



Hybridivaikuttamiselta suojautuminen

Timo Lukkari

2024 Laurea



Laurea-ammattikorkeakoulu

Hybridivaikuttamiselta suojautuminen

Timo Lukkari
Turvallisuus ja riskienhallinta
Opinnäytetyö
Joulukuu, 2024

Timo Lukkari

Hybridivaikuttamiselta suojautuminen

Vuosi

2024

Sivumäärä

29

Tämän opinnäytetyön tavoitteena oli selvittää, millaisia keinoja hybridivaikuttamiselta suojautumiseen löytyy suomalaisista julkaisuista. Opinnäytetyö tehtiin kuvailevana kirjallisuuskatsauksena. Opinnäytetyölle ei ollut toimeksiantajaa.

Tietoperustassa käsitellään hybridivaikuttamiseen liittyviä käsitteitä ja määritelmiä. Käsitteiden ja määritelmien ymmärtämisellä on mahdollista ymmärtää millaista toimintaa hybridivaikuttaminen ja millaisin eri tavoin se voi ilmetä. Tietoperustassa pohditaan myös suojautumisen käsitettä ja sitä mitä hybridivaikuttamiselta suojautuminen voi mahdollisesti pitää sisällään.

Tutkimuksellinen osio toteutettiin kuvailevana kirjallisuuskatsauksena. Kuvaileva kirjallisuuskatsaus on yleiskatsaus, joka ei noudata tiukasti määriteltyjä sääntöjä tai menetelmiä. Kuvaileva kirjallisuuskatsaus edellyttää tutkimuskysymyksen määrittelyn. Tässä opinnäytetyössä tutkimuskysymykseksi asetettiin: Millaisia suojautumis- ja varautumiskeinoja hybridivaikuttamiselta suojautumiseen on olemassa? Tutkimuksen aineistona käytettiin seitsemää eri lähettä, jotka valittiin kahdesta eri tietokannasta. Aineiston valinnassa käytettiin viittä eri hyväksymisperustetta, jotka olivat julkaisun ajankohta, julkaisija, julkaisukieli, aineiston relevanttius sekä tutkimuskysymykseen vastaaminen. Aineiston sisällöstä etsittiin tietoperustassa ilmeneviä käsitteitä ja määritelmiä, sekä vastauksia tutkimuskysymykseen.

Kirjallisuuskatsauksen tuloksista oli mahdollista havaita seitsemän eri osa-alueita, joiden avulla on mahdollista varautua hybridivaikuttamiseen tai suojautua siltä. Kyseiset osa-alueet olivat yhteistyö, tilannekuva, tietoisuuden lisääminen, lainsäädäntö, johtaminen ja johtosuhteet, käytänteiden ja käytäntöjen jakaminen ja resilienssi. Tuloksista oli havaittavissa myös se, että usein hybridivaikuttamiseen varautuminen tai siltä suojautuminen edellyttää useiden eri osa-alueiden yhdistämistä ja yhteen toimimista.

Opinnäytetyöllä kyettiin vastaamaan tutkimuskysymykseen melko hyvin. Tutkimusaineisto on luotettavaa, mutta tutkimusaineistoa ei ole kasattu kovin monipuolisista lähteistä. Ottaen huomioon hybridivaikuttamisen lukuisat muodot, opinnäytetyössä ei kyetty vastaamaan hankitun aineiston perusteella kovin yksityiskohtaisesti eri hybridivaikuttamisen muotoihin.

Asiasanat: hybridivaikuttaminen, suojautuminen, kybervaikuttaminen, informaatiovaikuttaminen

Timo Lukkari

Protection against hybrid influencing

Year

2024

Pages

29

The objective of this thesis was to map means of protection against hybrid influence activities that can be found in Finnish publications. The thesis was carried out a descriptive literature review. There was no commissioning party for the thesis.

The theoretical framework discusses concepts and definitions related to hybrid influence activities. By understanding concepts and definitions, it is possible to understand the nature of hybrid influence activities that can take place and in what ways it can manifest itself. The theoretical framework also discusses the concept of protection and what protecting against hybrid influence activities may possibly entail.

The research was carried out as a descriptive literature review. A descriptive literature review is an overview that does not follow strictly defined rules or methods. A descriptive literature review requires a research question. Consequently, this thesis addresses the protection and preparedness measures available for protection against hybrid influence activities. Seven different sources were used as data for the study, selected from two different databases. Five different acceptance criteria were used in selecting the material. These were date of publication, publisher, language of publication, relevance of the data and answering the research question. The content of the data was searched for concepts and definitions that appear in the theoretical framework, as well as answers to the research question.

From the results of the literature review, it was possible to identify seven different areas that make it possible to prepare for or protect against hybrid influence activities. These areas were cooperation, situational awareness, awareness-raising, legislation, leadership and management relations, sharing best practices and resilience. The results also showed that preparing for or protecting against hybrid influence activities often requires the involved parties to combine and work together in several different areas of protection against hybrid influence activities.

The thesis was able to answer the research question quite well. The research material is reliable, but the research material has not been compiled from very diverse sources. Given the numerous forms of hybrid influence activities, the thesis was not able to answer the different forms of hybrid influence activities in detail based on the research material.

Keywords: hybrid influencing, protection, cyber influencing, information influencing

Sisällys

1	Johdanto.....	6
2	Hybridivaikuttaminen ja hybridisodankäynti	7
2.1	Hybridivaikuttamiseen liittyvät käsitteet.....	8
2.2	Hybridivaikuttamisen keinoja	8
2.3	Hybridivaikuttamiselta suojautuminen.....	10
3	Kuvaileva kirjallisuuskatsaus opinnäytetyön menetelmänä	11
4	Tulosten esittely.....	14
4.1	Yhteistyö ja viestintä	14
4.2	Tilannekuva ja johtaminen	15
4.3	Tietoisuuden lisääminen	16
4.4	Parhaiden käytänteiden jakaminen.....	17
4.5	Resilienssin kasvattaminen	18
4.6	Tekniset suojautumiskeinot	18
4.7	Lainsäädäntö.....	19
4.8	Muut suojautumiskeinot.....	20
5	Johtopäätökset	22
6	Pohdinta	25
	Lähteet.....	27

1 Johdanto

Hybridivaikuttaminen on noussut paljon julkisuudessa esillä olevaksi teemaksi Venäjän Ukrainaan vuonna 2022 aloittaman hyökkäyssodan jälkeen. Hybridivaikuttamista on tehty jo ennen Ukrainan sotaa, mutta hybridivaikuttamisen käyttäminen ja sen pohtiminen on noussut laajempaan keskusteluun sodan myötä. Hybridivaikuttamiskeinoja on lukuisia erilaisia ja tulevaisuudessa erilaisia vaikuttamiskeinoja tulee melko todennäköisesti ilmaantumaan lisää. Hybridivaikuttamiskeinojen tarkoituksena on kuitenkin vaikuttaa demokraattisiin valtioihin ilman, että hybridivaikuttamisen alullepanijaa saadaan selville. Koska hybridivaikuttamiskeinoja on useita, myös hybridivaikuttamiselta suojautuminen voi tapahtua lukuisin erilaisin toimenpitein ja keinoin.

Tässä opinnäytetyössä pyritään selvittämään, millaisia suojautumiskeinoja hybridivaikuttamista vastaan on olemassa. Suojautumiskeinoja haetaan suomenkielisistä julkaisuista, joita ovat julkaisseet Suomen valtiolliset toimijat ja ministeriöt, valtion tutkimuslaitokset ja Euroopan unionin alaisuudessa julkaisevat toimijat sekä suomalaiset organisaatiot, oppilaitokset ja yritykset.

Opinnäytetyön tavoitteena on käydä läpi aineistot ja tiivistää niistä löydetty suojautumiskeinot hybridivaikuttamista vastaan. Opinnäytetyön on tarkoitus sisältää mahdollisimman selkeästi esitettyjä suojautumiskeinoja erilaisiin hybridivaikuttamiskeinoin. Tämän lisäksi tavoitteena on pohtia ohjeita, joiden avulla organisaatiot voivat varautua hybridivaikuttamiseen.

Opinnäytetyössä selvitetään ensin hybridivaikuttamisen määritelmä ja käydään läpi erilaisia hybridivaikuttamiskeinoja. Opinnäytetyö on tehty kuvailevana kirjallisuuskatsauksena, jotta käsitellystä aineistosta on mahdollista hakea suojautumiskeinoja hybridivaikuttamista vastaan mahdollisimman vapaasti. Kirjallisuuskatsauksen tarkempien yksityiskohtien kertomisen jälkeen työssä kerrotaan millä tavoin aineistoa on etsitty ja millä kriteerein löydetty teokset on hyväksytty aineistoksi. Tulosten esittely -kappaleessa perehdytään siihen, millaisia suojautumiskeinoja aineistosta on havaittu. Johtopäätökset ja pohdinta -kappaleet avaavat tarkemmin havaittujen suojautumiskeinojen merkitystä ja käyttötapoja sekä sisältävät enemmän opinnäytetyön tekijän ajatuksia ja havaintoja aineistosta.

Hybridivaikuttaminen on hyvin laaja ja moniulotteinen käsite. Tämä työ voi osaltaan olla auttamassa yksilöitä ja organisaatioita taistelussa tätä monitahoista ongelmaa vastaan.

2 Hybridivaikuttaminen ja hybridisodankäynti

Hybridivaikuttamisella tarkoitetaan toimintaa, jolla valtiolliset tai ei-valtiolliset toimijat pyrkivät vaikuttamaan hybridivaikuttamisen kohteena olevaan valtioon tavoitteenaan aiheuttaa eripuraa valtion sisällä, horjuttaa demokratiaa, lisätä epävakautta ja asettaa valtioiden suvereniteetti kyseenalaiseksi. (Hybridiosaamiskeskus 2024a). Hybridivaikuttamisen keinoina voivat olla esimerkiksi erilaiset informaatiovaikuttamisen keinot, kyberhyökkäykset, taloudellinen vaikuttaminen tai pakottaminen sekä poliittiset ja diplomaattiset keinot. Olennaisena elementtinä hybridivaikuttamisessa on se, että toiminnan on tarkoitus tapahtua mahdollisimman peiteltysti, jotta todellista hybridivaikuttamisen käynnistäjää ei saada selville. (Hybridiosaamiskeskus 2024b). Hybridivaikuttamisessa toinen olennainen elementti on keinojen yhdisteleminen toisiinsa järjestelmällisesti (Kytömaa 2024.)

Hybridivaikuttaminen on merkittävä ilmiö turvallisuuskentässä niin valtion, organisaatioiden kuin joissain tilanteissa yksilöidenkin tasolla. Aihetta käsitellään eri ministeriöissä ja tutkimuksissa tasaisin väliajoin. Yhtenä esimerkkinä ammatillisesta keskustelusta käy Sisäministeriössä toimii hybridiuhkaverkosto, jota koordinoi sisäministeriön kansallisen turvallisuuden yksikkö. Verkostossa käsitellään EU-tasolla ja valtioneuvostossa valmisteltavia asioita. Verkosto toimii myös linkkinä sisäministeriön toimialan sisällä. (Kytömaa 2024.)

Hybridivaikuttamista on myös tutkittu jo useiden vuosien ajan. Ulkopoliittinen instituutti on valmistellut raportin hybridivaikuttamisesta ja demokratian resilienssistä vuonna 2018. Raportissa käsitellään hybridivaikuttamista strategisella tasolla mutta siinä paneudutaan myös geoeconomiseen vaikuttamiseen, informaatiovaikuttamiseen ja vaalivaikuttamiseen. Hybridivaikuttamisen kerrotaan olevan kyseessä tilanteessa, jossa toiminta on ei-sotilaallista ja piilossa tapahtuvaa, eikä toimintaa välttämättä havaita negatiiviseksi kohdemaassa. (Aaltola, Mikkola, Juntunen, Vihma & Wigell 2018.) Hybridikäsitteitä on tutkittu myös Maarit Möllerin (2020) kandidaattityössä, jossa tarkastellaan hybridikäsitteitä, hybridisotaa, hybridivaikuttamista ja hybridihäirintää.

Hybridivaikuttaminen ja hybridisodankäynti ovat termeinä toisiaan muistuttavia ja ne ovat merkityksiltäänkin lähellä toisiaan. Ne eivät ole kuitenkaan synonyymejä toisilleen.

Hybridisodankäynnistä voi kyse olla tilanteesta, jossa jollain perinteisellä sodankäynnin muodolla pyritään vaikuttamaan toiseen valtioon sodan ja rauhan välimaastossa, mutta pitäydään kuitenkin varsinaisista perinteisistä sotatoimista. Yksi esimerkki tällaisesta toiminnasta on Venäjän valtion joukkojen ryhmittely ja harjoittelu ennen hyökkäyssodan aloittamista Ukrainaa vastaan helmikuussa 2022. Myös ydinaseilla uhittelu on tyypillinen esimerkki hybridisodankäynnissä käytettävästä keinosta. Hybridisodankäynnistä on kyse myös silloin, mikäli epätavanomaisia hyökkäyskeinoja käytetään varsinaisen sotatilanteen aikana kohdemaata

vastaan. Tällaisia epätavanomaisia keinoja voivat olla esimerkiksi kyberoperaatiot tai informaatiovaikuttaminen. (Tiilikainen 2024.)

2.1 Hybridivaikuttamiseen liittyvät käsitteet

Hybridivaikuttamisen ja hybridisodankäynnin käsittelyä varten on tärkeää ymmärtää teemoihin liittyviä käsitteitä ja termejä. Käsitteet ja termit sisältävät hybriditoiminnan erilaisia esiintymismuotoja ja niillä tavoiteltavia vaikutuksia.

Hybridivaikuttamisesta on kyse, kun kohteeseen pyritään vaikuttamaan käyttämällä useita keinoja kerralla. Hybridivaikuttamiskeinoilla on tarkoitus muokata geopoliittista asetelmaa, jotta autoritaarisilla valtioilla olisi mahdollisuus kasvattaa omaa vaikutusvaltaansa globaalissa aselelmassa. Hybridiopeaatioiden tarkoituksena on iskeä kohdevaltioon tiettyihin heikkouksiin ja ohittaa samalla kohteen vahvuudet. (Aaltola ym. 2018, 8.)

Aaltola ym. (2018, 9-10) kertovat hybridihäirinnästä. Hybridihäirinnällä tarkoitetaan monimuotoista, tarkasti koordinoitua häirinnän muotojen yhdistelmää, jonka avulla pyritään luomaan syviä jakolinjoja kohdemaan yhteiskuntaan. Tällöin valtio tai muu toimija, joka hyödyntää ei-sotilaallisia ja refleksiivisen kontrollin menetelmiä, pyrkii vaikuttamaan kohdemaan poliittisiin prosesseihin niin, että kohdemaahan ikään kuin itse vahvistaa vaikuttajan agendaan tai heikentää omaa päätöksentekokykyään. Hybridihäirintä tarkoittaa siis rauhanajan psykologisia kampanjoita, joiden tarkoituksena on heikentää vastapuolen kansalaisyhteiskuntaa sekä liittolaissuhteiden sosiaalista ja kulttuurista eheyttä.

Hybridiuhat ovat monimuotoisia, epätavallisia uhkavälineitä, joilla uhataan demokraattisia yhteiskuntia. Niiden käyttämisessä hyödynnetään demokraattisten valtioiden arvoja ja haavoittuvuuksia. Hybridiuhallalla viitataan kaikkiin monimuotoisiin epäkonventionaalisiin välineisiin, joilla voidaan vaikuttaa demokraattisten yhteiskuntien vakauteen. (Tiilikainen 2024.) Hybridiuhilla voidaan kuvata uhkia, joita hybridivaikuttamisella saadaan aikaiseksi.

2.2 Hybridivaikuttamisen keinoja

Hybridivaikuttamisen yhtenä merkittävimpana keinona on informaatiovaikuttaminen. Informaatiovaikuttamisella tarkoitetaan toimintaa, jonka tarkoitus on vaikuttaa yhteiskunnan toimintakykyyn esimerkiksi disinformaatiota levittämällä ja siten vaikuttamalla kansalaisten mielipiteisiin ja toimintaan sekä päätöksentekijöihin. Informaatiovaikuttamisen tarkoituksena on saada vaikuttamisen kohde tekemään omalta kannaltaan epäedullisia päätöksiä tai toimimaan omaa etuaan vastaan. (Valtioneuvoston kanslia 2019, 9-16.) Informaatiovaikuttamisen yksi työkalu on disinformaation levittäminen. Disinformaatiolla tarkoitetaan paikkansa pitämättömiä tai manipuloitua tietoa, jota levitetään harhaanjohtamistarkoituksessa. (Valtioneuvoston kanslia 2019, 31.) Disinformaatiolla pyritään herättämään provosoivaa keskustelua,

rajoittamaan avoimia väittelyjä ja tukahduttamaan moniarvoista keskustelua. Sen päämääränä on heikentää kansallista arvopohjaa, demokratiaa ja luottamusta yhteiskunnassa, samalla kun se uhkaavaa sananvapauden, mielipiteenvapauden ja lehdistönvapauden toteutumista. (Valtioneuvoston kanslia 2019, 9.)

Kyberhyökkäykset ovat yksi hybridivaikuttamisen olennaisimmista keinoista. Kyberhyökkäyksillä tarkoitetaan tietoverkkovälitteisesti tapahtuvaa toimintaa, jolla pyritään vaikuttamaan tietoverkon, tietojärjestelmän tai laitteen toimintaan tai datan vahingoittamiseen tai luvattomaan käyttöön. (Turvallisuuskomitea 2018, 30.)

Turvallisuuspolitiikan tietopankki (2024a) kertoo kolmenlaisesta haitallisesta kybertoiminnasta: tiedustelusta tai vakoilusta, hyökkäyksistä ja tietojen manipuloinnista. Kybertiedustelu muistuttaa perinteistä tiedustelu- ja vakoilutoimintaa, sillä sen pääasiallinen tavoite on kerätä luottamuksellisia tietoja.

Turvallisuuspolitiikan tietopankin (2024a) mukaan kybertiedustelulla hankittuja tai varastettuja tietoja voidaan käyttää omiin tarkoituksiin ilman, että niiden hallussapidosta kerrotaisiin ulkopuolisille, mutta niitä on mahdollista hyödyntää myös vuotamalla tietoja julkisuuteen ja siten vaikuttaa joko tiedustelun kohteena olevaan tahoon tai tahoon, jota tiedustelumateriaali koskettaa. Kyberhyökkäys on kybertiedustelun seuraava vaihe ja viittaa hyökkäykseen, joka suuntautuu erityisesti yhteiskunnan elintärkeisiin infrastruktuureihin, kuten sähkö-, viestintä-, vesihuolto-, rahoitus- ja muihin kriittisiin tietoverkkoinfrastruktuureihin.

Kyberhyökkäystä on mahdollista käyttää myös toimijaa vastaan, joka ei ole suoranaisesti kriittisen infrastruktuurin toimija, mutta johon vaikuttamalla voidaan välisesti aiheuttaa haittaa kriittiselle infrastruktuurille.

Kybermanipuloinnilla tarkoitetaan tilannetta, jossa hyökkääjä tietojärjestelmään tai -verkkoon tunkeutumisen jälkeen muokkaa alustalla olevia tietoja. Tämän tarkoituksena on johtaa siihen, ettei tietojärjestelmän tai -verkon hallinnoija enää luota omaan järjestelmäänsä. (Turvallisuuspolitiikan tietopankki 2024a). Kybermanipuloinnilla voidaan pyrkiä myös siihen, että alustalla olevia tietoja onnistuttaisiin muokkaamaan omia tarkoituksia suosivaksi ilman, että alustan käyttäjät huomaisivat tietojen luvattoman muokkaamisen.

Taloudellisella vaikuttamisella tai pakottamisella pyritään vaikuttamaan kohdevaltion päätöksiin pakotteita tai sanktioita hyödyntäen tai muokkaamalla kohdevaltioon suuntautuvaan matkailuun tai kohdevaltion maksuihin esimerkiksi energian suhteen. Taloudellinen vaikuttaminen ja pakottaminen voi kohdistua suoraan valtioon tai yksittäisiin henkilöihin, jotka ovat merkittävässä roolissa vaikutusvaltion päätöksenteossa tai lähellä päätöksentekijöitä. (Turvallisuuspolitiikan tietopankki 2024b.)

Taloudellinen vaikuttamisella ja pakottamisella voidaan tarkoittaa myös tilannetta, jossa kohdevaltion ei kohdisteta suoria taloudellisia toimia, vaan kohdevaltion yhteistyökumppaneihin tai muihin kohdevaltiota lähellä oleviin tahoihin kohdistetaan joko taloudellisia houkuttimia tai rangaistuksia. Tällä tavoin on mahdollista saada eri toimijat käyttäytymään siten, että taloudellinen vaikuttaminen vaikuttaa kohdevaltioon muiden toimijoiden kautta. (Aaltola ym. 2018, 28-29.)

Hybridivaihtamisen yhteydessä poliittisella vaikuttamisella pyritään muokkaamaan toimijoiden, organisaatioiden ja laitosten käyttäytymistä, jotka hallitsevat valtaa tai aluetta poliittisin keinoin. Tällöin poliittinen vaikuttaminen kytkeytyy tiiviisti myös diplomaattisiin toimiin. (Gianopoulos, Smith & Theodoridou 2021, 32.)

Aaltola ym. (2018, 27-28) kertovat hämärän diplomatian vaikuttamiskeinoista. Hämärän diplomatian vaikuttamiskeinona on vahvistaa vaikuttamisvaltiossa olevia toimijoita, jotka eivät hyväksyä vallalla olevaa hallintoa. Tällä on tarkoitus vähentää hallituksen suosiota ja pyrkiä saamaan aikaan entistä suurempia jakolinjoja ja eripuraa yhteiskunnan sisällä. Hämärän diplomatian keinojen käyttämisessä on mahdollista hyödyntää myös rikollisjärjestöjä tai yksittäisiä rikollisia, jotka toimisivat ”syntipukkeina” tapahtumille, joiden on mahdollista aiheuttaa juridisia seuraamuksia. Näiden toimijoiden kautta on myös mahdollista levittää haluttua propagandaa muiden ryhmien pariin.

Välineellistetyllä maahanmuutolla tarkoitetaan tilannetta, jossa valtion rajalle ohjataan kolmannen valtion toimesta laittomia muuttovirtoja. Tällaisella toiminnalla pyritään vaikuttamaan rajaturvallisuuteen, yleisen järjestyksen ylläpitämiseen ja kansallisen turvallisuuden suojaamiseen. (Sisäministeriö 2022, 11.)

Vaalivaikuttamisen suhteen ulkomaisella sekaantumisella tarkoitetaan kohdennettuja toimia, joiden tarkoituksena on vaikuttaa kansalaisten, poliittisen johdon tai kansalaisyhteiskunnan tärkeimpiin sidosryhmiin ja muuttaa heidän käsityksiään. Ulkomaisella vaikuttamistoiminnalla viitataan pitkäaikaisempiin vaikutusmuotoihin, joiden tarkoitus on esimerkiksi toteuttaa propaganda- ja viestintäkampanjoita tai tukea lobbausryhmiä poliittisten muutosten saavuttamisessa. (Henschke, O’Connor, & Sussex. 2020, 5.)

2.3 Hybridivaikuttamiselta suojautuminen

Hybridivaikuttamisen keinoja on useita erilaisia, jonka vuoksi ei ole yhtä yksittäistä suojautumiskeinoja, jonka avulla voidaan suojautua kaikilta hybridivaikuttamisen tavoilta. Hybridivaikuttamiselta suojautuminen voi pitää sisällään myös toimia, jotka eivät ole suoraan suojautumistoimia, vaan enemmänkin varautumista hybridivaikuttamiseen. Tällöin tarkoituksena on varautumisen keinoin pienentää hybridivaikuttamisen vaikutusta tai ennalta estää hybridivaikuttamista kokonaisuudessaan. On yksi työkalu, jolla voidaan vaikuttaa ainakin jossain

määrin kaikkien hybridivaikuttamiskeinojen toimintaan ja tuo työkalu on tietoisuuden lisääminen. Mitä laajemmin tiedostetaan hybridivaikuttamisuhkien olemassaolo ja ymmärretään havainnoida omaa ympäristöä hybridivaikuttamista silmällä pitäen, sitä paremmin hybridiuhkia on mahdollista estää ennalta. Toinen suojautumiskeino, jolla voidaan suojautua useilta erilaisilta vaikuttamistavoilta, on resilienssin ja kriisinkestävyyden tehostaminen. (Aaltola ym. 2018, 10-11.)

Resilienssi voidaan kuitenkin määritellä eri tavoin. Aaltola ym. (2018, 11) kertovat kolmesta eri tavasta määritellä resilienssi. Ensimmäisen määritelmän mukaan resilienssillä kuvataan kykyä jättää huomioitta poliittisen yhteisön ulkopuolelta tulevia uhkatekijöitä. Toinen määritelmä kuvaa yhteisön kyvykkyyttä sietää kriisejä ja palautua kriiseistä niiden jälkeen. Kolmannen määritelmän mukaan resilienssillä tarkoitetaan kykyä oppia uhkakuvien toteutumisesta aiheutuneista vaikutuksista.

Informaatiovaikuttamisen torjumisessa ja ehkäisemisessä keskeistä on tietoisuuden lisääminen ja laaja yhteistyö. Koska kohteena on koko yhteiskunta - sen toiminnot, arvot ja normit - koko yhteiskunnan olisi osallistuttava informaatiovaikuttamisen torjuntaan. Informaatiovaikuttamiseen vastaaminen ei ole vain viranomaisten vastuulla, vaan se on myös yritysten, yhteisöjen, järjestöjen ja yksilöiden yhteinen tehtävä. (Valtioneuvoston kanslia 2019, 9.)

Maigre (2022, 14) on määritellyt muutaman suosituksen, joiden avulla kyberhyökkäyksiltä on mahdollista suojautua. Maigren mukaan tietoturvan parantamiseksi on tärkeää huolehtia siitä, että kaikki järjestelmät pidetään ajan tasalla asentamalla säännöllisesti suojauspäivitykset ja korjaukset. Lisäksi on tärkeää parantaa pääsynhallintaa ja ottaa käyttöön monivaiheinen tunnistautuminen, jotta estetään luvattomien käyttäjien pääsy järjestelmiin. Tehokkaiden häiriötilanteiden hallintasuunnitelmien laatiminen ja suunnitelmien jatkuva ylläpitäminen mahdollistaa nopean reagoinnin mahdollisiin uhkisiin. On myös varmistettava, että varmuuskopiointi- ja palautusmekanismit toimivat moitteettomasti, jotta tietojen menetykseltä voidaan välttyä. Lisäksi on tärkeää seurata jatkuvasti uusia uhkia ja torjuntakeinoja, jotta voidaan reagoida nopeasti kehittyviin riskeihin ja suojautua mahdollisilta hyökkäyksiltä.

3 Kuvaileva kirjallisuuskatsaus opinnäytetyön menetelmänä

Kuvaileva kirjallisuuskatsaus on yleiskatsaus, joka ei noudata tiukasti määriteltyjä sääntöjä tai menetelmiä. Käytetyt aineistot ovat laajoja, eikä niiden valintaa rajoita tietyt metodiset säännökset. Kuitenkin tutkittava ilmiö voidaan kuvata kattavasti ja tarvittaessa sen ominaisuuksia voidaan luokitella tarkemmin. Kuvailevassa kirjallisuuskatsauksessa on kaksi eri suuntausta: narratiivinen ja integroiva katsaus. Narratiivinen kirjallisuuskatsaus on menetelmänä kevyempi ja se pyrkii lopputulokseen, joka on helppolukuinen. Narratiivisen

kirjallisuuskatsauksen avulla hankittua aineistoa ei ole seulottu systemaattisesti, mutta kirjallisuuskatsauksen lopputulemana on silti mahdollista saada tuloksia, joita kirjallisuuskatsauksella tavoitellaan. Narratiivisesta kirjallisuuskatsauksesta on erotettavissa kolme erilaista toteuttamistapaa, joita ovat toimituksellinen, kommentoiva ja yleiskatsaus. Toimituksellisessa toteuttamistavassa on kyse artikkelissa tai lehdessä käsiteltävään teemaan liittyvästä kirjallisuuskatsausta. Kommentoivan kirjallisuuskatsauksen tavoitteena on synnyttää keskustelua, eikä sen tavoitteena ole välttämättä synnyttää objektiivista näkemystä. Yleiskatsauksena tehtävän kirjallisuuskatsauksen tavoite on tiivistää aiemmin tehtyjä tutkimuksia. (Salminen 2011, 6-7.)

Tämä opinnäytetyö toteutetaan kuvailevana kirjallisuuskatsauksena ja tarkemmin sanottuna narratiivisena kirjallisuuskatsauksena. Toteuttamistapana käytetään yleiskatsausta. Valitulla menetelmällä on mahdollista hyödyntää kerättyä aineistoa mahdollisimman monipuolisesti ja vapaasti. Sen ansiosta hybridivaikuttamiseen liittyviä suojautumis- ja varautumiskeinoja pysytään tarkastelemaan vapaammin ja siten, että etsittäviä vastauksia on mahdollista analysoida ja vertailla jouhevammin. Menetelmä myös mahdollistaa lopputuotoksena syntyviä johdopäätelmiä tai toimintaehdotuksia, mutta ei edellytä niitä ehdottomasti.

Tutkimuskysymys, johon kirjallisuuskatsauksessa etsitään vastauksia: Millaisia suojautumis- ja varautumiskeinoja hybridivaikuttamiselta suojautumiseen on olemassa? Maantieteellisenä rajauksena on se, että suojautumis- ja varautumiskeinojen on liityttävä Suomen varautumiseen. Suojautumis- ja varautumiskeinojen arvioidaan olevan ohjeita, toimintamalleja tai käytänteitä, joilla kyetään suojautumaan tai varautumaan johonkin nimettyyn hybridivaikuttamiskeinoon tai useampaan hybridivaikuttamiskeinoon.

Opinnäytetyön aineistoa haettiin hakupalveluita käyttäen. Hakupalveluiksi valittiin Laurea Finna ja Google Scholar.

Laurea Finnasta haku tehtiin hakusanalla ”hybridivaikuttaminen”. Hakusanoja kokeillessa havaittiin, että pelkällä hybridivaikuttaminen-termillä haettaessa saadaan käsiteltäväksi sellainen määrä julkaisuja, joista on mahdollista seuloa tarkempaan tarkasteluun tulevat julkaisut. Mikäli hakuja tehdessä hybridivaikuttamisen lisäksi käytettiin muita termejä, oli havaittavissa, että suurin osa aineistosta karsiutui. Julkaisujankohdaksi säädettiin 2014-2024. Tuloksia haulilla löytyi 78 kappaletta, joista opinnäytetöitä oli 31 kappaletta. Opinnäytetyöt eivät täytä tämän tutkimuksen kriteeristöä, jonka vuoksi niitä ei tarkasteltu. Muista tuloksista seulottiin tarkempaan tarkasteluun teokset, joissa julkaisija oli tämän työn kriteeristön mukainen. Teoksia, joissa julkaisija täyttää asetetun kriteeristön, löytyi kuusi kappaletta. Laurea Finnan kautta löydettyistä teoksista etsittiin hybridivaikuttamiselta suojautumiseen liittyviä tekstejä. Tarkemmassa seulomisessa havaittiin, että yksi teos viittasi suojautumis- ja varautumismenpiteiden osalta toiseen hyväksytyyn aineistoon. Tästä syystä toinen teos jätettiin

ottamatta aineistoksi. Tämän vuoksi Laurea Finnan kautta löydetyistä teoksista viidestä etsittiin hybridivaikuttamiselta suojautumiseen liittyviä osia.

Google Scholariin tehtiin haku käyttäen termejä ”hybridivaikuttaminen+suojautuminen”. Tuloksia saatiin 54 kappaletta. Haun tulokset käytiin läpi otsikkotasolla pohtien aineistojen relevanttiutta ja julkaisun ajankohtaa. Tämän jälkeen olennaisimpiin hakutuloksiin liittyen tehtiin tarkempaa tarkastelua sen suhteen, vastaavatko tulokset tutkimuskysymykseen. Hakutuloksien tarkastelun jälkeen hyväksytyksi aineistoksi valikoitui kaksi teosta.

Aineiston valinta tehtiin hyväksymis- ja hylkäämiskriteeristöä hyödyntäen. Kriteeristöön valittiin neljä kriteeriä. Kyseiset kriteerit ovat julkaisun ajankohta, julkaisija, julkaisukieli ja tutkimuskysymykseen vastaaminen.

Hyväksytyksi ajankohdaksi asetettiin se, että aineisto on julkaistu vuonna 2014 tai sen jälkeen. Ajankohta valikoitui Venäjän vuonna 2014 toteuttaman Krimin niemimaan valtauksen mukaan. Kyseinen tapahtuma on merkittävä hybridivaikuttamisen näkökulmasta ja Krimin valtaamisen myötä hybridivaikuttamiseen ja -sodankäyntiin liittyen on alettu kiinnittämään enemmän huomiota. Ennen vuotta 2014 julkaistuja aineistoja ei hyväksytty opinnäytetyön aineistoksi.

Hyväksytyjä julkaisijoita ovat valtiolliset toimijat ja ministeriöt, valtion tutkimuslaitokset ja Euroopan unionin alaisuudessa julkaisevat toimijat sekä suomalaiset organisaatiot, oppilaitokset ja yritykset. Myös olennaisesti valtiollisiin toimijoihin, tutkimus- tai oppilaitoksiin kytköksissä olevien asiantuntijoiden tekemät julkaisut hyväksytään aineistoksi. Näiden kriteerien ulkopuolelle jäävien julkaisijoiden materiaalia ei hyväksytty materiaaliksi.

Aineiston suhteen keskityttiin Suomessa julkaistuihin ja Suomeen liittyviin julkaisuihin. Tämän vuoksi aineistoon hyväksyttiin vain suomeksi julkaistuja aineistoja. Muilla kielillä julkaistuja aineistoja ei hyväksytty aineistoksi.

Aineiston hyväksymiseksi on aineiston vastattava tutkimuskysymykseen. Tämä tarkoittaa sitä, että aineistossa on käsiteltävä hybridivaikuttamiselta suojautumista tai siltä varautumista. Aineiston ei tarvitse pohjautua kokonaisuudessaan hybridivaikuttamiselta suojautumiseen tai varautumiseen, mutta aineiston on käsiteltävä tätä teemaa. Vastauksiin voidaan hyväksyä myös sellaisia tuloksia, jotka eivät nimeä erikseen mitä hybridivaikuttamiskeinoa vastaan suojautumis- tai varautumiskeino on olemassa, mikäli ohjeen, toimintamallin tai käytänteen katsotaan liittyvän yleisesti hybridivaikuttamiselta suojautumiseen. Aineiston on kuitenkin käsiteltävä jotain hybridivaikuttamiskeinoa.

4 Tulosten esittely

Tulosten esittelyssä esitellään kustakin aineistosta havaitut tutkimuskysymykseen vastaavat löydökset. Valittuja aineistoja kertyi kokonaisuudessaan seitsemän kappaletta, joissa käsiteltiin erilaisiin hybridivaikuttamismuotoihin varautumista tai niiltä suojautumista. Aineistot olivat Suomen valtioon liittyvien toimijoiden julkaisemia tekstejä. Aineistoon hyväksytyihin materiaaleihin tutustuttiin ja aineistosta etsittiin suojautumis- ja varautumiskeinoja hybridivaikuttamiseen liittyen. Kappale on jaettu alalukuihin havaittujen suojautumis- tai varautumiskeinojen mukaan.

4.1 Yhteistyö ja viestintä

Informaatiovaikuttamiseen varautumiseen, siihen vastaamiseen sekä siitä palautumiseen liittyen yhteistyöllä on huomattava merkitys. Viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten välille on luotava mahdollisimman hyvin toimivat viestintäyhteydet jo ennen informaatiovaikuttamisen kohteeksi joutumista. (Valtioneuvoston kanslia 2019, 48.) Kansainvälistä tiedusteluyhteisöä on mahdollista hyödyntää siinä, että omia resursseja pystytään kohdentamaan tehokkaasti hybridivaikuttamiseen liittyen. (Ulkoministeriö 2022, 29.)

Informaatiovaikuttamiselta suojautumisesta ja varautumista on mahdollista tehdä tehokkaalla viranomaisviestinnällä. Viestinnän ollessa avointa, aktiivista ja monikielistä, sillä on mahdollista tavoittaa eri kohderyhmiä, vahvistaa luottamusta yhteiskuntaan, edistää turvallisuuden tunnetta ja osallistaa yksilöitä ja yhteisöjä sekä lisätä yhteenkuuluvuuden tunnetta. Viestinnän on oltava toimivaa myös kriisitilanteessa, jolloin julkisen sektorin ja suurien medioiden on kyettävä toimittamaan ajantasaista ja totuudenmukaista tietoa sekä tietoa informaatiovaikuttamisen tunnistamisesta, että sen torjumiskeinoista. Tehokas viestintä tukee hyvin kansalaisten kriisinsietokykyä. (Ulkoministeriö 2022, 30.)

Kybervaikuttamiseen varautumiseen liittyen ulkoministeriö (2022, 34) nostaa esille EU-maiden ja muiden samanmielisten maiden kanssa tapahtuvan koordinoitujen uhkien tunnistamistoiminnan ja uhkiin vastaamisen ennakoinnin. Lisäksi, koska kyberympäristö muuttuu nopeasti, on tarpeellista myös pyrkiä nopeuttamaan päätöksentekomenettelyä ja kehittää kyberdiplomatian keinovalikoimaa.

Vaalivaikuttaminen on yksi hybridivaikuttamisen ilmenemismuoto, jota on mahdollista tehdä erilaisin keinoin. Viestinnällisesti vaalivaikuttamiseen on mahdollista varautua eri viranomais- ja muiden toimijoiden välisellä yhteistyön tiivistämisellä ja tietojen vaihdolla, sekä johtamissuhteiden ja -toimintamallien suunnittelulla ennen häiriötilanteiden syntymistä. (Jääskeläinen, Sillanpää, Valtonen, Huotarinen & Toivanen 2019, 11-12.)

Viranomaisten ja sosiaalisen median yritysten välisellä yhteistyöllä on myös mahdollista suojautua vaalivaikuttamiselta. Yhteistyön tavoitteena on luoda verifioituja käyttäjätilejä luotettaville tahoille ja samalla raportoida ja mahdollisesti poistaa tilejä, jotka levittävät sosiaalisessa mediassa vääristeltyä informaatiota tai syyllistyvät joihinkin rikkomuksiin. (Jääskeläinen ym. 2019, 15.)

Lehdon ja Limnellin mukaan (2017, 208-209) kansainvälisen yhteistyön tehostaminen ja laajentaminen ovat olennaisia toimia hybridivaikuttamiselta suojautumisessa. Kansainvälisesti voidaan kehittää maiden välisiä kyvykkyksiä, harjoitella eri tavoin yhdessä ja vaihtaa tietoja toimivista käytänteistä.

Tervonen (2024, 44-45) painottaa yhteistyön merkitystä informaatiovaikuttamiselta varautumisessa ja resilienssin kasvattamisessa. Yhteistoimintaa tulisi pitää yllä viranomaisten, poliittisten päättäjien, median ja kansalaisten välillä. Viestinnälliset keinot ovat merkittävässä roolissa informaatiovaikuttamiseen varautumisessa. Viranomaisviestinnän tulee olla avointa ja aktiivista sekä sitä tulee tehdä riittävän monikielisesti, jotta tavoitetaan mahdollisimman monia ryhmiä. Myös kansainvälisellä yhteistyöllä on merkitystä informaatiovaikuttamiseen varautuessa.

4.2 Tilannekuva ja johtaminen

Ulkoministeriön (2022, 29) mukaan jatkuva uhka-arvio ja yhteistyö eri tahojen, niin kotimaisten kuin kansainvälisten, välillä ovat merkittäviä tekijöitä hybridiuhkiin varautumisessa. Tärkeää on myös haavoittuvuuksien tunnistaminen ennakkoon, jolloin haavoittuvuuksia on mahdollista hallita ennen kuin niitä on käytetty vahingon aiheuttamiseen. Hybridiuhkiin varautumisen kannalta olennaista on myös tilannekuvan luominen ja osittain päällekkäiset johtamis- ja vastuusuhteet uhkien torjunnassa.

Lehto, Limnell, Innolla, Pöyhönen, Rusi & Salminen (2017, 66) näkevät, että kyberturvallisuusuhat on mieltettävä osaksi hybridivaikuttamista. Kyberuhkiin varautuminen vaatii vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä, tilanneymmärrystä ja selkeitä johtamisvastuita ja -rooleja sekä toimivaa tiedonkulkua ja tehokasta tietojen vaihtoa.

Kyberuhkiin varautumisen kannalta tilannekuvan ja valmiiden toimintamallien rakentaminen ovat merkittävässä asemassa. Tärkeää on myös luotettavan yhteistyöverkoston rakentaminen ongelmatilanteiden varalle ja etukäteen tapahtuvan tiedonvaihdon varmistamiseksi. Kyberuhkien havaitsemis- ja torjuntakyky on ratkaiseva kyvykkyys yhteiskunnan elintärkeiden toimintojen turvaamisen osalta. Kyberuhkien havaitsemisella ja toimivalla tilannekuvalla on suuri merkitys myös ennakkovaroitusten antamiselle ylimmälle valtionjohdolle. (Lehto ym. 2017, 28-32.)

Eräiksi merkittäviksi asioiksi kyberturvallisuuden kehittämisessä Lehto ym. (2017, 67-68) kokevat strategisen johtamisen selkeyttämisen ja vahvistamisen, johon kuuluu myös vuorovaikutuksen lisääminen julkisen ja yksityisen sektorin välillä, mutta myös tiede- ja tutkimusyhteisöjen ja järjestöjen välillä. Merkittävänä tärkeäksi nähdään myös se, että Suomen poliittinen johto ymmärtää kyberympäristön aiheuttamat haasteet ja riskit ja kyberasioiden edistämiseen löytyy poliittinen tahto ja sitoutuminen. Suomen tulisi luoda julkiset tavoitteet omaan kybertoiminnan edistämiseen liittyen ja viestiä tavoitteet ja niissä edistyminen kansainvälisesti.

Lehto ym. (2017, 69-73) korostavat tilannekuvan ylläpitämisen ja kehittämisen, uusien uhkien havaitsemiskyvyn kehittämisen ja tilannekuvan riittävän tehokkaan jakamisen olevan elintärkeitä kehityskohteita kyberuhkiin varautumisessa.

Lehto ym. (2017, 69-73) mukaan kyberturvallisuuteen liittyvää koulutusta tulisi tehostaa ja koordinoida paremmin. Kyberturvallisuutta pitäisi pystyä myös mittaamaan ja arvioimaan, jonka mahdollistaa tehokkaamman kehittymisen toimialaan liittyen.

Lehto ja Limnell (2017, 208-209) kertovat kyberturvallisuuden strategisen johtamisen tehokkaan toimimisen edellyttävän tilanneymmärrystä, selkeitä rooleja ja johtovastuita sekä tehokasta tiedonvaihtoa.

4.3 Tietoisuuden lisääminen

Valmistautuessa informaatiovaikuttamiseen on tärkeää lisätä ihmisten tietoisuutta informaatiovaikuttamisen olemassaolosta ja keinoista. Proaktiivisesti on syytä myös kehittää narratiiveja ja viestejä sekä parannettava ymmärrystä ryhmien riskeistä ja haavoittuvuuksista. Valmistautumiseen liittyen tulee myös arvioida mitkä kohderyhmät ovat alttiimpia informaatiovaikuttamisella ja suunnattava oikea-aikaista ja nopeaa viestintää etenkin näille kohderyhmille. Olennaisin puolustautumiskeino informaatiovaikuttamista vastaan on ongelmien ja uhkien käsittely mahdollisimman rakentavasti ja avoimesti. (Valtioneuvoston kanslia 2019, 37-39.)

Jääskeläinen ym. (2019, 13) mainitsevat vaalivaikuttamisen varautumiskeinoiksi myös koulutautumisen ja tietoisuuden lisäämisen. Koulutus tulee suunnata viranomaisille, puolueille ja järjestöille, kun taas viestintää tulee tehdä kansalaisten suuntaan. Kansalaisille viestimisellä on mahdollista kertoa vaalivaikuttamisen tavoista ja tavoitteesta, mutta samalla myös muistuttaa kansalaisia suomalaisen vaalijärjestelmän luotettavuudesta. Viestimisellä kyetään nostamaan kansalaisten tietoisuutta vaalivaikuttamisesta ja samalla vahvistamaan kansalaisten luottamusta suomalaiseen järjestelmään.

Informaatiovaikuttamiselta suojautumisessa merkityksellistä on uhiin varautuminen laajalaisesti eri yhteiskunnallisten toimijoiden kesken. Tärkeää on väestön koulutustason nostaminen informaatiovaikuttamisen osalta, jotta yksilöt kykenevät paremmin havaitsemaan disinformaatiota ja hybridivaikuttamista. Koulutuksen osalta medialukutaidon kehittäminen on olennaista ja sen avulla tulisi pyrkiä lisäämään tietoisuutta eri disinformaatiotyypeistä ja erilaisista informaatiovaikuttamisen keinoista. (Tervonen 2024, 41-43.)

4.4 Parhaiden käytänteiden jakaminen

Viestintään liittyvien parhaiden käytäntöjen kokeileminen ja jakaminen eri ryhmien välillä auttaa valmistautumaan informaatiovaikuttamisen kohtaamiseen. Merkityksellistä on myös luottamuksen rakentaminen eri yhteiskunnan instituutioihin, sillä informaatiovaikuttamisella pyritään heikentämään ihmisten luottamusta yhteiskunnallisiin toimijoihin. Tämän takia hallinnon maine ja legitimiteetti ovat merkittävässä roolissa informaatiovaikuttamiselta varautumisessa. (Valtioneuvoston kanslia 2019, 37-39.)

Vuoden 2019 europarlamenttivaaleihin liittyen EU:n komissio perusti yhteistyöryhmän, johon nimitettiin jäsen jokaisesta EU-jäsenvaltiosta. Yhteistyöryhmän tavoitteena oli parhaiden käytäntöjen jakaminen liittyen vaalirahoitukseen, lainsäädäntöön, tiedotuskampanjoihin ja tietosuojaan. (Jääskeläinen ym. 2019, 18.)

Lehto ym. (2017, 48-62) ovat käyneet läpi Suomen verrokkimaiden kyberturvallisuuden toimintamalleja, joista he ovat poimineet Suomelle sopivia käytäntöjä ja tavoitteita. Alankomaiden osalta Suomeen sopiviksi toimintamalleiksi on katsottu jatkuva tuotteiden ja palveluiden kehittäminen kyberturvallisuuden uhkakuvia vastaan sekä julkisen ja yksityisen sektorin yhteistyön kehittäminen pidemmälle ja yhteistyön tiivistäminen. Iso-Britannian osalta Suomeen toivottaisiin innovatiiviseen kyberturvallisuuteen panostamista ja kyvykkäiden yksilöiden ja startupin tunnistamista, turvallisuusviranomaisten ja julkisen sektorin vahvistaminen kyberhyökkäysten ennakointiseksi, estämiseksi, havaitsemiseksi ja keskeyttämiseksi sekä parantamalla kyberuhkien tunnistamista ja tuntemista yhdessä teollisuudenalan kanssa. Israelin toimista Suomea hyödyttäisivät vahvemmin eri kansallisten toimijoiden osaamisen yhteen tuominen, vahva poliittinen sitoutuminen kyberturvallisuuden parantamiseen, kokonaisvaltainen kyberturvallisuus, joka sisältää tekniset ja operatiiviset kyvyt, tiedustelun, tietoisuuden lisäämisen, fyysisen ulottuvuuden ja toimivat organisaatiot. Israelista mallia toivottaisiin otettavan myös yksityisen sektorin sääntelyä lainsäädännöllä. Ruotsissa kehitetään siviilikyberpuolustusta ja kyberturvallisuus nähdään jatkumona, jossa vapaus, vastuut ja riskit muuttuvat siirtymän mukaisesti. Lehto ym. (2017, 58) kokevat, että Suomi voisi ottaa tässä asiassa mallia Ruotsista. Singaporen toiminnasta harkittavaksi voitaisiin ottaa kyberturvallisuusalan pitämisen kasvusektorina strategiatasolta alkaen ja valtionhallinnon tukema kyberosaamisen kehittäminen koululaisesta huippuasiantuntijaan asti. Viron toimintatavoista voitaisiin pohtia Viron

tapaa profiloitua kyberpuolustuksen edelläkävijämaaksi, julkisen kyberturvallisuuskatsauksen julkaisemista vuosittain ja strategian toimeenpanon arviointia ja mitattavuuden parantamista osatavoitteiden avulla.

4.5 Resilienssin kasvattaminen

Heino ym. (2023, 24-25) kertovat kollektiivisen resilienssin kasvattamisesta ja vahvistamisesta osana hybridivaikuttamisen vaikutusten vähentämisessä. Kollektiivinen resilienssi muodostuu jonkin tietyn ryhmän jakaman identiteetin kautta ja sitä on mahdollista vahvistaa muun muassa solidaarisuuden ja yhteenkuuluvuuden lisäämisellä. Tämän vuoksi on tärkeää, että julkinen sektori on tietoinen erilaisista yhteisöistä ja pyrkii mahdollistamaan eri ryhmille jaetun identiteetin syntymisen ja kehittymisen. Julkisen sektorin ja viranomaisten on käytävä kaksisuuntaista keskustelua, jotta ryhmät ja niiden yksilöt tulevat kuulluksi ja myös kokevat tulleensa kuulluksi. Keskusteluyhteyden olemassaolon avulla on mahdollista varmistaa, että ryhmillä ja yhteisöillä on saatavilla viranomaisten tarjoamaan realistista tietoa epävarmoina aikoina ja tapahtumiin liittyen on mahdollista käydä keskustelua yksipuolisen viestinnän sijasta. Heino ym. (2023, 25) nostavat merkittävämmäksi tekijäksi hybridiuhkiin varautumisen osalta yhteisöjen sisäiset ja yhteisöjen väliset suhteet ja suhteiden laadun. Suhteiden ja suhteiden laadun tarkastelu edellyttää jatkuvaa kommunikointia yhteisöjen suuntaan ja tilannekuvan ylläpitämistä.

Tervosen (2024, 41-43) mukaan resilienssin vahvistaminen kasvattamalla kansalaisten luottamusta viranomaisiin ja osallistamalla kansalaisia mukaan toimintaan ja keskusteluun on merkityksellistä hybridivaikuttamiselta suojautumisessa.

4.6 Tekniset suojautumiskeinot

Kybervaikuttamiselta suojautumisen osalta oleellisia toimia ovat tietoturvaluottoihin ja palveluihin panostaminen sekä säännöllinen kybervaikuttamistilanteisiin liittyvä harjoittelu. Harjoittelun tulee olla julkisen sektorin ja yritysten keskinäistä toimintaa, jonka avulla voidaan kehittää yhteisöjen ja yksilöiden kyberturvallisuustaitoja. Kyberuhkiin varautuminen edellyttää lisäksi laaja-alaista ja tarkkaa tilannekuvaa, jotta hyökkäyksiä on mahdollista pysäyttää tai niiden vaikutuksia saadaan rajattua. (Ulkoministeriö, 33.)

Välineellistetyltä maahanmuutolta suojautumiseen liittyen tarvittaviksi kehittämistoimiksi ulkoministeriö mainitsee laitteisto- ja materiaalihankinnat. Laitteisto- ja materiaalihankinnat pitävät sisällään rajojen tekniseen valvontaan liittyviä hankintoja ja kyberosaamiseen liittyviä hankintoja. (Ulkoministeriö 2022, 36.)

Lehto ym. (2017, 18) kiinnittävät huomiota pilvipalveluiden turvallisuuteen ja luotettavuuteen kyberuhkiin varautumisen osalta. Pilvipalveluiden konfigurointi ja pilvessä olevan datan

suojaus on varmistettava. Huomiota tulee myös kiinnittää pääsynhallintaan, johon liittyen suositellaan kaksiosaista todentamismenetelmää. Pilvipalveluiden turvallisuutta voi lisätä myös useilla eri toimenpiteillä. Tällaisia toimenpiteitä ovat muutostiedostojen ja päivitysten ajan tasalla pitäminen, tietoturvapalveluiden käyttöönotto, vahvan palomuurin käyttäminen, lokien tarkastaminen säännöllisesti, monikerroksisen suojauksen hyödyntäminen, tehokaiden tietoturvapoliitikoiden luominen ja henkilöstölle kouluttaminen, ”vähiten oikeuksia” -periaatteen noudattaminen, hyökkäyksenesto- ja tunnistusjärjestelmien käyttäminen, varmuuskopioiden taltioiminen muualle kuin toimitilaan, need-to-know -periaatteen soveltaminen ja pilvipalveluiden auditointi.

Lehto ym. (2017, 37-38) korostavat, että kyberturvallisuuden parantamiseksi, ja sitä kautta myös kybervaikuttamiselta suojautumiseksi, olisi tärkeää keskittyä ennaltaehkäisyyn ja turvallisten sisäänrakennettujen järjestelmien käyttöön ottamiseen. Olennaista on myös järjestelmien kestokyvyn kehittäminen. Järjestelmien suhteen on tarpeellista myös huomioida kyberalan nopea kehittyminen, joka edellyttää ketteryyttä ja joustavuutta.

Lehto ja Limnell (2017, 196-197) kertovat kybertiedustelun olevan merkittävässä roolissa kybertoimintaan liittyvään suojautumiseen, tilannetietoisuuteen, uhkavaroitukseen ja maalinosoitukseen liittyen. Kybersuojautumisen tavoitteena on estää hyökkääjää pääsemästä järjestelmiin ja verkkoihin sekä rajata tai lieventää hyökkääjän aiheuttamia vaikutuksia. Kybersuojaamisen pitää sisällään tietoverkoissa tapahtuvaa havainnointia, valvontaa, analysointia ja vastatoimenpiteitä. Kybersuojaamisella pyritään suojaamaan oma data ja omat johtamis- ja tietojärjestelmät. Kybersuojaamista kehitetään Puolustusvoimien, eri viranomaisten ja muiden yhteiskunnan toimijoiden kanssa.

4.7 Lainsäädäntö

Lainsäädännön muutoksilla on mahdollista varautua kyberuhkiin. Yhtenä esimerkkinä tällaisesta toimesta toimii vuonna 2021 voimaantunut laki, joka kieltää turvallisuutta vaarantavien tietoteknisten laitteiden käyttämisen kriittisissä järjestelmissä tai verkoissa. (Ulkoministeriö, 33.)

Lainsäädännön muutoksilla on mahdollista varautua myös välineellistettyyn maahanmuuttoon. Lakimuutoksilla on mahdollista luoda toimivaltaa viranomaisille rajoilla tapahtuvaan vaikuttamistoimintaan liittyen. (Ulkoministeriö 2022, 36.)

Lehto ym. (2017, 69-73) kertovat, että tärkeää on myös teknologian kehittymisen mukana pysyminen ja lainsäädännön riittävän nopea reagointi kehityksen luomiin muutostarpeisiin. Kyberala kehittyy nopeasti, jonka vuoksi lainsäädännön on reagoitava riittävällä nopeudella alan muutoksiin.

4.8 Muut suojautumiskeinot

Valtioneuvoston kanslia (2019, 41–43) kertoo neljästä eri vahvuisesta informaatiovaikuttamisen vastatoimesta. Vastatoimia tulee tässä yhteydessä pitää osana informaatiovaikuttamiseen valmistautumista, sillä vastatoimien suunnittelu on tärkeää tehdä tai ainakin aloittaa jo ennen informaatiovaikuttamistilanteen syntymistä. Vastatoimista kaksi lievempää ovat faktapohjaisia vastatoimia: arviointi ja viestiminen. Arvioinnin tullessa kyseeseen tapahtumaan liittyen tehdään tilannekartoitusta ja faktantarkistus, jonka pohjalta informoidaan tarvittavia kohderyhmiä. Viestiminen työkaluna tässä tapauksessa tarkoittaa lausunnon tekemistä ja julkaisemista sekä väärin tietojen tai väittämien korjaamista. Lausunnon yhteydessä voidaan hyödyntää ulkopuolisia toimijoita tai asiantuntijoita. Kaksi järeämpää vastatoimea ovat kannatusviestintä ja puolustautuminen, jotka ovat argumenttipohjaisia vastatoimia. Kannatusviestintää käytettäessä viestintä ei ole niin neutraalia kuin faktapohjaisissa vastatoimissa ja viestintää pyritään tekemään yhteistyössä omien avaintoimijoiden kanssa. Tapahtumaan liittyen tulee tehdä julkaista tiivistelmä tapahtumista ja tosiasioista sekä sijoittaa tilanne oman organisaation narratiiviin. Puolustamisvastatoimeen kuuluvat suorat vastatoimet informaatiovaikuttamisen tekijää kohtaan. Puolustautumiseen turvauduttaessa on mahdollista sivuuttaa hyökkäys, mikäli arvioidaan, ettei siihen ole tarvetta reagoida. Mahdollista on myös tehdä ilmoitus rikkomuksista tai rikoksista ja asettaa esto informaatiovaikutusta käyttävälle toimijalle tai poistaa käyttäjätili. Puolustautumiseen kuuluu myös esimerkiksi valetilin takana toimivan tekijän paljastaminen.

Hybridivaikuttamisen tehokkuus perustuu osittain psykologiseen vaikutukseen, jonka vuoksi on tärkeää ymmärtää ihmisen psykologisia reaktioita pohdittaessa hybridivaikuttamiseen varautumista tai suojautumista. Tämä pätee etenkin informaatiovaikuttamiseen. (Heino, Korkalainen, Lassander, Ojanen & Tuominen 2023, 7.)

Vuoden 2019 eduskuntavaaleihin ja europarlamenttivaaleihin liittyen oli perustettu vaali-VIRT-ryhmä, jonka tehtävänä oli muun muassa tietotarpeiden kartoitus ja tiedonvaihdon käytännöistä sopiminen. Tällä tavoin vaalivaikuttamisen varalta kyettiin varautumaan sopimaan käytännöistä ja eri viestimistavoista, jolloin toiminta kriisitilanteessa on tehokkaampaa ja jouhevampaa. (Jääskeläinen ym. 2019, 16.)

Insider-uhkiin liittyen Lehto ym. (2017, 19) kertovat kartoitustarpeesta siihen liittyen, kenellä sisäpiiriin kuuluvilla on luottamuksellisia käyttöoikeuksia. Sisäpiiriin kuuluvien on mahdollista ohittaa tietoturvakontrolleja, joita ulkopuolisen hyökkääjän varalle on tehty.

Lehto ym. (2017, 20) viittaavat ENISA:n tekemään tutkimukseen, jossa on ehdotettu kybertoimintaryhmien perustamista. Kybertoimintaryhmien tavoitteena olisi saada vapaaehtoisia ryhmiä mukaan kyberriskien torjuntaan ja kyberpuolustusaloitteisiin.

Kyberuhkiin varautumisiin liittyviin strategisiin toimintatapoihin liittyen Lehto ym. (2017, 23) nostavat esille viisi AT&T raportissa mainittua seikkaa: kulttuuri, kyberturvallisuus liiketoiminnan osana, työkalut ja sovellukset, kumppanuudet ja rahoitus. Kulttuurilla viitataan tässä yhteydessä siihen, että kyberturvallisuuden on oltava organisaation kulttuurin perusta. Liiketoiminnan suhteen on tärkeää, että kyberturvallisuus otetaan huomioon teknologia- ja liiketoimintapäätöksissä. Työkalut ja sovellukset on oltava tehokkaita ja ajantasaisia niin torjuntaan kuin tiedon ja varojen suojaamiseenkin liittyen. Organisaation tulee myös pohtia, millaisen kumppanin kanssa organisaation kyberturvallisuutta on mahdollista kehittää. Tämän lisäksi on syytä arvioida tulisiko kumppaneita olla useampia. Rahoitus liittyy olennaisesti työkaluihin ja sovelluksiin, sillä erilaisiin kyberturvallisuushankintoihin on varattava riittävä rahoitus.

Yksi keino, jolla kybervaikuttamiseen on mahdollista varautua pitkän aikavälin keinoin, on kyberturvallisuuden opettamisen sisällyttäminen eri koulutusasteisiin aina perusopetuksesta korkeakouluopetukseen asti. Kyberturvallisuuteen liittyviä asioita tulisi opettaa opetustasojen mukaisesti vahvistaen osaamistasoa opetustasojen noustessa. Kyberturvallisuuden opetus myös aikuiskoulutuspuolella edistäisi kybervaikuttamiseen varautumista. (Lehto ym. 2017, 34-35.)

Kyberuhkiin liittyen on tärkeää saada riittävästi havaintoja poikkeavista tapahtumista. Osassa tilanteista eri toimijat ovat juridisesti velvoitettuja ilmoittamaan häiriötilanteista, mutta niiden hallinta, analysointi, selvittäminen ja niihin varautuminen vahvistuisi, mikäli toimijat ilmoittaisivat myös häiriötilanteista, joissa ilmoittamispakkoa ei ole. Eri hallinnonaloille olisi tarpeellista tehdä myös riskiarvioinnit ja kypsyyssanalyysit, joiden pohjalta tulisi laatia toimenpano-ohjelmat huoltovarmuusorganisaation kanssa toimimista helpottamaan. (Lehto ym. 2017, 36.)

Niin Puolustusvoimien kuin suomalaisen yhteiskunnan yleisestikin tulee pyrkiä huolehtimaan riittävästä kyberomavaraisuudesta liittyen kriittisiin yrityksiin ja teknologiaratkaisuihin. Osavat tekijät ja muut toimijat olisikin hyvä saada motivoitua pysymään Suomessa, jotta heidän panostaan voidaan hyödyntää osana kansallista kyvykkyyttä. (Lehto & Limnell 2017, 207.)

Tervonen (2024, 46-48) kertoo Ukrainan käyttämistä Venäjän informaatiovaikuttamisen suojauskeinoista. Ukraina on rajoittanut venäläisten medioiden ja internetsivujen toimintaa, jotta informaatiovaikuttamisen kanavia olisi vähemmän. Ukraina oli myös valmistellut omaa viestintäänsä varten varakanavia, jotka otettiin käyttöön Venäjän iskun kaataessa Ukrainan pääviestintäkanavat. Ukrainassa on myös onnistuneesti hyödynnetty siviiliorganisaatioita internetissä leviävän disinformaation tunnistamisessa ja sen kiistämisessä sekä venäläisten narratiivien tunnistamisessa ja niihin reagoimisessa. Ukrainalaiset ovat pyrkineet löytämään valheellista informaatiota tuottavan tahon ja paljastamaan sen. Ukraina on hyödyntänyt omassa

viestinnässään myös huumoria ja meemejä, joiden avulla se on saanut levitettyä omaa narraatiiviaan sosiaalisessa mediassa tehokkaasti.

5 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli selvittää, millaisia suojautumiskeinoja hybridivaikuttamista vastaan on olemassa suomenkielisten julkaisujen perusteella. Aineistoiksi valittujen teoksien tuloksista oli havaittavissa yhdeksän eri keinoa, jotka auttavat varautumaan ja suojautumaan hybridivaikuttamiselta. Tässä luvussa käydään läpi kyseiset keinot ja pohditaan miten eri toimijoiden tulisi pyrkiä toimimaan kuhunkin keinoon liittyen, jotta hybridivaikuttamiselta suojautuminen olisi mahdollisimman tehokasta.

Merkittävämpänä suojautumiskeinona aineistosta nousi esiin yhteistyö. Yhteistyö itsessään ei ole tarkka määritelmä suojautumiskeinoksi, mutta yhteistyön merkitystä korostettiin aineistossa niin voimakkaasti, että yhteistyö on syytä nostaa yhdeksi arvioitavaksi toiminnaksi. Yhteistyö liittyy myös olennaisesti useisiin muihin suojautumiskeinoihin. Yhteistyötä tulee tehdä niin ryhmien, yhteisöjen ja organisaatioiden sisällä, mutta myös eri toimijoiden välillä. Kansainvälinen yhteistyö on suuressa roolissa, kun halutaan jakaa ja vastaanottaa hybridivaikuttamiseen liittyvää tietoa mahdollisimman tehokkaasti. Yhteistyön edistämiseksi on tarpeellista rakentaa toimivat yhteistyökanavat ja verkostoitua eri toimijoiden kanssa proaktiivisesti. Yhteistyön varmistamiseksi on tärkeää, että kommunikointikanavat ja varakanavat on sovittu jo ennen varsinaista hybridivaikuttamistilannetta.

Tilannekuvan muodostaminen ja ylläpitäminen ovat aineiston perusteella erittäin olennaisia hybridivaikuttamiselta varautumiseen liittyen. Tilannekuvan muodostaminen on edellytys tehokkaalle hybridivaikuttamisen havaitsemiselle. Ilman toimivaa ja jatkuvasta päivitettävää tilannekuvaa hybridivaikuttamiselta suojautuminen on tehotonta tai jopa mahdotonta. Tilannekuva on myös jaettava sitä eniten tarvitseville toimijoille. Eri organisaatioiden on tarpeellista pitää yllä tilannekuvaa omaan toiminta-alueeseensa liittyen. Suurin vastuu toimivasta tilannekuvasta on organisaation johdolla ja johtohahmoilla. Mikäli tilannekuvan merkityksellisyys sivuutetaan ja jätetään huomioitta, ei hybridivaikuttamiskeinojen havaitseminen ja niistä sidosryhmille tiedottaminen ole tehokasta. Yksilöiden osalta tilannekuva edellyttää kullekin yksilölle asetettujen tehtävien suorittamista.

Tietoisuuden lisääminen on aineiston perusteella yksi suositelluimmista keinoista hybridivaikuttamiselta suojautumisessa. Aineistossa puhutaan myös ymmärryksen parantamisesta, joka liittyy tietoisuuden lisäämiseen. Tietoisuuden lisäämisellä ja ymmärryksen parantamisella pyritään vahvistamaan jokaisen yhteiskunnassa toimivan tietoja erilaisista hybridivaikuttamiskeinoista ja niiden ilmenemistavasta. Tietoisuuden lisääminen auttaa varautumaan ja ennalta

estämään useita eri hybridivaikuttamistapoja, sillä monien hybridivaikuttamiskeinojen toimiminen edellyttää kohteina olevien yksilöiden tietämättömyyttä tai ymmärtämättömyyttä. Esi-merkeiksi tällaisista tilanteista voi käyttää informaatiovaikuttamista ja kybervaikuttamista. Informaatiovaikuttaminen on tehokasta, mikäli vaikuttamisen kohteena oleva henkilö uskoo vastaanottamansa informaation ilman tiedon levittämisen tarkoituksen pohdintaa. Informaatiovaikuttamisen ja sen välittämisen keinojen ymmärtäminen ja tarkkailu edistävät huomattavasti informaatiovaikuttamisen toimimista. Kybervaikuttamisen osalta yksilöiden on mahdollista torjua kybervaikuttamista omalta osaltaan pitämällä omat tietotekniset laitteensa suojattuina ja päivittämällä ohjelmistot tarvittaessa.

Lainsäädännön merkitystä korostettiin osassa aineistoista. Uusia hybridivaikuttamisen keinoja tulee ilmenemään myös tulevaisuudessa. On tärkeää, että lainsäädännöllä voidaan mahdollistaa työkalut, joilla sekä nykyisiin että myöhemmin ilmeneviin hybridivaikuttamiskeinoin pysytään vaikuttamaan. Lainsäädännön tehokkuus on eduskunnan vastuulla, joten itse lainsäädännön nopeuden ja toimivuuden osalta tärkeimmät toimijat ovat kansanedustajat ja eduskunnan virkahenkilöstö. Yksittäiset yksilöt voivat vaikuttaa lainsäädännön osalta kansalaisaloitteiden kautta, mutta myös äänestämällä ehdokkaita, jotka tiedostavat lainsäädännön merkityksen liittyen hybridivaikuttamiselta suojautumiseen.

Johtaminen ei ole itsessään suojautumiskeino hybridivaikuttamiselta, mutta johtaminen esiintyi useaan kertaan aineistoa tutkittaessa. Organisaatioiden johdon tulee tiedostaa hybridivaikuttamisen olemassaolo ja pyrkiä päätöksillä edesauttamaan hybridivaikuttamiseen varautumiskeinojen ja -suojautumiskeinojen käyttöönottoa. Johtamisen osalta olennaista on tilanteen ymmärtäminen, roolituksien jakaminen ja johtovastuun määrittelemineen. Johdon on oltava sitoutunut organisaatiossa tapahtuvaan harjoitustoimintaan hybridivaikuttamiselta suojautumiseksi.

Parhaiden käytänteiden ja käytäntöjen jakaminen yhteistyökumppanien kanssa koetaan myös toimivaksi keinoksi varautua hybridivaikuttamiseen. Käytänteiden ja käytäntöjen jakaminen liittyy suoraan jo edellä mainittuun yhteistyöhön, mutta aineistosta oli havaittavissa, että toimivien toimintamallien levittäminen yhteistyökumppaneille on oma olennainen varautumiskeinonsa. Käytänteiden ja käytäntöjen toimivuuden tiedostaminen edellyttää organisaatioilta oman toiminnan tarkastelua ja mittaamista. Parhaat käytänteet ja käytännöt saadaan esille vain, jos niiden vaikutusta seurataan objektiivisesti. Käytänteiden ja käytäntöjen jakamisen sijaan vaatii yhteistyösuhteiden luomisen ja viestintäkanavista sopimisen.

Resilienssin vahvistaminen ja kasvattaminen on yksi tapa, jolla voidaan vähentää hybridivaikuttamisen tehoa tai jopa ennalta ehkäistä sen toimiminen. Resilienssiä on mahdollista parantaa luomalla ryhmien välistä ja ryhmien sisäistä yhteenkuuluvuuden tunnetta sekä parantamalla yksilöiden luottamusta yhteiskunnallisiin toimijoihin. Tähän liittyy myös erilaisten

ryhmien tavoittaminen, joiden suhteen tilannekuvalla ja viestinnällä on olennainen roolinsa. Erilaisille yksilöille ja ryhmille on osattava viestiä eri tavoin, koska muutoin viestintä ei ole tehokasta. On otettava huomioon se, että toimijoilla on ennakkokäsityksiä sekä yksilöinä että ryhmässä muodostuneita ajatuksia, jonka vuoksi viestintä tulee räätälöidä vastaanottajan mukaan.

Aineistosta havaittujen suojautumis- ja varautumiskeinojen perusteella on mahdollista nostaa esille muutamia toimenpiteitä, joiden avulla on mahdollista parantaa hybridivaikuttamiselta suojautumiseen. Seuraavaksi käydään läpi joitain tuloksista havaittuja suojautumistapoja, joita organisaatioiden on mahdollista hyödyntää omassa toiminnassaan.

Yhteistyö, viestintä ja parhaiden käytänteiden jakaminen linkittyvät jossain määrin toisiinsa. Hybridivaikuttamiseen liittyen on olennaista, että tietoa hybridivaikuttamisen kohtaamisesta ei pidetä omana tietona, vaan tapahtumasta kerrotaan omille yhteistyötahoille ja haetaan apua tai vinkkejä hybridivaikuttamisen kanssa toimimiseen. Tärkeää on myös, että ollaan valmiita auttamaan, mikäli apua pyydetään. Tiedon panttaaminen omilta yhteistyötahoilta, oli kyseessä sitten kohdattu vaikuttaminen tai hyväksi havaittu käytäntö, ei hybridivaikuttamiselta suojautumiseen liittyen ole koskaan järkevä vaihtoehto. Yhteistyökumppaneiden kanssa on olennaista sopia viestimistavoista ja -väylistä mahdollisimman pian yhteistyön aloittamisen jälkeen ja viestintäkanavia on hyvä käyttää myös kriisiajan ulkopuolella. Tulee myös huolehtia, että viestintään on olemassa useampia tapoja, sillä pääasiallisessa käytössä olevat viestintätavat eivät välttämättä kriisitilanteessa ole käytettävissä.

Johtaminen, tilannekuvan muodostaminen ja tietoisuuden levittäminen ovat myös asioita, joita on mahdollista parantaa jokaisessa organisaatiossa. Olennaista on se, että organisaation johto ymmärtää hybridivaikuttamisen olevan mahdollista myös omaan organisaatioon kohdistuen tai oma organisaatio tai sen osa voi olla osana hybridivaikuttamistilannetta. Johdon ollessa tietoinen riskeistä, on mahdollista, että organisaatio luo omaan toimintaansa liittyen tilannekuvan, jossa arvioidaan omaan toimintaan liittyvät tilanteet, joissa hybridivaikuttamista on mahdollista ilmetä. Tilannekuvaa ja riskien arviointia on pidettävä yllä periaatteessa jatkuvasti. Kun tilannekuva ja riskit ovat selvillä, niihin on mahdollista kehittää organisaation sisäisiä suojautumiskeinoja tai valmistautua muuten riskien varalle. Muita varautumistapoja voisi olla esimerkiksi prosessien pohtiminen hybridivaikuttamistapauksen varalle. Tällöin organisaatiolla on valmiiksi pohdittuna toimenpiteet ja niiden tekijät, mikäli hybridivaikuttamista ilmenee. Kun organisaatio tiedostaa olemassa olevat riskit ja varautuu niihin, on hybridivaikuttamisen tehokkuutta mahdollista samalla pienentää viestimällä henkilöstölle ja sidosryhmille hybridivaikuttamiseen varautumisesta ja hybridivaikuttamisen tavoista, joita on havaittu.

Kokonaisuudessaan hybridivaikuttamiselta suojautuminen ja siihen varautuminen on enemmän kuin vain yksittäisiä keinoja. Suojautuminen ja varautuminen vaikuttaakin olevan prosessi, jossa eri keinot ja toiminnot liittyvät toisiinsa ja vahvistavat tai heikentävät toisiaan sen mukaan, kuinka hyvin toiminnot hoidetaan. Prosessia on syytä mitata ja tarkkailla jatkuvasti ja kehitystä edellyttäviä huomioita tehtäessä, prosessia tulee myös muokata ja parantaa. Hybridivaikuttamisen tapoja on lukuisia erilaisia, mutta parhaiten hybridivaikuttamiselta pystyy suojautumaan huolehtimalla siitä, että organisaatio tai yksilö tiedostaa hybridivaikuttamisen mahdollisuuden ja ymmärtää, mikäli on tällaisen kohteeksi joutunut. Hybridivaikuttamisen kohtaaminen tai sen kohteeksi joutuminen ei tarkoita, ettei mitään olisi enää tehtävissä. Usein on keinoja, joiden avulla hybridivaikuttamisen vaikutuksen voi katkaista, mutta tapahtuman arvioinnilla ja siitä muille viestimällä voidaan parantaa muiden varautumismahdollisuuksia samankaltaista toimintaa vastaan.

6 Pohdinta

Hybridivaikuttamista voi tehdä lukuisin eri tavoin mutta opinnäytetyössä ei kyetty vastaamaan käsitellyn aineiston perusteella kovin yksityiskohtaisesti eri hybridivaikuttamisen muotoihin. Poliittiseen ja diplomaattiseen vaikuttamiseen liittyen ei löydetty yhtäkään suojautumiskeinoja. Siihen, ettei suojautumis- tai varautumiskeinoja löytynyt, voi osaltaan syynä olla se, että poliittiseen ja diplomaattiseen vaikuttamiseen liittyvät suojauskeinot ovat luonteensa vuoksi salassa pidettäviä. On mahdollista, jopa todennäköistä, että niihin liittyen on varauduttu, mutta aineistoa ei ole salassapidon vuoksi saatavilla julkisista lähteistä. Myöskään taloudelliseen vaikuttamiseen liittyen ei havaittu suojautumiskeinoja.

Opinnäytetyö vastaa tutkimuskysymykseen melko hyvin. Tutkimusaineisto on luotettavaa, mutta aineisto ei ollut kovin monipuolisia. Suurin osa kybervaikuttamiseen liittyvästä aineistosta oli osittain samojen henkilöiden tekemää, jonka vuoksi suojautumiskeinoista ei saatu kattavaa kuvaa, sillä samoja suojautumiskeinoja käsiteltiin useammassa eri aineistossa. Tässä opinnäytetyössä ongelmaksi suppean aineiston osalta muodostui rajaukset aineiston hyväksymiskriteereissä ja aineiston etsimisessä käytetyt hakusanat sekä palvelut, joista aineistoa haettiin. Mikäli aineistoon olisi hyväksytty myös muita, kuin suomenkielisiä lähteitä, aineisto olisi ollut varmasti monipuolisempi. Tosin tämän opinnäytetyön yhtenä tavoitteena oli selvittää nimenomaan suomenkielisten lähteiden sisältöä hybridivaikuttamisen suojautumiskeinoihin liittyen, joka on jälkikäteen pohdittaessakin relevantti tekijä. Aineistoa olisi voitu kuitenkin hakea useampaa palvelua hyödyntäen ja muokkaamalla hakuheitoja. Todennäköisesti hakuheitojen muokkaaminen jo käytettyjen palveluiden osalta olisi tuonut erilaisia aineistoja tarkasteltavaksi. Esimerkkinä tästä voi käyttää taloudelliselta vaikuttamiselta suojautumista, johon aineistosta ei löydetty suojautumiskeinoja. Eri hakusanoin olisi ollut voinut olla

mahdollista löytää suojautumiskeinoja taloudelliseen vaikuttamiseen, mutta nyt suojautumiskeinoja siihen ei löydetty ainoatakaan.

Jatkossa voisi olla aiheellista tehdä tutkimus, jossa keskitytään vain joltain tietyltä hybridivaikuttamiskeinolta suojautumiseen. Tämä mahdollistaisi pureutumisen vielä syvemmin kyseen vaikuttamiskeinon ja siltä suojautumiseen. Yksi tutkimuslähtökohta voisi olla myös jonkin tietyn suojautumiskeinon tutkiminen, jolla pyrittäisiin selvittämään, kuinka suojautumiskeinoa on mahdollista hyödyntää paremmin tai onko suojautumiskeinoa mahdollista parantaa jotenkin.

Tulevaisuudessa aihetta olisi syytä tutkia hyödyntämällä myös kansainvälistä aineistoa tai muita kuin suomenkielisiä aineistoja. Suomenkieliseen aineistoon keskittyminen on melko suurella todennäköisyydellä rajannut pois tehokkaita suojautumiskeinoja, joita olisi ollut löydettävissä muulla kuin suomeksi kirjoitetuista aineistoista. Yksi pohdittava seikka on, että käytettyjen hakusanojen avulla suomenkielinen aineisto ei ollut niin monipuolista kuin olisi voinut toivoa. Tämän takia voidaan päätellä, että suomenkielistä aineistoa hybridivaikuttamiselta suojautumiseen liittyen olisi mahdollisesti tarvetta lisätä. Yksi seuraava tutkimusaihe voisikin olla selvittää ulkomaisista aineistoista suojautumiskeinoja ja kirjoittaa löydöksistä tutkimus suomeksi. Tämä mahdollistaisi suojautumiskeinojen kattavamman saatavuuden myös suomeksi.

Olisi hyvä, että jatkossa suojautumis- tai varautumiskeinoin liittyviin tutkimuksiin saataisiin vielä enemmän konkreettisia suojautumiskeinoja. Osa tämän opinnäytetyön suojautumista-voista on enemmän strategisen tason keinoja. Strategisen tason suojautumiskeinot ovat tietenkin olennaisia ja niiden avulla voidaan ohjata myös käytännön toimintaa. Kuitenkin olisi mahdollista tehdä tutkimusta, joissa keskityttäisiin enemmän konkreettisiin toimenpiteisiin.

Lähteet

Aaltola, M., Mikkola H., Juntunen T., Vihma A. & Wigell M. 2018. Hybridivaikuttaminen ja demokratian resilienssi. Ulkopoliittinen instituutti. Viitattu 13.10.2024.

https://www.fiia.fi/wp-content/uploads/2018/05/fiia_report55_web_hybrdivaikuttaminen-ja-resilienssi.pdf

Giannopoulos, G., Smith, H. & Theocharidou, M. 2021. The Landscape of Hybrid Threats: A Conceptual Model Public Version. Euroopan unioni ja Hybridiosaamiskeskus. Viitattu 13.10.2024.

https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

Günther, K., Hasanen, J. & Juhila, K. 2021. Johdanto: Analyysi ja tulkinta. Tietoarkisto. Viitattu 10.10.2024.

<https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/analyysi-ja-tulkinta/>

Heino, M., Korkalainen, E., Lassander, M., Ojanen V. & Tuominen J. 2023. Keskustelupaperi: Kognitiivinen intruusio. Miksi hybridivaikuttaminen toimii? Käyttäytymistieteellinen ennakointi ja tieto tulevaisuuden hallinnossa. Valtioneuvoston kanslian julkaisuja 2023:14. Viitattu 18.11.2024.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165102/VNK_2023_14.pdf;jsessionid=3B4E3369C93F186700EF501EC68A299E?sequence=1

Henschke, A., O'Connor, C. & Sussex, M. 2020. Countering foreign interference: election integrity lessons for liberal democracies. Journal of Cyber Policy. Viitattu 20.11.2024.

<https://www.tandfonline.com/doi/epdf/10.1080/23738871.2020.1797136?needAccess=true>

Hybridiosaamiskeskus 2024a. COI Hybrid Influence. Viitattu 9.10.2024. <https://www.hybridcoe.fi/coi-hybrid-influencing/>

Hybridiosaamiskeskus 2024b. Hybrid threats as a concept. Viitattu 11.11.2024.

<https://www.hybridcoe.fi/coi-hybrid-influencing/>

Juhila, K. 2021. Koodaaminen. Tietoarkisto. Viitattu 10.10.2024.

<https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/koodaaminen/>

Jääskeläinen, A., Sillanpää, A., Valtonen, V., Huotarinen, H. & Toivanen, J. 2019. Vaalivaikuttamisen koulutushankkeen loppuraportti. Valtioneuvoston julkaisuja 2019:22. Viitattu 22.11.2024.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161669/VN_22_19_Vaalivaikuttamisen%20koulutushankkeen%20loppuraportti.pdf;jsessionid=EEF906E80052349C0BBC2D7F0C5AC40E?sequence=1

Kytömaa, E. 2024. Hybridiuhat ja hybridi vaikuttaminen. Sisäministeriö. Viitattu 9.10.2024.
<https://intermin.fi/kansallinen-turvallisuus/hybridiuhat>

Lehto, M. & Limnell, J. 2017. Kybersodankäynnin kehityksestä ja tulevaisuudesta. Artikkelitiede ja ase -artikkelikokoelmasta 75. Viitattu 23.11.2024.
<https://journal.fi/ta/issue/view/4726>

Lehto, M., Limnell, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Viitattu 23.11.2024.
https://valtioneuvosto.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi.pdf

Maigre, M. 2022. Cyber threat actors: how to build resilience to counter them. COI Hybrid Influence. Viitattu 8.11.2024.
<https://www.hybridcoe.fi/wp-content/uploads/2022/02/20220209-Hybrid-CoE-Paper-11-Cyber-threat-actors-WEB.pdf>

Möller, M. 2020. Ilmiöstä aikakauteen? Hybridikäsitteet tarkastelussa. Kandidaatin tutkielma. Jyväskylän yliopisto. Viitattu 13.10.2024.
<https://jyx.jyu.fi/bitstream/handle/123456789/69223/URN%3ANBN%3Afi%3Ajyu-202005263475.pdf?sequence=1>

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. Viitattu 11.11.2024.
https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Sisäministeriö. 2022. Varautuminen muuttoliikettä hyväksikäyttävään hybridi vaikuttamiseen. Maahanmuutto | Sisäministeriön julkaisuja 2022:20. Viitattu 19.11.2024.
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163861/SM_2022_20.pdf?sequence=4

Tervonen, R-M. 2024. Informaatio vaikuttamiseen varautuminen ja informaatiopuolustus - kokonaisvaltaista varautumista ja yhteiskunnallista resilienssiä. Teoksessa Sodan usvaa III: varautuminen, valmius ja nykyaikainen sodankäynti. Maanpuolustuskorkeakoulu. Toim. Kallio-maa, Mika. Viitattu 22.11.2024.

https://www.doria.fi/bitstream/handle/10024/189683/Palokangas%20et%20al.%20-%20So-dan%20usvaa%20III_verkkoversio.pdf?sequence=6&isAllowed=y

Tiilikainen, T. 2024. Herrasmieshakkerit-podcastin jakso Hybridiuhkien äärellä, vieraana Teija Tiilikainen. Julkaistu Spotify-palvelussa 19.2.2024.

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Viitattu 9.10.2024.

<https://turvallisuuksomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf>

Turvallisuuspolitiikan tietopankki 2024a. Kyberuhat ja tietoverkkovaikuttaminen. Kadettikunta ry. Viitattu 8.11.2024.

<https://turpopankki.fi/turvallisuushaasteita/hybridi-ja-kybervaikuttaminen/kyberuhat-ja-tie-toverkkovaikuttaminen/#toggle-id-1>

Turvallisuuspolitiikan tietopankki 2024b. Hybridivaikuttamisen keinovalikoima. Kadettikunta ry. Viitattu 11.11.2024.

<https://turpopankki.fi/turvallisuushaasteita/hybridi-ja-kybervaikuttaminen/hybridivaikuttamisen-keinovalikoima/#toggle-id-1>

Ulkoministeriö. 2022. Ajankohtaisseurantatieto turvallisuusympäristön muutoksesta. Valtioneuvoston julkaisu 2022:18. Viitattu 18.11.2024.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163999/VN_2022_18.pdf;jsessionid=991A87C312D016F57C031EEE9224A57C?sequence=1

Valtioneuvoston kanslia 2019. Informaatiovaikuttamiseen vastaaminen, opas viestijöille. Viitattu 9.10.2024.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161512/VNK_11_2019_Informaatiovaikuttamisen%20vastaaminen_web.pdf

Valtioneuvoston kanslia 2023. Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa. Viitattu 13.10.2024.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164793/VN_2023_31.pdf;jsessionid=243DD1CC460595115F5BD71326398876?sequence=1