielman aineistona toimivat *Suomen kyberturvallisuusstrategiat 2013*, *2019* sekä *2024–2035*. Kyseiset strategiat tarjoavat mielenkiintoisen aineiston, jonka kautta voidaan tarkastella, miten valtio viestii kyberturvallisuudesta kansalaisilleen, millaisia uhkakuvia se rakentaa, ja millaisia identiteettejä se tarjoaa toimijoille digitaalisen toimintaympäristön kansalaisina ja suojeltavina subjekteina. Kyberturvallisuusstrategiat eivät ole vain teknisiä tai hallinnollisia asiakirjoja, vaan ne heijastavat myös syvempää käsitystä turvallisuudesta, erilaisista uhkista ja ympäröivästä maailmasta. Kyberturvallisuusstrategiat ovat osa valtion turvallisuusstrategioita, joita ohjaa *Yhteiskunnan turvallisuusstrategia (2025).*

Tutkielmani on laadullinen tutkimus. Aineiston analysoimiseksi käytän tutkielmassa laadullista sisällönanalyysia. Laadullinen sisällönanalyysi on tekstianalyysin muoto, joka keskittyy tekstissä sisältyviin merkityksiin. Näiden tekstissä sisältyvien merkityksien löytämiseksi aineisto järjestetään selkeään ja tiiviiseen muotoon ilman, että tekstin sisältämää tietoa kadotetaan. Laadullinen

sisällönanalyysi toimii tutkielmani analyysityökaluna, jonka avulla hajanaisesta aineistosta on mahdollista luoda selkeää, tiivistä ja yhtenäistä informaatiota tutkimuskysymykseen vastaamiseksi. (Tuomi & Sarajärvi 2018, 122.)

Aiempi tutkimus (mm. Jansson & Sihvonen 2018; Lehto & Limnell 2021; Lehto, Limnell, Kokkomäki, Pöyhönen, Salminen 2018; Keinonen 2023) on tarkastellut Suomen kyberturvallisuusstrategioita teknologisten ratkaisujen, riskienhallinnan, kokonaisturvallisuuden, hallinnollisten ja johtamisen toimintamallien näkökulmista. Ontologisen turvallisuuden teoreettinen viitekehys mahdollistaa kokonaisvaltaisen turvallisuuden tunteen ja yhteiskunnallisen jatkuvuuden ja eheyden tarkastelun kyberturvallisuusstrategioissa. Ontologisen turvallisuuden näkökulma auttaa myös ymmärtämään valtion omaa näkemystä itsestään ja sen kansainvälistä asemaa. Tämän tutkielman tavoitteena on ymmärtää, miten turvallisuuden tunnetta tuotetaan Suomen kyberturvallisuusstrategioissa ja miten se vaikuttaa yhteiskunnalliseen turvallisuuteen, luottamukseen ja kansalliseen identiteettiin digitaalisena aikana.

Seuraavassa luvussa esittelen tutkielmassani käyttämää teoreettista viitekehystä sekä sitä tukevia käsitteitä ja miten ne soveltuvat valitsemaani tutkimusaiheeseen. Teoreettisen viitekehyksen jälkeen esittelen valitsemani aineiston ja analyysimenetelmän. Tutkielmani tulokset koostuvat kolmesta luvusta ja kokonaisuudesta, joiden avulla vastaan asettamaani tutkimuskysymykseen. Luvuissa analysoin ja pohdin kyseisiä kokonaisuuksia tarkemmin teoreettisen viitekehyksen avulla sekä käyttäen avukseni havaintojani aineistosta. Tutkielman lopussa pohdin vielä mahdollisia jatkotutkimusaiheita ja tutkittavan ilmiön mahdollisia kehityskulkuja sekä tiivistän tutkielman keskeisen sisällön ja argumentoin löytämäni keskeisimmät havainnot.

2 SUOMEN KANSALLINEN KYBERTURVALLISUUS JA ONTOLOGINEN TURVALLISUUS

2.1 Suomen kansallinen turvallisuus

Kansallinen turvallisuus on käsitteenä abstrakti ja sille ei voi tehdä yksiselitteistä määritelmää. Kansallisen turvallisuuden käsite sekä sen määritelmä on aina yhteiskunnan tilanne- ja kontekstisidonnainen. (Martelius 2024, 112). Kansallinen turvallisuus määrittyy usein uhkien kautta, jotka vaikuttavat koko yhteiskuntaan. Näitä uhkia ovat muun muassa terrorismi, vakoilu, vieraan valtion vahingollinen toiminta, kyberuhkat sekä kriittiseen infrastruktuuriin vaikuttavat uhkat. (Sisäministeriö, kansallinen turvallisuus, intermin.fi.) Kansallinen turvallisuus on yhä enemmän muodostumassa eri valtioiden turvallisuusstrategioiden keskeiseksi, lainsäädännössäkin tunnustetuksi käsitteeksi. Suojeltavana kohteena on voimassa oleva yhteiskunta- ja oikeusjärjestys ja viime kädessä yhteiskunnan olemassaolo. (Martelius 2024, 113.) Yhteiskunnassa suojeltavat arvot ovat usein abstrakteja (kuten hyvinvointi, tasa-arvo, turvallisuus, yksilönvapaus) tai sen toimintaperiaatteeseen liittyviä (kuten itsenäisyys, demokratia, oikeudenmukaisuus). Näitä arvoja järjestetään eri perusteilla ja ne suhteutetaan toisiinsa muun muassa kulttuurista ja historiasta johtuen. (Limnell, Majewski, Salminen 2014.) Konkreettisimmillaan, kansallinen turvallisuus on valtion suvereniteetin ja alueellisen koskemattomuuden turvaamista, jolloin on kyse valtion ja suvereenin yhteiskunnan olemassaolosta sekä uhasta tämä yhteiskunnan kansalaisille (Martelius 2024, 113). Kansallinen turvallisuus kattaa koko suomalaisen yhteiskunnan turvallisuuden ja Suomen suvereniteetin. Kansallinen turvallisuus käsitteenä on liikkeessä koko ajan ja se on suhteessa aikaan sekä Suomen toiminta- ja uhkaympäristöön. (Sisäministeriö, kansallinen turvallisuus, intermin.fi.)

Kansallisen turvallisuuden käsitteellä on erilaisia ulottuvuuksia, joiden avulla ilmiötä voidaan tarkastella. Käsitteenä kansallinen turvallisuus on altis poliittisille vaikutteille, koska käsitteessä yhdistyvät kansallisvaltio ja turvallisuus (Paasonen & Widlund 2021, 2–3). Käsitteellä on oikeudellisia sekä poliittisia ulottuvuuksia, jotka vaikuttavat sen käyttöön ja sisältöön. Kansallisen turvallisuuden poliittinen ulottuvuus keskittyy käsitteen funktioon. Käsitettä käytetään esimerkiksi ulko- ja turvallisuuspoliittisissa keskusteluissa ja ratkaisuissa. Käsitteen poliittisen ulottuvuuden takia, eri tahoilla on erilaisia mielipiteitä, siitä mitä käsite sisältää, miten sitä tulee käyttää ja mitä sen avulla voidaan tehdä. (ibid., 3.) Tämän takia poliittiset toimijat eivät usein halua määritellä käsitettä tarkasti, koska se mahdollisesti rajoittaisi käsitteen käyttöä poliittisessa keskustelussa (ibid., 3). Tästä nouseekin kysymys kansallisen turvallisuuden käsitteen määrittelystä. Kuka määrittelee käsitteen ja

kenen etuja se palvelee? Demokraattisessa valtiojärjestelmässä avainasemassa on kansalaisten motivaatio vaatia valitsemiltaan kansanedustajilta turvallisuuteen liittyvien kysymysten ja ilmiöiden vahvaa ylläpitoa. Ilman kansalaisten motivaatiota ja osallistumista vaarana on, että kansallinen turvallisuus määritellään ja ylläpidetään usein pienen ja eliittisen asiantuntija- ja päätöksentekijäjoukon omaisuutena ja vallan työkaluna. (Huhtinen & Laitinen 2021, 70.)

Kansallisen turvallisuuden keskiössä on valtion selviytyminen kaikissa olosuhteissa. Tästä syystä valtiolla tulee olla oikeus tietyissä olosuhteissa hylätä kansalaisten subjektiivinen turvallisuus, jotta se varmistaa oman selviytymisensä. (Huhtinen & Laitinen 2021, 66–67.) Tässä selviytymisessä yleinen valtiollinen ja yhteiskunnallinen etu ohittaa yksilön edun. Tämänlainen kansallisen turvallisuuden politiikka sisältää niitä arvoja, joita on suojeltava ja ne päätökset sekä toimet, jotka ovat välttämättömiä valtion turvaamiseksi ja selviytymiseen. (ibid., 68.) Näihin suojeltaviin arvoihin vaikuttavat useat erilaiset seikat, kuten historia, kulttuuriperinne, maantiede, yhteiskuntajärjestys sekä muun muassa julkinen mielipide. Kansallisen turvallisuuden käsite onkin altis ajalle ja yhteiskunnalle. Kansallisen turvallisuuden intressit muuttuvat yhteiskuntien muuttuessa.

2.2 Kyberturvallisuutta kybertoimintaympäristössä

Suomen kielessä ei ole yhtä oikeaa vakiintunutta määrittelyä sanalle *kyber*. Käsitteelle ei ole maailmanlaajuisestikaan yhtä hyväksyttyä määritelmää. Sana kyber tulee kreikan kielestä sanasta *kybereo*, joka tarkoittaa ohjata, hallita, opastaa. Suomen kieleen sana kyber tulee englannista sanasta *cyber*, joka yhdistyy tietokoneiden kulttuuriin, informaatioteknologiaan ja virtuaaliseen todellisuuteen, Oxfordin sanakirjan mukaan. (Limnell 2014, 3.) Kyber yhdistetään yleensä tietotekniikkaan, digitaalisiin viestiyhteyksiin ja -järjestelmiin, tiedonsiirtoon ja tietojärjestelmiin sekä tietokoneisiin. Kyber -sanaa käytetään usein yhdyssanan osana, jonka avulla voidaan viedä fyysisen maailman ilmiö tai toiminto ihmisen luomaan digitaaliseen ympäristöön, kuten kybersodankäynti, kybervakoilu tai kyberrikollisuus. (Laari et al. 2019, 9.)

Digitaalisista tietojärjestelmistä muodostuvaa toimintaympäristöä kutsutaan *kybertoimintaympäristöksi*. Digitaalisten tietojärjestelmien lisäksi tähän toimintaympäristöön kuuluu fyysinen infrastruktuuri sekä kaikki muut toimijat, jotka ovat kybertoimintaympäristössä. Kybertoimintaympäristölle on ominaista, että datan ja informaation varastoinnissa, muokkaamisessa ja siirtämisessä käytetään elektronisia viestintäverkkoja. (Laari et al. 2019, 9.) Tämä kybertoimintaympäristö ei ole maantieteellisesti rajoitettu ja tämä hajauttaa käyttäjiä sekä

komponentteja. Esimerkiksi sosiaalisen median palvelimet saattavat sijaita yhdessä valtiossa, mutta käyttäjiä on ympäri maailmaa. Kybertoimintaympäristö on lähes kaikkien ulottuvilla maailmanlaajuisesti ja sinne voi päästä lähes kuka vain lukuisin eri tavoin. Tästä syystä kybertoimintaympäristö on haavoittuva useista kohdista. (Laari et al. 2019, 10–11.)

Kybertoimintaympäristöön kohdistuva uhka on *kyberuhka.* Kyberuhkat kohdistuvat kybertoimintaympäristöön ja toteutuessaan ne vaarantavat myös siitä riippuvaiset tekijät ja toiminnot. Kyberuhkat voivat kohdistua erilaisiin tietoaineistoihin tai niiden käyttäjiin. (Laari et al. 2019, 29.) Kyberuhkat voivat myös kohdistua fyysiseen toimintaympäristöön, jos niillä pyritään vaikuttamaan järjestelmien infrastruktuuriin ja aiheuttamaan materiaalisia vahinkoja ja fyysistä kärsimystä. Kyberuhkat voivat olla organisaatioille hyvin fataaleja ja niiden ydintoimintaan vaikuttavia. (ibid., 29.)

Kybertoimintaympäristön haavoittuvuuksia ja uhkia torjuu sekä ehkäisee *kyberturvallisuus*. Kyberturvallisuus on olennainen osa yhteiskunnan kokonaisvaltaista turvallisuutta (Lehto & Limnell 2021, 139). Kyberturvallisuudessa tavoitteena on luotettava ja turvattu kybertoimintaympäristö. Kyberturvallisuus on digitaalisten tietojen, verkkojen ja ohjelmistojen sekä fyysisen infrastruktuurin turvaamista koko niiden elinjakson ajan (Laari et al. 2019, 10). Kyberturvallisuus huomioi myös digitaalisten järjestelmien infrastruktuurin sekä erilaisten prosessien ja käyttäjien toiminnan. (Laukkanen 2018, 19). Kyberturvallisuus koostuukin ylläpitäjien ja käyttäjien välisestä suhteesta, jossa huomioidaan kybertoimintaympäristön vaikutukset niin digitaaliseen kuin fyysiseen maailmaan. (Laari et al. 2019, 10). Kyberturvallisuus ei ole koskaan valmista vaan sitä kehitetään jatkuvasti yhteistyössä eri toimijoiden kanssa. Suomessa kyberturvallisuuden kannalta keskeisimpiä toimijoita ovat muun muassa valtioneuvosto, liikenne- ja viestintäministeriö, keskusrikospoliisi, suojelupoliisi sekä digi- ja väestötietovirasto. Näiden lisäksi erilaisia kyberturvallisuuden keskeisiä toimijoita ovat elinkeinoelämän yritykset, oppilaitokset sekä erilaiset järjestöt. (ibid., 14).

Kybermaailma on nykyään läsnä kaikkialla ja sen vaikutus yhteiskunnan ja sen turvallisuuden kaikille tasoille on ilmeistä. Yksiselitteistä jakoa kybertoimintaympäristöön ja fyysisen maailman toimintaympäristöön ei voi, eikä kannata tehdä, koska kybertoimintaympäristön tapahtumilla on selkeitä seurauksia fyysiseen toimintaympäristöön ja arkipäiviemme toimivuus on riippuvainen bittien maailmasta. (Limnell, Majewski, Salminen 2014.)

2.3 Ontologinen turvallisuus teoreettisena viitekehyksenä

Tutkielman keskeisimmän teoreettisen viitekehyksen muodostaa ontologisen turvallisuuden teoria. Teorian kiinnostuksen kohteina ovat muun muassa suhteet, tunteet, uskomukset ja identiteetti. Ontologisen turvallisuuden teoria keskittyy olemuksen turvallisuuteen perinteisessä turvallisuustutkimuksessa keskitytyn fyysisen turvallisuuden sijaan, joka taas keskittyy selviytymiseen (Lupovici 2023, 154). Ontologinen turvallisuus keskittyy toimijan kykyyn suojella identiteettiään ja rutiinejaan sekä siten toimijan kykyyn säilyttää ja suojella itseään (ibid., 154). Epävarmuus itsestä ja ympäristöstä luo uhkan identiteetille. Epävarmuus luo vaikeuksia toimia, joka heijastuu yksilön omakuvaan. (Mitzen 2006, 345.) Ontologinen turvallisuus on tila tai tunne, joka saavutetaan, kun yksilöllä on selvät oletukset syy-seuraussuhteista, jotka määrittelevät tämän sosiaalista elämää. Ontologisen turvallisuuden avulla yksilö tietää miten toimia ja kuinka olla oma itsensä. (ibid., 345.) Yksilöt, jotka kokevat ontologista turvallisuutta pystyvät luomaan toimivia ja vakaita identiteettejä, jotka luovat järjestystä, ennustettavuutta ja varmuutta (Lupovici 2023, 154). Ontologinen turvallisuus on kehon turvallisuuden sijaan itsen turvallisuutta, joka on subjektiivinen kokemus ja tunne siitä, kuka tämä on. Tämä käsitys ja tunne itsestä vaikuttaa ja mahdollistaa tekoihin ja valintoihin. (Bachleitner 2023, 27.)

Ontologisen turvallisuuden käsite pohjautuu britannialaisen sosiologin Anthony Giddensin (1938–) ajatuksiin. Giddensin mukaan ontologinen turvallisuus on tunne ja kokemus asioiden ja tapahtumien jatkuvuudesta ja järjestyksestä, joka myös käsittää sellaisia asioita, jotka eivät ole ihmisen välittömässä havainto- ja vaikutuspiirissä (Heino 2018, 7). Giddensin ajattelu on saanut vaikutteita skotlantilaiselta psykiatrilta R.D.Laingilta (1927–1989), joka käsitteli töissään ontologisen turvallisuuden puutetta yksilöillä, eli ontologista turvattomuutta, psykologisena ilmiönä (Saurama, Nurmi & Heino 2020, 137). Ontologinen turvattomuus viittaa syvään lamauttavaan tilaan, jossa yksilö ei tiedä mihin uhkiin ja vaaroihin tulisi reagoida ja mitkä tulisi sivuuttaa. Tämä vaikuttaa yksilön kykyyn yksinkertaisesti selviytyä maailmassa. (Mitzen 2006, 345.)

Ontologinen turvallisuus perinteisesti soveltuu yksilön tarkasteluun ja sitä on käytetty psykologiassa sekä yhteiskuntatieteissä tarkastelemaan yksilön kokemaa turvallisuutta erilaisissa ilmiöissä. Ontologisen turvallisuuden käsite laajeni kuitenkin kollektiiveihin ja muun muassa kansainvälisten suhteiden tutkimukseen 1990-luvulla, jolloin laajennettiin ja syvennettiin turvallisuuden käsiteettä (Floyd 2024, 6). Etenkin kansainvälisten suhteiden professorin Jennifer Mitzenin artikkeli *”Ontological security in world politics: State Identity and the Security Dilemma”* (2006) nosti ontologisen turvallisuuden teorian kansainvälisen politiikan tutkimukseen. Mitzen pohtii

artikkelissaan, kuinka ontologisen turvallisuuden teoriaa on mahdollista käyttää valtioiden ja näiden turvallisuuskäsitysten ymmärtämiseen sekä miten valtioiden turvallisuustarpeita voidaan hahmottaa. Keskeisenä argumenttinaan Mitzen toteaa, että valtiot välittävät ontologisesta turvallisuudestaan yhtä paljon kuin fyysisestä turvallisuudestaan. (ibid., 7.)

Ontologisen turvallisuuden teoriaa sovelletaankin myös kansainvälisten suhteiden tutkimuksessa. Ontologisen turvallisuuden tutkimuksen nousu osaksi kansainvälisten suhteiden tieteenalaa liittyy laajemmin 1990-luvulla tapahtuneisiin muutoksiin. Kylmä sota oli päättynyt ja eurooppalaiset valtiot sekä kansainvälinen järjestys hakivat uutta muotoaan. Kylmän sodan päättyessä ja etenkin Neuvostoliiton hajoamisen jälkeen eurooppalaisten valtioiden piti määritellä uudelleen kansallinen turvallisuutensa ja yleisesti käsitys turvallisuudesta, joka oli kylmän sodan aikana perustunut sotilaalliseen uhkaan. Resurssit, jotka laitettiin kylmän sodan aikana sotilaallisen uhkan torjumiseen, piti allokoida uudelleen ei-sotilaallisiin uhkiin, kuten muun muassa huumeisiin, kansainväliseen muuttoliikkeeseen, ympäristöuhkiin sekä kansainväliseen köyhyyteen. (Baldwin 1995, 126.)

Valtiota pidetään perinteisessä turvallisuustutkimuksessa ja kansainvälisessä politiikassa pääasiallisena turvallisuuden tuottajana ja ylläpitäjänä. Valtio tarjoaa alueellaan sen sisällä oleville ihmisille alueen ja ympäristön elää. Valtio kuitenkin rajoittaa joissakin määrin ihmisten elämää määrittelemällä mikä yhteiskunnassa on oikein ja väärin, määrittäen yksilöiden ja instituutioiden oikeuksia ja vapauksia. Nyky-yhteiskunnassa, kuten aikaisemmin jo mainittuna, on yhä enemmän uhkia ja ilmiöitä, jotka haastavat yhteiskunnan valta-asemia ja järjestystä, jotka eivät aina ilmene fyysisinä, vaan muun muassa digitaalisina kybertoimintaympäristössä, kuten kyberrikollisuus. Tämä haastaa valtion perinteistä roolia turvallisuuden tuottajana, ja ontologinen turvallisuus pyrkiikin tutkimaan tätä asetelmaa, miten valtio pystyy ylläpitämään roolinsa pääasiallisena turvallisuuden ja yleisen järjestyksen tuottajana yksilöille ja kansalle. (Lupovici 2023, 155.) Valtiot pitävät ontologista turvallisuutta yhtä tärkeänä turvallisuuden ulottuvuutena, kuin fyysistä turvallisuuttaan. Ontologinen turvallisuus on perustarve, jota voidaan verrata fyysisen turvallisuuden tarpeeseen. (Mitzen 2006, 343.) Valtioiden tarve ontologiselle turvallisuudelle perustuu pelkoon kaaoksesta. Valtiot pyrkivät kontrolloituun sosiaalisesti järjestäytyneeseen ympäristöön. Tämä sosiaalisesti järjestäytynyt ympäristö voi esimerkiksi perustua konfliktille. Konfliktit luovat valtioiden identiteettiä ja toimivat yhdistävänä tekijänä valtion sisällä. Sosiaalisesti järjestäytymätön ympäristö taas luo ontologista turvattomuutta, jota valtiot haluavat välttää. (Mitzen 2006, 342–343.)

Ontologinen turvallisuus perinteisesti pyrkii selittämään yksilöiden turvallisuuden tarpeita ja tuntemuksia yksilön näkökulmasta. Ontologisen turvallisuuden käsitettä voidaan soveltaa myös kansainvälisten suhteiden tutkimuksessa valtioihin. Yhtä lailla kuin yksilöt kokevat ontologista

turvallisuutta, myös valtiot kokevat ja tarvitsevat ontologista turvallisuutta. Tämä valtioiden tarve ontologiselle turvallisuudelle perustuu niiden olemassaolon varmistamiseksi ja kaaoksen välttämiseksi. Tutkiakseen tätä valtion ontologista turvallisuutta on pystyttävä perustelemaan, miten valtio soveltuu teoriaan, joka on lähtökohtaisesti suunnattu yksilön ymmärtämiseen. Kansainvälisten suhteiden professori Jennifer Mitzen artikkelissaan "*Ontological Security in World Politics: State Identity and the Security Dilemma"* (2006) perustelee tätä kolmella tavalla.

> Valtiot koetaan maailmanpolitiikassa yksittäisinä toimijoina, joilla katsotaan olevan keho, jota ne suojelevat fyysisellä turvallisuudella. Tällä keholla viitataan valtion rajoihin, jotka muodostavat alueen, jonka sisällä valtio on olemassa. Valtion tarve ontologiselle turvallisuudelle kumpuaa myös sen kansalaisista. Kansalaiset yksilöinä tarvitsevat ontologista turvallisuutta, jotta voivat olla osa jotain suurempaa sosiaalista yhteisöä. Yhteiskunnan tulee olla kognitiivisesti vakaa, jotta yksilöt voivat muodostaa identiteettejä ja liittää niitä osaksi erilaisia sosiaalisia yhteisöjä. Tämänlaisen kuulumisen tunteen menettäminen uhkaa yksilön ontologista turvallisuutta ja täten valtioille on tärkeä pitää yllä kansallista identiteettiä eikä vain aluetta, jossa ihmiset vain fyysisesti ovat. Valtio luo myös kuvaa itsestään, jossa jokaisella kansalaisella on jonkinlainen suhde siihen. Ontologisen turvallisuuden soveltaminen valtioihin auttaa myös ymmärtämään mikroilmiöiden vaikutusta makrotason ilmiöihin ja kehityskulkuihin. Valtioiden ontologinen turvallisuus antaa sosiologisen pohjan tarkastella, muun muassa miksi valtio käyttäytyy kansainvälisessä politiikassa samalla tavalla vuosikymmenestä toiseen poliittisten päättäjien vaihtuessa. (Mitzen 2006, 351–353.)

Ontologisessa turvallisuudessa kodin (engl. *home*) käsite on keskiössä. Tästä voidaan käyttää myös käsitystä "*omasta paikasta maailmassa*". Koti on sosiaalinen ja materiaalinen ympäristö, joka ylläpitää ontologista turvallisuutta, jossa ihmiset saavat toteuttaa päivittäisi rutiinejaan. Kodissa ihmiset tuntevat olevansa vastuussa omasta elämästään ja vapaita valvonnasta. Koti on paikka, jossa toimijat voivat määritellä itse itsensä ja toteuttaa itseään ja täten kokea ontologista turvallisuutta ja rakentaa identiteettiään. (Lupovici 2023, 156.) Valtiot tarjoavat ihmisille rajojensa sisällä tämänlaisen abstraktin kodin, jossa ihmiset voivat harjoittaa rutiinejaan ja toteuttaa itseään. Valtiot ovat olemassa tuottaakseen järjestystä ja ennustettavuutta, sekä tehdäkseen yksilöiden elämästä ymmärrettävämpää. (ibid., 157.) Valtion olemassaolon ennustettavuus sekä sen luoma sosiaalinen järjestys luo ihmisille vapautta ja liikkumatilaa toteuttaa itseään – ontologista turvallisuutta yksilöille. Jos yksilö menettää tunteen kodista, joutuu se etsimään vaihtoehtoista uutta kotia jostain muualta (ibid., 156).

Luomalla yksilöille ”kodin”, jossa yksilöt voivat toteuttaa itseään ja rutiinejaan, luo valtio samalla narratiivia itsestään toimijana ja paikkana. Valtiot tarvitsevat ontologista turvallisuutta, jotta voivat ylläpitää johdonmukaista minäkäsitystä. Tämä valtioiden minäkäsitys konstituoituu ja sitä ylläpidetään narratiivien avulla, jotka synnyttävät rutiininomaisia ulkopoliittisia toimia ja käyttäytymistä. Tähän kiteytyy valtioiden ajatus siitä, kuinka se näkee itsensä sekä kuinka se haluaa muiden valtioiden näkevän itsensä. (Steele 2008, 2–3.)

Ontologinen turvallisuus antaa työkalun tarkastella valtion syvää olemusta ja sen tarvetta kokea turvallisuutta. Valtion tarve ontologiselle turvallisuudelle voidaan nähdä sisäänpäin suuntautuvana keskusteluna identiteetin ja valtion käyttäytymisen välillä, jotta se voi saavuttaa ”elämänkerronnallisen jatkuvuuden”. (Bachleitner 2023, 27.) Ontologisen turvallisuuden kautta pystytään tarkastelemaan valtion itselle tärkeiksi määrittelemiä elementtejä. Ontologinen turvallisuus tarjoaa näkökulmia siihen, miten identiteetin ja käyttäytymisen välinen suhde toimii valtioilla. Valtion identiteetti ei muodostu ainoastaan sen vuorovaikutuksesta poliittisen toiseuden kanssa, vaan enemmänkin sen omista kokemuksista historiassa: minkälainen valtio on ollut, minkälainen se on ja minkälaiseksi se tulee. Tämä kansallinen elämänkerta, joka löytyy valtion omasta historiasta määrittää valtion itsensä suhteessa toisiin valtioihin. (ibid., 28.) Kansainvälisten suhteiden tutkimus onkin muotoillut uudelleen Anthony Giddensin näkemyksiä yksilöstä yhteiskunnassa. Kansainvälisten suhteiden tutkimus muotoilee tämän asetelman keskusteluksi valtioiden roolista kansainvälisessä yhteisössä. (ibid., 27.)

2.4 Identiteetti osana ontologista turvallisuutta

Identiteetin käsite liittyy läheisesti ontologiseen turvallisuuteen, joten käsitteen määrittely ja tarkastelu on mielestäni perusteltua tässä työssä. Identiteetti on joukko merkityksiä, jotka määrittelevät yksilöt yhteiskunnan rooleissa, ryhmien tai sosiaalisten kategorioiden jäseninä tai ainutlaatuisina yksilöinä. Identiteettiin vaikuttavat yksilöstä ulkoiset sosiaaliset järjestykset, säännöt ja normit. Identiteetit eivät ole vain yksilötason ilmiöitä, vaan ne vaikuttavat niin mikro- kuin makrotason sosiaalisiin järjestyksiin ja normeihin. (Burke & Stets 2022, 1, 3.) Nykyisin identiteetillä on suuri joukko erilaisia merkityksiä. Se voi viitata sosiaalisiin ryhmiin tai rooleihin ja joskus taas yksilöä koskettaviin perustavanlaatuisiin tietoihin. (Fukuyama 2020, 25.) Identiteetti ei ole vakio, vaan sosiaalinen luomus, joka on sosiaalisen konstruoinnin tulos. Sen rakentaminen on prosessi, joka

tapahtuu aina ajassa ja tilassa (Harle & Moisio 2000, 12). Identiteetti ei ole koskaan annettua tai valmiiksi rakentunutta, vaan se on sosiaalisesti ja poliittisesti muodostunutta (Harle 2000, 4).

Identiteetit yhdistävät ihmisiä. Ihmiset ryhmäytyvät heitä keskenään yhdistävien seikkojen perusteella. Ryhmään kuulumisella ihminen hakee hyväksyntää sekä tunnustamista omalle olemassaololleen ja arvokkuudelleen. Ihmisen omanarvontunne kaipaa tunnustetuksi tulemista eikä oma tietoisuus omasta arvosta riitä, vaan siihen tarvitaan julkista tunnustamista (Fukuyama 2020, 26). Ihmisten on tiedettävä keitä he ovat ja keitä he eivät ole sekä mihin he kuuluvat ja mihin he eivät kuulu. Ihmiset tarvitsevat sosiaalista järjestystä, jossa kaikella on nimensä ja paikkansa. (Harle 2000, 4.) Ihmiset identifioivat itsensä muihin etnisyyden, rodun, kansallisuuden, kulttuurin, uskonnon, sukupuolen, seksuaalisten tottumusten, sosioekonomisen aseman, iän, ideologian ja muiden sosiaalisten normien perusteella (Gutmann 2003, 9). Näihin ominaisuuksiin identifioitumalla ihmiset muodostavat ryhmäidentiteettejä. Ryhmäidentiteetit auttavat yksilöitä saamaan varmemman tunteen itsestä sekä sosiaalisesta kuulumisesta (ibid., 9). Ryhmäidentiteetit sisältävät kuitenkin aina toiseuden käsityksen, joka on yhdistetty niihin, jotka eivät kuulu kyseiseen ryhmään eivätkä jaa samoja tarinoita ja hetkiä kyseisen ryhmän kanssa (Paasi 1995, 46).

Kansallinen identiteetti on identiteetin yksi monista ilmentymistä. Kansallinen identiteetti on ilmiö, jossa ihminen tuntee kuuluvansa johonkin tiettyyn valtioon tai kansaan tietyn alueellisen rajauksen määrittelemänä (Verdugo & Milne 2016, 2). Kansallinen identiteetti on yleensä nähty perustavanlaatuisena kehyksenä poliittiselle osallistumiselle sen kaikissa muodoissa. Se on väistämätön perusta ihmisyhteisöjen yleiselle järjestäytymiselle sekä se on osoittautunut tehokkaaksi keinoksi luoda me-hengen tuntemuksia läpi modernin ajan. (Larguèche 2016, 26.) Me-he-dikotomian rakenteessa hyödynnetään yleensä stereotyyppisiä määritelmiä meistä ja heistä, mutta erityisesti heistä. Kansallisvaltioiden tapauksessa näitä määritelmiä voidaan hyödyntää kansallisten yksiköiden (esim. suomalaiset, venäläiset yms.) tai ylikansallisten yksiköiden (eurooppalaiset, skandinaavit, slaavit) rakentamisessa. (Paasi 1995, 13.) Kansallinen identiteetti on sitä, miten kansalaiset, varsinkin sukupolvet, tulkitsevat menneitä ja nykypäivän tapahtumia kehittäessään ja ylläpitäessään kiintymystä kansakuntaansa tai valtioonsa (Karnaukhova & Verdugo 2016, 149).

Kansallinen identiteetti koostuu ihmisten itsestään kertovista kertomuksista, joita kerrotaan toisille ihmisille. Nämä kertomukset kattavat yksilön ja yhteisön historiaa, syntyä, taisteluja ja paikkaa maailmassa (Fukuyama 2020, 157). Kansalliset tai yhteisölliset identiteetit kertovat ihmisten yhteisistä historiallisista kokemuksista ja kulttuurisista toimintatavoista, jotka luovat yksilöihin muuttumattomia ja jatkuvia merkityksiä, joiden avulla he kokevat itsensä osaksi ”yhtä kansaa” (Hall 1999, 224). Kansallisen identiteetin avulla yksilöt kokevat kuuluvansa osaksi jotain suurempaa

yhteisöä, jossa heilläkin on arvonsa ja merkityksensä. Tämänlaiset itseämme suuremmat yhteisöt luovat kertomusta itsestään, joissa yksilöt kokevat olevansa osana tätä kansakunnan kertomusta. Tämä osallisuuden tunne antaa merkitystä yksilön arkiselle olemassaololle ja liittää jokapäiväisen elämän kansalliseen kohtaloon, joka oli olemassa ennen yksilöä ja jää myös olemaan yksilön jälkeen. (ibid., 47–48.)

2.5 Kyber ja ontologinen turvallisuus

Ontologisen turvallisuuden teoria tarjoaa uudenlaisia näkökulmia kyberteknologioiden tutkimiseen. Ontologisen turvallisuuden teoria tarjoaa työkalun, jonka avulla voidaan yhdistellä useita elementtejä, kuten narratiiveja, rutiineja, tunteita ja näkemystä paikasta maailmassa. Näiden eri elementtien tarkastelulla voidaan paremmin hahmottaa ilmiöitä, joilla kyberteknologiat haastavat valtioita (Lupovici 2023, 154). Ontologinen turvallisuus ilmenee kaikissa sosiaalisissa konteksteissa (Mitzen 2006, 353). Ontologisen turvallisuuden teoria tarjoaa työkalun, jonka avulla voidaan hahmottaa kyberturvallisuuden ilmiöitä ja seurauksia monelta eri yhteiskunnan tasolta. Kehittyvien kyberteknologioiden tapaan, myös ontologinen turvallisuus on muuttuva ja liikkeessä oleva käsite (Vuorelma 2025, 4). Tämänlainen käsitteiden ja ilmiöiden dynamiikka mahdollistaa ajankohtaisen analyysin vallitsevista yhteiskunnallisista ilmiöistä.

Kybertoimintaympäristö on uniikki siinä mielessä, että kyberteknologioista voi tulla alusta, jossa muovataan ja levitetään tunteita (Lupovici 2023, 157). Osaltaan kybertoimintaympäristö tarjoaa jo paikan tunteille ja niiden muovaamiselle ja levittämiselle. Kybertoimintaympäristö asettaa myös valtioille useita haasteita liittyen turvallisuuden tunteen ylläpitämiseen sekä tunteiden ja yleisen mielipiteen kontrolloimiseksi. Suomalaisessakin yhteiskunnassa teknologia ulottuu yhä laajemmalle ja syvemmälle yhteiskunnan kriittisempiin kohteisiin. Näistä teknologioista riippuvaiset yhteiskunnan kriittiset kohteet ovat yhä enemmän haavoittuvaisempia erilaisia uhkia ja häiriöitä vastaan. (Limnell 2014, 20). Modernien kehittyvien teknologioiden myötä perinteiset valtiorajat sekä raja fyysisen ja digitaalisen maailman välillä menettävät merkitystään (Górka 2018, 12).

Politiikkatieteiden professori Amir Lupovici (2023) esittää kolme ulottuvuutta, jossa kybertoimintaympäristön ilmiöt haastavat valtioita. Kyberteknologiat haastavat valtioiden kykyä ylläpitää yhtenäisiä narratiiveja, rutiineja sekä tunnetta omasta paikasta maailmassa. Ne myös haastavat valtioiden roolia ontologisen turvallisuuden tuottajana niille ihmisille, jotka asuvat valtion rajojen sisällä. Viimeisenä, kyberteknologiat haastavat valtioiden kykyä monopolisoida ontologisen

turvallisuuden tuottajan roolia. Kyberteknologiat haastavat valtioiden perinteistä roolia tarjoamalla erilaisia keinoja yksilölle täyttää ontologisen turvallisuuden tarpeensa. Nämä kyberteknologioiden keinot ja vaihtoehdot tarjoavat mahdollisuuden kokea yhteisöllisyyttä, jatkuvuutta ja keinon osallistua ja vaikuttaa maailmaan. Tämä voi eriyttää valtiota yksilöstä ontologisen turvallisuuden turvaajana, ja vaikeuttaa valtion tehtävää monopolisoida ontologisen turvallisuuden tuottajan rooli itselleen. (Lupovici 2023, 158.)

Kybertoimintaympäristössä ilmenevät uhkat eroavat perinteisistä valtion suvereniteettia tai fyysistä turvallisuutta koskevista uhkista, kuten sotilaallisesta uhkasta. Kyberuhkat keskittyvät enemmän valtion käsitykseen itsestä (*states´sense of self*) – valtion ontologiseen turvallisuuteen – ja valtioiden kykyyn jatkaa ensisijaisina ontologisen turvallisuuden tuottajina. Modernit valtiot eivät vain pyri tuottamaan ontologista turvallisuutta yksilöille, vaan pyrkivät myös monopolisoimaan tämän. (Lupvici 2023, 168.) Valtiot pyrkivät luomaan roolin ja asetelman, jossa sen luoma sosiaalinen ympäristö on ainoa ontologista turvallisuutta yksilöille tuottava voima. Täten valtiot pystyvät paremmin turvaamaan oman olemassaolonsa ja intressinsä, luomalla sen rajojen sisällä asuville ihmisille ainoan vaihtoehdon, jossa he elämäänsä toteuttavat.

Kyberuhkat haastavat valtioiden ja instituutioiden luomaa ja ylläpitämää sosiaalista monopolia vaikuttamalla esimerkiksi yksilöiden tunteisiin, mielipiteisiin ja uskomuksiin. Kyberuhkat vaikuttavat ihmisten käsitykseen, uskoon ja etenkin luottamukseen valtiota ja sen instituutioita kohtaan. Kyberteknologiat mahdollistavat ilmiöitä, jotka uhkaavat ihmisten perinteitä ja uskomuksia, jolloin ontologisen turvallisuuden tunne on haastettuna ja turvallisuutta ylläpitävät mekanismit aktivoituvat (Vuorelma 2025, 4–5). Ihmiset olettavat valtion ja sen instituutioiden pitävän heidät turvassa erinäisiltä uhkilta, mutta kun jokin uhka pääsee järjestelmien lävitse, on valtion turvallisuusmonopoli haastettuna.

Suomen kyberturvallisuusstrategiat pyrkivät vahvistamaan tätä luottamusta valtiota ja sen instituutioita kohtaan erilaisten kybertoimintaympäristössä ilmenevien uhkien osalta. Strategiat linjaavat valtion viranomaisille ja sidosryhmille erilaisia toimintalinjoja mutta myös antavat ulospäin viestin, että kyberturvallisuuteen ja valtioon on luottamista. Kyberturvallisuusstrategiat ovat osa valtion kokonaisturvallisuuden mallia ja Yhteiskunnan turvallisuusstrategiaa, jotka tarjoavat yhden ulottuvuuden Suomen valtion turvallisuuden tarkasteluun.

3 AINEISTO JA ANALYYSIMENETELMÄ

3.1 Kyberturvallisuusstrategiat

Tutkielmani aineistona toimivat Suomen valtion kyberturvallisuusstrategiat eri vuosilta. *Suomen kyberturvallisuusstrategia 2013*, *Suomen kyberturvallisuusstrategia 2019* sekä uusin *Suomen kyberturvallisuusstrategia 2024–2035*. Kyberturvallisuusstrategiat ovat strategisia asiakirjoja, joiden tarkoituksena on kartoittaa Suomen kyberturvallisuuden tilaa osana kokonaisturvallisuutta ja linjata sen kehittämisestä. ”*Strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus”* (Kyberturvallisuusstrategia 2013, 1).

Suomen kyberturvallisuusstrategia 2013 on tasavallan presidentin sekä valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan (TP-UTVA) 8.3.2011 käynnistämä hanke, jossa laaditaan kansallinen kyberturvallisuusstrategia osaksi yhteiskunnan turvallisuusstrategian toimeenpanoa. Strategian laatimisessa on ollut mukana poikkihallinnollinen työryhmä, jossa on viranomaistahojen lisäksi ollut mukana edustajia muun muassa elinkeinoelämästä. (Valtioneuvosto, Puolustusministeriö 24.1.2013.) Tässä strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. ”*Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset.”* (Kyberturvallisuusstrategia 2013, 1–2.)

Suomen kyberturvallisuusstrategia 2019 asettaa keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Strategia nojautuu vuoden 2013 kyberturvallisuusstrategian yleisiin periaatteisiin. (Valtioneuvoston periaatepäätös PLM/2019/52.)

Suomen kyberturvallisuusstrategia 2024–2035 on uusin kyberturvallisuusstrategia ja edellisistä strategioista uusittu vastaamaan ajantasaista toiminta- ja uhkaympäristöä. Strategian uudistamista on toteutettu hallitusohjelman mukaisesti, ja strategian valmisteluun on kuulunut eri hallinnonalojen jäseniä sekä useita julkisen ja yksityisen sektorin, tiedeyhteisön sekä järjestökentän organisaatioita ja edustajia. (Valtioneuvosto, 2024.) ”*Strategia käsittelee erityisesti kansallista kyberturvallisuutta, jolla tarkoitetaan niitä toimia, joiden seurauksena digitaalinen yhteiskunta kykenee varautumaan, tunnistamaan, torjumaan ja kestämään sähköisten ja verkotettujen järjestelmien häiriöitä ja niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin, toipumaan niistä sekä*

varmistamaan kansallisen turvallisuuden, maanpuolustuksen ja huoltovarmuuden toimintaedellytykset." (Kyberturvallisuusstrategia 2024–2035, 10.)

Aineiston lisäksi käytän tutkielmassa ilmiön syventämiseksi sekä havainnollistamiseksi asiantuntijoiden, poliitikkojen ja viranomaisten antamia haastatteluja, tiedotteita sekä kommentteja mediassa. Pääasiallisen aineiston muodostavat kuitenkin kyberturvallisuusstrategiat, joiden tukena toimivat medialähteet. Medialähteet ovat merkitty tekstiin asianmukaisilla lähdeviittauksilla sekä lähdeluetteloon.

Aineisto kattaa kolme valtion strategista asiakirjaa, jotka löytyvät julkisista lähteistä. Strategiat ovat pituudeltaan noin 10–60 sivua. Koen, että tämänlaisen aineiston avulla pystyn toteuttamaan tutkielman onnistuneesti sekä vastaamaan asettamaani tutkimuskysymykseen tarkoituksenmukaisella tavalla. Medialähteet on kerätty eri uutistoimistojen internet-sivuilta sekä viranomaisten tiedotteista ja julkaisuista, jotka on merkitty lähdeluetteloon. Valtion kyberturvallisuusstrategiat on kerätty julkisista lähteistä internetistä ja niiden linkit löytyvät empiirisen aineiston kohdalta tutkielman lopusta.

3.2 Tutkielman menetelmälliset ratkaisut

Tämä tutkielma on laadullinen tutkimus. Aineiston analysoimiseksi käytän tutkielmassa laadullista sisällönanalyysia. Laadullinen tutkimus on eräänlainen kattokäsite, jonka alla on useita hyvin erilaisia laadullisen tutkimuksen tyyppejä. Näin se mahdollistaa laadullisen tutkimuksen tarkastelun laajassa merkityksessä mutta myös kapeassa merkityksessä. (Tuomi & Sarajärvi 2018, 13). Laadullisessa tutkimuksessa pyritään kuvaamaan, ymmärtämään sekä tulkitsemaan tutkittavaa aihetta, jonka kautta pyritään tutkittavan ilmiön syvälliseen ymmärtämiseen (Kananen 2017, 35). Laadullinen tutkimus pyrkiikin ymmärtämään tutkimuksen kohteena olevaa ilmiötä, selittämään sen koostumusta sekä ilmiön tekijöiden välisiä suhteita. Se pyrkii tutkimaan yksittäistä tapausta ja tarjoamaan mahdollisuuden saada ilmiöstä syvällinen näkemys. (ibid., 33, 36, 44.) Sisällönanalyysi on tekstianalyysia, jossa etsitään tekstistä sen sisältämiä merkityksiä. Laadullinen sisällönanalyysi tarjoaa tutkielmaani mielestäni parhaimman tavan analysoida aineistoa ja ymmärtää ilmiötä. Tutkielmassani tarkoituksena on ymmärtää tutkittavaa ilmiötä analysoitavan aineiston perusteella.

Laadullisessa sisällönanalyysissa järjestetään tutkittava aineisto sellaiseen muotoon, jossa sen sisältämä informaatio on vielä havaittavissa. Laadullisessa analyysissa aineisto nähdään ja sitä tarkastellaan kokonaisuutena. (Alasuutari 1995, 38.) Aineiston analysoinnilla pyritään lisäämään

informaatioarvoa, sillä erilaisesta hajanaisestakin aineistosta yritetään saada selkeä ja yhtenäinen kokonaisuus, jonka sisältämää informaatiota voidaan käyttää tutkittavaan ilmiöön (Tuomi & Sarajärvi 2018, 122).

Aineistolähtöisessä sisällönanalyysissä voidaan hahmottaa kolme eri vaihetta. Redusointi, klusterointi sekä abstrahointi. Ensimmäinen vaihe on redusointi eli pelkistäminen, jossa aineistosta karsitaan tutkimukselle epäolennainen tieto pois. Redusoinnin jälkeistä prosessia seuraa klusterointi, eli ryhmittely, jossa aineistosta löytyneitä samankaltaisuuksia tai eroavaisuuksia yhdistellään uusiksi kokonaisuuksiksi. Tästä seuraa prosessin viimeinen vaihe, abstrahointi, eli teoreettisten käsitteiden koostaminen aineistosta saadun informaation avulla. (Tuomi & Sarajärvi 2018, 122–127.)

Laadullisen sisällönanalyysin avulla etsin aineiston tekstistä erilaisia merkityksiä, jotka ovat relevantteja tutkielmani kannalta. Pelkistän aineistosta tutkimukselle epäolennaisen pois hyödyntämällä esimerkiksi värikoodausta, jolla merkitsen oleellisen tiedon aineistosta. Värikoodattujen kohtien avulla muodostan kokonaisuuksia, jotka auttavat vastaamaan esittämääni tutkimuskysymykseen. Muodostuneista kokonaisuuksista erottelen vielä tutkimukselle relevantin tiedon ja näistä tiedoista muodostuu tutkimuskysymykseen vastaava kokonaisuus.

Analyysin perusteella strategiat painottuvat kokonaisvaltaiseen uhkien torjumiseen, ennaltaehkäisyyn sekä varautumiseen, painottaen kyberturvallisuuden roolia osana kokonaisturvallisuuden mallia. Strategiat pyrkivät enemmänkin kuvaamaan sitä, mitä ollaan suojaamassa ja mihin erilaisiin kyberturvallisuuden ulottuvuuksiin Suomen on syytä kiinnittää huomiota. Mielestäni valitsemani aineisto, analyysimenetelmä sekä teoria tukevat toisiaan ja auttavat vastaamaan tutkimuskysymykseeni.

3.3 Tutkimusetiikka

Yhteiskunnan luottamus tutkimusta kohtaan sekä tieteen yleinen uskottavuus rakentuu tieteen hyvien käytäntöjen ja eettisten näkökulmien noudattamisesta ja huomioonottamisesta. Tutkimusta on pyrittävä tarkastelemaan eettisesti koko sen laajuudella ja koko tutkimusprosessin ajalta. Tutkimuksen eettiset valinnat ja ratkaisut vaikuttavat tutkimuksen ja tieteen uskottavuuteen. (Suomen akatemia.fi.) Vastuu näistä eettisistä valinnoista ja ratkaisuista on pääsääntöisesti tutkimuksen tekijällä tai tutkimusryhmällä. Eettisiä vastuita voidaan kuitenkin myös katsoa olevan tutkimusyksikön johdolla ja tutkimusta harjoittavien organisaatioiden johdolla. (Suomen akatemia.fi). Eurooppalaisen tutkimuseettisen ohjeistuksen mukaan hyviä tieteellisiä käytännön

perusperiaatteita ovat luotettavuus, arvostus sekä vastuunkanto (Tutkimuseettinen neuvottelukunta (TENK) 2023, 11). Hyvät tieteelliset menettelytavat ovat osa tiede- ja tutkimusyhteisöön kuuluvien organisaatioiden laatujärjestelmää. Näillä menettelytavoilla huolehditaan hyvän tieteellisen käytännön toteutumisesta tieteellisen toiminnan koko elinkaaren ajan. (ibid.)

Tässä tutkielmassa on huomioitu tutkimuseettiset ulottuvuudet. Laadullinen tutkimus perustuu aina tietyssä määrin tutkijan subjektiivisiin käsityksiin, jolloin täysin objektiivista tietoa ei ole olemassa. Laadullisessa tutkimuksessa tutkijan ja tutkittavan ilmiön välillä on suora yhteys (Kananen 2017, 36). Ei ole olemassa objektiivisia, ”puhtaita” havaintoja itsessään, vaan muun muassa jo käytetyt käsitteet, tutkimusasetelma ja menetelmät ovat tutkijan asettamia ja vaikuttavat aina tuloksiin (Tuomi & Sarajärvi 2018, 109). Laadullisessa tutkimuksessa luotettavuus sekä eettisyys ovat tinkimättömiä asioita, vaikka niihin löytyy erilaisia tapoja suhtautua (ibid., 20).

Olen pyrkinyt tässä tutkielmassa huolelliseen, tarkkaan ja johdonmukaiseen työskentelyyn tutkimusprosessin eri vaiheissa tutkielman laadun ja päämäärän varmistamiseksi. Tutkielmassa on pyritty mahdollisimman objektiivisiin ja vastuullisiin tutkimuksellisiin menetelmiin. Olen pyrkinyt tarkastelemaan tutkittavaa ilmiötä ja aineistoa mahdollisimman objektiivisesta näkökulmasta, ilman, että omat kokemukseni ja ennakko-oletukseni vaikuttavat tutkielmani tuloksiin. Tutkimukselliset valinnat, havainnot ja päätelmät on perusteltu tutkielmassa.

Tutkielmassa ei vaarannu kenenkään henkilöllisyys, yksityisyys tai muu arkaluontoinen tai yksityinen tieto, koska tutkielma ei perustu henkilöhaastatteluihin tai henkilöhistoriaan. Tutkielmassa käytettävät henkilöiden nimet ja tittelit ovat julkisista lähteistä, jotka perustuvat lähteen julkaisuaikaan. Tutkielmassa käytettävä tieto ja aineisto ovat julkisia ja kaikki tutkielmassa käytettävät lähteet on merkitty lähdeluetteloon. Tutkielmassa on käytetty ChatGPT -tekoälyohjelmaa tiedonhakuun sekä kielenhuoltoon.

Siirryn seuraavaksi tarkastelemaan tutkielmani tuloksia, jotka vastaavat asettamaani tutkimuskysymykseen, *millä tavoilla Suomi vahvistaa ontologista turvallisuuttaan kyberturvallisuusstrategioissa.* Laadullisen sisällönanalyysin ja ontologisen turvallisuuden teoreettisen viitekehyksen avulla tekemäni tutkimusaineiston analyysin perusteella Suomen ontologista turvallisuutta vahvistavat keinot ilmenevät kolmen kokonaisuuden kautta, jotka muodostavat tutkielmani tulokset. *1) Kokonaisvaltainen kansallinen yhteistyö, 2) Kansainvälinen yhteistyö kyberturvallisuudessa* ja *3) Yksilö kybertoimintaympäristössä.* Kyseisiä kokonaisuuksia käsittelen ja analysoin edellä mainitussa järjestyksessä tutkimusaineistosta löytämieni havaintojen

avulla sekä hyödyntäen julkisista lähteistä löytyviä asiantuntijoiden näkemyksiä ja muita tutkielmalle relevantteja lähteitä.

4 KOKONAISVALTAINEN KANSALLINEN YHTEISTYÖ

Suomalaisen yhteiskunnan turvallisuus rakentuu monen tekijän summasta. Viranomaiset, elinkeinoelämä, järjestöt sekä kansalaiset ovat kaikki osa yhteiskunnan turvallisuutta ja turvallisuustoimijoita. Tällöin kaikki yhteiskunnan toimijat osallistuvat elintärkeiden toimintojen turvaamiseen. Tämä muodostaa perustan suomalaisen yhteiskunnan kriisinkestävyydelle. (Yhteiskunnan turvallisuusstrategia 2025, 12.) Tämä osallistamisen malli ulottuu myös kyberturvallisuuden alalle, jossa kaikki yhteiskunnan toimijat osallistuvat elintärkeän digitaalisen infrastruktuurin turvaamiseen ja kehittämiseen kokonaisturvallisuuden mallin mukaisesti.

”Kyberturvallisuuden tekemiseen on saatava jokainen yhteiskuntamme toimija osalliseksi”, toteaa kansanedustaja ja dosentti Jarno Limnell (Suomen tietotoimisto, 10.10.2024). Valtiot tarvitsevat viranomaisten lisäksi akateemisten instituutioiden, yksityisten yritysten sekä asiantuntijoiden osaamista, jotta ne voivat pärjätä jatkuvasti kehittyvässä digitalisoituvassa maailmassa. (Suojelupoliisi, Kansallisen turvallisuuden katsaus 2025). Suomi on tunnettu viranomaisten välisestä yhteistyöstä, etenkin turvallisuuden alalla ja Suomessa sovelletaan kokonaisturvallisuuden mallia, johon sisältyy kaikki erilaiset turvallisuuden ulottuvuudet ja yhteiskunnan toimijat. Kyberturvallisuus on osa kokonaisturvallisuutta, joka määritellään valtioneuvoston antamassa periaatepäätöksessä seuraavasti.

> *”Kokonaisturvallisuus on tavoitetila, jossa valtion itsenäisyyteen, väestön elinmahdollisuuksiin ja muihin yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ovat hallittavissa. Yhteiskunnan elintärkeät toiminnot turvataan viranomaisten, elinkeinoelämän sekä järjestöjen ja kansalaisten yhteistoimintana. Turvaamisen toimiin kuuluvat uhkiin varautuminen, häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen.”* (Valtioneuvoston periaatepäätös kokonaisturvallisuudesta 5.12.2012, 7.)

Kyberturvallisuus suojaa yhteiskunnan elintärkeitä toimintoja, kuten digitaalista infrastruktuuria ja palveluita. Kyberturvallisuudella tavoitellaan turvallista kybertoimintaympäristöä, johon voidaan luottaa ja jonka toiminta on turvallista kaikille toimijoille (Laari et al. 2019, 10). Kyberturvallisuuden kehittämiseksi on tehtävä yhteistyötä kaikkien yhteiskunnan sektoreiden välillä. Pienenä valtiona yhteistyö turvallisuuden eteen on välttämätöntä.

> *”Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Meillä on vahva osaamisperusta sekä pitkät*

> *perinteet tiivistä ja luottamuksellisesta yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojen välisestä yhteistyöstä."* (Kyberturvallisuusstrategia 2013, 3.)

Kyberturvallisuus on alistettu osaksi kokonaisturvallisuutta, joten se edellyttää yhteiskunnan eri toimijoiden yhteistyötä. "*Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS) määritettyjä periaatteita ja toimintatapoja"* (Kyberturvallisuusstrategia 2013, 5). "*Kyberturvallisuuden varautumistyötä tehdään tiiviissä yhteistyössä kokonaisturvallisuuden mallin mukaisesti"* (Kyberturvallisuusstrategia 2024–2035, 28). Yhteistyötä on kuitenkin johdettava, jotta yhteistyö tuottaa haluttuja tuloksia. "*Suomen kyberturvallisuuden johtamisen ylimmän tason muodostaa valtioneuvosto, jonka tehtävänä on kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen"* (Kyberturvallisuusstrategia 2013, 4). Keskitetyn johtamisen ja kehittämisen tärkein tehtävä on luoda visio ja kansallinen mentaliteetti, joka tunnistetaan kaikilla kyberturvallisuuden toimijoiden tasoilla (Lehto & Limnell 2021, 141).

Valtioneuvoston johdolla valtio pystyy määrittelemään kyberturvallisuuden suunnalle ja kehittämiselle sen tavoitteet ja reunaehdot. Valtion kykyä turvallisuuden tuottajana yksilöille on kritisoitu sen liiallisesta yhteydestä yksityisen sektorin toimijoihin, jotka turvaavat valtion tietojärjestelmiä. Iso kysymys onkin, että onko valtiolla oikeus määrätä kybertoimintaympäristöstä, jos ne eivät ole niiden varsinaisia ylläpitäjiä (Jansson 6& Sihvonen 2018, 14). Yksityiset yritykset toimivat kumppaneina ja käytännön mahdollistajina, mutta valtio on viimekädessä se, joka johtaa ja hallinnoi toimintaa ja sen kehittämistä valtiossa (Lupovici 2023, 159). Valtion johtava rooli kyberturvallisuuden koordinoimisessa tunnustetaan myös Suomen kyberturvallisuusstrategioissa.

> *"Kyberturvallisuuden kansallista kehittämistä koordinoimaan perustetaan liikenne- ja viestintäministeriöön kyberturvallisuusjohtajan tehtävä. […] Kyberturvallisuusjohtajan rooli on kyberturvallisuuden kehittämistä, suunnittelua ja varautumista yhteiskunnallisesti sovittava. […] Kyberturvallisuusjohtaja toimii myös valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa. Hänen johdollaan laaditaan ministeriöiden, Turvallisuuskomitean ja kyberturvallisuustoimijoiden asiantuntemista hyödyntäen kyberturvallisuuden kokonaiskuva ja kehittämisohjelma."* (Kyberturvallisuusstrategia 2019, 6.)

> *"Kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja analysoinnista vastaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus eri yhteistyötahojen kanssa."* (Kyberturvallisuusstrategia 2024–2035, 20–21.)

Kansallisen kyberturvallisuuden kehittäminen tehdään monialaisella yhteistyöllä. Liikenne- ja viestintävirasto Traficomin entinen pääjohtaja Kirsi Karlamaa toteaa viranomaisten, yritysten ja huoltovarmuuskriittisten toimijoiden tekevän aktiivisesti torjuntatoimia hyvässä yhteistyössä kyberhyökkäysten välttämiseksi (Rautio, Yleisradio, 21.4.2023). Julkisen ja yksityisen sektorin laaja-alainen yhteistyö nousee vahvasti esille myös kyberturvallisuusstrategioissa.

> *”Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, ja jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme”.* (Kyberturvallisuusstrategia 2019, 8).

> *”Strategisten linjausten toimeenpanolla vahvistetaan suomalaisen turvallisuusyhteistyön vahvuudeksi koettua julkisen ja yksityisen sektorin välistä yhteistoimintaa. Tämän yhteistyön avulla voidaan parhaiten palvella koko yhteiskuntaa ja tukea sen elintärkeitä toimintoja tuottavia toimijoita.”* (Kyberturvallisuusstrategia 2013, 6.)

> *”Kyberturvallisuuden varautuminen edellyttää yhteiskunnan eri toimijoiden, julkishallinnon ja elinkeinoelämän välistä yhteistyötä ja osaamisen vahvistamista eri sektoreilla. Digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria.”* (Kyberturvallisuusstrategia 2019, 6–7.)

Kyberturvallisuus koskettaa yhteiskunnan kaikkia toimijoita aina kansalaisia myöten. Turvallisen ja toimivan kyberturvallisuuden toteuttamiseen tarvitaan kokonaisen yhteiskunnan osallistumista ja toimijoiden välistä yhteistyötä. (Suomen tietotoimisto, 10.10.2024). Kyberturvallisuuden valtakunnallinen kehittäminen ja toimivuus perustuvat yhteiskunnalliseen yhteistyöhön lukuisten eri toimijoiden kesken. Yhteiskunnan eri sektoreilla toteutetaan tiivistä yhteistyötä, jossa tietoa jaetaan koko ajan toimijoiden kesken (Suojelupoliisi, 29.8.2025). Yhteistyöllä, jolla on yhteisesti asetetut tavoitteet ja strategia, luo yhtenäistä turvallisuuden tunnetta. Yhtenäinen turvallisuuden tunne luo luottamusta valtion kykyyn turvata kansalaistensa turvallisuus kybertoimintaympäristössä. Turvallisuuden tunne on tärkeä yhteisöllisyyttä ylläpitävä voima. Oleellista on ymmärtää, että mikäli ihmisten luottamus kybermaailman toimivuuteen edelleen heikkenee, sillä on merkittäviä vaikutuksia niin turvallisuuden tunteeseen kuin todellisuuteen. (Limnell, Majewski & Salminen 2014.) Yhteiskunnan häiriöttömälle toiminnalle ja yksittäisten ihmisten turvallisen elämän varmistamiseksi on välttämätöntä, että kyberturvallisuus sekä tieto- ja viestintäjärjestelmät ovat luotettavia ja toimivat

niille kuuluvalla tavalla. Kyse on myös kansalaisten luottamuksen ylläpitämisestä hyvin toimivaan yhteiskuntaan. (Lehto & Limnell 2021, 139.)

Palomuurien ja suojauksien läpi pääsevät kyberhyökkäykset, varsinkin kun ne paljastuvat julkisuuteen, kyseenalaistavat kyberturvallisuuden tilaa. Esimerkiksi eduskuntaan tehty kyberhyökkäys vuonna 2020 sai paljon huomiota mediassa. Syksyllä 2020 eduskunnan sisäinen tekninen valvonta havaitsi kyberhyökkäyksen, jonka seurauksena joidenkin eduskunnan sähköpostitilien tietoturvallisuus vaarantui. Osa vaarantuneista sähköpostitileistä kuului kansanedustajille. (MTV, 28.12.2020.) Valtion keskeisimpään demokraattiseen instituutioon kohdistunut kyberhyökkäys koettiin iskuna valtion sisimpään ja syvimpään itseensä. Silloinen tasavallan presidentti Sauli Niinistö kommentoi kyberhyökkäystä vakavaksi loukkaukseksi suomalaista demokratiaa ja yhteiskuntajärjestystä vastaan. Myös silloinen eduskunnan puhemies Anu Vehviläinen kommentoi asiaa vakavaksi hyökkäykseksi demokratiaa ja suomalaista yhteiskuntaa kohtaan. (MTV, 28.12.2020.) Tapaus paljastui lopulta kybervakoiluoperaatioksi, jonka toteuttaja yhdistettiin Kiinaan (Yle, 18.3.2021).

Poliittisessa puheessa eduskuntaan kohdistunut kyberhyökkäys koettiin hyökkäykseksi koko suomalaista yhteiskuntaa ja demokratiaa kohtaan. Poliittisessa puheessa tämänlainen kyberhyökkäys saadaan koskemaan koko yhteiskuntaa ja yhteiskunnan selviytymistä. Turvallisuuden tunne on järkkynyt ja järjestäytyneen yhteiskunnan olemusta on haastettu. Tämänlaiset tapahtumat luovat valtioissa ontologista turvattomuutta ja kyseenalaistavat valtion kyvykkyyttä ylläpitää kokonaisvaltaista turvallisuutta. Yksi keskeinen turvallisuuden tunteeseen vaikuttava tekijä on luottamus siihen, että yhteiskunta pystyy puuttumaan tämänlaisiin ilmiöihin. Keskeistä on pyrkiä ennalta estämään vahingolliset ilmiöt tai viime kädessä hoitamaan ja selvittämään kiireelliset hätätilanteet. (Kolehmainen, Turvallisuuskomitea, 2020.) Kyberuhkiin liittyen valtioilla onkin haasteita pysyä digitaalisen kehityksen mukana ja luoda sääntelyä ja rajoitteita kybertoimintaympäristössä. Valtiot eivät ole pystyneet luomaan käytäntöjä tai teorioita, joiden avulla valtiot hallitsisivat tai säätelisivät kybertoimintaympäristön jatkuvaa kehitystä (Lupovici 2023, 158).

Kybertoimintaympäristössä toimijan status on vaikeaa tunnistaa, ja yhä vaikeampaa on saada tekijä vastuuseen teostaan. Kybertoimintaympäristössä ei-valtiolliset toimijat voivat vaarantaa valtioiden turvallisuutta ja yhteiskuntaa muun muassa kyberrikollisuuden muodossa, jolloin myös rangaistusten asettaminen vaikeutuu. (Jansson & Sihvonen 2018, 13.) Toimijat eivät ole kybertoimintaympäristössä samalla viivalla. Valtio ei välttämättä kohtaa valtiota, vaan esimerkiksi toinen valtio voi käyttää kyberoperaatioihinsa yksityistä toimijaa kiistääkseen teon ja välttääkseen teon sen ulkopoliittisilta seurauksilta. Nykypäivän kybertoimintaympäristössä yksittäisen ihmisen toimilla voi olla vakavia

seurauksia valtiolle (Akyeşilmen 2025, 510). Kybertoimintaympäristön ja teknologian kehitys sumentaa perinteisiä valtiorajoja sekä fyysisen maailman ja digitaalisen maailman rajaa. Perinteisillä rajajaoilla ei ole enää merkitystä. (Górka 2018, 13.) Turvattomuutta aiheuttaakin tietoisuus teknologioista ja kyvyistä, joilla yksittäiset toimijat voivat haastaa yhteiskuntia ja kokonaisia valtioita kybertoimintaympäristössä mistä päin maailmaa tahansa. Nämä yksittäiset toimijat voivat myös operoida valtion sisältä ja vaikuttaa valtioon haitallisesti. Näillä haitallisilla toimilla on vaikutuksia niin digitaalisessa maailmassa kuin fyysisessä maailmassa.

Ei-valtiollisten toimijoiden osallisuus kybertoimintaympäristössä haastaa valtioiden asemaa, jossa nämä toimivat turvallisuuden ensisijaisina tuottajina. Valtion turvallisuuden tuottajan rooli on haastettuna, kun ei-valtiollinen toimija haastaa valtiota, mutta myös silloin kun ei-valtiollinen toimija toimii valtion puolesta. Turvallisuuden tuottamista täten ulkoistetaan. Valtiot käyttävät ei-valtiollisia toimijoita defensiivisiin ja offensiivisiin kyberoperaatioihin sekä kyberkyvykkyyksien kehittämiseen. (Lupovici 2023, 159.) Tämä haastaa valtioiden suvereniteettia sekä turvallisuuden tuottajan monopolia.

Erilaisia kyberuhkia tarkasteltaessa on myös kyberturvallisuusstrategioissa mainittu erinäisiä haasteita liittyen kyberuhkien torjuntaan. Vaikka kyberturvallisuutta vaarantavissa tilanteissa jokainen toimivaltainen viranomainen johtaa häiriötilanteiden hallintaa kukin oman tehtävänsä ja toimivaltansa puitteissa, on näissä myös tunnistettu heikkouksia kyberuhkien torjuntaan ja niihin vastaamiseksi.

> *”Siitä huolimatta, että yhteistyö on jo nykyisellään toimivaa, viranomaisilla on kuitenkin arvioitu olevan nykytilassa riittämättömät toimintaedellytykset tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia.”* (Kyberturvallisuusstrategia 2024–2035, 20.)

> *”Kyberturvallisuuden yhteistoiminnalle tuovat haasteita sääntelyn ja tehtävien hajautuminen usealle eri toimijalle sekä yhteistoiminnan erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute.”* (Kyberturvallisuusstrategia 2024–2035, 20.)

Puolustusministeriössä palveleva vanhempi osastoesiupseeri Tuomo Rusila mainitsee kehittämiskohteita kansallisessa kyberturvallisuudessa. Rusilan mukaan suurimmat haasteet ovat puutteet lainsäädäntöpohjassa, kankea ja lokeroitunut viranomaisyhteistyö, esteet tiedonjakamisessa sekä riittämättömät resurssit. (Buchtova, Putilin, Vehmaa, The Ulkopolitist, 16.6.2025.) Läpinäkyvyyden ja avoimuuden puute heikentää kyberturvallisuuden toimijoiden välistä luottamusta

ja täten läpinäkymättömyys tulisi olla poikkeava toimintamalli (DCAF 2019, 15). Rusilan mukaan Suomesta uupuu toimintamalli, jossa valtiolliset toimijat ja yksityinen sektori vastaisivat yhteistyöllä ja koordinoidusti toisen valtion vihamieliseen kybertoimintaan. Tämä tunnistetaan myös strategioissa.

> *”Suomessa ei toistaiseksi ole kuitenkaan riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta kybertoimintaympäristössä, eikä säännöksissä ole otettu riittävästi huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa”* (Kyberturvallisuusstrategia 2024–2035, 20).

Suomalaisen kyberturvallisuuden vahvuuksiksi Rusila mainitsee valtion pienen koon, jossa keskeiset yksityisen ja julkisen sektorin toimijat tuntevat toisensa ja toimivat yhdessä luottamukseen ja vapaaehtoisuuteen perustuvissa verkostoissa (Buchtova, Putilin, Vehmaa, The Ulkopolitist, 16.6.2025).

Kansallinen yhteistyö toimii myös toimijoiden yhdistäjänä kyberturvallisuusstrategioissa. Siitä luodaan arvo, joka itsessään on arvokas yhteiskunnassamme. Kansallinen yhteistyö kyberturvallisuusstrategioissa nähdään arvokkaana suomalaisen yhteiskunnan toimintona, joka kattaa kaikki yhteiskunnan toimijat. Kansallinen yhteistyö tai pelkästään kyberturvallisuusstrategiat voivat tuottaa kansallista yhteenkuuluvuuden tunnetta tai ylpeyttä oman valtion saavutuksista. Näihin tunteisiin sisältyvää ideologiaa ei ole yksilön vaikea omaksua itselleen omaan ajatteluun. (Jansson & Sihvonen 2018, 22). Viranomaisten, yritysten ja kansalaisjärjestöjen sekä yksilöiden on tehtävä yhteistyötä toimivan kansallisen kyberturvallisuuden edistämiseksi ja varmistamiseksi.

> *”Kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön”* (Kyberturvallisuusstrategia 2013, 5).

> *”Suomalaisen kyberturvallisuuden toimintamallin ytimessä on yhteistyö eri toimijoiden välillä”* (Kyberturvallisuusstrategia 2024–2035, 8).

Näin turvataan yhtenäisesti myös laajemmin kansallisen turvallisuuden tilaa. Yhteistyössä on kyse yhteisestä projektista, jossa jokaisella on merkitystä ja jokaisella on paikka täytettävänä, jokainen toimija kuuluu johonkin. Tämänlaisten narratiivien rakentaminen antaa valtion eri toimijoille mahdollisuuden rakentaa kybertoimintaympäristöä kontrolloidummaksi ja ennustettavammaksi ympäristöksi (Lupovici 2023, 166). Vaikka kontrolloitu ja ennustettava kybertoimintaympäristö on

tärkeä ontologisen turvallisuuden tuottaja, se ei silti saa rajoittaa liikaa eri toimijoiden mahdollisuuksia, oikeuksia ja vapauksia kybertoimintaympäristössä. Tässäkin suhteessa oikeuksien ja vapauksien punnitseminen on otettava huomioon, kun pohditaan, miten luodaan kokonaisvaltaista yhtenäistä ontologista turvallisuutta.

Kyberturvallisuus on erottamaton osa myös Suomen elinkeinoelämää. ”*Elinkeinoelämä vastaa Suomessa pitkälti digitaalisen infrastruktuurin ja sen palveluiden ylläpidosta ja kehityksestä”* (Kyberturvallisuusstrategia 2024–2035, 18). WithSecuren entinen tutkimusjohtaja Mikko Hyppönen kommentoi, että merkittävä Suomeen kohdistuva kyberuhka on taloudellisen menestyksen perässä olevat järjestäytyneet rikollisjengit. Tätä Hyppönen perustelee maantieteellisellä riippumattomuudella ja rikollinen toiminta voi kohdistua keneen tahansa tasapuolisesti. Näiden rikollisjengien ensisijainen toiminta on rahan kiristäminen ja se on muuttunut Hyppösen mukaan yhä ammattimaisemmaksi. Hyppönen mainitseekin, että näiden kiristäjien ykköskohteita ovat yritykset, joiden maksukykyä on helppo arvioida, jolloin vaadittavat lunnaat voidaan määritellä kohteen maksukyvyn mukaan. (Kärkkäinen, Iltasanomat, 1.6.2022.)

> *”Viranomaiset ja yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin alihankkijoidensa piirissä hallitakseen kyberturvallisuutta koskevia riskejä”* (Kyberturvallisuusstrategia 2019, 8).

> *”Yhteiskunnan kyberturvallisuuden ja elinkeinoelämän näkökulmasta on keskeistä, kuinka kyberturvallisuus saadaan tärkeäksi osaksi myös muiden kuin kyberturvallisuustuotteita, -palveluita ja ratkaisuja tuottavien yritysten toimintaa. Yhä merkittävämmässä roolissa ovat tulevaisuudessa ne yritykset, joiden varsinainen liiketoiminta on kyberturvallisuusalan ulkopuolella mutta joiden toimintaan kyberturvallisuus ja siihen liittyvät häiriöt vaikuttavat merkittävästi. Tällaisia aloja on hahmotettu erityisesti verkko- ja tietoturvaa koskevissa lainsäädäntöhankkeissa, joissa tallaisiksi aloiksi katsottiin muun muassa tietoliikenne, energiatuotanto ja -jakelu, finanssi- ja vakuutusala ja terveydenhuolto.” (*Kyberturvallisuusstrategia 2019, 8–9.)

Viranomaisten ja elinkeinoelämän sujuvan ja mutkattoman yhteistoiminnan varmistamiseksi on oltava resursseja ja osaavaa henkilöstöä. Ilman osaavaa henkilöstöä ei ole toimivaa kyberturvallisuutta. Kyberturvallisuuden kehittäminen, tutkiminen, opettaminen ja toteuttaminen varmistetaan toimivalla yhteistyöllä kansallisilla markkinoilla. Tietojen ja kokemusten vaihto on avainasemassa, kun tunnistetaan erilaisia uhkia ja vastataan niihin. Monialaisella yhteistyöllä voidaan

luoda digitaalisia innovaatioita, joilla on vaikutusta kansalliseen turvallisuuteen. (Yarovoy et al. 2024, 6.)

> *”Kyberuhkiin varautuminen, suojautumisen kehittäminen ja suomalaisten kyberturvallisuusalan yritysten kasvu ovat mahdollisia vain, jos osaavaa työvoimaa on saatavilla. Yhteiskunnallisesti vaikuttavalle ja innovatiiviselle tutkimus- ja kehitystoiminnalle luodaan perusta tukemalla alan perustutkimusta ja koulutusta.”* (Kyberturvallisuusstrategia 2024–2035, 24.)

> *”Kansallisella tasolla on varmistettava, että yrityksillä on sekä huippuosaajia että muuta osaavaa henkilöstöä riittävästi saatavilla. Osaamisen kehittäminen korostuu myös elinkeinoelämän ja tutkimuksen välisessä yhteistyössä. Tiiviillä yhteistyöllä, vaihtamalla tietoja asiakastarpeista ja kehittämällä palvelunkehitystä voidaan luoda merkittävää uutta osaamista jo pelkästään kansallisilla sisämarkkinoilla.”* (Kyberturvallisuusstrategia 2019, 8.)

Kansallinen yhteistyö julkisen hallinnon ja elinkeinoelämän kanssa luo yhteistä näkemystä kyberturvallisuuden tilasta ja kehittämistarpeista. Läpinäkyvä toiminta ja yhteistyö parantavat yleistä ymmärrystä kyberturvallisuuteen liitettävistä riskeistä ja kannustavat yhteiskunnan eri toimijoita toimimaan yhdessä näiden riskien ehkäisemiseksi ja vastaamiseksi (DCAF 2019, 15). Tuomo Rusilan mukaan Suomesta kuitenkin puuttuu elinkeinoelämän ja valtion yhteistä operatiivista kybertoimintaa. Yhteisen operatiivisen toiminnan kautta yritykset saisivat havaintoja, kokemuksia ja ideoita oman toimintansa ja tuotteidensa kehittämiseen, mutta olisivat myös tuomassa omaa tietoa ja osaamistaan viranomaisten käyttöön sekä tietoisuuteen. (Buchtova, Putilin, Vehmaa,The Ulkopolitist, 16.6.2025.) Elinkeinoelämä on myös keskeinen tekijä suomalaisessa kokonaisturvallisuuden mallissa ja siksi kriittinen turvallisuuden osa-alue. Suurinta osaa Suomen kansallisen turvallisuuden kannalta kriittisestä infrastruktuurista, palveluista sekä tuotannoista, vastaa, operoi ja omistaa, yksityisen sektorin toimijat. Yhteiskunnan kriittisillä aloilla toimiville yrityksille onkin asetettu lakiin perustuvia velvoitteita huolehtia oman toiminnan jatkuvuudesta kaikissa olosuhteissa. (Yhteiskunnan turvallisuusstrategia 2025, 42.)

Tietoevryn Tech Services -yksikön turvallisuusjohtaja Jari Pirhonen huomauttaa kuitenkin, että kaikki yritykset eivät ole yhtä hyvin varautuneita kasvaviin kyberuhkiin nykyään. Tämä on tunnistettu myös strategioissa.

> *”Suomessakin on havaittavissa globaali trendi, joka jakaa yrityksiä ja toimialoja: organisaatiot jakautuvat yhä selkeämmin niihin, jotka ovat huolehtineet omasta*

> *kyberturvallisuudestaan ja niihin, jotka eivät ole. Keskinäisriippuvaisessa maailmassa tämä aiheuttaa riskejä koko yhteiskunnalle."* (Kyberturvallisuusstrategia 2024–2035, 18.)

Pirhosen mukaan parhaiten varautuneita yrityksiä ovat ne, joiden toimialalla vallitsee tiukasti säännelty lainsäädäntö. Näitä ovat teleliikenne-, ICT- ja ohjelmisto- sekä finanssialat. Pirhosen mukaan tämä kertoo siitä, että *"tiukempi sääntely ohjaa yrityksiä panostamaan järjestelmällisemmin kyberturvaan."* Säännelty kybertoimintaympäristö nähdään myös mahdollisuutena liiketoiminnan kehittämiselle ja mahdollisille investoinneille. Säännelty kybertoimintaympäristö sekä yritysten toimiva kyberturvallisuus luo luottamusta ulkomaalaisille toimijoille sijoittaa liiketoimintaa sekä pääomaa Suomeen. Kansanedustaja ja kyberturvallisuuden dosentti Jarno Limnellin mukaan: *"kyberturvallisuus luo merkittäviä Suomen talouskasvua tukevia liiketoimintamahdollisuuksia. Suomen kannattaa panostaa kasvaviin kansainvälisiin kyberturvallisuusmarkkinoihin, sillä Suomessa on arvostettua osaamista ja erinomaisia alan yrityksiä."* (Suomen tietotoimisto, 10.10.2024.)

> *"Kybertoimintaympäristöä säätelevän kansallisen lainsäädännön tulee olla sellaista, että liiketoiminnan kehittämiselle on olemassa suotuisat edellytykset. Tämä mahdollistaa osaltaan kansainvälisesti tunnustetun, kilpailukykyisen ja vientimahdollisuudet omaavan kyberosaamisklusterin syntymisen. Samalla Suomesta kehittyy houkutteleva kyberturvallinen toimintaympäristö, johon kannattaa tehdä investointeja ja yritysten toimintojen sijoituspäätöksiä."* (Kyberturvallisuusstrategia 2013, 10.)

> *"Turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä lisää taloudellista aktiviteettia. […] Kyberturvallisuuskehityksen varmistamiseksi huolehditaan siitä, että Suomessa on voimassa sellainen lainsäädäntö ja kannustimet, jotka tukevat tämän alueen yritystoimintaa ja sen kehittymistä. Alan osaaminen kehittyy keskeiseltä osaltaan yritystoiminnan kautta."* (Kyberturvallisuusstrategia 2013, 1, 5.)

> *"Tavoitteena on, että Suomi pystyy tuottamaan globaalisti kilpailukykyisiä kyberturvallisuusalan teknologisia ratkaisuja kasvun mahdollistamiseksi. Suomen TKI-ympäristön tulee kannustaa ja tukea kyberturvallisuutta vahvistavien ratkaisujen kehittämistä ja hyödyntämistä sekä niitä kaupallistavien yritysten kansainvälistä kilpailukykyä. Samalla edistetään sekä Suomen kyberturvallisuusalan että laajemmin*

> *turvallisen TKI- ja liiketoimintaympäristön houkuttelevuutta suomalaisille ja ulkomaalaisille osaajille, yrityksille ja investoinneille."* (Kyberturvallisuusstrategia 2024–2035, 26.)

Yhteisen toimivan ja turvallisen kybertoimintaympäristön ja kansallisen lainsäädännön kehittämiseksi vaaditaan julkisen ja yksityisen sektorin vuoropuhelua kehittämistarpeista. Pirhosen näkemyksen mukaan velvoittavuuden ja toimivan vapaaehtoisen toiminnan välille täytyy löytää toimiva kompromissi. (Buchtova, Putilin, Vehmaa, The Ulkopolitist, 16.6.2025.) Toimivan kompromissin löytäminen on edellytys yhtenäiselle kyberturvallisuuden kehittämiselle ja toiminnalle. Yhteisesti hyväksytty ratkaisu luo toimijoille myös ennustettavuutta ja luottamusta toisiinsa, jolloin toisen toimijan kanssa toimiminen on entistä helpompaa. Yhteiskunnan toimijoiden keskinäinen luottamus on nostettu strategioissakin esiin tärkeänä turvallisuuden tunteen luojana.

> *"Yhteiskunnan eri toimijoiden keskinäinen luottamus sekä luottamus julkisiin instituutioihin ja niiden palveluihin rakentavat vahvaa kansallista resilienssiä. Luottamus on onnistuneen kansallisen kyberturvallisuustyön, varautumisen, yhteisesti jaetun tilanneymmärryksen ja oikea-aikaisen reagoinnin edellytys."* (Kyberturvallisuusstrategia 2024–2035, 28–29.)

Kyberturvallisuusstrategiat itsessään ovat myös turvallisuuden viestinnän väline ja niiden tarkoitus on herättää erinäisiä tuntemuksia vastaanottajassa. Strategioilla valtio viestii niin kansalaisilleen, mutta myös ulkoisille liittolaisilleen ja vastustajilleen. Strategiatekstit mahdollistavat valtioille oman toiminnan esittelemisen muille ja keinon saada ne vakuuttuneiksi tämän suorituskyvyistä erinäisissä ongelmatilanteissa. Ne toimivat niin sisäisinä kuin ulkoisina viesteinä. Kyberturvallisuusstrategiat ovat valtion intressien ja tavoitteiden perusteella tuotettuja asiakirjoja, joissa luodaan erilaisia näkemyksiä suorituskykyisestä ja luotettavasta kybervaltiosta. Strategia-asiakirjoissa nimetyt uhkat ja häiriötilanteet toimivat näyteikkunana sille, että valtio pystyy esittelemään omaa kykyään varautua erilaisiin uhkiin ja turvaamaan oman suvereniteettinsa sekä kansalaisensa. (Jansson & Sihvonen 2018, 17.)

Ontologisen turvallisuuden tunteeseen ja kokemiseen vaikuttaa myös tietoisuus uhkista ja kyvyistä niiden ennaltaehkäisemiseksi ja torjumiseksi. Tiedostettuja uhkia vastaan on helpompi varautua ja siten myös tapahtuessaan torjua, kuin sellaisia, joita ei ole tiedostettu. Nämä uhkat vaikuttavat niin yksittäisen ihmisen kuin yhteisöjen ja yhteiskunnan toimintaan.

> *”Vihamielinen valtiollinen toiminta, kyberrikollisuus, palvelunestohyökkäykset, tietovuodot ja erilaiset haittaohjelmat sekä muut häiriötilanteet ovat yleistyneet myös Suomessa”* (Kyberturvallisuusstrategia 2024–2035, 17).

> *”Kun vihamielinen kybertoiminta lisääntyy ja kohdistuu yhä laajemmin myös hallituksiin, demokraattisiin instituutioihin, yrityselämään ja yksilöihin, kasvaa tarve rajat ylittävälle yhteistyölle. Tämän vuoksi oman toimintaympäristön, tietojärjestelmien ja etenkin näiden keskinäisriippuvuuksien tuntemus on entistä tärkeämpää.”* (Kyberturvallisuusstrategia 2024–2035, 14.)

Kansallinen kokonaisvaltainen yhteistyö perustuu yhteiskunnan toimijoiden väliseen yhteistyöhön kyberturvallisuuden alalla. Viranomaiset, elinkeinoelämä sekä yksilöt ovat osa tätä yhteistyön kenttää. Yhteistyö nähdään strategioissa jo arvona itsessään ja se nähdään mahdollisuutena parantaa Suomen asemaa esimerkiksi talouselämässä. Kokonaisvaltainen kansallinen yhteistyö antaa mahdollisuuden kehittää suomalaista kyberturvallisuutta suunnitelmallisesti ja kaikille toimijoille toimivaksi. Kansallinen yhteistyö on myös toimijoita yhdistävä tekijä. Toimivalla, luotettavalla ja läpinäkyvällä kyberturvallisuudella voidaan vaikuttaa yksilöiden suhtautumiseen julkisia instituutioita kohtaan. Valtiollekin on etunsa mukaista, että yksilöt luottavat sen toimintaan ja palveluihin. Toimijoiden välinen luottamus heijastelee myös kyberturvallisuuden kehittämiseen. Yhteiset kansalliset intressit ja toimijoiden välinen luottamus rakentavat yhtenäistä suomalaista kyberpolitiikkaa ja luovat ehjää kokonaista turvallisuuden tilaa, joka heijastuu myös yhteiskunnan kriisinkestävyyteen ja kykyyn vastata kybertoimintaympäristössä ilmeneviin uhkiin.

5 KANSAINVÄLINEN YHTEISTYÖ KYBERTURVALLISUUDESSA

Kybertoimintaympäristö on maailmanlaajuinen ja se on haavoittuva useasta kohdasta. Kokonaisuutena kybertoimintaympäristö on rakennettu laajan verkon ympärille, jossa yksilöt kommunikoivat ja vaikuttavat toistensa kanssa kansalaisuudesta, etnisyydestä, poliittisesta suuntautumisesta tai sukupuolesta huolimatta, ilman selkeitä omistussuhteita ja valtasuhteita. Kybertoimintaympäristön globaali luonne ja rakenne edellyttääkin laajaa kansallista sekä kansainvälistä yhteistoimintaa. (Laari et al. 2019, 10–14; Mihr 2014, 24.) Suomikin osallistuu valtiona kansainväliseen kyberturvallisuuden yhteistoimintaan sen liittolaisten ja samanmielisten valtioiden kanssa. Suomen harjoittama kansainvälinen yhteistyö liittolaisten ja samanmielisten valtioiden kanssa vaikuttaa sen käsitykseen itsestään ja sen paikasta maailmassa. Tämä kansainvälinen yhteistyö on yhteydessä Suomen ontologisen turvallisuuden muotoutumiseen.

Kansainvälinen yhteistyö valtioiden kesken ei palvele vain yksittäin yhtä tai yksittäisiä valtioita, vaan myös laajemmin kansainvälistä yhteisöä. Kansainvälinen yhteistyö edesauttaa kansainvälisen turvallisuuden ylläpitämisessä. Kansainvälinen yhteistyö ehkäisee valtioiden välistä epävarmuutta toisistaan. Epävarmuus onkin turvallisuuden keskeisin dilemma (Mitzen 2006, 341). Ilman ennustettavuutta, jatkuvuutta ja tietoisuutta toisten valtioiden toimista ja intresseistä, syntyy epävarmuutta, joka useimmiten johtaa konflikteihin ja sotiin valtioiden välillä, kun turvallisuusintressit ja -pyrkimykset joutuvat ristiriitaan toimijoiden välillä. Valtioiden keskeinen motiivi turvallisuustoimilleen on ehkäistä kansainvälistä anarkiaa (mm. Mearsheimer 2009).

Kybertoimintaympäristö vaikuttaa yhä vahvemmin myös kansainvälisissä suhteissa. Politiikkaa tehdään fyysisen maailman lisäksi kybermaailmassa yli valtiorajojen. Kybertoimintaympäristö tarjoaa kustannustehokkaan alustan politiikan tekemiselle ja kampanjoimiselle. Kansainvälisen politiikan toimintaympäristö ja toimijat ovat laajentuneet myös kybertoimintaympäristöön ja se haastaa perinteistä käsitystä kansainvälisestä järjestelmästä. Valtioiden perinteistä valtaa hallita rajojaan, politiikkaa ja taloutta on haastettu kybertoimintaympäristössä jo pitkään. Kybertoimintaympäristön laajuus, nopea kehitys sekä alhaisemmat kustannukset kansainväliselle toiminnalle haastavat valtioita yhä enemmän. (Lupovici 2023, 158.) Kybertoimintaympäristöä hyödynnetäänkin aktiivisesti erilaisten poliittisten päämäärien saavuttamiseksi niin kansallisesti kuin kansainvälisestikin. Kybertoimintaympäristössä valtioita haastavat elementit pakottavat näitä etsimään ja vahvistamaan niiden valtaa ja paikkaansa maailmassa. Valtioiden on kyettävä luomaan uusia erilaisia käytäntöjä ja periaatteita hallitakseen kybertoimintaympäristön jatkuvaa muutosta.

> *”Toimintaympäristön muutos haastaa kansainvälistä sääntöpohjaista järjestelmää. Uhkat ovat moninaistuneet ja kyberympäristöä hyödynnetään laajalti hybridivaikuttamisessa, rikollisuudessa, terrorismissa ja sodankäynnissä. Valtioiden välillä kybervaikuttamista käytetään myös poliittisten päämäärien ajamiseen.”* (Kyberturvallisuusstrategia 2024–2035, 13.)

> *”Kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella”* (Kyberturvallisuusstrategia 2013, 1).

Suomen harjoittama kansainvälinen yhteistyö kyberturvallisuuden alalla nousee esiin kyberturvallisuusstrategioissa. Etenkin Suomen tuore Nato -jäsenyys tuo uusia mahdollisuuksia mutta myös velvollisuuksia kyberturvallisuuteen liittyen. Myös Euroopan Unioni (EU) on aineistossa merkittävä kansainvälinen yhteistyökumppani. Suojelupoliisin entisen päällikön Antti Pelttarin mukaan Nato tuo Suomelle uuden kansainvälisen yhteistyön ympäristön kyberturvallisuudessa (Rautio, Yle, 21.4.2023). Kyberturvallisuusstrategioissakin tunnistetaan kansainvälisen yhteistyön merkitys.

> *”Kansainvälinen yhteistyö on Suomen kyberturvallisuudelle elintärkeää.”* (Kyberturvallisuusstrategia 2019, 5).

> *”Nato-jäsenyys vahvistaa Suomen turvallisuutta ja puolustusta, mutta asettaa samanaikaisesti uusia haasteita ja velvollisuuksia. Nato-jäsenyyden pelotevaikutus saattaa johtaa vihamielisen toiminnan painopisteen siirtymiseen perinteisistä uhkista entistä enemmän kybertoimintaympäristöön, jossa tekijän on helpompi kiistää osallisuutensa. Teknologian kehittyminen, datalähtöisyys, kansainvälinen yhteistyö sekä kybertoiminnan geopoliittisten yhteyksien analysointi luovat kuitenkin entistä paremmat mahdollisuudet erityisesti valtiollisten toimijoiden attribuoimiseksi eli syyksilukemiseksi.”* (Kyberturvallisuusstrategia 2024–2035, 14.)

> *”Euroopan unionin päätökset sekä EU:ssa tehtävä yhteistyö luovat selkärangan Suomen kansalliselle kyberturvallisuuspolitiikalle ja sen kehittämiselle. Suomi on aktiivisesti mukana kehittämässä EU:n kyberturvallisuuteen liittyvää yhteistä ulko- ja turvallisuuspolitiikkaa.”* (Kyberturvallisuusstrategia 2019, 5.)

> *”Euroopan unioni sekä monet kansainväliset järjestöt, kuten YK, ETYJ, Nato ja OECD, ovat Suomelle tärkeitä foorumeita kyberturvallisuutta kehitettäessä. EU toimii yhä*

> *aktiivisemmin kyberturvallisuuden alalla ja sillä on myös yhteistyötä kolmansien maiden kanssa. Suomi osallistuu aktiivisesti tähän kehittämistyöhön."* (Kyberturvallisuusstrategia 2013, 9.)

Kansainvälisillä foorumeilla tehtävä kyberturvallisuuden yhteistyö on aineiston perusteella Suomelle tärkeää. Ennen Nato-jäsenyyttä (Kyberturvallisuusstrategioissa 2013 ja 2019) Suomen kansainvälinen operatiivinen kyberyhteistyö nojautui pitkälti EU:n ja sen jäsenmaiden virastojen kanssa tehtävään yhteistyöhön kyberturvallisuudessa.

> *"Jatketaan ja syvennetään kansainvälistä operatiivista yhteistyötä ja tiedonvaihtoa EU:n ja muiden maiden lainvalvontaviranomaisten ja vastaavien toimijoiden kuten Europolin kanssa"* (Kyberturvallisuusstrategia 2013, 8).

> *"Vastatoimien kehittämisessä otetaan huomioon EU:n vahvan kyberpuolustuksen kehittämisen linjaukset"* (Kyberturvallisuusstrategia 2019, 5).

Suomen kyberturvallisuusstrategiat toimivat osana EU:n kyberturvallisuusstrategian toimeenpanoa sekä EU:n kyberturvallisuusdirektiiviä (EU 2022/2555). EU:n kyberturvallisuusstrategian tavoitteena on kehittää EU:n yhteisiä valmiuksia vastata merkittäviin kyberhyökkäyksiin sekä hahmotella kumppaneiden kanssa tehtävää yhteistyötä kansainvälisen turvallisuuden ja vakauden varmistamiseksi. (Euroopan komissio, ec.europa.eu.) EU:n kyberturvallisuusdirektiivin (NIS 2-direktiivi) tavoitteena on kyberturvallisuuden yhteisen tason varmistaminen koko EU:n alueella (kyberturvallisuuskeskus.fi). Suomen kyberturvallisuusstrategiat toimivat näiden dokumenttien jatkeena kansallisella tasolla, jolla muodostetaan unionin tasoista kyberturvallisuuspolitiikkaa. Suomen kyberturvallisuusstrategioissa linjataan myös Suomen tavoitteesta olla aktiivinen toimija unionin tason kyberlainsäädännön kehittämisessä.

> *"Kyberturvallisuusstrategia ja sen toimeenpano ovat myös osa EU:n kyberturvallisuusstrategian toimeenpanoa"* (Kyberturvallisuusstrategia 2019, 4).

> *"Kyberturvallisuusstrategian uudistamista on edellyttänyt myös Euroopan unionin kyberturvallisuusdirektiivi (NIS 2) ja sen kansallinen täytäntöönpano"* (Kyberturvallisuusstrategia 2024–2035, 10).

> *"EU:n uuteen kyberlainsäädäntöön kytkeytyy standardointi- ja sertifiointityö. Suomen etu on olla aktiivinen kyberturvallisuuden standardien ja sertifiointijärjestelmien kehittämisessä sekä käyttämisessä."* (Kyberturvallisuusstrategia 2024–2035, 25.)

EU:n lisäksi Suomi tekee yhteistyötä myös Natossa. Naton osalta Suomi joutui ennen täysjäsenyyttään toimimaan kumppanuusohjelman puitteissa, jolloin Suomen osallistuminen oli rajattua muun muassa tiedonvaihdon osalta. Suomen Nato-jäsenyyden astuessa voimaan Suomella on ollut mahdollisuus osallistua Naton sisällä tehtävään kyberturvallisuuden yhteistyöhön täysin oikeuksin ja mahdollisuuksin. On Suomen kansallisen edun mukaista sekä Suomen kansainvälisen aseman vahvistamiseksi keskeistä, että Suomi on mukana kehittämässä koko puolustusliiton kyberturvallisuutta ja -puolustusta aktiivisena jäsenmaana, joka tuottaa myös turvallisuutta liittokunnassa. (Suomen tietotoimisto, 10.10.2024).

> *”Sotilaallisesti liittoutuneena maana Suomi edistää jatkossa Naton kyberpuolustuksen kehittämistä ja hyödyntää liittokunnan suorituskykyjä. Tätä tukee kyberpuolustuksen suunnitelmallinen kehittäminen ja ylläpitäminen osana kansallista kyberturvallisuutta. Suomen infrastruktuuria kehitetään osana liittokunnan infrastruktuuria, mikä vahvistaa yhteistyötä ja kyberpuolustusta.”* (Kyberturvallisuusstrategia 2024–2035, 33.)

Suomen kyberturvallisuusstrategiat ja niissä mainittu kansainvälinen yhteistyö vahvistavat Suomen paikkaa maailmassa. Suomi identifioituu läntiseen arvomaailmaan, jossa oikeusvaltioperiaate, demokratia, kansainvälinen oikeus sekä ihmisoikeudet ovat keskiössä. Strategioissa mainitaankin, että Suomen tärkeimmät kumppanit liittyen kyberturvallisuuteen ovat samanmieliset valtiot, jotka jakavat saman arvopohjan. Tämä sisältää Suomen liittolaiset EU:ssa sekä Natossa.

> *”Kyberyhteistyötä tehdään laajasti ja syvennetään erityisesti keskeisten samanmielisten EU-maiden, Pohjoismaiden sekä euroatlanttisten ja myös joidenkin indopasifisen alueen maiden kanssa yhteisten arvojen pohjalta”* (Kyberturvallisuusstrategia 2024–2035, 32).

> *”Kansainvälinen yhteistyö nojaa voimassa olevaan kansainväliseen oikeuteen, kansainvälisiin sopimuksiin ja ihmisoikeuksien kunnioittamiseen myös kybertoimintaympäristössä. Suomi haluaa säilyttää universaalin, vapaan ja vakaan internetin ja mahdollistaa sen turvallisen käytön. Suomi ei hyväksy pyrkimystä rajoittaa internetin vapautta ja avoimuutta ja sitä kautta yksilön perusoikeuksia ja -vapauksia. Suomi korostaa kaikessa kyberturvallisuuden yhteistyössä oikeusvaltionäkökohtia, demokratiaa ja läpinäkyvyyttä.”* (Kyberturvallisuusstrategia 2019, 5.)

Samanmielisten valtioiden ja liittolaisten kanssa tehtävä yhteistyö vahvistaa Suomen ontologista turvallisuutta. Liittolaismaiden kanssa tehtävän kansainvälisen yhteistyön kautta Suomi vahventaa asemaansa osana läntisiä instituutioita, kuten EU:ta ja Natoa. Keskeinen osa yhteiskuntaa on sen

identiteetti ja omaleimaisuus muihin yhteiskuntiin nähden. Kansakunnat peilaavat ja vertaavat itseään muihin kansoihin ja etsivät eroavaisuuksia, jotka erottavat ne muista. Yksi tärkeä tapa, jolla yhteiskunnat säilyttävät omaleimaisuutensa, on rutiininomaisesti muokata suhteitaan muihin yhteiskuntiin. Tämänlaiset valtioiden väliset rutiinit auttavat ylläpitämään kunkin yhteiskunnan identiteetin yhtenäisyyttä, mikä puolestaan tarjoaa yksilöille ontologista turvallisuutta, kun yksilöt kokevat kuuluvansa johonkin suurempaan sosiaaliseen yhteisöön. Yksilöiden kokema omaleimaisuus ja identiteetti omasta kansastaan ovat yhteiskuntia ylläpitäviä ja muokkaavia tekijöitä, joka vaikuttaa perustavanlaatuisesti myös ontologiseen turvallisuuteen. (Mitzen 2006, 352.)

Suomen harjoittama kansainvälinen kyberturvallisuusyhteistyö, strategioissa mainittujen samanmielisten valtioiden ja liittolaisten kanssa (EU ja Nato), viestii kansalaisille, että Suomi kuuluu tiettyyn kansainväliseen yhteisöön ja kansalaiset ovat osa tätä suurempaa yhteisöä. Tämänlainen kuuluminen ilmenee konkreettisesti Suomen EU- ja Nato-jäsenyyksien kautta. Kansallista identiteettiä täytyy ylläpitää, jotta kansalaiset eivät menetä tunnettaan omasta omaleimaisuudestaan ja identiteetistään. Tämä identiteetin ylläpitäminen liittyy Lupovicin (2023) mainitsemaan valtion käsitykseen itsestään (*state´s sense of self*) ja valtion omasta paikasta maailmassa. Identiteetin ja omaleimaisuuden menettäminen lisää ontologista turvattomuutta yksilöissä, kun he eivät koe kuuluvansa enää mihinkään sosiaaliseen yhteisöön ja ovat vaarassa jäädä sosiaalisesti yksin (Mitzen 2006, 352). Kansallista identiteettiä ja omaleimaisuuden tunnetta – ontologista turvallisuutta – ylläpidetään ja luodaan kansainvälisellä toiminnalla peilaamalla omaa asemaa toisiin toimijoihin.

> *”Suomi on luotettava toimija euroatlanttisessa yhteistyössä ja turvallisuuden tuottaja ja vastuullinen valtiotoimija myös kyberympäristön osalta”* (Kyberturvallisuusstrategia 2024–2035, 32).

> *”Suomen tavoite on edelleen olla kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa”* (Kyberturvallisuusstrategia 2019, 4).

Strategioissa Suomesta luodaan aktiivista toimijaa kansainvälisessä kyberpolitiikassa. Strategioissa Suomi vaikuttaa kyberturvallisuuden kehittämiseen kaikilla sen kansainvälisillä yhteistyöfoorumeilla ja kaikilla kyberturvallisuuden osa-alueilla.

> *”Suomi jatkaa tiivistä osallistumista kybertoimintaympäristöä koskevaan normatiiviseen kansainväliseen yhteistyöhön ja näkemysten vaihtoon siitä, miten kansainvälinen oikeus tietyissä kysymyksissä sääntelee valtioiden informaatio- ja kommunikaatioteknologioiden käyttöä”* (Kyberturvallisuusstrategia 2024–2035, 32).

> *”Suomi vaikuttaa kansainväliseen kyberturvallisuusagendaan aktiivisesti Euroopan unionissa ja keskeisissä kansainvälisissä järjestöissä (mm. YK, OECD, ETYJ, Nato-kumppanuuden puitteissa). Tämä on osa kansainvälisen sääntöpohjaisen järjestelmän vahvistamista, mikä on Suomen ulkopolitiikan keskeinen tavoite.”* (Kyberturvallisuusstrategia 2019, 5.)

> *”Suomi edistää monenvälistä kyberdiplomatiaa tavoitteenaan avoimen, vapaan, turvallisen ja vakaan kyberympäristön luominen ja säilyttäminen”* (Kyberturvallisuusstrategia 2024–2035, 32).

Suomen Nato-jäsenyys on tuonut myös uusia velvoitteita ja haasteita mutta myös mahdollisuuden Suomelle nousta esille ja kasvattaa omaa kansainvälistä asemaa muiden valtioiden silmissä. Strategioissa Suomi esitetään vahvana kyberturvallisuuden osaajana ja turvallisuuden tuottajana yhtenä liittokunnan jäsenenä. Strategioissa Suomi esitetään arvokkaana liittokunnan jäsenenä, jonka tavoitteena on vaikuttaa liittokunnan toimintaan.

> *”Nato-jäsenyytemme vahvistaa Suomen kyberturvallisuutta ja -puolustusta, mutta asettaa myös uusia velvollisuuksia. Haluamme olla vahva kyberturvallisuuskumppani Euroopan unionissa ja Natossa*.” (Kyberturvallisuusstrategia 2024–2035, 8.)

Suomi tekee strategioissa itsensä näkyväksi kansainvälisessä liittokunnassa. Tämä on Suomen kannalta tärkeää sisäisen kansallisen identiteetin luomiseksi ja ylläpitämiseksi. Näin suomalaiset näkevät itsensä yhä vahvemmin läntisen maailman jäseninä. Suomen paikkaa maailmassa vahvistetaan kansainvälisellä yhteistyöllä kertomalla, että yhteistyötä tehdään muiden läntisten yhteisöjen kanssa. Nykyisessä poliittisessa ajassa Ukrainan sodan laajennettua vuonna 2022, Naton sisälläkin väitellään jäsenmaiden aktiivisuudesta ja panostuksesta yhteiseen puolustukseen (Natosta mm. Gheciu & von Hlatky 2024). Aktiivisesta puolustuksesta ja varautumisesta on luotu tavoiteltava tila, jonka kautta pääsee vaikuttamaan maailmanpolitiikassa. Uskottavalla puolustuksella ja toimivalla turvallisuuspolitiikalla saa luotua suhteita ja luottamusta etenkin Yhdysvaltoihin, jonka merkitys Euroopan turvallisuuteen on edelleen merkittävä. Aktiiviset liittokunnan jäsenet, jotka pitävät huolta omasta puolustuksestaan ja turvallisuudestaan, eivätkä ole pelkästään turvallisuuden kuluttajia, saavat luotua läheisiä suhteita Yhdysvaltoihin.

> *”Suomi on rakentava, luotettava ja suorituskykyinen Nato-liittolainen. Suomi ylläpitää vahvaa kansallista puolustuskykyä osana Naton yhteistä pelotetta ja puolustusta ja osallistuu aktiivisesti Naton kyberpuolustuksen kehittämiseen. Naton jäsenenä Suomi pyrkii kybersuorituskykyjen kehitystyön ytimeen. Tavoitteena on olla merkittävä*

> *liittokunnan ratkaisujen tuottaja kyberturvallisuudessa ja kyberpuolustuksessa."* (Kyberturvallisuusstrategia 2024–2035, 33.)

Suomalainen kyberturvallisuusosaaminen nähdään myös vientituotteena ja kansainvälisenä tavoitteena kyberturvallisuusstrategioissa. Etenkin suomalainen kokonaisturvallisuuden malli, varautumisajattelu sekä moniviranomaisyhteistyö koetaan ainutlaatuisina suomalaisen turvallisuustyön malleina, joita kannattaa lähteä markkinoimaan kansainvälisesti. Jarno Limnellin mukaan, *"kyberturvallisuus ei ole vain uhkiin varautumista, vaan myös merkittävä Suomen talouskasvua tukeva liiketoimintamahdollisuus."* (Suomen tietotoimisto, 10.10.2024). Suomessa on paljon kyberturvallisuuteen ja teknologiaan keskittyviä yrityksiä, joiden osaamista arvostetaan myös kansainvälisesti. Suomelle olisi eduksi, jos nämä kyberturvallisuuteen keskittyneet yritykset pääsisivät panostamaan kansainvälisiin kyberturvallisuuden markkinoihin. Tätä kautta Suomelle avautuisi myös mahdollisuus esitellä sekä edistää omaa kansallista varautumisen ja kokonaisturvallisuuden mallia vientituotteena. (ibid.) Suomalaisen kyberturvallisuusosaamisen edistäminen kansainvälisesti on mainittu yhdeksi strategiseksi tavoitteeksi myös kyberturvallisuusstrategiassa 2024–2035.

> *"Suomi edistää yhteistyötä ja vuoropuhelua korostavaa varautumisen toimintamallia myös EU- ja Nato-yhteistyössä ja edesauttaa kyberturvallisuuden varautumismallin ja parhaiden käytäntöjen soveltamista myös kumppanimaissa"* (Kyberturvallisuusstrategia 2024–2035, 28).

> *"Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Meillä on vahva osaamisperusta sekä pitkät perinteet tiivistä ja luottamuksellista yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojen välisestä yhteistyöstä."* (Kyberturvallisuusstrategia 2013, 3.)

> *"Suomi edistää kyberturvallisuuden varautumismalliaan vientituotteena"* (Kyberturvallisuusstrategia 2024–2035, 27).

Kyberturvallisuusstrategioissa tunnistetaan myös kansainväliset kyberharjoitukset mahdollisuutena edistää kansainvälistä yhteistyötä. Harjoitukset ovat konkreettinen mahdollisuus päästä näyttämään suomalaista kyberosaamista kansainvälisessä ympäristössä. Harjoitukset toimivat osaltaan edellä mainitun kokonaisturvallisuuden ja varautumisajattelun sekä suomalaisen kyberturvallisuusosaamisen markkinointikeinona, mutta myös mahdollisuutena oppia uutta, jolla voidaan kehittää kansallista kyberosaamista.

> *”Kansainväliset kyberharjoitukset tukevat rajat ylittäviin kyberuhkiin ja häiriöihin varautumista, päätöksentekoa ja vastaamista. Suomelle on tärkeää osallistua kansainvälisiin kyberharjoituksiin, vaikuttaa niissä aktiivisesti sekä kehittää ja tarjota kyberharjoitusosaamista kansainvälisille kumppanimaille.”* (Kyberturvallisuusstrategia 2024–2035, 30.)

> *”Toimijat parantavat kansainvälisissä harjoituksissa parhaiden käytänteiden ja saatujen oppien hyödyntämistä tehostamalla tiedonvaihtoa ja koordinaatiota. Harjoitustoiminnan tavoitteena on parantaa osallistujien mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kehittää suorituskykyjään ja kouluttaa henkilöstöään.”* (Kyberturvallisuusstrategia 2013, 7.)

Strategioissa on huomattavissa eroja kansainvälisen toiminnan suhteen. Vuoden 2013 strategiassa mainitaan kansainvälisestä yhteistyöstä niukasti. Verrattuna uusimpaan strategiaan (2024–2035), Suomen kansainvälisestä yhteistyöstä kerrotaan jo enemmän ja laajemmin. Strategioissa erottuu myös Suomen motiivit osallistua kansainväliseen yhteistoimintaan. 2013 vuoden strategiassa Suomen kansainvälisen toiminnan perusta on oman kansallisen kyberturvallisuuden kehittäminen, kun taas uusimmassa strategiassa Suomi osallistuu aktiivisesti kansainväliseen kyberpolitiikan kehittämiseen. 2013 vuoden strategiassa kansainvälisestä yhteistyöstä halutaan saada oppia ja toimintamalleja oman kansallisen kyberturvallisuuden järjestämiseen ja kehittämiseen.

> *”Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa”* (Kyberturvallisuusstrategia 2013, 9).

> *”Jokainen viranomainen omalla toimialallaan harjoittaa yhteistyötä erityisesti niiden valtioiden ja organisaatioiden kanssa, jotka ovat maailmanlaajuisesti edelläkävijöitä kyberturvallisuuteen liittyvissä asiakokonaisuuksissa”* (Kyberturvallisuusstrategia 2013, 9).

Vuoden 2013 strategiassa Suomi esitetään vielä oppijan roolissa kansainvälisessä yhteistoiminnassa, kun taas uusimmassa strategiassa (2024–2035) Suomi esitetään aktiivisena toimijana, joka on päättämässä ja vaikuttamassa kansainvälisesti kyberturvallisuuteen, etenkin muiden länsimaiden keskuudessa.

> *”Suomi vaikuttaa kyberturvallisuutta, kyberrikollisuutta ja kyberpuolustusta koskevaan päätöksentekoon niin YK:ssa, EU:ssa, Natossa kuin muissakin keskeisissä*

> *kansainvälisissä järjestöissä ja verkostoissa. […] Vaikuttamalla EU:ssa Suomi edistää kokonaisturvallisuuden kannalta tärkeitä hankkeita ja päätöksiä, jotka kehittävät unionin ja sen jäsenmaiden varautumista."* (Kyberturvallisuusstrategia 2024–2035, 32.)
>
> *"Suomi osallistuu ja vaikuttaa aktiivisesti EU:n kyberturvallisuustyöhön, mukaan lukien EU:n kyberturvallisuusvirasto ENISA:n ja Euroopan kyberturvallisuuden kompetenssikeskuksen ECCC:n toiminta. […] Suomi vaikuttaa aktiivisesti EU:n kyberturvallisuuspolitiikan- ja sääntelyn kehittämiseen ja vie omaa kansallista kokonaisturvallisuuteen ja ennakolliseen varautumiseen pohjautuvaa malliaan unioniin ja muihin jäsenmaihin."* (Kyberturvallisuusstrategia 2024–2035, 32.)

Kansainvälistä yhteistyötä analysoitaessa on kuitenkin otettava huomioon kyberturvallisuusstrategioiden rajallisuus. Strategiat eivät yksiselitteisesti ohjaa Suomen harjoittamaa kyberpolitiikkaa kansainvälisesti. Tähän ulkopolitiikkaan vaikuttavat myös monet muut valtion strategiat ja ulkopoliittiset käytännöt. Kyberturvallisuusstrategiat ovat alistettu yhteiskunnan turvallisuusstrategioihin ja käsittelevät vain yhtä turvallisuuden ulottuvuutta – kyberturvallisuutta. Strategioiden linjauksia on pystyttävä katsomaan osana kokonaisuutta, kun pohditaan valtion turvallisuus- tai ulkopolitiikkaa.

Kyberturvallisuusstrategioissa kansainvälinen yhteistyö ei kuitenkaan jää huomiotta, vaikka sitä käsitelläänkin strategiakohtaisesti eri laajuudella ja syvyydellä. Syytä sille, miksi strategiat ovat sisällöltään ja pituudeltaan eriäviä, ei ole löydettävissä tietoa. Syitä voi tietenkin spekuloida, mutta näen, että tässä se ei ole tarkoituksenmukaista. Tästä huolimatta kansainvälinen yhteistyö kyberturvallisuusstrategioissa vaikuttaa Suomen kokemaan ontologiseen turvallisuuteen. Strategiat ilmentävät Suomen paikkaa maailmassa ja linjaavat Suomen aktiivisuutta kansainvälisessä kyberpolitiikassa ja -diplomatiassa. Kansainvälisen toiminnan motiiveina on kehittää omaa kansallista kyberturvallisuutta, mutta myös edistää suomalaista kyberosaamista ja turvallisuusajattelua maailmalla.

6 YKSILÖ KYBERTOIMINTAYMPÄRISTÖSSÄ

Kybertoimintaympäristön kehityksen myötä sekä digitalisaation kehittyessä yksilöiden suhtautuminen itseensä, toisiin ihmisiin sekä ympäröivään yhteiskuntaan on jatkuvassa muutoksessa. Kybertoimintaympäristössä yksilö ei ole pelkästään teknisen järjestelmän käyttäjä, vaan toimija, jonka valinnat, osaaminen, tunnetilat sekä vuorovaikutus vaikuttavat toisiin toimijoihin ja ympäröivään yhteiskuntaan. Teknologisen kehityksen myötä kybertoimintaympäristö koostuu monista toimijoista, joilla on kyky ja mahdollisuus olla yhteydessä toisiinsa monin eri keinoin (Mihr 2014, 24). Tämä yksilöiden mahdollisuus kommunikoida ja luoda sosiaalisia verkostoja sekä yhteenkuuluvuuden tunnetta kybertoimintaympäristössä vaikuttaa yksilön kokemaan todellisuuteen ja turvallisuuden tunteeseen. Kybertoimintaympäristö voi vahvistaa yksilön kuulumista yhteiskuntaan ja yksilön kokemaa turvallisuuden tunnetta tarjoamalla erilaisia yhteiskunnallisen vaikuttamisen, osallistumisen ja yhteenkuuluvuuden mahdollisuuksia ja tuntemuksia, mutta kybertoimintaympäristö voi myös horjuttaa näitä tuntemuksia tarjoamalla vaihtoehtoisia mahdollisuuksia.

Suomalainen kansallinen yhteiskunta perustuu luottamukseen toimijoiden välillä. Luottamus näkyy kaikilla yhteiskunnan aloilla, eikä pelkästään kyberturvallisuuden tai yleisesti turvallisuuden toiminnoissa. Kansanedustaja ja dosentti Jarno Limnell toteaa, että *”kyberturvallisuus ja luottamusyhteiskunta kulkevat käsi kädessä”* (Suomen tietotoimisto, 10.10.2024). Luottamus rakentaa turvallisuuden tunnetta ja luo ennustettavuutta sekä järjestystä ympäristöön. Turvallisuuden kantavana voimana on tunne yhteisöllisyydestä ja yhdessä tekemisestä (Kolehmainen, Turvallisuuskomitea, 2020). Suomalaista yhteiskuntaa voidaankin luonnehtia luottamusyhteiskunnaksi.

> *”Suomi on luottamusyhteiskunta, jossa julkinen, yksityinen ja kolmas sektori tekevät tiivistä yhteistyötä. Viranomaiset torjuvat yhteiskunnan kyberuhkia, ja niiden kanssa toimivat yritysten ja yhteisöjen kyberammattilaiset sekä kansalaisyhteiskunta omissa organisaatioissaan.”* (Kyberturvallisuusstrategia 2024–2035, 19.)
>
> *”Positiiviset kokemukset yhteisestä vuorovaikutuksesta kasvattavat luottamusta”* (Kyberturvallisuusstrategia 2024–2035, 19).

Yhdenvertainen ja luotettava viranomaistoiminta sekä toimivat yhteiskunnan palvelut vahvistavat yksilön ontologista turvallisuutta. Kun yksilöt kokevat tulevansa huomioiduiksi ja kokevat yhteiskunnan välittävän heistä, syntyy sosiaalinen ympäristö, jonka yksilö kokee omakseen ja jossa

on mahdollisuus toteuttaa itseään ja arjen rutiinejaan. Tällä viittaan yksilön tunteeseen omaan paikkaansa maailmassa. Tuo yksilön kokema paikka maailmassa - ”koti” - on keskeinen paikka, jossa yksilön itse tuntee yhteenkuuluvuutta sekä luottamusta johonkin sosiaaliseen kokonaisuuteen (Lupovici 2023, 156).

Yksilön kokemalle ontologiselle turvallisuudelle on tärkeää, että yhteiskunnan palvelut toimivat ja viranomaisten toiminta vastaa yksilön tarpeita. Tähän sisältyy myös yhteiskunnan digitaaliset palvelut ja niiden toimivuus. Yhteiskunta vastaa yksilön vaikeuksiin ja huoliin, jolloin yksilön ja valtion välille syntyy yhteys. Ihmiset luottavat vahvasti julkisiin instituutioihin, järjestelmiin sekä muihin ihmisiin, varsinkin kun nämä tuottavat ihmisille näiden käyttämiä palveluita ja toimintoja. (Limnell, Majewski, Salminen 2018). Kybertoimintaympäristö voi parhaimmassa tapauksessa olla ympäristö, jossa valtio kohtaa kansalaisensa ja muodostaa oikeanlaisen kuvan näiden tarpeista, velvollisuuksista sekä oikeuksista. Tällöin valtio pystyy tarjoamaan personoituja palveluita yksilöille, jolloin asiointikokemuksesta tulee yksilöille viiveettömämpää ja vaivattomampaa, joka voi täten parantaa yksilöiden suhtautumista valtioon. (Jansson & Sihvonen 2018, 15).

Valtiolle on myös oman etunsa mukaista vastata yksilön vaikeuksiin auttavalla kädellä, jotta yksilön tunneside valtioon ei katkea. Yksilön positiivinen suhtautuminen valtioon turvallisuuden tuottajana ja elämän mahdollistajana on eduksi valtiolle. Mikäli valtion tarjoamat toimet yksilön turvallisuuden ja arvokkuuden tarpeiden tyydyttämiseksi eivät kohtaa, etsii yksilö apua tarpeisiinsa jostain vaihtoehtoisesta toimijasta tai yhteisöstä. Positiivisesti yhteiskuntaan ja valtioon suhtautuva yksilö haluaa kehittää omaa sosiaalista ympäristöään ja olla siinä mukana, jolloin yksilö kokee ympäristönsä turvalliseksi. Osallistuvan yksilön ja turvallisen ympäristön kautta syntyy ryhmäidentiteettejä ja yhteenkuuluvuuden tunteita sekä kertomuksia, joiden puolesta ihmiset ovat valmiita jopa taistelemaan toisia ihmisiä vastaan. Mikäli tämä yhteenkuuluvuuden tunne menetetään, yksilöt lähtevät etsimään yhteenkuuluvuuden ja arvokkuuden tunnetta jostain muualta (Lupovici 2023, 156). Yhteenkuuluvuuden tunteen heikkeneminen ja vaihtoehtoisten elämäntapojen ja sosiaalisen elämän näkeminen muun muassa digitaalisten viestintäjärjestelmien kautta irrottaa identiteettejä ajankohdista, paikoista, historiasta ja traditioista. Tällöin identiteetti esittäytyy ”vapaasti leijuvana” ja on altis ulkopuolisille vaikuttimille. (Hall 1999, 62.)

Tämä yhteenkuuluvuuden ja arvokkuuden tunteen vaatimus on myös nostettu esiin kyberturvallisuusstrategioissa yhdessä luottamuksen kanssa. Strategioissa yksilö on mukana kehittämässä ja toteuttamassa valtion turvallisuutta yhdessä osana kokonaisuutta. Kyberturvallisuusstrategiat toimivat keinoina vaikuttaa yksilöiden käsitykseen ja suhtautumiseen valtiota kohtaan. Strategiat voivat parhaimmassa tapauksessa poistaa ristiriitaisia käsityksiä valtiosta

kansalaisten valvojina ja parantaa yksilöiden käsitystä valtion toimista ja keinoista turvata yksilöiden elämää. (Jansson & Sihvonen 2018, 22.)

> *”Viranomaistoiminta on oltava luotettavaa ja palvelut on turvattava kaikille – kansalaisia on kohdeltava yhdenvertaisesti ja varmistettava, että digitaaliseen teknologiaan ja palveluihin voivat luottaa sekä käyttäjät että palvelun tarjoajat”* (Kyberturvallisuusstrategia 2024–2035, 19).

> *”On varmistettava, että digitalisaatio on inhimillistä ja kuuluu jokaiselle […] käyttäjän on tiedettävä, kenen palvelusta on kyse tai kuka on tiedon lähde. Varmuus viestinnän osapulista sekä viestinnän oikeellisuudesta ja turvallisuudesta on tärkeää.”* (Kyberturvallisuusstrategia 2024–2035, 19.)

> *”Jokainen yksilö on siten tärkeä kyberturvallisuustoimija, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen. Kansallisesti on varmistettava, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä.”* (Kyberturvallisuusstrategia 2019, 8.)

Digitalisoituneessa yhteiskunnassa ei palveluja tai muita yhteiskunnan toimintoja voi toteuttaa ilman digitaalisia laitteita ja järjestelmiä. Digitaalisissa järjestelmissä sijaitsee myös ihmisten ja organisaatioiden arkaluotoisiakin tietoja ja muita arkeen vaikuttavia asioita. Esimerkiksi terveystiedot, pankkipalvelut sekä viestiliikenne toimivat digitaalisesti ja ovat riippuvaisia toimivasta digitaalisesta infrastruktuurista. Toimivilla ja turvallisilla digitaalisilla palveluilla sekä järjestelmillä yhteiskunta luo yksilöille tunnetta turvallisesta ja luotettavasta elinympäristöstä. Entinen liikenne- ja viestintäministeri Timo Harakka pitää olennaisena, että digitaalisiin tuotteisiin ja palveluihin voidaan luottaa yhteiskunnassamme (aalto.fi, 8.2.2022). Yksilöiden on voitava luottaa siihen, että heidän yksityisasiansa ja yksityiselämänsä pysyy turvassa yhteiskunnan järjestelmissä. Heidän tulee myös pystyä luottamaan digitaalisten palveluiden ja järjestelmien turvallisuusjärjestelyihin ja -ratkaisuihin sekä näiden kehittämiseen ajan vaatimusten mukaisesti. (Suomen tietotoimisto, 10.10.2024.) Oleellista on ymmärtää, että mikäli ihmisten luottamus kybermaailman toimivuuteen heikkenee, sillä on merkittäviä vaikutuksia niin turvallisuuden tunteeseen kuin todellisuuteen (Limnell, Majewski, Salminen 2018).

Kyberturvallisuus koskettaa yhtä lailla yksilöitä kuin yhteisöjäkin. Yksilöiden toiminta kybertoimintaympäristössä vaikuttaa suorasti yksilöiden elämään, mutta toiminnalla voi olla myös vaikutuksia organisaatioille ja yhteisöille. Yksittäistä ihmistä pidetään monesti helpoimpana reittinä

tunkeutua erilaisiin järjestelmiin kybertoimintaympäristössä (Laari et al. 2019, 14). ”*Tietoturvan ymmärtäminen ja perustaidot ovat yhä tärkeämpiä ja ovat kansalaistaito jokaiselle digitaalisissa yhteiskunnissa”,* toteaa Jarno Limnell (aalto.fi, 8.2.2022). Uusimmassa kyberturvallisuusstrategiassa (2024–2035) kyberturvallisuusosaaminen rinnastetaan yleisesti kansalaistaitoihin. Nämä kansalaistaidot ja yksilön rooli kyberturvallisuudessa saa suuren huomion uusimmassa strategiassa. Vanhemmissa strategioissa yksilön merkitys jää selvästi vähemmälle.

> *”Kyberturvallisuusosaaminen kuuluu kansalaistaitoihin, ja jokainen voi omalla toiminnallaan myötävaikuttaa yhä turvallisemman kybertoimintaympäristön syntyyn. […] Kyberhygienia eli hyvien tietoturvakäytänteiden noudattaminen osana päivittäisiä rutiineja tuleekin nähdä luonnollisena osana jokaisen yksilön yhteiskuntavastuuta. Vastuullisesti kybertoimintaympäristössä toimivat ihmiset lisäävät merkittävällä tavalla myös yhteisöjen ja organisaatioiden turvallisuutta.”* (Kyberturvallisuusstrategia 2024–2035, 24–25.)

Kyberturvallisuusstrategioissa on myös mainittu yhteiskunnallisesta tarpeesta panostaa tietoturvallisuuden ja kyberturvallisuuden koulutukseen ja kasvatukseen, tutkimukseen sekä työelämään eri osa-alueille. Tietoturva- ja kyberturvallisuusosaaminen lisää luottamusta digitaalisiin palveluihin ja näin luo varmuutta yksilöille toimia turvallisesti digitaalisessa ympäristössä. Luottamus digitaalisiin palveluihin edellyttää tietoturva- ja kyberturvallisuusosaamisen lisäksi yksilöiltä esimerkiksi medialukutaitoa ja tietoisuutta informaatiovaikuttamisesta kybertoimintaympäristössä. (Lehto & Niemelä 2019, 19.)

> *”Lisätään panostuksia tutkimukseen, tuotekehitykseen ja koulutukseen sekä toimenpiteitä kyberturvallisuuden osaamisen kehittämiseksi koko yhteiskunnan osalta”* (Kyberturvallisuusstrategia 2013, 9).

> *”Kokonaisuudessaan suomalainen kyberturvallisuusosaaminen varmistetaan vahvistamalla kyberturvallisuuden roolia laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla”* (Kyberturvallisuusstrategia 2024–2035, 24).

Yksilöiden tietoturva- sekä kyberturvallisuusosaamisen koulutusta järjestetään kouluissa, työelämässä sekä erilaisten järjestöjen toimesta. Oppimisen mahdollistamiseksi, opetus- ja koulutusmateriaali on kyettävä tuottamaan siten, että kaikilla on yhtäläiset mahdollisuudet saada tarvittavaa tietoa. Tiedon merkitys kasvaa, kun digitaaliset järjestelmät ja teknologiat kehittyvät koko ajan. Ajantasainen tieto kyberturvallisuudesta vaikuttaa myös yksilöiden kyberkäyttäytymiseen, jolla

voi olla mittaviakin seurauksia yksilön elämään mutta myös yhteiskuntaan. (Lehto & Niemelä 2019, 20) Kyberturvallisuus- ja tietoturvaosaamista lisätään esimerkiksi koulujen opetussuunnitelmiin ja opettajien osaamista vahvistetaan. Myös erilaiset järjestöt järjestävät yksilöille tietoturva- ja kyberkoulutusta. Eri organisaatioissa henkilöstön osaamisen kehittämistä kyber- ja tietoturva-asioissa pidetään kyberturvallisuusstrategioissa vastuullisena toimintana. Kybertoimintaympäristö on tarkoitettu käytettäväksi, mutta ei ole syytä unohtaa oman toiminnan vastuita ja vaikutuksia. Turvallinen toiminta kybertoimintaympäristössä edellyttää ajantasaisia tietoja ja taitoja, mutta myös varovaisuutta ja puhdasta järjenkäyttöä. (Laari et al. 2019, 14).

> *”Kouluissa opettajien valmiuksia kasvattaa oppilaita kriittiseen medialukutaitoon sekä tietoisuuteen kyberriskeistä on vahvistettava laajan yhteiskunnallisen resilienssin lujittamiseksi. Tavoitteisiin pääsemiseksi kyberturvallisuus on huomioitava digitaalisen osaamisen osana opetussuunnitelmia laadittaessa ja opettajien kyberturvallisuusosaamista on edistettävä. Kansalaisjärjestöillä on merkittävä rooli yksilöiden osaamisen kehittämisessä koulupolun jälkeen. […] Organisaatioiden vastuulliseen toimintaan kuuluu kehittää henkilöstön osaamista, tunnistaa uhkat, reagoida haitalliseen toimintaan ja ilmoittaa häiriöistä kybertoimintaympäristössä.”* (Kyberturvallisuusstrategia 2024–2035, 24.)

Yksilöiden digitaalinen tietoturvatietoisuus ja -osaaminen kasvattaa yhteiskunnallista resilienssiä ja turvallisuutta. Kybertoimintaympäristön käyttäjien resilienssi koostuu yksilöistä ja näiden kyberturvallisuus- ja tietoturvallisuusosaamisesta. Tämän resilienssin avulla, ja sitä kehittämällä, voidaan sietää paremmin erilaisia kybertoimintaympäristön häiriöitä koko yhteiskunnan tasolla. (Keinonen, 2023, 573.) Yksilöiden käsitys omasta tietoturvaosaamisesta heijastelee laajemmin yhteiskuntaan, mutta se myös vaikuttaa yksilön henkilökohtaiseen turvallisuuden tunteeseen. Kyberturvallisuusriskien ymmärtäminen auttaa yksilöä tekemään tietoisia päätöksiä digitaalisessa maailmassa. (DCAF 2019, 15). Kun yksilöllä on selkeä käsitys siitä, miten hänen oma toimintansa vaikuttaa digitaalisessa toimintaympäristössä, on tämän myös helpompi välttää digitaalisessa toimintaympäristössä olevia vaaroja, kuten esimerkiksi kyberrikollisuutta. Yksilöiden kyberkäyttäytymisellä on vaikutuksia muihin ihmisiin ja laajemmin myös yhteisöihin.

Yksilön kyberkäyttäytymiseen ja kansalaistaitoihin liittyy myös tietoisuus siitä, että yksilö on vaikuttamisen kohde kybertoimintaympäristössä. Kybertoimintaympäristö tarjoaa ympäristön, jossa yksilöön voidaan vaikuttaa huomaamattomasti ja laaja-alaisesti. Esimerkiksi palvelunestohyökkäysten avulla välitetään viestiä, joka pyrkii luomaan epäluottamusta ja pelkoa yhteiskuntaa kohtaan (Suojelupoliisi, kansallisen turvallisuuden katsaus 2025). Siksi yksilöiden

tietoturva-, kyber- ja informaatio-osaaminen on tärkeässä asemassa digitalisoituneessa yhteiskunnassa.

> *”Tietoturvaloukkausten vaikutukset ihmisten hyvinvointiin ja luottamukseen yhteiskunnan toimivuuteen voivat olla mittavia”* (Kyberturvallisuusstrategia 2024–2035, 18).

Jarno Limnellin mukaan merkittävimmät kybertaistelut tullaankin käymään ihmisten mielistä. *”Suomalaisten on tunnistettava erilaiset informaatiovaikuttamisen keinot ja huolehdittava täten kyberturvallisuuden psykologisesta puolesta, jossa taistelutilana on ihmisten mieli.”* (Suomen tietotoimisto, 10.10.2024.) Yksilön rooli kybertoimintaympäristössä onkin varsin kompleksinen. Yksilö toimii kybertoimintaympäristössä vaikuttajana, mutta on samalla myös vaikutuksen objektina. Tähän yksilön toimintaan informaatiovaikuttajana ja vaikutuksen objektina olemiseen liittyy yksilön kokemus omasta ontologisesta turvallisuudestaan. Turvallisuuden kokemus vaikuttaa yksilön kyberkäyttäytymiseen kybertoimintaympäristössä, samalla tavalla kuin fyysisessä toimintaympäristössäkin turvallisuuden kokemukset vaikuttavat yksilön käyttäytymiseen.

Yksilöt ovat merkittävässä asemassa, kun pohditaan valtion ontologista turvallisuutta. Yksilöiden on tunnettava kuuluvansa johonkin sosiaaliseen rakennelmaan, joka luo yksilöille ennustettavuutta ja hallittavuutta elämään. Näissä sosiaalisissa rakennelmissa yksilöt luovat ja pitävät yllä omia identiteettejään. (Mitzen 2006, 342.) Yksilöiden omanarvontuntemuksia tai yhteenkuuluvuuden tunnustuksen tarvetta ei tule väheksyä valtiollista koheesiota tarkasteltaessa. Yksilöiden kokema ontologinen turvallisuus heijastuu sosiaalisiin rakennelmiin, jotka voivat joutua toistensa kanssa ristiriitaan. Tämänlainen eri sosiaalisten yhteisöjen ja rakennelmien yhteentörmäys vaikuttaa yhteiskunnan turvallisuuden tilaan ja yhteiskunnan olemukseen.

Kybertoimintaympäristö voi olla yksilölle sosiaalisia rakennelmia luova ja vahvistava ympäristö, mutta se voi myös olla niitä heikentävä ja yksilöä syrjäyttävä ympäristö. Kybertoimintaympäristö sisältää paljon mahdollisuuksia luoda sosiaalisia verkostoja globaalisti, mutta se sisältää myös sudenkuoppia, joissa yksilön identiteettiä ja luottamusta yhteiskuntaan yritetään horjuttaa. Läpinäkyvillä ja osallistavilla digitaalisilla ratkaisuilla voidaan lujittaa yksilöiden suhtautumista ja luottamusta yhteiskunnallisia instituutioita kohtaan. Yksilöiden kokema ontologinen turvallisuus sosiaalisissa yhteisöissään on elintärkeä elementti turvallisen ja vakaan yhteiskunnan ylläpitämiseksi. Yksilön merkityksen ymmärtäminen osana valtion ontologisen turvallisuuden tarkastelua on konkreettinen esimerkki Mitzenin (2006) mainitsemista mikrotason ilmiöiden ymmärtämisestä osana makrotason ilmiöiden tarkastelua.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä pro gradu -tutkielmassa olen tarkastellut, millä tavoin Suomi vahvistaa omaa ontologista turvallisuuttaan kyberturvallisuusstrategioissa. Tutkielman tavoite on ollut ymmärtää minkälaisilla keinoilla ja missä yhteyksissä Suomi vahvistaa ja rakentaa omaa ontologista turvallisuuttaan kyberturvallisuuden näkökulmasta. Tutkielma pyrkii ymmärtämään miten kybertoimintaympäristö ja sen erinäiset ilmiöt vaikuttavat suomalaiseen yhteiskuntaan ja yksilöön sekä näiden kokemaan ontologisen turvallisuuden tunteeseen. Tutkielmani ei keskity kyberturvallisuuden teknisiin ratkaisuihin tai mekaniikkoihin, vaan tarkastelee kyberturvallisuutta inhimillisenä, sosiaaliseen ja poliittiseen vaikuttavana ilmiönä. Tämänlainen tarkastelu auttaa ymmärtämään kyberturvallisuuden yhteiskunnallisia ja sosiaalisia vaikutuksia niin yksilöihin kuin laajemmin yhteisöihin ja yhteiskuntaan. Tämän tutkielman tarkoituksena on tarjota uudenlaisia näkökulmia ja havaintoja kyberturvallisuuteen ja turvallisuuden kokemiseen eri yhteiskunnallisilla tasoilla.

Tutkimusaineistona käyttämäni Suomen kyberturvallisuusstrategiat 2013, 2019 sekä 2024–2035, ontologisen turvallisuuden teoreettinen viitekehys sekä laadullinen sisällönanalyysi luovat tutkielmalle kokonaisuuden, jonka avulla pystyn vastaamaan asettamaani tutkimuskysymykseen. Tutkielmassani löytämieni tulosten perusteella argumentoin, että Suomi vahvistaa omaa ontologista turvallisuutta kolmen eri kokonaisuuden kautta. 1) *Kokonaisvaltainen kansallinen yhteistyö*, 2) *Kansainvälinen yhteistyö kyberturvallisuudessa*, sekä 3) *Yksilö kybertoimintaympäristössä*. Vaikka nämä Suomen ontologista turvallisuutta vahvistavat kokonaisuudet nousivat aineistosta omiksi itsenäisiksi tutkielmani tuloksiksi, ovat ne myös osittain limittäin ja vuorovaikutteisia toistensa kanssa. Kuitenkin keskeistä näille kokonaisuuksille on niiden vaikutus yhteiseen toimijaan, eli Suomeen valtiona. Jokainen kokonaisuus vaikuttaa omalta osaltaan Suomen kokemaan ontologiseen turvallisuuteen.

Nämä kolme edellä mainittua kokonaisuutta muodostavat tutkielmani tulokset, mutta näen, että näitä olisi myös mahdollista pohtia ja tutkia syvemmin itsenäisinä tutkimusaiheinakin. Kaikki kolme kokonaisuutta itsenäisinä tutkimuskohteina tarjoaisivat mielenkiintoisen aiheen ja erilaisia lähestymistapoja kyberturvallisuuden ymmärtämiseen. Aiheiden syvempi tarkastelu toisi esille näkökulmia kyberturvallisuuden yhteiskunnallisista vaikutuksista, joita voitaisiin hyödyntää kyberturvallisuutta kehitettäessä ja sen jatkotutkimuksessa.

Ensimmäinen kokonaisuus, joka analyysini perusteella vahvistaa Suomen ontologista turvallisuutta on *kokonaisvaltainen kansallinen yhteistyö.* Kansallinen yhteistyö käsittää viranomaisten ja yksityisen sekä kolmannen sektorin välisen yhteistyön kyberturvallisuuden alalla. Kansallisessa yhteistyössä konkretisoituu kokonaisturvallisuuden malli, jossa kaikki yhteiskunnan toimijat ovat osana turvallisuusajattelua sekä turvallisuuden tuottamista. Kyberturvallisuusstrategioissa kansallinen yhteistyö esitetään välttämättömänä toimintana pienelle valtiolle. Kansallinen yhteistyö vahvistaa myös kansallisten kybertoimijoiden välistä luottamusta toisiinsa. Avoimella ja luotettavalla kyberturvallisuudella voidaan luoda yhteisiä kansallisia kehityskohteita ja parantaa kansallista kyberresilienssiä. Avoimella ja läpinäkyvällä yhteistyöllä vaikutetaan myös kansalaisten suhtautumiseen valtioon turvallisuuden tuottajana. Osallistavalla, luotettavalla ja avoimella kyberturvallisuudella luodaan kansalaisille ja yhteiskunnan toimijoille turvallista ympäristöä, jossa nämä voivat toteuttaa omia rutiinejaan. Yhteiskunnan yksilöiden ja yhteisöjen tuntiessa oman olemisensa turvalliseksi, se heijastelee myös valtion turvallisuuden tilaan. Kansallinen ontologinen turvallisuus on kaksisuuntainen ilmiö, jossa valtion tuottamat turvalliset mahdollisuudet ja ympäristöt heijastelevat yksilöiden olemisen tuntemuksien kautta valtion olemukseen.

Yksi Suomen ontologista turvallisuutta vahvistava kokonaisuus on myös Suomen harjoittama *kansainvälinen yhteistyö kyberturvallisuudessa.* Suomen kansainvälinen kyberyhteistyö painottuu kyberturvallisuusstrategioiden perusteella EU:n ja sen jäsenmaiden kanssa tehtävään yhteistyöhön. Myös Suomen Nato-jäsenyyden myötä kyberturvallisuusyhteistyö lisääntyy ja syvenee Naton kanssa. Näiden yhteistyökumppaneiden ja kansainvälisen yhteisön kautta Suomi asemoi itseänsä vahvemmin osaksi läntistä arvomaailmaa.

Tämä asemoituminen vaikuttaa Suomeen valtiona, mutta myös sen kansalaisiin. Strategioiden ja kansainvälisen poliittisen asemoitumisen avulla Suomi viestii sen poliittisista ystävistä ja vastustajista (poliittisista ystävistä ja vihollisista mm. Schmitt 1932; Harle 2023). Vaikka poliittisia vihollisia ei strategioissa nimellä suoraan mainita, on ystävät nimetty. *EU:n* ja *Naton* lisäksi Suomi harjoittaa kansainvälistä kyberyhteistyötä *samanmielisten maiden* kanssa (Kyberturvallisuusstrategia 2024–2035, 15). Poliittisten vastustajien ja ystävien nimeämisellä sekä kansainvälisellä poliittisella asemoitumisella vaikutetaan yksilöiden kykyyn kokea ainutlaatuisuutta omasta itsestään ja yhteiskunnastaan.

Kyberturvallisuusstrategioissa Suomi esitetään aktiivisena kansainvälisen kyberturvallisuuden toimijana. Strategioissa linjataan Suomen aktiivisesta osallistumisesta YK:n, EU:n ja Naton kyberpolitiikan kehittämiseksi. Etenkin uusimmassa strategiassa (2024–2035) Suomen

kansainvälisestä asemasta linjataan paljon. Kyberturvallisuusstrategioissa asetetaan Suomen pitkän ajan tavoitteeksi tulla maailman johtaviksi valtioiksi kyberturvallisuuden alalla.

Suomen pyrkimystä yhdeksi maailman johtavista kybervaltioista edesauttaa kyberturvallisuuden mahdollisuus vientituotteena kansainvälisille markkinoille ja yhteistyökumppaneille. Suomalainen kyberturvallisuus ja suomalainen kyberosaaminen halutaan strategioissa viedä kansainvälisille markkinoille. Suomalainen kyberosaaminen koetaan lisäarvoa tuovana elementtinä esimerkiksi Natolle ja kansainvälisille yrityksille. Suomalaisen kyberturvallisuuden edistäminen EU:n ja Naton konteksteissa edistää myös suomalaista kokonaisturvallisuuden mallin vientiä muiden maiden viranomaisten turvallisuusajatteluun, joka vahvistaa kollektiivista turvallisuuden kokemista ja osaamista liittolaisten kesken. Suomalaisen kyberturvallisuusosaamisen vieminen edistää kokonaisturvallisuuden edistämistä myös kansallisesti.

Kyberturvallisuuden kansainvälinen yhteistyö on myös keino viestiä muille valtioille Suomen valtion kyberturvallisuuden tilasta ja järjestelyistä. Esimerkiksi kansainväliset kyberharjoitukset tarjoavat mahdollisuuden näyttää suomalaista kyberosaamista, suomalaisia kyberturvallisuuden ratkaisuja sekä kokonaisturvallisuuden ja varautumisen ajattelumallia. Kyberharjoitusten kautta Suomi pystyy konkreettisesti edistämään strategista tavoitettaan tulla yhdeksi maailman johtavista kyberturvallisuuden osaajista ja tuottajista. Kansainvälinen kyberyhteistyö on mahdollisuus näyttää oman valtion kykyjä toisille valtioille, niin poliittisille ystäville kuin vastustajillekin.

Viimeisenä kokonaisuutena, joka aineistosta nousi esille, on *yksilö kybertoimintaympäristössä*. Nykyaikaisten digitaalisten laitteiden ja järjestelmien avulla yksilöllä on lähes rajattomat mahdollisuudet toimia kybertoimintaympäristössä. Tämä toiminta ei rajoitu valtiorajojen sisälle tai muiden fyysisten tai maantieteellisten rajojen sisäpuolelle. Nämä yksilöiden mahdollisuudet kybertoimintaympäristössä haastavat valtioiden perinteistä turvallisuusmonopolia omalla maantieteellisellä alueellaan.

Yksilön ja valtion välinen suhde on muuttunut teknologisen kehityksen myötä. Kyberteknologiat haastavat valtion turvallisuusmonopolia tarjoamalla yksilöille mahdollisuuksia hakea tunnustusta ja omanarvontunnetta identiteetilleen jostain muualta. Kyberteknologiat voivat tarjota yksilöille ontologisen turvallisuuden tunnetta vaihtoehtoisista lähteistä kuin yksilön omasta maasta. Siksi valtioille onkin tärkeää pitää yllä turvallisuuden monopolia, myös kybertoimintaympäristössä, jotta yksilöt eivät menetä luottamustaan valtioon ja lähde etsimään vaihtoehtoisia lähteitä ontologiselle turvallisuudelleen. Ontologinen turvattomuus heikentää valtion ja yksilöiden suhdetta toisiinsa. Tämä vaikuttaa myös yhteiskunnan toimintaan ja sen edellytyksiin kehittyä. Kun ihmiset eivät koe olevansa

osana jotain suurempaa sosiaalista yhteisöä, eivät he halua osallistua tai kehittää ympäröivää yhteiskuntaa.

Valtion ja yksilön välisestä symbioosista syntyy luottamusta. Suomea kuvaillaan luottamusyhteiskunnaksi, jossa yhteiskunnan toiminta perustuu sen toimijoiden väliseen luottamukseen. Yksilöillä on oltava luottamusta yhteiskunnan tarjoamiin palveluihin ja niiden toimivuuteen. Tämä yksilöiden luottamus yhteiskunnan toimintoihin palvelee valtiota. Valtiolle ei ole edullista menettää kansalaistensa luottamusta, mikäli tämä haluaa säilyttää turvallisuuden monopolinsa alueellaan. Yksilöiden kokema ontologinen turvattomuus heijastelee myös valtion kokemaan ontologiseen turvallisuuteen.

Kyberturvallisuusstrategioissakin on analyysin perusteella huomioitu yksilöiden merkitys yhteiskunnan turvallisuuden ulottuvuutena. Yksilöiden merkityksen tunnustaminen on tärkeää yksilöiden omanarvontunteen kannalta, mutta myös yhteiskunnallisesti merkittävää. Kyberturvallisuus ei ole vain valtion instituutioiden tekemää turvallisuustyötä, vaan kokonaisturvallisuuden mallin mukaisesti koko yhteiskunta – yksilöitä myöten – tuottaa turvallisuutta omilta osiltaan. Strategioissa tunnistetaan yksilöiden osaaminen kyberturvallisuuden alalla ja tarve kouluttaa yksilöiden kyber- ja tietoturvaosaamista. Yksilöiden kyberturvallisuus- ja tietoturvaosaaminen rinnastetaan strategioissa kansalaistaitoihin, jonka vaikutukset sidotaan kansalliseen yhteiskunnalliseen turvallisuuteen.

Kyberturvallisuus on nykytutkimuksessa paljon tutkittu aihe. Kuitenkin kyberturvallisuus ja sen tutkimus painottuu vahvasti aiemmassa tutkimuksessa kyberturvallisuuden johtamiseen, sodankäyntiin, teknologisiin ratkaisuihin ja sen suhteeseen fyysiseen turvallisuuteen. Tutkielmani yksi tarkoitus onkin tuoda kyberturvallisuutta lähemmäs kokonaisvaltaista turvallisuutta ja sen kokemista. Perinteisesti kyberturvallisuus luetaan pois fyysisestä maailmasta olevaksi turvallisuuden ulottuvuudeksi, jota se tietyllä tavalla onkin, mutta se helposti johtaa harhaan. Kyberturvallisuuteen liittyvät toimet voivat tapahtua kybertoimintaympäristössä bittien välityksellä, mutta niiden seuraukset ovat yhä enemmän nähtävissä ja koettavissa fyysisessä maailmassa. Tarkoitukseni onkin tutkielmani myötä tarjota uusi näkökulma kyberturvallisuuden ja myös laajemmin turvallisuuden tarkasteluun sekä ymmärryksen laajentamiseen. Turvallisuus on yhä moninaisempi ilmiö ja turvallisuuden kokeminen voi olla kompleksista ja riippua monesta erilaisesta tekijästä. Turvallisuus ei ole vain fyysisiä ilmiöitä ja toimia vaan myös ennen kaikkea tunne- ja kokemuspohjaista.

Kyberturvallisuutta ei tule nähdä erillisenä turvallisuuden ilmiönä. Kyberturvallisuus on yksi kansallisen turvallisuuden ulottuvuus ja osa kansallista kokonaisturvallisuutta mutta sillä voi myös

olla kansainvälisiä ulottuvuuksia. Kyberturvallisuutta rakentavat yksilöt, yhteisöt ja julkiset instituutiot, eikä kyberturvallisuutta voida sivuuttaa pohdittaessa valtion turvallisuutta laaja-alaisesti. Kyberturvallisuus antaa mahdollisuuden lähestyä ja tarkastella turvallisuuden ilmiötä tietystä näkökulmasta, joka huomioi sille ominaiset tekijät ja vaikutukset. Turvallisuutta ja sen kokemista voidaan myös kuitenkin haastaa tietyn ulottuvuuden, kuten kyberturvallisuuden kautta. Kyberturvallisuus integroituu nykypäivänä kaikkialle ja kaikkeen, eikä sitä täten voida sivuuttaa turvallisuutta pohdittaessa.

Tutkielmassani käyttämä ontologisen turvallisuuden teoria tarjosi mahdollisuuden uudenlaiselle kyberturvallisuuden tarkastelulle. Etenkin kun ensisijaisesti tarkastelin ontologista turvallisuutta valtion näkökulmasta. Ontologinen turvallisuus aiemmassa tutkimuksessa keskittyy pitkälti yksilön turvallisuuden kokemisen tarkasteluun, johon se on alun perin tarkoitettukin. Ontologisen turvallisuuden soveltaminen valtion tasolle tarjosi mielenkiintoisen ja uudenlaisen lähestymistavan valtion turvallisuuden tarpeiden ymmärtämiselle sekä laajensi turvallisuuden käsitettä perinteisestä fyysisestä turvallisuudesta. Tähän toisaalta sisältyi myös tutkimukseni suurimmat haasteet. Valtiotasolle vietyä ontologisen turvallisuuden analyysia ei ole tehty suomeksi, ja englannin kielellä tutkimusta on jonkin verran, joten teoreettisen aineiston löytäminen oli tutkimusprosessin alussa haastavaa. Suomen kansallisesta identiteetistä löytyy aikaisempaa tutkimusta (mm. Paasi 1995; Harle & Moisio 2000), mutta ontologista turvallisuutta käsittelevää tutkimusta on vähän. Suomen kyberturvallisuusstrategioita ei ole aiemmin tutkittu ontologisen turvallisuuden näkökulmasta, joten tästä aiheesta olisi mielenkiintoista saada lisää tutkimusta. Suomalaista yhteiskuntatiedettä ajatellen, olisi arvokasta saada lisää suomenkielistä tutkimusta ontologisen turvallisuuden näkökulmasta kansainvälisissä suhteissa.

On kiinnostavaa pohtia, miten erilaisia tutkimuksia olisi mahdollista saada Suomen kyberturvallisuusstrategioista. Strategiat tarjoavat toimivan aineiston, jota voisi analysoida eri analyysimenetelmien keinoin. Politiikkatieteellisesti on kiinnostavaa pohtia miten esimerkiksi narratiivit ilmenevät strategioissa ja minkälaista narratiivia strategioissa luodaan Suomesta ja suomalaisesta kyberturvallisuudesta. Kiinnostavaa olisi myös tarkastella miten kyberturvallisuusstrategioissa asetetut tavoitteet on jalkautettu ja miten ne ilmenevät yhteiskunnassa. Tämänlaisessa tutkimuksessa olisi otettava huomioon strategioiden jalkauttamiseen kuluva aika, jolloin strategioissa asetetut tulokset näkyvät usein vasta vuosien päästä. Pitkällä aikavälillä olisi kuitenkin mielenkiintoista tarkastella, mihin suuntaan suomalainen kyberturvallisuus on menossa ja miten Suomen kyberturvallisuuden intressit ovat muuttuneet. Kyberturvallisuutta voisi myös tarkastella tietyn kyberuhkan tai teknisen näkökulman kautta ja analysoida turvallisuutta

tapausesimerkkien avulla. Toisaalta koen, että yhteiskuntatieteellisessä tutkimuksessa tekniset tiedot ja näkökulmat eivät välttämättä palvelisi yhteiskuntatieteellistä tutkimusta tai toisi siihen merkittävästi lisäarvoa. Mahdollinen jatkotutkimuksen aihe voisi myös olla analysoida Suomen kyberturvallisuusstrategioita suuremmassa mittakaavassa osana Naton tai EU:n kyberturvallisuus- tai -puolustusstrategioita.

Kyberturvallisuus ja erilaiset digitaaliset teknologiat ovat jatkuvassa muutoksessa ja niitä kehitetään aktiivisesti. Paljon keskustelua aiheuttaa etenkin kehittyvä tekoäly- sekä kvanttiteknologia, jotka luovat mahdollisuuksia mutta herättävät myös paljon kysymyksiä ja huolta tulevaisuudesta. Kyberturvallisuuden sekä teknologian ja valtioiden suhteita onkin mielenkiintoista tarkastella tulevaisuudessa. Etenkin kun kehittyviä teknologioita tuottavat ja kehittävät yritykset, joita valtiot hyödyntävät, ovat globaalisti merkittävässä asemassa. On mielenkiinoista nähdä vaikuttaako teknologiayritysten menestyminen ja täten saavutettu valta, valtioiden turvallisuuden tarpeisiin tai turvallisuusintresseihin. Turvallisuuspolitiikan määrittely ja sen määrittäjä on tulevaisuudessa relevantti kysymys ja tutkimusaihe, kun pohditaan teknologioiden kehitystä. Nouseeko teknologiayrityksistä kansainväliseen järjestelmään valtioiden kanssa toimivia subjekteja, jotka voivat olla luomassa ja määrittelemässä kansainvälistä kyberpolitiikkaa. Tämänlaisesta tematiikasta olisi mielenkiintoista tehdä jatkotutkimusta tulevaisuudessa.

Yhteenvetona totean, että Suomen kyberturvallisuusstrategiat vahvistavat osaltaan Suomen ontologista turvallisuutta. Strategioissa analyysin perusteella ilmenee kolme kokonaisuutta, jotka vaikuttavat Suomen ontologiseen turvallisuuteen; *kansallinen*, *kansainvälinen* ja *yksilö.* Näiden kolmen kokonaisuuden kautta Suomi vahvistaa omaa ontologista turvallisuuttaan valtiona kyberturvallisuuden alalla. Nämä kolme kokonaisuutta ovat vuorovaikutuksessa keskenään, eivätkä yksin riitä turvaamaan ontologista turvallisuutta. Kyberturvallisuusstrategioissa ilmenevät ontologista turvallisuutta vahvistavat kokonaisuudet eivät kuitenkaan absoluuttisesti ilmennä valtion kokonaisvaltaista turvallisuuden tilaa ja sen kokemista eivätkä valtion ulko- ja turvallisuuspolitiikkaa. Kyberturvallisuusstrategiat ovat tässäkin suhteessa osa *Yhteiskunnan turvallisuusstrategiaa* (2025) ja luovat, kartoittavat sekä linjaavat turvallisuutta omalta osaltaan osana laajempia strategiakokonaisuuksia.

EMPIIRINEN AINEISTO

Puolustusministeriö. Kyberturvallisuusstrategia 2013. https://www.defmin.fi/files/2347/Suomen_Kyberturvallisuusstrategia.pdf (haettu 13.1.2025).

Turvallisuuskomitea. Suomen kyberturvallisuusstrategia 2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf (haettu 13.1.2025).

Valtioneuvosto. Suomen kyberturvallisuusstrategia 2024–2035. https://julkaisut.valtioneuvosto.fi/handle/10024/165860 (haettu 13.1.2025).

LÄHTEET

Aalto.fi. Aalto yliopisto. *Suomi kehittää kyberturvallisuuden kansalaistaitoja koko Euroopan unionin alueelle.* 8.2.2022. https://www.aalto.fi/fi/uutiset/suomi-kehittaa-kyberturvallisuuden-kansalaistaitoja-koko-euroopan-unionin-alueelle (haettu 24.9.2025).

Akyeşilmen, Nezir (2024) Geopolitical Implications of Cyberspace on International Relations: An Indepth Analysis. *Global Transformations and Türkiye*, s. 501–520. https://tuba.gov.tr/files/yayinlar/bilim-ve-dusun/TUBA-978-625-6110-04-5_ch36.pdf (haettu 22.10.2025).

Alasuutari, Pertti (1995) *Laadullinen tutkimus*. 3. uudistettu painos, Vastapaino, Jyväskylä.

Bachleitner, Kathrin (2023) Ontological security as temporal security? The role of "significant historical others" in world politics. *International Relations*, 37(1) 25-47. https://journals.sagepub.com/doi/pdf/10.1177/00471178211045624 (haettu 14.4.2025).

Baldwin, David A. (1995) Security Studies and the end of the Cold War. *World Politics*, 48:1, 117-141. https://dbaldwin.scholar.princeton.edu/sites/g/files/toruqf4596/files/dbaldwin/files/baldwin_1995_security_studies_and_the_end_of_the_cold_war.pdf (haettu 11.2.2025).

Buchtova, Katerina; Putilin, Katarina; Vehmaa, Anni (2025) The Kyberist: Suomi etsii keinoja vastata kasvaviin kyberuhkiin valtion ja yritysten yhteistyöllä. *The Ulkopolitist*, 16.6.2025.

https://ulkopolitist.fi/2025/06/16/the-kyberist-suomi-etsii-keinoja-vastata-kasvaviin-kyberuhkiin-valtion-ja-yritysten-yhteistyolla/ (haettu 15.9.2025).

Burke, Peter. J. & Stets, Jan. E. (2022) *Identity Theory; Revised and Expanded*. Oxford University Press, New York.

DCAF (2021) *Guide to Good Governance in Cybersecurity*. Geneva Centre for Security Sector Governance. Sveitsi. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf (haettu 22.10.2025).

Euroopan komissio, Euroopan Unionin kyberturvallisuusstrategia. https://digital-strategy.ec.europa.eu/fi/policies/cybersecurity-strategy. (haettu 12.11.2025).

Floyd, Rita (2024) Ontological vs. societal security: same difference or distinct concepts? *International Politics*. https://link.springer.com/article/10.1057/s41311-024-00581-w (haettu 27.1.2025).

Fukuyama, Francis (2020) Identiteetti – arvostuksen vaatimus ja kaunan politiikka. Docendo, Jyväskylä.

Gheciu, Alexandra & von Hlatky, Stéfanie (2024) Irreconcilable Differences? NATO´s Response to Russian Aggression Against Ukraine. *International Journal*, 79(2), 275- 296. https://doi.org/10.1177/00207020241255999 (haettu 18.9.2025).

Górka, Marek (2018) Cyberconflicts as a Threat for the Modern State. *Computer Science and Information Technology* 6(1): 11-20. https://www.researchgate.net/publication/324519540_Cyberconflicts_as_a_Threat_for_the_Modern_State (haettu 29.4.2025).

Gutmann, Amy (2003) *Identity in Democracy*. Princeton University Press, Princeton, New Jersey. https://doi.org/10.1515/9781400825523. (haettu 26.1.2025).

Hall, Stuart (1999) *Identiteetti.* Suom. ja toim. Mikko Lehtonen ja Juha Herkman. 5.painos. Tammer- Paino Oy. Tampere 2005.

Harle, Vilho (2000) *The Enemy with a Thousand Faces – The Tradition of the Other in Western Political Thought and History*. Praeger Publisher, Connecticut, Westport.

Harle, Vilho (2023) *Hyvä, paha, ystävä, vihollinen*. Toinen uudistettu laitos, Rosebud Books, Keuruu.

Harle, Vilho, Moisio, Sami (2000*) Missä on Suomi? Kansallisen identiteettipolitiikan historia ja geopolitiikka*. Vastapaino, Jyväskylä.

Heino, P. (2018) *Kotoutuminen ja turvattomuuskokemukset.* Helsingin yliopisto. https://helda.helsinki.fi/server/api/core/bitstreams/b7474ca4-bca6-4347-8ee5-bddf399a5aed/content (haettu 27.1.2025).

Huhtinen, Aki-Mauri & Laitinen, Kari (2021) *Kansallinen turvallisuus murroksessa*. Docendo Oy, Jyväskylä.

Hyppönen, Mikko (Johdannon lainaus) *We´re in the Middle of an Online Arms Race / Mikko Hyppönen (CRO of F-Secure).* Slush 2015. https://www.youtube.com/watch?v=AV9gnLKw8P0 (haettu 23.9.2025).

Jansson, Saara & Sihvonen, Tanja (2018) Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä* 41:1, 1–28. https://journal.fi/mediaviestinta/article/view/69950/31049 (haettu 23.9.2025).

Kananen, Jorma (2017) *Laadullinen tutkimus pro graduna ja opinnäytetyönä*, Jyväskylän ammattikorkeakoulun julkaisuja 234, Suomen Yliopistopaino Oy – Juvenes Print, Jyväskylä.

Keinonen, Maria (2023) *The Concept of Comprehensive Security as a Tool for Cyber Deterrence*. European Conference on Cyber Warfare and Security, 22(1), 567-574. https://papers.academic-conferences.org/index.php/eccws/article/view/1254 (haettu 23.9.2025).

Kolehmainen, Seppo; Turvallisuuskomitea (21.2.2020) *Luottamus viranomaisiin tukee turvallisuuden tunnetta.* https://turvallisuuskomitea.fi/luottamus-viranomaisiin-tukee-turvallisuuden-tunnetta/ (haettu 14.4.2025).

Kyberturvallisuuskeskus.fi. NIS 2 – Euroopan unionin kyberturvallisuusdirektiivi. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi (haettu 12.11.2025).

Kärkkäinen, Henrik; Iltasanomat (1.6.2022) *Mikko Hyppönen: Tässä on Suomen suurin uhkaaja verkossa nyt,* https://www.is.fi/digitoday/tietoturva/art-2000008856961.html (haettu 13.1.2025).

Laari, Tommi (toim.); Flyktman, Jouni; Härmä, Katriina; Timonen, Jussi; Tuovinen, Jussi (2019) *#kyberpuolustus – Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, sotataidon laitos, Helsinki.

https://www.doria.fi/bitstream/handle/10024/173254/%23kyberpuolustus%20verkko%20%28interaktiivinen%20pdf%29%20%28002%29.pdf?sequence=1&isAllowed=y (haettu 4.2.2025).

Laukkanen, Matti (2018) *Kyberturvallisuus Suomessa*. Vaasan yliopisto, tekniikan ja innovaatiojohtamisen yksikkö. https://osuva.uwasa.fi/bitstream/handle/10024/9363/osuva_8154.pdf?sequence=1&isAllowed=y (haettu 4.2.2025).

Lehto, Martti & Limnell, Jarno (2021) Strategic leadership in cyber security, case Finland. *Information Security Journal*, 30(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851 (haettu 8.9.2025).

Lehto, Martti & Niemelä, Jukka (2019) *Kyberalan tutkimus ja koulutus Suomessa 2019*. Informaatioteknologian tiedekunnan julkaisuja (83/2018). Jyväskylän yliopisto. https://urn.fi/URN:ISBN:978-951-39-7829-7 (haettu 2.10.2025).

Lehto, Martti; Limnell, Jarno; Kokkomäki, Tuomas; Pöyhönen, Jouni; Salminen, Mirva (2018) *Kyberturvallisuuden strateginen johtaminen Suomessa*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf;jsessionid=2F783B61BFCC4DE8102827003865B6B0?sequence=1 (haettu 23.9.2025).

Limnell, Jarno (2014) Kyber rantautui Suomeen. Aalto-yliopisto, sähkötekniikan korkeakoulu. *Tiede+Teknologia* 12/2014. https://aaltodoc.aalto.fi/server/api/core/bitstreams/f2bf5267-790d-447c-bc98-de3044f12704/content (haettu 4.2.2025).

Limnell, Jarno; Majewski, Klaus; Salminen, Mirva (2014) *Kyberturvallisuus*. Docendo Oy, Jyväskylä. https://books.google.fi/books?hl=fi&lr=&id=Nx4rEQAAQBAJ&oi=fnd&pg=PT3&dq=kyberturvallisuus&ots=5ABCo_ANpU&sig=R_qlGvK_DkfVeZxEOMvCxnWVGSI&redir_esc=y#v=onepage&q=kyberturvallisuus&f=false (verkkokirjassa ei sivunumeroita) (haettu 4.2.2025).

Lupovici, Amir (2023) Ontological security, cyber technology, and states´ responses. *European Journal of International Relations*, Vol. 29(1) 153 – 178. https://journals.sagepub.com/doi/10.1177/13540661221130958 (haettu 28.1.2025).

Mearsheimer, John (2009) Reckless States and Realism. *International Relations*, 23(2), 241 – 256. https://doi.org/10.1177/0047117809104637 (haettu 19.11.2025).

Mihr, Anja (2014) Good Cyber Governance – The Human Rights and Multi-Stakeholder Approach. *International Engagement on Cyber IV* (2014), s. 24-34. Georgetown Journal of International Affairs. https://www.jstor.org/stable/43773646 (haettu 22.10.2025).

Mitzen, J., (2006) Ontological Security in World Politics: State Identity and the Security Dilemma. *European Journal of International Relations.* SAGE Publications and ECPR-European Consortium for Political Research, Vol 12(3): 341-370. https://www.researchgate.net/publication/241065178_Ontological_Security_in_World_Politics_State_Identity_and_the_Security_Dilemma (haettu 4.2.2025).

MTV (28.12.2020) *Presidentti Niinistö eduskuntaan kohdistuneesta kyberhyökkäyksestä: "Vakava loukkaus demokratiaa ja yhteiskuntajärjestystä vastaan,* https://www.mtvuutiset.fi/artikkeli/presidentti-niinisto-eduskuntaan-kohdistuneesta-kyberhyokkayksesta-tama-on-vakava-loukkaus-suomalaista-demokratiaa-ja-yhteiskuntajarjestysta-vastaan/8023714 (haettu 13.1.2025).

Paasi, Anssi (1995) *Territories, boundaries, and consciousness – The changing geographies of the Finnish-Russian border.* John Wiley & Sons Ltd. Chichester.

Paasonen, Jyri & Widlund, Joonas (2021) *Kansallisen turvallisuuden käsite: oikeutta vai politiikkaa?* Edilex 2021/44. Edita Publishing Oy. https://www.riksdagen.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2021-AK-397814.pdf (haettu 1.2.2025).

Palokangas, Marko; Jouko, Petteri (toim.); Karjalainen, Mikko; Säämänen, Juuso; Seppo, Antti; Martelius, Juha; Huhtinen, Aki-Mauri; Kukkola, Juha; Wuolijoki, Sakari; Liuhto, Kari; Mononen, Toni; Puranen, Matti; Pajunen, Jussi (2024) *Hybridisodankäynti – Laaja-alaista vaikuttamista moninaisilla sodankäyntimenetelmillä.* Maanpuolustuskorkeakoulu, sotataidon laitos. Helsinki. https://www.doria.fi/bitstream/handle/10024/190432/Hybridisodanka%cc%88ynti_linkit.pdf?sequence=1&isAllowed=y (haettu 29.1.2025).

Rautio, Marjatta; Yleisradio (21.4.2023) *Supon ja Traficomin arvio: Kyberturvallisuuden uhkataso pysynyt kohonneena ja kohdistettujen hyökkäysten määrä Suomessa noussut*, https://yle.fi/a/74-20028240 (haettu 13.1.2025).

Saurama, E., Nurmi, A., Heino, P. (2020) Pakotettu muutto ja ontologisen turvallisuuden rakentuminen. *Yhteiskuntapolitiikka* 85:2.

https://www.julkari.fi/bitstream/handle/10024/139443/YP2002_Sauramaym.pdf?sequence=2&isAllowed=y. (haettu 4.2.2025).

Schmitt, Carl (1932) *Poliittisen käsite*. (suom.) Kuusterä, Arto & Palmusaari, Jussi. Tutkijaliitto (2015), Helsinki.

Sisäministeriö, kansallinen turvallisuus. https://intermin.fi/kansallinen-turvallisuus/mita-on-kansallinen-turvallisuus (haettu 14.4.2025).

Sisäministeriö, kyberturvallisuus.https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus (haettu 23.9.2025).

Steele, Brent J. (2008) *Ontological Security in International Relations – Self-identity and the IR state.* Routledge, Oxford. https://www.academia.edu/15829412/Ontological_Security_in_International_Relations_Self_Identity_and_the_IR_state (haettu 9.9.2025).

Suojelupoliisi. Kansallisen turvallisuuden katsaus 2025. https://katsaus.supo.fi/etusivu (haettu 8.9.2025).

Suojelupoliisi. Tiedote (29.8.2025) *Traficom ja Supo: Kyberturvallisuuden uhkataso pysynyt koholla – vakavien tapausten määrät kasvussa*. https://supo.fi/-/kyberturvallisuuden-uhkataso-pysynyt-koholla-vakavien-tapausten-maarat-kasvussa (haettu 8.9.2025).

Suomen akatemia. https://www.aka.fi/tutkimusrahoitus/vastuullinen-tiede/tutkimusetiikka/ (haettu 15.1.2024).

Suomen tietotoimisto (10.10.2024) *Kokoomuksen Limnell: Uusi kyberturvallisuusstrategia vahvistaa Suomen kokonaisturvallisuutta ja reagointia kyberuhkiin,* https://www.sttinfo.fi/tiedote/70578089/kokoomuksen-limnell-uusi-kyberturvallisuusstrategia-vahvistaa-suomen-kokonaisturvallisuutta-ja-reagointia-kyberuhkiin?publisherId=69819275&lang=fi (haettu 13.1.2025).

Tuomi, Jouni & Sarajärvi, Anneli (2018) *Laadullinen tutkimus ja sisällönanalyysi*, Kustannusosakeyhtiö Tammi, uudistettu laitos, Helsinki.

Valtioneuvosto. Puolustusministeriö. Suomen kyberturvallisuusstrategia valmis. Tiedote. 24.1.2013. https://valtioneuvosto.fi/-/strategi-for-cybersakerheten-i-finland-klar (haettu 13.1.2025).

Valtioneuvosto. Valtioneuvoston periaatepäätös PLM/2019/52. https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80655af5 (haettu 13.1.2025).

Valtioneuvosto. *Yhteiskunnan turvallisuusstrategia*. Turvallisuuskomitea 16.1.2025. https://julkaisut.valtioneuvosto.fi/handle/10024/166024 (haettu 15.9.2025).

Verdugo, Richard R.; Milne, Andrew (toim.); Largueche, Aladin; Luong, Francis; Duclos, Nathalie; Guillaumond, Julien; Karnaukhova, Oxana; Vukovic, Djordje; Savanovic, Aleksandar; Vranjes, Aleksandar; Martin, Dana; Van Kerckem, Klaartje; Anjum, Saliha; McKinlay, Andrew; McVittie, Chris (2016*) National Identity: Theory and Research*. Information Age Publishing, Charlotte.

Vuorelma, Johanna (2025) *An existential threat in the North: ontological insecurity and the Nordic path to NATO*. SAGE Publications. https://doi.org/10.1177/00108367251372862 (haettu 17.11.2025).

Yarovoy, Tikhon; Koval, Yana; Kyrychenko, Anna; Havrilechko, Yury; Moskalets, Inna; Sokol, Mariya (2024) Utilization of digital technologies in the development of state policy on national security issues. *Multidisciplinary Science Journal*, 6 (2024). https://doi.org/10.31893/multiscience.2024ss0227 (haettu 15.4.2025).

Yhteiskunnan turvallisuusstrategia 2025. Valtioneuvosto. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/817eb584-f510-49a2-ad2f-9106226b2f20/content (haettu 12.11.2025).

Yleisradio. Elsa Olsipova, STT (18.3.2021) *Supo: Eduskuntaan kohdistunut vakoilu viittaa Kiinaan – poliisin mukaan verkkovakoilulla on yritetty kalastella tietoja vieraalle valtiolle*. https://yle.fi/a/3-11843261 (haettu 8.9.2025).