Anni Klemetti

TIETOTURVAN JOHTAMINEN KRIISITILANTEISSA POHJOISMAISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Klemetti, Anni
Tietoturvan johtaminen kriisitilanteissa pohjoismaissa
Jyväskylä: Jyväskylän yliopisto, 2024, 49 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

2020-luvulla tietoturvaa uhkaavat kriisit ovat lisääntyneet huomattavasti, mikä tekee aiheesta hyvin ajankohtaisen ja tärkeän. Tämä tutkimus tarkastelee eri tietoturvauhkia, joita valtiot, erityisesti pohjoismaat Ruotsi, Norja, Tanska, Islanti sekä päätarkastelukohteena Suomi, ovat kohdanneet kyseisenä aikana. Tutkimuksessa käsitellään, miten näihin uhkiin ja kriiseihin valmistaudutaan ja vastataan niin valtioiden sisällä, kuin kansainvälisen yhteistyön kautta. Tarkastelun kohteena ovat vuoden 2020 aikana ja jälkeen alkaneet kriisit, kuten COVID-19 pandemia ja Ukrainan sota. Tutkimus korostaa kehittyvän teknologian roolia kriisitilanteissa sekä teknologian tuomia haasteita ja mahdollisuuksia tietoturvan johtamisessa ja kriisitilanteista selviytymisessä. Tulokset osoittavat, että pohjoismaat ovat korostaneet erityisesti kansainvälisen yhteistyön merkitystä, teknologian hyödyntämistä sekä jatkuvaa kehittämistä. On tärkeää ymmärtää teknologian monimutkaiset haasteet, jotta voidaan luoda vahvoja strategioita, jotka suojelevat sekä kansallista turvallisuutta että yksittäisten kansalaisten turvallisuutta. Tämä tutkimus toteutettiin kirjallisuuskatsauksena. Kirjallisuus kerättiin vertaisarvioiduista tutkimusartikkeleista, aikakauslehdistä ja muusta kirjallisuudesta. Tutkimus auttaa ymmärtämään, minkälaisia tietoturva- ja kyberuhkia erilaiset kriisitilanteet voivat aiheuttaa ja miten ne vaikuttavat edelleen valtioihin ja kansalliseen turvallisuuteen. Tietoturvauhat voivat vaikuttaa valtioihin monilla eri tavoilla ja tässä tutkimuksessa ehdotetaankin myös toimenpiteitä paremman tietoturvan saavuttamiseksi tulevaisuudessa.

Asiasanat: tietoturva, kyberturvallisuus, kriisinhallinta, kansallinen turvallisuus, tietoturvajohtaminen.

ABSTRACT

Klemetti, Anni
Information security management in crisis situations in the Nordic countries
Jyväskylä: University of Jyväskylä, 2024, 49 p.
Information systems, bachelor's thesis
Supervisor: Clements, Kati

In the 2020s, cybersecurity threats have significantly increased, making the topic very relevant and important. This study examines various cybersecurity threats faced by states, particularly the Nordic countries, Sweden, Norway, Denmark, Iceland, and primarily Finland, during this period. The study explores how these threats and crises are prepared for and responded to both within states and through international cooperation. The focus is on crises that began or had an impact during and after 2020, such as the COVID-19 pandemic and the war in Ukraine. The study emphasizes the role of emerging technologies in crisis situations, as well as the challenges and opportunities they present for information security management and crisis response. The results show that the Nordic countries have emphasized the importance of cooperation, technology, and continuous development of international cooperation in particular. It is crucial to understand the complex challenges posed by technology to develop strong strategies that protect both national security and individual citizens' safety. This study was conducted as a literature review. Literature was collected from peer-reviewed research articles, journals, and other sources. The research helps understand the types of cybersecurity threats that various crisis situations can cause and how they continue to affect states and national security. Cybersecurity threats can impact states in various ways which is why this study also proposes measures to achieve better cybersecurity in the future.

Keywords: information security, cybersecurity, crisis management, national security, information security management.

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

2020-luvulla tietoturvaa uhkaavat kriisit ovat lisääntyneet huomattavasti (Chigada ja Madzinga, 2021), mikä tekee aiheesta hyvin ajankohtaisen ja tärkeän. Tutkielman tarkoituksena on avata eri tietoturvauhkia, joita valtiot, erityisesti pohjoismaat Ruotsi, Norja, Tanska, Islanti sekä päätarkastelukohteena Suomi, ovat kohdanneet kyseisenä aikana sekä, miten näihin uhkiin ja kriiseihin valmistaudutaan sekä vastataan niin valtioiden sisällä, kuin kansainvälisen yhteistyön kautta. Tarkastelukohteena on tarkemmin vuoden 2020 aikana ja jälkeen alkaneet sekä vaikuttaneet kriisit, COVID-19 pandemia sekä Ukrainan sota, jotka ovat tuoneet esiin uusia ja monimutkaisia tietoturvauhkia, jotka ovat vaikuttaneet valtioiden, yritysten ja yksilöiden turvallisuuteen (Chigada & Madzinga, 2021; Willett, 2022.) Tutkimalla, miten Pohjoismaat ovat vastanneet näihin uhkiin, voimme oppia tehokkaista strategioista ja toimintamalleista, jotka parantavat tietoturvaa ja kriisinhallintaa. Tämä tieto voi auttaa muita valtioita ja organisaatioita valmistautumaan ja reagoimaan vastaaviin uhkiin tulevaisuudessa.

Tutkielmassa tulee esille kehittyvän teknologian rooli tarkasteltavissa kriisitilanteissa. Päätavoitteena on tarkastella erilaisia johtamisen malleja sekä strategioita, joiden avulla kriisejä on pyritty hallitsemaan ja samalla arvioida niiden toimivuutta kyseisten kriisien kohdalla konkreettisia esimerkkejä käyttäen. Tutkimuksen tarkoitus on siis vastata kysymykseen:

- Miten tietoturvaa johdetaan kriisitilanteissa pohjoismaissa?

Tutkielma pyrkii myös tuomaan esille, miten tietoturvaa voidaan johtaa tulevaisuudessa entistä tehokkaammin eri teknologioita käyttäen. Tutkielmassa arvioidaan niin aiheen kannalta oleellisia tutkimuksia, kuin eri kriisijohtamisen strategioita sekä malleja.

Aiheenvalinnan perusteena on pääosin aiheen ajankohtaisuus, josta johtuu myös rajaus 2020-luvulle ja siitä eteenpäin. Valtiot ovat joutuneet kohtaamaan useita erilaisia uhkia, kuten pandemian ja muita eri valtioiden tilanteiden aiheuttamia tietoturvauhkia. Tietoturva on myös oleellinen osa kansallista turvallisuutta (Alguliyev, Imamverdiyev, Mahmudov ja Alguliyev, 2021), ja aiheen

tutkiminen auttaa ymmärtämään, miten valtiot todellisuudessa toimivat uhkien minimoimiseksi. Uhkien voidaan tämän takia päätellä liittyvän myös yksittäisten kansalaisten sekä yritysten turvallisuuteen ja yksityisyyteen, minkä vuoksi aiheen tutkiminen on entistä tärkeämpää. Tutkielma myös esittelee tietoturvan eri osa-alueiden merkitystä kansalliselle turvallisuudelle ja pyrkii selittämään, miten tietoturva liittyy laajempaan turvallisuuteen. Tietoturva-ala ja teknologia ovat jatkuvasti kehittyviä alueita, joten on myös mielenkiintoista ymmärtää niiden luomia mahdollisuuksia sekä niistä aiheutuvia vaaroja. Tietoturva ei ole vain valtioiden ja suurten organisaatioiden huolenaihe, vaan se koskettaa myös yksittäisiä kansalaisia. Jokainen meistä käyttää päivittäin digitaalisia palveluja, ja niiden turvallisuus on olennaista yksityisyytemme ja turvallisuutemme kannalta. Aihe liittyykin myös tietojärjestelmätieteen tieteenalaan, sillä se käsittelee eri teknologioita, jotka ovat osana itse tietoturvauhkia sekä niihin vastaamista.

Tutkielma on toteutettu kirjallisuuskatsauksena ja tiedon etsimiseen on käytetty tietokantoja, kuten JYKDOK, Google Scholar ja Scopus. Hakusanoina lähteiden etsimisessä on käytetty: *information security, national security, information security management, crisis management, kansallinen turvallisuus, tietoturva.* Aineisto on kerätty aikakausilehdistä, kirjoista, tieteellisistä artikkeleista sekä muusta kirjallisuudesta. Tutkielmassa käytetty aineisto koostuu pääasiassa englanninkielisistä kirjallisuudesta, mutta myös suomenkielistä aineistoa on käytetty esimerkiksi käsitteiden määrittelyssä. Tutkielmassa on pyritty käyttämään ajantasaista vertaisarvioitua aineistoa, mutta myös vanhempia lähteitä on käytetty vakiintuneiden konseptien selittämisessä.

Tutkielma jakautuu kolmeen osaan, johdantoon, kolmeen sisältölukuun sekä yhteenvetoon. Johdanto pyrkii tarjoamaan yleiskatsauksen tutkielman aiheeseen. Ensimmäinen sisältöluku keskittyy tietoturvan määritelmiin sekä osatekijöihin ja sen rooliin valtion toiminnassa. Ensimmäisessä luvussa tarkastellaan, mitä tietoturva tarkoittaa eri näkökulmista ja miten se näkyy valtioiden toiminnassa. Tämän lisäksi ensimmäinen luku käsittelee tietoturvan keskeisiä elementtejä: tiedon eheyttä, luottamuksellisuutta sekä saatavuutta (Andress & Leary, 2017.) Toinen luku taas määrittelee kriisitilanteita, niiden hallintaa sekä vaikutuksia valtiollisella tasolla. Kappaleessa määritellään laajemmin tutkielmassa käsiteltäviä kriisitilanteita ja niiden esille tuomia uhkia pohjoismaissa. Lisäksi tarkastellaan kriisinhallinnan prosesseja, joita valtiot käyttävät kriisien hallinnassa. Viimeinen luku käsittelee tietoturvan roolia kriisitilanteissa konkreettisten menetelmien ja esimerkkien avulla. Kappaleessa käydään läpi pohjoismaihin kohdistuneita tietoturvauhkia, joita määritetyt kriisitilanteet ovat mahdollistaneet. Lisäksi käydään läpi konkreettisia menetelmiä, joita tietoturvan parantamiseksi kriisitilanteissa käytetään. Viimeisessä luvussa, eli yhteenvedossa kootaan kirjallisuuskatsauksen löydökset yhtenäiseksi kokonaisuudeksi sekä pyritään esittämään vastaus tutkimuskysymykseen. Yhteenveto myös pyrkii tarjoamaan mahdollisia jatkotutkimusaiheita ja suuntia.

2 TIETOTURVA

Nykypäivänä tietoturva on kasvanut hyvin tärkeäksi osaksi kansallista turvallisuutta ja nyky-yhteiskuntaa. Se on myös nopeasti kehittyvää, joten sen merkitys tulee vain kasvamaan entisestään. Koronan ja muiden konfliktien myötä on noussut esille entistä monimutkaisempia uhkia ja niiden seuraukset voivat olla suuria. On siis myös tärkeää ymmärtää, kuinka eri valtiot takaavat tietoturvan kansalaisilleen ja millaisia toimia niillä on käynnissä tietoturvan takaamiseksi myös tulevaisuudessa.

Pohjoismaiden on kehitettävä ja ylläpidettävä erilaisia strategioita turvatakseen niin kansalaistensa, kuin organisaatioidensakin tietoja mahdollisten uhkien ja riskien varalta sekä niiden aikana. Jotta tämä olisi mahdollista, täytyy ymmärtää mitä valtioiden tietoturva on ja mistä se koostuu.

Tässä luvussa käsitellään tietoturvan määritelmää sekä sitä, mistä tietoturva koostuu. Kappaleessa myös käydään läpi, mitä tietoturva on valtion näkökulmasta sekä, miten se näkyy valtion toiminnassa ja prosesseissa.

2.1 Tietoturvan määritelmä ja osatekijät

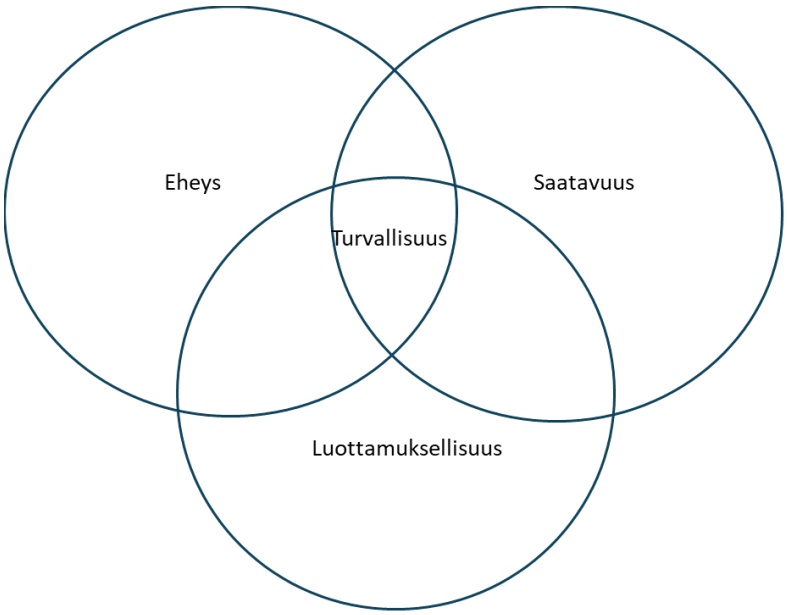
Traficomin (2020) määritelmän mukaan tietoturvalla tarkoitetaan erilaisia hallinnollisia sekä teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys sekä käytettävyys (Kyberturvallisuuskeskus, 2020.) Tämä tarkoittaa siis sitä, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, eivätkä niitä voi muuttaa muut, kuin siihen oikeutetut ja sitä, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hallinnoitavissa (Kyberturvallisuuskeskus, 2020.) Toisin sanottuna turvallisuudella tarkoitetaan resurssien turvaamista ja tietoturvan suhteen se tarkoittaa, että niitä suojellaan hyökkääjiltä, jotka tunkeutuvat verkkoihimme (Andress & Leary, 2017.) Andreaksen ja Learyn (2017) mukaan nämä resurssit voivat olla joko fyysisiä tai aineettomia, kuten ohjelmistoja, lähdekoodia tai dataa. Chai ja Zolkipli (2021) lisäävät, että myös tiedon siirto sekä staattinen tallennus ovat tällaisia resursseja. Andreas ja Leary (2017)

korostavat, että nämä resurssit voivat olla jopa arvokkaampia, kuin fyysiset resurssit. Heidän mukaansa tietoturvaan kuuluu niiden ihmisten turvaaminen, jotka ovat osa toimintoja, sillä he ovat yksi arvokkaimmista resursseista. Chai ja Zolkipli (2021) kirjoittavat myös loppukäyttäjäobjektien, eli näppäimistöjen, hiirien ja verkko- ja viestintäkanavien sekä verkko-objektien, eli reitittimien, kytkinten, yhdyskäytävien, palomuurien ja keskittimien suojaamisen olevan tärkeää.

Tietoturva koostuu kolmesta osasta, joita ovat luottamuksellisuus, eheys ja saatavuus. (KUVIO 1) Tiedon luotettavuudella tarkoitetaan yksityisyyden osaa ja se perustuu valmiuteen suojata tietoa niiltä, joilla ei ole lupaa nähdä tai käsitellä sitä. Luottamuksellista tietoa ovat esimerkiksi pankkitilien pin-koodit, salasanat, tilinumerot ja tilin saldo. Näiden tietojen vaarantuminen voi johtaa tietoturvaloukkaukseen (Andress & Leary, 2017). Tiedon luottamuksellisuus siis määritellään erilaisten tietotyyppien käytön sekä tallennuksen rajoituksina (Chai & Zolkipli, 2021.) Luottamus voi siis vaarantua hyvin helposti esimerkiksi julkisella paikalla luottamuksellisia tietoja tarkastelemalla tai käyttämällä. Esimerkiksi salasanojen käyttämisessä ja sähköpostien ja muiden viestin lähettämisessä kannattaa olla varovainen.

Tiedon eheydellä taas tarkoitetaan kykyä estää tietojen muuttumista luvattomasti tai muuten ei toivotulla tavalla. Toisin sanottuna tietoa ei poisteta tai muuteta ilman lupaa, eikä tietoja muuteta vääränlaisiksi. Eheyden saavuttamien vaatii mekanismeja estämään luvattomat muutokset ja kyvyn peruuttaa epätoivotut muutokset (Andress & Leary, 2017). Andreaksen ja Learyn (2017) mukaan muun muassa käyttöjärjestelmissä käytettävät käyttöoikeudet ovat juuri eheyden säilyttämistä ja ylläpitämistä varten. Tietokantoja taas hyödynnetään heidän mukaansa epätoivottujen muutosten kumoamiseen.

Tiedon saatavuus puolestaan tarkoittaa mahdollisuutta päästä käsiksi tietoon silloin kun sille on tarve ja valtuus (Andress & Leary, 2017.) Chai ja Zolkipli (2021) antavat ymmärtää, että eheyden varmistaminen identiteettipohjaista yksityisyyttä suojaamalla johtaisi myös saatavuuden toteutumiseen.



KUVIO 1 Tietoturva (Andress & Leary, 2017)

Alguliyev ym. (2021) puolestaan määrittelevät tietoturvan olevan valtion kansalaisten etujensuojelemistaso informaatiotilassa sisäisiä sekä ulkoisia uhkia vastaan. He kuitenkin tarjoavat myös vaihtoehtoisen perspektiivin, jonka mukaan tietoturva on joukko laadullisia indikaattoreita, jotka varmistavat kohteen ominaisuuksien eheyden, hallinnan, oleellisuuden, erilaiset potentiaalit ja maineen sekä kehityssuunnat (Alguliyev ym., 2021).

Alguliyev ym. (2021) ovat jakaneet tietoturvan eri osiin. Näistä ensimmäinen on tiedonlähteet. Tällä he tarkoittavat fyysisiä sekä sähköisiä tiedonlähteitä, jotka muodostavat valtion salaisuuksia, liikesalaisuuksia sekä luottamuksellisia ja yleisesti saatavilla olevia tiedonlähteitä. Toisena on tiedonlähteiden muodostamisen, jakelun ja käytön järjestelmät, eli esimerkiksi erilaiset tietojärjestelmät, kirjastot, arkistot tietokannat, pankit ja muut tiedonlähteet. Kolmantena tietoinfrastruktuuri, jolla he viittaavat tiedon analysointi- ja käsittelykeskuksiin, tiedonvaihtokanaviin, tietoliikenteeseen sekä tietoturvajärjestelmiin ja laitteisiin. Neljäntenä listalla on julkisen tietoisuuden muodostumisen järjestelmä, eli maailmankuva, poliittiset näkemykset, moraaliset arvot ja muut vastaavat. Viimeisenä he listaavat tieto- ja oikeusjärjestelmän. Tähän kuuluu heidän mukaansa kansalaisten, oikeushenkilöiden ja valtion tieto-oikeudet sekä luottamuksellisen tiedon ja immateriaalioikeuksien suoja (Alguliyev ym., 2021).

Sapiński (2023, s. 53) yhtyy näihin määritelmiin tietoturvasta, mutta on jakanut sen kolmeen osaan: teknisiin osiin, laillisiin osiin sekä organisationaalisiin osiin. Hänen mukaansa teknisiin osiin kuuluvat tietojärjestelmät, tietoverkot sekä tietokannat, joista jokaista tulee erikseen suojella kyberhyökkäyksiä, kuten viruksia, tietojenkalastelua, lunnasohjelmia sekä DDoS hyökkäyksiä, eli palvelunestohyökkäyksiä vastaan (Sapiński, 2023, s. 53). Tietoturvan lakiin liittyvästä puolesta Sapiński viittaa muun muassa erilaisiin tietosuojalakeihin,

joita valtiot ovat voineet asettaa yritysten sekä instituutioiden seurattavaksi. Valtioilla on myös tietoturvastandardeja, joita yritysten, instituutioiden ja muiden tulee seurata. Tällaisia säädöksiä ovat esimerkiksi Personal Data Protection Act ja GDPR, eli Yleinen tietosuoja-asetus (Sapiński, 2023, s. 53). Kolmantena Sapiński kirjoittaa organisationaalisista toimista tietoturvan säilyttämiseksi. Kuten organisaatio, niin myös valtio tarvitsee kunnollisen IT-infrastruktuurin sekä turvallisuustoimenpiteet tietoturvan varmistamiseksi. Yrityksissä on oltava käytössä tietojenkäyttömenettelyt, varmuuskopiot on oltava suojattuna sekä tietovuotoriskiä vähennettävä tietojenminimoimiskäytännöillä (Sapiński, 2023, s. 53). Valtioiden organisaatioille ja muille asettamat lait sekä standardit ovat siis myös osa valtioiden omaa tietosuojaa ja näin ollen hyvin tärkeitä ja tarpeellisia.

Sapiński (2023) kuitenkin korostaa erityisesti kyberturvan roolia tietoturvan osatekijänä. Hänen mukaansa kyberturva ja tietoturva eroavat toisistaan siten, että kyberturva suojaa erityisesti digitaalista tietoa sekä järjestelmiä hakkeroinnilta, viruksilta sekä muilta hyökkäyksiltä, kun taas tietoturva suojaa kaikenlaista tietoa, ei ainoastaan IT-järjestelmiin tallennettua (Sapiński, 2023). Myös Alguliyev ym. (2021) ottavat artikkelissaan huomioon näiden termien käyttämisen synonyymeinä ja huomauttavat, että tietoturva on laajempi käsite ja kyberturvallisuus osa sitä. Heidän mukaansa kyberturvallisuus kattaa ainoastaan elektronisen tietoympäristön. (Alguliyev ym., 2021)

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa tietosuojavaltuutetun toimiston mukaan muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen (Tietosuojavaltuutetun toimisto, 2024).

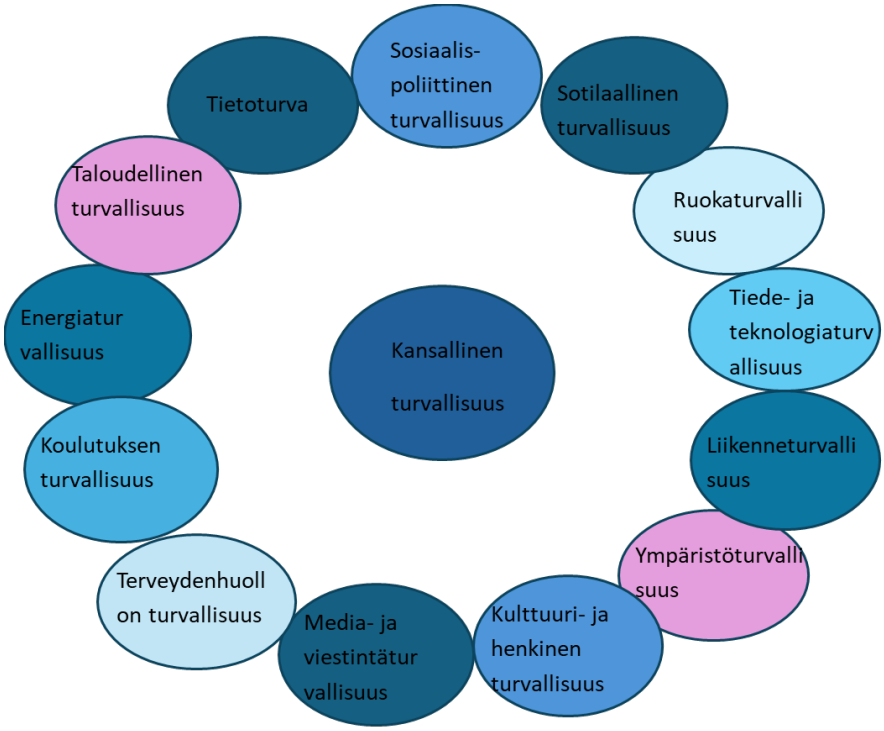
2.2 Tietoturvan rooli valtion toiminnassa

Suomen sisäministeriön mukaan kansallisella turvallisuudella tarkoitetaan koko yhteiskunnan yhteistä turvallisuutta ja valtion suvereniteettia. Se muuttuu niin ajassa, kuin suhteessa muuttuvaan uhka- ja toimintaympäristöön. Suomessa se on siis yhteiskunnan tila, jossa yhteiskunnan ja demokraattisen valtiojärjestelmän toiminta ja toimintaedellytykset sekä valtiosuvereniteetti on suojattu vakavilta uhkilta (*Sisäministeriö*, 2024). Alguliyev ym. (2021) Määrittelevät kansallisen turvallisuuden koostuvan sosiaalisesta ja poliittisesta turvallisuudesta, ekonomisesta turvallisuudesta, sotilaallisesta turvallisuudesta, tietoturvasta, tieteellisestä ja teknologisesta turvallisuudesta, koulutusjärjestelmän turvallisuudesta, terveydenhuoltojärjestelmän turvallisuudesta, elintarviketurvallisuudesta, energiaturvallisuudesta, liikennejärjestelmän turvallisuudesta, joukkoviestinnän turvallisuudesta, ympäristöturvallisuudesta sekä kulttuurillisesta ja henkisestä turvallisuudesta. (KUVIO 2)

Esimerkiksi koronapandemian aikana levinnyt väärä tieto ja disinformaatio heikensivät luottamusta viranomaisiin ja lisäsivät sosiaalista epävarmuutta (Hansson, Orru, Torpan, Bäck, Kazemekaityte, Meyer ja Pigrée, 2021.) Pandemia aiheutti myös taloudellisia menetyksiä ja lisäsi kyberrikollisuutta, kuten tietojen kalastelua sekä kiristysohjelmia (Chigada & Madzinga, 2021.) Pandemian aikaiset terveydenhuoltojärjestelmiin kohdistuneet kyberhyökkäykset osoittivat, kuinka tärkeää tieteellisen ja teknologisen infrastruktuurin suojaaminen on (Alawida, Omolara, Abiodun & Al-Rajab, 2022.)

Ukrainan sota taas on lisännyt poliittisia jännitteitä sekä vaikuttanut poliittiseen vakauteen (Willett, 2022.) Se on myös vaikuttanut taloudellisiin suhteisiin ja kaupankäyntiin, mikä taas on lisännyt taloudellisia kyberuhkia (European parliament, 2023.) Ukrainan sota on korostanut kyberturvallisuuden merkitystä sotilaallisessa kontekstissa, sillä hyökkäyksiä on kohdistunut kriittiseen infrastruktuuriin ja sotilaallisiin kohteisiin. Tämä on lisännyt tarvetta kyberpuolustukselle (Willett, 2022). Myös Ukrainan sota on korostanut teknologisen turvallisuuden merkitystä muun muassa tiedustelutiedon suojaamisessa (Willett, 2022.)

Myös Alguliyev ym. (2021) korostavat tietoturvan roolia nykyisessä tietoyhteiskunnassa ja kuten Andress ja Leary (2017), he toteavat, että tietoturva kattaa niin fyysisen, kuin sähköisen tietoympäristön. Valtion kannalta tietoturva tarkoittaa Alguliyevin ym. (2021) mukaan tietoinfrastruktuurin kestävää ja tasapainoista kehittämistä, kansalaisten perustuslaillisten tietoon liittyvien oikeuksien toteuttamista ja sille suotuisten olosuhteiden luomista, valtion tietoresurssien suojaamista laittomalta pääsyltä sekä valtion tieto- ja tietoliikennejärjestelmien turvallisuuden varmistamista. Kansallisen turvallisuuden kannalta tärkeää on varmistaa tasapaino kansalaisten tietoon liittyvien oikeuksien toteuttamisen ja tietoturvan välillä. Tärkeää on myös tietoturvastruktuurin edistäminen tukemalla uusien tieto- ja viestintäteknologioiden kehittämistä, levittämistä ja soveltamista kaikilla tarvittavilla alueilla ja yhtenäistää tiedon haun, keräämisen, tallentamisen käsittelyn ja analyysin välineet globaalin tietoturvainfrastruktuurin vaatimusten mukaisesti. On myös tärkeää parantaa tietoturvan oikeudellista kehystä ja koordinoida asianomaisten valtionvirastojen toimintaa, kehittää kansallista telekommunikaatio- ja tietotekniikkateollisuutta sekä suojata luotettavasti julkiset tietoresurssit valtion virastoissa ja muissa strategisesti tärkeissä paikoissa (Alguliyev ym., 2021).



KUVIO 2 Kansallinen turvallisuus (Alguliyev ym., 2021)

Tietoturva siis vaikuttaa hyvin laajalla alueella ja sen merkitys korostuu erityisesti kehittyvässä yhteiskunnassa ja valtion lisäksi myös yritysten ja kansalaisten toiminta on enemmän sidoksissa tietojärjestelmiin. Näiden järjestelmien ja niiden sisältämien tietojen vaarantuminen voi johtaa vakaviin seurauksiin, joten on tärkeää, että valtioilla on keinoja niiden ehkäisemiseksi ja niiltä suojautumiseen. Valtioilla on keskeinen rooli niin kansallisen turvallisuuden, kuin tietoturvan ylläpitämisessä.

Pohjoismaista Suomi, Ruotsi, Tanska ovat EU-maita, minkä vuoksi niihin vaikuttaa myös EU-lainsäädäntö. Norja ja Islanti eivät ole EU-maita, mutta myös ne seuraavat EU:n asettamia tietoturvalakeja ja -säädöksiä, sillä Norja ja Islanti kuuluvat Euroopan talousalueeseen (ETA). Tämä käy ilmi säädöksistä merkinnällä ”EEA relevance”. GDPR on yleinen tietosuoja-asetus, joka asettaa yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat vaatimukset. Asetusta sovelletaan, jos organisaatio käsittelee henkilötietoja ja sijaitsee EU:ssa tai, jos Organisaatio sijaitsee EU:n ulkopuolella, mutta käsittelee henkilötietoja tavaroiden tai palvelujen tarjoamiseen henkilölle EU:ssa tai seuraa yksilöiden käyttäytymistä EU:ssa (*Your Europe*, 2024).

ENISA:n mukaan network and information security direktiivi ja NIS2 ((EU) 2022/2555) on kyberturvallisuutta koskeva lainsäädäntö, joka säätää oikeudellisista toimenpiteistä kyberturvallisuuden yleisen tason parantamiseksi EU:ssa. Direktiivin tarkoitus on luoda tarvittava kyberkriisihallintarakenne, lisätä harmonisoinnin tasoa turvallisuusvaatimuksissa sekä raportointivelvoitteissa, kannustaa jäsenvaltioita ottamaan kyberturvallisuusstrategioihinsa uusia kohteita, tuoda uusia ideoita yhteistyön ja tiedonjakamisen edistämiseksi jäsen-

valtioiden välillä, ottaa mukaan useampia sektoreita, mikä velvoittaa useampia tahoja ryhtymään toimiin kyberturvallisuuden tason parantamiseksi (*ENISA*, 2024.).

Cybersecurity act eli kyberturvallisuusasetus vahvistaa Euroopan unionin kyberturvallisuusviraston ENISA:n tavoitteet, tehtävät ja organisatoriset näkökohdat ja vahvistaa kehyksen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta riittävän tasoinen kyberturvallisuus tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille unionissa voidaan varmistaa sekä välttää sisämarkkinoiden hajauttaminen unionissa kyberturvallisuuden sertifiointijärjestelmien osalta (*Asetus - 2019/881 - FI - EUR-Lex*, 2019.) ENISA:n tehtävänä on siis operatiivisen yhteistyön lisääminen EU-tasolla, auttaa jäsenvaltioita kyberturvahyökkäysten käsittelyssä ja tukea EU koordinaatiota laajamittaisissa rajat ylittävissä kyberhyökkäyksissä ja kriiseissä (*The EU Cybersecurity Act*, 2024.)

Pohjoismaat kuuluvat myös ISO (International Organization for Standardization) jäsenmaihin ja seuraavatkin myös esimerkiksi ISO/IEC säädöksiä, jotka eivät ole EU:n asettamia. ISO on järjestö, joka tuo yhteen globaaleja asiantuntijoita, sopiakseen parhaista toimintatavoista (*ISO*, 2024). Näitä säädöksiä ovat ISO/IEC 2700 säädökset, joihin kuuluu yli tusina eri standardeja. ISO/IEC207001 on maailman tunnetuin standardi tietoturvan hallintajärjestelmille, joka auttaa yhdessä muiden ISO/IEC standardien kanssa käsittelemään kyberresilienssin ja tietoturvan parhaita käytäntöjä auttamalla kaiken kokoisia organisaatioita kaikilta sektoreilta hallitsemaan omaisuutta, kuten taloudellista tietoa, immateriaalioikeuksia, työntekijätietoja ja kolmansien osapuolten luovuttamia tietoja (*ISO*, 2022).

Suomessa vastuu kansainvälisistä tietoturvavelvoitteista on hajautettu useille eri viranomaisille. Puolustusministeriö, suojelupoliisi ja pääesikunta ovat niin sanottuja määrättyjä turvallisuusviranomaisia (DSA, Designated Security Authority) (Kyberturvallisuuskeskus, 2024). Edellä mainitut vastuutahot ja niiden tehtävät on määritelty kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) (Puolustusministeriö, 2024.) Kansallisesta tietoturvallisuudesta vastaa myös muun muassa sisäministeriö, jonka tehtävänä on huolehtia kansallisesta turvallisuudesta valtioneuvostotasolla sekä ohjata ja valvoa suojelupoliisin toimintaa ja valmistella sitä koskeva lainsäädäntö (Sisäministeriö, 2024.) Tämä siis kattaa myös esimerkiksi kyberturvallisuuden varmistamisen kansallisen turvallisuuden näkökulmasta. Myös suojelupoliisi, SUPO ehkäisee ja torjuu kansallisen turvallisuuden uhkia kuten kybervakoilua, terrorismia, mukaan lukien kyberterrorismia sekä valtionhallinnon tietoturvaa (Supon tehtävät, 2024.)

Liikenne- ja viestintävirasto Traficomin vastuulla on sen alaisuudessa toimiva Kyberturvallisuuskeskus. Kyberturvallisuuskeskus ehkäisee tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. Se vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista, tietoturvan sääntelystä ja valvonnasta sekä ohjaa ja valvoo toimivaltaan kuuluvia tietoturvallisuuden, häiriöttömyyden ja luottamuksellisen viestinnän suojan säädöksiä. Kyberturvallisuuskeskus säätää velvollisuuden huolehtia tarjoamiensa verkkojen ja palvelujen tietoturvasta sekä oikeuksia tämän toteuttami-

seen eri toimijoille. Se valvoo tietoturvavelvoitteiden noudattamista, sähköisen viestinnän tietosuojaa viestinnän välittäjien toiminnassa sekä sähköisen tunnistautumisen palveluja (Kyberturvallisuuskeskus, 2024).

Muita Kyberturvallisuuskeskuksen vastuita ovat kansallisen kyberturvallisuusyhteistyön kehittäminen, kansallisen kyberturvallisuuden toimintakyvyn kasvattaminen, kansallisten toimijoiden osallistumisen edistäminen rajat ylittäviin EU-hankkeisiin sekä tunnettavuuden ja tietoisuuden kasvattaminen kansallisten koordinointikeskusten ja kyberturvallisuusyhteisön työstä. Kyberturvallisuuskeskus myös parantaa kyberomavaraisuutta, tukee kyberturvallisuusalan tutkimusta ja vauhdittaa teknologian kehittämistä koko EU:ssa. Yhteistyö jäsenvaltioiden välillä lisääntyy ja tiivistyy, minkä myötä pyritään vahvistamaan muun muassa EU:n kyberturvallisuusvalmiuksia sekä toimialan kilpailukykyä. Kyberturvallisuuskeskus myöntää rahoitustukea pienten ja keskisuurten yritysten kyberturvallisuusratkaisujen ja -innovaatioiden käyttöönottoprojekteihin. Kyberturvallisuuskeskus kokoaa yhteen keskeiset kyberturvallisuuden julkisen, yksityisen ja kolmannen sektorin toimijat. Tiivistyvän yhteistyön tavoitteena on kansallisen kyberturvallisuuden tutkimuksen, kehittämisen ja innovoinnin parantaminen. Kyberturvallisuuskeskuksen sisäinen NCSA (National Communications Security Authority) toimii määrättynä turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena ja vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista (Kyberturvallisuuskeskus, 2024). Kansainvälisten tietoturvavelvoitteiden kokonaisvastuu on ulkoministeriöllä. Se toimii kansallisena turvallisuusviranomaisena (NSA, National Security Authority), joka ohjaa kansallista toimintaa, vastaa muun muassa kansainvälisten turvallisuussopimusten valmistelusta, sekä ohjaa ja valvoo, että kansainväliset erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti (Kyberturvallisuuskeskus, 2024).

Tietosuojavaltuutetun toimisto taas on tietosuojalainsäädännön noudattamista valvova kansallinen valvontaviranomainen, jossa tietosuojavaltuutettu ja muut asiantuntijat huolehtivat muun muassa tietosuojalainsäädännön valvonnasta, henkilötietojen käsittelyä koskevien lakien noudattamisesta. Tietosuojavaltuutettu edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista, velvollisuuksista ja oikeuksista. Hän tekee myös selvityksiä ja tarkastuksia sekä määrää hallinnollisia seuraamuksia tietosuoja-asetuksen rikkomisesta, antaa lausuntoja lainsäädännöllisistä ja hallinnollisista uudistuksista, jotka koskevat henkilöiden oikeuksien ja vapauksien suojaamista henkilötietojen käsittelyssä. Hän valvoo luottotietojen ja yritysluottotietojen käsittelyä sekä käsittelee pyyntöjä rekisteröidyn oikeuksia koskevien määräysten antamiseksi ja ilmoituksia muista henkilötietojen käsittelyyn liittyvistä epäkohdista. Tietosuojavaltuutettu vastaanottaa ilmoituksia tietosuojavastaavista ja henkilötietojen tietoturvaloukkauksista. Hän laatii luetteloita siitä, milloin vaaditaan tietosuojaa koskeva vaikutustenarviointi ja arvioi ennakkokuulemisia korkean riskin tietojenkäsittelystä. Tietosuojavaltuutettu hyväksyy käytännesääntöjä ja vakiosopimuslausekkeita sekä kannustaa ottamaan käyttöön sertifiointeja ja akkreditoi sertifiointielimiä. Lisäksi hän edustaa Suomea Euroopan tietosuojaneuvostossa ja tekee yhteistyötä muiden EU tietosuojavi-

ranomaisten kanssa sekä vie tarvittaessa asioita Euroopan tietosuojaneuvoston arvioitavaksi. (Tietosuojavaltuutetun toimisto, 2024).

Puolustusministeriö on kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) määrätty turvallisuusviranomainen, jonka tehtäviin kuuluu ohjata ja valvoa, että kansainvälistä turvallisuusluokiteltua tietoa suojataan puolustushallinnossa säädösten ja määräysten mukaisesti. Se vastaa valtioneuvoston osana ja hallinnonalansa ohjaajana kansallisesta puolustuspolitiikasta ja turvallisuudesta sekä kansainvälisestä puolustuspoliittisesta yhteistyöstä. Puolustusministeriö myös ohjaa Suomen puolustuksen kehittämistä EU:n ja Naton jäsenenä sekä kansainvälisessä puolustusyhteistyössä. Lisäksi sen vastuulla on Suomen osallistuminen kansainväliseen kriisinhallintaan sekä Euroopan turvallisuusrakenteisiin vaikuttaminen kansallisten etujen turvaamiseksi. (*Puolustusministeriö*, 2024.) Puolustusvoimat puolestaan vastaa kyberpuolustuksen kokonaisuuden suunnittelusta ja puolustusvoimien johtamisjärjestelmäkeskus suojaa tietoverkkoja ja -palveluita sekä kehittää kyberpuolustusta. Osasto myös ylläpitää puolustusvoimien kybertilannekuvaa (Puolustusvoimien johtamisjärjestelmäkeskus, 2024).

Valtion tieto- ja viestintätekniikkakeskus Valtori vastaa usean tahon, kuten valtionhallinnon virastojen ja laitosten, valtion liikelaitosten, julkisen hallinnon viranomaisten, julkisoikeudellisten laitosten, eduskunnan, valtion talousarvion ulkopuolisten rahastojen ja julkista hallinto- tai palvelutehtävää hoitavien yritysten tai yhteisöjen perustietotekniikkapalveluiden tuottamisesta. Valtori tuottaa toiminta-alasta riippumattomia ICT-palveluita, korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja ja integraatiopalveluja. Se vastaa Suomen laajimman ICT-ympäristön ylläpidosta, suojelemisesta ja kehittämisestä sekä valtionhallinnon arjen sujuvuuden ja turvallisuuden huolehtimisesta ICT-palveluiden ja -työvälineiden kanssa. Valtori mahdollistaa yhteensopivat ratkaisut ja joustavat organisaatiomuutokset valtion eri virastojen välillä, saavuttaa säästöjä yhdenmukaisten prosessien ja palveluiden avulla sekä varmistaa normaali- ja poikkeusoloissa valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten yhteistoiminnan edellyttämän viestinnän häiriöttömyyden ja jatkuvuuden. Lisäksi Valtori turvaa päätöksenteossa ja johtamisessa tarvittavan tiedon käytettävyyden, eheyden ja luottamuksellisuuden (*Valtori,* 2024).

Tietoturva on siis keskeisessä roolissa valtioiden toiminnassa ja vaikuttaa usealla sektorilla sekä kansallisen turvallisuuden, että yhteiskunnan toiminnan takaajana. Pohjoismaissa tietoturvaa käsitellään laajasti eri sektoreilla ja vastuut on jaettu useiden toimijoiden kesken, jotta tietoturvan haasteisiin voidaan vastata tilanteiden vaatimalla vakavuudella. Myös muilla pohjoismailla on esimerkiksi omat kyberturvallisuuskeskuksensa. (Suomen Kyberturvallisuusstrategia, 2019; Danish Cyber and Information Security Strategy 2022–2024, 2022; Regeringskansliet, 2017; Netöryggi, 2022; Government.no, 2019)

3 KRIISITILANTEET

Tässä luvussa käsitellään erilaisia aiheita, jotka liittyvät kriisien hallintaan ja niiden vaikutuksiin valtioiden näkökulmasta. Kappaleessa määritetään kriisitilanteet, joita tässä tutkielmassa myöhemmin tarkastellaan sekä pyritään antamaan ymmärrys siitä, mitkä tilanteet luokitellaan kriiseiksi ja kuinka niiden vaikutus näkyy valtion toiminnassa. Kappale myös tarkastelee kriisinhallinnan roolia valtiollisella tasolla ja korostaa valtiollisen valmiuden sekä hallinnan tärkeyttä valtiollisen sekä kansallisen turvallisuuden sekä tehokkaan toiminnan varmistamiseksi. Lisäksi kappale käsittelee valtioiden käyttämiä kriisinhallinnan strategioita ja menetelmiä pohjoismaiden, etenkin Suomen, näkökulmasta.

3.1 Kriisitilanteiden määrittely ja luokittelu

Kriisitilanteiden tai kriisien voidaan Euroopan unionin kyberturvallisuusviraston ENISA:n (2024) mukaan määritellä olevan epänormaali tai poikkeuksellinen tapahtuma tai tilanne, joka uhkaa organisaatio tai yhteisöä ja vaatii sekä strategista, mukautuvaa, että nopeaa reagointia sen elinvoimaisuuden sekä koskemattomuuden säilyttämiseksi. Kriisi voi myös olla poikkeuksellinen tapahtuma, joka eroaa normaalista ja aiheuttaa vakavaa häiriötä tai häiriöriskin yhteiskunnan elintärkeille toiminnoille. Tarkemmin kriisi on vakava uhka järjestelmän perusrakenteille tai keskeisille arvoille ja normeille. Erittäin epävarmoissa oloissa ja ajanpaineessa se vaatii keskeisten päätösten tekemistä. Kriisi on tapahtuma, joka vaikuttaa moniin ihmisiin ja yhteiskunnan eri osiin laajasti sekä uhkaa perustavanlaatuisia arvoja sekä toimintoja. Se on tila, jota ei voida hallita tavanomaisin resurssein, sillä se on odottamaton ja kaukana arkipäiväisestä ja tavallisesta. Sen ratkaiseminen edellyttää useiden toimijoiden yhteistä toimintaa ja vaatii riskien, seurausten, vakavuuden sekä ajan tarkkaa ja perusteellista arviointia (ENISA, 2024).

ENISA (2024) tunnistaa kolme eri kriisityyppiä, joita ovat hiipivä, akuutti sekä krooninen tai toistuva kriisi. Hiipivällä kriisillä viitataan kriisiin, joka ke-

hittyy hiljalleen ja purkautuu yleensä odottamatta. Akuutti kriisi taas on sellainen, joka tapahtuu odottamatta hyvin yllättäen ja vaikuttaa laajasti hyvin nopeassa ajassa (ENISA, 2024). Myös McConnell (2003) kirjoittaa yhtäkkisestä, hiipivästä sekä kroonisesta kriisistä. Yhtäkkisellä kriisillä hän viittaa tavanomaisimpaan näkemykseen kriiseistä, jossa jokin asia tai sarja asioita tapahtuu hyvin odottamattomasti tai varoituksetta. Esimerkkinä tästä WTC-iskut. Toinen taas on hiipivä kriisi, jossa ei ole dramaattisia tapahtumia, vaan paine kasautuu hitaasti, usein jopa vuosien ajan. Tällaisia kriisejä ei usein huomata ja ne saatetaan jopa sivuuttaa alkuvaiheissa. Kolmas kriisi McConnellin (2003) mukaan on krooninen kriisi, joka saattaa sisältää niin yhtäkkisiä tapahtumia, kuin hiipiviäkin asioita. Hän kirjoittaa tällaisista kriiseistä tekevän kroonisia sen, että niihin ei ole selviä ratkaisuja ja ne ovat jatkuvia (McConnell, 2003). Ne ovat kriisejä, jotka esiintyvät säännöllisesti tai ovat pitkäkestoisia (ENISA, 2024.) Kroonisiin kriiseihin ei välttämättä ole mitään ratkaisua, vaan niihin reagoidaan tarpeen vaatiessa valmiiksi laadituilla keinoilla (McConnell, 2003.) Myös Wincott, Davies ja Wager (2020, s.1529) kirjoittavat kriisin määritelmästä samaan tyyliin. He kuitenkin antavat artikkelissaan ymmärtää sen tarkoittavan enemmän, kuin politiikan kiivautta sekä poliittisten instituutioiden toimintaa stressin ja paineen alla. Näin ollen kriisi tarkoittaa heidän mielestään ratkaisevan muutoksen laukeamista siitä, mikä on ollut ennen. Kriisin tulkinta voi siis riippua tilanteesta ja kokemuksesta sekä seuraamuksista, mutta näiden tulkintojen perusteella on tärkeää osata tunnistaa, kriisit ja niiden muoto, jotta niihin voidaan niin valmistautua, kuin reagoida tilanteen vaatimalla tavalla. Kriisit ovat siis moniulotteisia tapahtumaketjuja ja toimivat välttämättä muutoksen aikaansaajina, minkä takia on tärkeää, että niihin osataan vastata valtionjohdon toimesta tehokkaasti (Wincott ym., 2020, s.1529).

Tässä tutkielmassa keskitytään kriisien, erityisesti koronapandemian sekä Ukrainan sodan aiheuttamiin tietoturvauhkiin, jotka vaativat toimenpiteitä valtion taholta pohjoismaissa, päätarkastelukohteena Suomi. Alawidan ym. (2022, s.8177) mukaan vuoden 2019 joulukuussa alkanut Covid-19 pandemia mahdollisti kyberrikollisten käyttää hyväksi sosiaalisia puutteita mikä on muutenkin kriisitilanteissa yleistä. Koronapandemia on nimitetty maailman suurimmaksi kyberturvallisuusuhaksi ja on vaikuttanut laajasti esimerkiksi terveydenhuoltoon ja pankkiteollisuuteen. Esimerkiksi toiminnan siirtyminen laajasti verkkoon etätyönteon muodossa altisti tietomurroille. Covid-19 julistettiin maailmanlaajuiseksi pandemiaksi tammikuussa 2020 ja se mahdollisti erilaisten kyberhyökkäysten yleistymisen ympäri koko maailmaa. Hakkerit käyttivät hyväkseen haavoittuvaista tilannetta ja pääsivät käsiksi esimerkiksi kriittisiin tietoihin sekä organisaatioiden omaisuuteen (Alawida ym., 2022, s.8177).

Toisena tutkielmassa tarkastellaan Ukrainan sotaa ja tarkemmin sitä, kuinka Venäjän hyökkäys Ukrainaan vuonna 2022 on vaikuttanut tietoturvaan Pohjoismaissa. Venäjä on niin kehittänyt, kuin käyttänytkin erilaisia kybertoimia vastustajiinsa jo useiden vuosien ajan. Esimerkiksi oman informaatiotilansa hallinta ja vastustajiensa saman horjuttaminen on eräs näistä keinoista (Willett, 2022). Voidaan siis päätellä, että tilanne Ukrainassa ei ole poikkeus. Willett (2022) kirjoittaa, että tämä on Venäjän keino horjuttaa vastustajiensa infrastruktuuria ja jopa sotilaallista kykyä ja siksi valtiollisella tasolla hyvin merkittävä

uhka. Venäjän toimet Ukrainaa vastaan ovat jatkuneet vuodesta 2014 ja etenivät lopulta hyökkäykseen vuonna 2022. Tämän sodan aikana Venäjä on muun muassa hyökännyt eurooppalaiseen verkkoon (Viasat), mikä lopulta vaikutti myös muihin Euroopan maihin. Tämä osoitti, että Venäjä on valmis ottamaan sen riskin, että hyökkäys ja sen vaikutukset leviäisivät myös Ukrainan ulkopuolelle (Willett, 2022, s. 12).

3.2 Kriisinhallinnan merkitys valtiollisella tasolla

Kriisinhallinnalla on hyvin keskeinen rooli kansallisen turvallisuuden ylläpitämisessä ja yhteiskunnan elintärkeiden toimintojen turvaamisessa. Tietoturvan ja kyberturvallisuuden osalta kriisinhallinta edellyttää valmiutta sekä tehokasta yhteistyötä eri toimijoiden ja viranomaisten välillä niin yrityssektorissa, kuin valtiossa sekä kansainvälisesti.

Kriisinhallinnalla tarkoitetaan institutionaalista ja organisatorista suunnitteluprosessia ja laajaa rakennetta, joka kattaa päätöksentekijät tietyillä rooleilla ja toimilla. Kriisinhallinta ymmärretään vaikeiden päätösten tekemisenä ja toteuttamisena vaikeissa olosuhteissa. Kriisinhallinta on laaja viitekehys, johon myös kyberkriisinhallinta kuuluu. Kyberkriisinhallinta voidaan nähdä sellaisen kriisin hallintana, jolla on kyberalkuperä tai merkittävä kyberkomponentti (*ENISA*, 2024., s.16). Koska Covid-19 sekä Ukrainan sota ovat kriisejä, jotka sisältävät merkittäviä kyberkomponentteja, voidaan niihin soveltaa kyberkriisinhallintaa.

Kriisinhallinta ei rajoitu ainoastaan yksittäisten toimijoiden tai valtioiden toimiin, vaan vaatii yhteistyötä useiden poikkisektoristen toimijoiden ja eri valtioiden välillä muun muassa jakamalla tietoa (ENISA, 2024., s.16.) Kriisinhallinta siis edellyttää valmiutta sekä tehokasta yhteistyötä kansallisella sekä kansainvälisellä tasolla. Kyberkriisinhallinnassakin tärkeinä suuntaa antavina asetuksina toimii NIS, NIS2 ja kyberturvallisuuslaki. Erityisesti NIS2 esittelee uusia tapoja kyberturvallisuustapausten ehkäisyyn, hallintaan ja reagointiin. Kyberkriisinhallinta vaatii osallistumista niin yksityisen puolen, kuin julkisen puolen eri sektoreilta ja nämä toimijat operoivat eri tasoilla. Eri tasoja, jotka osallistuvat kyberkriisinhallintaan ovat organisaatio ja korporaatiotaso, sektoritaso, alueellinen taso, kansallinen taso, EU-taso sekä kansainvälinen taso (ENISA, 2024).

Organisaatiotasolla keskeisiä toimijoita ovat kyberkriisistä kärsivät kriittiset toimijat, joten heidän yhteistyönsä sekä tietonsa ovat olennaisia lieventämistoimenpiteiden asianmukaisen toteutuksen kannalta. Heidän roolinsa on myös viestiä tietojärjestelmiensä kartoituksesta kriisinhallinnasta vastaaville kansallisille viranomaisille. Kriisinhallinta voi myös noudattaa sektorikohtaista menetelmää, jossa NIS2 toimii perustana, sillä se määrittää tärkeiksi katsotut sektorit, joille räätälöidään kyberkriisinhallintasuunnitelma, mikä parantaa toimijoiden välistä koordinointia ja yhteistyötä. Alueellisella tasolla taas viranomaiset voi-

vat olla mukana kyberkriisien hallinnassa esimerkiksi siksi, koska he ovat lähellä kriisistä kärsiviä toimijoita (ENISA, 2024., s.17).

Kansallisella tasolla vastuussa kyberturvallisuudesta, kriisinhallinnasta ja kyberkriisinhallinnasta ovat EU:n jäsenvaltiot. Ne toteuttavat tarvittavia toimenpiteitä kansallisten turvallisuusetujen suojaamisen ja yleisen järjestyksen ja turvallisuuden turvaamisen varmistamiseksi. NIS2 velvoittaa jäsenvaltioita laatimaan kyberkriisinhallintasuunnitelman ja perustamaan kansalliset kriisinhallintaviranomaiset. EU-tasolla kyberkriisi on tilanne, jossa kriisi vaikuttaa vähintään kahteen jäsenvaltioon. EU asettaa yhteisiä vertailuarvoja, jotka edistävät Euroopan kyberkriisikestävyyden tason nostamista esimerkiksi vahvistamalla jäsenvaltioiden kriisinhallintakykyä ja parantamalla kollektiivista tilannetietoisuutta. Kyberkriisit voivat kuitenkin ylittää EU:n jäsenvaltioiden rajat, mikä vaatii kansainvälistä väliintuloa tilanteen ratkaisemiseksi. Näitä tapauksia varten on olemassa ja voidaan luoda kahdenvälisiä sopimuksia, kuten kyberdiplomatiatyökalupakki, joka tarjoaa kehyksen EU:n yhteiselle diplomaattiselle vastaukselle haitallisiin kybertoimiin. (ENISA, 2024, s.17, 18).

Kyberkriisin ilmentyessä EU:n jäsenvaltioiden ja EUIBA:iden (Euroopan unionin instituutiot, elimet ja virastot) ja näin ollen myös Norjan sekä islannin tulee tehdä yhteistyötä kyberkriiseihin vastaamisen asianmukaiseksi koordinoimiseksi koko EU:ssa (ENISA, 2024, s.18.) Tämä tapahtuu kolmella eri tasolla.

ENISA:n mukaan strateginen taso vastaa kriisien sekä kyber- että ei-kybernäkökulmien strategisesta sekä poliittisesta hallinnasta. Näitä toimia suorittavat valtioiden kyberturvallisuudesta vastaavat ministerit, Eurooppaneuvosto ja sen puheenjohtaja, Euroopan unionin neuvoston puheenjohtajavaltio ja Euroopan unionin neuvosto, Euroopan komissio, mukaan lukien puheenjohtaja tai valtuutettu varapuheenjohtaja/komissaari, sekä Euroopan ulkosuhdehallinto, mukaan lukien unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja (ENISA, 2024, s.18). Operatiivinen taso puolestaan keskittyy päätöksenteon valmisteluun strategisella tasolla kyberkriisinhallinnan koordinointiin ja tilannetietoisuuteen sekä vaikutusten arviointiin ja lieventämistoimiin. Operatiivisen tason määritelmä voi kuitenkin muuttua valtion mukaan. ENISA:n julkaisussa se määritellään kulmakivenä jäsenvaltioiden ja EU:n instituutioiden välisen yhteistyön vahvistamiseksi sekä strategisen ja teknisen tason välisen koordinoinnin helpottamiseksi (ENISA, 2024, s.18). Tekninen taso taas käsittää kyberkriisin aikana tapahtuvien tapausten käsittelyn, seurannan sekä valvonnan sisältäen uhkien ja riskien jatkuvan analysoinnin. Toimijoihin kuuluvat CSIRTs-verkosto, kansalliset CSIRTs, Euroopan komissio, EEAS, EU:n instituutioiden, elinten ja virastojen tietokonehätätilanteiden ryhmä, ENISA ja Euroopan unionin lainvalvontayhteistyöviraston Euroopan kyberrikollisuuskeskus (ENISA, 2024, s.18).

Hu ja Liu (2022) kirjoittavat, että keskeisintä valtioiden kriisinhallinnassa ovat kognitio, koordinaatio sekä kommunikaatio ja viestintä. Olennainen ensimmäinen askel on ilmentyvien riskien tunnistaminen ja niihin reagoiminen. Ilman riskien sekä niistä koituvien vakavien seurausten ymmärtämistä, hätätilanteiden hallinnan päättäjät menettävät mahdollisuuden viestiä yleisölle ja koordinoida toimintaa sidosryhmien kesken ajoissa. Toinen kriittinen osa kriisinhallintaa on riskien viestiminen laajasti eri sidosryhmille, sillä se auttaa ti-

lannekuvan kehittämisessä eri sektoreiden ja toimialueiden kesken. Selkeän, ytimekkään ja ajantasaisen tiedon viestiminen voi lisätä kansalaisten luottamusta ja edistää julkista politiikkaohjeiden noudattamista. Politiikka kuitenkin usein häiritsee kriisiviestintää, mikä johtaa liialliseen keskittymiseen maineenhallintaan ja kriisiviestinnän politisoitumiseen (Hu & Liu, 2022, s. 737). Kriisien koordinointi taas mahdollistaa vastaavien henkilöiden ja organisaatioiden tiedonvaihdon, resurssien mobilisoinnin ja toimien yhdenmukaistamisen yhteisen tavoitteen saavuttamiseksi. Koordinoinnin monimutkaisuus kasvaa, kun eri kokoisten ja taustaisten toimijoiden määrä kasvaa rajat ylittävässä kriisissä. Organisaatioiden kulttuuriset ja toiminnalliset erot korostuvat usein kriisin aikana. Vakiintuneet koordinointirakenteet ja -prosessit ovat välttämättömiä resurssien nopeaan käyttöönottoon. Rajat ylittävän kriisin laajuus ja mittakaava voivat kuitenkin nopeasti ylittää olemassa olevat koordinointirakenteet. Tämän vuoksi ylhäältä alas suuntautuva ja verkostopohjainen koordinointi on tarpeen suurimittaisiin kriiseihin vastaamiseksi. Rajat ylittäviin suuriin kriiseihin, kuten COVID-19, vastaaminen vaatii kriisinhallintakykyjen kehittämistä sekä kansallisilla että kansainvälisillä alueilla (Hu & Liu, 2022, s. 737).

4 TIETOTURVAJOHTAMINEN KRIISITILANTEISSA

Tässä luvussa pyritään selittämään, kuinka tietoturva ja kriisitilanteet sekä kriisijohtaminen ovat käytännössä sidoksissa toisiinsa ja millaisia konkreettisia toimia tietoturvan takaamiseksi kriisitilanteiden aikana tehdään. Ensin käydään läpi tapauksia, joissa kriisitilanteet ovat haavoittaneet tietoturvaa ja millaiset haavoittuvuudet ovat mahdollisia. Tämän lisäksi tarkastellaan, miten kriisinhallinta järjestetään sopeuttamalla tietoturvatoimenpiteitä osaksi kriisijohtamista. Myös konkreettiset esimerkit valtioiden toimista sekä valmiussuunnitelmista ovat olennainen osa tätä lukua. Lopussa käydään läpi yhteistyötä Pohjoismaiden välillä ja tarkastellaan niin onnistuneita, kuin epäonnistuneitakin tapauksia tietoturvasta osana kriisinhallintaa.

4.1 Tietoturvajohtaminen

Tietoturvajohtamisen on aikaisemmin ajateltu olevan tekninen osa-alue, mutta nykyään sen ajatellaan koskevan koko organisaatiota ja onkin tärkeää, että sen toteutuminen varmistetaan jokaisella sektorilla (Somepalli, Tangella & Yalamanchili, 2020.) Somepallin ym. (2020) mukaan ISO-standardointijärjestö kuvaa tietoturvan hallintajärjestelmän koostuvan juuri ihmisistä, järjestelmistä ja IT-järjestelmistä muodostaen näin pohjan teknisen tiedonhallinnan tietojen hallinnalle.

Culot., Nassimbeni, Podrecca, & Sartor, 2021) kirjoittavat ISO27001 -standardin määrittävän vaatimukset tietoturvallisuuden hallintajärjestelmän (ISMS) perustamiselle, toteuttamiselle, ylläpitämiselle ja jatkuvalle parantamiselle. Esimerkiksi pohjoismaat seuraavat standardia (*ISO*, 2022.) Standardin seuraaminen voi parantaa kansallista tietoturvallisuutta ja tehostaa julkishallinnon prosesseja. Sertifiointi voi parantaa valtion mainetta luotettavana ja turvallisena toimijana, sekä houkutella kansainvälisiä investointeja. Vaikka standardi tarjoaa ohjeita, valtioiden on itse päätettävä, miten ne saavuttavat vaaditut tavoitteet. Sertifiointi voi parantaa muun muassa riskienhallintaa, kansallista tur-

vallisuutta ja julkishallinnon prosessien sujuvuutta. Se voi myös parantaa sidosryhmäsuhteita ja vähentää kumppaneiden opportunismia. Siitä voi olla myös taloudellisia hyötyjä, joihin kuuluu markkina-arvon nousu ja vakuutuskustannusten aleneminen. Turvallisuusvalvontatoimenpiteiden arviointi ja toteuttaminen voi olla vaikeaa, ja valtioiden onkin sopeutettava standardin vaatimukset omiin tarpeisiinsa. Johtoryhmän sitoutuminen ja poikkihallinnollinen koordinointi ovat tärkeitä onnistuneen toteutuksen kannalta (Gulot ym., 2020).

Myös ISO27002 on Somepallin ym. (2020) mukaan tärkeä tietoturvajohtamisen standardi, joka tarjoaa yleisen oppaan yleisesti hyväksyttyihin tietoturvan hallinnan tavoitteisiin. ISO 27002:n käytännöllisin standardi on opas kehittämään ja organisoimaan turvallisuusasemia, tehokasta turvallisuuden hallintaa ja luottamuksen rakentamista liiketoiminnan jatkuvuuteen organisaatioiden välillä. ISO27002 sisältää 14 pääkohtaa, joita ovat Somepallin ym. (2020) mukaan seuraavat osat:

- Tietoturvastrategiat: Strategiat, joita tarvitaan tietoturvajärjestelmän toteuttamiseen.
- Tietoturvatoimisto: Määrittelee ja noudattaa prosessien ja tietoturvatoimintojen tehtäviä ja toimintoja.
- Henkilöstöturvallisuus: Varmistaa, että työntekijät tietävät roolinsa ja vastuunsa tietoturva-alueella.
- Omaisuuden hallinta: Omaisuuden omistajan tunnistaminen ja vastuu omaisuuden turvallisuudesta, myös luokittelun hallinta, rekisteröinti ja tiedot.
- Pääsynhallinta: Hallitsee pääsyä tietoihin ja suojaa tietoja vahingoilta, menetyksiltä ja muilta uhkilta.
- Salaus: Käyttää salauskontrollia tietojen luottamuksellisuuden, luotettavuuden ja eheyden varmistamiseksi.
- Fyysinen ja ympäristön suojaus: Suojaa tietoja luvattomalta pääsyltä, vahingoilta, häirinnältä, menetyksiltä ja tuhoilta.
- Toiminnan turvallisuus: Yrityksen kyky tarjota petosten ja riskien raportointia tarkasti ja turvallisesti sekä tukea valvontaa ja operatiivisen järjestelmän hallintaa.
- Viestinnän turvallisuus: Suojaa tietoja verkostoissa ja ylläpitää riittävää tietoturvaa ulkoisten medioiden kanssa.
- Pääsy-, kehitys- ja ylläpitojärjestelmät: Sisältää tietojärjestelmien keräämisen ja suunnittelun niiden toteuttamiseksi tietojärjestelmien kehittämisessä.
- Suhde toimittajiin: Kaikkien omaisuuserien ja pääsyn ulkomaisiin toimittajiin on oltava ylläpidettyjä.
- Tietoturvatapahtumien hallinta: Tehokkaat ja asiaankuuluvat strategiat tietoturvatapahtumien käsittelemiseksi.
- Liiketoiminnan jatkuvuuden edistäminen: Tietoturvayhteistyö liiketoiminnan kehittämisjärjestelmissä.
- Tietoturvajärjestelmien noudattaminen: Turvalliset ja suojatut tietoturvajärjestelmät.

Tietoturvajohtaminen on myös oleellinen osa kansallista turvallisuutta Alguliyevin ym. (2021) mukaan. Heidän mukaansa tietoturvajohtaminen auttaa varmistamaan ja turvaamaan teknologisen ympäristön vakautta ja estää ideologisia sekä teknologisia vaikutuksia, jotka voivat horjuttaa yhteiskunnallista ja poliittista vakautta. Tietoturvajohtaminen on myös keskeistä sotilaallisen tiedon suojaamisessa ja sotilaallisten kyvykkyyksien parantamisessa, mikä sisältää esimerkiksi salauksen ja automaattisten ohjausjärjestelmien suojauksen. Myös taloudellisen infrastruktuurin ja tietojärjestelmien suojaaminen on osa tietoturvajohtamista. Tämä kattaa esimerkiksi sähköisten maksujärjestelmien ja taloudellisten tietojen suojauksen. Tämän lisäksi tietoturvajohtaminen on kriittistä energiajärjestelmien turvallisuuden varmistamiseksi. Tämä sisältää energian tuotannon, siirron ja jakelun hallinnan tietoturvan. Tietoturvajohtamisella voidaan myös suojata tärkeää digitaalista oppimateriaalia, sähköisiä tenttejä ja opiskelijoiden tietoja. Tietoturvajohtaminen on välttämätöntä myös terveydenhuollossa potilastietojen ja lääketieteellisten järjestelmien suojaamiseksi. Tämä sisältää muun muassa sähköisten potilastietojärjestelmien ja etälääketieteen suojauksen. Liikennejärjestelmän turvallisuuden kannalta tietoturvajohtaminen kattaa esimerkiksi älykkäät liikenteenhallintajärjestelmät ja henkilökohtaisten tietojen suojauksen. Tietoturvajohtaminen on tärkeää ympäristön ja luonnonvarojen seurantajärjestelmien suojaamiseksi. Tämä voidaan varmistaa esimerkiksi sensoriverkkojen ja tietojärjestelmien suojauksella. Tietoturvajohtaminen ulottuu myös massamediaan ja sen turvallisuuteen median luotettavuuden ja kansallisten etujen suojaamiseksi. Tämä sisältää esimerkiksi väärän tiedon levittämisen estämisen. Tietoturvajohtaminen liittyy tämän lisäksi myös kulttuuriseen ja henkiseen turvallisuuteen, johon sisältyy esimerkiksi digitaalisten kulttuurituotteiden ja perinteiden suojaus. (Alguliyev ym., 2021)

Esimerkiksi Suomessa on olemassa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämistä kokeva laki, TORI-laki, jonka mukaan valtiovarainministeriön tehtävänä on ohjata valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämistä ja palvelujen laatua sekä näiden palvelujen yhteentoimivuutta ja kokonaisarkkitehtuurin mukaisuutta. Valtiovarainministeriön vastuulla on myös palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintätekninen, valmiuden ja turvallisuuden ohjauksen varautuminen. Myös turvallisuusverkkotoiminnan yleishallinnollisesta taloudellisesta ja tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta ja valvonnasta vastaa Suomessa valtiovarainministeriö. Valtiovarainministeriö saa kuitenkin tukea tehtäviinsä valtioneuvoston asettamalta turvallisuusverkkotoiminnan neuvottelukunnalta. (Valtiovarainministeriö, 2024)

Suomessa julkisen hallinnon digi- ja kyberturvallisuutta ohjataan Suomen Digitaalisen kompassin Kokonaisturvalliset julkiset palvelut -tavoitteen mukaisesti. Julkisen hallinnon digi- ja kyberturvallisuuden ohjauksen keskeiset päämäärät ovat lueteltuna kyberturvallisuusstrategiassa 2024, jossa on asetettu tavoitetila, strategiset tavoitteet ja kehittämisehdotukset. Digitaalisten palvelujen tarjoamisesta annetun lain mukaisesti viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu. julkisessa hallinnossa nouda-

tettavat tietoturvallisuustoimenpiteiden vähimmäisvaatimukset on kuvattu julkisen hallinnon tiedonhallinnasta annetussa laissa. (Valtiovarainministeriö, 2024)

4.2 Tietoturvan haavoittuvuudet kriisitilanteissa

Kriisitilanteet voivat synnyttää vakavia haavoittuvuuksia tietoturvalle sekä kyberturvallisuudelle, minkä vuoksi haavoittuvuuksien tunnistaminen on olennainen osa tietoturvaa sekä sen johtamista. Kyberrikokset määritellään kaikiksi luvattomiksi tietokoneavusteisiksi toiminnoiksi, jotka kohdistuvat yrityksen tai yksilön tietoon pahantahtoisella aikomuksella. Kyberrikolliset pääsevät luvattomasti tietoihin varastamaan, väärinkäyttämään ja vaarantamaan tiedon eheyden henkilökohtaisen taloudellisen hyödyn saamiseksi (Chigada & Madzinga, 2021). Kyberrikoksiin voi sisältyä esimerkiksi tietojenkalastelua, roskapostitusta, tietomurtoja, informaation tai identiteettien varkauksia, petoksia, verkkovainoa, kyberkiusaamista, lasten hyväksikäyttöä, kiristystä, osakemarkkinoiden manipulointia, vakoilua, hyökkäyksiä kriittiseen infrastruktuuriin tai tietojärjestelmiin sekä kyberterroria (Lallie, Shepherd, Nurse, Epiphaniou, Maple & Bellekens, 2021.)

On myös olemassa erilaisia ohjelmistoja, joita käytetään kyberrikosten toteuttamiseen. Tällaisia ohjelmistoja ovat esimerkiksi troijalaiset, virukset, botit kuten FriendBot, näppäinlokerot, takaovet, e-skimming-tekniikat, vakoiluohjelmat, kiristysohjelmat, pelotteluohjelmat, mainosohjelmat, madot, haittakoodit ja palvelunestohyökkäykset. Myös lailliset ohjelmat, kuten sähköposti- ja verkkoselaussovellukset, voivat toimia rikosten apuvälineinä, mutta eivät ole sinällään rikollishaittaohjelmia. Kyberrikolliset hyödyntävät myös uutisia, hyperlinkkejä, kuvia, videoita ja sovelluksia rikostensa välineinä. Kyberrikokset voivat kohdistua sekä teknisiin että inhimillisiin kohteisiin esimerkiksi hyödyntäen loppukäyttäjien ja IT-järjestelmien haavoittuvuuksia tehokkaasti (Lallie ym., 2021.).

Kyberturvallisuutta vaarantava tapaus voi olla samanaikaisesti niin tietoturvauhka, rikos, kuin uhka kansalliselle turvallisuudelle ja puolustukselle ja se voi vaikuttaa sekä ulko-, että turvallisuuspolitiikkaan (Finnish Government, 2023.) Chigada ja Madzinga (2021) kirjoittavat, että rikokset ja tietoturvauhat kuten vakoilu, tietojenkalastelu, palvelunestohyökkäykset (DDoS), valeuutisportaalit ja sovellukset ovat lisääntyneet erityisesti koronapandemian aikana. He tunnistavat Covid-19 pandemian aikana yleisimmin esiintyneitä uhkia olevan kiristyshaittaohjelmat, haittaohjelmat, roskapostit, haitalliset verkkotunnukset ja DDoS. Taulukko 1 kuvastaa yleisimpiä uhkia, joita pohjoismaat kohtasivat pandemian aikana ja aiempi kuvio 2 havainnollistaa näiden uhkien vaikutusten jakautumista eri sektoreille sekä merkitystä kansallisen turvallisuuden näkökulmasta. Interpolin tutkimuksen mukaan kyberuhat, kuten tietojenkalastelu, nettihuijaukset sekä muut rikokset lisääntyivät kaiken kaikkiaan 59 prosentilla Covid-19 pandemian seurauksena (Interpol, 2021.)

Kyberrikolliset ovat tunnistaneet COVID-19-misinformaation mahdollisuutena kohdistaa hyökkäyksiä tutkimuslaitoksia, terveydenhuollon organisaatioita, valtion virastoja ja rahoituslaitoksia kohtaan tietäen, että nämä organisaatiot keskittyvät pandemiaan. Korona-aikana lisääntynyt etätyöskentely on heidän mukaansa monista eri syistä yksi suurimmista kyberuhille altistavista tekijöistä. Kirjallisuus viittaa Lallien ym. (2021) mukaan siihen, että kyberrikollisten on helpompaa "murtaa ihmispalomuuri", kuin hyödyntää teknisiä haavoittuvuuksia, eli ihmisten haavoittuvuuksien käyttäminen hyväksi on helpompaa. Muita keskeisiä korona-ajan uhkia ovat haitalliset ja väärennetyt verkkotunnukset, impersonointi, mobiilihyökkäykset, terveysalan haavoittuvuudet sekä rahoitus- ja sosiaalisen median hyökkäykset (Chigada & Madzinga, 2021.)

Ulkoministeriön julkaisun mukaan Maailman terveysjärjestö WHO kertoo, että pandemian lisäksi on kohdattu globaali ”infodemia”, mikä on nähty esimerkiksi väärän tiedon levittämistoimina Venäjän sekä Kiinan toimesta. Sekä EU, että NATO ovat kiinnittäneet tähän huomiota. Myös sairaalat sekä lääkeyhtiöt, lääketieteelliset tutkimusorganisaatiot ja yliopistot ovat kokeneet lisääntynyttä painetta hakkerointitoimista, jotka ovat kriisin aikana lisänneet kyberhyökkäyksiä terveydenhuoltoalalle. Koska COVID-19:n vuoksi terveys- ja geenitietoihin perustuva kysyntä on noussut räjähdysmäisesti globaalisti, se voidaan luokitella hybridiuhaksi. Tämä johtuu siitä, että yritykset, usein valtion yhteyksissä olevat, keräävät biometrisiä tietoja, kuten DNA-näytteitä, yksilöiltä ympäri maailmaa. Tietosuojaviranomaisten ja kokonaisturvallisuus- tai siviilipuolustuslaitosten rooli on analysoida ja ryhtyä toimiin tällaisten uhkien torjumiseksi (Ministry for Foreign Affairs, 2024).

Hansson ym. (2021) kirjoittavat, että COVID-19-pandemian alkuvaiheessa haitallista informaatiota levisi useissa eri muodoissa, mikä vaaransi yhteiskunnan tietoturvallisuuden ja yksilöiden hyvinvoinnin. Erityisesti viestit, jotka väittivät, että suojatoimenpiteet olisivat haitallisia tai tarpeettomia, loivat pelkoa ja heikensivät viranomaisten ohjeistusten uskottavuutta. Samalla jaettiin virheellisiä ja vaarallisia ohjeita viruksen hoitamiseen ja ehkäisyyn, kuten tieteellisesti perustelemattomia terveysvinkkejä, jotka saattoivat altistaa ihmiset todellisille riskeille. Koronaviruksen leviämismekanismeista levitettiin virheellistä tietoa, joka saattoi saada ihmiset uskomaan, että he olivat immuuneja tai epätodennäköisiä sairastumaan jonkin henkilökohtaisen tekijän, kuten veriryhmän tai elämäntapojen, vuoksi. Pandemian vakavuuden vähättely ja vääristely eri kyberkeinojen kautta alensivat riskitietoisuutta ja johtivat mahdollisesti varotoimien laiminlyöntiin. Samalla huijarit hyödynsivät epävarmuutta saadakseen ihmiset ostamaan vääriä suojautumiskeinoja tai paljastamaan luottamuksellisia tietojaan. Tiettyjä yksilöitä ja ryhmiä syytettiin viruksen levittämisestä, mikä johti vihapuheeseen ja häirintään. Nämä haitallisen informaation muodot korostavat kuinka tärkeää on varautua niin teknisiin uhkiin, kuin informaation manipuloinnista johtuviin riskeihin (Hansson ym., 2021). Toisin sanottuna Pandemian aiheuttamat yksittäiset uhat muodostivat myös todellisen ja hyvin vakavan uhan koko kansalliselle turvallisuudelle, mikä teki pandemiasta ja sen aikaisista tietoturva- ja kyberuhista ja -vaikutuksista erittäin vaarallisia.

TAULUKKO 1 Pohjoismaiden yleisimmät kyberuhat covid-19 pandemian aikana.

Maa	**Yleisimmät tietoturvauhkat**	**Lähteet**
Suomi	COVID-19 aiheiset tietojenkalastelu-viestit, kiristysohjelmat terveydenhuollon toimijoita vastaan.	(ENISA, 2020, 2021) (Traficom Kyberturvallisuuskeskus, 2021)
Ruotsi	Terveydenhuoltoa ja julkista sektoria koskevat toimitusketjuhyökkäykset, valeverkkosivustot liittyen rokotuksiin, tietojenkalastelu.	(ENISA, 2021) (Myndigheten för samhällsskydd och beredskap, 2020)
Norja	Kiristysohjelmat terveydenhuollossa, palvelunestohyökkäykset kriittiseen infrastruktuuriin.	(ENISA, 2021) (Nasjonal sikkerhetsmyndighet, 2020)
Tanska	Etätyöntekijöihin kohdistuneet tietojenkalasteluviestit, toimitusketjun haavoittuvuudet hallituksen virastoissa.	(ENISA, 2022) (Center for Cybersikkerhed, 2020)
Islanti	Tietojenkalastelu ja sosiaalisen manipuloinnin hyökkäykset pienempiin terveydenhuollon laitoksiin ja yrityksiin etätyön takia.	(ENISA, 2020) (Agustsdottir, 2024) (Islannin hallitus, 2022)

Myös Ukrainan sota on aiheuttanut vakavaa uhkaa pohjoismaille monilla eri tavoilla, minkä vuoksi pohjoismaiden yhteisen kyberturvallisuusstrategian luomiselle on esitetty tarve vuonna 2022 (Ministry of Foreign Affairs, 2024.) Vaikka sota onkin kohdistettu Ukrainaan, näkyvät sen vaikutukset paljon laajemmin, mikä johtuu kyberavaruuden luontaisesta yhteenliitettävyydestä. Kyberhyökkäysten leviämisvaikutus yhdistettynä laajaan hyökkääjien joukkoon tarkoittaa, että mikä tahansa maa voi joutua niiden kohteeksi. Kriittinen infrastruktuuri on ollut säännöllinen kohde Ukrainan sodassa. Koska kaikki välttämättömät palvelut ovat riippuvaisia tieto- ja viestintätekniikasta sekä tiedon käsittelystä ja siirrosta verkossa, on kohteena oleviin organisaatioihin ja hallituksiin kohdistuva vaikutus ollut huomattava (*European parliament*, 2023). Ukrainan sodan vuoksi kyberhyökkäykset ovat yleistyneet ympäri maailmaa ja sekä valtion, että paikallishallinnon toimijat ja yritykset ovat joutuneet niiden kohteeksi myös Suomessa (Valtioneuvosto, 2022.)

Euroopan parlamentin mukaan toukokuuhun 2023 mennessä raportoituja kyberhyökkäyksiä kirjattiin 1998 ja ne kohdistuivat Ukrainan lisäksi noin 49 muuhun valtioon ja 23 eri kriittisen infrastruktuurin sektoriin (*European parliament*, 2023.) Hyökkäyksiä on toteutettu tietojen ja järjestelmien tuhoamiseksi, kriittisen infrastruktuurin ja palveluiden häiritsemiseksi, informaatiotilan hallinnan saavuttamiseksi, merkittävien tietomäärien anastamiseksi, tiedusteluseksä vakoilutarkoituksiin ja vaikutusoperaatioiden toteuttamiseksi. Tämä on tehty sillä tarkoituksella, että luottamus julkiseen tietoon ja instituutioihin murenee. Ne myös luovat hämmennystä ja mustamaalaavat sotivia osapuolia ja heidän liittolaisiaan sektoriin (*European parliament*, 2023). Euroopan parlamentti

on jaotellut hyökkäykset tuhoisiin hyökkäyksiin, häiritseviin hyökkäyksiin, tietojen aseistamiseen ja disinformaatioon. Tuhoisia ovat hyökkäykset, joiden tavoitteena on tietojen pysyvä poistaminen tai järjestelmien vahingoittaminen siten, että ne eivät ole palautettavissa. Esimerkiksi haittaohjelmat lukeutuvat niihin. Häiritsevät hyökkäykset, kuten palvelunestohyökkäykset, joiden tavoitteena on palveluiden ja toimintojen häirintä, ovat olleet merkittävässä roolissa konfliktin aikana. Tietojen aseistamisella viitataan hyökkäyksiin, jotka johtavat tietojen varastamiseen tai anastamiseen tai tietojen hankkimiseen vakoilu-, valvonta- tai tiedustelutarkoituksiin. Tämä voi tapahtua muun muassa tietojenkalasteluviestien muodossa. Disinformaatioon ja propagandaan perustuvat operaatiot ovat myös saavuttaneet ennenäkemättömän laajuuden (European parliament, 2023).

Valtioneuvoston mukaan Suomeen kohdistuvat kyberoperaatiot ovat olleet Ukrainan sodan aikana odotettavissa (Valtioneuvosto, 2022.) Kuitenkin Kaczmarekin (2023) mukaan Lukuun ottamatta muutamia hyökkäyksiä, kuten eduskunnan verkkosivujen keskeyttämistä, ei vakavista kyberhyökkäyksistä Suomea vastaan ole tietoa. Hän kertoo tämän olevan seurausta joko onnistuneesta hyökkäysten salaamisesta, Venäjän vihamieleisten hyökkäysten mahdollisuuden yliarvioinnista, tai täydellistä valmistautuneisuutta torjua kaikki hyökkäykset (Kaczmarek, 2023.). Myöskään Islanti ei ole suora kohde Ukrainan sodan aiheuttamille tietoturva- ja kyberuhille, vaikka myös he, kuten muut pohjoismaat ovat osoittaneet tukea ukrainalle (*CERT-IS*, 2022.)

Esimerkiksi Tanskaan kohdistuvat kyberuhat ovat olleet kyberturvallisuuskeskus CFCS: n mukaan vakavia jo pitkään. Ulkomaalaiset valtiot sekä erityisesti hakkerit ovat merkittävin Tanskaa kohtaava uhka, muun muassa Venäjä kohdistaa säännöllisesti kyberhyökkäyksiä Tanskan julkisia viranomaisia ja yksityisiä yrityksiä vastaan. Osa näistä hyökkäyksistä tehdään suoraan vastauksena Ukrainan sotaan, mutta kyberhyökkäykset ovat olleet jatkuva haaste jo ennen Venäjän hyökkäystä – ja ne tulevat olemaan huolenaihe riippumatta sodasta (CFCS, 2022). CFCS: n raportin mukaan kybervakoilun uhka Tanskaa vastaan on edelleen erittäin korkea, huolimatta Ukrainan sodasta. Myös kyberrikollisuuden uhka on erittäin korkea. Tanska kohtaa näitä uhkia huolimatta venäjän hyökkäyksestä Ukrainaan, joten vakavuus on pysynyt samana (CFCS, 2024).

Ruotsissa ja Norjassa on CERT-EU:n mukaan raportoitu vähemmän kyberhyökkäyksiä venäjän sodan takia, kuin esimerkiksi Suomessa (CERT-EU, 2023.) Vaikka pohjoismaat eivät olekaan varsinaisesti suoria kohteita, se ei tarkoita, etteikö uhkaa olisi ja, että niissä ei varauduttaisi ja valmistauduttaisi mahdollisiin uhkiin tai valtioiden rajoja ylittäviin uhkiin.

4.3 Kriisijohtaminen ja tietoturvan sopeuttaminen siihen

Kuvion 2 avulla voidaan hahmottaa, miten eri tietoturvan osa-alueet ovat haavoittuvaisia kriisitilanteissa. Esimerkiksi sosiaalisen ja poliittisen turvallisuuden näkökulmasta disinformaatio ja väärä tieto voivat heikentää kansalaisten luottamusta esimerkiksi viranomaisiin ja lisätä sosiaalista epävarmuutta kriisitilanteissa (Hansson ym., 2021). Ekonominen turvallisuus, jossa taloudelliset menetykset ja kyberrikollisuus, kuten tietojenkalastelu ja kiristysohjelmat, voivat kohdistua yrityksiin sekä yksityishenkilöihin kriisien aikana (Chigada & Madzinga, 2021). Sotilaallisen turvallisuuden kannalta taas kyberhyökkäykset kriittiseen infrastruktuuriin ja sotilaallisiin kohteisiin voivat heikentää valtion puolustuskykyä (Willett, 2022.) Tieteellisessä ja teknologisessa turvallisuudessa kyberhyökkäykset terveydenhuoltojärjestelmiin ja tieteelliseen infrastruktuuriin voivat vaarantaa kriittistä tietoa ja teknologiaa (Alawida ym., 2022.) Tämän vuoksi on tärkeää tarkastella valtioiden kriisinhallintamalleja erityisesti tietoturvan osalta, jotta voidaan estää ja hillitä näiden seikkojen mahdolliset laajat negatiiviset vaikutukset kansalliselle turvallisuudelle.

Kriisijohtamisen onnistuminen edellyttää selkeitä toimintamalleja, jotka tukevat tietoturvan joustavaa sopeuttamista erityisesti kriiseissä, jotka vaikuttavat informaatioympäristössä. On tärkeää, että organisaatioilla ja viranomaisilla on valmiudet havaita ja torjua tietoturvauhat ajoissa sekä hallita niitä tehokkaasti. Tämä on tärkeää erityisesti kriisien, kuten pandemioiden ja sotien, jotka lisäävät kyberuhkien todennäköisyyttä ja vaikutuksia aikana. Pohjoismaat seuraavat erilaisia direktiivejä, lakeja, säännöksiä ja suosituksia tietoturvan ja kyberturvan takaamiseksi valtiollisella tasolla, mutta myös konkreettisia kriisinhallinnan toimia on tehty. Tietoturvan johtaminen ei rajoitu pohjoismaissa ainoastaan EU:n lainsäädännön ja sääntelyn noudattamiseen, vaikka ne muodostavatkin merkittävän perustan tietoturvakäytäntöjen kehittämiselle ja ylläpitämiselle

Minkä tahansa johtamisen onnistuminen on kytköksissä suunnitteluun ja strategiaan, ja Covid-19-pandemia ja Ukrainan sota eivät ole poikkeuksia tässä suhteessa. Interpolin kyberstrategiaraportin mukaan onnistunut kyberturvallisuusstrategia koostuu kuudesta osasta: strategian valmistelu, strategian muotoilu, strategian hyväksyminen, toteutus, seuranta ja arviointi sekä mukautukset ja innovaatiot (Interpol, 2021.) EU:n kyberkriisinhallinta tapahtuu eri EU-laitosten ja -virastojen kautta kriisin tyypin mukaan. Kyberkriisien hallintaan sovelletaan EU:n kriisinhallintamekanismeja, kuten neuvoston integroidun politiikan vastauksen mekanismia IPCR:ää ja komission ARGUS-järjestelmää. Näiden mekanismien avulla EU tavoittelee parempaa kyberkriisien hallintaa, joka on tiiviisti kytkeytynyt myös jäsenvaltioiden kansallisiin suunnitelmiin (ENISA, 2024).

Lähtökohtana valtioiden kyberturvallisuudelle toimii EU:n kyberturvallisuusdirektiivi NIS2, jonka mukaan kansallista kyberturvallisuusstrategiaa päivitetään viiden vuoden välein, painottamalla parhaiden käytäntöjen tunnistamista ja poikkeustilanteista opittujen toimintatapojen laajaa hyödyntämistä. Valtiot myös mitoittavat kyberresilienssiään, eli kyberuhkien sietokykyä, jotta

ne voivat luoda kokonaisturvallisuuden päämäärien mukaisen varautumis- ja ennakointikyvyn, toimintakyvyn kyberhäiriötilanteissa ja jälkitoipumiskyvyn (Kyberturvallisuusstrategia, 2019.). Taulukosta 2 nähdään, millaisia toimia pohjoismaat ovat tehneet kansallisen turvallisuuden eri sektoreilla tietoturva- ja kyberuhkiin vastaamiseksi tutkielmassa tarkasteltujen lähteiden pohjalta. Taulukko vastaa tutkielman tutkimuskysymykseen kansallisen turvallisuuden näkökulmasta hahmottamalla, miten kukin pohjoismaa on toiminut kyberuhkien suhteen käsiteltyjen kriisien aikana ja johdosta.

TAULUKKO 2 Tietoturvajohtamistoimet pohjoismaissa

Turvallisuuden osa-alue	**Suomi**	**Ruotsi**	**Norja**	**Tanska**	**Islanti**	**Lähteet**
Tietoturva	Kansallinen kyberturvallisuusstrategia, viranomaisten välinen yhteistyö, kyberpuolustuksen kehittäminen	Kansallinen kyberturvallisuuskeskus, viranomaisten yhteistyö	Digitaalisen turvallisuuden edistäminen, ennakoivat toimenpiteet	Kyberturvallisuuskeskus, kansalliset ja alakohtaiset uhkaarvioinnit	Digitaalisen muutoksen strategiat, kansainvälinen yhteistyö	(Kyberturvallisuusstrategia, 2024) (Strengthening civil preparedness, 2021) (Nasjonalt digitalt risikobilde, 2021) (Danish Cyber and Information Security Strategy, 2022) (Government of Iceland, 2020)
Sosiaalipoliittinen turvallisuus	Disinformaation torjunta, kansalaisten luottamuksen ylläpito	COVID-19-huhujen ja disinformaation torjunta	Digitaalisten haavoittuvuuksien hallinta, riskin pienentämistoimet	Kansalaisten tiedottaminen ja ohjeistus	Ihmisoikeuksien suojelu verkossa	(Hansson ym., 2021) (Regeringskansliet, 2021) (Nasjonalt digitalt risikobilde, 2021) (Danish govern-

						ment, 2021)

Sotilaallinen turvallisuus	Kyberpuolustuksen vahvistaminen, yhteistyö NATO:n kanssa	Asevoimien ja turvallisuuspalvelun yhteistyö	Totaalisen puolustuksen ylläpito, kansainvälinen yhteistyö	Puolustusministeriön koordinoima strategia	Kansainvälinen yhteistyö kyberuhkien torjunnassa	(Revised Cyber Security Strategy Responds to Changed Security Environment, 2024) (Strengthening civil preparedness, 2021) (Nasjonalt digitalt risikobilde, 2021) (Danish government, 2021) (Government of Iceland, 2020)
Taloudellinen turvallisuus	Kyberrikollisuuden torjunta, yritysten suojaaminen	Investoinnit käytännön suojelutoimiin	Julkisen ja yksityisen sektorin yhteistyö	Yritysten digitaalisen turvallisuuden vahvistaminen	Kilpailukyvyn lisääminen, turvallinen infrastruktuuri	(Chigada & Madzinga, 2021) (Regeringskansliet, 2021) (Nasjonalt digitalt risikobilde, 2021) (Danish government, 2021) (Government of Iceland, 2020)
Koulutuksen turvallisuus	Kyberosaamisen kehittäminen	Ei mainintaa	Ei mainintaa	Ei mainintaa	Ei mainintaa	(Kyberturvallisuusstrategia, 2024)
Terveydenhuollon turvallisuus	Kyberhyökkäysten torjunta terveydenhuoltojärjestelmissä	Ei mainintaa	Ei mainintaa	Ei mainintaa	Ei mainintaa	(Alawida ym., 2022)

Media- ja viestintä-turvalli-suus	Suojatut viestintäjär-jestelmät	COVID-19-huhujen ja disin-formaa-tion tor-junta	Ei mai-nintaa	Viestin-täverkko-jen tur-vallisuu-den pa-rantami-nen	Ei mai-nintaa	(Johansson ym., 2023) (Regering-skansliet, 2021) (Dan-ish govern-ment, 2021)
Ympäris-töturval-lisuus	Ei mainintaa	Ei mai-nintaa	Ei mai-nintaa	Ei mai-nintaa	Vihreän siirty-män edistä-minen	(Govern-ment of Ice-land, 2020)
Tiede- ja teknolo-giaturval-lisuus	Kyberhyök-käysten tor-junta tieteel-lisessä infra-struktuurissa	Ei mai-nintaa	Ei mai-nintaa	Ei mai-nintaa	Teko-älypoli-tiikka ja turvalli-suus-haasteet	(Kyberturval-lisuusstrate gia, 2024) (Govern-ment of Ice-land, 2020)

Jokaisella pohjoismaalla on omat kyberturvallisuusstrategiansa, minkä osalta tietoturvajohtaminen on näiden valtioiden kannalta onnistunutta. Esimerkiksi Suomen kyberturvallisuusstrategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus (Kyberturvallisuusstrategia, 2019) Suomen kyberturvallisuusstrategia keskittyy kansalliseen yhteistyöhön, elintärkeiden toimintojen turvaamiseen, toimintakyvyn kehittämiseen, poliisin valmiuksien parantamiseen, puolustuskyvyn varmistamiseen, kansainväliseen yhteistyöhön ja kyberosaamisen kehittämiseen (kyberturvallisuusstrategia, 2019) Suomi on myös vahvistanut ja kehittänyt viranomaisten välistä yhteistyötä systemaattisesti. Tämä sisältää eri sektoreiden hallinnonalojen välisen tiiviin yhteistyön ja prosessien parantamisen, jotta kyberuhkiin voidaan vastata tehokkaasti (Revised Cyber Security Strategy Responds to Changed Security Environment, 2024). Suomen viranomaiset ovat parantaneet valmiuttaan torjua vakavia kyberuhkia, mikä on sisältänyt kyberpuolustuksen kehittämistä ja kyberrikollisuuden torjuntaa koskevien toimenpiteiden tehostamista (Finnish government, 2023). Suomi on myös lisännyt yhteistyötä kansainvälisten kumppaneiden, kuten NATO:n ja EU:n kanssa kyberturvallisuuden parantamiseksi. Tämä yhteistyö on ollut keskeistä erityisesti pandemian aikana, jolloin kyberuhkien määrä on kasvanut (Revised Cyber Security Strategy Responds to Changed Security Environment, 2024)

Suomi on reagoinut Venäjän hyökkäykseen Ukrainaan monin tavoin tietoturvan ja kyberturvan osalta esimerkiksi kansallisen kyberturvallisuuden ja kyberpuolustuksen vahvistamiseksi (Valtioneuvosto, 2022.) Valtioneuvoston mu-

kaan kyberturvallisuuskeskus on antanut tarkempia ohjeita ja tukea kriittisten organisaatioiden valmiuden parantamiseksi. Lisäksi kansallisten tietoverkkojen ja tietoresurssien suojaamista on tehostettu. Yhteistyö viranomaisten välillä, kuten kyberturvallisuuskeskuksen, poliisin, tiedusteluviranomaisten ja puolustusvoimien kesken, on tiivistynyt kansallisen kyberturvallisuuden varmistamiseksi ja kyberhyökkäysten estämiseksi. Siviili- ja sotilasviranomaisten yhteistyötä on myös tehostettu ja tiedonvaihtoa parannettu (Valtioneuvosto, 2022). Valtioneuvoston raportin mukaan kybervalmiuden parantamiseksi on järjestetty säännöllisesti kybervalmiusharjoituksia julkisen ja yksityisen sektorin yhteistyönä. Suomessa on myös pyritty kehittämään kyberturvallisuuden ekosysteemiä, joka tuo yhteen julkisen ja yksityisen sektorin toimijat. Digitaalisten ja kyberturvallisuustaitojen parantaminen kaikilla tasoilla, mukaan lukien yritykset, organisaatiot ja kansalaiset, on myös ollut keskeisessä roolissa. Myös lainsäädäntöä on raportin mukaan uudistettu. Esimerkiksi sähköisen viestinnän palveluista annettua lakia, joka parantaa viestintäverkkojen turvallisuutta on uudistettu. Lisäksi valmiuslakia on uudistettu hybridivaikuttamistilanteiden huomioimiseksi (Valtioneuvosto, 2022). Nämä toimenpiteet osoittavat Suomen kattavan lähestymistavan ja valmistautumisen kyberturvallisuuden ja tietoturvan vahvistamiseksi muuttuvassa turvallisuusympäristössä.

Toisaalta esimerkiksi Simola (2022) esittää, että suomen toimet kyberturvallisuuden takaamiseksi eivät ole riittäviä. Hänen mukaansa Suomessa ei ole toimivia komento- ja valvontaelimiä odottamattomiin kriiseihin varautumiseksi. Vaikka presidentti johtaa ulkopolitiikkaa yhdessä hallituksen kanssa, hänellä ei ole operatiivista komentajan roolia maan sisäisissä asioissa. COVID-19-pandemia on Simolan mukaan paljastanut puutteita viranomaisten ja poliitikkojen välisessä tiedonvaihdossa, ja kansalaiset ovat jääneet tietämättömiksi noudatettavista ohjeista. Simolan (2022) mielestä se, että yksi työntekijä vastaa kaikista tietoturvaan ja yksityisyydensuojaan liittyvistä asioista tai, että yritykset luottavat omatoimivalvontaan erityisesti terveydenhuollon sektorilla ei ole riittävää, erityisesti kun rikolliset voivat käyttää yksityisiä tietoja vaarallisilla tavoilla, kuten kiristämällä päätöksentekoprosessiin vaikuttamiseksi. Vastaamo-tapauksessa tietovuodon havaitsemisessa kesti lähes kaksi vuotta. Ei ole ratkaisevia esteitä ehdotetun hybridihätätilajärjestelmän käyttöönotolle älykkäässä kaupunki-infrastruktuurissa (Cyber Security: Critical Infrastructure Protection, 2022.).

Ruotsi taas on vastannut koronan luomiin kyberturvauhkiin tekemällä yhteistyötä EU:n ja muiden toimijoiden kanssa, erityisesti torjuakseen COVID-19-virukseen liittyviä huhuja ja disinformaatiota (Regeringskansliet, 2021). Ruotsi priorisoi investointeja käytännön suojelutoimiin ja perusti tämän takia myös kansallisen kyberturvallisuuskeskuksen. Keskukseen kuuluvat Ruotsin asevoimat, Ruotsin turvallisuuspalvelu, puolustusvoimien radioasema ja MSB, eli Swedish Civil Contingencies Agency. Keskuksen tehtävänä on yhdistää tehtävät ja toimet Ruotsin kyvyn vahvistamiseksi sekä estää, havaita ja vastata vihamielisiin kyberuhkiin. Keskus tukee yksityisiä ja julkisia toimijoita kyberhyökkäyksiltä suojautumisessa. Keskus tekee tiivistä yhteistyötä poliisiviranomaisten, puolustusmateriaalilaitoksen sekä posti- ja telehallituksen kanssa (Strengthening civil preparedness, 2021).

Norja taas esimerkiksi kommunikoi eri virastojen kesken. Uusien digitaalisten haavoittuvuuksien myötä on syntynyt tarve uusille riskin pienentämistoimille ja Norja onkin mukauttanut ohjeita, varoituksia ja suosituksia uuteen digitaaliseen ympäristöön sekä arkeen sopiviksi. Sekä julkinen, että yksityinen sektori ovat osoittaneet kykyä mobilisoitua poikkeustilanteissa keskittymällä digitaalisen turvallisuuden edistämiseen (Nasjonalt digitalt risikobilde, 2021). Monet pandemian nopeuttamat digitaaliset ratkaisut ja haavoittuvuudet ovat Norjassa pysyviä ratkaisuja. Norjassa kaikilla organisaatioilla on vastuu huolehtia omasta digitaalisen turvallisuuden tasostaan, mutta mikään taho, ei viranomaiset, organisaatiot tai kansalaiset, voi yksinään hallita digitaalisia haasteita. Totaalisen puolustuksen ylläpitämiseksi on tärkeää, että digitaalinen turvallisuustyö seuraa nopeaa digitalisaatiota. Rakenteellinen yhteistyö kansallisten ja kansainvälisten kumppaneiden sekä eri sektoreiden välillä on ratkaisevaa, jotta voidaan estää, havaita ja käsitellä digitaalisia tapahtumia, jotka vaikuttavat Norjan kansallisiin arvoihin. Norjan kyberturvallisuuskeskus NCSC ylläpitää ajantasaista riskikuvaa digitaalisessa tilassa ja teki näin myös kyseisten uhkien kohdalla. Keskeinen väline uhkien torjumiseksi on vahvistettu julkisen ja yksityisen sektorin yhteistyö, mutta myös ennakoivaa työtä käytetään vähentämään digitaalista riskiä. Norjan yhteinen tavoite on luoda kestävyyttä ennakoivilla toimenpiteillä ja kyvyllä torjua, havaita ja estää uhkia. Viranomaiset ovat edistäneet yhteistyötä ja kehittäneet ennaltaehkäiseviä toimenpiteitä, jotka auttavat suojaamaan yhteiskunnan digitaalisia järjestelmiä ja varmistamaan kriittisten toimintojen jatkuvuuden. Norja on myös pyrkinyt antamaan ohjeita digitaalisiin palveluihin ja ohjelmistoihin, mikä tarkoittaa niin teknisesti turvallisen vaalitoteutuksen tukemista, kuin kansan vaikutusvaltaisen ja salaisen manipuloinnin estämistä (Nasjonalt digitalt risikobilde, 2021).

Tanskan hallitus on määritellyt neljä strategista tavoitetta, jotka luovat perustan vahvemman ja turvallisemman digitaalisen Tanskan kehittämiselle. Näistä ensimmäinen on yhteiskunnan elintärkeiden toimintojen vahva suojaaminen. Tanska pyrkii siis ylläpitämään yhteiskunnalle ja taloudelliselle toiminnalle välttämättömiä toimintoja kriisitilanteessa, jossa kriittinen ICT-infrastruktuuri on toimimaton lyhyen tai pidemmän ajan. Toinen on taitojen ja johdon sitoutumisen tason nostaminen. Tämä tarkoittaa, että kyber- ja tietoturvallisuuden on oltava ylimmän johdon sitoutumisen kohteena, ja taitoja on vahvistettava. Tämä koskee omaisuuserien, haavoittuvuuksien ja mahdollisten uhkien tuntemusta. Kolmas tavoite on julkisen ja yksityisen sektorin yhteistyön vahvistaminen, minkä eteen valtion virastojen ja yritysten on tehtävä tiiviimpää yhteistyötä ja jaettava tietoa ja kokemuksia uhkista ja tapahtumista. Neljäs on aktiivinen osallistuminen kansainväliseen kyberuhkien torjuntaan. Kansainvälistä yhteistyötä EU:ssa, YK:ssa, NATO:ssa ja samanmielisten maiden kanssa on vahvistettava. Kyberhyökkäysten tekeminen Tanskaa vastaan on tehtävä vaikeaksi ja seuraukselliseksi (Danish Cyber and Information Security Strategy, 2022.)

Tanskassa Kyberturvallisuuskeskus on kansallinen ICT-turvallisuusviranomainen, joka vastaa useista ennaltaehkäisevistä ja lieventävistä tehtävistä, mukaan lukien neuvontapalveluista. Kyberturvallisuuskeskuksen infrastruktuuri- ja internet-turvallisuuspalvelu voi auttaa havaitsemaan ja

varoittamaan edistyneistä kyberhyökkäyksistä viranomaisille ja yrityksille, jotka tilaavat palvelun. Kyberturvallisuuskeskus myös varoittaa viranomaisia ja yrityksiä erityisistä kyberuhkista ja laatii myös kansallisia ja alakohtaisia tilannekatsauksia ja uhka-arviointeja (Danish government, 2021). Poliisi vastaa Tanskassa IT-rikollisuuden ehkäisystä ja tutkinnasta sekä tällaisen rikollisuuden pysäyttämisestä. Poliisi toimii myös koordinoivana tahona suurten, sektorirajat ylittävien tapahtumien yhteydessä (Danish government, 2021). Tanskan turvallisuus- ja tiedustelupalvelu tarjoaa konsultointia ja apua julkisille viranomaisille ja yksityisille yrityksille turvallisuusasioissa ja se onkin Tanskan kansallinen turvallisuusviranomainen. Tanskan digitaalihallinnon virasto puolestaan tukee tietoturvallisuutta julkisella sektorilla ja ohjeistaa ISO 27001 -standardista ja vaatimusten asettamisesta valtion virastoille osana hallituksen ICT-portfolion hallintaa. Lisäksi virasto toteuttaa useita kansalaisiin keskittyviä tiedotustehtäviä, kuten Sikkerdigital.dk ja identiteettivarkaushotline. Virasto vastaa myös strategian toteuttamisen koordinoinnista yhteistyössä puolustusministeriön kanssa. (Danish government, 2021). Tanskan yritysvirasto vastaa tiedon, ohjeiden ja työkalujen kehittämisestä ja tarjoamisesta sekä toimien koordinoinnista, joiden tavoitteena on vahvistaa digitaalista turvallisuutta laajemmassa yritysyhteisössä, erityisesti pk-yrityksissä (Danish government, 2021).

Islanti taas on julkaissut useita tietotekniikkaan ja digitaaliseen muutokseen liittyviä politiikkoja ja strategioita, joita on kehitetty sekä valtion että paikallisviranomaisten toimesta. Näihin kuuluvat muun muassa julkisten palveluiden digitaalinen strategia vuodelta 2021, jonka tavoitteina ovat kilpailukyvyn lisääminen, paremmat julkiset palvelut, turvallisempi infrastruktuuri ja nykyaikaisempi työympäristö (Government of Iceland, 2024). Pilvipalvelupolitiikka vuodelta 2022 keskittyy tietojärjestelmien ja tietojen turvallisuuden lisäämiseen, tehokkaampiin palveluihin ja innovaatioiden edistämiseen. Kyberturvallisuusstrategian vuodelta 2021 tavoitteina ovat poikkeuksellinen osaaminen ja turvallinen internetympäristö. Tekoälypolitiikka vuodelta 2021 pyrkii puolestaan eettiseen tekoälyn kehittämiseen ja turvallisuushaasteiden ymmärtämiseen (Government of Iceland, 2024).

Islanti keskittyy digitaalisen muutoksen strategioihin, joiden tavoitteena on tarjota tehokkaampia julkisia palveluja, edistää vihreää siirtymää ja hyödyntää teknologiaa älykkäästi. Vahva tekninen infrastruktuuri ja kansalaisten kasvavat odotukset tukevat näitä pyrkimyksiä. Islanti painottaa kyberturvallisuuden ja yhteiskunnallisen resilienssin ylläpitoa sekä kansainvälisen yhteistyön merkitystä kyberuhkien torjunnassa. Lisäksi Islanti korostaa YK:n hyväksymien raporttien ja kansainvälisen oikeuden soveltamista kyberavaruudessa. Islanti korostaa myös vastuullisten tahojen tilille saattamista haitallisesta kybertoiminnasta ja tukee kansainvälistä apua kapasiteetin kehittämiseen. Kyberturvallisuustoimien tulee Islannin hallituksen mukaan edistää myös ihmisoikeuksien suojelua verkossa (Government of Iceland, 2024).

Pohjoismaat ovat ottaneet käyttöön monipuolisesti erilaisia strategioita tietoturvan ja kyberturvallisuuden takaamiseksi kriisitilanteissa. Kaikki pohjoismaat myös korostavat kansainvälisen yhteistyön merkitystä, teknologian hyödyntämistä sekä jatkuvaa kehittämistä. Suomi on parantanut kyberpuolustustaan ja kehittänyt viranomaisten välistä yhteistyötä, Ruotsi on perustanut kan-

sallisen kyberturvallisuuskeskuksen, joka yhdistää eri viranomaisten toimet. Norja taas on mukauttanut ohjeita ja suosituksia digitaalisen turvallisuuden edistämiseksi ja keskittyy ennakointiin ja torjumiseen. Tanska on puolestaan kehittänyt integroidun kriisinhallintajärjestelmän, joka yhdistää eri viranomaisten ja organisaatioiden tietojärjestelmiä. Islanti keskittyy digitaalisen muutoksen strategioihin ja kansainväliseen yhteistyöhön kyberuhkien torjunnassa.

Kansallisen turvallisuuden näkökulmasta jokainen sektori on altis tietoturvauhille, minkä vuoksi on hyvä, että valtiot ovat myös kehittäneet sektorikohtaisia puolustustoimia, kuten Tanskan kyberturvallisuuskeskus, joka laatii myös kansallisia ja alakohtaisia tilannekatsauksia ja uhka-arviointeja (Danish Cyber and Information Security Strategy, 2022) Tämä kokonaisvaltainen lähestymistapa varmistaa, että maat pystyvät tehokkaasti vastaamaan nykyisiin ja tuleviin kyberuhkiin, suojaten samalla kansalaistensa ja organisaatioidensa turvallisuutta.

Pandemian aikana Pohjoismaat ovat laajentaneet digitaalisten ratkaisujen käyttöä, erityisesti julkisen ja yksityisen sektorin välisen yhteistyön parantamiseksi. Esimerkiksi Norjassa, Ruotsissa ja Suomessa hyödynnettiin erilaisia digitaalisia alustoja koordinoimaan kriisiajan toimia. Nämä järjestelmät osoittautuivat erityisen hyödyllisiksi rokotusohjelmien organisoinnissa sekä terveydenhuollon resurssien seurannassa ja hallinnassa (Johansson, Ihlen, Lind-holm & Blach-Ørsten, 2023). Lisäksi Pohjoismaat ovat kiinnittäneet erityistä huomiota kyberturvallisuuden vahvistamiseen kriittisen infrastruktuurin suojelemiseksi kyberuhkilta. DDoS-hyökkäysten torjunta ja suojatut viestintäjärjestelmät ovat olleet keskeisiä keinoja. Suomen ja Ruotsin viranomaiset ovat myös ottaneet käyttöön kyberturvallisuusohjelmia, joissa hyödynnetään analytiikkaa ja varhaisen varoituksen järjestelmiä kyberuhkiin ennalta varautuessa (Johansson ym., 2023). Ruotsissa ja Tanskassa tekoälyn ja automaation käyttö on tukenut resurssien kohdentamista ja tehostanut näin julkisten palveluiden päätöksentekoa kriisiaikana. Näiden teknologioiden avulla pandemiaan liittyviä haasteita pystyttiin ratkaisemaan nopeammin ja tehokkaammin (Johansson ym., 2023).

Voidaan siis todeta, että pohjoismaat ovat valmistautuneita kohtaamaan ja käsittelemään tietoturvaa kriisitilanteissa. Ne ovat kehittäneet kattavia strategioita ja toimintamalleja, jotka tukevat tietoturvan joustavaa sopeuttamista ja kriisinhallintaa. Yhteistyö kansallisten ja kansainvälisten toimijoiden välillä on keskeisessä roolissa, ja pohjoismaat ovat sitoutuneet jatkuvaan kehittämiseen ja parantamiseen tietoturvan ja kyberturvallisuuden alalla.

5 Yhteenveto

Tämän Kandidaatintutkielman tavoitteena oli tutkia kriisitilanteiden luomien kyberuhkien hallintaa pohjoismaissa. Tutkielma toteutettiin kirjallisuuskatsauksena, jossa lähteiden hakemiseen käytettiin useita eri tietokantoja, kuten JYKDOK, Google Scholar ja Scopus. Tutkielmassa käytiin läpi Covid-19 pandemian ja Ukrainan sodan aikana ilmenneitä yleisimpiä tietoturva- ja kyberturvallisuus uhkia kussakin pohjoismaassa sekä sitä, miten pohjoismaiden valtiot valmistautuivat ja reagoivat niihin. Tutkielman aiheenvalinta perustui sen erittäin ajankohtaiseen luonteeseen, mikä myös rajasi tarkastelun 2020-luvulla ja siitä eteenpäin vaikuttaneisiin kriisitilanteisiin. Aiheenvalintaa pohjusti myös digitalisaation nopea kehitys, ja sen myötä kasvanut tietoturvan merkitys, uhat ja mahdollisuudet. Tutkielman tarkoituksena oli syventää ymmärrystä konkreettisista toimista uhkiin valmistautumiseen sekä niihin vastaamiseen ja erityisesti tietoturva- ja kyberuhkiin, sillä ne eivät ole samalla tavalla nähtävissä, kuin monet muut uhat. Tämän tutkielman tavoitteena oli vastata tutkimuskysymykseen:

- Miten pohjoismaisten valtioiden johdot kohtaavat ja käsittelevät tietoturvaa kriisitilanteissa?

Ennen tutkimuskysymykseen vastaamista tutkielmassa pyrittiin luomaan kattava käsitys tietoturvasta, kyberturvasta ja kriisinhallinnasta sekä niiden merkityksestä valtiollisella tasolla. Aluksi määriteltiin, mitä tietoturva on, mistä se koostuu ja miten se ilmenee valtiotasolla. Tutkielmassa tarkasteltiin, miten eri viranomaiset vastaavat tietoturvasta Pohjoismaissa, erityisesti Suomessa. Lisäksi esiteltiin erilaisia strategioita ja toimia, joita Pohjoismaiden hallitukset noudattavat tietoturvan takaamiseksi kansalaisilleen.

Seuraavaksi käsiteltiin kriisejä, niiden hallintaa ja vaikutuksia valtion näkökulmasta. Tutkielmassa pyrittiin antamaan selkeä kuva siitä, miten kriisejä luokitellaan ja miten ne voivat ilmetä. Lisäksi esiteltiin erilaisia säädöksiä, lakeja ja standardeja, joita pohjoismaiden hallitukset noudattavat kriisinhallinnan ja tietoturvan osalta. Erityistä huomiota kiinnitettiin myös EU:n rooliin pohjoismaiden toiminnassa. Tutkielmassa todettiin, että kriisinhallinta on moniulottei-

nen ja monitasoinen prosessi, joka vaatii jatkuvaa valmiutta, yhteistyötä ja tehokasta viestintää. Valtiollisella tasolla kriisinhallinta on välttämätöntä kansallisen turvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamiseksi.

Tutkielman tutkimuskysymykseen vastattiin pääluvussa neljä. Kappaleen tarkoituksena oli syventyä pohjoismaisten valtioiden, Suomen, Ruotsin, Norjan, Tanskan sekä Islannin toimiin Ukrainan sodan sekä Covid-19 pandemian takia ilmenneiden tietoturva- ja kyberuhkien estämiseksi sekä tulevaisuuteen varautumiseksi. Valtioiden toimet näiden uhkien poistamiseksi ja niihin vastaamiseksi olivat osin kohdistettu kyseisten uhkien lieventämiseksi, mutta tuloksista ilmeni, että toimia tehtiin myös pitkän tähtäimen hyötyjen saavuttamiseksi. Useat lähteet osoittivat, että pohjoismaat ovat ottaneet käyttöön monipuolisia ja kattavia strategioita tietoturvan ja kyberturvallisuuden takaamiseksi kriisitilanteissa. Esimerkiksi Suomen kyberturvallisuusstrategia korostaa kansallista yhteistyötä, elintärkeiden toimintojen turvaamista ja kansainvälistä yhteistyötä. Ruotsi on perustanut kansallisen kyberturvallisuuskeskuksen, joka yhdistää eri viranomaisten ja toimijoiden toimet kyberuhkien torjumiseksi. Norja on mukauttanut ohjeita ja suosituksia digitaalisen turvallisuuden edistämiseksi, ja Tanska on määritellyt neljä strategista tavoitetta vahvemman ja turvallisemman digitaalisen yhteiskunnan kehittämiseksi. Islanti puolestaan keskittyy digitaalisen muutoksen strategioihin ja kansainväliseen yhteistyöhön kyberuhkien torjunnassa.

Tulevaisuudessa on tärkeää jatkaa näiden strategioiden kehittämistä ja sopeuttamista muuttuviin uhkakuviin. Erityisesti teknologian nopea kehitys ja digitalisaation lisääntyminen asettavat uusia haasteita tietoturvalle, joten valtiot ja organisaatiot joutuvat jatkuvasti päivittämään ja parantamaan tietoturvakäytäntöjään. Lisäksi kansalaisten tietoisuuden ja osaamisen lisääminen tietoturvaasioissa on keskeistä, jotta yhteiskunta voi paremmin suojautua kyberuhkilta.

Vaikka tietoturvaa johdetaan ja hallitaankin useiden eri käytäntöjen avulla, ei tietoturvan toteutuminen joka tilanteessa ole taattua, kuitenkin asianmukaisilla toimenpiteillä ja koulutuksella voidaan pienentää tietoturvauhkien riskejä. Tietoturva on olennainen osa kansallista turvallisuutta ja sen merkitys korostuu erityisesti kriisitilanteissa.

Tämä tutkielma on pyrkinyt tarjoamaan kattavan kuvan siitä, miten Pohjoismaat kohtaavat ja hallitsevat tietoturvaan ja kyberturvallisuuteen liittyviä haasteita kriisitilanteissa. Vaikka tutkittavaa sekä käsiteltävää on vielä paljon, tarkastelu on osoittanut, että Pohjoismailla on vahva perusta ja laajat valmiudet vastata tietoturvauhkiin sekä ennakoida tulevia riskejä. Eri valtioiden strategiat, kuten Suomen kansallinen kyberturvallisuusstrategia ja Ruotsin kyberturvallisuuskeskus, ilmentävät maiden sitoutumista digitaalisen turvallisuuden parantamiseen.

Vaikka Pohjoismaat ovat saavuttaneet merkittäviä edistysaskeleita tietoturvan kehittämisessä, tutkielman perusteella ilmeni myös, että jatkuvaa kehitystä tarvitaan, erityisesti monimutkaisempien kyberuhkien ja nopeiden teknologisten muutosten vuoksi. Tulevaisuuden onnistuminen riippuu pitkälti siitä, kuinka hyvin valtiot ja organisaatiot kykenevät sopeutumaan uusiin haasteisiin ja tekemään yhteistyötä sekä kansallisella että kansainvälisellä tasolla. Jatkotutkimus voisi keskittyä esimerkiksi tietoturvakulttuurin vahvistamiseen organi-

saatioissa, kansainvälisen yhteistyön parantamiseen tai uusien teknologioiden hyödyntämiseen tietoturvan parantamiseksi.

Vaikka tutkielma tarjoaa kattavan käsityksen pohjoismaiden tietoturvajohtamiseen kriisitilanteissa, on tärkeää huomata, että aineisto rajoittuu julkisesti saatavilla oleviin lähteisiin. Tämä voi vaikuttaa tulosten laajuuteen ja luotettavuuteen. Myöskään valtioiden käyttämiä teknologioita ja järjestelmiä ei ole selkeästi mainittu julkisissa tietolähteissä, joten niiden tarkka käsittely jää vähemmäksi. Lisäksi tutkimus keskittyy 2020-luvun kriiseihin, mikä voi rajata tulosten yleistettävyyttä muihin aiempiin tai tuleviin tilanteisiin. Kirjallisuutta esimerkiksi ukrainan sodan aiheuttamista tietoturvauhista oli tarjolla rajallisesti, sillä kriisi on edelleen hyvin ajankohtainen ja saattaa muuttua. Tämä voi osaltaan rajoittaa tulosten luotettavuutta. COVID-19 pandemiaa käsittelevät aineistot keskittyivät enimmäkseen terveydenhuollon ympärille, joten uhkien tarkastelu sektorikohtaisesti voi olla puutteellista. On myös otettava huomioon, että suuri osa lähteistä on ovat valtiollisia tekstejä, joten akateemisia lähteitä on saatavilla rajallisesti

Tämä tutkielma korostaa, että tietoturvan kehittäminen ja johtaminen eivät ole vain tekninen tai operatiivinen kysymys, vaan ne liittyvät myös yhteiskunnan kulttuuriin, johtamiseen ja lainsäädäntöön. Näiden tekijöiden ymmärtäminen ja niiden vahvistaminen ovat keskeisiä yhteiskunnan rakentamisessa. ja kriisinhallinnassa Tämän työn tulokset voivat tarjota hyödyllisiä näkökulmia niin päätöksentekijöille ja tutkijoille, kuin käytännön toimijoille, jotka pyrkivät parantamaan tietoturvaa ja kyberturvallisuutta pohjoismaissa ja muualla maailmassa. Taulukko 2 ei käsittele kaikkia kansallisen turvallisuuden osa-alueita, lähteiden saatavuuden puutteen takia, mikä tarjoaa laajasti tulevaisuuden tutkimuskohteita. Taulukosta on jätetty pois alueet ruokaturvallisuus, liikenneturvallisuus, kulttuuri- ja henkinen turvallisuus ja ympäristöturvallisuus, mikä rajoittaa tässä tutkielmassa tarkasteltavaa näkökulmaa. Tulevaisuudessa näitä alueita voitaisiin tutkia enemmän, jotta saadaan. laajemmin tietoa niiden vaikutuksesta tietoturvaan ja sen johtamiseen.

LÄHTEET

Asetus - 2019/881 - *FI - EUR-Lex*. (2019). Noudettu 12. marraskuuta 2024, osoitteesta https://eur-lex.europa.eu/eli/reg/2019/881/oj

Agustsdottir, T. (2024). *Securing Iceland's digital future: A call for political action*. *Internet Policy Review*. Noudettu 25. marraskuuta 2024

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences,* 34(10, Part A), 8176–8206.

Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. Sh., & Aliguliyev, R. M. (2021). Information security as a national security component. *Information Security Journal: A Global Perspective,* 30(1), 1–18.

Andress, J. & Leary, M. (2017). *Building a Practical Information Security Program.* Syngress.

Asp, C. (2021.). *Strengthening civil preparedness.* Noudettu 29. lokakuuta 2024, osoitteesta https://www.msb.se/siteassets/dokument/publikationer/english-publications/strengthening-civil-preparedness.pdf

Best Practices for Cyber Crisis Management. (2024). [Report/Study]. ENISA. Noudettu 29. lokakuuta 2024, osoitteesta https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

Chai, K. Y. & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT In Education, 8(2), 34–42.

Chigada, J. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1–11.

COVID-19 forsterker digitale sårbarheter - Nasjonal sikkerhetsmyndighet. (2020). Noudettu 24.marraskuuta 2024, osoitteesta https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/det-digitale-risikobildet/covid-19-forsterker-digitale-sarbarheter/

Cyber Security : Critical Infrastructure Protection. (2021). Noudettu 27. marraskuuta 2024

Cybersäkerhet i Sverige – i skuggan av en pandemi. (2021). Noudettu 24. marraskuuta 2024, osoittees-

ta https://www.msb.se/siteassets/block/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cybercenter/cybersakerhet-i-sverige--i-skuggan-av-en-pandemi-2021.pdf

Danish Cyber and Information Security Strategy 2022-2024. (2022). Centre for Cybersecurity. Noudettu 30. marraskuuta 2024, osoitteesta https://www.cfcs.dk/en/about-us/danish-cyber-and-information-security-strategy/

Do the Nordics need a common cyber security strategy? (2022). Nordic Co-operation. Noudettu 23. marraskuuta 2024, osoitteesta https://www.norden.org/en/news/do-nordics-need-common-cyber-security-strategy

ENISA Threat Landscape 2020. (2020). [Page]. ENISA. Noudettu 23. marraskuuta 2024, osoitteesta https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

ENISA Threat Landscape 2021. (2021). [Report/Study]. ENISA. Noudettu 24. marraskuuta 2024, osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA Threat Landscape 2022. (2022). [Report/Study]. ENISA. Noudettu 24. marraskuuta 2024, osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Europa.eu (2023). *Russia's war on Ukraine: one year of cyber operations.* Noudettu 25. marraskuuta 2024, osoitteesta https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Full article: Crisis, what crisis? Conceptualizing crisis, UK pluri-constitutionalism and Brexit politics. (2020). Noudettu 27. marraskuuta 2023

Government Offices of Sweden. (2020). Nordic Foreign and Security Policy 2020. Noudettu 22. marraskuuta 2024, osoitteesta https://www.government.se/contentassets/c128b79d0e9143469e7df83648eddb3c/nordic_foreign_security_policy_2020_final.pdf

Government report on changes in the security environment. (2022.). Valtioneuvosto. Noudettu 27. marraskuuta 2024 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164002/VN_2022_20.pdf

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *TQM journal, 33*(7), 76-105.

Hansson, S. (2021). COVID-19 information disorder: six types of harmful information during the pandemic in Europe. *Journal of Risk Research*, *24*(3–4), 380–393.

Hu, Q. & Liu, Y. (2022). Crisis Management and National Responses to COVID-19: Global Perspectives. Public Performance & Management Review, 45(4), 737–750.

Interpol. (2021). Kyberstrategian käsikirja. Interpol. Noudettu 24. marraskuuta 2024, osoitteesta https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf?inLanguage=eng-GB

ISO - About ISO. (2024). ISO. Noudettu 12. marraskuuta 2024, osoitteesta https://www.iso.org/about

ISO - ISO/IEC 27000 family — Information security management. (2024). Noudettu 25. marraskuuta 2024, osoitteesta ISO. https://www.iso.org/standard/iso-iec-27000-family

Johansson, B., Ihlen, Ø., Lindholm, J. & Blach-Ørsten, M. (2023). Communicating a Pandemic: Crisis Management and Covid-19 in the Nordic Countries. Nordicom, University of Gothenburg.

Joint Nordic Statement at the Arria formula meeting of the Security Council on Cyber-Attacks against Critical Infrastructure. (2020). Government of Iceland. Noudettu 30. marraskuuta 2024, osoitteesta https://www.government.is/diplomatic-missions/embassy-article/2020/08/26/Joint-Nordic-Statement-at-the-Arria-formula-meeting-of-the-Security-Council-on-Cyber-Attacks-against-Critical-Infrastructure/'

Joint Nordic Statement on Pandemics and Security. (2020). Noudettu 24. marraskuuta 2024, osoitteesta https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2020/07/02/Joint-Nordic-Statement-on-Pandemics-and-Security/

Kaczmarek, K. (2023). Finland in the light of cyber threats in the context of Russia's aggression against Ukraine. Cybersecurity and Law, 9(1), 204–214.

Kyberturvallisuusstrategia. (2024). Valtiovarainministeriö. Noudettu 24. marraskuuta 2024, osoitteesta https://vm.fi/kyberturvallisuusstrategia

Kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden kansallinen koordinointikeskus. (2024). Kyberturvallisuuskeskus. Noudettu 5. marraskuuta 2024, osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/kyberturvallisuuden-tutkimuksen-kehityksen-ja-innovaatioiden-kansallinen

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

McConnell, A. (2003). Overview: Crisis Management, Influences, Responses and Evaluation. Parliamentary Affairs, 56(3), 363–409.

Mitä on kansallinen turvallisuus? (2024). Sisäministeriö. Noudettu 16. lokakuuta 2024, osoitteesta https://intermin.fi/kansallinen-turvallisuus/mita-on-kansallinen-turvallisuus

Mitä tietosuoja on? (2024). Tietosuojavaltuutetun toimisto. Noudettu 30. lokakuuta 2023, osoitteesta https://tietosuoja.fi/tietosuoja

Nasjonalt digitalt risikobilde (2021). Noudettu osoitteesta https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

National Cyber Security Strategy for Norway (2019) Noudettu 22. joulukuuta 2024, osoitteesta https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

Netöryggi. (2022.). Noudettu 22. joulukuuta 2024, osoitteesta https://www.stjornarradid.is/verkefni/fjarskipti/netoryggi/

NIS Directive 2. (2024). [Topic]. ENISA. Noudettu 12. marraskuuta 2024, osoitteesta https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Nordic cooperation on foreign and security policy. (2024). Ministry for Foreign Affairs. Noudettu 22. marraskuuta 2024, osoitteesta https://um.fi/nordic-cooperation-on-foreign-and-security-policy

Paananen, R., Soikkeli, M., Starck, M., Aro, M., Kuusisto, T., Rusila, T. & Tuulensuu, T. (2024). *Suomen kyberturvallisuusstrategia 2024–2035* [Sarjajulkaisu]. fi=Valtioneuvoston kanslia | sv=Statsrådets kansli | en=Prime Minister's Office | . https://julkaisut.valtioneuvosto.fi/handle/10024/165860

Palveluiden ja turvallisuuden ohjaus. (2024). Valtiovarainministeriö. Noudettu 25. joulukuuta 2024, osoitteesta https://vm.fi/palveluiden-ja-turvallisuuden-ohjaus

Policies. (2024). Danish government. Noudettu 30. marraskuuta 2024, osoitteesta https://www.government.is/topics/information-technology/policies/

Regeringskansliet, R. och. (2017). *A national cyber security strategy* [Text]. Regeringskansliet; Regeringen och Regeringskansliet. https://www.government.se/legal-documents/2017/11/skr.-201617213

Regeringskansliet, R. och. (2021). Sweden's response in the global fight against the COVID-19 pandemic [Text]. Regeringskansliet; Regeringen och Regeringskansliet. https://www.government.se/articles/2021/03/swedens-response-in-the-global-fight-against-the-covid-19-virus/

Report: Finland's cyber security must be developed systematically – cooperation of the authorities and processes require further improvement. (2023). Finnish Government. Noudettu 27. marraskuuta 2024, osoitteesta https://valtioneuvosto.fi/en/-/1410869/report-finland-s-cyber-security-must-be-developed-systematically-cooperation-of-the-authorities-and-processes-require-further-improvement

Revised Cyber Security Strategy responds to changed security environment. **(**2024). Finnish Government. Noudettu 30. marraskuuta 2024, osoitteesta https://valtioneuvosto.fi/en/-/1410829/revised-cyber-security-strategy-responds-to-changed-security-environment

Sapinski, A. (2023). The importance and challenges of information security in the digital age: analysis of the current situation and prospects for development. Noudettu 5. maaliskuuta 2024

Somepalli, S. H., Tangella, S. K. R. & Yalamanchili, S. (2020). Information Security Management. *HOLISTICA – Journal of Business and Public Administration*, *11*(2), 1–16.

Supon tehtävät. (2024). Suojelupoliisi. Noudettu 5. marraskuuta 2024, osoitteesta https://supo.fi/supon-tehtavat

The Cyber Dimension of the Russia–Ukraine War. Willett, M. (2022). Survival, 64(5), 7–26.

The EU Cybersecurity Act | Shaping Europe's digital future.(2024). Noudettu 8. marraskuuta 2024, osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict | Think Tank | European Parliament. (2023). Noudettu 23. marraskuuta 2024, osoitteesta https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594

Tietoturva. (2020). Kyberturvallisuuskeskus. Noudettu 5. maaliskuuta 2024, osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle. (2021). Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-3-uhkaa-ja-3-ratkaisua-jokaiselle

Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien. (2020). Center for Cybersikkerhed. Noudettu 23. marraskuuta 2024, osoitteesta https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/covid-19/

Turvallisuus. (2024). Puolustusministeriö. Noudettu 5. marraskuuta 2024, osoitteesta https://www.defmin.fi/vastuualueet/turvallisuus

Tilkynning frá netöryggissveitinni CERT-IS – CERT-IS. (2022). Noudettu 3. joulukuuta 2024, osoitteesta https://cert.is/frettasafn/tilkynning-fra-netoryggissveitinni-cert-is-2/

Valtori. (2024). Tietoa toiminnastamme. Noudettu 5. marraskuuta 2024, osoitteesta https://valtori.fi/tietoa-valtorista

Yleinen tietosuoja-asetus (GDPR**).** (2024). Your Europe. Noudettu 12. marraskuuta 2024, osoitteesta https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm