Sami Puuperä

KYBERHUOLTOVARMUUS KOKONAISTURVALLISUUDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Puuperä, Sami Tapani
Kyberhuoltovarmuus kokonaisturvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2024, 60 s.
Kyberturvallisuus, pro gradu tutkielma
Ohjaaja: Lehto, Martti

Turvallisuusympäristön jatkuva muutos korostaa ennakoivan varautumisen ja huoltovarmuuden merkitystä yhteiskunnan kriisinsietokyvyn ylläpitämisessä. Etenkin digitaaliset ympäristöt ovat avainasemassa yhteiskunnan kriittisille toiminnoille, tarjoten uusia mahdollisuuksia mutta samalla lisäten kyberuhkia, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja kyberhyökkäysten kautta. Erityisesti Suomen kaltaisessa maassa, jossa digitaalinen infrastruktuuri on laajasti integroitunut yhteiskunnan perustoimintoihin, kyberturvallisuuden strateginen merkitys korostuu.

Kyberturvallisuuden ja huoltovarmuuden näkökulmasta kansainvälinen yhteistyö, lainsäädännön kehittäminen ja tehokkaat kansalliset strategiat sekä niiden toimeenpano ovat keskeisiä elementtejä kyberuhkien hallinnassa. Kansallisten toimien lisäksi Suomen aktiivinen osallistuminen kansainvälisiin kyberturvallisuusaloitteisiin ja -sopimuksiin tukee maan kyberturvallisuusstrategian tehokasta toteutumista. Tämä yhteistyö mahdollistaa tiedon, resurssien ja parhaiden käytäntöjen jakamisen, mikä vahvistaa globaalia kyberresilienssiä.

Suomi on tunnustettu kyberturvallisuuden edelläkävijä, joka jatkuvasti pyrkii ylläpitämään korkeaa turvallisuuden tasoa ja parantamaan huoltovarmuutta vastaamaan nopeasti muuttuviin kyberympäristön vaatimuksiin. Tämä tutkimus osoittaa, kuinka kyberulottuvuudessa tapahtuva huoltovarmuuteen vaikuttaminen on erottamaton osa kansallista ja kansainvälistä turvallisuutta, korostaen kyberhuoltovarmuuden strategista merkitystä.

Tutkimusraportti tarjoaa katsauksen kyberhuoltovarmuuden nykytilaan, sen haasteisiin ja tulevaisuuden kehityssuuntiin Suomessa ja kansainvälisesti. Se käsittelee kyberhuoltovarmuuden kriittisiä kysymyksiä, kuten teknologisen riippuvuuden kasvua, kyberhyökkäysten monimutkaisuutta, sekä infrastruktuurin haavoittuvuutta. Lisäksi raportissa pohditaan kyberresilienssin kehittämisen mahdollisuuksia ja haasteita, ja miten Suomi voi jatkaa rooliaan kyberturvallisuuden kärkimaiden joukossa. Lopussa tarjotaan suosituksia, joiden avulla voidaan edelleen parantaa Suomen kyberhuoltovarmuutta ja kokonaisturvallisuutta.

Avainsanat: Kyber, kyberhuoltovarmuus, kyberturvallisuus, kokonaisturvallisuus, kyberpuolustus, huoltovarmuus, resilienssi

ABSTRACT

Puuperä, Sami Tapani
Cyber Resilience in the Context of Comprehensive Security
Jyväskylä: University of Jyväskylä, 2024, 60 pp.
Cybersecurity, Master's Thesis
Supervisor: Lehto, Martti

The continuous evolution of the security environment underscores the importance of proactive preparedness and resilience in maintaining societal crisis resistance. Digital environments are particularly crucial for the critical functions of society, offering new opportunities but also increasing cyber threats that can endanger vital societal activities through cyber-attacks. This is especially true in a country like Finland, where the digital infrastructure is extensively integrated into the core functions of society, highlighting the strategic significance of cybersecurity.

From the perspectives of cybersecurity and resilience, international cooperation, legislative development, and effective national strategies and their implementation are key elements in managing cyber threats. In addition to national actions, Finland's active participation in international cybersecurity initiatives and agreements supports the effective implementation of the country's cybersecurity strategy. This cooperation allows for the sharing of information, resources, and best practices, strengthening global cyber resilience.

Finland is recognized as a leader in cybersecurity, continuously striving to maintain a high level of security and improve resilience to quickly respond to the evolving cyber environment. This study demonstrates how actions taken in the cyber dimension of resilience are an inseparable part of national and international security, emphasizing the strategic importance of cyber resilience.

The research report provides an overview of the current state of cyber resilience, its challenges, and future development directions in Finland and internationally. It addresses in detail the critical issues of cyber resilience, such as the growth in technological dependency, the complexity of cyber-attacks, and the vulnerability of infrastructure. Additionally, the report explores the possibilities and challenges of developing cyber resilience and how Finland can continue its role among the leading nations in cybersecurity. The report aims to provide recommendations to further enhance Finland's cyber resilience and Comprehensive security.

Keywords: Cyber, cyber resilience, cybersecurity, comprehensive security, cyber defense, supply chain security, resilience

KUVIOT

SISÄLLYS

1 JOHDANTO

Tutkimusraportin johdantoluvun ensimmäisessä osassa johdatellaan nimensä mukaisesti lukija sisään tutkimukseen ja kerrotaan sen taustoista. Seuraavassa osassa käsitellään tutkimuksen aihealuetta ja sen valintaa. Lopuksi kerrotaan tutkimuksen tässä vaiheessa tehdyt rajaukset ja perustellaan ne.

1.1 Tutkimuksen tausta

Suomen ja Euroopan toimintaympäristö on epävakaa, jännitteinen ja vaikeasti ennakoitavana. Vallitseva tilannekehitys haastaa yhteiskunnan kriisinsietokyvyn, jolloin ennakoivan varautumisen ja huoltovarmuuden merkitys kasvaa. (Valtioneuvosto, 2021a) Digitaaliset ympäristöt ovat välttämättömiä yhteiskunnan toiminnan kannalta kriittisille yrityksille ja organisaatioille. Digitaalisen toimintaympäristön muutos tarjoaa uusia mahdollisuuksia, mutta se myös lisää kyberuhkia. Kokonaisturvallisuutta voidaan uhata esimerkiksi vaikuttamalla yhteiskunnan elintärkeisiin toimintoihin kyberhyökkäyksin. (Turvallisuuskomitea, 2019; Euroopan komissio, 2017; Lehto & Limnéll, 2017)

Sodankäynnissä on perinteisesti ajateltu olevan kolme ulottuvuutta, maa-, meri- ja ilmaulottuvuudet. Teknologian kehittyminen ja digitalisaatio ovat laajentaneet alueita, jolla sotaa käydään. Nykyään sekä hyökkäyksellisiä, että puolustuksellisia operaatioita suoritetaan eri konflikteissa edellisten lisäksi myös informaatioympäristössä, avaruudessa sekä kyberympäristössä. Nämä toimintaympäristöt poikkeavat merkittävästi perinteisistä toimintaympäristöistä, sillä niissä ei ole fyysisiä rajoja, ja lisäksi hyökkääjä ja sen toiminta voi olla hankalaa osoittaa. Joidenkin näkökulmien mukaan informaatioulottuvuus poikkeaa muista edellä mainituista ulottuvuuksista niin, että se pitää ne sisällään ja on osa niitä. (Valtioneuvosto, 2017; Valtioneuvosto, 2021a; Turvallisuuskomitea, 2019) Informaatio- ja kybertoimintaympäristössä vaikuttaminen voi olla myös ei-kineettistä, jossa ei fyysisesti vaikuteta kohteeseen, vaan vaikuttaminen tehdään esimerkiksi tietoverkoissa tai ihmisten mielissä.

Euroopan hybridiuhkien torjunnan osaamiskeskuksen (Hybrid CoE - hybridiosaamiskeskus) konseptin *The landscape of Hybrid Threats: A conceptual model* julkisessa versiossa, jossa ei käsitellä vain sotilaallisia uhkia vaan hybridiuhkia ja vaikuttamista, ulottuvuuksia on yhteensä kolmetoista. Suurta ulottuvuuksien lukumäärää perustellaan sillä, että vähentämällä määrää ja yhdistämällä ulottuvuuksia samojen otsikoiden alle, ei voitaisi kuvata koordinoidun vaikuttamisen monimutkaisuutta. (Hybrid CoE, 2021)

Martti J Kari (2019) käyttää väitöskirjassaan strategisen kulttuurin teoriaa, ja selittää sen avulla Venäjän näkemystä kyberuhkista ja niihin reagoinnista. Väitöskirja käsittelee kyberavaruutta ja siellä vaikuttamisesta myös laajemmin, ja se tarjoaa hyvän pohjan ymmärtää varsinkin venäläisten ajattelua ja toimintaa. Venäjän strateginen kulttuuri, joka heijastaa sen historiallisia kokemuksia ja geopoliittista identiteettiä, vaikuttaa merkittävästi siihen, miten maa hahmottaa myös kyberuhkat ja kehittää strategioita niiden torjumiseksi. Tämä näkökulma tarjoaa arvokkaan kehyksen ymmärtää, miten eri valtiot - erityisesti Venäjä, joka kokee olevansa lännen hyökkäyksen kohteena - priorisoivat kyberuhkia ja kehittävät vastauksiaan niihin. Kari korostaa kyberuhkien moniulotteisuutta ja niiden kytkeytymistä laajempiin geopoliittisiin ja strategisiin tavoitteisiin. Venäjän esimerkki osoittaa, miten valtiot voivat käyttää kyberoperaatioita osana laajempaa strategista kamppailua, mikä lisää kyberhuoltovarmuuden merkitystä kansallisessa ja kansainvälisessä turvallisuudessa. (Kari, 2019)

Digitaalinen ja kybertoimintaympäristö ovat tänä päivänä olennaisia elementtejä yhteiskunnan toiminnan kannalta, ja niillä on merkittävä rooli turvallisuuden ylläpidossa ja kehittämisessä. Tämä ympäristö on jatkuvassa muutoksessa, kun uudet teknologiat kehittyvät ja tietoverkkojen käyttö laajenee. Kehitys tarjoaa uusia mahdollisuuksia mutta myös altistaa uusille haavoittuvuuksille ja uhkille. Kyberhyökkäykset ovat osa nykyajan turvallisuusuhkia ja ne voivat olla monimuotoisia, kohdistuen kriittiseen infrastruktuuriin ja laajasti yhteiskunnan toimintoihin. Digitaalisessa ympäristössä tapahtuva yksittäinen tapahtuma voi uhata laajasti yhteiskunnan elintärkeitä toimintoja. (Valtioneuvosto, 2021c; Valtioneuvosto, 2022a)

Kanniainen (2018) esittää väitöskirjassaan, että kybersodan aikakausi alkoi kesällä 2010 kun (todennäköisesti, kirjoittajan huomio) Yhdysvaltojen ja Israelin yhdessä kehittämä Stuxnet-haittaohjelma saatiin asennettua iranilaiseen Natanz uraanin rikastamoon. Erittäin kehittynyt ohjelma keräsi tietoa järjestelmästä ja vaikutti sitten hiukkaskiihdyttimien nopeuteen niin, että se käytännössä tuhosi itse itsensä. Kybervaikuttaminen sodankäynnin välineenä voi olla aseellista voimankäyttöä parempi vaihtoehto, sillä sen jäljet voidaan peittää, tai ainakin oma osallisuus kiistää, se voi olla kustannustehokkaampaa ja poliittisesti hyväksyttävämpää, sillä tuhovaikutus on säädettävissä tarpeen mukaan ja ulkopuolisia uhreja ei useinkaan tule, ja vahinkojen laajuutta on mahdollisuus säätää tarpeen mukaan. Stuxnetin tapauksessa haittaohjelma tosin pääsi leviämään ja se saastutti maailmanlaajuisesti satoja tuhansia tietokoneita ja -verkkoja. (Kanniainen, 2018)

Kanniaisen (2018) mukaan kyberhyökkäykset ovat osa asevoimien suorituskykyä, on olemassa paljon viitteitä myös siitä, että tietoverkoissa tapahtuva tiedustelu ja vahingoittaminen on jonkin muun, yleensä valtiollisen toimijan toimeenpanemaa. Sen lisäksi, että kybervaikuttamista kohdistetaan asevoimiin, myös yhteiskunnan elintärkeät toiminnot ovat kyberhyökkäysten kohteena (Lehto & Limnéll, 2017). Sodankäynnin raja on hämärtynyt etenkin kyberympäristössä. Kybervaikuttamisella voidaan vaikuttaa niin poliittiseen päätöksentekoon, johtamiskykyyn, kansalliseen turvallisuuteen, yhteiskunnan elintärkeisiin toimintoihin, kriittisiin yrityksiin ja organisaatioihin kuin esimerkiksi maanpuolustustahtoon yleisesti. Kyberhyökkäyksiä voidaan käyttää ennen perinteistä asevaikutusta ns. taistelutilan muokkaamiseen, ja verkostoitunut sodankäynti, etenkin johtamisjärjestelmien ja tilannekuvan hallinta voivat tuoda hyökkääjälle etua, mikäli menetelmiä käytetään myös hyökkäyksen aikana. (Turvallisuuskomitea, 2019)

Kovasen (2021) väitöskirjan *Cyber-Threat Aspects in a Complex System-of-Systems*, mukaan digitaalinen transformaatio ja verkottuminen vaikuttavat turvallisuuden haasteisiin ja riskeihin. Digitaalisten ympäristöjen ja järjestelmien lisääntyessä myös tahallisten kyberhäiriöiden riski kasvaa. Tämä korostaa kyberuhkien ymmärtämisen tärkeyttä turvallisuuden takaamiseksi näissä uusissa järjestelmissä. Tutkimus tuo esille tarpeen holistiselle lähestymistavalle kyberuhkien hallinnassa, joka yhdistää uhkatiedon ja haavoittuvuustiedot. Tämä lähestymistapa mahdollistaa tarkemman riskiarvioinnin ja edistää kyberresilienssin kehittämistä kriittisissä infrastruktuureissa. (Kovanen, 2021)

Venäjän käymä raaka hyökkäyssota Ukrainassa on muuttanut turvallisuustilannetta pysyvästi, ja tällä hetkellä tilanne on hyvinkin dynaaminen, ilman kuitenkaan näkymää ainakaan nopeasta tilanteen paranemisesta. Kriittinen infrastruktuuri ovat yhä monimutkaisempien riskien ja uhkien kohteena. (Telenor, 2023a)

1.2 Aihealue

Tämän pro gradun aihealue on kyberhuoltovarmuus kokonaisturvallisuuden näkökulmasta. Aihealue on muutaman iterointikierroksen jälkeen valittu yhdessä tutkimustyön ohjaajan Martti Lehdon kanssa. Näkökulmana oleva kokonaisturvallisuus on käsitteenä minulle tuttu aikaisemman työni vuoksi ja olen käsitellyt sitä etenkin edellisen työni parina viimeisenä vuonna toimiessani Pääesikunnan suunnitteluosastolla strategiavastuualueen johtajana. Myös huoltovarmuus on tuttu käsite, ja minulla on selkeä ajatus siitä kuinka edelliset liittyvät tutkimukseeni. Aineiston keräämisessä ja analyysissä pyrin siihen, että aikaisemmin hankittu tieto ja ymmärrys tai käsitykset tutkimukseen liittyvistä asioista eivät ohjaisi tutkimuksen tuloksia, vaan edellä mainitut perustuisivat tutkimuksen lähdeluettelon materiaaliin.

1.3 Tutkimuksen rajaus

Tutkimus käsittelee kokonaisturvallisuutta normaaliolojen ja normaaliolojen häiriötilanteiden näkökulmasta. Poikkeusolojen ja laajamittaisen sodankäynnin aikana uhkakuva on erilainen.

Tutkimus käsittelee vain julkisista lähteistä saatavaa materiaalia. Vaikka kokonaisturvallisuus on vahvasti riippuvainen myös sotilaallisesta suorituskyvystä, rajataan sotilaallinen vaikuttaminen tutkimuksen ulkopuolelle niiltä osin kuin se ei koske kybertoimintaympäristössä tehtävää vaikuttamista. Myös kineettinen vaikuttaminen rajataan tutkimuksen ulkopuolelle, vaikka se kohdistuisi kybertoimintaympäristöön.

Venäjän laiton, laajamittainen hyökkäys Ukrainaan kevättalvella 2022 sisältää monenlaista kybervaikuttamista molemmilta osapuolilta, ja etenkin Ukrainan kyberpuolustukseen on osallistunut myös länsimaisia toimijoita. Nämä viimeaikaiset, ja edelleen aktiiviset tapahtumat rajataan kuitenkin pääsääntöisesti tutkimuksen ulkopuolelle, sillä varmistetun, relevantin tiedon saaminen sotatoimialueelta on hyvin vaikeaa, ja tilanne Ukrainan alueella elää jatkuvasti.

2 TUTKIMUSONGELMA JA TUTKIMUSKYSYMYKSET

2.1 Tutkimuksen tavoitteet

Tutkimuksen päätavoitteena on selvittää, että mitä kyberhuoltovarmuus merkitsee ja mitkä asiat siihen vaikuttavat. Erityisesti tutkin kyberhuoltovarmuuden merkitystä kokonaisturvallisuudelle. Tutkimuksen osatavoitteina on määritellä kyberhuoltovarmuus, tunnistaa kyberhuoltovarmuuden osatekijät ja selvittää kyberhuoltovarmuuden vaikutus kokonaisturvallisuuteen.

2.2 Tutkimusongelma

Tutkimuksen keskeinen ratkaistava ongelma on ”Miten kyberhuoltovarmuus vaikuttaa kokonaisturvallisuuteen?”. Tutkimusongelman ratkaisemiseksi olen asettanut seuraavan alaluvun mukaisen pääkysymyksen ja alakysymykset.

2.3 Tutkimuskysymykset

Tutkimuksen pääkysymys:

- Mikä on kyberhuoltovarmuuden merkitys huoltovarmuudelle?

Alakysymykset:

- Mitä kyberhuoltovarmuudella tarkoitetaan?

- Mikä on kyberhuoltovarmuuden tilanne Suomessa?
- Kuinka kyberulottuvuudessa tapahtuva, huoltovarmuuteen vaikuttaminen heikentää kokonaisturvallisuutta?
- Minkälaisia kyberhaavoittuvuuksia huoltovarmuuden toiminnoissa ja toimijoilla on?

Tutkimuksen pääkysymykseen ja alakysymyksiin etsitään vastauksia etenkin tutkimusraportin luvuissa 5–9. Näiden lukujen lopussa kysymyksiin vastataan kunkin luvun sisällön perusteella, pois lukien ensimmäinen alakysymys *Mitä kyberhuoltovarmuudella tarkoitetaan?*, johon vastataan luvussa 10.

3 TUTKIMUKSEN KESKEISET KÄSITTEET

Seuraavana on lyhyesti lueteltu tutkimuksen tärkeimmät käsitteet. Seuraavissa alaluvuissa perehdytään näihin käsitteisiin tarkemmin.

Kokonaisturvallisuus:

> Kokonaisturvallisuus on suomalaisen varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä. (Turvallisuuskomitea, 2017b)

Kyberturvallisuus:

> Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. (Turvallisuuskomitea, 2018)

Huoltovarmuus:

> Huoltovarmuus tarkoittaa varautumista mahdollisiin kriiseihin ja häiriötilanteisiin. Lisäksi se on jatkuvuudenhallintaa. Huoltovarmuudella turvataan yhteiskunnalle ja elinkeinoelämälle elintärkeät toiminnot, jotta arki voi jatkua mahdollisimman häiriöttä. Huoltovarmuustyö luo puskureita, joilla ostetaan aikaa yhteiskunnan ja elinkeinoelämän toimijoiden omien valmiussuunnitelmien aktivointia varten. (Valtioneuvosto, 2022b)

Yhteiskunnan elintärkeä toiminto:

> Elintärkeät toiminnot ovat yhteiskunnan toimivuuden kannalta välttämättömiä, kaikissa tilanteissa ylläpidettäviä toimintokokonaisuuksia. (Turvallisuuskomitea, 2017b)

Yhteiskunnan elintärkeitä toimintoja ovat johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys. (Turvallisuuskomitea, 2017b)

Kriittinen infrastruktuuri:

> Kriittinen infrastruktuuri voidaan määritellä yhteiskunnan perusrakenteiksi ja järjestelmiksi, joita ilman yhteiskunnan elintärkeät toiminnot häiriintyvät vakavasti. Huoltovarmuuden näkökulmasta infrastruktuurin lisäksi kriittisiksi tulisi huomioida palvelut ja tuotanto, joita infrastruktuurin avulla tuotetaan ja jotka yhdessä mahdollistavat yhteiskunnan elintärkeät toiminnot. Valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (1048/2018) kriittisen infrastruktuurin todetaan kattavan perusrakenteiden lisäksi palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. (Turvallisuuskomitea, 2017b)

Hybridivaikuttaminen: Valtiollisen tai muun ulkoisen toimijan vaikuttaminen samanaikaisesti tai jatkumona, eri keinoja (ml. kybervaikuttaminen) käyttäen kohteen haavoittuvuuksiin omien tavoitteidensa saavuttamiseksi. (Turvallisuuskomitea, 2018)

3.1 Kokonaisturvallisuus

Kokonaisturvallisuus on virallisesti määritelty viimeksi Yhteiskunnan turvallisuusstrategiassa vuonna 2017, joka käsittelee yleisiä yhteiskunnan varautumisen periaatteita. Yhteiskunnan turvallisuusstrategia 2017, joka aiemmin tunnettiin nimellä Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, on neljäs päivitys strategiaan, seuraava päivitys julkaistaan ilmeisesti vuoden 2024 aikana. Nimi ja strategian sisältö muuttuivat vuoden 2010 päivityksessä, jolloin turvallisuustoiminta ulotettiin myös palveluihin ja toimintoihin. Uusin julkaistu strategia myös sisältää toimintaympäristön muutoksesta johtuvia osien päivityksiä, ja yksi sen keskeisistä tehtävistä on kokonaisturvallisuuden käytännöllinen kuvaus. Merkittävin muutos kokonaisturvallisuuden määrittelyssä on sen yhteistoimintamalli. Aiemmin toimet ovat keskittyneet valtioneuvostoon, mutta nykyisen strategian mukaan myöhemmin luetellut turvallisuustoimijat ja toimintatasot jakavat ja analysoivat tilannetta ja tietoa yhdessä, sekä yhdistävät suunnittelua, harjoittelua ja toimeenpanoa, sekä asettavat tarvittaessa yhteisiä tavoitteita. (Turvallisuuskomitea, 2017b)

Yhteiskunnan turvallisuusstrategia linjaa kokonaisturvallisuuden yleiset periaatteet, Turvallisuuskomitea seuraa strategian ajantasaisuutta, ja päivitystarpeet päättää valtioneuvosto. Kokonaisturvallisuuden käytännön toteutus on kirjattu poikkihallinnollisissa strategioissa ja toimeenpano-ohjelmissa. (Turvallisuuskomitea, 2017b)

Kokonaisturvallisuuden yhteistoimintamalli kattaa nykyään kaikki yhteiskunnan toimijat ja tasot. Valtionhallinnon lisäksi verkostoon kuuluvat viranomaiset, elinkeinoelämä, kunnat ja maakunnat, sekä tutkimuslaitokset, yliopistot, järjestöt ja yksittäiset kansalaiset. Kansalaisten osuus kokonaisturvallisuudessa tarkoittaa lähinnä yksilön omatoimista varautumista ja yhteiskunnan kriisinsietokyvyn vahvistamista. (Turvallisuuskomitea, 2017b)

3.2 Kyberturvallisuus

Kyberturvallisuus käsitteenä on määritelty useassa eri lähteessä, ja määritelmissä on havaittavissa jonkin verran eroja. Hieman yllättäen käsitettä ”kyberturvallisuus” ei ole kattavasti määritetty Suomen kyberturvallisuusstrategiassa vuodelta 2019, eikä myöskään sen toimeenpano-ohjelmassa (Turvallisuuskomitea, 2019). Uusin strategia asettaa keskeiset kansalliset tavoitteet, joiden mukaan kybertoimintaympäristöä on kehitettävä ja toimintaympäristöön liittyvien yhteiskunnan elintärkeiden toimintojen turvaamiseksi, sekä käsittelee Yhteiskunnan turvallisuusstrategian tyylisesti eri toimien ja toimintojen vastuuta yhteisestä kyberturvallisuudesta. (Turvallisuuskomitea, 2019)

Aikaisempi kyberturvallisuusstrategia vuodelta 2013 (Turvallisuus- ja puolustusasian komitea, 2013) määrittelee kyberturvallisuuden seuraavasti:

> Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.
>
> Tarkennus 1: Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriöitä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle.
>
> Tarkennus 2: Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia.
>
> Tarkennus 3: Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infra- struktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle. (Turvallisuus- ja puolustusasian komitea, 2013)

Lehto ja Kähkönen määrittelevät artikkelissa *Kyberturvallisuuden kansallinen osaaminen* (Lehto & Kähkönen, 2015) lyhyesti kyberturvallisuuden tarkoittavan toimia, jotka tehdään kyberhyökkäyksiltä ja niiden vaikutuksilta suojautumiseksi.

Pöyhösen väitöskirjassa *Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu* (Pöyhönen, 2020) kyberturvallisuuden todetaan olevan yksi kokonaisturvallisuuden alue, jonka pyrkimyksenä on digitalisoituneen ja verkottuneen yhteiskunnan turvallisuuteen. Siten kyberturvallisuus liittyy yhteiskunnan kriittisiin toimintoihin, ja se pitää sisällään myös tietoturvan, toimintojen jatkuvuuden hallinnan ja varautumisen häiriötilanteisiin. Kyberturvallisuus muodostuu organisaation kyvykkyyksistä (osaaminen, käytänteet, prosessit ja teknologiat), joilla suojataan verkot, järjestelmät, laitteet, ohjelmistot ja data. (Pöyhönen, 2020)

Valtioneuvoston puolustusselonteon 2021 mukaisesti kyberturvallisuus on tila, jossa kybertoimintaympäristöstä riippuvaisten toimintojen ja toimijoiden uhkat ja riskit ovat hallinnassa. (Valtioneuvosto, 2017)

3.3 Huoltovarmuus

Huoltovarmuuden tarkoituksena on turvata koko yhteiskunnan toimintakyky erilaisissa häiriötilanteissa. Toimintakyky taataan ennen mahdollista kriisiä varautumisen toimenpiteillä, ja kriisin aikana jatkuvuudenhallintana. Keskeistä on turvata yhteiskunnan elintärkeät toiminnot ja siten mahdollistaa yhteiskunnan toiminta, elinkeinoelämän toimintaedellytykset ja ihmisten turvallinen arki. Huoltovarmuuden tavoitteena on lisäksi turvata kriittinen infrastruktuuri, sekä tuotanto ja palvelut. (Huoltovarmuuskeskus, ei pvm.)

Yleisesti huoltovarmuus käsitetään välttämättömän materiaalin ja tarvikkeiden (esim. ruoka, polttoaine ja lääkkeet) hankintana, sekä varastointina. Käsitteen sisältöä on kuitenkin syytä laajentaa, ja tämä tutkimus pyrkii osaltaan avaamaan etenkin kybertoimintaympäristön vaatimusten ja vaikutusten merkitystä huoltovarmuudelle.

Kyberturvallisuuden huomioon ottaminen on yhä tärkeämpää yritysten huoltovarmuudelle, erityisesti kun digitalisaation rooli liiketoiminnan perusedellytyksenä kasvaa. Huoltovarmuusorganisaation digipoolin kyberturvallisuuden nykytilan selvitys toi esiin, että huoltovarmuuden kannalta keskeistä on tarkastella ja kehittää kyberturvallisuutta yli toimialarajojen ja yritysten välillä. Huoltovarmuuskriittisten yritysten kyky jatkaa toimintaansa kaikissa tilanteissa, mukaan lukien digitaalisten uhkatilanteiden aikana, on keskeistä. Tämä korostaa sitä, kuinka tärkeää on rakentaa vahva ja joustava infrastruktuuri, joka pystyy vastaamaan nopeasti ja tehokkaasti erilaisiin kyberuhkiin. (Huoltovarmuusorganisaation digipooli, 2020)

3.4 Yhteiskunnan elintärkeä toiminto

Yhteiskunnan turvallisuusstrategian mukaan yhteiskunnan elintärkeät toiminnot ovat(Turvallisuuskomitea, 2017b):

- Johtaminen
- Kansainvälinen ja EU-toiminta
- Puolustuskyky
- Sisäinen turvallisuus
- Talous, infrastruktuuri ja huoltovarmuus
- Väestön toimintakyky ja palvelut
- Henkinen kriisinkestävyys

Ne ovat välttämättömiä kokonaisuuksia, jotka on turvattava kaikissa olosuhteissa. Ne ulottuvat tyypillisesti useiden eri toimijoiden lakisääteisiin tehtäviin. Toiminnot ovat lähtökohtana varautumisen suunnittelulle. Erillistä vastuutahoa toiminnoille ei ole määritelty, mutta hallinnonalojen strategiset tehtävä ja vastuut on kuvattu Yhteiskunnan turvallisuusstrategiassa. Alla olevassa kuvassa on esitetty strategian mukaiset elintärkeät toiminnot ja niiden väliset suhteet. (Turvallisuuskomitea, 2017b)

KUVIO 1 Yhteiskunnan elintärkeät toiminnot (Turvallisuuskomitea, 2017b)

3.5 Kriittinen infrastruktuuri

Kriittinen infrastruktuuri tarkoittaa niitä järjestelmiä ja verkkoja, jotka ovat elintärkeitä yhteiskunnan toiminnan kannalta. Kriittisen infrastruktuurin verkkoja ovat muun muassa energia-, vesi-, liikenne- ja viestintäverkostot. Digitaalisten teknologioiden kehittyminen ja laajamittainen käyttöönotto ovat lisänneet tietoverkkojen merkitystä kriittisen infrastruktuurin osana. Tämän seurauksena tietoverkkojen turvallisuus on noussut keskeiseksi huolenaiheeksi, sillä niiden haavoittuvuudet voivat vaarantaa koko yhteiskunnan toiminnan. Tietoverkkojen haavoittuvuudet voivat ilmetä monin tavoin, mukaan lukien fyysiset vauriot, tietoturvaloukkaukset ja palvelunestohyökkäykset. Näiden haavoittuvuuksien hyväksikäyttö voi johtaa tietoliikenteen katkeamiseen, järjestelmien

toimintahäiriöihin ja jopa kriittisten palvelujen, kuten sairaaloiden, pelastuspalveluiden ja sähköverkkojen, toimintakyvyn menetykseen. (Telenor, 2023a)

3.6 Hybridivaikuttaminen

Hybridivaikuttamista ei ole kansainvälisesti ja yhteisesti hyväksytyllä tavalla vielä määritelty (Valtioneuvosto, 2021a). Yleisesti sana hybridi, joka nykyään yhdistetään moneen yhdyssanaan, tarkoittaa yhdistelmää tai sekamuotoa (*hybridi - Kielitoimiston sanakirja*, 2022). Hybridivaikuttaminen on terminä yleistynyt Venäjän hyökättyä Ukrainaan ja vallattua Krimin niemimaan vuonna 2014. TEPA-termipankin mukaan hybridivaikuttaminen on erilaisten, toisiaan täydentävien keinojen poliittisesti motivoitunutta käyttöä, jossa pyritään hyödyntämään kohteen heikkouksia. Termipankin mukaan keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia, ja hybridivaikuttamista voidaan tehdä esimerkiksi informaatio-, kyber-, fyysisen ja taloudellisten operaatioiden avulla. (*hybridivaikuttaminen | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)*, 2022) Tämä määritelmä on mielestäni kuitenkin puutteellinen, ja esimerkiksi keinojen ja erilaisten operaatioiden valikoima menee sekaisin. Hybridivaikuttamisesta käytettään joissain yhteyksissä myös suomenkielistä termiä yhdistelmävaikuttaminen (Harjanne ym., 2018).

Valtioneuvoston tuorein selonteko sisäisestä turvallisuudesta (Valtioneuvosto, 2021b) käsittelee hybridivaikuttamista useassa kohdassa, mutta sanalle ei esitetä määritelmää. Selonteon tekstissä hybridivaikuttaminen erotetaan usein virheellisesti monista vaikuttamisen keinoista, ja sotilaallisen vaikuttamisen keinoja ei juuri käsitellä. (Valtioneuvosto, 2021b) Sen sijaan Valtioneuvoston ulko- ja turvallisuuspoliittisessa selonteossa (Valtioneuvosto, 2020) hybridivaikuttamiselle tarjotaan määritelmää, jonka mukaan toimia (valtiollinen tai joku muu) vaikuttaa useita eri keinoja käyttäen, samaan aikaan tai jatkumona kohteen haavoittuvuuksia hyödyntäen. Vaikuttamisen keinovalikoimaan voi kuulua poliittiset, diplomaattiset, taloudelliset, sotilaalliset toimet, sekä kyber- ja informaatiovaikuttaminen. Vaikuttaminen tehdään niin, että se on tarvittaessa mahdollisuus kiistää. (Valtioneuvosto, 2020) Tämä määritelmä kuvaa hyvin hybridivaikuttamisen keinoja ja päämääriä.

Vuoden 2021 puolustusselonteossa käytetään hybridivaikuttamisen sijaan käsitettä laaja-alainen vaikuttaminen, joka vastaa paremmin sotilaallisen varautumisen mukaisia uhkia. (Valtioneuvosto, 2021a)

3.7 Johtopäätökset / Yhteenveto

Seuraavassa kappaleessa esitetyn, tutkimuksen viitekehyksen mukaisia tärkeimpiä käsitteitä on tarkasteltu useassa eri lähdeteoksessa. Yleisesti ne on määritelty hyvin ja melko yksiselitteisesti, mutta etenkin hybridi-sanan käyttö on sekä

tutkimuksen lähteissä, että myös muissa lähteissä, jotka eivät valikoituneet mukaan tutkimukseen, on melko kirjavaa. Hybridistä tuli Venäjän vuonna 2014 aloittaman hyökkäyksen jälkeen muotisana, jonka käyttö laajeni nopeasti hybridivaikuttamisesta laajalle käytyyn keskusteluun. Usein hybridi-alkuisia yhdyssanoja on käytetty erilaisen vaikuttamisen ja operaatioiden kuvaamisessa ilman, että se varsinaisesti kuvaisi esimerkiksi laajan keinovalikoiman käyttöä niissä.

4 TUTKIMUKSEN TEOREETTINEN PERUSTA

Tässä luvussa kuvataan tutkimuksen teoreettinen tausta. Se on perusta ja selitys sille, kuinka koko tutkimusprosessi ja tutkimuksen raportointi on tehty. Tässä tutkimuksessa ei ole varsinaista teoriaa, johon tutkimus perustuu. Tutkimusprosessin aikana selvitin, että voisiko tutkimustuloksena syntyä yleistettävä teoria, jota voi käyttää jatkotutkimuksiin, mutta sellaista ei löytynyt.

4.1 Tutkimussuuntaus

Tutkimukset jaetaan suuntauksen mukaan yleensä laadullisiin (kvalitatiivinen) ja määrällisiin (kvantitatiivisiin) tutkimuksiin. Jaottelu on edelleen yleistä, vaikka myös kasvavaa kritiikkiä tähän jaotteluun on esitetty. Joissain tutkimuksissa myös näiden suuntausten yhdistäminen on mahdollista. (Hirsjärvi, Remes & Sajavaaara, 1997)

Laadullinen tutkimus pitää lähtökohtana todellisen elämän kuvaamista, ja siihen sisältyy ajatus siitä, että todellisuus on moninainen. Tarkoituksena on tutkia valittua aihetta niin kokonaisvaltaisesti kuin mahdollista. Kokonaisvaltaisuus asettaa omat vaatimukset esimerkiksi aineiston määrälle. Voidaan sanoa, että laadullisessa tutkimuksessa on perusteltua pitää aineiston määrä rajallisena, ja määrän sijasta keskittyä kerättyyn materiaaliin syvällisesti. Laadullisen tutkimuksen tarkoituksena on olemassa olevien väittämien todistamisen sijaan löytää uutta tietoa. (Hirsjärvi ym., 1997)

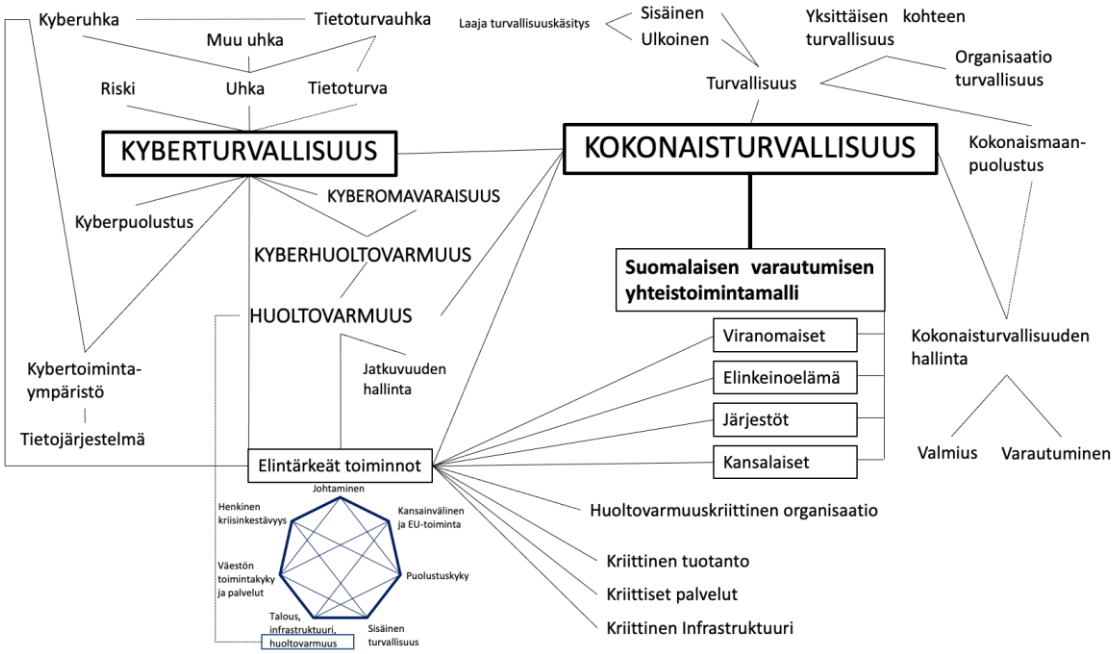
Määrällinen tutkimus käsittelee syyn ja seurauksen vuorovaikutusta. Tutkimuksen voidaan sanoa tutkivan ilmiöitä, joita voidaan mitata ja asettaa niiden ominaisuuksien mukaan järjestykseen. Määrälliselle tutkimukselle on ominaista esimeriksi hypoteesien esittäminen, aineiston numeerinen mittaaminen, erilaisten taulukoiden ja tilastojen esittäminen ja päätelmien teko tilastollisin menetelmin. (Hirsjärvi ym., 1997)

Edellä kuvatun perusteella tämän tutkimuksen suuntaukseksi on valittu laadullinen tutkimus.

4.2 Tutkimuksen viitekehys

Laadullisen tutkimuksen teorian ja viitekehyksen voidaan katsoa tarkoittavan samaa asiaa, sillä molemmat muodostuvat tutkimuksen kannalta keskeisistä käsitteistä ja niiden välillä olevista merkityssuhteista. (Tuomi & Sarajärvi, 2018)

Edellisessä luvussa on kuvattu ja määritelty tutkimuksen kannalta keskeiset käsitteet. Seuraavassa kuviossa on liitetty kokonaisuuteen myös muita vaikuttavia käsitteitä, sekä piirretty niiden väliset merkityssuhteet. Kuvio on tutkijan näkemys käsitteistä ja niiden välisistä suhteista. On perusteltua väittää, että käsitteitä voisi lisätä ja suhteet voisi piirtää myös toisin. Tähän esitystapaan on päädytty osittain myös yksinkertaistamisen vuoksi. Kaikkien mahdollisten käsitteiden sisällyttäminen ja heikkojenkin suhteiden piirtäminen kuvioon tekisi siitä vaikeaselkoisen, jolloin kokonaisuuden hahmottaminen olisi vaikeaa.



KUVIO 2 Tutkimuksen keskeiset käsitteet

4.3 Tutkimustyyppi

Tuomen ja Sarajärven (Tuomi & Sarajärvi, 2018), sekä Kanasen (Kananen, 2014) mukaan tutkimustyypit jaetaan usein miten joko teoreettiseen, tai empiiriseen perustyyppiin, samaa ilmiötä voidaan tutkia molemmilla menetelmillä. Laadullinen tutkimus nojaa havaintojen tekemisessä teoriaan, missä yksilön käsitys ilmiöistä, tutkittavalle ilmiölle annettava merkitys ja tutkimukseen käytettävät välineet vaikuttavat tutkimustuloksiin. Vaikka teoriapitoisuus on laadullisen tutkimuksen lähtökohta, on tämän pro gradun tutkimustyyppi empiirinen. Valittu

tutkimuslaji, sekä aineiston keräämiseen ja analysointiin käytetyt menetelmät puoltavat empiirisen tutkimustyypin valintaa. (Tuomi & Sarajärvi, 2018)

Vaikka joissakin laadullisissa tutkimuksissa niiden kerrotaan olevan teoreettisia tutkimuksia, esimerkiksi Laadullisen tutkimuksen verkkokäsikirjassa todetaan laadullisen tutkimuksen olevan aina empiiristä, aineistoihin ja niiden analyysiin perustuvaa tutkimusta. (Juhila, 2021)

4.4 Aineiston kerääminen ja hallinnointi

Laadullisen tutkimuksen aineisto kerätään tyypillisesti erilaisista dokumenteista, haastatteluista tai kyselyistä ja tutkijan tekemien havaintojen kautta. Menetelmiä voidaan yhdistää ja kaikkia niistä ei välttämättä ole tarpeen käyttää. Materiaalin keräämiseen ja analysointiin käytetyt menetelmät, sekä havaintojen pohjalta tehty argumentointi korostuvat empiirisessä tutkimuksessa. (Tuomi & Sarajärvi, 2018) Tämän pro gradun aineistona ja analyysin pohjana käytetään tieteellisiä tutkimuksia, artikkeleja ja muita julkaisuja. Kyberhuoltovarmuutta suoraan käsitteleviä tutkimuksia en ole vielä löytänyt, mutta turvallisuutta ja kyberturvallisuutta on tutkittu myös viime aikoina. Edellisten lisäksi valtionhallinnon eri selonteot, strategiat ja raportit ovat tutkimuksen keskeisiä lähteitä.

Harkitsin myös tutkimustyön aikana, ja aineiston alustavan analysoinnin jälkeen, että täydentäisin kirjallista materiaalia puolistrukturoiduista haastatteluista saatavalla haastatteluaineistoilla. Luovuin kuitenkin ajatuksesta, sillä keräämäni aineisto antoi tutkimuksen kannalta tarvittavat vastaukset avoimiin kysymyksiin. Lisäksi olen aikaisempia tutkimuksia tehdessäni havainnut haastattelujen tekemisen varsin työlääksi ja aikaa vieväksi, eikä niillä välttämättä saada lisäarvoa tutkimukselle. Haastateltavien asiantuntijoiden rajallinen mahdollisuus sitoutua tutkimusprosessiin, ja etenkin heidän käytettävissä oleva aika asettaa usein haasteen tutkijalle.

Rajasin ja karsin kertynyttä aineistoa koko tutkimusprosessin ajan, sillä esimerkiksi Tuomen ja Sarajärven mukaan (Tuomi & Sarajärvi, 2018) aineiston suurta määrää tärkeämpää laadullisessa tutkimuksessa on perehtyä analysoitavaan tutkimusaineistoon syvällisesti. Tutkimustyön aikana keräsin yli kaksisataa eri lähdettä, joista vain osa päätyi tutkimusraportin lähdemateriaaliksi. Aineiston hallintaa pyrin helpottamaan teemoittamalla lähdemateriaalin muun muassa aihealueen, julkaisijan, julkaisuajankohdan ja tutkimukseni sisällöllisen rakenteen mukaan.

Aineiston hallintaan käytin aluksi Mendeley -viiteidenhallintaohjelmaa, jolla voi organisoida ja hallita lähteitä, sekä automatisoida tutkimusraportin viittaukset ja lähdeluettelon. Mendeleyn käytettävyydessä, etenkin lähdeluettelon muodostamisessa ja lähteiden tuomisessa ja niiden tietojen muokkaamisessa, oli pieniä epäloogisuuksia ja ongelmia. Vaikka materiaalin kerääminen, siihen tutustuminen ja analysointi, sekä itse raportin kirjoitustyö olivat jo melko pitkällä, päädyin vaihtamaan käytettävän ohjelman Zotero:on, joka tukee hyvin esimerkiksi eri tietokannoista haettujen lähteiden tuomista, ja sen toiminnot on

paremmin automatisoitu. Vaikka jouduin vaihdon jälkeen tekemään viittaukset ja lähdeluettelon uudestaan, oli Zotero:n käyttöönotto jatkotyön kannalta järkevää. Työtä helpotti se, että Zotero:on oli mahdollista tuoda lähteet suoraan Mendeley:n tietokannasta.

4.5 Aineiston analyysimenetelmä

Tutkin sisällönanalyysin menetelmällä kyberhuoltovarmuuden, kybersietoisuuden ja kyberomavaraisuuden merkitystä ja vaikutuksia kokonaisturvallisuuteen. Tuomen ja Sarajärven (Tuomi & Sarajärvi, 2018) mukaan sisällönanalyysiä voidaan pitää myös teoreettisena viitekehyksenä, tai ainakin osana sitä. Sisällönanalyysi on analyysimuoto, jota ei ohjaa teoria, eikä epistemologia, vaikka siihen voidaan näitä lähtökohtia soveltaakin.

Laadullisen tutkimuksen analyysi on perinteisesti käsitetty joko induktiivisena, tai deduktiivisena. Tällainen tiukka jako yksittäisestä yleiseen ja yleisestä yksittäiseen on kuitenkin ongelmallinen. Tässä tutkimuksessa edellä mainittua jakoa ei käytetä, sillä jako ei huomioi abduktiivista päättelyä, jossa teoria voidaan muodostaa silloin kun jokin johtoajatus on käytettävissä teorian muodostukseen. (Tuomi & Sarajärvi, 2018) Sen sijaan käytän aineistolähtöistä analyysiä, jossa aineistosta luodaan kokonaisuus ja valitaan sitten tutkimuksen ongelman ja tutkimuskysymysten mukaiset analyysiyksiköt. Tutkimustyön tulosten kannalta koen tärkeäksi myös eri aineistoista saatujen tietojen vertaamisen ja analysoinnin yhdessä, ei pelkästään erikseen. Nimensä mukaisesti aineistolähtöisessä analyysissä aikaisemmalla tiedolla tutkittavasta aiheesta ei ole merkitystä, analyysia, ja sitä kautta tutkimustuloksia ohjaa valittu aineisto. (Tuomi & Sarajärvi, 2018) Toki täytyy ymmärtää, että tutkimustuloksiin vaikuttavat myös tutkijan tekemät valinnat tärkeimmistä käsitteistä, itse tutkimusasetelmasta ja menetelmistä, valitun aineiston lisäksi.

Laaja lähdeaineisto kasvoi vielä melko luonnollisesti tutkimustyön etenemisen aikana, sillä ajankohtaisesta aiheesta ilmestyy jatkuvasti uusia julkaisuja. Tutkimusraportin lähteinä on käytetty paljon valtioneuvoston, viranomaisten ja tutkimuslaitosten julkaisuja, sillä oman näkemykseni mukaan ne ovat laadultaan usein erinomaisia ja riittävän kattavia. Olen itsekin ollut aikaisemmassa työtehtävässäni kirjoittamassa esimerkiksi vuoden 2021 valtioneuvoston puolustusselontekoa, sekä erilaisia puolustusvoimien strategioita ja operatiivisia suunnitelmia, ja tiedän siksi miten huolellisen kirjoitus-, ja arviointiprosessin kautta ne valmistuvat. Julkisten organisaatioiden julkaisujen lisäksi olen käyttänyt joitain opinnäytetöitä, ja pyrkinyt niissä painottamaan vertaisarvioituihin väitöskirjoihin ja artikkeleihin.

Iteratiivisen analyysimenetelmän käyttö aineiston analyysissä on keskeinen osa tämän tutkimuksen metodologista lähestymistapaa. Menetelmä pohjautuu periaatteeseen, jossa aineiston käsittely ja sen syvällinen ymmärtäminen syntyvät toistuvien tarkastelukierrosten kautta, joissa jokainen iteraatio syventää ja tarkentaa aikaisempien vaiheiden havaintoja. Iteratiivisen prosessin myötä

tutkimusaineistoa lähestytään joustavasti, mahdollistaen näin tutkimuskysymysten ja teoreettisen viitekehyksen jatkuvan tarkentumisen tutkimuksen edetessä. Tämä menetelmä ei ainoastaan tue aineiston perusteellista analysointia vaan myös edesauttaa tutkijaa tunnistamaan uusia teemoja, yhteyksiä ja mahdollisia aukkoja aineistossa. Iteratiivisuus tässä kontekstissa tarkoittaa sitä, että tutkimusprosessin aikana voidaan palata aineistoon useita kertoja uusin kysymyksin tai tarkennetuin näkökulmin, mikä tekee menetelmästä erittäin soveltuvan monimutkaisten ja monikerroksisten aineistojen analysointiin. Näin ollen iteratiivinen menetelmä ei ainoastaan rikasta analyysin laatua ja syvyyttä, vaan myös vahvistaa tutkimustulosten luotettavuutta ja validiteettia.

Hyödynsin tutkimuksen ja sen raportin kirjoittamisen aikana ChatGPT 3.5 tekoälypohjaista keskustelurobottia. Tekoälyn käytössä ensisijainen tavoitteeni oli oppia paremmin käyttämään tekoälyä, ja toissijaisesti hyödyntää tekoälyä tutkimuksessa. Olen suorittanut tekoälyyn liittyviä opintoja, ja tunsin jo aikaisemmin melko hyvin tekoälyn toimintaperiaatteen ja sen käyttöön liittyviä rajoitteita, mutta en sen suomia mahdollisuuksia. Annoin esimerkiksi tekoälylle tehtävän jäsennellä raporttini tekstiä uudelleen loogisempaan järjestykseen, mutta se ei suoriutunut tämänkaltaisista tehtävistä ainakaan yrittämilläni komennoilla. Tekoäly ei myöskään kyennyt käsittelemään lähteenä annettua tekstiä riittävän laadukkaasti, mutta lyhyiden itse kirjoittamieni osien analyysiin ja tutkimuskysymysten vastausten etsimiseen niistä se soveltui vaihtelevasti. Lisäksi ChatGPT oli avuksi esimerkiksi synonyymien ehdottamisessa. Ainakaan käyttämäni ilmainen versio ei tuonut merkittävää apua tutkimuksen tekoon, sillä vastaukset olivat usein selkeästi vääriä, eikä viittausten puuttuessa saatua vastausta pysty tarkastamaan. ChatGPT 3.5. tuottama teksti ei myöskään ole kovin laadukasta, ja vaikka tekoälyä käyttämällä sain joitain ideoita tutkimusraportin tekoon ja aihioita raportin tekstiä varten, on raportin teksti omaani. Ensimmäinen tavoitteeni oppia käyttämään ChatGPT:n tyyppistä tekoälyä toteutui, ja olen tutkimustyön ulkopuolella hyödyntänyt sitä jo useasti.

5 KYBERTURVALLISUUDEN KANSALLISET JA KANSAINVÄLISET ULOTTUVUUDET

Kyberturvallisuus on tärkeä osa kansallista turvallisuutta ja yhteiskunnan kestävyyttä. Kansallisella ja kansainvälisellä tasolla kybertoimintaympäristön ymmärtäminen ja siihen varautuminen, ovat avainasemassa tämän päivän verkottuneessa maailmassa. Kyberturvallisuus on yhä merkittävämmässä asemassa globaalissa, verkottuneessa maailmassa, jossa teknologiset rajapinnat ja kyberturvallisuuden haasteet ovat yhä sidoksissa toisiinsa kansallisella ja kansainvälisellä tasolla.

5.1 Kansalliset strategiat

Tässä alaluvussa käsitellään Suomen kansallisia strategioita, selontekoja ja muita hallinnollisia julkaisuja maan asemaa kansainvälisessä kontekstissa ja kansainvälisen yhteistyön merkitystä kyberhuoltovarmuuden edistämisessä.

Kansalliset kyberturvallisuusstrategiat ovat perusta, jonka päälle rakennetaan maan kyberpuolustuksen toimintamallit. Strategioiden tarkoituksena on määritellä selkeät periaatteet ja toimintatavat, jotka ohjaavat kyberturvallisuuden hallintaa kansallisella tasolla. Strategiat määrittelevät selkeät tavoitteet, politiikat ja toimenpiteet, joita tarvitaan kyberuhkien torjumiseen ja kyberturvallisuusvalmiuksien ylläpitämiseen. Ne ovat yhteydessä laajempiin turvallisuus- ja puolustuspolitiikkoihin ja niitä päivitetään säännöllisesti vastaamaan nopeasti muuttuvia kyberympäristön vaatimuksia. Tällaiset strategiat kattavat usein kyberturvallisuuden riskienhallinnan, varautumisen kyberuhkiin ja kyberturvallisuuden parantamiseen tähtäävät toimenpiteet. Suomessa, kuten muissakin maissa, kyberturvallisuusstrategiat pyrkivät turvaamaan kansallisia etuja ja suojaa kriittistä infrastruktuuria ja toimintoja kyberuhilta ja häiriöiltä. (Lehto ym., 2018)

Suomi on tehnyt merkittäviä panostuksia kansallisen kyberturvallisuusstrategian kehittämiseen, vuoden 2022 huoltovarmuusselonteon mukaan (Valtioneuvosto, 2022b) turvallisuuspoliittisilla linjauksilla pyritään aktiivisesti vastaamaan sekä kansallisiin että kansainvälisiin turvallisuushaasteisiin. Erityisesti huoltovarmuuden ylläpitäminen on keskeistä, minkä vuoksi Suomi on kehittänyt omia varautumistoimiaan sekä osallistuu kansainväliseen yhteistyöhön. Huoltovarmuuden kansainvälisessä toimintaympäristössä Suomi painottaa sekä EU:n että pohjoismaisen yhteistyön merkitystä, erityisesti globaalien turvallisuusuhkien havainnoinnissa ja torjunnassa. (Valtioneuvosto, 2022b)

Suomen kyberturvallisuusstrategia perustuu kansalliseen kokonaisuuden ymmärrykseen ja sen toteuttaminen on monivaiheinen prosessi. Kyberturvallisuuden kehittämisohjelma 2021 (Liikenne- ja viestintäministeriö, 2021) korostaa kansallisen kyberturvallisuuskeskuksen roolia kyberuhkien tunnistamisessa ja

vastaamisessa, edistäen samalla kansallisten toimijoiden yhteistyötä. Suomen kyberturvallisuusstrategia vuodelta 2013 (Turvallisuus- ja puolustusasian komitea, 2013) käsittelee kehitystyön yksityiskohtia tarkemmin, kuvaten esimerkiksi kuinka strategian tavoitteena on lisätä yleistä tietoisuutta kyberuhkista ja kehittää kansallista kyberturvallisuusosaamista. Pääministeri Petteri Orpon hallitusohjelma 2023 *Vahva ja välittävä Suomi* (Valtioneuvosto, 2023) tuo esiin, että on kyberturvallisuuden edistäminen yhtenä avaintekijänä kansallisessa turvallisuuspolitiikassa, mikä osoittaa hallituksen sitoutumista kyberturvallisuuden kehittämiseen.

Suomalainen digi-alan edunvalvoja FiCom on julkaissut huomionsa edellisen kappaleen lopussa käsiteltyyn Orpon hallitusohjelmaan. Ohjelmaa ja sen tavoitteita pidetään kokonaisuutena hyvänä etenkin digitaalisen infrastruktuurin kehittämisen ja hallinnollisen taakan keventäminen vuoksi, mutta vanhentuneen teknologian, esimerkiksi 2G verkon käytön jatkaminen ja kriittisen tiedon keskittäminen saavat kritiikkiä. (FiCom, 2023)

Kyberturvallisuus on noussut yhdeksi Suomen kansallisen turvallisuuden keskeisistä pilareista, sillä digitaalisen toimintaympäristön laajentuessa kyberuhkien merkitys on kasvanut. Tämä on johtanut tarpeeseen kehittää kattavia kansallisia strategioita, jotka eivät ainoastaan torju kyberuhkia vaan myös vahvistavat kansallista kyberhuoltovarmuutta. Lisäksi Suomen rooli kansainvälisessä kyberturvallisuusyhteistyössä korostuu, kun pyritään yhteisiin toimiin globaalien kyberuhkien torjumiseksi. (Turvallisuuskomitea, 2019)

Suomi on tunnustettu kyberturvallisuuden edelläkävijäksi, mikä heijastuu maan kattavissa ja jatkuvasti päivitettävissä kansallisissa kyberturvallisuusstrategioissa. Nämä strategiat kattavat laajan kirjon toimenpiteitä, jotka tähtäävät siihen, että Suomi pystyy suojaamaan elintärkeät toimintonsa kaikissa olosuhteissa kyberuhkia vastaan. Strategiat korostavat kyberturvallisuuden keskeistä roolia kansallisessa turvallisuudessa ja sisältävät toimenpiteitä kyberuhkien ennaltaehkäisemiseksi, havaitsemiseksi ja niihin vastaamiseksi. Erityistä huomiota kiinnitetään kansallisen kyberturvallisuuden tilannekuvan ylläpitoon, joka perustuu jaettuun tietoon viranomaisten, yksityisen sektorin, tutkijoiden ja asiantuntijoiden välillä, mikä on elintärkeää tehokkaan havainnointikyvyn ja päätöksentekokyvykkyyden kannalta. (Lehto & Limnéll, 2017)

Sisäisen turvallisuuden strategia (Sisäministeriö, 2017) sisältää kattavan suunnitelman kansallisen turvallisuuden varmistamiseksi, mukaan lukien kyberturvallisuuden toimenpiteet. Strategia nostaa kyberturvallisuuden integrointia tärkeäksi osaksi kansallista turvallisuutta, tavoitteena kehittää monipuolisia varautumistoimia muuttuvaan toimintaympäristöön. Varautumisen tulee olla osa jokapäiväistä toimintaa kaikilla yhteiskunnan tasoilla, ja siinä korostetaan tarvetta jatkuvasti päivittää toimintasuunnitelmia vastaamaan uusia uhkia. (Sisäministeriö, 2017)

Suomen kansalliset kyberturvallisuusstrategiat on suunniteltu vastaamaan nykyaikaisen digitaalisen maailman haasteisiin, keskittyen erityisesti yhteiskunnan kriittisten infrastruktuurien suojaamiseen. Strategioiden ydin sisältää toimenpiteitä, jotka kattavat uhkien ennaltaehkäisyn, havaitsemisen ja niihin

reagoinnin, kyberturvallisuusosaamisen kehittämisen ja kansainvälisen yhteistyön. Kansallisessa kyberturvallisuusstrategiassa korostetaan yhteistyön merkitystä eri toimijoiden, kuten valtion virastojen, yritysten ja kansalaisten välillä. Tavoitteena on luoda yhtenäinen ja joustava toimintaympäristö, joka kykenee vastustamaan kyberuhkia ja turvaamaan kansalaisten turvallisuuden ja toimeentulon, sekä yhteiskunnan elintärkeiden toimintojen jatkuvuuden. (Valtioneuvosto, 2022b)

5.2 Suomi kansainvälisessä kontekstissa

Kansainvälisesti Suomi tunnetaan aktiivisena ja innovatiivisena toimijana kyberturvallisuuden alalla. Maan panos kansainväliseen dialogiin ja yhteistyöhön, kuten EU:n ja Naton kaltaisten organisaatioiden kautta, on merkittävä. Suomi osallistuu moniin kansainvälisiin aloitteisiin ja yhteistyöhankkeisiin, joilla pyritään parantamaan globaalia kyberturvallisuutta ja kehittämään kansainvälisiä normeja ja standardeja. Suomen kokemukset ja osaaminen kyberturvallisuuden alalla ovat arvokkaita globaalissa yhteistyössä, ja maa onkin usein kutsuttu jakamaan parhaita käytäntöjään ja osallistumaan kansainvälisiin kyberturvallisuushankkeisiin. Tämä kansainvälinen yhteistyö ja vuoropuhelu auttavat Suomea pysymään ajan tasalla uusimmista kehityssuunnista ja parhaista käytännöistä kyberturvallisuuden alalla, ja lisäksi se edistää myös kansainvälistä vakautta ja turvallisuutta. (Valtioneuvosto, 2021a; Lehto ym., 2018)

Globaalissa kontekstissa Suomi pyrkii olemaan aktiivinen toimija, joka edistää avointa ja turvallista kyberavaruutta kansainvälisen yhteistyön ja sopimusten avulla. Suomen osallistuminen kansainvälisiin hankkeisiin ja foorumeihin, kuten Euroopan unionin kyberturvallisuusaloitteisiin ja YK:n kyberturvallisuusneuvotteluihin, osoittaa maan sitoutumisen globaalin kyberturvallisuusyhteisön vahvistamiseen. Suomi painottaa tarvetta vahvistaa kansainvälisiä normeja ja standardeja, jotka tukevat vastuullista toimintaa kyberavaruudessa ja edistävät globaalia kyberturvallisuutta. (Valtioneuvosto, 2022b)

Kyberuhkien monimutkaistuminen ja digitalisaation nopea eteneminen korostavat tarvetta kattavalle kyberturvallisuusstrategialle. Strategian tulisi ottaa huomioon kansallisen ja kansainvälisen tason yhteistyön kehittäminen, jotta voidaan vastata kybertoimintaympäristön globaaliin luonteeseen. Lisäksi on tärkeää kehittää kyberturvallisuuden osaamista ja varmistaa, että kaikilla yhteiskunnan toimijoilla on tarvittavat resurssit ja tietotaito kyberuhkien tunnistamiseen ja torjuntaan. Suomi pyrkii vahvistamaan kyberturvallisuuttaan osallistumalla aktiivisesti Euroopan unionin ja muiden kansainvälisten organisaatioiden toimintaan. Suomen strategiana on säilyttää kybertoimintaympäristön avoimuus ja turvallisuus, johon sisältyy kansainvälisten sopimusten ja oikeusvaltioperiaatteiden kunnioittaminen. Suomi korostaa myös aktiivista rooliaan EU:n kyberturvallisuusstrategian kehittämisessä ja osallistuu EU:n kybervastatoimiin, mukaan lukien kyberrikollisuuden torjuntaan oikeus- ja lainvalvontaviranomaisten kansainvälisellä yhteistyöllä. (Turvallisuuskomitea, 2019)

Suomen turvallisuuspoliittinen asema muuttui ratkaisevasti, kun siitä 4.4.2023 tuli puolustusliitto Naton täysivaltainen jäsen. Venäjän helmikuussa 2022 käynnistäneen täysimittaisen hyökkäyssodan alkuun asti Suomen kansa ja valtaosa poliitikoista ja valtionjohdosta olivat liittoutumattomuuden kannalla, mutta sota Euroopassa käänsi niin kansalaisten, kuin päättäjien mielen Natojäsenyyden kannalle. Suomi ei jäsenenä ole pelkästään turvallisuuden saaja, vaan myös sen tuottaja ja Naton vahvistaja. Suomessa maanpuolustus on hoidettu (useista länsimaista poiketen) hyvin, ja lisäksi Suomen kokonaisturvallisuuden malli ja koko yhteiskunnan kriisinsietokyky ovat arvostettuja liittolaisten keskuudessa. (Laajava, 2023) Suomen asema idän ja lännen välissä, ja useiden lännen edustajien mielikuvat Suomesta muuttuivat nopeasti Ukrainan sodan aikaisesta, jolloin Suomea usein pidettiin venäjän mielistelijänä ja myötäilijänä. Liittoutumattomuus nähtiin heikkoutena, ja kylmän sodan jälkeen suomettumisesta puhuttiin taas yhä enemmän. (Henttonen, 2021) Nyt Suomi hakee uutta suuntaa ja asemaa puolustusliiton jäsenenä, ja entistä tiukemmin integroituneena läntiseen yhteisöön ja sen arvoihin. Venäjä on edelleen Suomen suurin turvallisuusuhka, ja sijainti roistovaltiona nähtävän Venäjän naapurissa asettaa sille edelleen haasteita.

Venäjän suorittamat kyberhyökkäykset ovat olleet keskeinen osa maan kansainvälistä toimintaa, erityisesti kriittiseen infrastruktuuriin kohdistuvat iskut ovat herättäneet huolta. Venäjä on toteuttanut useita operaatioita, jotka ovat kohdistuneet muun muassa energia-alan tietojärjestelmiin eri maissa. Nämä hyökkäykset eivät ainoastaan häiritse palveluita, vaan ne luovat myös poliittista painetta ja epävarmuutta kohdemaissa. Erityisesti Venäjän kyky käyttää kybersodankäyntiä strategisena välineenä on merkittävä huolenaihe Suomelle, joka pyrkii varmistamaan omien kriittisten infrastruktuuriensa turvallisuuden. Venäjän toiminta kyberavaruudessa on monimutkaista, sisältäen sekä avoimia että piilotettuja operaatioita, jotka voivat vaihdella tiedustelusta infrastruktuurin suoranaisiin vahingoittamisiin. Tällainen toiminta on osa laajempaa hybridisodankäyntiä, jossa kyberhyökkäykset yhdistetään perinteiseen sotilasvoimaan ja psykologiseen vaikuttamiseen. (Kukkola, 2020)

Myös Kiinaa pidetään aktiivisena toimijana ja kyberhyökkäysten tekijänä. Se pyrkii vahvistamaan globaalia asemaansa monin keinoin, erityisesti kybertoimintaympäristössä. Maan strategia on ollut kehittää kyberturvallisuusosaamistaan sekä lisätä kykyään hyödyntää kyberteknologioita valtion ja talouden tasolla. Tämä näkyy selvästi Kiinan panostuksessa kyberkapasiteetin kehittämiseen, mikä mahdollistaa niin teknologisen kilpailukyvyn kasvun kuin sotilaallisten kyvykkyyksien parantamisen. Kiina on aktiivisesti hankkinut länsimaista teknologiaa, mikä on kiihdyttänyt sen kyberosaamisen kehitystä. Tämä teknologinen edistys on osaltaan myös tukemassa Kiinan sotilaallista kehitystä, sillä se mahdollistaa laajemmat ja monipuolisemmat sotilaalliset toimet kansainvälisissä konflikteissa ja turvallisuuskysymyksissä. Kiinan kansainvälisissä suhteissa tämä kapasiteetti luo maalle uusia mahdollisuuksia toimia globaalilla näyttämöllä, haastaa muiden suurvaltojen teknologinen ja sotilaallinen ylivalta, ja sitä kautta muokata kansainvälistä järjestystä suosimaan sen omia etuja ja

maailmankuvaa. Kiina pyrkii edistämään yhteiskuntamalliaan, joka perustuu autoritaarisuuteen ja valtion kontrolliin, myös kyberavaruudessa. Tämä on haaste läntiselle demokratialle ja avoimuuden periaatteille, jotka ovat hallitsevia länsimaissa. Kiinan pyrkimykset vahvistaa asemiaan globaaleissa kyberstruktuureissa ja standardisoinnissa, samalla kun se pyrkii säilyttämään hallinnan omassa sisäpolitiikassaan ja teknologiapolitiikassaan, heijastavat sen strategisia tavoitteita sekä kyberympäristössä että laajemmassa kansainvälisessä politiikassa. (Ulkoministeriö, 2021)

Yleisradio uutisoi kesällä 2023 artikkelissaan *Yhdysvaltojen hallinto etsii kiinalaishakkereiden "tikittävää aikapommia" järjestelmistään – haittaohjelmalla aiheuttaa laajaa häiriötä* (Yleisradio, 2023), että presidentti Bidenin hallinto epäilee Kiinan asentaneen viestiverkkoon ohjelman, jolla se voisi tarvittaessa vaikuttaa Yhdysvaltojen asevoimiin katkaisemalla esimerkiksi sähkö-, vesi- ja viestintäyhteydet sotilastukikohtiin. Saamaa ohjelmaa voisi tiedustelutietojen mukaan käyttää myös yrityksiä ja jopa kotitalouksia vastaan. Laitevalmistaja Microsoft ja tarkemmin nimeämättömät valtiot uskoivat, että sama kriittisen infrastruktuurin verkkoihin tunkeutuminen olisi maailmanlaajuista. (Yleisradio, 2023)

5.3 Kansainvälinen yhteistyö kyberhuoltovarmuudessa

Kansainvälinen yhteistyö on keskeinen elementti kyberhuoltovarmuuden kehittämisessä, sillä kyberuhkat eivät tunne kansallisia rajoja. Tämä yhteistyö eri maiden ja kansainvälisten järjestöjen välillä mahdollistaa tiedon, resurssien ja parhaiden käytäntöjen jakamisen. Suomi tekee tiivistä yhteistyötä eri maiden, kansainvälisten organisaatioiden ja yksityisen sektorin kanssa kehittääkseen ja ylläpitääkseen tehokkaita mekanismeja kyberhyökkäysten ennaltaehkäisyyn ja niihin reagointiin, ja osallistuu aktiivisesti useisiin kansainvälisiin kyberturvallisuusaloitteisiin ja -harjoituksiin, edistäen globaalia kyberturvallisuutta ja vahvistamalla kansainvälistä yhteistyötä. Lisäksi Suomi tekee tiivistä yhteistyötä Pohjoismaiden ja muiden lähialueiden maiden kanssa kyberturvallisuuden alalla. Pohjoismainen yhteistyö kyberturvallisuuden alalla on esimerkki alueellisesta yhteistyöstä, joka hyödyttää kaikkia osapuolia ja vahvistaa alueen kyberturvallisuutta. Tämä yhteistyö kattaa muun muassa yhteiset harjoitukset, tiedonvaihdon ja yhteiset kehityshankkeet. (Lehto & Limnéll, 2017; Lehto ym., 2018)

Norjan tiedusteluviranomaisen mukaan (The Norwegian Intelligence Service, 2024) kansainvälinen yhteistyö on olennainen osa häiriötilanteiden hallintaa huoltovarmuuden näkökulmasta. Kyberuhkien globaali luonne edellyttää tiivistä yhteistyötä maiden ja kansainvälisten organisaatioiden välillä tiedonvaihdon, parhaiden käytäntöjen jakamisen ja yhteisten turvallisuusstandardien kehittämisen alueilla. Tämä mahdollistaa nopeamman reagoinnin ja tehokkaamman puolustuksen yhteisiä uhkia vastaan. (The Norwegian Intelligence Service, 2024)

Suomen kansainvälinen yhteistyö kyberhuoltovarmuudessa kattaa laajan kirjon toimia, joilla pyritään varmistamaan kansallinen turvallisuus kyberuhkilta.

Yhteistyö EU:n ja NATO:n kaltaisten organisaatioiden kanssa on merkittävässä roolissa, ja Suomi pyrkii parantamaan kyberturvallisuusinfrastruktuurinsa vastustuskykyä yhdessä kansainvälisten kumppaneiden kanssa. Erityisesti huoltovarmuusyhteistyö keskittyy kyberuhkien ennakointiin ja vastaamiseen, strategisen kyberosaamisen kehittämiseen sekä sotilaallisen huoltovarmuuden vahvistamiseen kansainvälisissä verkostoissa. (Valtioneuvosto, 2022b)

5.4 Päätelmät, vastauksia tutkimuskysymyksiin ja yhteenveto

Kyberhuoltovarmuus kokonaisturvallisuuden näkökulmasta on moniulotteinen ja kriittinen alue, joka edellyttää jatkuvaa huomiota, kehitystä ja kansainvälistä yhteistyötä. Tämän luvun tarkastelun perusteella voidaan tehdä useita keskeisiä päätelmiä Suomen kyberhuoltovarmuuden tilasta, sen merkityksestä huoltovarmuudelle ja sen roolista kokonaisturvallisuuden kontekstissa.

Kyberhuoltovarmuuden merkitys huoltovarmuudelle on keskeinen, sillä se mahdollistaa yhteiskunnan kriittisten toimintojen suojaamisen ja jatkuvuuden digitaalisessa ympäristössä. Kyberturvallisuusstrategiat ja kansalliset toimenpiteet ovat elintärkeitä kansallisen huoltovarmuuden ylläpitämiseksi ja vahvistamiseksi, mikä on erityisen tärkeää, kun otetaan huomioon kyberuhkien jatkuva evoluutio ja digitalisaation nopea eteneminen. Kyberhuoltovarmuuden merkitys korostuu, kun teknologinen riippuvuus kasvaa ja kyberuhkat monimutkaistuvat.

Kyberhuoltovarmuuden tilanne Suomessa on vahva, ja maa on kansainvälisesti tunnustettu kyberturvallisuuden edelläkävijä, joka pyrkii ylläpitämään korkeaa kyberturvallisuuden tasoa ja parantamaan huoltovarmuutta vastaamaan nopeasti muuttuviin kyberympäristön vaatimuksiin. Suomi on kehittänyt kattavia kansallisia strategioita ja osallistuu aktiivisesti kansainväliseen yhteistyöhön. Tämä proaktiivinen lähestymistapa ja jatkuva päivitys varmistavat, että Suomi pysyy kyberturvallisuuden kehityksen kärjessä, suojaten kriittisiä infrastruktuureja ja edistäen kansalaisten turvallisuutta. Jotta strategioiden tavoitteet voidaan saavuttaa, ne on ”jalkautettava”, eli strategioiden perusteella täytyy tehdä toimenpiteitä, ja niiden toteutusta ja vaikutuksia on seurattava.

Kyberulottuvuudessa tapahtuvan huoltovarmuuteen vaikuttaminen heikentää kokonaisturvallisuutta, ja on merkittävä riski, joka korostaa kyberhuoltovarmuuden keskeistä roolia. Kyberhyökkäykset voivat heikentää kriittistä infrastruktuuria ja häiritä yhteiskunnan perustoimintoja, mikä vaikuttaa suoraan kansalliseen turvallisuuteen, ja tekee kyberhuoltovarmuudesta erottamattoman osan kansallista ja kansainvälistä turvallisuutta.

Huoltovarmuuden toimintojen ja toimijoiden kyberhaavoittuvuudet ovat moninaisia ja jatkuvasti muuttuvia. Tämän vuoksi on tärkeää ylläpitää jatkuvaa tietoisuutta uhista, kehittää tehokkaita havainnointi- ja reagointivalmiuksia sekä edistää kyberturvallisuusosaamista kaikilla tasoilla. Lisäksi on keskeistä jatkaa investointeja kyberturvallisuuden kehittämiseen, erityisesti kriittisen infrastruktuurin osalta. Kansainvälinen yhteistyö ja tietojenvaihto ovat avainasemassa, kun pyritään vastaamaan yhteisiin haasteisiin ja vahvistamaan globaalia

kyberhuoltovarmuutta. Suomen on tärkeää toimia aktiivisesti kansainvälisissä foorumeissa ja tehdä yhteistyötä muiden maiden kanssa kyberuhkien torjumiseksi ja kyberresilienssin parantamiseksi.

Suomen asema idän ja lännen välissä, sekä sen fyysinen sijainti ja rooli kansainvälisissä kyber- ja hybridivaikuttamisen konteksteissa, lisäävät maan kyberhuoltovarmuuden merkitystä. Venäjän ja Kiinan kaltaiset toimijat asettavat erityisiä haasteita, jotka vaativat huomiota ja strategista lähestymistapaa. Tämä korostaa tarvetta laaja-alaiselle yhteistyölle ja vuoropuhelulle sekä kehittyneiden kyberpuolustusvalmiuksien kehittämiseen.

Kansallisen kyberturvallisuuden tila ja siihen kohdistuvat haasteet vaativat jatkuvaa arviointia ja päivittämistä, jotta voidaan varmistaa yhteiskunnan elintärkeiden toimintojen suojaaminen. Kyberturvallisuuden kehittämisen on oltava joustavaa ja mukautuvaa, ja siinä on huomioitava uusien teknologioiden tuomat mahdollisuudet sekä uhkat. Tehokkaiden kyberturvallisuusmekanismien toteuttaminen edellyttää merkittäviä resursseja sekä julkiselta, että yksityiseltä sektorilta, ja tämä resurssien kohdentaminen on kriittinen osa kyberturvallisuusstrategian toteuttamista. (Lehto ym., 2017; Turvallisuuskomitea, 2019)

6 KYBERUHKIEN TUNNISTAMINEN, HALLINTA JA TORJUNTA

Kyberuhkien tunnistaminen, havainnointi ja torjunta ovat keskeisiä osia nykyaikaisen yhteiskunnan turvallisuusstrategioissa, muodostavat perustan modernin yhteiskunnan kyberturvallisuudelle. Tietotekniikan ja digitalisaation keskeinen rooli kaikilla elämänalueilla tekee kyberturvallisuudesta elintärkeän koko yhteiskunnan toimivuuden ja turvallisuuden kannalta. Kyberuhkien monimuotoisuus ja jatkuva evoluutio edellyttävät jatkuvaa valppautta, uusien teknologioiden ja menetelmien kehittämistä sekä yhteistyötä eri toimijoiden välillä.

Kyberuhkien tunnistaminen ja hallinta vaatii jatkuvaa valppautta ja kehittyneitä analytiikkamenetelmiä. Hybridisodankäynnin evoluutio osoittaa, että kyberhyökkääjät pyrkivät häiritsemään yhteiskunnan perusrakenteita ja kansalaisten turvallisuutta usein taloudellisin motiivein. Tämän torjumiseksi on keskeistä kehittää kykyjä tunnistaa, arvioida ja vastata kyberuhkiin, jotka kohdistuvat kriittisiin infrastruktuureihin ja kansalaisten elinolosuhteisiin. Kattava uhkien havainnointi ja ennaltaehkäisy, mukaan lukien tiedustelutiedon analysointi ja kyberturvallisuusvalmiuksien jatkuva päivitys, ovat välttämättömiä. (Uusipaavalniemi & Puistola, 2016)

Ensimmäisessä vaiheessa, tunnistamisessa, keskitytään mahdollisten kyberuhkien ja niiden alkuperien ymmärtämiseen. Tässä vaiheessa teknologia on avainasemassa, mutta myös inhimillinen asiantuntemus on korvaamatonta. Jatkuvasti kehittyvä teknologia edellyttää, että uhkatunnistusmekanismit ovat ajan tasalla ja kykenevät tunnistamaan uusia haavoittuvuuksia ja hyökkäystyyppejä tehokkaasti. (Harjanne ym., 2018)

Toinen vaihe, havainnointi, keskittyy aktiiviseen seurantaan ja epätavallisen toiminnan ja liikenteen havaitsemiseen sekä verkkoliikenteessä, että verkkojen ja järjestelmien sisällä. Tämän vaiheen tavoitteena on mahdollistaa nopea reagointi havaittuihin poikkeamiin, estäen näin potentiaalisten hyökkäysten eskaloitumisen suuremmiksi vahingoiksi. (Harjanne ym., 2018)(Valtioneuvosto, 2021a)

Kolmannessa vaiheessa, torjunnassa, yhdistyvät erilaiset turvatoimet, jotka kattavat tekniset ratkaisut, kuten virustorjuntaohjelmistot, sekä hallinnolliset toimet, kuten turvallisuuskäytännöt ja koulutusohjelmat. Tämän monitasoisen lähestymistavan tarkoituksena on luoda vahva puolustus kyberuhkia vastaan, suojellen näin organisaation kriittisiä tietoja ja infrastruktuureja. (Harjanne ym., 2018; Valtioneuvosto, 2022b)

Kyberturvallisuuden haasteiden monimutkaisuus edellyttää laajaa yhteistyötä sekä kansallisella että kansainvälisellä tasolla. Tämä yhteistyö ei ainoastaan lisää tietoturvaa, vaan myös nopeuttaa toipumista mahdollisista hyökkäyksistä, mikä on kriittistä yhteiskunnan sujuvan toiminnan ja turvallisuuden kannalta. (Valtioneuvosto, 2022b; Valtioneuvosto, 2021a; Harjanne ym., 2018)

6.1 Kyberuhkien evoluutio ja luokittelu (tai tunnistaminen ja arviointi)

Kyberuhkien määrittely ja luokittelu on tärkeä askel kohti tehokasta kyberturvallisuusstrategiaa. Kyberuhkia luokitellaan usein niiden alkuperän, kuten valtiolliset toimijat, rikollisjärjestöt tai yksittäiset hakkerit, ja niiden vaikutusten, kuten tiedon varastaminen, palvelunestohyökkäykset tai infrastruktuurin sabotointi, perusteella. Tämä luokittelu auttaa organisaatioita ymmärtämään, millaisia toimenpiteitä niiden tulee priorisoida uhkien torjumiseksi. (Rantapelkonen & Salminen, 2013)

Suojelupoliisin tuoreiden raporttien, Supo Vuosikirja 2022 (Suojelupoliisi, 2023b) ja Kansallisen turvallisuuden katsaus 2022 (Suojelupoliisi, 2023a), mukaan kyberuhkien kehittyminen on yhteydessä teknologisen edistyksen ja digitaalisen ympäristön laajentumisen kanssa. Niiden tunnistaminen vaatii ymmärrystä uhkien monimuotoisuudesta ja niiden jatkuvasta evoluutiosta. Kyberuhkia voidaan luokitella monin tavoin, esimerkiksi niiden alkuperän, tavoitteiden tai toteutustavan perusteella. Valtiolliset toimijat, kuten Venäjä ja Kiina, ovat merkittäviä uhkien lähteitä, jotka kykenevät kehittyneisiin kybervakoilu- ja vaikuttamistoimiin. Myös järjestäytynyt rikollisuus ja erilaiset aktivistiryhmät muodostavat uhkia, jotka vaihtelevat tietojen varastamisesta palvelunestohyökkäyksiin. (Suojelupoliisi, 2023a; Suojelupoliisi, 2023b)

Kyberuhat kehittyvät jatkuvasti, tämä näkyy niiden monimutkaistumisessa ja uusien hyökkäystapojen kehittymisessä. Kuten Suojelupoliisi, myös Norjan tiedusteluviranomainen arvio valtiollisten toimijoiden, erityisesti Venäjän, tavoitteiden ulottuvan tiedustelusta ja vaikuttamisesta aina kriittisen infrastruktuurin sabotointiin, mikä korostaa kyberuhkien moniulotteisuutta ja niiden potentiaalista vaikutusta kansalliseen turvallisuuteen. (The Norwegian Intelligence Service, 2024)

Kyberuhkien luokittelu on olennainen osa niiden ymmärtämistä ja torjuntaa. Luokittelussa voidaan hyödyntää useita kriteereitä, kuten uhkien alkuperä, hyökkäyksen kohde ja käytetyt taktiikat, tekniikat ja menetelmät, sekä niiden strategiset tavoitteet. Luokittelu voi perustua esimerkiksi uhkien vakavuuteen, todennäköisyyteen tai potentiaaliseen vahinkoon. Valtiolliset toimijat, kuten Venäjä ja Kiina, sekä muut autoritaariset valtiot, käyttävät kyberoperaatioita osana laajempaa strategista valtapeliä, pyrkien heikentämään lännen vaikutusvaltaa ja edistämään omia geopoliittisia tavoitteitaan. Toisaalta rikollisryhmät saattavat keskittyä taloudellisen hyödyn tavoitteluun esimerkiksi kiristysohjelmien ja finanssialan petosten kautta. (The Norwegian Intelligence Service, 2024)

6.2 Uhkien havainnointi ja ennaltaehkäisy

Suojelupoliisin raportin (Suojelupoliisi, 2023b) mukaan uhkien havainnointi ja niiden ennaltaehkäisy ovat kyberuhkien hallinnan kulmakiviä. Järjestelmällinen lokitietojen kerääminen ja analysointi, päivitetyt tietoturvakäytännöt sekä järjestelmien ja ohjelmistojen säännöllinen päivittäminen ovat keskeisiä toimenpiteitä havainnoinnissa. Lisäksi organisaatioiden on tärkeää tehdä tiivistä yhteistyötä niin kansallisten kuin kansainvälistenkin kumppaneiden kanssa ja hyödyntää esimerkiksi kyberturvallisuuskeskusten tuottamaa tietoa ja ohjeita uhkien torjumiseksi. (Suojelupoliisi, 2023b)

Kyberuhkien havaitseminen ja niiden ennaltaehkäisy edellyttävät jatkuvaa tietoturvavalvontaa ja -analytiikkaa. Organisaatioiden tulee kehittää kykyään tunnistaa epätavalliset verkkoaktiviteetit ja reagoida niihin nopeasti. Tämä sisältää kehittyneitä tunkeutumisen havaitsemisjärjestelmiä ja automatisoituja turvallisuustyökaluja, jotka pystyvät estämään hyökkäyksiä reaaliajassa. (Rantapelkonen & Salminen, 2013)

6.3 Häiriötilanteiden hallinta huoltovarmuuden näkökulmasta

Häiriötilanteiden hallinta edellyttää kattavaa suunnittelua ja valmiuksia toimia nopeasti kyberuhkien ilmetessä. Keskeistä on kyky palauttaa järjestelmien toiminta mahdollisimman nopeasti häiriön jälkeen, minimoiden näin yhteiskunnalliset vaikutukset. Erityisesti kriittisen infrastruktuurin osalta on tärkeää, että on olemassa selkeät protokollat ja yhteistyömekanismit, jotka mahdollistavat nopean ja koordinoidun toiminnan eri toimijoiden välillä. (Suojelupoliisi, 2023a)

Norjan tiedusteluviranomaisen vuosittaisen raportin (The Norwegian Intelligence Service, 2024) mukaan häiriötilanteiden hallinta kyberuhkien yhteydessä edellyttää ennakointia ja valmiutta toimia nopeasti uhkatilanteiden ilmetessä. Kyberhyökkäykset voivat vaikuttaa merkittävästi yhteiskunnan kriittiseen infrastruktuuriin, mikä korostaa huoltovarmuuden merkitystä. Huoltovarmuuden näkökulmasta on tärkeää varmistaa, että kriittiset palvelut ja infrastruktuuri pystyvät jatkamaan toimintaansa myös kyberhyökkäysten aikana. Valtion ja yksityisen sektorin välinen yhteistyö on avainasemassa häiriötilanteiden hallinnassa, jotta voidaan varmistaa yhteiskunnan toimintakyky myös poikkeustilanteissa. (The Norwegian Intelligence Service, 2024)

Kybertoimintaympäristöön kohdistuvien häiriötilanteiden hallinta ja yhteistyö operatiivisella tasolla ovat olennaisia, kun kehitetään kyberturvallisuusmekanismeja. Häiriötilanteiden hallinnassa on tärkeää hyödyntää olemassa olevia häiriötilanteiden hallintamalleja ja varmistaa, että on olemassa tehokkaita kommunikaatiokanavia kyberturvallisuustoimijoiden välillä. Tämä yhteistyö ja varautuminen ovat avainasemassa, kun pyritään varmistamaan, että yhteiskunnan elintärkeät toiminnot ovat suojattu kaikissa tilanteissa kyberuhkia vastaan. (Turvallisuuskomitea, 2019)

6.4 Päätelmät, vastauksia tutkimuskysymyksiin ja yhteenveto

Kyberuhkien tunnistaminen, havainnointi ja torjunta ovat kriittisiä kyberhuoltovarmuuden ylläpitämisessä ja kehittämisessä, mikä puolestaan on olennainen osa laajempaa huoltovarmuuskokonaisuutta. Tietotekniikan ja digitalisaation keskeinen rooli kaikilla elämänalueilla tekee kyberturvallisuudesta elintärkeän koko yhteiskunnan toimivuuden ja turvallisuuden kannalta. Kyberuhkien monimuotoisuus ja jatkuva evoluutio edellyttävät valppautta, uusien teknologioiden ja menetelmien kehittämistä sekä yhteistyötä eri toimijoiden välillä.

Kyberhuoltovarmuuden merkitys huoltovarmuudelle korostuu nykyaikaisessa yhteiskunnassa digitaalisen ympäristön ja tietoteknologian keskeisen roolin vuoksi. Kyberhuoltovarmuuden keskeinen merkitys huoltovarmuudelle ilmenee kykyinä tunnistaa, havainnoida ja torjua kyberuhkia, mikä on elintärkeää yhteiskunnan kriittisten infrastruktuurien ja palveluiden suojaamiseksi. Kyberuhkien tehokas hallinta minimoi huoltovarmuuden häiriöitä ja ylläpitää yhteiskunnan toimivuutta ja turvallisuutta.

Kyberhuoltovarmuuden tilanne Suomessa on vahva, kiitos aktiivisen ja jatkuvasti päivittyvän kyberstrategian sekä kansallisen ja kansainvälisen yhteistyön. Suomi pyrkii ylläpitämään korkeaa kyberturvallisuuden tasoa ja parantamaan huoltovarmuutta vastaamaan nopeasti muuttuviin kyberympäristön vaatimuksiin. Suomen kyky tunnistaa, havaita ja torjua kyberuhkia osoittaa maan sitoutumista kyberhuoltovarmuuden ylläpitämiseen ja kehittämiseen. Tämä sitoutuminen heijastuu niin teknologisissa ratkaisuissa kuin hallinnollisissa toimenpiteissäkin, kuten koulutusohjelmissa ja turvallisuuskäytännöissä.

Kyberulottuvuuden vaikutus kokonaisturvallisuuteen on merkittävä. Onnistuneet, kyberulottuvuudessa tapahtuvat hyökkäykset voivat heikentää huoltovarmuutta ja sitä kautta kokonaisturvallisuutta, erityisesti kun otetaan huomioon kriittisen infrastruktuurin riippuvuus digitaalisista järjestelmistä. Kyberhyökkäykset voivat aiheuttaa laajoja häiriöitä, jotka vaikuttavat kaikkiin yhteiskunnan sektoreihin ja peruspalveluihin, korostaen näin kyberhuoltovarmuuden merkitystä osana kokonaisvaltaista turvallisuussuunnittelua.

Kyberhaavoittuvuudet huoltovarmuuden toiminnoissa ja toimijoissa voivat olla monimuotoisia ja jatkuvasti muuttuvia, mikä vaatii jatkuvaa valppautta ja adaptiivista lähestymistapaa niiden hallintaan. Tämä kattaa teknologiset päivitykset, tietoturvakäytäntöjen noudattamisen, sekä yhteistyön kansallisten ja kansainvälisten kumppaneiden kanssa. Tähän sisältyy riski vanhentuneiden teknologioiden, kuten 2G-verkkojen, käytöstä sekä kriittisen tiedon keskittämisen haavoittuvuudesta. Haavoittuvuudet eivät rajoitu vain teknisiin järjestelmiin, vaan myös ihmisiin ja prosesseihin, mikä korostaa kattavan ja monikerroksisen lähestymistavan tarvetta kyberuhkien torjunnassa. Lisäksi, kuten Norjan tiedusteluviranomainen raportoi, valtiolliset toimijat ja järjestäytynyt rikollisuus kykenevät kehittyneisiin ja monimuotoisiin hyökkäyksiin, jotka voivat kohdistua erityisesti kriittiseen infrastruktuuriin.

Kyberhuoltovarmuuden kehittäminen ja ylläpitäminen on siis kriittistä koko yhteiskunnan turvallisuuden ja toimivuuden kannalta. Se vaatii jatkuvaa

valppautta, innovaatiota ja yhteistyötä niin kansallisella kuin kansainväliselläkin tasolla, jotta voidaan tehokkaasti vastata jatkuvasti kehittyviin kyberuhkiin.

7 KYBERHUOLTOVARMUUDEN MERKITYS KRIITTISILLE INFRASTRUKTUUREILLE

7.1 Digitalisaation vaikutus huoltovarmuuteen

Digitalisaation myötä yhteiskunnan toiminnot ovat entistä riippuvaisempia digitaalisista järjestelmistä ja verkkojen toimivuudesta. Tämä kehitys on tehostanut toimintoja mutta samalla lisännyt haavoittuvuuksia. Kyberhuoltovarmuus on tässä yhteydessä elintärkeää, sillä se varmistaa, että kriittiset järjestelmät voivat jatkaa toimintaansa myös häiriötilanteissa ja kyberuhkien alla. (Suojelupoliisi, 2023a) Myös Marko Palokankaan toimittaman *Sodan usvaa* -kirjan luvussa 9 *Kompleksisuuskuilu toimitusketjujen hallinnan haasteena kybertoimintaympäristössä* (Savolainen, 2022) mukaan Digitalisaatio on mullistanut yhteiskunnan toimintatapoja, mukaan lukien kriittisen infrastruktuurin hallinnan. Se on tuonut mukanaan merkittäviä tehokkuusetuja mutta myös lisännyt riippuvuutta digitaalisista järjestelmistä ja verkkojen toimintakyvystä. Tämä kehityskulku korostaa kyberhuoltovarmuuden merkitystä, sillä digitaalisen toimintaympäristön häiriöt voivat vaikuttaa laajasti yhteiskunnan elintärkeisiin toimintoihin. (Savolainen, 2022)

Myös Bo Österlundin väitöskirjan *Suomen meriliikenteen huoltovarmuudelle asetetut tavoitteet ja niiden toteutuminen* (Österlund, 2019) mukaan digitalisaation eteneminen on vahvistanut yhteiskunnan riippuvuutta digitaalisista järjestelmistä, ja tämä on tuonut uusia haasteita kriittisen infrastruktuurin turvaamiseen. Hän käyttää esimerkkinä merikuljetuskapasiteetin kaltaista infrastruktuuria keskeisenä huoltovarmuudelle, jossa niiden monimutkaisuus ja laaja toimijaverkosto korostavat selkeän tiedonkulun, toimivan tilannekuvan ja tehokkaan johtamisen merkitystä. Digitaaliset ratkaisut voivat tarjota uusia työkaluja häiriötilanteiden hallintaan, mutta samalla ne tuovat lisähaasteita tietoturvaan ja kyberresilienssiin. (Österlund, 2019)

Huoltovarmuusorganisaation Digipoolin vuonna 2020 julkaiseman kartoituksen, *Kyberturvallisuuden nykytila eri toimialoilla*, (Huoltovarmuusorganisaation

digipooli, 2020) mukaan huoltovarmuuden kannalta kriittisten yritysten toimintojen digitalisaatio lisää kyberturvallisuuden merkitystä huoltovarmuudelle. Selvitys tarkasteli yli sadan yrityksen ja kahdentoista eri toimialan nykyistä kyberturvallisuustilannetta. Digitalisaation myötä myös yhteiskunnan peruspalveluiden tarjoajien on yhä enemmän huolehdittava kyberturvallisuudesta, mikä tekee siitä kriittisen osan liiketoimintaprosesseja. Raportin mukaan kyberturvallisuuden kehittämisen haasteena on puutteelliset vertailutiedot, jotka vaikeuttavat toimenpiteiden oikeanlaista kohdentamista ja niiden vaikutusten arviointia. (Huoltovarmuusorganisaation digipooli, 2020)

Digitalisaation lisääntyminen on kaksiteräinen miekka huoltovarmuuden kannalta. Toisaalta se mahdollistaa tehokkaamman ja joustavamman infrastruktuurin hallinnan, mutta toisaalta se lisää haavoittuvuuksia kyberhyökkäyksille, erityisesti kriittisissä infrastruktuureissa kuten energia- ja vesihuollossa. Kyberhyökkäyksillä voidaan hyödyntää kriittisen infrastruktuurin haavoittuvuuksia ja aiheuttaa laajamittaisia häiriöitä, jotka voivat vaarantaa kansallisen turvallisuuden ja talouden. Digitalisaation laajentuminen lisää riippuvuutta verkkojärjestelmistä, mikä korostaa tarvetta vahvistaa näiden järjestelmien kyberresilienssiä. Kyberturvallisuuden parantaminen on olennaista, sillä hyökkäykset voivat johtaa kriittisten palveluiden katkeamiseen ja vakaviin taloudellisiin ja yhteiskunnallisiin seurauksiin. (Cybersecurity & Infrastructure Security Agency, 2024)

7.2 Kriittinen infrastruktuuri ja sen kyberhaavoittuvuudet

Kriittiseen infrastruktuuriin, kuten energia-, vesi- ja liikennejärjestelmiin, telekommunikaatioon sekä terveydenhuoltoon kohdistuvat kyberuhkat voivat aiheuttaa laajoja häiriöitä yhteiskunnan toiminnoille. Tietojen kerääminen infrastruktuurin heikkouksista ja niiden teknisestä rakenteesta on yleinen valtiollisten toimijoiden tavoite, mikä korostaa kriittisen infrastruktuurin kyberhaavoittuvuuksien tunnistamisen ja torjunnan merkitystä. (Suojelupoliisi, 2023a) Kriittisen infrastruktuurin digitalisoituminen on lisännyt sen haavoittuvuutta kyberhyökkäyksille. Haavoittuvuudet voivat ilmetä sekä fyysisissä komponenteissa että tietojärjestelmissä, mikä tekee niiden suojauksesta monimutkaista. Kyberhaavoittuvuudet ovat erityisen merkittäviä, kun ne kohdistuvat infrastruktuurin ydinprosesseihin tai kun niitä käytetään laajempien häiriöiden aikaansaamiseen toimitusketjuissa. (Österlund, 2019) Sähköverkkoon, tietoverkkoihin tai tilannekuva-, ja johtamisjärjestelmiin vaikuttaminen voi kerrannaisvaikutusten vuoksi olla erittäin tehokasta, ja siksi ne on suojattava mahdollisimman hyvin.

Norjan tiedustelupalvelun mukaan tuotantoketjujen keskittyminen yhä harvemmille toimijoille, lisää sekä ketjujen haavoittuvuutta, että todennäköisyyttä niiden joutumisesta vaikuttamisen kohteeksi. Lisäksi se hankaloittaa korvaavien tuotantoketjujen käyttöönottoa. (The Norwegian Intelligence Service, 2024) Edellä oleva voidaan yleistää kaikkeen kriittiseen infrastruktuuriin liittyvänä riskinä. Toisaalta eri toimijoiden suuri määrä voi vaikeuttaa tilannekuvan ylläpitoa, ja mahdollisten vastatoimien koordinointia ja toimeenpanoa.

Tanskalainen SektorCERT on julkaissut raportin *Attack against Danish Critical infrastructure* (SektorCERT, 2023), jossa hyökkääjä käytti hyväkseen yksinkertaista, Zyxelin palomuurissa ollutta kriittistä haavoittuvuutta, joka mahdollisti siihen kytkettyjen järjestelmien ohjaamisen ilman käyttäjätunnusta ja salasanaa. Hyökkäys kohdistui erityisesti teollisuuden ohjausjärjestelmiin, jotka ovat kriittisiä energia-, vesi- ja tietoliikenneinfrastruktuurin toiminnalle, ja 22 tanskalaista energia-alan yritystä joutui sen kohteeksi. (SektorCERT, 2023)

Edellisiä havaintoja tukee Ulkopoliittisen instituutin julkaisu *Digital resilience beyond data localisation: National approaches to global challenges* (Holmgren, 2022). Kriittiset infrastruktuurit, kuten sähköverkot ja vesihuolto, ovat entistä riippuvaisempia digitaalisista ohjausjärjestelmistä. Tämä tekee niistä alttiita kyberhyökkäyksille, jotka voivat aiheuttaa laajoja häiriöitä ja vakavia seurauksia yhteiskunnalle. Tietoturvallisuuden puutteet, kuten vanhentunut ohjelmisto ja puutteellinen seuranta, lisäävät riskiä, että ulkopuoliset toimijat voivat häiritä tai tuhota kriittistä infrastruktuuria. Siksi on tärkeää tunnistaa ja korjata kyberhaavoittuvuudet, vahvistaa kyberturvallisuusstandardeja ja kehittää jatkuvaa valmiutta vastata kyberuhkiin. (Holmgren, 2022)

Kriittisen infrastruktuurin sijainti, ja muiden tietojen jakamista julkisesti on pidetty uhkana kokonaisturvallisuudelle. Vuoden 2023 Orpon hallitusohjelmassa on päätetty tarkastella vallitsevaa käytäntöä uudelleen kansallisen turvallisuuden parantamiseksi. (Valtioneuvosto, 2023) Toisaalta samassa ohjelmassa on esitetty tietojen keskittämistä yhteen paikkaan, minkä FiCom arvio julkaisemissaan havainnoissa turvallisuusriskiksi. (FiCom, 2023) Myös Helsingin sanomien artikkelissa 8.3.2024 (Tuohinen, 2024) nähdään kriittisten tietojen yhdistäminen sijaintitietopalveluun riskinä, joka saattaa johtaa tietojen vuotamiseen ja mahdollistaa iskut yhteiskunnan kriittisiin toimintoihin.

7.3 Kriittisen infrastruktuurin kyberresilienssi

Kyberresilienssi eli kyky selviytyä ja toipua kyberhyökkäyksistä on kriittisen infrastruktuurin kannalta välttämätöntä. Kybertoimintaympäristössä toimitusketjun erityispiirteet, kuten kansainväliset häiriöt ja digitalisaation tuomat haasteet, edellyttävät vahvaa kyberresilienssiä. Tämä tarkoittaa paitsi teknisten suojatoimien kehittämistä, myös toimitusketjun eri osien yhteistyötä ja valmiussuunnitelmien laatimista häiriötilanteiden varalle. (Savolainen, 2022)

Resilienssin eli häiriönsietokyvyn vahvistaminen on yksi keskeisistä elementeistä häiriötilanteiden hallinnassa. Tämä tarkoittaa myös kykyä palautua nopeasti kyberhyökkäysten aiheuttamista vahingoista ja jatkaa toimintaa mahdollisimman häiriöttömästi. Resilienssi saavutetaan monikerroksisella turvallisuusstrategialla, joka sisältää tekniset, organisatoriset ja inhimilliset tekijät. Tekninen resilienssi voi sisältää redundanssit kriittisissä järjestelmissä, vahvat salausmenetelmät ja jatkuvan tietoturvan seurannan, sekä varmuuskopioinnin ja palautussuunnitelmat. Organisatorinen resilienssi puolestaan viittaa selkeisiin

vastuualueisiin, toimintasuunnitelmiin, käytäntöjen kehittämiseen ja kyberhyökkäysten simulointiin valmistautumisessa. Inhimillinen tekijä korostaa koulutuksen, tietoisuuden ja valmiuden merkitystä kyberuhkien torjunnassa. (The Norwegian Intelligence Service, 2024; Suojelupoliisi, 2023a)

Kriittisten infrastruktuurien kyberresilienssi tarkoittaa kykyä ennakoida, havaita, reagoida ja toipua kyberuhista siten, että yhteiskunnan elintärkeät toiminnot säilyvät häiriötilanteissa. (Suojelupoliisi, 2023a) Kyberresilienssin vahvistaminen kriittisessä infrastruktuurissa edellyttää monitasoista lähestymistapaa, joka sisältää tekniset suojatoimet, henkilöstön koulutuksen, prosessien kehittämisen ja kriisinhallintavalmiudet. Merkittävä osa resilienssistä on kykyä tunnistaa potentiaaliset uhat, minimoida niiden vaikutukset ja palautua nopeasti häiriötilanteista. Tämä edellyttää jatkuvaa investointia teknologian kehitykseen, osaamisen vahvistamiseen ja kansalliseen sekä kansainväliseen yhteistyöhön. (Österlund, 2019) Kyberresilienssin parantaminen kattaa muun muassa riskienhallintatoimenpiteet, jatkuvat turvallisuusauditoinnit ja -arvioinnit sekä säännölliset koulutukset henkilöstölle. Organisaatioiden on tehtävä tiivistä yhteistyötä kansallisten kyberturvallisuusviranomaisten kanssa ja hyödynnettävä kansainvälistä tietoa ja parhaita käytäntöjä kyberturvallisuuden varmistamiseksi. Tämä edellyttää jatkuvaa valmiutta ja kykyä vastata nopeasti kyberuhkiin, mikä on kriittistä koko yhteiskunnan toimintakyvyn kannalta. (Cybersecurity & Infrastructure Security Agency, 2024)

DNA Oy:n 14.3.2024 järjestämässä tilaisuudessa *Kyberresilienssi liiketoiminnan turvana* esiteltiin DNA:n omistavan Telenorin teettämä tutkimus *Security that goes beyond technology to empower societies* (Telenor, 2023b). Norstat:in tekemän tutkimuksen mukaan yritysten ja kansalaisten kyberturvaa haastavat esimerkiksi tekoälyn kehitys, jatkuvasti muuttuva maailmantilanne ja yksinkertaisesti hektisyys työssä ja arjessa. Kriittisen infrastruktuurin suojaamisessa ja kyberresilienssin kehittämisessä keskeistä on kyberturvallisuusstrategioiden toteuttaminen. Tutkimuksessa on kerätty tietoa pohjoismaisilta yritysjohtajilta, ja raportin mukaan heidän luottamuksensa omaan kyberturvallisuusosaamiseen on korkea, mutta organisaatioiden ymmärryksen puute nähdään suurimpana esteenä kyberturvallisuuden kehittämisessä. Suomalasista yritysjohtajista 87% luotti organisaationsa kykyyn havaita kyberhyökkäykset ja torjua niitä, mutta vain 33%:lla oli niitä varten jonkinlainen varautumissuunnitelma. Yritysjohtajat tunnistavat myös resurssien ja rahoituksen puutteen merkittäviksi haasteiksi. Kyberturvallisuuden parantamiseksi tehdään jatkuvia ponnistuksia, mutta tietotaidon ja resurssien puute estää osittain näiden toimenpiteiden tehokkuuden. Kyberturvallisuustoimenpiteiden aktiivinen käyttöönotto, kuten palomuurit, antivirusohjelmat, kaksivaiheinen tunnistautuminen ja säännölliset tietovarannot, osoittavat kuitenkin, että kriittisen infrastruktuurin suojaamiseen kiinnitetään huomiota. Raportin esittelytilaisuudessa puhunut Puolustusvoimien digitalisaatiojohtaja, insinöörieverstiluutnantti Tero Solante nosti esiin huoltovarmuuden ja varautumisen lisäksi kybersietoisuuden merkityksen kokonaisturvallisuudelle. (DNA Oy, 2024)

Kyberresilienssin kehittäminen kriittisille infrastruktuureille edellyttää monipuolista lähestymistapaa, joka sisältää teknologisia, organisatorisia ja koulutuksellisia toimenpiteitä. On tärkeää kehittää kyberresilienssiä, joka mahdollistaa infrastruktuurin nopean palautumisen ja toiminnan jatkumisen kyberhyökkäyksen sattuessa. Tämä tarkoittaa muun muassa redundanssien rakentamista, vahvoja tietoturvakäytäntöjä ja jatkuvaa koulutusta henkilöstölle kyberuhkien tunnistamiseksi ja niihin reagoimiseksi. Lisäksi on olennaista tehdä yhteistyötä kansainvälisten ja kansallisten toimijoiden kanssa, jotta voidaan jakaa tietoa uhista ja parhaista käytännöistä. (Holmgren, 2022)

7.4 Päätelmät, vastauksia tutkimuskysymyksiin ja yhteenveto

Digitalisaation aikakaudella kyberhuoltovarmuus on noussut huoltovarmuuden keskeiseksi tekijäksi, joka varmistaa yhteiskunnan kriittisten toimintojen jatkuvuuden kyberhyökkäysten ja -häiriöiden tilanteessa. Tämän luvun tarkastelu tarjoaa käsityksen kyberhuoltovarmuuden merkityksestä, sen nykytilasta Suomessa, sekä digitalisaation ja kyberuhkien vaikutuksesta kokonaisturvallisuuteen.

Kyberhuoltovarmuuden merkitys huoltovarmuudelle on merkittävä, koska yhteiskunnan peruspalvelut ja kriittinen infrastruktuuri ovat yhä riippuvaisempia digitaalisista järjestelmistä ja verkoista. Kyberhuoltovarmuuden avulla varmistetaan, että kyberhyökkäykset eivät onnistu, tai elintärkeät järjestelmät voivat toipua hyökkäyksistä, mikä on elintärkeää yhteiskunnan toimivuuden ja kansalaisten turvallisuuden kannalta.

Kyberhuoltovarmuuden tilanne Suomessa on myös tästä näkökulmasta hyvä. Strategioiden mukainen jatkuva vahva panostaminen turvallisuuteen parantaa kyberresilienssiä kansallisella tasolla. Suomessa on tunnistettu kyberuhkien merkitys ja kyberhuoltovarmuuden kehittämiseen on panostettu. Tämä sisältää kyberuhkien ennakoinnin, havainnoinnin ja vastaamisen kykyjen kehittämisen. Suomen aktiivinen osallistuminen sekä kansalliseen että kansainväliseen kyberturvallisuusyhteistyöhön sekä huomattavat investoinnit kyberturvallisuusosaamiseen ja -teknologiaan tukevat maan kykyä puolustautua kyberuhkia vastaan ja varmistaa kriittisen infrastruktuurin suoja.

Kyberulottuvuudessa tapahtuva huoltovarmuuteen vaikuttaminen voi merkittävästi heikentää kokonaisturvallisuutta. Kyberhyökkäykset kohdistuvat yhä useammin kriittiseen infrastruktuuriin, mikä voi aiheuttaa laajoja häiriöitä ja vahingoittaa yhteiskunnan perusrakenteita. Tämä korostaa kyberhuoltovarmuuden strategista merkitystä. Kyberhuoltovarmuuden tavoitteena on minimoida kyberuhkien aiheuttamat riskit ja varmistaa kriittisten toimintojen jatkuvuus.

Huoltovarmuuden toiminnoissa ja toimijoilla voi olla monenlaisia kyberhaavoittuvuuksia, jotka johtuvat laajasta digitalisaation käytöstä ja riippuvuudesta digitaalisista järjestelmistä. Haavoittuvuudet voivat ilmetä sekä fyysisissä komponenteissa että tietojärjestelmissä. Erityisesti keskeiset ohjausjärjestelmät, kuten sähköverkot ja vesihuolto, ovat alttiita kyberhyökkäyksille, jotka

voivat aiheuttaa laajoja häiriöitä ja vakavia seurauksia yhteiskunnalle. Kyberhaavoittuvuuksien tunnistaminen, arviointi ja torjunta vaativat resursseja, jatkuvaa valppautta, teknologisia innovaatiota ja yhteistyötä kaikkien yhteiskunnallisten toimijoiden kesken.

Kyberhuoltovarmuus on olennainen osa kokonaisturvallisuutta ja se vaatii jatkuvia ponnistuksia ja investointeja kyberturvallisuuden kehittämiseen. Tämä kattaa paitsi teknologiset ratkaisut myös organisatoriset käytännöt ja inhimillisen tekijän huomioon ottamisen. Suomen proaktiivinen lähestymistapa ja sitoutuminen kyberhuoltovarmuuden parantamiseen tarjoavat vankan perustan, joka auttaa maata navigoimaan digitaalisen aikakauden monimutkaisessa ja jatkuvasti muuttuvassa turvallisuusympäristössä.

8 KYBERTURVALLISUUDEN MERKITYS KOKONAISTURVALLISUUDELLE

Tässä luvussa käsitellään yhtä merkittävää tutkimuksen alakysymystä: Kuinka kyberulottuvuudessa tapahtuva, huoltovarmuuteen vaikuttaminen heikentää kokonaisturvallisuutta?

Venäjän ja Kiinan kaltaiset valtiot harjoittavat laajamittaista tiedustelua ja vaikuttamista kyberavaruudessa, mikä nostaa kyberturvallisuuden tärkeäksi osaksi kansallista ja kansainvälistä turvallisuuspolitiikkaa. Valtiollisen tason kybervakoilu ja vaikuttamistoimet, erityisesti Suomen kriittistä infrastruktuuria kohtaan, ovat osoitus kyberturvallisuuden keskeisestä roolista kokonaisturvallisuuden ylläpidossa. Lisäksi, kun otetaan huomioon kyberavaruuden rajattomuus ja monimutkaiset toimintaympäristöt, ymmärrämme, että kyberturvallisuuden haasteet ovat globaaleja. Kybervakoilu ja -hyökkäykset eivät tunne valtioiden rajoja, mikä tekee kansainvälisestä yhteistyöstä ja tiedonvaihdosta olennaisia osia tehokkaan kyberturvallisuuden rakentamisessa. Kyberuhkien ennaltaehkäisy, havainnointi ja torjunta vaativat yhteistyötä niin kansallisten viranomaisten, yksityisen sektorin kuin kansainvälisten kumppaneidenkin kesken. Kyberturvallisuus on myös välttämätön osa yhteiskunnan resilienssin rakentamista, sillä se mahdollistaa häiriötilanteiden nopean hallinnan ja palautumisen. Erityisesti kriittisen infrastruktuurin osalta kyberturvallisuuden varmistaminen on avainasemassa huoltovarmuuden takaamisessa. Kyberturvallisuuden parantaminen ja kyberresilienssin kehittäminen ovat keskeisiä toimia kokonaisturvallisuuden vahvistamiseksi, mikä edellyttää jatkuvaa teknologian ja turvallisuusstrategioiden kehittämistä vastaamaan jatkuvasti muuttuvia kyberuhkia. (Suojelupoliisi, 2023a) (Suojelupoliisi, 2023b)

Koko yhteiskunnan toiminta on nykyään riippuvainen tietojärjestelmistä ja niitä yhdistävistä verkoista, ja kyberturvallisuus voidaan vaarantaa kybervaikuttamisella. Näin ollen yhteiskunnan kriittiset toiminnot ovat alttiita kyberhyökkäyksille ja niiden vaikutuksille. Kyberpuolustusta hankaloittaa merkittävästi hyökkääjän mahdollisuudet salata tai kiistää oma toiminta. (Turvallisuuskomitea, 2017a) Yhteiskunnan elintärkeät toiminnot ja kriittinen infrastruktuuri perustuvat entistä enemmän digitaalisiin ratkaisuihin, kuten

tietoverkkoihin, pilvipalveluihin ja erilaisten älyteknologian käyttöön. Vallitsevan kehityksen takia fyysisen ja virtuaalisen maailman rajat hämärtyvät. Jatkuva verkostoitumisen kasvu ja tietoverkoissa oleva ja liikkuva tieto avaa hyökkääjälle useita hyökkäysvektoreita. (Suojelupoliisi, 2022)

Kyberturvallisuus on noussut keskeiseksi osaksi kokonaisturvallisuutta teknologisen kehityksen ja digitalisoitumisen syvenemisen myötä, ja merkitys korostuu, kun digitaalisen toimintaympäristön haavoittuvuudet ja kyberuhkat kehittyvät nopeasti. Kyberturvallisuuden strateginen johtaminen on avainasemassa koko yhteiskunnan toimintavarmuuden ja turvallisuuden ylläpidossa. Kokonaisturvallisuuden kannalta kyberturvallisuus edellyttää tehokasta tiedonkeruuta, sekä tilannetietoisuuden ja poikkeusolojen hallintaa, joilla varmistetaan jatkuvuus ja resilienssi häiriötilanteissa. (Lehto ym., 2018) Kyberturvallisuuden merkitys kokonaisturvallisuudelle korostuu entisestään, kun huomioidaan eri toimijoiden ja toimintojen vuorovaikutus ja niiden väliset suhteet, ja toisiinsa kytkeytyvät uhkat. (Limnéll, 2009) Työ- ja elinkeinoministeriön raportin (Viljasta verkostoihin – Huoltovarmuuskeskuksen arviointi) mukaan digitaalista turvallisuutta on Suomessa kehitetty erityisesti kriittisen infrastruktuurin vaatimusten mukaan. Tämä on mahdollistanut valtiolähtöisen kyberturvallisuuden kehittämisen sijaan sen, että voimavaroja on voitu keskittää yritysten ja organisaatioiden kyberturvallisuutta parantaviin toimenpiteisiin. (Työ- ja elinkeinoministeriö, 2021)

Österlund kirjoittaa väitöskirjassaan (Österlund, 2019), että kyberturvallisuus on integraalinen osa nykyaikaisen yhteiskunnan kokonaisturvallisuutta. Digitaalisen ja kyberulottuvuuden kasvava merkitys yhteiskunnan perusrakenteille tarkoittaa, että kyberturvallisuuden haasteet ja ratkaisut ovat yhä enemmän sidoksissa fyysiseen turvallisuuteen ja yhteiskunnan laajempiin turvallisuusstrategioihin. Valtiollisten ja ei-valtiollisten toimijoiden kyky vaikuttaa kyberavaruuden kautta luo uudenlaisia uhkia, jotka vaativat uudenlaisia vastatoimia ja kansainvälistä yhteistyötä. Kyberturvallisuuden parantaminen ei ole pelkästään tekninen tai operatiivinen kysymys, vaan se vaatii laajaa poliittista, taloudellista ja yhteiskunnallista sitoutumista. (Österlund, 2019)

Tietoverkkojen turvallisuus ei ole ainoastaan tekninen kysymys, vaan se vaatii laajaa yhteistyötä eri toimijoiden, kuten hallitusten, yritysten ja kansalaisjärjestöjen, välillä. Yhteistyöllä voidaan kehittää ja toteuttaa kattavia turvallisuusstrategioita, jotka kattavat sekä ennaltaehkäisevät toimenpiteet että toimintasuunnitelmat mahdollisten tietoturvauhkien varalta. Tietoverkkojen keskeinen rooli kriittisessä infrastruktuurissa korostaa tarvetta jatkuvalle valppaudelle ja innovatiivisille ratkaisuille, jotka voivat parantaa verkkojen kestävyyttä ja turvallisuutta. Tämä sisältää sekä fyysisten että kyberuhkien torjumisen, mukaan lukien kehittyneet tietoturvaohjelmistot, salaustekniikat ja säännölliset turvallisuustarkastukset. Tietoverkkojen turvallisuus on olennainen osa kriittisen infrastruktuurin suojaamista. (Telenor, 2023a)

Kyberhuoltovarmuuden kehittäminen vaatii kokonaisvaltaista lähestymistapaa, jossa huomioidaan niin teknologian kehityksen tuomat mahdollisuudet kuin uudet haasteetkin. Digitalisaation syvällinen integroituminen yhteiskunnan

elintärkeisiin toimintoihin tekee kyberhuoltovarmuudesta entistä keskeisemmän tekijän kriittisen infrastruktuurin turvallisuuden ja toimintavarmuuden kannalta. (Savolainen, 2022)

Kokonaisturvallisuuden näkökulmasta kyberturvallisuus vaatii ennakoivaa ja adaptiivista lähestymistapaa. Häiriötilanteiden hallinta ja ennaltaehkäisy ovat avainasemassa, ja ne edellyttävät jatkuvaa tilannekuvan päivittämistä ja analysointia. Tämä mahdollistaa nopeat ja tehokkaat toimenpiteet mahdollisissa kyberhyökkäyksissä tai teknologisissa vioissa, jotka voivat vaikuttaa kriittisiin infrastruktuureihin tai kansalliseen turvallisuuteen. Kansallisen turvallisuuden näkökulmasta kyberturvallisuuden johtamismallit tulee suunnitella niin, että ne tukevat laajamittaista varautumista ja kykyä reagoida nopeasti muuttuviin uhkiin. Tämä sisältää kykyjä, jotka ulottuvat teknisestä asiantuntemuksesta strategiseen päätöksentekoon, mikä vaatii jatkuvaa koulutusta, resurssien joustavaa allokaatiota ja monialaista yhteistyötä. (Lehto ym., 2018)

8.1 Päätelmät, vastauksia tutkimuskysymyksiin ja yhteenveto

Tämän päivän maailmassa, jossa teknologia ja digitaaliset palvelut ovat integroituneet kaikkiin yhteiskunnan osa-alueisiin, kyberturvallisuuden merkitys ylittää perinteiset turvallisuuskäsitykset. Se kattaa laajan kirjon toimia, jotka varmistavat kansalaisten, yritysten, kriittisen infrastruktuurin ja valtion toimielinten suojan kyberuhkilta.

Kyberulottuvuudessa tapahtuvat valtiolliset tiedustelu- ja vaikuttamistoimet, erityisesti kriittistä infrastruktuuria vastaan, osoittavat kyberturvallisuuden merkityksen kansallisessa ja kansainvälisessä turvallisuuspolitiikassa. Kyberavaruuden rajattomuus ja monimutkaisuus tekevät kyberturvallisuuden haasteista globaaleja, korostaen kansainvälisen yhteistyön ja tiedonvaihdon tärkeyttä.

Kriittinen infrastruktuuri on ainakin jollakin tavalla yhteydessä tietoverkkoihin. Verkostoituminen parantaa käytettävyyttä ja voi helpottaa uhkien havainnointia ja vastatoimenpiteitä, mutta toisaalta se lisää myös hyökkäysvektoreita. Yhteiskunnan toiminta on yhä enemmän riippuvainen digitaalisista järjestelmistä, mikä tekee kriittiset toiminnot alttiiksi kyberhyökkäyksille. Tämä korostaa kyberturvallisuuden ja kyberresilienssin kehittämisen merkitystä huoltovarmuuden takaamiseksi. Kyberturvallisuuden kehittäminen vaatii laajaa yhteistyötä ja jatkuvaa teknologian sekä turvallisuusstrategioiden päivitystä, jotta voidaan vastata jatkuvasti muuttuviin kyberuhkiin ja vahvistaa kokonaisturvallisuutta.

Kyberhuoltovarmuuden merkitys kokonaisturvallisuudelle on olennainen, ja tämä luku on tuonut esille, kuinka kyberulottuvuudessa tapahtuva huoltovarmuuteen vaikuttaminen heikentää kokonaisturvallisuutta. Venäjän, Kiinan ja muiden valtioiden harjoittama laajamittainen kybertiedustelu ja vaikuttaminen, sekä digitalisaation syveneminen kaikilla yhteiskunnan toiminta-alueilla, korostavat kyberturvallisuuden kriittistä roolia kansallisessa ja kansainvälisessä turvallisuuspolitiikassa.

Kyberhuoltovarmuuden merkitys huoltovarmuudelle liittyy suoraan kykyyn suojata ja ylläpitää yhteiskunnan kriittisten toimintojen jatkuvuutta kyberuhkien keskellä. Kyberhuoltovarmuus on olennainen tekijä huoltovarmuuden kannalta, koska se varmistaa, että yhteiskunnan kriittiset järjestelmät ja infrastruktuurit voivat jatkaa toimintaansa häiriötilanteissa ja kyberuhkien alla. Valtiollisen tason kybervakoilu ja -vaikuttamistoimet, sekä kyberuhkien globaali luonne tekevät kansainvälisestä yhteistyöstä ja tiedonvaihdosta kriittisiä elementtejä tehokkaan kyberturvallisuuden rakentamisessa. Kyberresilienssin kehittäminen on avainasemassa huoltovarmuuden takaamisessa.

Kyberhuoltovarmuuden tilanne Suomessa on edistynyt, heijastuen maan aktiivisessa osallistumisessa kyberturvallisuuden kehittämiseen sekä kansallisella että kansainvälisellä tasolla. Suomi on tunnustanut kyberuhkien monimuotoisuuden ja laajentanut kyberturvallisuuden toimenpiteitä vastaamaan nykyisiä ja tulevia uhkia.

Kyberulottuvuudessa tapahtuvan huoltovarmuuteen vaikuttaminen heikentää kokonaisturvallisuutta, sillä kyberhyökkäykset voivat vaarantaa kriittisten infrastruktuurien toiminnan ja siten vaikuttaa yhteiskunnan kaikkiin toimintoihin. Hyökkääjät voivat käyttää kyberavaruutta vaikuttamistoimiin, jotka voivat ulottua tiedustelusta ja vaikuttamisesta aina kriittisen infrastruktuurin sabotointiin, mikä korostaa kyberturvallisuuden roolia kokonaisturvallisuuden ylläpidossa. Tämän vuoksi on tärkeää kehittää monitasoista suojaa ja resilienssiä kyberturvallisuudessa.

Kyberhaavoittuvuudet huoltovarmuuden toiminnoissa ja toimijoilla ovat monimuotoisia ja liittyvät digitalisaation tuomiin riskitekijöihin, kuten laajamittaiseen tietojen ja palveluiden siirtymiseen verkkoon. Tämä lisää riippuvuutta digitaalisista järjestelmistä ja verkko-olosuhteista, mikä puolestaan laajentaa mahdollisten hyökkäysvektorien kirjoa.

Yhteenvetona voidaan todeta, että kyberhuoltovarmuuden kehittäminen on kriittistä yhteiskunnan kokonaisturvallisuuden kannalta. Tämä edellyttää jatkuvaa teknologista innovointia, lainsäädännöllisiä toimenpiteitä, kansainvälistä yhteistyötä ja ennen kaikkea, yhteiskunnan eri toimijoiden välistä tiivistä yhteistyötä ja tiedonvaihtoa. Kyberturvallisuusstrategioiden ja niiden perusteella tehtävien toimien on oltava dynaamisia ja mukautuvia vastaamaan jatkuvasti kehittyvään uhkaympäristöön, jotta voidaan varmistaa yhteiskunnan huoltovarmuus ja kokonaisturvallisuus.

9 TULEVAISUUDEN HAASTEET JA KEHITYSSUUNNAT

9.1 Teknologian kehityksen vaikutukset kyberhuoltovarmuuteen

Teknologinen kehitys tarjoaa sekä mahdollisuuksia parantaa kyberturvallisuutta, että tuo esiin uusia uhkia ja haavoittuvuuksia. Teknologiset innovaatiot, kuten tekoäly, lohkoketjut ja IoT-laitteet (sekä kvanttilaskenta, kirjoittajan huomio), tarjoavat uusia keinoja kyberuhkien torjumiseen ja huoltovarmuuden parantamiseen, ne asettavat samalla yhteiskunnan uusien haasteiden eteen. (Turvallisuuskomitea, 2019) Digitalisaation ja kyberteknologioiden laajamittainen käyttöönotto on muuttanut yhteiskunnan perusrakenteita, mukaan lukien energianjakelu, liikenne ja vesihuolto, ja näiden kriittisten infrastruktuurien kyberresilienssi on muodostunut elintärkeäksi tekijäksi niiden toimintakyvyn ja yhteiskunnan turvallisuuden kannalta. Samaan aikaan, kun digitalisaatio tarjoaa tehokkuutta ja joustavuutta, se myös lisää riippuvuutta tietojärjestelmistä ja verkko-olosuhteista, mikä tuo mukanaan uudenlaisia haavoittuvuuksia ja altistaa infrastruktuurit mahdollisille kyberhyökkäyksille. (Valtioneuvosto, 2022b; Valtioneuvosto, 2021a)

Kybertiedustelun ja -puolustuksen kehittäminen on keskeistä kansallisen turvallisuuden varmistamiseksi, mikä edellyttää kattavaa lainsäädäntöä, tehokasta tiedonvaihtoa ja poikkihallinnollista yhteistyötä. Lisäksi yhteiskunnan turvallisuuden ja perus- ja ihmisoikeuksien turvaamiseksi on tärkeää, että tiedusteluviranomaisten toimintaa ohjataan ja valvotaan strategisesti, varmistaen samalla, että tiedustelutiedot saavuttavat oikea-aikaisesti tarvittavat viranomaiset ja valtionjohdon. Kyber- ja digitaalisen toimintaympäristön dynaamisuus asettaa vaatimuksia tiedustelun prosesseille ja järjestelmille. Jotta voidaan tuottaa merkityksellistä ja käyttökelpoista tiedustelutietoa, on tarpeellista kehittää tiedustelun tiedonhankintajärjestelmiä kaikissa toimintaympäristöissä, mukaan lukien kyber- ja avaruustoimintaympäristössä. Nopea teknologinen kehitys edellyttää merkittäviä investointeja tiedonhankintajärjestelmiin ja henkilöstön osaamisen kehittämiseen, jotta voidaan ylläpitää ja parantaa toimintakykyä muuttuvassa uhkaympäristössä. (Valtioneuvosto, 2021c; Valtioneuvosto, 2022a)

9.2 Uudet uhkakuvat ja niiden hallinta

Muuttunut turvallisuusympäristö vaikuttaa hallintoon, teollisuuteen ja koko yhteiskuntaan. Turvallisuus- ja tiedustelupalvelujen mukaan tele- ja IT-yrityksiin, niiden asiakkaisiin ja muihin yrityksiin kohdistuvat uhkat ovat seurausta etenkin Kiinan aktiivisesta toiminnasta ja Venäjän valmistautumisesta pysyvään erkaantumiseen lännestä. Norjalaisen, Suomessa tytäryhtiönsä DNA:n kautta toimivan,

tietoverkkopalveluja ja infraa tarjoavan Telenor:in mukaan kriittinen infrastruktuuri muuttuu yhä haavoittuvammaksi. Kriittisen infrastruktuurin turvallisuuden varmistaminen vaatii uusien teollisten kumppanuuksien perustamista ohjelmistojen ja ratkaisujen kehittämiseksi, jotka auttavat suojaamaan teollisia yrityksiä ja kriittistä infrastruktuuria. Kriittisen asiantuntemuksen ja kapasiteetin hyödyntäminen eri toimialojen välillä tarjoaa mahdollisuuksia innovaatioille ja arvonluonnille teollisessa kyberturvallisuudessa. (Telenor, 2023a)

Koska kyberturvallisuuden kenttä on jatkuvassa muutoksessa, ja uudet uhkakuvat vaativat jatkuvaa valppautta ja sopeutumiskykyä. Uusien uhkien, kuten edistyksellisten pysyvien uhkien ja haittaohjelmien, torjunta edellyttää kehittyneitä tietoturvaratkaisuja ja -strategioita. (Österlund, 2019)

Kybervakoilu nähdään jatkuvasti kasvavana uhkana, ja se voi kohdistua esimerkiksi kriittiseen infrastruktuuriin, valtion päätöksentekoon, puolustusliittoa koskeviin asioihin, erityisesti teknologia ja puolustusteollisuuden yrityksiin, sekä yliopistoihin ja tutkimuslaitoksiin. Vakoilulta puolustautumisessa on kokonaisturvallisuuden mallin mukaisesti yhteistyötä viranomaisten ja yritysten kesken, mutta myös kansainvälisten kumppaneiden tukea tarvitaan. (Limnéll, 2024)

9.3 Kyberhuoltovarmuuden kehittämisen strategia

Häiriötilanteiden hallinta kyberuhkien yhteydessä on keskeinen osa nykyaikaista yhteiskunnallista huoltovarmuutta. *Focus 2024* -dokumentin mukaan on elintärkeää, että yhteiskunnan kriittiset toiminnot säilyttävät operatiivisen kapasiteettinsa kyberhyökkäysten aikana, mikä vaatii huolellista suunnittelua ja ennakointia. (The Norwegian Intelligence Service, 2024)

Kyberturvallisuusstrategian (Turvallisuuskomitea, 2019) mukaan on erityisen tärkeää suojata yhteiskunnan elintärkeitä toimintoja kyberrikollisuuden, vakoilun ja valtiollisen tiedustelun kaltaisilta uhkilta. Strategia pyrkii käynnistämään kansallisen kyberturvallisuuden kehittämisohjelman, jossa korostetaan julkisen hallinnon ja elinkeinoelämän yhteistyötä kyberturvallisuuden parantamiseksi. Kehittämisohjelman valmistelua tukee uusi johtamisen koordinaatiomalli, jonka tavoitteena on parantaa kyberturvallisuuden tilannekuvaa ja integroida suunnittelu tiiviimmin muuhun yhteiskunnalliseen toimintaan, kuten talouden suunnitteluun.

9.4 Kyberoperaatioiden tilannekuva ja johtaminen

Alaluvussa 6.3 *Häiriötilanteiden hallinta huoltovarmuuden näkökulmasta* käsittelin kriittisen infrastruktuurin kyberresilenssiä. Norjan kansallinen tiedusteluviranomainen (NSM) näkee oman roolinsa vakavien kyberoperaatioiden koordinoinnissa ja hallinnassa keskeisenä. NSM:n vastuulla on muun muassa varmistaa, että kyberuhkiin reagoidaan nopeasti ja koordinoidusti koko valtionhallinnon ja

elinkeinoelämän toimijoiden kesken. Tämä sisältää jatkuvan uhkien seurannan, varoitusjärjestelmien ylläpidon ja reagointisuunnitelmien päivittämisen. (The Norwegian Intelligence Service, 2024).

Kyberoperaatioiden tehokas johtaminen ja tilannekuvan ylläpito ovat avainasemassa modernissa kyberpuolustuksessa. Tämä sisältää reaaliaikaisen tiedonkeruun, uhkien arvioinnin ja resurssien dynaamisen allokoinnin. Kyberoperaatioiden johtamisen kehittäminen vaatii sekä teknologisia että operatiivisia parannuksia, jotta voidaan varmistaa nopea ja koordinoitu vastaus kyberuhkiin. (Kukkola, Ristolainen ja Nikkarila, 2019)

Kyberturvallisuuden tehokas kehittäminen ja hallinta edellyttävät viranomaisten ja yritysjohdon vahvaa sitoutumista ja ohjausta, jolloin kyberturvallisuusstrategiat, tavoitteet ja vastuut asetetaan selkeästi. Tämä lähestymistapa varmistaa, että kyberturvallisuuden parantaminen on johdonmukaista ja perustuu riskianalyysiin, eikä se ole riippuvainen yksittäisten asiantuntijoiden erityisosaamisesta. Tällöin kyberturvallisuus muodostuu osaksi organisaatioiden ja yhteiskunnan kriittisten toimijoiden jokapäiväistä toimintaa ja vahvistaa yrityksen kykyä hallita häiriötilanteita sekä ylläpitää huoltovarmuutta. (Huoltovarmuusorganisaation digipooli, 2020)

9.5 Päätelmät, vastauksia tutkimuskysymyksiin ja yhteenveto

Tulevaisuuden haasteet ja kehityssuunnat kyberhuoltovarmuuden alalla korostavat jatkuvan valmiuden, innovoinnin ja kansainvälisen yhteistyön merkitystä yhteiskunnan perustoimintojen suojelemiseksi kasvavilta kyberuhkilta. Tämän luvun havaintojen perusteella voidaan tehdä useita kyberhuoltovarmuuden kehittämisen strategioihin, uusiin uhkakuviin ja niiden hallintaan sekä kyberoperaatioiden tilannekuvan ja johtamisen parantamiseen liittyviä löydöksiä.

Kyberhuoltovarmuuden merkitys huoltovarmuudelle korostuu entisestään, kun teknologinen kehitys avaa uusia mahdollisuuksia mutta tuo samalla esiin uusia haavoittuvuuksia. Kyberhuoltovarmuus muodostaa yhä tärkeämmän osan huoltovarmuutta, sillä se mahdollistaa kriittisten infrastruktuurien toiminnan jatkuvuuden kyberhyökkäysten ja häiriöiden aikana. Teknologisen kehityksen myötä kyberhuoltovarmuus edellyttää jatkuvaa valppautta ja sopeutumiskykyä uusiin uhkiin ja haavoittuvuuksiin, mikä puolestaan vahvistaa huoltovarmuuden perustaa.

Kyberhuoltovarmuuden tilanne Suomessa heijastaa maan aktiivista sitoutumista kyberuhkien torjuntaan ja kyberresilienssin vahvistamiseen. Suomi on investoinut merkittävästi kybertiedustelun ja -puolustuksen kehittämiseen, mikä varmistaa kansallisen turvallisuuden ja yhteiskunnan kriittisten toimintojen suojan.

Kyberulottuvuudessa tapahtuvan vaikuttamisen vaikutus huoltovarmuuteen ja kokonaisturvallisuuteen on moniulotteinen, sillä yhteiskunnan perustoiminnot ovat yhä riippuvaisempia digitaalisista järjestelmistä, mikä lisää haavoittuvuuksia. Uudet uhkakuvat, kuten valtiolliset toimijat ja järjestäytynyt

rikollisuus, käyttävät hyväkseen näitä haavoittuvuuksia, mikä voi heikentää kokonaisturvallisuutta merkittävästi. Kyberulottuvuudessa tapahtuva vaikuttaminen heikentää kokonaisturvallisuutta, koska se altistaa yhteiskunnan kriittiset infrastruktuurit ja toiminnot ulkoisille uhkille, kuten kybervakoilulle, -hyökkäyksille ja muille tietoturvahaavoittuvuuksille. Tämä korostaa kyberturvallisuuden merkitystä osana kokonaisturvallisuutta ja osoittaa, että kyberhuoltovarmuuden strateginen johtaminen on keskeistä toimintavarmuuden ja turvallisuuden ylläpidossa.

Kyberhaavoittuvuudet huoltovarmuuden toiminnoissa ja toimijoilla ovat moninaisia, ja niiden hallinta vaatii jatkuvaa teknologista kehittämistä, yhteistyötä sekä kyberturvallisuustietoisuuden lisäämistä kaikilla yhteiskunnan osa-alueilla. Tehokas kyberhuoltovarmuus rakentuu paitsi teknisten ratkaisujen myös kattavien organisatoristen käytäntöjen ja inhimillisen tekijän ymmärtämisen varaan.

Edellisten perusteella voidaan sanoa, että kyberhuoltovarmuuden kehittäminen edellyttää monitahoista lähestymistapaa, joka yhdistää teknologisen innovaation, lainsäädännön, kansainvälisen yhteistyön ja jatkuvan koulutuksen. Tulevaisuudessa kyberhuoltovarmuuden keskeinen tehtävä on säilyttää yhteiskunnan toimintakyky muuttuvassa ja yhä monimutkaisemmaksi käyvässä kyberuhkaympäristössä, mikä on olennaisen tärkeää kokonaisturvallisuuden kannalta.

10 YHTEENVETO JA JOHTOPÄÄTÖKSET

10.1 Tutkimuksen pääkohdat ja löydökset

Tutkimuksen keskeinen havainto on, että vaikka myös parannettavaa löytyy, on kyberturvallisuus integroitunut osa Suomen kansallista turvallisuutta ja yhteiskunnan resilienssiä. Tutkimus korostaa, kuinka teknologian ja verkostoituneen maailman kehitys on tehostanut tarvetta vahvistetulle kyberstrategialle, joka suojaa kriittistä infrastruktuuria ja edistää kansainvälistä yhteistyötä. Suomen rooli kansainvälisessä kyberturvallisuusyhteistyössä on tunnustettu, ja maa on aktiivinen osallistuja monissa kansainvälisissä foorumeissa. Tämä kansainvälinen yhteistyö on merkittävä osa Suomen strategiaa kyberuhkien torjunnassa. Myös Suomen Nato-jäsenyys on vahvistanut maan asemaa turvallisuuden tuottajana ja lisännyt sen roolia kansainvälisissä turvallisuusyhteyksissä.

Kokonaisturvallisuuden mallin uhkakuvat ovat yhdistelmä eri toimijoiden kohtaamista uhkista ja voidaan siis sanoa, että verkottuneessa yhteiskunnassa sen eri sektoreita vastaan suunnatut toimet ovat kerrannaisvaikutusten vuoksi jopa suurempia kuin yksittäisten uhkien summa. Myös muualle osoitettu hyökkäys voi laajentua alueelle, johon sitä ei oltu alun perin edes tarkoitettu. (Turvallisuuskomitea, 2017a) Sekä kybervaikuttamisen keinojen, että vaikutusten voidaan sanoa olevan yleisellä tasolla verrattavissa hybridivaikuttamiseen. Keinovalikoima on laaja, ja jopa yksittäisillä hyökkäyksillä tarkasti valittuun kohteeseen, kuten sähkönjakeluverkko, voidaan saada merkittävää vaikutusta aikaan.

Tutkimustyötä aloittaessani ensimmäinen suuri haasteeni oli selvittää mitä kyberhuoltovarmuudella tarkoitetaan. Tutkimuksen alussa myös yksi tutkimuskysymys oli *Mitä kyberhuoltovarmuudella tarkoitetaan?*. Vaikka kysymys vaivasi minua jatkuvasti, otin sen välillä pitkäksi aikaa pois tutkimuskysymysten listalta, sillä en tuntunut löytävän sille sopivaa määritelmää. Tässä raportissa kysymys on taas mukana, ja tutkimukseni, sekä sen löydösten perusteella määrittelen kyberhuoltovarmuuden näin:

- **Kyberhuoltovarmuus** tarkoittaa yhteiskunnan kriittisen infrastruktuurin ja toimintojen turvallisuuden ja toimintakyvyn ylläpitoa kyberuhkat huomioiden. Kyberhuoltovarmuus kattaa ennakoinnin, havainnoinnin, tehokkaan torjunnan, vastatoimet ja nopean palautumisen kyberuhkista, varmistaen, että yhteiskunnan kriittiset toiminnot voivat jatkua häiriötilanteissa. Kyky torjua, havaita ja toipua kyberhyökkäyksistä on keskeinen osa kyberhuoltovarmuutta, joka sisältää valmiudet minimoida kyberhyökkäysten aiheuttamat vahingot ja ylläpitää yhteiskunnan perustoimintoja häiriöttöminä kaikissa olosuhteissa.

10.2 Johtopäätökset

Tämän tutkimuksen aikana on käynyt selväksi, että kyberhuoltovarmuus on kriittinen elementti nykyaikaisen yhteiskunnan kokonaisturvallisuudessa ja, että maan kyberturvallisuusstrategiat ja kansainvälinen osallistuminen ovat ratkaisevia tekijöitä kansallisen ja globaalin turvallisuuden edistämisessä. Suomen kyberturvallisuuden vahvuus perustuu jatkuvaan sitoutumiseen strategioiden päivittämiseen, riskienhallintaan ja kansainväliseen yhteistyöhön, mikä mahdollistaa nopeat ja koordinoidut toimet kyberuhkien ilmetessä. Digitaalisen ja verkottuneen toimintaympäristön monimutkaisuus sekä kriittisen infrastruktuurin suojelun haasteet vaativat kestäviä turvallisuusstrategioita, jotka ovat mukautuvia ja vastaavat jatkuvasti muuttuvaan uhkakenttään.

Kovasen (Kovanen, 2021) mukaan kyberuhkien monimutkaisuuden ja skenaarioanalyysin ymmärtäminen on olennaisen tärkeää rakennettaessa turvallisuusstrategioita, jotka ottavat huomioon digitaalisen ja verkottuneen toimintaympäristön haasteet. Tämä korostaa tarvetta syvälliselle ymmärrykselle siitä, kuinka kriittisen infrastruktuurin eri osat ovat toisiinsa kytkeytyneitä ja kuinka haavoittuvuuksia voidaan minimoida. Telenor (Telenor, 2023a) viittaa siihen, kuinka nykyajan yhteiskunta muodostuu verkottuneista systeemeistä, joissa yksittäisiin kohteisiin kohdistuvilla hyökkäyksillä voi olla kauaskantoisia seurauksia.

Kyberhuoltovarmuuden ymmärtäminen edellyttää myös tietoa eri valtioiden strategisista kulttuureista, kansallisista intresseistä ja kansainvälisen yhteisön dynamiikasta. Martti J Kari (Kari, 2019) korostaa kyberturvallisuuden monimutkaisen luonteen ja teknologisten sekä geopoliittisten tekijöiden kytkeytymisen tarvetta monitieteelliseen lähestymistapaan ja kansainväliseen yhteistyöhön.

Häiriötilanteiden hallinta kyberuhkien yhteydessä vaatii monitahoista lähestymistapaa, jossa teknologian, organisatorisen valmiuden ja kansainvälisen yhteistyön elementit yhdistyvät (The Norwegian Intelligence Service, 2024). Tämä monikerroksinen lähestymistapa varmistaa, että yhteiskunnan kriittiset toiminnot voivat jatkaa häiriöttä myös poikkeusoloissa, mikä on välttämätöntä kansalaisten hyvinvoinnin ja yhteiskunnan kokonaisvaltaisen huoltovarmuuden turvaamiseksi.

Teknologian nopea kehitys asettaa turvallisuusstrategioille vaatimuksen jatkuvasta valppaudesta ja mukautumiskyvystä. Uudet teknologiat tuovat mukanaan sekä uusia mahdollisuuksia kyberuhkien torjuntaan että uusia haasteita ja haavoittuvuuksia, joita ei aiemmin ole ollut olemassa.

Tutkimuksen perusteella voidaan todeta, että kyberhuoltovarmuuden kehittämisen ja ylläpidon on oltava jatkuvaa, kattavaa ja monitieteellistä. Turvallisuusstrategioiden on oltava eläviä dokumentteja, jotka päivittyvät vastaamaan teknologian kehitystä ja muuttuvaa geopoliittista tilannetta. Kansainvälinen yhteistyö ja tiedonvaihto ovat avainasemassa rakennettaessa globaalia kyberturvallisuusarkkitehtuuria, joka suojaa niin yksittäisiä valtioita kuin koko kansainvälistä yhteisöä kyberuhkilta.

Kyberuhkien monimutkaisuuden ja kriittisen infrastruktuurin suojelun ymmärtäminen on keskeistä rakennettaessa kestäviä turvallisuusstrategioita, jotka huomioivat nykyaikaisen digitaalisen ja verkottuneen toimintaympäristön haasteet. (Kovanen, 2021) Moderni yhteiskunta on digitaalinen ja verkottunut systeemien systeemi, jossa kriittisen infrastruktuurin muodostama kokonaisuus voi olla haavoittuva monella tavalla. Yksittäiseen kohteeseen vaikuttamisella voi olla seurannaisvaikutuksia myös muihin kohteisiin, ja etenkin tietoverkkojen haavoittuvuus on saatava mahdollisimman pieneksi. (Telenor, 2023a)

Kyberhuoltovarmuuden ymmärtäminen edellyttää syvällistä tietämystä eri valtioiden strategisista kulttuureista, kansallisista intresseistä ja kansainvälisen yhteisön dynamiikasta. Kyberturvallisuuden monimutkainen luonne, joka kytkeytyy sekä teknologisiin että geopoliittisiin tekijöihin, korostaa tarvetta monitieteelliselle lähestymistavalle ja kansainväliselle yhteistyölle. (Kari, 2019)

Häiriötilanteiden hallinta kyberuhkien yhteydessä vaatii monitahoista lähestymistapaa, jossa teknologiset ratkaisut, organisatorinen valmius ja kansainvälinen yhteistyö yhdistyvät saumattomasti. Näin voidaan varmistaa, että yhteiskunnan kriittiset toiminnot voivat jatkaa häiriöttä myös poikkeusoloissa, turvaten näin kansalaisten hyvinvoinnin ja yhteiskunnan kokonaisvaltaisen huoltovarmuuden. (The Norwegian Intelligence Service, 2024)

Teknologian nopea kehitys vaatii jatkuvaa valppautta ja mukautumiskykyä turvallisuusstrategioissa, sillä uudet teknologiat voivat myös avata ovia uudenlaisille hyökkäyksille ja haavoittuvuuksille.

10.3 Kyberhuoltovarmuuden kehittämisen suositukset

Tämän tutkielman analyysi osoittaa, että kyberhuoltovarmuuden parantamiseen tarvitaan kattavia toimia, jotka kohdistuvat strategioiden kehittämiseen, toimeenpanon seurantaan, yhteistyöhön, tiedonjakoon, koulutukseen sekä lainsäädännön uudistamiseen. Tässä luvussa esitetään keskeiset suositukset kyberhuoltovarmuuden kehittämiseksi:

1. **Strategioiden jalkauttaminen ja seuranta:** Vaikka strategioita on laadittu, niiden toimeenpanon seuranta jää usein puutteelliseksi. On olennaisen

tärkeää varmistaa, että strategiat toteutetaan täysimääräisesti ja että niiden toimeenpanoa seurataan jatkuvasti. Tämä edellyttää selkeitä toimeenpanon indikaattoreita ja säännöllistä arviointia.

2. **Strategioiden joustavuus:** Kyberturvallisuuden nopean kehityksen vuoksi on välttämätöntä, että strategiat ovat joustavia ja mahdollistavat nopean reagoinnin toimintaympäristön muutoksiin. Strategioiden tulisi olla dynaamisia ja sallia jatkuva päivitys teknologisen ja operatiivisen kehityksen myötä.

3. **Kyberuhkien jatkuva päivitys:** On kriittistä, että kyberuhkia koskevat skenaariot päivitetään jatkuvasti uuden tiedon valossa. Tämä edellyttää jatkuvaa uhkakuvien seurantaa ja analyysia, jotta voidaan varmistaa yhteiskunnan kybersietoisuuden riittävä taso.

4. **Laaja yhteistyö ja tiedonjako:** Kriittisten infrastruktuurien, kuten viestiverkkojen ja energiaverkkojen, kyberturvallisuus edellyttää laajaa yhteistyötä ja avointa tiedonjakoa eri toimijoiden välillä. Tämä tarkoittaa paitsi kansallista yhteistyötä myös kansainvälistä koordinaatiota.

5. **Kyberpuolustuksen keskitetty johtaminen:** Tehokkaan kyberpuolustuksen johtamisen ja toimeenpanon seurannan varmistamiseksi vastuu on keskitettävä yhdelle valtiolliselle organisaatiolle, jolla on tarvittavat toimivaltuudet ja resurssit.

6. **Henkilöstön koulutus:** Kyberhuoltovarmuuden parantaminen edellyttää jatkuvaa henkilöstön koulutusta kyberuhkien tunnistamisessa ja niihin reagoimisessa. Tämä koulutus tulee kohdentaa kaikille tasoille organisaatiossa.

7. **Kansainvälinen yhteistyö:** NATO, EU ja kahden- tai kolmenväliset sopimukset tarjoavat mahdollisuuksia tehostaa kyberturvallisuutta kansainvälisen yhteistyön kautta. On tärkeää hyödyntää näitä alustoja tiedonvaihtoon ja yhteisten turvallisuusstandardien kehittämiseen.

8. **Lainsäädännön uudistaminen:** Nykyisen lainsäädännön, joka saattaa vaatia televerkkojen hallinnan kansallistamista tai palvelimien fyysisen sijainnin tietyssä maassa, tulisi kehittyä vastaamaan nykyajan kyberturvallisuuden tarpeita. Lainsäädännön tulisi tukea kahdennettuja palvelimia turvallisissa maissa ja mahdollistaa joustavuus verkkojen hallinnassa.

Strategiat ovat keskeinen osa kyberhuoltovarmuuden varmistamista, mutta niiden toimeenpano ja jatkuvuuden seuranta jäävät usein puutteellisiksi. Nopeasti muuttuvassa digitaalisessa ympäristössä, jossa kyberuhkat ja puolustuskeinot kehittyvät jatkuvasti, perinteiset pitkän aikavälin strategiasuunnitelmat eivät ole

riittäviä. Tehokkaampi tapa varmistaa joustavuus on soveltaa puolustusvoimien kehitysohjelmien kaltaisia aikajaksoja, jotka mahdollistavat nopeat reagoinnit muutoksiin.

Kyberuhkien jatkuva päivitys ja skenaarioiden ajantasaisuus ovat avainasemassa kyberturvallisuuden ylläpitämisessä. Kriittisten infrastruktuurien, kuten viestintäverkkojen, energiaverkkojen ja sairaanhoidon turvallisuus vaatii laajaa yhteistyötä ja tiedonjakoa eri toimijoiden kesken. Yhteistyö auttaa luomaan kattavan kyberpuolustuksen tilannekuvan ja mahdollistaa tehokkaan johtamisen ja seurannan.

Vastuun keskittäminen yhdelle valtiolliselle organisaatiolle, jolla on riittävät toimivaltuudet, parantaisi kyberpuolustuksen johtamista ja operointia. Lisäksi henkilöstön jatkuva koulutus kyberuhkien tunnistamiseen ja niiden torjuntaan on kriittinen elementti kyberhuoltovarmuuden vahvistamisessa.

Kansainvälinen yhteistyö, mukaan lukien NATO:n ja EU:n roolit sekä kahden- tai kolmenväliset puolustussopimukset, on tärkeää kyberturvallisuuden tehostamisessa. Lainsäädännön kehittäminen on myös keskeistä; esimerkiksi televerkkojen hallinnan kansallistaminen ja palvelimien fyysinen sijoittaminen kohdemaahan ovat vanhentuneita käytäntöjä. Palvelinten ja tarvittaessa myös muun infran kahdentaminen toiseen maahan parantaisi kyberresilienssiä.

10.4 Jatkotutkimusaiheet ja -tarpeet

Tämän tutkimuksen *Kyberhuoltovarmuus kokonaisturvallisuuden näkökulmasta* tulokset tarjoavat perustan laajemmalle keskustelulle kyberhuoltovarmuuden ja kokonaisturvallisuuden välisestä suhteesta. Vaikka tutkimus on valottanut kyberhuoltovarmuuden keskeisiä osa-alueita, se on myös nostanut esiin useita kysymyksiä ja aiheita, jotka vaativat lisätutkimusta. Tässä luvussa esitellään ehdotuksia jatkotutkimusaiheiksi ja -tarpeiksi kyberhuoltovarmuuden ja kokonaisturvallisuuden kontekstissa.

1. **Teknologisen kehityksen ja kyberuhkien dynamiikka**: Jatkotutkimuksissa tulisi tarkastella syvällisemmin, miten teknologinen kehitys, kuten tekoälyn ja kvanttitietokoneiden nousu, muokkaa kyberuhkien kenttää. Tutkimus voisi keskittyä siihen, miten nämä teknologiat vaikuttavat kyberhuoltovarmuuden strategioihin ja käytäntöihin.

2. **Kyberresilienssin rakenteelliset tekijät**: Tarvitaan lisää tutkimusta siitä, miten erilaiset organisaatiot ja yhteiskunnan sektorit rakentavat kyberresilienssiä. Tutkimuksen kohteena voisi olla erityisesti se, miten resilienssiä voidaan vahvistaa organisaatioiden ja toimialojen välisen yhteistyön kautta.

3. **Kansainvälinen kyberdiplomatia ja -sääntely**: On tarpeen tutkia, miten kansainvälinen yhteisö voisi kehittää yhteisiä normeja, sääntöjä ja

yhteistyömekanismeja kyberuhkien hallintaan. Tutkimus voisi keskittyä erityisesti siihen, miten valtioiden välinen yhteistyö ja diplomatia voivat edistää globaalia kyberturvallisuutta.

4. **Kyberhybridivaikuttamisen moniulotteisuus**: Jatkotutkimuksissa tulisi syventää ymmärrystä siitä, miten kyberavaruutta käytetään osana laajempia hybridivaikuttamisen kampanjoita. Erityisesti olisi tärkeää tutkia, miten kyberoperaatiot kytkeytyvät muihin vaikuttamisen muotoihin ja miten näitä hybridiuhkia voidaan torjua tehokkaasti.

5. **Kyberharjoitusten ja -koulutuksen kehittäminen**: On tarpeen tutkia, miten kyberharjoitukset ja -koulutusohjelmat voivat parantaa yksilöiden, organisaatioiden ja yhteiskunnan valmiuksia vastata kyberuhkiin. Tutkimus voisi keskittyä siihen, miten simulaatioita ja harjoituksia voidaan hyödyntää kyberresilienssin rakentamisessa.

6. **Kansallisen kyberturvallisuuspolitiikan vertaileva analyysi**: Kansainväliset vertailututkimukset, jotka tarkastelevat eri maiden kyberturvallisuuspolitiikkoja ja -toimenpiteitä, voivat tarjota arvokkaita oivalluksia parhaiden käytäntöjen jakamiseen ja kansainvälisen yhteistyön kehittämiseen.

7. **Kansalaisten kyberturvallisuustietoisuuden kehittäminen**: Tutkimuksen kohteena voisi olla se, miten kansalaisia voidaan tehokkaasti kouluttaa tunnistamaan kyberuhkia ja suojaamaan itseään verkossa. Tämä voisi sisältää tarkastelua erilaisista valistuskampanjoista, koulutusohjelmista ja digitaalisen lukutaidon kehittämisestä.

8. **Kansallinen kyberturvallisuuden johtamisen malli**: Tutkimuksen tavoitteena olisi kehittää kansallinen kyberturvallisuuden johtamisen malli, joka on yhteensopiva kansainvälisten standardien ja käytäntöjen kanssa. Tutkimuksessa voisi keskittyä erityisesti siihen, miten eri toimijat, mukaan lukien hallitus, eri viranomaiset ja yksityinen sektori, voivat tehdä yhteistyötä kyberturvallisuuden parantamiseksi. Tutkimus pyrkii myös tunnistamaan parhaita käytäntöjä, vastuunjakoa ja toimintamalleja, jotka tukevat tehokasta ja joustavaa reagointia kyberuhkiin sekä ylläpitävät kansallista ja kansainvälistä kyberturvallisuuden tilannetietoisuutta.

LÄHTEET

Cybersecurity & Infrastructure Security Agency. (2024). *PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS*.

DNA Oy. (2024, maaliskuuta 15). *Tutkimus: Suomalaisyrityksillä petrattavaa kyberuhkiin varautumisessa*. https://www.sttinfo.fi/tiedote/70120504/tutkimus-suomalais-yrityksilla-petrattavaa-kyberuhkiin-varautumisessa?publisherId=1881 & lang=fi.

Euroopan komissio. (2017). *Pohdinta-asiakirja Euroopan puolustuksen tulevaisuudesta*. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CE-LEX:52017DC0315&from=FI

FiCom. (2023). *FiComin nakemyksiä pääministeri Orpon hallitusohjelman kyberpolitiikkaan*.

Harjanne, A., Muilu, E., Pääkkönen, J., & Smith, H. (2018). *Helsinki yhdistelmäuhkien aikakaudella-Yhdistelmävaikuttaminen ja kaupunki*.

Henttonen, U. (2021, toukokuuta 10). *Ikuisesti idän ja lännen välissä? Miltä Suomi näyttää Washingtonista käsin ja mitä suurvallat voivat oppia pienemmiltään*. The Ulkopolitist. https://ulkopolitist.fi/2021/05/10/ikuisesti-idan-ja-lannen-valissa-milta-suomi-nayttaa-washingtonista-kasin-ja-mita-suurvallat-voivat-oppia-pienemmiltaan/

Hirsjärvi, S., Remes, P., & Sajavaara, P. (1997). *Tutki ja kirjoita*. Kirjayhtymä Oy.

Holmgren, M. (2022). *Digital resilience beyond data localisation: National approaches to global challenges*.

Huoltovarmuuskeskus. (ei pvm.). *Tietoa huoltovarmuudesta*. Noudettu 28. huhtikuuta 2022, osoitteesta https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta

Huoltovarmuusorganisaation digipooli. (2020). *Kyberturvallisuuden nykytila eri toimialoilla—Kartoituksen keskeiset havainnot*.

Hybrid CoE. (2021). *The Landscape of Hybrid Threats: A Conceptual Model—Public Version*. https://doi.org/10.2760/44985

Hhybridi—Kielitoimiston sanakirja. (2022, huhtikuuta 28). https://www.kielitoimiston-sanakirja.fi/#/hybridi

Hybridivaikuttaminen | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma). (2022, huhtikuuta 28). https://termipankki.fi/tepa/fi/haku/hybridivaikuttaminen

Juhila, K. (2021). *Laadullinen tutkimus ja teoria*. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja.

Kananen, J. (2014). *Laadullinen tutkimus opinnäytetyönä*. Suomen Yliopistopaino Oy – Juvenes Print.

Kanniainen, V. (2018). *Essays in national defence*. *28*. https://urn.fi/URN:ISBN:978-951-25-3027-4

Kari, M. J. (2019). *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture—A tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats*. http://urn.fi/URN:ISBN:978-951-39-7837-2

Kovanen, T. (2021). *Cyber-Threat Aspects in a Complex System-of-Systems Environment A Case Study in Remote Pilotage*. http://urn.fi/URN:ISBN:978-951-39-8771-8

Kukkola, J. (2020). *Digital Soviet Union—The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas* [Maanpuolustuskorkeakoulu]. https://urn.fi/URN:ISBN:978-951-25-3132-5

Kukkola, J., Ristolainen, M., & Nikkarila, J.-P. (2019). *Game Player—Facing the structural transformation of cyberspace*. Puolustusvoimien tutkimuslaitos.

Laajava, M. (2023, syyskuuta 16). *Nato-jäsenenä Suomi on turvallisuuden tuottaja, aktiivinen ja luotettava toimija*. Kouvolan turvallisuus. https://www.kouvolanturvallisuus.fi/ajankohtaiset/nato-jasenena-suomi-on-turvallisuuden-tuottaja-aktiivinen-ja-luotettava-toimija/

Lehto, M., & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. Teoksessa P. Neittaanmäki (Toim.), *Informaatioteknologian tiedekunnan julkaisuja* (Vsk. 20).

Lehto, M., & Limnéll, J. (2017). Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede ja ase*, *75*. https://journal.fi/ta/article/view/67730

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi_. Teoksessa *Valtioneuvoston selvitysja tutkimustoiminnan julkaisusarja 30/2017*. Valtioneuvoston kanslia. https://tietokayttoon.fi/julkaisu?pubid=17805

Lehto, M., Limnéll, J., Kokkomäki, T., & Salminen, M. (2018). *Kyberturvallisuuden strateginen johtaminen Suomessa*.

Liikenne- ja viestintäministeriö. (2021). *Kyberturvallisuuden kehittämisohjelma*. http://urn.fi/URN:ISBN:978-952-243-599-6

Limnéll, J. (2009). *Suomen uhkakuvapolitiikka 2000-luvun alussa* [Maanpuolustuskorkeakoulu]. https://urn.fi/URN:USBN:978-951-25-2037-4

Limnéll, J. (2024, maaliskuuta 1). Kybervakoilu on kasvava uhka Suomelle. *Turvallisuus & riskienhallinta*, *1/2024*.

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu. Teoksessa *JYU dissertations*. http://urn.fi/URN:ISBN:978-951-39-8258-4

Rantapelkonen, J., & Salminen, M. (2013). *The Fog of Cyber Defence*. National Defence University.

Savolainen, A. (2022). Kompleksisuuskuilu toimitusketjujen hallinnan haasteena kybertoimintaympäristössä. Teoksessa M. Palokangas (Toim.), *Sodan usvaa*. Maanpuolustuskorkeakoulu, Sotataidon laitos. https://urn.fi/URN:ISBN:978-951-25-3286-5

SektorCERT. (2023). *Attack against Danish Critical infrastructure*. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Sisäministeriö. (2017). *Hyvä elämä -Turvallinen arki*. Sisäministeriö. http://urn.fi/URN:ISBN:978-952-324-138-1

Suojelupoliisi. (2022). *Supo Vuosikirja 2021*.

Suojelupoliisi. (2023a). *Kansallisen turvallisuuden katsaus 2022*.

Suojelupoliisi. (2023b). *Supo Vuosikirja 2022*.

Telenor. (2023a). *Digital Security 2023—It gets serious*. https://www.etterretningstjenesten.no/publikasjoner/focus/contents/Russia

Telenor. (2023b). *Security that goes beyond technology to empower societies*.

The Norwegian Intelligence Service. (2024). *Focus2024—The Norwegian Intelligence Service's assessment of current security challenges.pdf*. https://www.etterretningstjenesten.no/publikasjoner/focus

Tuohinen, P. (2024, maaliskuuta 8). ”Valtava turvallisuusriski” – Suunnitelma keskittää kaikki kriittiset infratiedot yhteen paikkaan kerää kritiikkiä. *Helsingin sanomat*.

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi: Vsk. uudistettu laitos*. Tammi.

Turvallisuus- ja puolustusasian komitea. (2013). *Suomen kyberturvallisuusstrategia 2013*.

Turvallisuuskomitea. (2017a). *Turvallinen Suomi 2018 – Tietoja Suomen kokonaisturvallisuudesta*. Turvallisuuskomitea. https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/

Turvallisuuskomitea. (2017b). *Yhteiskunnan turvallisuusstrategia*. www.turvallisuuskomitea.fi

Turvallisuuskomitea. (2018). *Kyberturvallisuuden sanasto*.

Turvallisuuskomitea. (2019). *Suomen kyberturvallisuusstrategia 2019*. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Työ- ja elinkeinoministeriö. (2021). *Viljasta verkostoihin, Huoltovarmuuskeskuksen arviointi*. http://urn.fi/URN:ISBN:978-952-327-733-5

Ulkoministeriö. (2021). *Suomen valtionhallinnon Kiina-toimintaohjelma*. https://um.fi/julkaisut/-/asset_publisher/TVOLgBmLyZvu/content/valtionhallinnon-kiina-toimintaohjelma

Uusipaavalniemi, S., & Puistola, J.-A. (2016). Hybridiuhat ja yhteiskunnan varautuminen. Teoksessa *Puolustusvoimien tutkimuslaitos Tutkimuskatsaus 04 – 2016* (Vsk. 2016).

Valtioneuvosto. (2017). *Valtioneuvoston puolustusselonteko 2017*. http://urn.fi/URN:ISBN:978-952-287-370-5

Valtioneuvosto. (2020). *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko*. valtioneuvosto. http://urn.fi/URN:ISBN:978-952-287-876-2

Valtioneuvosto. (2021a). *Valtioneuvoston puolustusselonteko 2021*. http://urn.fi/URN:ISBN:978-952-383-820-8

Valtioneuvosto. (2021b). *Valtioneuvoston selonteko sisäisestä turvallisuudesta—Valto*. http://urn.fi/URN:ISBN:978-952-383-769-0

Valtioneuvosto. (2021c). *Valtioneuvoston selonteko tiedustelulainsäädännöstä*. https://urn.fi/URN:ISBN:978-952-383-500-9

Valtioneuvosto. (2022a). *Ajankohtaisselonteko turvallisuusympäristön muutoksesta*. https://urn.fi/URN:ISBN:978-952-383-772-0

Valtioneuvosto. (2022b). *Valtioneuvoston huoltovarmuusselonteko*. Valtioneuvosto. http://urn.fi/URN:ISBN:978-952-383-803-1

Valtioneuvosto. (2023). *Pääministeri Petteri Orpon hallituksen ohjelma 2023*.

Yleisradio. (2023, heinäkuuta 29). *Yhdysvaltojen hallinto etsii kiinalaishakkereiden ”tikittävää aikapommia” järjestelmistään – haittaohjelmalla aiheuttaa laajaa häiriötä*. https://yle.fi/a/74-20043066

Österlund, B. (2019). *Suomen meriliikenteen huoltovarmuudelle asetetut tavoitteet ja niiden toteutuminen* [Maanpuolustuskorkeakoulu]. https://urn.fi/URN:ISBN:978-951-25-3058-8