Maria Keinonen

KYBEROPERAATIOIDEN KÄYTTÖ PELOTEVAIKUTUSTEN LUOMISEEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Keinonen, Maria
Kyberoperaatioiden käyttö pelotevaikutusten luomiseen
Jyväskylä: Jyväskylän yliopisto, 2023, 65 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tutkimuksessa selvitettiin kyberoperaatioiden käyttöä valtion pelotevaikutusten luomiseen. Tutkimuksen tavoitteena oli määritellä kyberpelote, löytää sen yhteys valtion pelotteeseen ja määritellä keinoja kyberoperaatioiden käytöstä pelotevaikutusten luomiseen. Tutkimuksen tarkoituksena oli luoda teoreettinen tietopohja käsitellystä aiheesta. Tutkimuksen päätutkimuskysymykseksi asetettiin: Miten kyberoperaatioita voidaan käyttää pelotevaikutusten luomiseen?

Tutkimus toteutettiin hermeneuttisen tieteenfilosofian mukaisesti aineistolähtöisenä sisällönanalyysinä. Tutkijan esiymmärryksen ohjaamana asetettiin kolme teemaa, joiden mukaan aineisto kerättiin ja analysoitiin. Nämä teemat olivat pelote, kyberpelote ja kyberoperaatiot. Analyysin edetessä lähdeaineistoa teemoiteltiin ja tyypiteltiin, lopuksi havainnot koottiin synteesiksi.

Tutkimuksen ensimmäisten analyysikierrosten aikana tehtiin kaksi havaintoa, jotka ohjasivat analyysin jatkamista. Ensinnäkin, Toisen maailmansodan jälkeen syntynyt jako kielto- ja rankaisupelotteeseen on perustavanlaatuinen. Vaikka globaalin uhkaympäristön ja kybertoimintaympäristön kehitys ovat asettaneet uudenlaisia vaatimuksia pelotestrategioille, pohjautuvat ne kuitenkin mainitulle kahtiajaolle. Toisekseen, kyberpelote on haastavaa rakentaa pelkin kybersuorituskyvyin kybertoimintaympäristössä tapahtuvaksi toiminnaksi muun muassa attribuutiohaasteen ja valtioiden pyrkimyksen salata kybersuorituskykynsä takia. Tämän vuoksi kybertoimintaympäristön suvereniteetin suojeleminen edellyttää valtion voiman instrumenttien, kuten poliittisten ja taloudellisten sekä lakia ja informaatioympäristöä hyödyntävien keinojen käyttöä.

Tutkimuksen lopputuloksena voidaan todeta, että jokaista kyberoperaatioiden tyyppiä; hyökkäyksellisiä ja puolustuksellisia kyberoperaatioita sekä JOJÄ-operaatioita, voidaan käyttää valtion pelotevaikutusten luomiseen. Kyberoperaatioilla, etenkin JOJÄ- ja puolustuksellisilla kyberoperaatioilla, on selkeä rooli pelotteen luomisessa kybertoimintaympäristössä tai sen välityksellä tapahtuvia uhkatoimia vastaan. Puolustukselliset kyberoperaatiot yhdessä JOJÄ-operaatioiden kanssa luovat kyberturvallisuutta ja resilienssiä, jotka puolestaan toimivat erityisesti kieltopelotteen keinoina. Hyökkäykselliset kyberoperaatiot toimivat parhaiten osana rankaisupelotetta, johon liittyy asevoiman käytön lisäksi myös poliittiset ja taloudelliset keinot.

Asiasanat: Kyberpelote, pelote, kyberoperaatio, kybertoimintaympäristö

ABSTRACT

Keinonen, Maria
Using Cyber Operations as a Deterrent
Jyväskylä: University of Jyväskylä, 2023, 65 pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

This study investigated the use of cyber operations as a deterrent. The goal was to define cyber deterrence, find its connection to deterrence strategies, and define ways to use cyber operations as deterrents. The purpose of the research was to create a theoretical base on the discussed topic. The main research question of the study was: How can cyber operations be used as deterrents?

The research was carried out in accordance with the hermeneutic philosophy of science as a material-oriented content analysis. Guided by the researcher's pre-understanding, three themes were set according to which the material was collected and analyzed. These themes were deterrence, cyber deterrence and cyber operations. As the analysis progressed, the source material was themed and typified, and finally, the findings were compiled into a synthesis.

During the first rounds of analysis of the study, two findings occurred, which guided the continuation of the analysis. First, the division between deterrence by denial and deterrence by punishment created after the Second World War is fundamental. Although the development of the global threat environment and cyberspace have set new requirements for deterrence strategies, they are nevertheless based on the aforementioned division. Second, it is challenging to build cyber deterrence into an activity that takes place in cyberspace with only cyber capabilities due to, among other things, the attribution challenge and the efforts of states to conceal their cyber capabilities. Therefore, protecting the sovereignty of cyberspace requires the use of instruments of state power, such as political and economic means, as well as means that utilize the law and the information environment.

As a result of the study, it can be stated that each type of cyber operations; offensive and defensive cyber operations, as well as C5 operations, can be used as deterrents. Cyber operations, especially C5 and defensive cyber operations, have a clear role in creating deterrence against threats that take place in or through cyberspace. Defensive cyber operations together with C5 operations create cyber security and resilience, which in turn act especially as means of deterrence by denial. Offensive cyber operations work best as part of deterrence by punishment, which involves not only the use of armed force but also political and economic means.

Keywords: Cyber Deterrence, Deterrence, Cyber Operation, Cyberspace

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

1.1 Tausta

Turvallisuusympäristö on muuttunut 2000-luvulla epävakaammaksi. Voimapolitiikka on palannut valtioiden strategioihin ja näkyy esimerkiksi Venäjän pyrkimyksinä vahvistaa suurvalta-asemaansa ja Naton painopisteen muuttumisena rauhaturvaoperaatioista Euroopan puolustuksen vahventamiseen. Hybridiuhkat ovat nousseet turvallisuusympäristön keskiöön ja tätä kautta rajanveto normaaliolojen ja poikkeusolojen välillä on hämärtynyt. (Valtioneuvosto, 2018)

Hybridiuhkien ilmentymisen myötä myös syyt eritasoisten konfliktien aloittamiseen ovat moninaistuneet ja ottavat muotonsa politiikan, kulttuurin, talouden, uskonnon ja etnisyyden varjolla. Kybertoimintaympäristö tarjoaa huokean ja helppokäyttöisen väylän vaikuttamiseen. Kyberkonflikteissa valtioiden toimintakenttä on muuttunut puhtaasti sotilaallisesta kontekstista kansalliseen, samalla konfliktin kohteet tai ratkaisu eivät nojaa vain sotilaalliseen voimaan vaan koko yhteiskuntaan. Kybertoimintaympäristö tarjoaa niin yksilöille kuin valtioille kuin myös yhteisöille ja kansoille väylän toimia pelikentällä ilman yhteisiä sääntöjä. (Hurley & Watkins, 2016)

Teknologian kehityksen myötä yhteiskuntien riippuvuus kybertoimintaympäristöön on korostunut. Samalla myös valtioiden haavoittuvuus on kasvanut, koska riippuvuus tekee yhteiskunnista haavoittuvaisia. Kyberhyökkäysteknologiat kehittyvät nopeammin kuin uhkia vastaan kyetään rakentamaan suojaavia mekanismeja. Uhkiin vastataan yhteistyötä, toimintatapoja ja järjestelmiä kehittämällä. Kansainvälinen yhteistyö ja lainsäädännön kehittäminen tukevat yhteiskunnallisen kyberturvallisuuden kehittämistä. (Lehto & Limnéll, 2017)

Valtion turvallisuuden ja suvereniteetin yksi keskeinen tekijä on uskottavan pelotteen luominen. Pelote tarkoittaa riittävän suuren kynnyksen luomista, jotta voitaisiin estää vastapuoli toimimasta vahingoittavilla tavoilla omaa valtiota vastaan. Kylmän sodan jälkeen pelotevaikutuksen rakentaminen muuttuneessa

turvallisuusympäristössä on vaatinut kybertoimintaympäristön huomioimista. (Klimburg, 2012) Kyberoperaatiot mahdollistavat toiseen valtioon vaikuttamisen poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi. Usea valtio luokittelee kyberoperaatiot pehmeiksi keinoiksi, joten niiden käytön kynnys on alempi kuin perinteisen asevoiman. (Lehto, 2018)

Kylmän sodan jälkeen perinteistä tapaa tarkastella pelotetta on kritisoitu, koska se vastaa parhaiten kahden valtion välisiin suhteisiin ja toimintaan. Terrorismin nousu, epäsymmetrinen sodankäynti ja kyberhyökkäykset eivät täysin sovi perinteiseen peloteteoriaan, koska vastapuoli ei välttämättä ole toinen valtio. Lisäksi motivaatiotekijät vaihtelevat, koska vastustajalla ei välttämättä ole tarvetta suojella omaa infrastruktuuriaan tai kansalaisiaan. Tällöin hyökkääjän hyöty-panossuhde voi olla täysin erilainen kohdevaltioon verrattuna. (Arie, 2016)

Kyberpelotetta voidaan lähestyä edellä kuvatuilla tavoilla joko rankaisu- tai kieltopelotteen näkökulmasta. Ensiksi mainitun keskiössä on perinteisen kineettisen asevoiman käyttö kostotoimenpiteinä. Toiseksi mainittu keskittyy puolustuksellisiin toimenpiteisiin ja resilienssin vahvistamiseen. Koska nämä peloteteoriat pohjautuvat kineettisiin toimiin, eivät ne täysin sovellu kybertoimintaympäristön ainutlaatuisiin piirteisiin. (Chen, 2017a)

Kyberoperaatiot voidaan määritellä eri tavoin, mutta niille yhteistä on jako hyökkäyksellisiin ja puolustuksellisiin operaatioihin. Kybersuorituskykyjen käyttöön liittyy aina myös toimintaympäristön valvonta ja siinä tapahtuma tiedustelu sekä oman kriittisen kyberinfrastruktuurin suojaaminen. Kybersuorituskyvyt ja niiden avulla toteutettavat kyberoperaatiot ovat osa valtion sotilaallista suorituskykyä. (Laari, Flyktman, Härmä, Timonen & Tuovinen, 2019) Kuten konventionaaliset suorituskyvyt, kuten asevoimat ja ydinaseistus, ovat kybersuorituskyvytkin osa pelotteen rakentumista. (Sweijs & Zilincik, 2021)

Tämän tutkimuksen tavoitteena on luoda käsitys kyberpelotteen rakentamiseen ja sen uskottavuuteen vaikuttavista tekijöistä. Pelote ilmiönä on kompleksinen kokonaisuus ja nykyajan monimutkaisessa turvallisuusympäristössä perinteiset käsitykset vaativat uudistusta. Hybridiuhkat, teknologian kiihtyvä kehitys ja yhteiskuntien digitalisoituminen asettavat vaatimuksia kybertoimintaympäristön suojaamiselle ja uskottavan kyberpelotteen luomiselle.

Raja normaali- ja poikkeusolojen välillä on hämärtynyt hybridiuhkien kehittymisen myötä. Kyberoperaatioita voidaan käyttää valtioiden politiikan ja sodankäynnin välineenä jo normaaliaikana. Kyberpelotteen luominen on välttämätöntä, koska sillä tavoin valtio viestii puolustavansa omia rajojaan ja kansalaisiaan myös kybertoimintaympäristössä. Onkin mielenkiintoista tarkastella, mitä keinoja kyberpelotteen luomiseen on ja millä tavalla se yhdistyy konventionaaliseen pelotteeseen.

1.2 Tutkimusmenetelmä

Tutkimus pohjautuu hermeneuttisen tieteenfilosofian periaatteisiin, joissa ”teoreettinen tietämys, oikean tutkimusaineiston löytäminen, tulkinta, tiedon luokittelu ja esittäminen sekä teorian kehittäminen vuorovaikuttavat keskenään tuottaen ymmärrystä ja löytäen uusia piirteitä alkuperäiseen ongelmaan” (Kuusisto, 2008, s.25). Tutkimuksen aikana tutkijan oma ymmärrys ilmiöstä kasvaa ja se tuo esille uusia tietotarpeita ja lähteitä. Näin ollen tutkimus kehittyy hermeneuttisen spiraalin mukaisesti. (Kuusisto, 2008) Tässä tutkimuksessa hermeneuttisen tieteenfilosofian periaatteet ilmenevät aineiston rikastumisena tutkijan ymmärryksen lisääntyessä sekä teemoittelun ja tyypittelyn tarkentumisena tutkimuksen edetessä. Luvussa 3 esitetään aineiston analyysin avulla tuotetut kategoriat etukäteen asetettujen teemojen mukaisesti ja myös sellaiset tutkimustulokset, jotka analyysin edetessä jätetiin pois lopputuotteesta. Lukijan on siis mahdollista seurata tutkimuksen kehittymistä lopulliseen muotoonsa.

Laadullista tutkimusta käsitellään usein sisällönanalyysillä, jossa kerätystä aineistosta muodostetaan tiivistetty kuvaus eritellen sisältöä ja etsien yhtäläisyyksiä ja eroja. Aineistoa analysoidaan myös teemoittelemalla siten, että aineistossa esiintyviä teemoja vertaillaan keskenään. Löydettyjen teemojen perusteella tutkija esittää omia johtopäätöksiään. Teemoittelun perusteella aineistoa voidaan myös tyypitellä. Tyypittelyn tarkoituksena on esittää aineiston yksittäisistä osista suurempia tiivistyksiä ja löytää aineistosta keskeisimmät kokonaisuudet. (Metteri, 2008) Tässä tutkimuksessa kirjallinen aineisto käsitellään asiakokonaisuuksittain sisällönanalyysillä, jonka jälkeen se teemoitellaan ja tyypitellään. Tällainen analyysitapa mahdollistaa systemaattisen tavan muodostaa johtopäätöksiä käsitellystä aineistosta. Nämä johtopäätökset esitetään sekä teksti- että taulukkomuodossa luvussa 3.

Hermeneuttisessa tutkimuksessa ei tehdä selkeitä eroja aineiston luokittelu-, tulkinta- ja analyysivaiheiden välille. On kuitenkin mahdollista etukäteen päättää ne tavat, joilla aineistoa käsitellään. (Puusa & Juuti, 2021) Tässä tutkimuksessa aineistoa käsitellään aineistolähtöisesti, jolloin ei olla etukäteen päätetty mitään tiettyä teoriaa, jota seurataan. Sen sijaan tutkimustulokset nousevat aineistosta itsestään tutkijan tulkitsemana.

Aineistolähtöisessä tutkimuksessa aineistoon tutustutaan usealla lukukerralla ja sen aikana tutkija muodostaa käsityksiä aineistosta, esimerkiksi tarkastelemalla esitettyjä tulkintoja aiheesta ja etsimällä eroavaisuuksia ja yhteneväisyyksiä. Kun aineistosta on muodostettu kokonaiskuva, pilkotaan se osiin ja teemoittelemalla etsitään yhteneväisyyksiä. Asetettu tutkimusongelma ohjaa tätä työvaihetta ja auttaa rajaamaan hankittua aineistoa. (Puusa & Juuti, 2021)

Teemoittelu voidaan tehdä aineiston keruuvaiheessa laadittujen teemojen mukaisesti tai niitä voidaan myös täydentää teemoittelun edetessä. Samankaltaiset teemat yhdistetään yhteen kategoriaan. Samankaltaisia alakategorioita yhdistetään yläkategorioiden alle, joka nimetään kuvaavasti. Tällaista menettelyä kutsutaan tyypittelyksi. Teemoittelun ja tyypittelyn jälkeen kutakin tyyppiä tulee

tarkastella osana kokonaisuutta ja sen suhteita muihin tyyppeihin. (Puusa & Juuti, 2021)

Tässä tutkimuksessa oli päätetty tutkijan aiempaan tietämykseen pohjautuen käytettäviksi teemoiksi pelote, kyberpelote ja kyberoperaatiot. Näiden teemojen mukaan kerättiin aineisto sekä teemoiteltiin ja tyypiteltiin se tutkimuskysymyksiä tukeviin kokonaisuuksiin. Luvussa 3 esitetään tarkemmin aineiston teemoittelu ja tyypittely sekä sen perusteella muodostetut johtopäätökset.

1.3 Tutkimuskysymykset, viitekehys ja aiheen rajaus

Tutkimuksen tavoitteena on määritellä kyberpelote, löytää sen yhteys valtion pelotteeseen ja määritellä keinoja kyberoperaatioiden käytöstä pelotevaikutusten luomiseen. Tutkimuksen tarkoituksena on luoda teoreettinen tietopohja aiheesta mahdolliselle jatkotutkimukselle tutkijan jatko-opintoja varten.

Päätutkimuskysymys: Miten kyberoperaatioita voidaan käyttää pelotevaikutusten luomiseen?

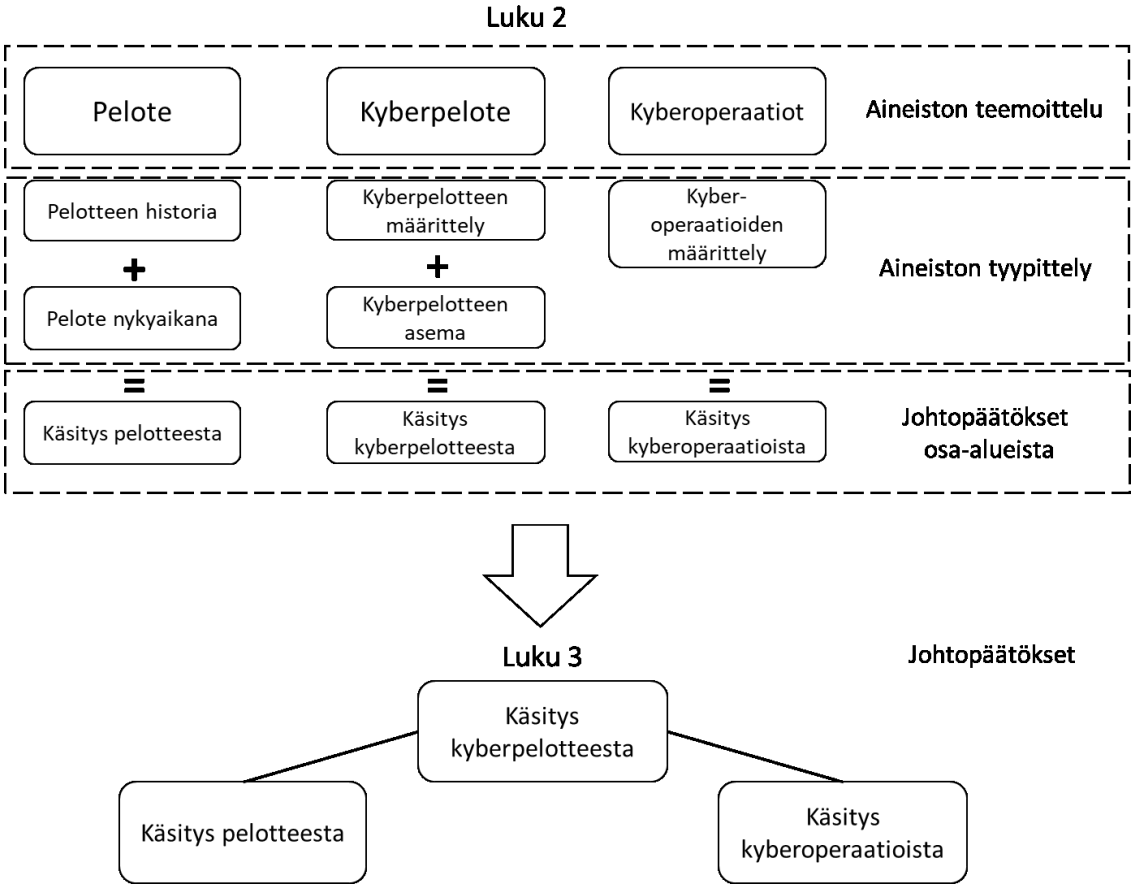
1. alatutkimuskysymys: Miten valtion pelote rakentuu?
2. alatutkimuskysymys: Miten muodostetaan kyberpelote?
3. alatutkimuskysymys: Millaisia vaikutuksia kyberoperaatioilla saadaan aikaan?

Ensimmäisen alatutkimuskysymyksen avulla tarkastellaan klassista peloteteoriaa ja suorituskykyjä, joita konventionaalisessa sodankäynnissä käytetään. Kun teoriapohja on ensin näin luotu, siirrytään tarkastelemaan nykyajan turvallisuusympäristön vaatimuksia pelotevaikutuksen luomiselle toisen valtion taholta syntyvää uhkaa vastaan. Alatutkimuskysymykseen vastaamalla saadaan tietoa siitä, miten klassista peloteteoriaa voidaan nykyaikana soveltaa ja mitä vaihtoehtoisia teorioita voidaan käyttää. Alatutkimuskysymykseen vastataan luvussa 2.1.

Toisen alatutkimuskysymyksen avulla määritellään kyberpelote käsitteenä ja selvitetään mahdollisuuksia kyberpelotteen muodostamiselle. Alatutkimuskysymykseen vastaamalla muodostetaan myös käsitys niistä kybersuorituskyvyistä, joita pelotteen luomiseen tarvitaan. Alatutkimuskysymykseen vastataan luvussa 2.2.

Kolmannen alatutkimuskysymyksen avulla määritellään kyberoperaatiot sekä tutkitaan niiden toimintoja ja vaikutuksia. Alatutkimuskysymykseen vastaamalla muodostetaan käsitys kyberoperaatioiden tyypeistä ja käyttötavoista. Alatutkimuskysymykseen vastataan luvussa 2.3.

Alatutkimuskysymyksien tuottaman tiedon perusteella muodostetaan synteesi päätutkimuskysymykseen vastaamiseksi luvussa 3. Kuviossa 1 esitetään tutkimuksen tutkimusasetelma.



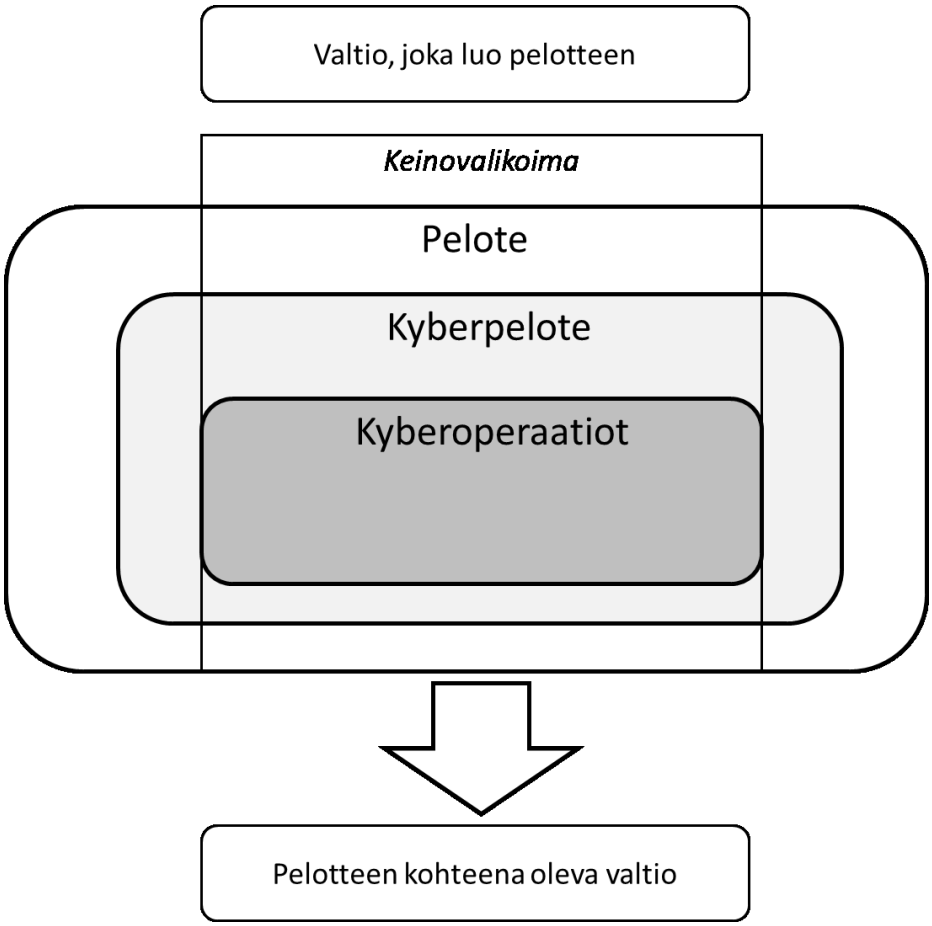
KUVIO 1 Tutkimusasetelma

Tutkimuksen näkökulmana on pelotteen teoreettinen tarkastelu. Tutkimuksessa ei oteta kantaa teknologian käyttöön pelotteen rakentamisessa, koska tutkimuksessa ollaan kiinnostuneita strategisen tason toiminnasta, jolloin tekninen näkökulma muodostuu liian pienipiirteiseksi tutkimuskysymyksiin vastaamisen näkökulmasta. Tutkimuksessa ei myöskään tarkastella toteutuneita kyberhyökkäyksiä, koska on vaikeaa todistaa jonkin hyökkäyksen liittyneen pelotteen luomiseen tai sen epäonnistumiseen.

Tutkimuksessa tarkastellaan länsimaista tulkintaa pelotteesta ja kyberoperaatioista. Tutkimuksen painopisteenä on pelotevaikutuksen luominen toiseen valtioon nähden ja näin ollen tutkimus rajaa pois esimerkiksi pelotteen luomisen terrorismia tai rikollisuutta vastaan.

Tutkimus tuottaa teoreettisen pohjan tutkittavasta ilmiöstä ja vetää yhteen 2000-luvulla esiintyvät käsitykset kyberpelotteesta. Tutkimus toimii pohjana mahdolliselle jatkotutkimukselle, jonka aiheena on Suomen kyberpuolustuksen kehittäminen. Tutkimuksen perusteella voidaan esimerkiksi jatkotutkia pienen valtion, kuten Suomen, kyberpelotteen luomiseen liittyviä seikkoja. Tutkimus antaa myös tiivistelmän aihealueen käsityksistä länsimaisessa tiedeyhteisössä ja kyberpelotteen luomiseen liittyvistä haasteista.

Tutkimuksen viitekehyksen keskiössä on valtion luoma pelote toista valtiota kohtaan. Tutkimuksen hypoteesina on, että kyberpelote sisältyy pelotteen teoreettiseen kokonaisuuteen ja sitä ei ole tarkoituksenmukaista käsitellä tästä kokonaisuudesta erillisenä ilmiönä. Näin ollen kyberpelotteen keinovalikoima, eli kyberoperaatiot, ovat osa pelotteen käytännön toteutusta. Kyberoperaatiot ovat yksi tapa kyberpelotteen rakentamiseen ja tämän tutkimuksen mielenkiinnon kohde. Kuviossa 2 esitetään tutkimuksen teoreettinen viitekehys.



KUVIO 2 Tutkimuksen viitekehys

1.4 Lähdeaineisto ja aikaisempi tutkimus

Strategiseen pelotteeseen liittyvää tutkimusta ja muuta kirjallista lähdeaineistoa löytyy runsaasti. Suurin osa kirjallisuudesta koskee ydinasepelotetta etenkin Yhdysvaltojen ja Venäjän näkökulmista. Näiden tutkimusten perusteella muodostetaan käsitys pelotteesta ilmiönä ja muodostetaan teoriapohja, jota vasten kyberpelotetta tarkastellaan.

Kyberoperaatioiden määrittelyyn käytetään länsimaalaisia julkaisuja, joista suurin osa koostuu viranomaisten doktriineista ja ohjesäännöistä. Suomenkieliset julkaisut ovat pääsääntöisesti tietoturvaluokiteltuja, joten lähdeaineisto muodostuu pääsääntöisesti Yhdysvaltojen, Naton ja Iso-Britannian internetistä löytyvistä viranomaisjulkaisuista.

Lähdeaineisto painottuu tieteellisiin artikkeleihin, tutkimustöihin ja konferenssijulkaisuihin, joista suurin osa on englanninkielisiä julkaisuja. Suomalaista tutkimusta löytyy niukasti ja se keskittyy pääsääntöisesti ydinasepelotteeseen. Lähdeaineistoa täydennetään muulla kirjallisella materiaalilla, kuten esimerkiksi suomeksi ja englanniksi löytyvillä viranomaisasiakirjoilla.

Aineiston keruun aikana havaittiin, että kyberpelotetta on tutkittu eri näkökulmista. Tutkimuksista on erotettavissa tiettyjä teemakokonaisuuksia, tämä luokittelu on tutkijan tekemä. Yksi kokonaisuus on kyberpelotteen tutkiminen ilmiönä. Nämä tutkimukset ovat luonteeltaan yleisluonteisia ja niissä keskitytään aiheen filosofiseen tarkasteluun. Toinen kokonaisuus sisältää perinteisen peloteteorian soveltamista kybertoimintaympäristöön. Näissä tutkimuksissa etsitään mahdollisuuksia ennaltaehkäistä vastustajan toimia kybertoimintaympäristössä sekä keinoja vastatoimien tekemiseen. Kolmannessa tutkimuskokonaisuudessa keskitytään kyberpelotteen rakentamisen problematiikkaan, joka voi johtua esimerkiksi attribuutio-ongelmasta, teknologisista haasteita ja lain asettamista rajoituksista. Neljäs kokonaisuus käsittelee uusien teknologisten ratkaisujen, kuten tekoälyn, käyttöä kyberpelotteen luomiseen. Tässä tutkimuksessa kiinnostavimmat aihekokonaisuudet ovat kolme ensimmäistä, koska tutkimus keskittyy asian määrittelyyn ja rajaa pois tekniset ratkaisut.

Kyberpelotetutkimuksen fokus on monessa tutkimuksessa siinä, millä keinoin voidaan ennaltaehkäistä ja reagoida kybertoimintaympäristössä tapahtuviin hyökkäyksiä. Moni tutkimus keskittyy tarkastelemaan joko kyberpelotteen toteuttamismahdollisuuksia ylipäätään tai kyberpelotetta osana muuta pelotetta. Vähemmistö akateemisesta keskustelusta painottuu kyberoperaatioiden tarkasteluun pelotteen mahdollistajana ja niiden roolista pelotevaikutusten rakentamisessa. Kyberoperaatioita käsitellään eri näkökulmista muun muassa kyberaseiden ja varsinaisten operaatioiden muodossa sekä kyberkampanjoiden osana. Yhteistä näille näkökulmille on kybersuorituskykyjen käyttö jonkin teknisen, taktisen, operatiivisen tai strategisen tavoitteen saavuttamiseen. Seuraavissa kappaleissa on tarkasteltu viime vuosien uusimpia tutkimuksia nimenomaan kyberoperaatioiden näkökulmasta.

Sven Herpig (2015) käsittelee kyberoperaatioiden käyttöä osana kyberstrategioita ja niiden käytännön variaatioita. Herpigin mukaan kyberstrategiaan voidaan sisällyttää laaja variaatio erilaisia kyberoperaatioita, joilla pyritään saavuttamaan strateginen tai poliittinen päämäärä. Herpig nimeää viisi strategiaa: eristäytyminen (Going Dark), pelote (Deterrence), salassa toimiminen (Sub Rosa), peitelty vaikuttaminen (Shashou Jian) ja kybersodankäynti (Cyber War). Eristäytyminen tarkoittaa, että valtion kriittinen infrastruktuuri pidetään erillään Internetistä tai muista laajoista verkoista. Tällöin uhkatoimijalta evätään pääsy niihin verkkoihin, jotka sisältävät arvokasta tietoa tai joiden toimintahäiriöt voivat

johtaa huomattaviin vahinkoihin. Verkkojen eristäminen voidaan tehdä vain esimerkiksi korkeasti turvaluokitelluille tietojärjestelmille. Kyberpelotteeseen sisältyy sekä puolustuksellisia että hyökkäyksellisiä kyberoperaatioita, toteutettuna usein samanaikaisesti ja kustomoiden kuhunkin kohteeseen sopivaksi. Näiden mahdollistamiseksi tarvitaan myös kybertiedusteluoperaatioita. Salassa toiminen on yhdistelmä tiedustelu, informaatio- ja kyberoperaatiota. Tällaisen strategian päämääränä on ensisijaisesti tiedonhankinta. Peitelty vaikuttaminen on strategia, jossa vastustajaan pyritään iskemään salassa ja peitellysti. Tätä strategiaa voidaan toteuttaa kyberoperaatioin tai osana tiedusteluoperaatiota. Kybersodankäynti on aina osa varsinaista sotaa ja kyberoperaatioita käytetään ilman rajoituksia ja avoimesti. (Herpig, 2015)

Richard Harknett ja Max Smeets (2020) tarkastelevat kyberkampanjoilla saavutettavia strategisia vaikutuksia. Harknett ja Smeets määrittelevät kyberkampanjan sarjaksi koordinoituja kyberoperaatioita, jotka ajan kanssa tekevät kumuloituvia vaikutuksia kohteessa ja saavuttavat strategista etua. Kyberoperaatio puolestaan koostuu koordinoiduista toiminnoista, jotka kohdistuvat johonkin tiettyyn verkkoon tai laitteistoon. Kybertoimintaympäristössä toteutettavat kyberkampanjat tarjoavat valtioille keinoja vaikuttaa sodankäynnin kynnyksen alapuolella ja näin mahdollisuuksia suojata omia kriittisiä resurssejaan. Kyberkampanjoilla voidaan kääntää symmetrinen suhde epäsymmetriseksi, tai päinvastoin. (Harknett & Smeets, 2020)

Michael Fischerkeller (2017) tarkastelee hyökkäyksellisten kyberoperaatioiden (engl. Offencive Cyber Operations) roolia pelotteen ja pakottamisen näkökulmista. Hyökkäyskykyä ei voida täysin demonstroida, koska se paljastaisi vastustajalle liikaa omita kybersuorituskyvyistä. Edullisin asetelma luodaan, kun potentiaaliset kohteet kyetään luokittelemaan ja priorisoimaan etukäteen sekä omat operaatiot mitoittamaan ja kohdistamaan uhkan mukaan. Pelotevaikutuksen luomisessa hyökkäyksellisten kyberoperaatioiden yhdistäminen muihin pelotekeinoihin voi luoda vahvemman vaikutuksen kuin kyberoperaatiot yksinään. Hyökkäyksellisten kybersuorituskykyjen kehittäminen voi luoda uusia mahdollisuuksia ennen kriisiä ja myös konfliktin aikana vaikuttaa vastustajan päätöksentekoon. Koska hyökkäyksellisiä kyberoperaatioita ei lueta kuuluvaksi samaan kategoriaan kuin aseellisia hyökkäyksiä ja niiden vaikutukset ovat säädeltävissä, sopivat ne hyvin pelote- tai pakotepolitiikkaan yhdessä muiden sotilaallisten suorituskykyjen kanssa. (Fischerkeller, 2017)

Martin Libickin (2009) teosta *Cyberdeterrence and Cyberwar* voidaan pitää yhtenä kyberpelotetutkimuksen perusteoksista, johon monet myöhemmät tutkijat viittaavat. Libicki käsittelee kybertoimintaympäristössä ilmeneviä mekanismeja muun muassa pelotteen ja sodankäynnin näkökulmista, keskittyen hyökkäyksellisiin kyberoperaatioihin. Libicki nostaa esille kyberpelotteen erilaiset lainalaisuudet verraten konventionaaliseen ja ydinasepelotteeseen. Paras puolustus kybertoimintaympäristössä on hyvä puolustus. Hyökkäyksellisen kyberoperaation sijaan kannattaa pelotteessa ensin kokeilla diplomatian, taloudellisten pakotteiden ja lain suomia keinoja. Hyökkäyksellisten kybersuorituskykyjen kehittäminen on kuitenkin kannattavaa niiden tarjoaman hyötypanossuhteen takia.

Hyökkäyksellisellä kyberoperaatiolla voidaan saavuttaa etua vastustajaan nähden, mutta sen ei tulisi olla ainut keino vastata uhkiin. (Libicki, 2009)

Aaron Brantly (2018) kyseenalaistaa pelotteen roolin nykypäivän informaatioympäristössä, jossa yksittäinen taitava hakkeri voi uhata kokonaista valtiota koodinpätkän avulla. Brantly tarkastelee sekä rationaalista että kognitiivista teoriaa pelotteen viitekehyksessä. Brantlyn mukaan klassisen peloteteorian mukainen kielto- ja rangaistusvaikutus on haastavaa saavuttaa kybertoimintaympäristössä. Kyberpelotetta ei tulisi tarkastella vain kybertoimintaympäristössä tapahtuvina tekoina, vaan kokoelmana valtion strategisia keinoja, joilla vähennetään kyberhyökkäämisen kannustimia, anonymiteettiä ja toteuttamismahdollisuuksia. Peloteteorioita ei kuitenkaan tule kokonaan hylätä, vaan löytää niistä toteuttamiskelpoiset ratkaisut sekä myös ne asiat, jotka eivät enää nykyaikana toimi. (Brantly, 2018)

Christian Leuprecht, Joseph Szeman ja David Skillicorn (2019) kirjoittavat hyökkäyksellisten kyberoperaatioiden mahdollisuuksista ja rajoitteista muun muassa diplomatian ja pelotteen välineenä. Hyötynäkökulmia on useita. Kyberoperaatioita voidaan suorittaa avoimesti ja peitellysti. Attribuutioon liittyvät haasteet mahdollistavat valtiolle toiminnan kiistämisen. Koska kyberhyökkäys ei yleensä ylitä aseellisen konfliktin kynnystä, hämärtää niiden käyttö sodan ja rauhan rajaa. Kyberhyökkäyksen vaikutuksia voidaan säädellä ja mahdollistaa myös niistä palautuminen, joten kyberoperaatiot suovat etuja konflikteihin vastaamiseen sopivalla voimakkuudella. Toisaalta yhteisten sopimusten puute ei estä vastaamasta kyberhyökkäykseen konventionaalisin asein. Muita riskejä ovat kyberhyökkäyksen vaikutuksen leviäminen hallitsemattomasti, epävarmuus kohteen reaktioista ja kyberaseen tehokkuudesta sekä kansainvälisen yhteisön reaktioista. (Leuprecht, Szeman & Skillicorn, 2019)

1.5 Käsitteet ja määritelmät

Pääosa tutkimuksen lähdeaineistosta on kirjoitettu englanniksi. Aineisto sisältää sellaisia termejä, joita ei olla vielä suomennettu tai niistä on olemassa erilaisia tulkintoja. Sanastokeskus julkaisi vuonna 2018 kansallisen kyberturvallisuuden sanaston, joka ei kuitenkaan täysin kata tutkimuksen käännöstarpeita termien osalta. Seuraavaksi esitellään tämän tutkimuksen keskeisimmät käsitteet ja tutkimusraportissa käytettävät suomenkieliset vastineet. Kyber- ja pelotekäsitteistön vakiintumattomuuden vuoksi tutkimuksessa esitetään myös englanninkieliset vastineet termin esiintyessä ensimmäisen kerran.

Pelotetta on haastavaa yksiselitteisesti määritellä, koska pelote on määritelty eri aikoina eri tavoin. Eri aikakausien peloteteorioita käsitellään tarkemmin luvussa 2.1. Voidaan kuitenkin todeta, että pelotteen ydinidea on valtion pyrkimys vakuuttaa toinen valtio siitä, että aggressio ei ole kannattavaa ja että kumpikin osapuoli savuttaa tavoitteensa paremmin ilman toisen valtion provosoimista konfliktiin (Mazarr & Goodby, 2011). Tämä määritelmä rinnastetaan tässä

tutkimuksessa myös kyberpelotteeseen, eli valtio pyrkii vakuuttamaan toisen valtion kyberhyökkäyksen kannattamattomuudesta.

Suomen kielessä sana ”pelote” rinnastetaan usein rankaisupelotteeseen ja ”pidäke” kieltopelotteeseen (Hanska, 2019). Tässä tutkimuksessa vastaavaa jakoa ei tehdä, koska termi ”pidäke” on tarpeeton ja se voidaan korvata termillä ”pelote”, kun etuliitteenä käytetään kutakin pelotestrategiaa vastaavaa tarkennetta.

Kybertoimintaympäristö on ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö. Kybertoimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet” (Sanastokeskus, 2018, s. 21). Tässä tutkimuksessa erotetaan kybertoimintaympäristö (engl. Cyberspace) sotilaallisista ulottuvuuksista (engl. Domain), joita ovat maa-, meri-, ilma-, avaruus-, informaatio- ja kyberulottuvuus.

Kybertoimintaympäristö koostuu kolmesta kerroksesta: fyysinen, looginen ja käyttäjäkerros. Loogiseen kerrokseen kuuluvat sähköiset tiedonsiirtoon tarkoitetut toiminnot ja ohjelmistot. Fyysinen kerros koostuu fyysisistä laitteista, kuten palvelimet ja päätelaitteet. Käyttäjäkerros käsittää ihmiset ja ihmisten sähköiset identiteetit, kuten käyttäjätunnukset ja sähköiset tilit. (Laari ym., 2019)

Sanastokeskuksen (2018) määritelmän mukaan ”Kyberoperaatio on suunnitelmallinen ja johdettu sarja pääosin kybertoimintaympäristössä tapahtuvia toimintoja, joilla pyritään hankkimaan tietoa kohteesta tai vaikuttamaan sen toimintaan. Kyberoperaatio voi olla joko puolustuksellinen tai hyökkäyksellinen. Sen tekijänä voi olla valtio, ryhmä tai yksittäinen henkilö. Kyberoperaation tueksi vaaditaan usein tiedustelu- ja muita tukitoimia, jotka eivät välttämättä tapahdu kybertoimintaympäristössä (Sanastokeskus, 2018, s. 27)”.

Tietoverkkohyökkäyksellä tai verkkohyökkäyksellä tarkoitetaan sellaista toimintaa, jolla pyritään ”tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön (Sanastokeskus, 2018, s. 30)”. Esimerkiksi palvelunestohyökkäys ja haittaohjelmien käyttö ovat tietoverkkohyökkäyksiä, jotka kohdistuvat kybertoimintaympäristön loogiseen kerrokseen. Kyberhyökkäys on puolestaan laajempi termi, koska kyberhyökkäys on mahdollista toteuttaa myös muilla keinoin kuin tietoverkon kautta. (Sanastokeskus, 2018)

Lähdeaineistossa kyberhyökkäyksen toteuttajaa kutsutaan kontekstista riippuen joko uhkatoimijaksi (engl. Threat Actor tai Aggressor), vastustajaksi (engl. Opponent) tai hyökkääjäksi (engl. Attacker). Tässä tutkimuksessa englanninkieliset termit ovat suomennettu lähdeaineiston termin mukaan ja ne voivat viitata joko yksilöön tai valtioon, riippuen lähteen näkökulmasta. Luvussa 3 ja 4 vihamieliseen valtioon viitataan uhkatoimijana.

2 AIHEEN TEOREETTINEN TARKASTELU

Tässä luvussa tarkastellaan pelotteen, kyberpelotteen ja kyberoperaatioiden määritelmiä ja vastataan tutkimuksen alatutkimuskysymyksiin. Luvun tarkoituksena on muodostaa käsitys näistä kolmesta etukäteen määritellystä teemasta ja näin luoda edellytys kolmannen luvun analyysiosuudelle.

2.1 Peloteteoriat

2.1.1 Klassinen määritelmä

Pelotteen juuria voidaan jäljittää ihmiskunnan historiassa niin kauas kuin on ollut sotia. Esimerkkejä pelotteesta konventionaalisessa sodankäynnissä voidaan etsiä esimerkiksi Ensimmäisen maailmansodan ajalta, jolloin ilmapommituskyvyn ajateltiin olevan kehittyvä laajan tuhovaikutuksen ase. Merkkejä pelotevaikutuksesta voidaan nähdä Ensimmäisessä ja Toisessa maailmansodassa sellaisissa tilanteissa, joissa osapuolet pidättäytyivät pommittamasta siviilikohteita samanlaisten vastatoimien pelossa. Vastaavanlaista keskustelua käytiin myös merivoimien käytöstä liittyen kaupallisten merikuljetusten koskemattomuuteen. (Morgan, 2003)

Klassisen peloteteorian voidaan katsoa syntyneen Toisen maailmansodan päätteeksi vuonna 1945, jolloin Yhdysvallat demonstroi ydinaseiden tuhovaikutusta Japanissa ja Neuvostoliiton demonstroidessa omia ydinasesuorituskykyjään vuonna 1949. Suurvaltojen pelote muokkautui vahvasti Kylmän sodan johdosta. Pelote oli kaiken kattava ja johti ennennäkemätöntä asevarustelua ja asevoimien suorituskykyjen kehittämistä. Ydinase oli yksi merkittävä tekijä peloteteorian muovautumisen taustalla. Pelotteen tavoitteena oli estää seuraava suursota ja turvata oma ja alueellinen turvallisuus käyttämällä mielikuvaa niin suuren tuhovoiman vastatoimista, ettei hyökkäys kannattaisi. (Morgan, 2003)

1950 – 1960 -luvuilla kehitettiin peloteteorioiden perusta, jota muokkasi vahvasti ydinaseiden kehitys ja suurvaltojen välinen kilpavarustelu. Yleisenä

ajatuksena oli, että mahdollisen ydinaseiskun jälkeen puolustavalla valtiolla tuli olla kyky vastaiskuun. Totaalisen tuhon pelossa ydinasevallat pidättäytyivät ydinaseiden käytöstä. Eskalaation käsite syntyi ajatuksesta, että pienemmän mittakaavan konfliktit olivat edelleen mahdollisia ja voivat johtaa ydinasevaltojen väliseen sotaan. Tämän kaltaista kehitystä vastaan valtion oli mahdollista yrittää vakuuttaa vastapuoli siitä, että voiman käytön kasvattaminen ei ole kannattava vaihtoehto. Näin syntyi vilkasta keskustelua pelotteen rakentumisesta ja keskenään erilaisia näkemyksiä, jotka vaikuttavat nykypäivän pelotekeskusteluun. (Freedman, 2021)

Kylmän sodan aikana ydinasepelotteen rinnalle muodostui ajatus konventionaalisen asevoiman käyttämisestä pelotevaikutuksen luomiseen. Kehitykseen vaikutti muun muassa asekehitys, joka toi entistä pidemmälle ja tarkemmin vaikuttavia asejärjestelmiä markkinoille. Ydinaseiden merkitys kuitenkin säilyi rinnalla, joten mahdollisuus pienimuotoisen konfliktin ja konventionaalisen asevoiman käytön eskaloitumisesta ydinasesodaksi oli edelleen varteenotettava vaihtoehto. (Freedman, 2021)

Kylmän sodan päätyttyä jyrkkä vastakkainasettelu lännen ja idän välillä poistui. Pelotteen rakentamisessa ei enää ollut kyse kahden ydinasesuurvallan välisistä suhteista. Totuttu tapa jäsentää pelote ei enää toiminut, koska turvallisuuspoliittinen ympäristö muuttui monimuotoisemmaksi muun muassa terrorismin uhkan kasvamisen myötä. Tämän vuoksi peloteteorioiden ympärillä alkoi kansainvälistä järjestelmää peilaava keskustelu, josta puuttui yhteinen teoreettinen näkemys. (Freedman, 2021)

2000-luvulla kansainvälinen tasapaino muuttui jälleen Venäjän ajaessa etujaan muun muassa Ukrainassa ja Syyriassa sekä Kiinan vahvistuessa Aasiassa. Pelotekeskustelussa palattiin vanhoihin klassikoihin ja ydinaseen merkitys nousi jälleen esille. Toisaalta teknologian kiivas kehitys on johtanut siihen, että yhteiskunnissa on uudenlaisia haavoittuvuuksia esimerkiksi informaation hallinnan ja informaatioteknologian turvallisuuden osalta. Sodan ja rauhan välinen raja on hämärtynyt informaatiosodankäynnin ja kyberoperaatioiden myötä. Teknologian kehitys on nostanut esille myös attribuutio-ongelman, koska edellä mainittuja operaatioita voidaan toteuttaa matalalla profiililla ja syyllistä ei välttämättä koskaan voida aukottomasti osoittaa. (Freedman, 2021)

Pelotteen ydinajatus voidaan kiteyttää pyrkimykseksi vakuuttaa vastapuoli siitä, että vihamielisen toiminnan hyöty-panossuhde ei ole kannattava. Lähtökohtaoletuksena on, että pelotteen toimeenpanossa on aina kaksi osapuolta, jotka kommunikoivat toisilleen. Pelotteen toimiessa molempien osapuolten on uskottava kykenevänsä saavuttamaan tavoitteensa ilman vastapuolen provosointia konfliktiin. Pelote on luonteeltaan ennaltaehkäisevää ja eroaa tällä tavoin pakotteesta, joka tähtää jo alkaneisiin tai juuri alkavien toimien pysäyttämiseen. (Mazarr & Goodby, 2011)

Klassisen peloteteorian mukaan pelote koostuu kolmesta tekijästä. Ensiksi toimivan pelotteen taustalla on oltava riittävä suorituskyky. Toiseksi pelotteen aiheuttaman potentiaalisen uhkan on oltava uskottava ja kolmanneksi se on kyettävä viestimään muille toimijoille. Näiden kolmen elementin tulee esiintyä

uskottavan pelotteen yhteydessä. Pelote on onnistunut, kun potentiaalinen vastustaja pidättäytyy toiminnasta. (Paul, 2009)

Pelotteen voidaan katsoa perustuvan tiettyihin elementteihin, jotka esiintyvät valtion tai sen vastustajan toiminnassa. Klassisen peloteteorian taustaoletuksena on uhka, joka voi johtaa vakavaan konfliktiin ja josta aiheutuu mittavia vahinkoja. Tähän uhkaan voidaan varautua laaja-alaisesti ylläpitämällä mittavia sotilaallisia suorituskykyjä tai vaihtoehtoisesti varautua välittömään reagointiin valituilla aseilla, mikäli vastapuoli hyökkää. Nämä näkökulmat eroavat intensiteetissä: laaja-alainen lähestymistapa sopii tilanteeseen, missä vaaraa välittömästä hyökkäyksestä ei ole. Sen sijaan jälkimmäisessä näkökulmassa on oletus olemassa olevasta kriisistä, joka voi hetkellä millä hyvänsä eskaloitua aseelliseksi konfliktiksi. Kylmän sodan aikana oltiin ajoittain lähellä jälkimmäistä tilannetta ja suurvallat olivat jatkuvasti valmiudessa reagoida vastapuolen toimintaan. (Morgan, 2003)

Toinen klassisen peloteteorian taustaoletus on, että valtiot toimivat rationaalisesti. Rationaalisuus tarkoittaa, että kumpikin osapuoli kerää kaiken saatavilla olevan tiedon ja arvioi toiminnan hyöty-panossuhteen. Valtion on siis ilmaistava suorituskykynsä ja valmiutensa vastatoimiin, jotta vastapuoli omien laskelmiensa mukaan päätyy johtopäätökseen, ettei hyökkäys ole kannattavaa siitä saatavan liian pienen hyödyn ja omien tappioiden vuoksi. (Morgan, 2003)

Klassiseen peloteteoriaan kuuluu ajatus kostoiskusta, joka on niin mittava, että sen pelkkä mahdollisuus laskee oleellisesti vastapuolen halua vihamieliseen toimintaan. Ajatus perustuu ydinaseiden käyttöön niin laajassa mittakaavassa, että vastaisku pahimmillaan romahduttaa kohdevaltion yhteiskunnan. Haasteena tässä on ilmaista vastapuolelle sekä oma kyky että valmius aseen käyttämiseen. Keskiössä ei ole omat todelliset aikomukset tai kyvyt vaan se, mitä vastapuoli uskoo. (Morgan, 2003)

Perinteinen tapa jäsentää pelote on jakaa se kahteen erityyppiseen malliin. Rankaisupelote (engl. Deterrence by Punishment) nojaa käsitykseen, jonka mukaan vastapuoli pidättäytyy toimistaan vastareaktion ollessa liian suuri, jotta hyökkäys kannattaisi toteuttaa. Kieltopelotteessa (engl. Deterrence by Denial) luodaan vastustajalle mielikuva, että hyökkäys on kannattamaton, koska sillä ei saavuteta haluttuja vaikutuksia. (Raitasalo & Sipilä, 2008)

Pelotteeseen kuuluu oleellisesti valtion kyky viestiä ne asiat, joiden ajatellaan vaikuttavan vastapuolen harkintaan. Esimerkiksi omaa sotilaallista voimaa on kyettävä näyttämään uskottavasti, jotta vastapuolelle kommunikoidaan oma suorituskyky ja myös valmius käyttää sitä. Omia suorituskykyjä ei kuitenkaan voida paljastaa yksityiskohtaisesti, jotta vastapuoli ei voisi mitoittaa omia toimiaan niitä vastaan tai ei paljastettaisi omia haavoittuvuuksia. Pelotteeseen liittyvä viestintä onkin tasapainoilua riittävän ja liiallisen kommunikoinnin välillä. (Raitasalo & Sipilä, 2008)

Pelotteesta viestimiseen liittyy haasteita, koska viestintä on alun alkaenkin epätäydellistä edellä mainitun tasapainoilun takia. Valtio ei voi olla koskaan täysin varma siitä, onko viesti ymmärretty oikein tai edes huomattu. Toinen pelotteen haaste liittyy vastapuolen rationaaliseen päätöksentekoon. Peloteteoriat

nojaavat käsitykseen, että vastapuoli punnitsee hyökkäyksen hyötyjä ja haittoja rationaalisesti ja toimii hyöty-panossuhteen mukaan. (Raitasalo & Sipilä, 2008)

Michael Mazarr (2018) on koonnut peloteteorioiden jaottelua ja tyyppejä vuosikymmenten ajan käydystä akateemisesta keskustelusta sekä peloteteorioiden klassikoista. Jako kielto- ja rankaisupelotteeseen on perustavanlaatuinen. Mazarr huomauttaa, että kieltopelote ei saisi nojata vain sotilaalliseen voimaan, vaan huomioida myös muita keinoja vakuuttaa vastapuoli hyökkäyksen kannattamattomuudesta. Samoin rankaisupelotteessa keinovalikoiman ja rankaisun tulee olla laajempi kuin pelkästään uhkaan vastaaminen. Kieltopelote saattaa olla vakuuttavampi kuin rankaisupelote, koska vastapuoli voi epäillä valtion tahtoa rankaisutoimien toteuttamiseen. (Mazarr, 2018)

Toinen Mazarrin käyttämä jako on suora pelote (engl. Direct Deterrence) ja laajennettu pelote (engl. Extended Deterrence). Suora pelote tarkoittaa valtion pyrkimyksiä torjua hyökkäys omalla alueellaan. Laajennetussa pelotteessa valtio viestii, että hyökkäys liittolaisia tai kumppaneita vastaan aiheuttaa myös vastatoimia. Suora pelote on uskottavampi, koska suuremmalla todennäköisyydellä valtio puolustaa omaa suvereniteettiaan, mutta ei välttämättä riennä liittolaisten tai kumppanien avuksi. Yksi keino viestiä laajennettua pelotetta on sijoittaa sotilaallisia joukkoja liittolaisen tai kumppanin alueille. (Mazarr, 2018)

Kolmas tapa jakaa pelotteen käsitteitä on ajallinen tarkastelu. Yleinen pelote (engl. General Deterrence) tähtää jatkuviin ja systemaattisiin toimiin jo normaalioloissa. Välitön pelote (engl. Immediate Deterrence) vastaa tyypillisesti kriisiajan uhkaan ja sisältää, jotain tiettyä uhkaa kohtaan suunniteltuja välittömiä toimia. Pelotekirjallisuudessa on todettu yleisen pelotteen olevan helpompi toteuttaa, koska kriisin jo puhjettua voi olla vaikeaa muuttaa uhkatoimijan motivaatiota hyökkäykseen. Tämän vuoksi yleisen pelotteen yksi tavoitteista onkin vähentää todennäköisyyttä kriisin puhkeamiseen, jotta välitöntä pelotetta ei tarvittaisi. Tällöin vastustaja tulee vakuuttaa siitä, että kriisitilanteeseen ei kannata ajautua. (Mazarr, 2018)

Neljäs tapa jakaa pelote on kapea (engl. Narrow Deterrence) ja laaja pelote (engl. Broad Deterrence). Kapea pelote nojaa puhtaasti sotilaalliseen voimaan. Tätä laajemman pelotteen keinovalikoimaan voi kuulua poliittiset ja taloudelliset keinot tai informaatiovaikuttaminen. Nämä kaksi käsitystä nojaavat ajatukseen, että vastustaja suostutellaan pidättäytymään hyökkäyksestä uhkaan perustuvalla viestinnällä. Tämä voi tarkoittaa sekä kielto- että rankaisupelotteen mukaista viestintää omasta voimasta ja tahdosta käyttää sitä, tavoitteenaan vaikuttaa vastustajan arviointiin riskistä ja hyökkäyksestä saavutettavasta hyödystä. Näiden ajattelutapojen lisäksi on mahdollista jäsentää pelote vieläkin laajemmaksi kokonaisuudeksi, jossa päämääränä on suostutella vastustaja pidättäytymään voimakeinoista sekä peloteviestinnän keinoin että tarjoamalla vakuuksia ja etuja. Tässä lähestymistavassa yritetään vakuuttaa vastustaja siitä, että aggressio on tarpeeton ja yhteistyöstä saatava hyöty on monin verroin houkuttelevampi vaihtoehto. (Mazarr, 2018)

Patrick Morgan listaa kuusi klassisen peloteteorian elementtiä: vakava konflikti, rationaalisuus, vastaisku, vakava tuhovaikutus, uskottavuus ja pelotteen

stabiilius. Klassisen peloteteorian ytimessä on oletus vakavasta konfliktista, joka seuraa, mikäli vastustaja päättää toteuttaa hyökkäyksellisiä toimia. Rationaalisuus koskee konfliktin kumpaakin osapuolta. Rationaalisuuskäsitteen mukaan kumpikin osapuoli pyrkii hankkimaan tilanteesta niin paljon tietoa kuin mahdollista ja tekemään päätöksensä sen perusteella. Vastaisku tarkoittaa niin suuria vastatoimia koettuun hyökkäykseen, että se vavisuttaa hyökkääjän yhteiskunnan perustuksia. Samoin tuhovaikutuksen tulee olla niin suuri, että sen pelossa ei kannata hyökätä. Jotta pelote olisi uskottavaa, on omaa suorituskykyä viestittävä uskottavasti ja myös omaa sotilaallista voimaa julkisesti demonstroitava. Pelotteen stabiilius tarkoittaa tilannetta, jossa kummallakin osapuolella on samanlainen käsitys hyökkäyksen seurauksista. Esimerkiksi ydinsota aiheuttaisi peruuttamatonta vahinkoa kummallekin osapuolella ja siksi siitä on edullisempaa pidättäytyä. (Morgan, 2003)

2.1.2 Peloteteorioiden uusia suuntauksia

Klassista peloteteoriaa on kritisoitu sen puutteista ja epäjohdonmukaisuuksista, mutta suurin syy teorian haasteisiin pohjautuu aikaan, jolloin teoria luotiin. Teoria syntyi 1950-luvulla ja 1960-luvulla se kehittyi lopulliseen muotoonsa. Teorian muodostamiseen vaikutti vahvasti kyseisen aikakauden hallitsevien valtioiden väliset suhteet ja ydinasevarustelu. Tämän vuoksi peloteteoria jäi näkökulmiltaan kapeaksi, koska siinä tehtiin oletuksia edellä mainitun asetelman mukaan. (Zagare & Kilgour, 2000)

Globaali turvallisuusympäristö on muuttunut oleellisesti kylmän sodan jälkeen, jotta klassista peloteteoriaa voisi enää sellaisenaan soveltaa nykyaikana. Kylmän sodan aikaisesta kaksinapaisesta maailmanjärjestyksestä on tullut moninapainen ja samalla valtioiden intressit ovat jakautuneet moneen eri suuntaan. Kehitys on luonut asymmetriaa valtioiden välille, joka ilmenee eriävissä intresseissä ja vallankäytön kohteissa tai ylipäätään siinä, miten valtiot jäsentävät muuttuneen maailmanjärjestyksen. Valtiokeskeisten uhkien merkitys on vähentynyt ja saanut rinnalleen uusia, hitaasti kehittyviä ja toisinaan vaikeasti määriteltäviä uhkia. Näitä ovat esimerkiksi terrorismi ja keskinäisriippuvuuden mukanaan tuomat uhkat, kuten suurvaltioiden intressien kohteena olevien maiden epävakaus. (Mazarr, 2018)

Globalisaatio, muutokset yhteiskunnissa ja informaatioteknologian kehittyminen ovat taustalla olevia suuria muutostekijöitä. Valtioiden johtamisessa on entistä tarkemmin huomioitava reaaliaikaisen informaation leviämisen vaikutukset, koska kaikki toimet ovat välittömästi globaalisti saatavilla. Myös riski valtion toiminnan väärinymmärtämiseen on suuri ja toisaalta taas informaatiotulvassa jokin tarkoitettu viesti voi jäädä huomaamatta. (Mazarr, 2018)

Sodankäynti on muuttunut monella tavoin kylmän sodan aikakauden jälkeen. Teknologian kehitys on johtanut entistä verkottuneempiin johtamis-, ase- ja tiedustelujärjestelmiin. Samalla tiedon määrä on eksponentiaalisesti kasvanut ja järjestelmien on kyettävä käsittelemään suuria määriä dataa kerrallaan. Taistelujen tempo on kasvanut ja päätöksentekoon käytettävä aika vähentynyt

oleellisesti sitten maailmansotien. Teknologian kehitys on luonut miehittämättömiä järjestelmiä esimerkiksi tiedusteluun ja valvontaan. (Lehto, 2016)

Digitalisoituminen on kehittänyt uudenlaisia uhkia, kuten kyberuhkat ja mahdollistanut hyökkäysten toteuttamisen aivan uudella tavalla täysin anonyymisti. Ei-valtiollisiin uhkiin vastaaminen on vaikeaa ja kyvyttömyys aukottomasti tunnistaa ja rangaista ei-valtiollisia uhkatoimijoita vie uskottavuutta myös pelotteelta. Myös pelotteen kohteiden jäsentäminen voi olla vaikeaa, jos ei tunnisteta niitä uhkia, joita vastaan tulisi pelotetta käyttää. (Mazarr, 2018)

Asevoimien kehityksessä on viime vuosikymmeninä tapahtunut suuria muutoksia, jotka pohjautuvat teknologian kehitykselle ja yhteiskunnallisille muutoksille. Teknologian kehitys vaikuttaa yhteiskunnan rakenteisiin ja toimintatapoihin. Lateraaliset verkostot korvaavat perinteiset hierarkkiset organisaatiorakenteet ja teknologisten innovaatioiden rakentamisesta ja ylläpidosta on tullut entistä merkittävämpi ammattikunta. Nämä muutokset vaikuttavat väistämättä myös asevoimien toimintaan. (Morgan, 2003)

Teknologian kehitys näkyy etenkin kolmessa elementissä. Näistä ensimmäinen on tiedustelun parantunut suorituskyky havaita, seurata ja jäljittää kohteita. Muutos näkyy toiminnan jokaisella tasolla aina maanpinnalta yksittäisen sotilaan välineistä avaruuteen ja satelliittiteknologiaan. Toinen suuri muutos on taistelukentän digitalisoituminen, joka on tuonut mukanaan informaatiovirtojen massiivisen kasvun ja informaation välittämisen reaaliaikaisesti. Tämä on aiheuttanut myös uudenlaisten uhkien syntymisen, kuten esimeriksi kyberuhkat. Kolmas suuri muutos liittyy aseteknologian kehittymiseen, joka on tuonut mukanaan entistä tarkempia asejärjestelmiä ja myös miehittämättömiä asejärjestelmiä. (Morgan, 2003) Teknologia mahdollistaa siis asevoimien toiminnan globaalisti, mahdollisimman vähin omin tappioin ja myös ei-kineettisin keinoin esimerkiksi kyberulottuvuudessa. Tämä kehitys on muuttanut myös osittain sodan kuvaa, koska ei ole enää selkeää rajaa sodan ja rauhan välillä.

Edellä kuvattu kehitys on jatkuvaa ja myös syy siihen, miksi perinteinen tapa jäsentää pelote ei enää toimi. Klassinen peloteteoria nojaa kahden suurvallan väliseen valta-asetelmaan ja ydinaseiden tuhovoimaan. Tämän vuoksi myös peloteasetelma on molemminpuolinen ja uhkakuva selkeä. Nykyajan moninapaisessa maailmassa ei ole olemassa enää vastaavaa asetelmaa tai selkeää uhkaa. On siis vaikeaa määritellä, mitä vastaan pelote muodostetaan ja mitkä ovat ne keinot, joilla omaa pelotetta viestitään uhkaa vastaan. Vielä hankalampaa on tietää, tuleeko oma viesti kuulluksi ja ymmärretyksi.

Michael Mazarr (2018) esittää, että Yhdysvaltojen tulee omaa pelotettaan luodessa huomioida kolme seikkaa. Ensinnäkin toisen valtion aggressioiden torjumiseen kuuluu pelotevaikutuksen lisäksi myös vakuuksien tarjoaminen. Näin ollen pelote luodaan laaja-alaisella strategialla ja politiikan teolla. Toisekseen pelotetta tulee myös tarkastella vastapuolen näkökulmasta ja peilata omia keinoja vastapuolen uskomuksiin ja oletuksiin. Kolmanneksi vastapuolen motivaatiotekijöihin on suhtauduttava vakavasti, määriteltävä se mitä vastaan halutan pelote rakentaa sekä selkeästi kommunikoitava oma kyky ja tahto toimia tarvittaessa. (Mazarr, 2018)

Sodankäyntiin on noussut perinteisten sotilaallisten ulottuvuuksien (maa, meri, ilma) rinnalle myös informaatio- ja kyberulottuvuus, jotka läpileikkaavat kolme ensin mainittua. Tämä aiheuttaa sotilaallisille operaatioille haasteita, koska fyysiseen sodankäyntiin on sovitettava yhteen myös informaatio- ja kyberoperaatioita sekä niitä vastaan puolustautuminen. Hybridiuhkien yleistymisen myötä peloteajattelussa ei voida rakentaa pelotetta vain toista valtiota ja konventionaalista asevoimaa tai ydinvoimaa vastaan. Uhkatoimija voi vaikuttaa vastapuoleen informaatio- tai kyberulottuvuuden kautta ilman, että tekijän syyllisyyttä voidaan aukottomasti todistaa. Tällainen kehitys on haastanut perinteisen tavan jäsentää pelote ja ajanut keskustelua kohti kaikki ulottuvuudet sisältävää, kokonaisvaltaista pelotetta (engl. Cross-Domain Deterrence). (Sweijs & Zilincik, 2021)

Tutkijoilla on erilaisia käsityksiä siitä, miten kokonaisvaltainen pelote tulee määritellä ja miten se tulee rakentaa. Suppeamman määrittelyn mukaan se koskee vain sotilaallisia joukkoja ja asevoiman käyttöä kaikissa sodankäynnin ulottuvuuksissa. Hyökkäykseen jossain ulottuvuudessa voidaan vastata toimimalla jossain toisessa ulottuvuudessa, joten sodankäynnin ei tarvitse olla täysin symmetristä. Toiset tutkijat ottavat mukaan myös ei-sotilaallisia elementtejä, kuten vaikkapa taloudelliset sanktiot. Sweijs & Zilincik, 2021)

Will Goodman määrittelee kahdeksan pelotteen tekijää: intressi, pelotteen julkistaminen, kieltotoimet, rankaisutoimet, uskottavuus, vakuus, pelko ja riskihyötysuhteen laskeminen. Valtio rakentaa pelotepolitiikkaa suojellakseen omia intressejään. Onnistuakseen tässä tavoitteessa, valtio viestii muille niistä intressiin kohdistuvista uhkista, joita ei hyväksytä ja joita vastaan aiotaan toimia. Vastatoimet voivat sisältää keinoja kielto- tai rankaisutoimista, jommastakummasta tai molemmista. Kieltotoimiin sisältyy vastustajan toimien häiritseminen ja tekeminen hyödyttömiksi. Rankaisutoimet sisältävät jonkin vastahyökkäyksen, jonka tulee olla välitön ja tarpeeksi vakava. Uskottavuus tarkoittaa sitä, että valtion viestimä pelote koetaan luotettavaksi. Vakuus on valtion tae siitä, että pelotteen mukaisia toimia ei suoriteta, mikäli vastapuoli pidättäytyy uhkatoimista. Vastustajan tulee myös pelätä vastatoimia, jotta riskihyötysuhde kääntyisi epäedulliseksi suorittaa uhkatoimi. Kokonaisuutena nämä tekijät muodostavat onnistuneen pelotteen. (Goodman, 2010)

Johtopäätöksenä voidaan todeta, että turvallisuuspoliittisen ympäristön ja suurvaltojen välisten voimasuhteiden muutosten sekä teknologian kehityksen myötä, klassinen peloteteoria ei enää kata valtioiden tarvetta aggressioiden ennaltaehkäisyyn. Vaikka klassisen peloteteorian mukainen jako rankaisuun ja aggression vaikutusten kiistämiseen onkin perustavanlaatuinen, on valtiolle hyödyllistä rakentaa pelotestrategia hyödyntäen valtion voiman instrumentteja, kuten poliittista valtaa, taloudellisia sanktioita sekä lain ja informaatioympäristön suomia mahdollisuuksia. Sotilaallinen voima säilyy näiden pehmeämpien keinojen rinnalla ja valtion entistä laajempi pelotetyökalupakki mahdollistaa aktiiviset toimet jo ennen kriisejä ja sodan käynnin kynnyksen alapuolella.

2.2 Kyberpelote

Kybersotaan liittyvää terminologiaa esiteltiin ensimmäisiä kertoja 1990-luvulla. Tuolloin termi ”kyber” liittyi vaikuttamiseen johtamis- ja tilannekuvajärjestelmiin. Samaan aikaan esiintyi ajatuksia verkkosodankäynnistä ja pelotteen rakentamisesta siihen liittyen. Ajatus kyberpelotteesta oli 1990-luvulla vielä kovin jäsentymätön eikä se tarkoittanut vielä saamaa kuin nykyään termillä ymmärretään. Vuoteen 2006 saakka akateeminen keskustelu kyberpelotteesta oli vielä vähäistä, mutta Viron patsaskiistan jälkeen vuonna 2007 koettiin räjähdysmäinen kasvu tieteellisissä artikkeleissa aina vuoteen 2016 saakka, jonka jälkeen kirjoitusten määrä laski selvästi. (Soesanto & Smeets, 2021)

Nykyään kyberpelote voidaan käsittää ainakin kolmella eri tavalla sotilaallisessa kontekstissa. Ensinnäkin se voi tarkoittaa sotilaallisen kybervoiman käyttöä pelotetarkoituksessa sotilaallista hyökkäystä vastaan. Toisekseen se voi tarkoittaa juuri päinvastaista, eli sotilaallisten resurssien käyttöä pelotetarkoituksessa kyberhyökkäystä vastaan. Kolmanneksi se voi tarkoittaa sotilaallisten kybersuorituskykyjen käyttöä pelotetarkoituksessa kyberhyökkäystä vastaan. Suurin osa nykypäivän kybertutkimuksesta keskittyy kahteen jälkimmäiseen vaihtoehtoon. (Soesanto & Smeets, 2021) Vaikka tässä tutkimuksessa tarkastelun kohteena ovatkin sotilaalliset kyberoperaatiot, ei tarkastelua rajata vain asevoimien toimintaan. Kuten luvun 2.1 päätteeksi todettiin, valtiolle on edullista sisällyttää monipuolisia keinoja omaan pelotestrategiaansa. Näin ollen luvussa 2.2 tarkastellaankin kyberpelotetta rajaamatta sitä mihinkään ennalta valittuun kontekstiin.

Mariarosaria Taddeon (2018a) mukaan klassinen peloteteoria ei toimi kybertoimintaympäristössä, koska kyberhyökkäyksellä on ominaisuuksia, joita fyysisillä hyökkäyksellä ei ole: globaali ulottuvuus, hyökkäys on mahdollista tehdä anonyymisti ja sen vaikutukset voivat ulottua kohteen ulkopuolelle. Klassisen peloteteorian kolme elementtiä; uskottava viestintä, attribuutio sekä puolustus ja vastatoimet, eivät päde sellaisenaan kyberpelotteessa. Attribuutio on haasteellista, koska kyberhyökkäys voidaan tehdä kolmannen osapuolen kautta ja vaikka hyökkäävä taho sataisiinkin selville, voi syyllisyyden osoittaminen olla haasteellista. Ilman selkeää osoitusta hyökänneestä tahosta, ei myöskään vastatoimet ole mahdollisia. (Taddeo, 2018a)

Uskottava viestintä on pelotteen välttämätön osatekijä. Viestinnän tarkoitus on kertoa uhkatoimijalle, että hyökkäys ei kannata. Tällainen vaatii puolustavalta taholta uskottavuutta, joka perinteisessä pelotteessa rakennetaan ajan kanssa esimerkiksi sotilaallista voimaa ja kriisien ratkomiskykyä demonstroimalla. Tietyssä määrin sama pätee myös kybertoimintaympäristössä. Viestintää heikentää kuitenkin valtioiden halu salata oma suorituskyky ja omaan infrastruktuuriin kohdistuneet hyökkäykset. Tällöin valtiolla ei ole samanlaista mahdollisuutta viestiä omista kyvyistään kybertoimintaympäristössä kuin fyysisessä maailmassa. (Taddeo, 2018a)

Pelkkä omien verkkojen puolustaminen on tehotonta pelotteen näkökulmasta. Mikään järjestelmä ei ole aukoton, joten hyökkäys pääsee aina lopulta läpi.

Onnistuessaankaan kyberpuolustus ei tuo strategista etua hyökkääjään nähden, koska kyberhyökkäyksen epäonnistuminen tuskin tuo yksinään voittoa vastustajasta. Vastahyökkäys voi olla toimiva osa kyberpelotetta, mutta voi sisältää eskalaation riskin, koska kyberase voi olla hankalasti kontrolloitava ja levitä kohdejärjestelmän ulkopuolelle. (Taddeo, 2018a)

Taddeon (2018b) kyberpeloteteoria sisältää kolme elementtiä: kohteen tunnistaminen, vastahyökkäys ja voimannäyttö. Kohteen, eli hyökkäävän tahon tunnistaminen antaa puolustajalle mahdollisuuden estää hyökkäävä järjestelmä ja mahdollisesti vastahyökätä riippumatta siitä, kuka hyökkäävä taho on oikeasti. Tämä poistaa attribuutio-ongelman, kun hyökkääjää ei pyritäkään tunnistamaan, vaan järjestelmä, josta hyökkäys toteutetaan. Samalla näytetään omaa kybervoimaa ja hankitaan uskottavuutta. (Taddeo, 2018b)

Tim Stevens (2012) nostaa esille kyberpelotteen rakentamisen problematiikkaa verrattuna luvussa 2.1 esiteltyihin Patrick Morganin kuuteen pelotteen elementtiin (Morgan, 2003). Stevens nostaa esille seikkoja, joiden mukaan Morganin periaatteet eivät ole sovellettavissa kyberpelotteeseen:

1. Kybertoimintaympäristössä ei esiinny vakavia sotilaallisia konflikteja.
2. Klassisiin peloteteorioihin liittyvä olettamus rationaalisesta päätöksenteosta on vääristynyt, koska valtiosta riippumattomat toimijat eivät noudata tällaisia teoriamalleja.
3. Vastatoimien toteuttamismahdollisuudet heikentyvät attribuutio-ongelman ja maantieteellisen riippumattomuuden takia.
4. Vastustajaa on vaikeaa uhkata suurilla vahingoilla, koska vastatoimet saattavat olla kertakäyttöisiä ja kohdetta voi olla vaikeaa määritellä.
5. Kybertoimintaympäristössä on haastavaa esitellä sotilaallista voimaa, siellä ei ole voimankäytön sääntöjä ja vastahyökkäys on mahdollinen, joten kyberpelote ei saavuta tarvittavaa uskottavuutta.
6. Kybertoimintaympäristössä on haastavaa saavuttaa tasapainoa, koska kyberhyökkäyksillä on vaarana eskaloitua fyysiseksi konfliktiksi. (Stevens, 2012)

Stevensin ajattelu perustuu oletukseen, jossa kybertoimintaympäristöä suojataan kybersuorituskykyjen avulla. Tätä problematiikkaa on ratkonut muun muassa Scott Jasper (2015) ehdottamalla, että kyberpelote on edullisinta rakentaa aktiivisen kyberpuolustuksen keinoin. Tämä edellyttää reaaliaikaista valvontaa ja uhkien havaitsemiskykyä, analyysikykyä, kykyä vähentää uhkien vaikutusta sekä laillisten vastakeinojen toteuttamista tarvittaessa omien verkkojen ulkopuolelle. Aktiivinen kyberpuolustus tuottaa resilienssin keinoin mahdollisuuksia kieltää vastustajan toimien vaikutus sekä aiheuttaa vastahyökkäysten keinoin vastustajalle tappioita. (Jasper, 2015)

Uri Torin (2017) kehittämä kumulatiivinen peloteparadigma nojaa väitteeseen, jonka mukaan ydinasepelotteen periaatteet eivät sovellu kybertoimintaympäristössä esiintyvien uhkien torjumiseen. Väitteen mukaan on epärealistista olettaa, että kyberpelotteen avulla saataisiin torjuttua kaikki kybertoimintaympäristössä esiintyvät uhkat. Sen sijaan kyberuhkiin vaikutetaan vastatoimilla,

jotka ovat kohdennettu tietyntyyppisiin uhkiin. Näitä vastatoimia toistetaan pitkän ajan kuluessa useita kertoja. (Tor, 2017)

Kumulatiivisen peloteparadigman mukaan vastapuolelle on kommunikoitava selkeästi ne rajat, joiden ylityksestä seuraa vastatoimia. Kommunikoinnin onnistumiseksi on tunnettava uhkatoimijan strateginen kulttuuri, jotta pelotesignaalit ymmärretään oikein. Signaalien ilmaisemiseen on oltava selkeä ja yksiselitteinen tapa. On myös tiedustelun keinoin kyettävä seuraamaan lähetettyjä signaaleja ja vastapuolen reaktioita niihin. Tällaista kommunikointia voidaan toteuttaa kansainvälisen median, instituutioiden ja organisaatioiden kautta sekä diplomaattisuhteiden avulla ja antamalla vastapuolen tiedustelulle sopivia syötteitä. (Tor, 2017)

Kumulatiivisen peloteparadigman yksi periaatteista on kyky ja tahto reagoida kyberuhkiin hyökkäämällä, jotta vastapuoli joutuu harkitsemaan uhkatoimien kannattavuutta. Hyökkäyksellisen toiminnan on oltava jatkuvaa ja kybertoimintaympäristössä tapahtuvan toiminnan lisäksi on harkittava kineettisiä vastatoimia tai diplomatian ja talouden keinoja. Tällä tavoin vahvistetaan pelotevaikutusta jatkuvasti ja pitkällä aikavälillä. Kykyvalikoimaa on käytettävä ja demonstroitava jatkuvasti pelotevaikutuksen vahvistamiseksi. Lisäksi on pyrittävä osoittamaan ylivertaisuutta, joka saavutetaan jatkuvilla pienillä voitoilla tiedustelu- ja hyökkäyskykyä käyttämällä. Toistuvat onnistumiset kyberuhkiin reagoimisessa vakuuttavat vastapuolen siitä, että hyökkäys ei kannata. (Tor, 2017)

Kumulatiivisen peloteparadigman mukaan hyökkääminen tulee tehdä vaikeaksi ja kalliiksi vastapuolelle. Tämä saavutetaan kybertoimintaympäristön jatkuvalla kehittämisellä ja rakentamisella. Rakentamiseen sisältyy teknologisten ratkaisujen ja suojatoimien kehittäminen, joilla parannetaan oman kybertoimintaympäristön turvallisuutta. (Tor, 2017)

Kyberpelotetta voidaan käsitellä laajemman näkökulman kautta, kuin pelkkänä kybertoimintaympäristössä tapahtuvana toimintana. Annegret Bendiek ja Tobias Metzger (2015) esittävät neljää keinoa kyberpelotteen rakentamiseen: säännöspohjan kehittäminen kyberhyökkäyksiä ja häiriöitä vastaan, resilienssin kehittäminen kyberhyökkäyksistä toipumiseen, kansainvälisten sääntöjen luominen hyväksyttävästä toiminnasta ja kohteiden lainvoimaisuudesta kybertoimintaympäristössä sekä kansallista strategiaa kyberpelotteen luomiseen. Kyberpelotteen tulisi sisältää laaja-alaisia keinoja alkaen poliittisesta vaikuttamisesta päättyen aktiiviseen puolustukseen ja vastatoimiin. Vastatoimissa tulee huomioida kineettisten vastakeinojen mahdollisuus, mikäli kyberhyökkäys vaurioittaa vakavasti fyysistä infrastruktuuria tai uhkaa kansalaisten henkeä. (Bendiek & Metzger, 2015)

Joseph Nye (2017) esittää neljää varoitusmekanismia vihamielisen toiminnan torjumiseen kybertoimintaympäristössä: rankaisupelote, kieltopelote, suostuttelu ja normatiiviset tabut. Siitä huolimatta, että rankaisupelote ei ole kovinkaan tehokas kyberulottuvuudessa siihen liittyvän problematiikan takia, on se kuitenkin yksi oleellinen tekijä kyberpelotteen kokonaisuudessa. Rankaisun käyttö kuitenkin edellyttää tekijän tunnistamisen ja syylliseksi todistamisen. (Nye, 2017)

Kieltopelotteeseen kybertoimintaympäristössä kuuluu kyky toipua hyökkäyksistä. Kun vastustaja ei saa hyökkäyksellään toivottua vaikutusta aikaan, voi se jo itsessään toimia hyökkäyshaluja alentavana tekijänä. Aktiivinen puolustus sisältää niin teknisiä keinoja parantaa oman kybertoimintaympäristön resilienssiä kuin myös omien verkkojen monitorointia ja aktiivista uhkanmetsästystä. (Nye, 2017)

Suostuttelu perustuu ajatukseen, että osapuolilla on jotain yhteistä, jonka menettämisestä kärsivät molemmat. Tällöin kyberhyökkäyksestä saatava hyöty voi jäädä pienemmäksi, koska sen myötä hyökkäävä osapuoli menettää kohteensa kanssa jonkin yhteisen edun. Kansainväliset suhteet ovat monimutkaisia ja alat muuttuvia, joten yhteisten etujen merkitystä sekä oman valtion että vastapuolen näkökulmasta on arvioitava jatkuvasti. (Nye, 2017)

Neljäntenä varoitumekanismina Nye (2017) esittää normit ja tabut. Tämä mekanismi perustuu maineen menettämiseen, joka voi seurata yhteisesti sovittujen tai sääntöjen rikkomisesta tai hyökkäämisestä kohteeseen, joka on yleisesti luokiteltu suojelluksi. Tällaisen mekanismin rakentaminen edellyttää kansainvälisesti sovittuja sääntöjä, jotta hyökkäyksen riski kasvaisi liian suureksi hyökkääjän näkökulmasta kansainvälisten sanktioiden pelossa. (Nye, 2017)

Burtonin (2018) mukaan kokonaisvaltainen kyberpelote sisältää kolme pelotteen elementtiä: rangaistuksen, kiellon ja resilienssin. Rangaistus tulee skaalata uhkatoimijan ja tehdyn teon mukaan. Rangaistus voi olla vastaisku fyysisessä maailmassa tai kybertoimintaympäristössä, oikeudellinen toimenpide, taloudellinen pakote tai diplomaattinen eristys. Kieltovaikutus voi olla normatiivinen, sosiaalinen tai tekninen. Resilienssi koostuu kyvystä toipua ja jatkaa toimintaa uhkasta riippumatta sekä näiden tekijöiden suunnittelusta. Pelotevaikutus luodaan eri toimijoiden yhteistyöllä. Näitä ovat kansalliset ja kansainväliset organisaatiot ja viranomaiset, joihin kuuluu sekä julkisen että yksityisen sektorin toimijoita. Tällä tavoin luotu pelote kohdistuu valtiollisia toimijoita, valtion sisäisiä uhkia sekä rikollisuutta ja terrorismia vastaan. (Burton, 2018)

Kokonaisvaltainen kyberpelote sisältää sosiaalisia, normatiivisia, lakiin perustuvia ja teknologisia lähestymistapoja kyberuhkien torjumiseen. Kokonaisvaltaisuus tuo mukanaan myös haasteita, joista yksi on aika. Kyberpelotteeseen vaadittavan lainsäädännön valmistelu ja myös resilienssin rakentaminen ovat aikaa vieviä prosesseja ja vaativat jatkuvaa ylläpitoa. Myös sosiaalisten ja normatiivisten lähestymistapojen rakentaminen on hidasta. Kokonaisvaltaisen kyberpelotteen rakentaminen vaatii myös muita resursseja sekä kansallisesti että kansainvälisesti. Samoista resursseista kilpailevat muut yhteiskunnalliset ja kansainväliset tarpeet. On myös huomioitava, että mikäli pelotekonseptia laajennetaan koskemaan muita kuin sotilaallisia näkökulmia, voi pelotteen merkitys itsessään vähentyä. (Burton, 2018)

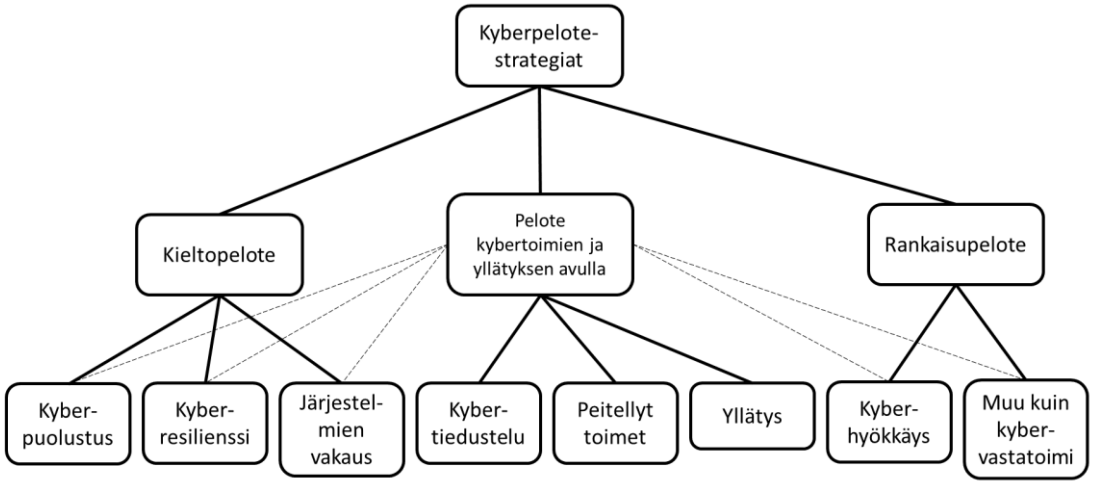
Yksi kyberpelotteen haasteista on attribuution osoittaminen. Tämä tarkoittaa, että on kyettävä uskottavasti esittämään todisteita tapahtuneesta hyökkäyksestä ja sen tekijästä. Kybertoimintaympäristössä on mahdollista peittää jälkensä teknisten ja sosiaalisten keinojen avulla. Hyökkäyksen alkuperää on voitu

häivyttää useiden etäpalvelinten taakse ja uhkatekijänä voi esiintyä jokin muu taho kuin varsinainen hyökkääjä. (Nye, 2017)

Attribuution osoittamiseen liittyy tärkeitä yleisöjä. Puolustavan valtion tulee saada tarpeeksi vakuuttava todistusaineisto omalta tiedusteluorganisaatioltaan, jotta vastatoimet ovat laillisesti oikeutettuja. Hyökännyt osapuoli ei voi kuitenkaan tietää vastapuolen täyttä kykyä tunnistaa tapahtunut hyökkäys. Se voi kieltää osallisuutensa, mutta ei voi olla varma siitä, kuinka uskottavaa tällainen kieltäminen on. Toisaalta hyökkäävä osapuoli voi tarkoituksella jättää vihjeitä hyökkäyksestä ja samalla kieltää osallisuutensa tapahtuneeseen. Joka tapauksessa sekä kansallinen että kansainvälinen yleisö tulee vakuuttaa vastatoimien oikeellisuudesta. Tiedon jakamisessa tulee tarkoin harkita, kenelle sitä jaetaan ja millaista tietoa. Liian tarkat tekniset paljastukset voivat vaarantaa omia suorituskykyjä, jolloin näitä ei välttämättä voida enää käyttää tulevaisuudessa. (Nye, 2017)

Jim Chenin (2017a) mukaan kyberpelotetta ei voida rakentaa vain rankaisutai kieltopelotteen varaan, vaan kokonaisuuteen tarvitsee sisällyttää näiden väliin elementtejä, jotka hyödyntävät kybertoimintaympäristössä esiintyviä mekanismeja. Näitä tekoälyä ja koneoppimista hyödyntävät elementit ovat tiedustelutiedon kokoaminen, peitellyt toiminnot ja yllätys. (Chen, 2017a)

Tiedustelutiedon kerääminen tähtää hyökkäävän tahon identiteetin paljastumiseen. Tiedustelusensorit syöttävät havainnot tekoälyn käsiteltäviksi ja koneoppimisen avulla lopulta hyökkääjän henkilöllisyys on mahdollista luotettavasti paljastaa. Tämä tuo avun attribuutio-ongelmaan. Tekoälyn avulla on mahdollista myös rakentaa kyberaseita, jotka kykenevät muuttumaan ja mukautumaan erilaisiin tilanteisiin. Näin toteutettuna voidaan tehdä peiteltyjä toimintoja, joista vastustaja ei koskaan tiedä mitä odottaa. Näin saavutetaan yllätystekijä. Seuraavassa kuvassa (kuvio 3) on esitelty Chenin ajatus kyberpelotekokonaisuudesta. Tekoälyteknologiaa hyödyntämällä voidaan tuoda myös uusia elementtejä perinteisiin pelotestrategioihin ja vastatoimet kyberhyökkäyksiin kyetään toteuttamaan reaaliaikaisesti. (Chen, 2017a)



KUVIO 3 Kyberpelotekokonaisuus Chenin mukaan (Chen, 2017a)

Chenin (2017b) mukaan tällainen kokonaisvaltainen lähestymistapa mahdollistaa kyberpelotteen rakentamisen yhdistelemällä virtuaalisia, psykologisia, moraalisia ja fyysisiä vaikutuksia. Edelleen tämä mahdollistaa kybersuorituskykyjen käytön yhdessä valtion voiman instrumenttien, kuten poliittisen, taloudellisen, oikeudellisen ja sotilaallisen vallan kanssa. (Chen, 2017b)

Chenin (2018a) myöhemmän tutkimuksen mukaan erityyppiset pelotteet ovat enemmän tai vähemmän sotaisia, kun verrataan esimerkiksi kovia keinoja, eli ydinpelotetta ja konventionaalista pelotetta pehmeisiin keinoihin, eli kyberpelotteeseen sekä taloudelliseen ja diplomaattiseen pelotteeseen. Kaikkia edellä mainittuja voidaan käyttää pelotteena kybertoimintaympäristön suojaksi, mutta vain kyberpelote kykenee välittömiin vastatoimiin ilman merkittäviä viiveitä. Tämän vuoksi valtion on rakennettava uskottava kyberpelote. (Chen, 2018a) Kybersuorituskykyjen käyttö pelotteen yhtenä keinona rikastaa valtion pelotetyökalupakkia, koska kybersuorituskyvyillä voidaan kybertoimintaympäristön lisäksi vaikutta myös sen ulkopuolella sijaitseviin kohteisiin. (Chen, 2018b)

Johtopäätöksenä voidaan todeta, että kybertoimintaympäristössä esiintyvien uhkien ennaltaehkäisy pelotestrategian avulla on haastavaa, mikäli kyberuhkiin varaudutaan vastaamaan pelkin kyberoperaatioin. Merkittävin haaste liittyy valtioiden pyrkimykseen salata kybersuorituskykynsä, koska tämä tahto hankaloittaa voiman demonstroimista, joka puolestaan kuuluu oleellisesti pelotteen ydinperiaatteisiin. Ilman kykyä osoittaa voimaa ja tahtoa käyttää tätä voimaa, jää pelotteen kaksi tärkeää kulmakiveä toteutumatta. Pyrkimys kybersuorituskykyjen salaamiseen haastaa myös attribuution onnistumista, koska jos hyökkäävää tahoa ei haluta julkisesti tunnistaa, on vaikeaa tehdä kansainvälisen yhteisön hyväksymiä vastatoimia.

Kyberpelotteeseen liittyvien haasteiden takia, on hyödyllisempää tarkastella kybertoimintaympäristöön liittyvän pelotteen rakentamista osana valtion pelotekokonaisuutta. Tällöin vastatoimet eivät rajoitu pelkästään

kyberoperaatioihin ja niiden toteuttamismahdollisuuksiin, jolloin pelote itsessään voi saavuttaa suurempaa uskottavuutta uhkatoimijan silmissä.

Resilienssi voi olla uskottavampaa pelotteen näkökulmasta kuin rankaisun uhka. Mikäli omat järjestelmät kyetään suojaamaan niin, että kyberhyökkäykseen vaadittavat resurssit ovat huomattavat, voi se toimia kieltopelotteen tavoin. Toisaalta, kuten Chen (2018a) toteaa, on valtiolla oltava myös uskottavuutta hyökkäyksellisten kybersuorituskykyjen osalta. Tosin pelkkä kyky ei riitä, vaan valtion on osoitettava myös tahto käyttää näitä suorituskykyjä tarvittaessa.

2.3 Kyberoperaatiot

Sotilaallinen operaatio on joukko toimia, joilla saavutetaan joukolle asetettu tehtävä tai tavoite. Sotilaallinen operaatio nimetään yleensä sen mukaan, mihin kyseisen operaation toimet keskittyvät ja millaisia toimintoja tavoitteen saavuttamiseksi käytetään. Esimerkiksi ilmaoperaatio keskittyy ilmavoimien käyttöön ja merioperaatio tapahtuu merellä merivoimien kalustoa ja toimintoja käyttämällä. Hyvin usein operaatio sisältää eri tyyppisiä aktiviteetteja. (US Joint Chiefs of Staff, 2017) Tällaisesta on hyvä esimerkki yhteisoperaatio, jossa sotilaallista voimaa voidaan käyttää taistelutilan kaikissa ulottuvuuksissa (maa, meri, ilma, kyber, informaatio).

Kyberoperaatio on kybertoimintaympäristössä tai sen välityksellä toteutettava sotilaallinen operaatio. (US Joint Chiefs of Staff, 2018) Tyypillisesti kybertoimintaympäristössä toteutettavat operaatiot ovat sellaisia operaatioita, jotka estävät vastustajan kybertoimintaympäristössä sijaitsevien resurssien käytön tai manipuloivat siellä sijaitsevia vastustajan käyttämiä tietoja, tietojärjestelmiä tai verkkoja. (US Army War College, 2022)

Kyberoperaatioilla vaikutetaan vastustajan kykyyn muodostaa tilannetietoisuutta sekä käyttää tieto- ja informaatiojärjestelmiään. Kyberoperaatioilla myös suojataan omia järjestelmiä ja turvataan oma toiminnanvapaus kybertoimintaympäristössä. Kyberoperaatioihin pätevät samankaltaiset lainalaisuudet kuin muuhunkin sotilaalliseen voimankäyttöön. Kohde pyritään ensin tiedustelemaan ja sen toiminta kartoittamaan ennen siihen vaikuttamista. (Lehto & Limnéll, 2017)

Jotta kyetään arvioida kyberoperaatioiden roolia kyberpelotteen rakentamisessa, tulee määritellä perusteet. Ensiksi tulee määritellä ympäristö, missä toimitaan. Toiseksi tulee määritellä kyberoperaatiot ja niihin liittyvät toiminnot, koska pelotteeseen liittyy oleellisesti suorituskyvyt ja niiden käyttö. Koska Yhdysvallat on länsimaissa kybertoimialan edelläkävijä ja Suomen Puolustusvoimat on seurannut muun muassa määritelmissä Yhdysvaltojen ajatuksia (Laari ym., 2019) on perusteltua käyttää Yhdysvaltojen käyttämiä kybertoimintaympäristön ja kyberoperaatioiden määritelmiä tässä tutkimuksessa. Kolmanneksi tulee tarkastella kyberoperaatioilla saavutettavia vaikutuksia, jotta ymmärretään niiden merkitys pelotteen rakentamisessa.

Tässä tutkimuksessa käytetään kybertoimintaympäristön määrittelynä kolmikerroksista mallia, jota käytetään esimerkiksi Yhdysvaltojen sotilaallisissa ohjesäännöissä ja Suomen Puolustusvoimien kyberpuolustus-ohjeessa. Mallin mukaan kybertoimintaympäristö koostuu loogisesta, fyysisestä ja käyttäjäkerroksesta. Looginen kerros sisältää sähköisessä muodossa olevia asioita, esimerkiksi kaiken mitä Internetistä, yksittäisiltä päätelaitteilta tai palvelimilta löytyy tiedon ja palveluiden jakamiseen, säilyttämiseen ja käyttämiseen liittyen. Loogisen kerroksen elementit eivät ole sidoksissa mihinkään fyysiseen sijaintiin. (Laari ym., 2019)

Fyysinen kerros koostuu nimensä mukaan fyysisistä laitteista ja tiedonsiirtovälineistä, kuten tietokoneet, palvelimet tai valokuitu. Fyysiseen kerrokseen kuuluvat myös verkon fyysisten osien ja tiedonsiirtojärjestelmien maantieteelliset osat. (Laari ym., 2019)

Käyttäjäkerros koostuu ihmisistä ja heidän virtuaalisista identiteeteistään. Virtuaalinen identiteetti on esimerkiksi henkilön sähköpostitili tai sosiaalisen median käyttäjätunnus. Yhdellä ihmisellä voi olla monta virtuaalista identiteettiä ja useampi ihminen puolestaan voi jakaa yhteisen identiteetin, esimerkiksi yhteiskäyttöisen sähköpostitilin kautta. (Laari ym., 2019)

2.3.1 Kyberoperaatiot ja niiden toiminnot

Kyberoperaatiot voidaan jakaa niiden tavoitteiden mukaisesti puolustuksellisiin, hyökkäyksellisiin ja tukeviin operaatioihin. (US Joint Chiefs of Staff, 2018) Tulee kuitenkin huomata, että kukin operaatiotyyppi voi sisältää samantyyppisiä toimia. Esimerkiksi puolustukselliseen kyberoperaatioon voi sisältyä hyökkäyksellisiä elementtejä ja päinvastoin.

Eräs tapa jakaa kyberoperaatioiden toiminnot on käsitellä niitä neljänä kokonaisuutena: kyberturvallisuus, kyberpuolustus, kybertoimintaympäristön hyväksikäyttö ja kyberhyökkäykset. Kyberturvallisuudella estetään omien verkkojen luvaton käyttö ja niihin tunkeutuminen. Kyberpuolustus tähtää omien verkkojen suojelemiseen aktiivisin toimin. Kybertoimintaympäristön hyväksikäyttö tähtää omien hyökkäyksellisten kyberoperaatioiden mahdollistamiseen tiedustelemalla ja luomalla jalansijoja vastustajan järjestelmiin. Kyberhyökkäyksellä aiheutetaan vaikutuksia vastustajan kybertoimintaympäristöön yhdellä tai useammalla kybertoimintaympäristön kerroksella. (US Department of the Army, 2021)

Kyberoperaatioihin liittyy myös kiinteästi taistelutilan valvonta, tiedustelu ja taistelutilan muokkaus kuten mihin tahansa muuhun operaatioon, mutta fyysisen ulottuvuuden sijaan toimet kohdistuvat kybertoimintaympäristöön. Nämä ovat kyberoperaatioita tukevia toimia. (Laari ym., 2019)

Puolustuksellisilla kyberoperaatioilla suojataan omaa johtamisjärjestelmäinfrastruktuuria aktiivisilta uhkilta kybertoimintaympäristössä. Suojattavia kohteita ovat tieto itsessään sekä tietoverkot ja kybertoimintaympäristöön liitetyt laitteet. Puolustuksellinen kyberoperaatio toteutetaan jotakin tiettyä uhkaa vastaan ja sen tarkoituksena on taata oman kybertoimintaympäristön turvallisuus. Puolustuksellisen kyberoperaation tavoitteena on estää tai häiritä vastustajan

toimia suojattavassa ympäristössä ja palauttaa vaarantunut ympäristö turvalliseksi. Keinovalikoimaan kuuluu sekä sisäisiä suojatoimia että vastatoimia. (US Joint Chiefs of Staff, 2018)

Suurin osa puolustuksellisen kyberoperaation toiminnoista ovat suojatoimia. Suojatoimet koostuvat aktiivisista keinoista uhkatekijän havaitsemiseksi ja siihen vastaamiseksi suojattavan ympäristön sisällä. Ennakoiva ja aggressiivinen uhkanmetsästys tai sisäiset vastatoimet tähtäävät uhkatekijän eliminoimiseen ja sen vaikutusten vähentämiseen jopa ennen kuin varmuus oman verkon vaarantumisesta on saatu. Sisäisiä vastatoimia ovat esimerkiksi vaarantuneen verkon eristäminen, uudelleenreititys tai palauttaminen. (US Joint Chiefs of Staff, 2018)

Puolustuksellisen kyberoperaation vastatoimet ulottuvat oman suojattavan ympäristön ulkopuolelle. Tämän vuoksi vastatoimet on koordinoitava muun sotilaallisen toiminnan kanssa. Vastatoimia suunniteltaessa tulee huomioida uhkatoimijan muut hyökkäykselliset toimet, arvioida uhkan vaikutus ja olla varma siitä, että hyökkääjän alkuperä on varmistettu. (US Joint Chiefs of Staff, 2018)

Hyökkäyksellisen kyberoperaation tavoitteena on projisoida voimaa vieraassa kybertoimintaympäristössä tai sen kautta omien tavoitteiden tukemiseksi. Hyökkäyksellinen kyberoperaatio voi kohdistua vastustajan kybertoimintaympäristön kohteisiin tai saada aikaan vaikutuksia fyysisessä ulottuvuudessa. Fyysisiä kohteita voivat olla esimerkiksi vastustajan asejärjestelmät, johtamisjärjestelmäinfrastruktuuri, logistiikka tai muut arvokkaat kohteet. Hyökkäyksellinen kyberoperaatio liittyy aina suurempaan kontekstiin sekä sen tavoitteet ja kohteet määritellään osana sotilaallisia tavoitteita. (US Joint Chiefs of Staff, 2018)

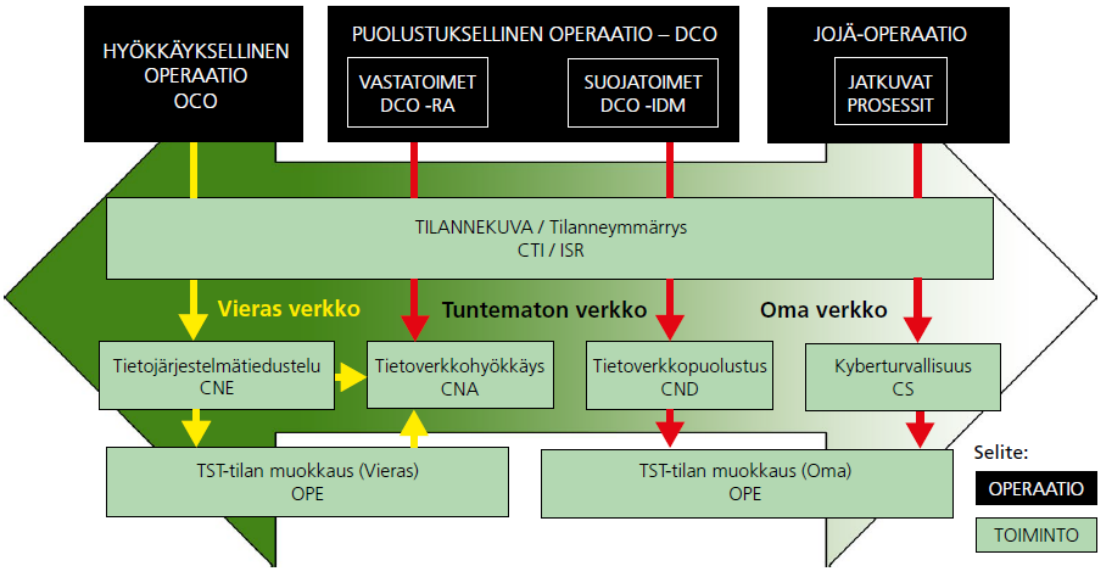
Tukevista kyberoperaatioista voidaan käyttää nimeä johtamisjärjestelmäoperaatiot (JOJÄ-operaatio). (Laari ym., 2019 Nämä sisältävät toimia, joilla turvataan ja ylläpidetään oman kybertoimintaympäristön elementtejä sekä mahdollistetaan omissa verkoissa toimiminen ja niiden hallinnointi. JOJÄ-operaatioiden perimmäinen tarkoitus on tiedon eheyden, luotettavuuden ja saatavuuden turvaaminen. (US Joint Chiefs of Staff, 2018)

Toisin kuin puolustukselliset kyberoperaatiot, JOJÄ-operaatioita ei toteuteta mitään tiettyä uhkaa vastaan, vaan niiden avulla varaudutaan kaikkia omaa kybertoimintaympäristöä heikentäviä uhkia vastaan. Tietoturvallisuutta kehitetään hyödyntämällä kaikkea saatavilla olevaa tietoa uhkatekijöistä. (US Joint Chiefs of Staff, 2018)

JOJÄ-operaatioiden keskeisimpiä tekijöitä ovat ennakoivat toimet, joilla hallitaan oman kybertoimintaympäristön haavoittuvuuksia. Näihin kuuluvat verkkojen ylläpidolliset toimenpiteet, auditoinnit ja testaus sekä kybertoimintaympäristön laajentaminen esimerkiksi taktisilla verkoilla. JOJÄ-operaatio voidaan käsittää jatkuvana kyberturvallisuutta ylläpitävänä operaationa. (US Joint Chiefs of Staff, 2018)

Kyberoperaatioiden toteuttaminen vaatii tehtävään sopivan valikoiman toimintoja, joilla asetettu tavoite saavutetaan. Toiminnoilla luodaan haluttu vaikutus kybertoimintaympäristössä. Puolustuksellisten kyberoperaatioiden suojatoimia ja JOJÄ-operaatioita toteutetaan omassa kybertoimintaympäristössä ja ne ovat luonteeltaan jatkuvia. Nämä operaatiot muodostavat suurimman osan

kyberturvallisuudesta. On kuitenkin tilanteita, joissa tarvitaan hyökkäyksellisiä toimintoja oman kybertoimintaympäristön ulkopuolella. Silloin tulevat kyseeseen puolustuksellisen kyberoperaation vastatoimet tai hyökkäykselliset kyberoperaatiot. Nämä ovat kestoltaan rajattuja ja vaativat aina asianmukaisen suunnittelun, oikeuden toteuttaa ja synkronoinnin muun sotilaallisen toiminnan kanssa. (US Joint Chiefs of Staff, 2018) Kuviossa xx esitetään kyberoperaatioihin sisältyviä toimintoja.



KUVIO 4 Kyberoperaatiot ja toiminnot (Laari ym., 2019)

Kyberturvallisuus (engl. Cyber Security) on jatkuva prosessi, joka sisältyy etenkin JOJÄ-operaatioon. (Laari ym., 2019) Kyberturvallisuuden päämääränä on suojata tiedon saatavuutta, yhteneväisyyttä ja luotettavuutta sekä estää tiedon luvaton käyttö ja muokkaaminen. Kyberturvallisuuteen kuuluu keinoja, joilla estetään vastustajaa hyödyntämästä haavoittuvuuksia ja vahvennetaan omia järjestelmiä uhkatoimintaa vastaan. Näihin keinoihin sisältyvät muun muassa salasanaturvallisuus, haavoittuvuuksien paikkaaminen, tiedon salaaminen, käyttäjien kouluttaminen, epäilyttävien nettisivustojen estäminen ja käyttämättömien reitittimen porttien sulkeminen. (US Joint Chiefs of Staff, 2018)

Tietoverkkopuolustus (engl. Computer Network Defense) on joukko teknisiä toimia, joita käytetään etenkin puolustuksellisen kyberoperaation suojatoimina. (Laari ym., 2019) Tietoverkkopuolustus kohdistuu omaan kybertoimintaympäristöön ja sen avulla torjutaan tunnistettuja uhkia. Se sisältää aktiivisia toimia, joilla havaitaan, luokitellaan ja torjutaan uhkia sekä vähennetään niiden vaikutusta. (US Joint Chiefs of Staff, 2018)

Tietojärjestelmätiedustelu (engl. Computer Network Exploitation) sisältää sotilaallisia toimia, joilla hankitaan tietoa kohteesta ja mahdollistetaan tulevia hyökkäyksellisiä kyberoperaatioita tai vastatoimioperaatioita. (Laari ym., 2019) Tietojärjestelmätiedusteluun kuuluu pääsyn hankkiminen ja ylläpitäminen kohdejärjestelmiin sekä omien hyökkäyksellisten suorituskykyjen käytön

mahdollistaminen. Tähän päästään keräämällä tietoa kohteen haavoittuvuuksista, mahdollistamalla hyökkäystyökalun kehitys ja tukemalla operaatioiden suunnittelua, toteutusta ja arviointia. (US Joint Chiefs of Staff, 2018)

Tietoverkkohyökkäyksillä (Computer Network Attack) luodaan vaikutuksia kybertoimintaympäristössä, jotka ilmenevät loogisella tai fyysisellä kerroksella. Tietoverkkohyökkäyksiä voidaan toteuttaa hyökkäyksellisessä kyberoperaatiossa tai puolustuksellisen kyberoperaation vastatoimina. Hyökkäyksellä kiistetään kohteen pääsy omiin järjestelmiinsä kokonaan tai tietyksi ajaksi, häiritään kohteen järjestelmiä tai tuhotaan kohde. Hyökkäyksellä voidaan myös manipuloida kohdetta tai vääristää sen sisältämä tietoa käyttäjän huomaamatta. Tällöin vaikutukset saattavat ilmetä ensin jossain muussa yhteydessä, kuin suoraan kohteessa. (US Joint Chiefs of Staff, 2018)

Kuten minkä tahansa operaation, myös kyberoperaation onnistunut toteuttaminen edellyttää tukitoimia. Näitä ovat tilanneymmärryksen muodostaminen ja tilannekuvan jatkuva ylläpitäminen sekä omasta että vastustajan toimintaympäristöstä ja toiminnasta, kuin myös taistelutilan muokkaaminen omille operaatioille suotuisaksi. (Laari ym., 2019)

Tilanneymmärrys muodostetaan eri lähteistä ja eri toiminnoilla. Tilannekuva koostuu omien verkkojen valvonnan ja tiedustelun tuottaman tiedon synteesinä. Kyberoperaatioita tukeva tiedustelu voidaan tuottaa millä tahansa tiedustelumenetelmällä ja -välineellä. Esimerkiksi kyberuhkatiedustelulla selvitetään potentiaalisia uhkatoimijoita ja hyökkäystapoja. Kyberuhkatiedustelun tavoitteena on kehittää omia valmiuksia varautua hyökkäyksiin. (Laari ym., 2019)

Tietoverkkotiedustelu on kokonaisuus, jossa selvitetään potentiaalisia uhkia ja kybertoimintaympäristön riskejä, muutostrendejä ja mahdollisuuksia omalle toiminnalle. Tietoverkkotiedustelu jakautuu tietojärjestelmätiedusteluun ja tietoliikennetiedusteluun. Tietoverkkotiedustelun tuottamaa tilanneymmärrystä voidaan täydentää muilla sotilastiedustelun keinoilla, kuten avointen lähteiden tiedustelulla (OSINT), henkilötiedustelulla (HUMINT), geotiedustelulla (GEOINT) tai signaalitiedustelulla (SIGINT), jonka yksi osa on yllä kuvattu tietoverkkotiedustelu. (Laari ym., 2019)

Taistelutilan muokkaaminen kohdistuu sekä omaan että vastustajan kybertoimintaympäristöön. Omien järjestelmien muokkaaminen vahvistaa kyberturvallisuutta. Keinoja tähän ovat esimerkiksi järjestelmäkovennukset tai vastustajan harhauttaminen omaan verkkoon luotavilla ansoilla (kuten hunajapurkki, Honey Pot). Vastustajan järjestelmien muokkaaminen luo edellytyksiä hyökkäykselliselle toiminnalle mahdollistamalla järjestelmiin pääsy tai niiden hallitseminen. Keinoja ovat esimerkiksi takaporttien tai piilohaittaohjelmien luominen vastustajan järjestelmiin. (Laari ym., 2019)

Dmitri Alperovitch (2011) jakaa kyberhyökkäykset kolmeen kategoriaan perustuen CIA-malliin (C= Confidentiality, I= Integrity, A= Availability). Tiedon luotettavuuteen kohdistuvat kyberhyökkäykset ovat vakoilua. Suuri osa kyberhyökkäyksistä tähtää tiedonhankintaan. On kansainvälisesti tunnustettu seikka, että valtiot harjoittavat tiedonhankintaa toisistaan riippumatta siitä, onko kohde kumppani, liittolainen tai vastustaja. Kyberhyökkäys

vakoilutarkoituksessa ei myöskään suurella todennäköisyydellä aiheuta kuin vastareaktion diplomaattisin keinoin. Tässä mielessä pelotevaikutusta ei ole tai se on hankalaa rakentaa. (Alperovitch, 2011)

Tiedon yhteneväisyyteen kohdistuvilla kyberhyökkäyksillä vastustaja yrittää hankkia taktista tai strategista etua sabotoimalla informaatiosysteemejä. Tämän tyyppiseen hyökkäykseen sisältyy esimerkiksi informaation muokkaaminen kohdejärjestelmässä, joka vaikuttaa tilannetietoisuuteen tai järjestelmän toimintaan. Kohteena voivat olla sekä sotilas- että siviilijärjestelmät. Tällaiset kyberhyökkäykset ovat suuri uhka etenkin kehittyneissä informaatioyhteiskunnissa, joissa riippuvuus verkottuneista digitaalisista järjestelmistä on suuri. (Alperovitch, 2011)

Tiedon saatavuuteen kohdistuvien hyökkäyksien päämääränä on estää kohteen pääsy tietoon joko sulkemalla järjestelmä tai tuhoamalla tietoa. Lyhytaikaisilla hyökkäyksillä voidaan vaikuttaa tiedon saantiin vaikuttaen tilannetietoisuuteen ja tiedustelutiedon keräämiseen. Pitkäaikaisilla hyökkäyksillä voidaan aiheuttaa mittaviakin vahinkoja yhteiskunnan toiminnalle, mikäli ne kohdistuvat esimerkiksi sähkö- tai rahajärjestelmiin. Tämän vuoksi tiedon saatavuuteen kohdistuvat hyökkäykset voivat aiheuttaa valtiolle suuren uhkan. (Alperovitch, 2011)

Samantapaista lähestymistapaa esittää Timothy McKenzie (2017). McKenzie jakaa hyökkäykselliset kyberoperaatiot tyypin, näkyvyyden ja vaikuttavuuden mukaan. Kaikista vahingollisimpia ja helpoimmin havaittavia ovat varsinaiset kyberhyökkäykset, jotka tähtäävät kohteen fyysiseen vaurioittamiseen tai ihmisten terveyden uhkaamiseen. Tällaisiin kyberhyökkäyksiin voi sisältyä myös kohteen käytön estäminen tai datan muuntaminen vaurioittamalla kohdetta. Lievempi kyberhyökkäysten muoto on kyberhäirintä, joka tähtää kohteen toiminnan tai informaation saatavuuden hankaloittamiseen ilman kohteen fyysistä vaurioittamista. Keinoja tällaiseen voi olla esimeriksi pienimuotoiset palvelunestohyökkäykset tai datan muuntaminen ilman fyysisten vahinkojen aiheuttamista. Vaikutukseltaan lievimmät, mutta samalla vaikeimmin havaittavat operaatiot tähtäävät tiedon ja pääsyn hankintaan liittyen kohdejärjestelmään. Keinoja tässä operaatiotyypissä ovat esimerkiksi kohteen kartoittaminen sekä haitallisten ohjelmistojen tai koodien asentaminen. (McKenzie, 2017)

2.3.2 Kyberoperaatioiden vaikutukset

Kyberoperaatioiden vaikutukset voidaan jakaa hyökkäyksellisiin, puolustuksellisiin, toimintaa tukeviin ja tietoa tuottaviin vaikutuksiin. Hyökkäykselliset vaikutukset kohdistuvat omien verkkojen ulkopuolelle ja niillä pyritäänkin muokkaamaan vastustajan kybertoimintaympäristöä ja mahdollisuuksia toimia siinä tai sen kautta. Hyökkäykselliset vaikutukset voivat olla pysyviä tai väliaikaisia. Puolustukselliset vaikutukset tähtäävät kyberuhkien ennaltaehkäisyyn ja niiden vaikutusten vähentämiseen omissa verkoissa. Toimintaa tukeva vaikutukset liittyvät kybertoimintaympäristössä sijaitsevien verkkojen ja järjestelmien hallintaan. Se tähtää kyberturvallisuuden parantamiseen systemaattisella

suunnittelulla ja johtamisella. Tietoa tuottavat vaikutukset aikaansaadaan tilannetietoisuudella ja tiedustelulla. Tiedon tuottamisella tuetaan kolmea edellä mainittua toimintaa. (UK Ministry of Defence, 2022)

Oman kybertoimintaympäristön suojaamiseen suunnitellut toimet voivat olla jatkuvia, jolloin ne eivät kohdistu mihinkään tiettyyn uhkaan. Tällaisten toimien päätarkoitus on kehittää oman kybertoimintaympäristön turvallisuutta ja toipumiskykyä verkkojen aktiivisen ylläpidon, testaamisen sekä kyberturvallisuuden kehittämisen keinoin. (US Joint Chiefs of Staff, 2018) Kaikki tällainen toiminta tähtää resilienssin rakentamiseen, joten niiden vaikutukset ovat puhtaasti puolustukselliset. Kyberresilienssillä tarkoitetaan järjestelmän kykyä kestää ja toipua kyberhyökkäyksestä ja säilyttää toimintojen ja palveluiden käytettävyys hyökkäyksen aikana (UK Ministry of Defence, 2022).

Puolustukselliset kyberoperaatiot kohdistuvat johonkin tunnistettuun uhkaan. Uhka voi olla jo toteutunut kyberhyökkäys tai ennakkovaroitus tulevasta kyberhyökkäyksestä. Aktiivisilla puolustustoimilla muokataan omaa verkkoa esimerkiksi uudelleenreititysten, palveluiden palauttamisen tai jonkin verkon osan eristämisen kautta. Myös aktiivinen uhkanmetsästys tai uhkan lyöminen pois omista verkoista on mahdollista. (US Joint Chiefs of Staff, 2018) Puolustukselliset toimet tähtäävät omien verkkojen suojelemiseen ja niiden vaikutuksista suurin osa kohdistuu omiin järjestelmiin, mutta osa voi sisältää myös hyökkäyksellisiä toimia.

Kyberhyökkäyksellä voidaan aikaansaada erityyppisiä vaikutuksia kohteessa. Tunnuksenomaista näille on, että ne hyvin usein huomataan varsin pian käyttäjän toimesta palvelun toiminnan häiriintyessä tai estyessä kokonaan. Hyökkäys voi tähdätä kohteen käytön estämiseen tai sen toiminnan manipulointiin. Estämisellä kielletään kohteeseen pääsy, sen käyttö tai saatavuus tietyn ajanjakson ajan. Tämä voi tapahtua myös jonkin tietyn käyttöasteen mukaan. Kohteen tuhoaminen tarkoittaa, että kohde ei ole ollenkaan käytössä, mutta sekin voi rajoittua johonkin tiettyyn ajanjaksoon ja kohde palautua käyttöön, kun kohdeorganisaatio on toteuttanut tarvittavat toipumisen toimenpiteet. Kohteen manipuloinnilla muutetaan kohdejärjestelmässä sijaitsevaa informaatiota tai kohdejärjestelmää itsessään. Kohteen manipulointi ei välttämättä paljastu heti kohdeorganisaatiolle. (US Joint Chiefs of Staff, 2018)

Kyberhyökkäyksen vaikutukset saattavat ilmetä odottamattomin tavoin ja levitä kohdeverkon ulkopuolelle. Vaikutukset voivat kertautua, jolloin ne leviävät odottamattomasti kohdejärjestelmän yhteydessä oleviin rinnakkaisiin tai ylemmän tason järjestelmiin. Vaikutukset voivat myös voimistua, kun erilaiset vaikutukset reagoivat toisiinsa ja synnyttävät tahattomia tai ennustamattomia vaikutuksia. Rinnakkaisia vaikutuksia ilmenee kohteissa, joita ei ollut suunniteltu hyökkäyksen kohteiksi. (US Joint Chiefs of Staff, 2018)

Kybertoimintaympäristöön kohdistuvan vihamielisen toiminnan kohteena voi olla mikä tahansa fyysinen tai ei-fyysinen elementti. Kohteet voidaan jakaa taktisen, operatiivisen tai strategisen tason kohteisiin. Taktisen tason kohde on jokin sellainen elementti, jota hallitsemalla tai johon vaikuttamalla saadaan taktista hyötyä omaan operaatioon liittyen. Tällainen elementti voi olla esimerkiksi

sellainen verkon osa, joka vaikuttaa paikallisen tason kommunikointiin tietoverkossa. Operatiivisen tason kohteen avulla voidaan vaikuttaa johonkin tiettyyn operaatioon tai yhteisoperaatioon. Tällainen kohde voi liittyä esimerkiksi sähkönjakeluun tai suljetun verkon tietoturvaohjelmistoon. Strategisen tason kohde on jokin kokonainen systeemi, johon vaikuttamalla vahingoitetaan kohteen toimintaa laajemmassa mittakaavassa. Tällainen kohde voi olla esimerkiksi valtion palvelinkeskus tai mobiiliverkon ohjausjärjestelmä. Eri tasojen välinen jako ei ole selkeä. Esimerkiksi vaikuttamalla taktisen tason kohteeseen voidaan saada aikaan vaikutuksia operatiivisella ja strategisella tasolla. (Conti, Cross, Nowatkowski & Raymond, 2014) Taulukossa 1 esitetään taktisen, operatiivisen ja strategisen tason kohteita. Taulukko on vapaasti suomennettu alkuperäisestä, englanninkielisestä taulukosta.

TAULUKKO 1 Esimerkkejä kyberhyökkäyksistä taktisella, operatiivisella ja strategisella tasolla (Conti ym., 2014)

Toiminnan taso / Kybertoimintaympäristön kerros	**Taktinen**	**Operatiivinen**	**Strateginen**
Fyysinen	Yksittäisen taistelijan USB-laite, älypuhelin tai tabletti	Alueellinen valokuitukaapeliverkko	Puolustusvoimien palvelinkeskus
Looginen	Komentopaikan tai esikunnan tietokoneiden ohjelmistot	Ilmapuolustuksen tilannekuvasovellus	Ydinaseen laukaisujärjestelmän hallintaohjelma
Käyttäjä	Yksittäisen joukon tilannekuvasovelluksen admin-tili	Puolustushaara komentajan tunnukset operatiiviseen järjestelmään	Presidentin tai valtionhallinnon avaintoimijoiden sähköpostitilit

Kybertoimintaympäristöön kohdistuvalla vaikuttamisella pyritään joko hankkimaan tietoa kohdejärjestelmistä tai niiden kautta tai aiheuttamaan haittaa kohdejärjestelmän toiminnalle häiritsemällä tai estämällä kohdejärjestelmän käyttöä tai tuhoamalla tietoa järjestelmän sisällä. Kybertoimintaympäristön kautta voidaan toteuttaa myös informaatio-operaatioita esimerkiksi kaappaamalla jokin tietty sivusto ja levittämällä tietoa sen kautta. Häiriöt kybertoimintaympäristössä saattavat palvella vastustajan psykologisia operaatioita, kun luottamus omiin järjestelmiin heikkenee. (Multinational Capability Development Campaign, 2014)

Kyberhyökkäysten keinovalikoima on laaja. Yksi tapa ryhmitellä keinovalikoimaa on jakaa se neljään kategoriaan: sosiaalinen hakkerointi, haittaohjelmat, kohteeseen tunkeutuminen ja kohteen elinkaareen vaikuttaminen. Sosiaalinen hakkerointi tarkoittaa yksilön hyödyntämistä jonkin sellaisen toiminnon suorittamiseen, jolla mahdollistetaan kyberhyökkäyksen toteuttaminen joko suoraan tai paljastamalla informaatiota kohteesta tai toimintaympäristöstä. Sosiaalisen hakkeroinnin keinoja ovat esimerkiksi sosiaalisen median hyödyntäminen tietojen kalasteluun tai käyttäjän houkutteleminen klikkaamaan linkkejä, jotka

johtavat haittaohjelman asentumiseen. Haittaohjelmat ovat tietokoneen, älylaitteen tai verkon vahingoittamiseen, hyödyntämiseen tai tunkeutumisen mahdollistamiseen tarkoitettuja ohjelmistoja. Niitä voidaan levittää tietokoneiden lisäksi mihin tahansa verkkoon liitettyyn älylaitteeseen, kuten älypuhelimiin ja tabletteihin. Kohteeseen tunkeutuminen on edellytys kyberhyökkäyksen toteuttamiselle ja se voidaan toteuttaa kolmella tavalla. Fyysinen tunkeutuminen tarkoittaa suoran yhteyden saamista kohdelaitteeseen tai -verkkoon. Haittaohjelma asennetaan esimerkiksi USB -laitteen avulla. Lähiyhteyden avulla tehtävä tunkeutuminen tarkoittaa toimenpiteitä, joilla päästään kohteeseen käsiksi jonkin alueella olevan välillisen yhteyden kautta. Tällainen voi olla esimerkiksi hyödyntämällä WIFI -yhteyksiä tai sosiaalisen hakkeroinnin avulla, jolloin kohteen lähellä työskenteleviä henkilöitä houkutellaan asentamaan esimerkiksi USB -laite kohteeseen. Etäyhteyden kautta suoritettava tunkeutuminen tapahtuu fyysisen ja virtuaalisen välimatkan päästä kohteesta ja kohdejärjestelmän verkon ulkopuolelta. Kohteen elinkaareen vaikuttamista voi tapahtua uuden laitteen toimittamisen tai vanhan laitteen huollon yhteydessä, jolloin laitteeseen asennetaan vahingollisia komponentteja. Nämä voivat vaikuttaa laitteen käyttö- ja tietoturvallisuuteen sekä toimintaan. (UK Ministry of Defence, 2016)

Paul Ducheine ja Jelle van Haaster (2014) käsittelevät kyberoperaatioilla aikaansaatavia vaikutuksia fyysisen ja ei-fyysisen kybertoimintaympäristön ulottuvuuden kautta. Kyberoperaatioilla voidaan vaikuttaa vastustajan johtamiskykyyn, moraaliin ja toiminnan edellytyksiin sekä neutraaleihin osapuoliin ja kumppaneihin hankkimalla näiltä tukea omalle operaatiolle. Näin ollen kyberoperaatioilla joko heikennetään vastustajan toimintaedellytyksiä tai parannetaan omia. Kyberoperaatioiden vaikutukset kohdistuvat kybertoimintaympäristön elementteihin ja virtuaalisiin identiteetteihin, mutta niillä voi olla seurannaisvaikutuksia myös fyysisiin kohteisiin, ihmisiin ja psyykeen. (Ducheine & van Haaster, 2014)

Tukevia operaatioita voidaan kohdistaa kumppanien ja neutraalien toimijoiden fyysiseen infrastruktuuriin tai kybertoimintaympäristön elementteihin ja identiteetteihin. Tukemalla näiden fyysisen infrastruktuurin kehittämistä ja valvontaa sekä tarjoamalla käyttöön esimerkiksi haittaohjelmien torjuntaohjelmistoja, saatetaan parantaa myös oman kybertoimintaympäristön turvallisuutta muun muassa tilannetietoisuuden laajentamisella ja yhteistyön vahventamisella. Tällä tavoin voidaan myös saavuttaa parempi jalansija kumppanien tai neutraalien kybertoimintaympäristössä. Kyberidentiteettejä, kuten sosiaalisen median tilejä, voidaan käyttää apuna informaatiovaikuttamisessa, jotta neutraalien osapuolten mielipide saadaan käännettyä omaa toimintaa tukevaksi ja samalla voidaan vahvistaa myös kumppanien mielipidettä oman toiminnan oikeutusta tukevaksi. (Ducheine & van Haaster, 2014)

Vastustajaan voidaan vaikuttaa vastaavasti fyysisessä ja ei-fyysisessä kybertoimintaympäristön ulottuvuudessa. Fyysinen pääsy kohteen infrastruktuuriin mahdollistaa monenlaisen toiminnan, koska vastassa ei ole palomuureja ja verkoissa sijaitseviin ohjelmiin ja palveluihin pääsee suoraan käsiksi. Tällöin mahdollistuu verkossa kulkevan liikenteen manipulointi. Kyberidentiteettejä

voidaan käyttää heikentämään vastustajan uskottavuutta tai kohdistaa psykologista vaikuttamista suoraan vastustajan avainhenkilöihin. Vastustajan avainhenkilöstön kyberidentiteetit voidaan puolestaan estää tai kaapata. Kybertoimintaympäristön välityksellä voidaan myös vaikuttaa vastustajan tilannetietoisuuteen. (Ducheine & van Haaster, 2014)

Johtopäätöksenä voidaan todeta, että vastustajan kybertoimintaympäristössä sijaitseviin kohteisiin voidaan vaikuttaa monella tapaa. Ensin vastustajan kybertoimintaympäristö on kartoitettava, jotta omille toimintaedellytyksille on olemassa tarpeeksi tiedustelutietoa. Vastustajan kriittisiin toimintoihin voidaan vaikuttaa ulkoisella hyökkäyksellä. Tällainen voi olla esimerkiksi palvelunestohyökkäys, jolla estetään jonkin palvelun toiminta. Mikäli pääsy vastustajan järjestelmiin on saavutettu, voidaan kerätä tietoa sekä hyödyntää järjestelmissä olevia haavoittuvuuksia esimerkiksi myöhemmin asennettaville haittaohjelmille. Edellä kuvatut keinot häiritä ja manipuloida vastustajan verkkojen ja palvelujen toimintaa voi aikaansaada tehokkaita vaikutuksia vastustajan toimintaan. Sen sijaan kohteen tuhoaminen voi olla kybertoimintaympäristössä hankalaa, koska usein on olemassa varajärjestelmiä tai -laitteita. Tuhoaminen aiheuttaa siis usein lähinnä väliaikaisia vaikutuksia, joista toivutaan, kun vioittunut laite korvataan.

Pelotteen näkökulmasta kyberhyökkäyksillä tuskin saadaan aikaan mittavia henkilövahinkoja tai fyysisten kohteiden tuhoutumista, mutta häiriöt sähköisissä järjestelmissä voivat yhteiskunnan elintärkeisiin toimintoihin kohdistuessaan vaikuttaa merkittävästi yhteiskunnan toimintaan ja turvallisuuteen. Tämän vuoksi valtion suojatessaan suvereniteettiaan kybertoimintaympäristössä, korostuu resilienssin merkitys. Myös kyky tunnistaa kyberhyökkäys ja eristää sen vaikutukset ovat merkittävässä roolissa. Pelotteen näkökulmasta resilienssiä lienee helpompi myös demonstroida, koska se ei liity yksinomaan kybersuorituskykyihin, vaan yhteiskunnan varautumiseen yleensä.

3 KYBEROPERAATIOT OSANA PELOTEVAIKUTUSTA

Tutkimukseen muodostettiin kolme pääteemaa jo tutkimuksen alussa tutkijan oman aiheentuntemuksen perusteella: pelote, kyberpelote ja kyberoperaatiot. Näiden teemojen ympärille muodostettiin tutkimuskysymykset ja suunnitelma kerättävästä aineistosta. Tutkimuksen edetessä oli havaittavissa näiden pääteemojen alle muodostuvia alateemoja, jotka auttoivat tutkijaa ymmärtämään syyseuraussuhteita ja taustoja, mutta jotka kuitenkaan eivät olleet relevantteja tutkimuskysymykseen vastaamisen näkökulmasta. Nämä alateemat kuitenkin dokumentoitiin tutkimusraporttiin, koska ne taustoittavat peloteteorioiden nykytilaa. Näitä teemoja olivat peloteteorioiden kehittymisen neljä aaltoa, jotka ovat raportoitu luvussa 2 ja teknologian kehityksen vaikutus pelotteen jäsentämiseen.

Muita mielenkiintoisia taustateemoja olivat 2000-luvun pelote- ja kyberpelotetutkimuksen trendit: mitä tutkitaan ja miksi. Peloteteorioissa oli havaittavissa suuntaus, jossa kyseenalaistetaan klassiset peloteteoriat, koska kylmän sodan aikakauden jälkeen kahden suurvallan välinen vastakkainasettelu on päättynyt ja kansainvälinen voimapolitiikka sekä uhkakuvat ovat muuttuneet moninaisemmiksi. Lisäksi valtiollisten toimijoiden rinnalle on astunut muita toimijoita, kuten terroristit, järjestäytynyt rikollisuus sekä vandalismin, nationalismin tai muiden syiden vuoksi toimivia tahoja.

Kyberpelotteen tutkimuksessa oli erotettavissa trendejä, joiden mukaan kyberpelote on mahdollista rakentaa klassisen peloteteorian lainalaisuuksia mukaillen. Toisaalta kirjallisuudesta ilmeni myös täysin päinvastaisia trendejä, joiden mukaan kybertoimintaympäristö poikkeaa ominaisuuksiltaan ja toiminnoiltaan niin paljon fyysisestä maailmasta, että klassisia peloteteorioita ei ole mahdollista soveltaa sellaisenaan kyberpelotteeseen. 2000-luvun alun akateeminen keskustelu keskittyy lähinnä edellä mainittuun väittelyyn ja myöhemmässä tutkimuksessa oli havaittavissa ehdotuksia kyberpelotteen rakentamisen eri keinoista joko itsenäisenä pelotteena tai osana kokonaisvaltaista pelotetta.

Tutkimuksessa käytettiin teemoittelua ja tyypittelyä, jotta kirjallisesta aineistosta löydettäisiin tekijöitä, joiden perusteella voitaisiin muodostaa vastaus

päätutkimuskysymykseen. Tutkimuksessa edettiin suurista kokonaisuuksista (teemat) pienempiin (tyypit). Tämän jälkeen yhdisteltiin toisiaan muistuttavia teemoja ja tyyppejä sekä järjestettiin tiedot kategorioihin, jotka esitellään tässä luvussa taulukkoina. Näin päättely eteni pienimmistä kokonaisuuksista takaisin suurempiin. Prosessia jatkettiin, kunnes toisiaan muistuttavia teemoja ja tyyppejä ei enää löytynyt ja aineisto oli järjestetty loogiseksi kokonaisuudeksi.

Ensin aineistosta etsittiin toistuvia teemoja. Nämä jaettiin edelleen alateemoihin ja tyyppeihin. Kyberoperaatioista löytyneitä teemoja ja tyyppejä verrattiin peloteteorioista muodostettuihin tyyppeihin. Tällää tavalla muodostettiin periaatteita kyberoperaatioiden käyttämisestä pelotteen luomiseen.

Seuraavissa alaluvuissa kerrotaan noudatellen tutkijan päättelyketjua, miten aineisto teemoiteltiin ja tyypiteltiin vaiheittain. Kaikki muodostetut kategoriat esitellään, vaikka osa niistä karsiutui pois lopullisesta mallista siksi, etteivät ne tuottaneet tietoa päätutkimuskysymykseen. Analyysin tulkinnan tukena esitetään myös jokaisen löydöksen yhteydessä ne lähteet, joista tieto on peräisin.

3.1 Pelotetutkimuksen teemoittelu ja tyypittely

Pelotetutkimuksesta oli löydettävissä useita alateemoja. Yksi tapa teemoitella pelotetta on jakaa se kielto- ja rankaisupelotteeseen. Kumpikin pelotetyyppi sisältää monia alateemoja, mutta nykyajan pelotetutkimuksessa on esitetty myös näiden kahden lisäksi muita pelotteen rakentamisen muotoja, jotka eivät tosin sulje pois rankaisu- ja kieltovaikutuksen ilmentymistä. Voidaankin todeta tämän jaottelun rankaisu- ja kieltopelotteen välillä perustavanlaatuinen (Mazarr, 2018). Näin ollen pelotetutkimuksen alateemoiksi muodostettiin kieltopelote ja rankaisupelote.

Toinen tapa jaotella pelotetta on määritellä pelotteen tekijät, eli ne elementit, joita ilman pelote ei toimi. Klassisen peloteteorian mukaan pelote koostuu kolmesta tekijästä: riittävä suorituskyky, uskottavuus ja onnistunut viestintä (Paul, 2009; Raitasalo & Sipilä, 2008; Morgan, 2003). Myöhemmissä tutkimuksissa on muodostettu myös muita tekijöitä, jotka ovat tässä tutkimuksessa huomioitu samanarvoisina alateemoina kuin kolme edellä mainittua. Will Goodmanin (2010) määritelmästä poimittiin kahdeksan pelotteen tekijää: intressi, pelotteen julkistaminen, kieltotoimet, rankaisutoimet, uskottavuus, vakuus, pelko ja riskihyötysuhteen laskeminen. Näistä kaikki tekijät eivät ole samanarvoisia tämän tutkimuksen teemoittelun mukaan, joten kielto- ja rankaisutoimet sijoitettiin ylemmän tason käsitteiksi.

Pelotetutkimuksissa on jaoteltu pelotetta myös sen mukaan, millaisia keinoja siihen sisältyy. Näitä on käsitelty osittain vastakkaisina pareina, kuten laaja ja kapea pelote, yleinen ja välitön pelote tai suora ja laajennettu pelote (Mazarr, 2018). Näitä alateemoja kuitenkin hyödynnettiin tarkastelemalla niitä elementtejä, joita kyseisiin pelotetyyppeihin sisältyy (taulukko 3).

Peloteteorioista koostettiin viisi päätyyppiä: pelotteen kulmakivet, tyypit, osatekijät, käyttötavat ja keinovalikoima. Näillä kuvataan pelotteen ominaisuuksia, joista jotkin ovat aina olemassa ja osa taas valittavissa. Kulmakivet, tyypit ja

osatekijät kuvataan taulukossa 2, käyttötavat taulukossa 3 ja keinovalikoima taulukossa 4.

Pelotteen kulmakivet ovat valtion suorituskyvyt ja niiden muodostama voima; uhka, jonka tämä voima muodostaa toiselle valtiolle ja uskottava viestintä, jolla kerrotaan omasta valmiudesta käyttää tätä voimaa uhkien torjuntaan ja aggressioista rankaisemiseen (Paul, 2009; Raitasalo & Sipilä, 2008; Morgan, 2003). Pelote rakennetaan useimmiten jotakin tunnistettua uhkatoimijaa vastaan (Mazarr & Goodby, 2011; Raitasalo & Sipilä, 2008; Morgan, 2003), vaikka pelote voidaankin rakentaa ilman tarkasti määriteltyä uhkatoimijaa (Sweijis & Zilincik, 2021; Mazarr, 2018). Uhkatoimija voi olla esimerkiksi toinen valtio, rikollisuus tai terrorismi (Mazarr, 2018). Tutkimuksen rajauksen mukaan tarkasteltiin vain toista valtiota uhkatoimijana, joten nämä uhkatekijöiden alatyypit jätettiin listaamatta. Uhkatoimijoita lukuun ottamatta kulmakivet ovat sellaisia tekijöitä, joiden on aina oltava olemassa, jotta pelote muodostuisi.

Pelotekirjallisuudessa on esitetty perustavanlaatuinen jako kielto- ja rankaisupelotteeseen (Mazarr, 2018; Raitasalo & Sipilä, 2008). Pelote pohjautuu aina joko uhkatoimijan toimien tyhjäksi tekemiseen ja rajoittamiseen tai rankaisutoimiin, jotka ovat reaktio hyökkäykselliseen toimintaan. Nämä kaksi tekijää kuvattiin pelotteen tyypeiksi.

Pelotteen osatekijöitä esitettiin kirjallisuudessa useita (Goodman, 2010; Paul, 2009; Raitasalo & Sipilä, 2008; Morgan, 2003). Osa näistä oli yhdisteltävissä saman nimikkeen alle, kuten esimerkiksi riskihyötysuhteen laskeminen ja rationaalisuus. Lopputuloksena muodostettiin kahdeksan pelotteen osatekijää, joiden pitää sisältyä pelotteeseen, jotta se toimisi halutulla tavalla. Moni osatekijä esiintyy myös pelotteen kulmakivissä ja niiden tulkinnassa. Pelotteen kulmakivet voidaankin ymmärtää yksinkertaisena mallina tai muistisääntönä niistä pelotteen tekijöistä, joiden on esiinnyttävä onnistuneessa pelotteessa. Pelotteen osatekijöissä nämä elementit puretaan pienemmiksi kokonaisuuksiksi.

TAULUKKO 2 Pelotteen tekijät

Tyyppi	Alatyyppi	Selite
Pelotteen kulmakivet	Suorituskyvyt	Valtion voima
	Uhka	Voiman käytön mahdollisuudesta muodostuva uhka
	Viestintä	Uskottava viestintä voiman olemassa olosta ja tahdosta käyttää sitä
	Uhkatoimijat	Näitä vastaan pelote rakennetaan
Pelotteen tyyppi	Kielto	Minimoidaan uhkatoimijan saama hyöty
	Rankaisu	Rankaistaan uhkatoimijaa
Pelotteen osatekijä	Viestintä	Miten oma pelote kommunikoidaan
	Suorituskyky	Poliittinen, sotilaallinen, yhteiskunnallinen suorituskyky
	Uskottavuus	Miten uhkatoimija tulkitsee peloteviestinnän
	Intressi	Omien intressien suojeleminen
	Vakuus	Julkisesti kommunikoitu tae siitä, että mitä uhkatoimija ei menetä/ hyötyy, jos pidättäytyy hyökkäämästä
	Pelko	Uhkatoimijassa herätetty pelko
	Rationaalisuus	Uhkatoimijan harkinta ja riskihyötysuhteen laskeminen hyökkäyksen kannattavuudesta
	Resilienssi	Oma kyky toipua hyökkäyksestä

Tyypittelyn perusteella muodostettiin myös sellaisia pelotteen tekijöitä (Mazarr, 2018), jotka ovat valinnaisia pelotetta muodostettaessa. Pelote voidaan jakaa alueellisesti tai ajallisesti tarkasteltuna sekä keinovalikoimaan perustuen (taulukko 3). Jaottelun mukaiset käyttötavat eivät sulje toisiaan pois, koska valtio voi samanaikaisesti viestiä pelotetta sekä omalla että liittolaistensa alueella, varautua sekä normaali- että poikkeusolojen uhkiin ja käyttää joko puhtaasti sotilaallisia suorituskykyjä tai monipuolista keinovalikoimaa riippuen arvioidusta uhkasta.

Analyysin aikana huomattiin, että kyberoperaatioiden näkökulmasta tämä jaottelu ei ole merkitsevä, koska kybersuorituskykyjä voidaan käyttää jokaisessa pelotteen muodostamisen tavassa. Tämän tutkimuksen fokus on kyberoperaatioiden tarkastelussa osana pelotevaikutusta ja tutkimuksessa ei oteta kantaa siihen, miten valtion tulee järjestää pelotteensa.

TAULUKKO 3 Pelotteen tyypittely käyttötavan mukaan

Tyyppi	**Alatyyppi**	**Alatyypin alatyyppi**	**Selite**
Käyttötapa	Alueellinen tarkastelu	Suora	Valtio torjuu hyökkäyksen omalla alueellaan
		Laajennettu	Hyökkäys liittolaista tai kumppania kohtaan aiheuttaa vastatoimia
	Keinovalikoiman tarkastelu	Laaja	Laaja keinovalikoima, mm. poliittiset, sotilaalliset ja taloudelliset keinot
		Kapea	Puhtaasti sotilaallinen voima
	Ajallinen tarkastelu	Yleinen	Jatkuvat ja systemaattiset toimet jo normaalioloissa
		Välitön	Jotain tiettyä uhkaa vastaan suunnitellut välittömät toimet, yleensä kriisioloissa

Toinen tyypittely, jossa esitetään valinnaisia tekijöitä pelotteen muodostamiseen, on keinovalikoima, johon kokonaisvaltainen pelote perustuu (Sweijis & Zilincik, 2021). Tämä ylätyyppi sisältää seitsemän alatyyppiä, joista valtio voi valita yhden tai useampia oman pelotestrategiansa mukaisesti (taulukko 4). Näistä tekijöistä voidaan käyttää samanaikaisesti niin montaa kuin on tarve, eivätkä ne sulje pois toisiaan.

Taloudelliset ja poliittiset keinot ovat sellaisia, joita valtiot käyttävät osana normaalia kansainvälistä politiikkaa, mutta joita voidaan käyttää myös pelotestrategian osana. Ne ovat vähemmän sotaisia, kuin perinteisellä asevoimalla tai ydinaseella uhkaaminen. (Sweijs, Zilincik, Bekkers & Meessen, 2021)

Konventionaalinen asevoima ja ydinase ovat klassisen peloteteorian mukaisia pelotekeinoja ja niiden voidaan katsoa sisältyvän olennaisina keinoina myös nykyajan pelotteeseen. Näiden käyttö kuitenkin rajoittuu sotilaalliseen konfliktiin, joten niillä uhkaaminen viittaakin sotatoimien alkamiseen, mikäli uhkatoimija toteuttaa aggressionsa. Näitä pehmeämpiä keinoja ovat ei-kineettisten sotilaallisten suorituskykyjen käyttö, kuten kybersuorituskyvyt, informaatiovaikuttaminen ja elektroninen sodankäynti.

TAULUKKO 4 Pelotteen keinovalikoima

Tyyppi	Alatyyppi	Selite
Keinovalikoima	Taloudelliset	Esim. sanktiot
	Poliittiset	Esim. poliittinen painostaminen
	Konventionaalinen asevoima	Pääosin kineettinen asevoima
	Ydinase	Vain ydinasevallat
	Kybersuorituskykyjen käyttö	Puolustukselliset ja hyökkäykselliset suorituskyvyt
	Informaatiovaikuttaminen ja suojautuminen	Puolustukselliset ja hyökkäykselliset suorituskyvyt
	Elektroninen sodankäynti	Puolustukselliset ja hyökkäykselliset suorituskyvyt

3.2 Kyberpelotetutkimuksen teemoittelu ja tyypittely

Lähdeaineistossa kyberpelotetta käsiteltiin joko hyökkäyksellisestä näkökulmasta (Taddeo, 2018b; Tor, 2017) tai puolustuksellisen ja hyökkäyksellisen näkökulman yhdistelmänä (Burton, 2018; Chen, 2017a; Nye, 2017; Bendiek & Metzger, 2015; Jasper, 2015). Yhtymäkohta rankaisu- ja kieltopelotteeseen oli selkeä, toisaalta myös kokonaisvaltaisen pelotteen (engl. Cross-Domain Deterrence) elementtejä esiintyi useassa tutkimuksessa (Burton, 2018; Chen, 2018a; Tor, 2017; Bendiek & Metzger, 2015). Kyberoperaatioiden näkökulmasta näkökulmat olivat jaettavissa rankaisu- ja kieltovaikutukseen, jotka jakautuivat ensimmäisen osalta kyberhyökkäyskykyyn sekä jälkimmäisen osalta aktiiviseen kyberpuolustukseen ja kyberresilienssiin (taulukko 5). Osassa lähdeaineistosta resilienssin käsitettiin olevan erillinen kokonaisuutensa (Burton, 2018; Chen, 2017a; Bendiek & Metzger, 2015), kun taas jotkut tutkijat sisällyttivät sen kyberpuolustuksen kokonaisuuteen (Nye, 2017; Tor, 2017; Jasper, 2015). Taulukossa 5 kyberpuolustus on luonteeltaan aktiivista ja ennakoivaa, kun taas resilienssin keinot tähtäävät kyberturvallisuuden ja oman kyberinfrastruktuurin häiriönsietokyvyn kasvattamiseen.

Kyberhyökkäyskyky luo valtiolle mahdollisuuden ennakointiin ja yllätykseen (Chen, 2017a). Peloteviestinnällä kerrotaan potentiaalisille uhkatoimijoille niistä rajoista, jotka ylittämällä on odotettavissa vastareaktio. Onnistunut peloteviestintä edellyttää uhkatoimijan tuntemista, jotta viesti osataan muotoilla yksiselitteisesti. Viestinnän onnistumista on myös seurattava niin kansallisella kuin kansainväliselläkin foorumilla. (Taddeo, 2018a; Tor, 2017; Nye, 2017)

Tiedustelun avulla tunnistetaan hyökkääjä ja se järjestelmä, josta hyökkäys on toteutettu. Onnistuessaan tiedustelu tuottaa myös perusteet hyökkääjän tunnistamiselle ja tuomitsemiselle, jotta vastatoimet ovat laillisesti perusteltuja niin kansallisesti kuin kansainvälisilläkin foorumeilla. (Taddeo, 2018b; Chen, 2017a; Nye, 2017)

Pelotekeinovalikoimasta kyberhyökkäys on ainoa vastatoimi, joka voidaan toteuttaa välittömästi, mikäli edellä mainitut perusteet ovat luoneet siihen mahdollisuuden (Chen, 2018a). Yksittäisten hyökkäysten sijaan kybervoimaa demonstroidaan jatkuvilla vastatoimilla ja pieniä voittoja hankkimalla (Tor, 2017).

Kyberhyökkäyskyvyn lisäksi tarvitaan kyky puolustautua, koska mikään järjestelmä tai verkko ei ole täysin läpäisemätön kyberhyökkäyksen näkökulmasta. Kyberpuolustuskykyyn kuuluu aktiivisia keinoja, joiden avulla kyetään havaitsemaan uhkat verkonvalvonnalla sekä luodaan kyky analysoida uhkien vaikutusta, hyökkäystapaa ja lähdettä. Kun nämä tekijät tunnetaan, on mahdollista vähentää kyberhyökkäyksen vaikutusta ja eristää haitallinen toiminto, jotta se ei leviä laajemmalle verkkoon tai aiheuta suurempia tuhoja. Uhkanmetsästyksellä voidaan ennakoivasti seuloa omia verkkoja ja etsiä niistä sellaisia poikkeavuuksia, jotka voivat indikoida kyberhyökkäystä. (Chen, 2017a; Nye, 2017; Jasper, 2015))

Kieltopelotteeseen kuuluu olennaisena osana kyky kiistää uhkatoimijan aggression vaikutukset oman valtion suvereniteettiin ja turvallisuuteen. Kybertoimintaympäristön tarjotessa lukuisia hyökkäysvektoreita verkkoihin ja järjestelmiin, nousee resilienssi tärkeäksi tekijäksi pelotevaikutusten luomisessa. Kyberresilienssi on kykyä sietää hyökkäyksen vaikutukset, säilyttää palvelut hyökkäyksen ajan ja palauttaa järjestelmät hyökkäystä edeltävälle tasolle sen päätyttyä tai kun se on saatu torjuttua. Pelotteen näkökulmasta tällainen kyky voi vähentää uhkatoimijan hyökkäyshalukkuutta, mikäli se kokee hyökkäykseen kuluvan liikaa resursseja. (Nye, 2017; Jasper, 2015; Bendiek & Metzger, 2015)

TAULUKKO 5 Kyberpelotteen tekijät

Tyyppi	Alatyyppi	Alatyypin alatyyppi	Selite
Rankaisuvaikutus	Kyberhyökkäyskyky	Viestintä	Viestintä rajoista, joita ei voida ylittää. Viestinnän onnistumisen seuraaminen
		Vastatoimet	Toistuvat vastatoimet, pienet ja jatkuvat voitot.
		Tiedustelu	Hyökkääjän tunnistaminen ja hyökkääjän järjestelmän tiedustelu
Kieltovaikutus	Kyberpuolustuskyky	Valvonta	Kyky havaita uhkat
		Analyysikyky	Kyky analysoida uhkien vaikutus, hyökkäystapa ja lähde
		Suojauskyky	Hyökkäyksen vaikutusten vähentäminen ja eristäminen
		Uhkanmetsästys	Aktiivinen uhkanmetsästys omissa verkoissa
	Kyberresilienssi		Häiriönsietokyvyn ja turvallisuuden parantaminen omissa verkoissa

Tutkitusta aineistosta löydettiin myös kyberpelotetta tukevia tekijöitä, joista osa on uniikkeja fyysiseen maailmaan verrattuna. Tekoälyn ja teknologisten ratkaisujen käyttö sekä kyberpuolustuksessa että -hyökkäyksessä nousi esiin yhtenä tällaisena tekijänä (Burton, 2018; Taddeo, 2018b; Chen, 2017a; Nye, 2017; Tor, 2017). Tekoäly voi mahdollistaa esimerkiksi hyökkääjän tunnistamisen nopeammin ja varmemmin sekä vastahyökkäyksen automaattisen toteutuksen (Taddeo, 2018b, Chen, 2017a). Puolustuksen näkökulmasta tekoälyä voidaan käyttää esimerkiksi suurten datamassojen analysoinnin apuna, jolloin valvonta- ja havaitsemiskyky tehostuu (Chen, 2017a).

Kyberoperaatioiden käyttöä pelotekeinoina tukevat kansalliset ja kansainväliset yhteisesti sovitut pelissäännöt. Näitä ovat muun muassa säädökset ja normit, joilla määritellään esimerkiksi tilanteet, joissa on hyväksyttävää käyttää hyökkäyksellisiä suorituskykyjä oman valtion suvereniteetin suojaamiseen kybertoimintaympäristössä. Valtion laki märittelee ja ohjaa kybersuorituskykyjen käyttöä erilaisissa tilanteissa ja sen pitää mahdollistaa tämä myös ennaltaehkäisevinä toimina, jotka saattavat edellyttää hyökkäyksellisten kybersuorituskykyjen käyttöä. (Burton, 2018; Bendiek & Metzger, 2015; Jasper, 2015) Hyökkäys suojelluksi luokiteltuun kohteeseen voi aiheuttaa myös mainehaittaa hyökkääjälle, mikäli kansainvälinen yhteisö on samaa mieltä hyökkäyksen laittomuudesta. (Burton, 2018; Nye, 2017)

Kansallinen kyberpelotestrategia on yksi niistä valtion viestinnän keinoista, joilla kommunikoidaan valtion tahto suojata omaa kybertoimintaympäristöään

hyökkäyksiltä. Tähän voidaan sisällyttää myös lain ja sopimusten mahdollistama toiminta. (Bendiek & Metzger, 2015)

Muita pelotekeinoja voidaan käyttää kybertoimintaympäristön suojaamiseen ja hyökkäysten ennaltaehkäisyyn kokonaisvaltaisen pelotestrategian hengessä. Tämä edellyttää, että ilmaistaan selkeästi ne rajat, joita ei sovi ylittää (Taddeo, 2018a; Tor, 2017; Nye, 2017).

TAULUKKO 6 Kyberpelotetta tukevat tekijät

Tyyppi	**Alatyyppi**	**Selite**
Tukevat tekijät	Muut pelotekeinot	Kineettinen asevoima, politiikka ja diplomatia, taloudelliset pakotteet, laki
	Laki	Attribuution tukena ja vastatoimien oikeuttajana
	Kansalliset ja kansainväliset säädökset ja normit	Attribuution tukena ja vastatoimien oikeuttajana, mainehaitan aiheuttaminen hyökkääjälle
	Kansallinen kyberpelotestrategia	Viestittävä asiakokonaisuus
	Tekoäly ja teknologiset ratkaisut	Puolustuksen tukena
		Hyökkäyksen tukena

3.3 Kyberoperaatioiden teemoittelu ja tyypittely

Tarkasteltaessa kyberoperaatioita, on ensin muodostettava ymmärrys siitä toimintaympäristöstä, jossa ja jonka välityksellä operaatioita on mahdollista toteuttaa. Tässä tutkimuksessa käytettiin kolmeportaista mallia, joka on käytössä Puolustusvoimissa (Laari ym., 2019). Malli jakaa kybertoimintaympäristön loogiseen, fyysiseen ja käyttäjäkerrokseen, joista ensimmäiseen sisältyvät sähköiset tiedonsiirtoon tarkoitetut toiminnot ja ohjelmistot, toiseen fyysiset laitteet ja kolmanteen ihmiset ja heidän käyttämänsä käyttäjätilit ja -tunnukset. Kyberoperaatiolla voi olla vaikutus näistä yhteen tai useampaan kerrallaan, joten kerrosten väliset yhteydet on huomioitava kyberoperaatioita suunniteltaessa. Taulukossa 7 esitellään kybertoimintaympäristön kerrosten ominaisuudet.

TAULUKKO 7 Kybertoimintaympäristön kerrokset

Tyyppi	Alatyyppi	Selite
Kybertoimintaympäristö	Looginen	Sähköiset tiedonsiirtoon tarkoitetut toiminnot ja ohjelmistot
	Fyysinen	Fyysiset laitteet, kuten palvelimet ja päätelaitteet
	Käyttäjä	Ihmiset, ihmisten sähköiset identiteetit, yhteiskäyttöiset sähköiset tilit

Kyberoperaatioita voidaan toteuttaa sotilaallisesta näkökulmasta kolmella tasolla: strategisella, operatiivisella ja taktisella tasolla. Strategisen tason operaatiot suunnitellaan ja toteutetaan ja johdetaan valtiollisten tavoitteiden mukaan ja se sisältää muun muassa poliittisen ja viranomaisen välisen yhteistyön. Operatiivisen tason voidaan käsittä olevan sotilaallisen päätöksenteon ylimmän tason johtamat operaatiot. Näihin kuuluvat esimerkiksi yhteisoperaatiot, jotka sisältävät joukkoja kaikissa sotilaallisissa toimintaympäristöissä (maa, meri, ilma, avaruus, kyber, informaatio). Taktisen tason operaatiot ovat yksittäisten joukkojen suorittamia operaatioita, esimerkiksi puolustushaaran suorittama uhkanmetsästys omissa verkoissaan tai siihen kohdistuva JOJÄ-operaatio. (UK Ministry of Defence, 2022; US Joint Chiefs of Staff, (2018; Conti, ym., 2014) On kuitenkin huomattava, että tällainen jako ei ole aina tarkoituksenmukainen, koska taktisenkin tason operaatiolla voi olla strategisen tason vaikutuksia. Tällainen tilanne voi syntyä esimerkiksi kyberhyökkäyksen vaikutuksen levitessä kohdejärjestelmää laajemmalle.

Kyberoperaatioiden kohde voidaan jakaa usealla tavalla, tarkasteltavasta näkökulmasta riippuen. Jako voidaan tehdä edellisessä kappaleessa mainittujen toiminnan tasojen mukaan tai kybertoimintaympäristön kolmen kerroksen perusteella. Strategisen toiminnan tason näkökulmasta jako voidaan tehdä edelleen kolmiportaisesti, jolloin eritellään omat, uhkatoimijan ja neutraalit verkot (Ducheine & van Haaster, 2014).

Kyberoperaatioiden vaikutusten kohdistuessa ennen kaikkea tietoon, on mahdollista tarkastella vaikutuksia myös CIA-mallin mukaan tiedon eheyden, käytettävyyden ja luotettavuuden näkökulmasta. (Alperovitch, 2011)

Taulukossa 8 esitellään kyberoperaatioiden toiminnan tasot ja kohteet.

TAULUKKO 8 Kyberoperaatioiden toiminnan tasot ja kohteet

Tyyppi	**Alatyyppi**	**Selite**
Kyberoperaatioiden toiminnan taso	Strateginen	Valtiollinen taso, ml. sotilaallinen, poliittinen, viranomaisyhteistyö
	Operatiivinen	Sotilaallinen taso, ylempi päätöksenteko
	Taktinen	Sotilaallinen taso, yksittäiset joukot
Kyberoperaatioiden kohde	Jako toiminnan tason mukaan	Strateginen, operatiivinen, taktinen
	Jako kybertoimintaympäristön kerrosten mukaan	Fyysinen, looginen, käyttäjä
	Jako CIA-mallin mukaan	Tiedon eheys, käytettävyys ja luotettavuus
	Jako toimijoiden mukaan	Omat verkot, uhkatoimijan verkot, neutraalit verkot

Tässä tutkimuksessa kyberoperaatiot jaoteltiin hyökkäyksellisiin, puolustuksellisiin ja JOJÄ-operaatioihin Puolustusvoimien käyttämän jaottelun mukaan (Laari, ym., 2019). Taulukossa 9 esitellyt jaottelu ja operaatioiden toiminnot, mukaan lukien tuki, on kerrottu tarkemmin luvuissa 2.3.1 ja 2.3.2.

TAULUKKO 9 Kyberoperaatioiden tyypit ja tuki

Tyyppi	**Alatyyppi**	**Alatyypin alatyyppi**	**Selite**
Kyberoperaation tyyppi	Hyökkäyksellinen	Tietojärjestelmätiedustelu	Tiedon ja jalansijan hankkiminen kohdejärjestelmästä
		Hyökkäykselliset toimet	Kohdejärjestelmän häirintä, käytön estäminen, toimintojen muokkaus
	Puolustuksellinen	Vastatoimet	Uhkatoimijan lyöminen omista verkoista tai pääsyn estäminen niihin
		Suojatoimet	Valvonta, uhkanmetsästys, harhautus
	Resilienssi	JOJÄ-operaatio	Resilienssin rakentaminen

Tyyppi	**Alatyyppi**	**Selite**
Kyberoperaatioiden tuki	Tiedonhankinta (ISR)	Tilannekuva, tilanneymmärrys
	JOJÄ-operaatio	Kyberturvallisuus jatkuvana prosessina

Kyberoperaatioiden vaikutukset voidaan jakaa karkeasti omiin verkkoihin ja omaan toimintaan kohdistuvaksi, eli puolustukselliseksi ja uhkatoimijan

verkkoihin kohdistuvaksi, eli hyökkäykselliseksi. (Laari ym., 2019; US Joint Chief of Staff, 2018; Ducheine & van Haaster, 2014) Jakoa ei tule käsittää kyberoperaatioiden tyyppejä vastaavaksi, koska puolustuksellisiin kyberoperaatioihin voi sisältyä hyökkäyksellisiä elementtejä esimerkiksi uhkanmetsästyksen tai vastatoimien muodossa ja hyökkäyksellisiin kyberoperaatioihin sisältyy väistämättä myös oman toiminnan suojaamiseen liittyviä toimenpiteitä.

Hyökkäykselliset vaikutukset liittyvät tiedon, järjestelmien ja palveluiden käytettävyyden tason laskuun. (Lehto & Limnell, 2017) Usein kyberhyökkäykset mielletään loogisessa kerroksessa tapahtuviksi toimiksi, jotka vaikuttavat tiedon saatavuuteen, käytettävyyteen ja luotettavuuteen ja ilmenevät esimerkiksi järjestelmän käytön häiriintymisenä tai tiedon virheellisyytenä. (Alperovitch, 2011) Fyysiseen ja käyttäjäkerrokseen kohdistuvia vaikutuksia ei pidä unohtaa. Kyberhyökkäys voi vaikuttaa fyysisen laitteen toimintaan ja ihmiset itsessään luovat potentiaalisen hyökkäysvektorin järjestelmiin. (US Joint Chief of Staff, 2018; McKenzie, 2017, Conti, ym., 2014; Ducheine & van Haaster, 2014)

Puolustukselliset vaikutukset tähtäävät toiminnanvapauden säilyttämiseen omissa verkoissa. Päämääränä on oman kybertoimintaympäristön suojaaminen kyberhyökkäysten vaikutuksilta joko aktiivisten tai passiivisten keinojen kautta. Vaikutukset ilmenevät parempana hyökkäysten sietokykynä ja toipumiskykynä sekä kykynä havaita omien verkkojen haavoittuvuudet ja siellä ilmenevät poikkeamat. (Laari, y., 2019; US Joint Chiefs of Staff, 2018; Ducheine & van Haaster, 2014)

Kyberoperaatioiden vaikutukset voivat joko suunnitellusti tai tahattomasti kertautua tai voimistua ja niillä voi ilmetä myös rinnakkaisia vaikutuksia. (US Joint Chiefs of Staff, 2018)

TAULUKKO 10 Kyberoperaatioiden vaikutukset

Tyyppi	**Alatyyppi**	**Selite**
Kyberoperaatioiden vaikutukset	Hyökkäykselliset	Tiedon katoaminen, tiedon vuotaminen, järjestelmän käytön estyminen tai häiriintyminen, fyysinen tuho
	Puolustukselliset	Oman verkon ja tiedon suojaaminen, vaikutusten vähentäminen, toipumiskyvyn lisääminen
	Kertautuvat, voimistuvat ja rinnakkaiset vaikutukset	Aktiivisista toimista johtuvat vaikutukset, kohteena omat ja muiden verkot

3.4 Analyysin tulokset ja vastaus päätutkimuskysymykseen

Tutkimuksen päätutkimuskysymys oli: Miten kyberoperaatioita voidaan käyttää pelotteen luomiseen? Päätutkimuskysymykseen vastaamiseksi tarkasteltiin

klassisia peloteteorioita ja niiden nykypäivän soveltamista, kyberpelotetta ja kyberoperaatioita kutakin erillisinä kokonaisuuksina. Nämä kokonaisuudet teemoiteltiin ja tyypiteltiin kirjallisen aineiston perusteella yksinkertaisiksi taulukoiksi. Tyypittelyssä oli oleellista löytää ne tekijät, joista pelote ja kyberpelote rakentuvat sekä millaisia vaikutuksia suorituskyvyillä tulee aikaansaada pelotevaikutuksen luomiseksi. Taulukossa 11 esitetään analyysin tulokset.

Koska kyberpelote voidaan ymmärtää eri tavoin luvussa 2.2 kuvatulla tavalla, tehtiin tässä tutkimuksessa tutkimusongelmaan sopiva valinta. Kyberpelotteella tarkoitetaan tässä tutkimuksessa sotilaallisen kybervoiman käyttöä pelotetarkoituksessa sotilaallista hyökkäystä vastaan. Vaikka näkökulma on akateemisessa tutkimuksessa vähemmän käytetty, saattaa se siksi olla hedelmällinen näkökulma tutkia.

Aineiston analyysin perusteella päädyttiin johtopäätökseen, jonka mukaan kyberpelote on pehmeänä vaikuttamisen keinona yksinään heikko. Uskottavampi asetelma saavutetaan, kun kybersuorituskykyjä käytetään yhdessä muiden sotilaallisten suorituskykyjen kanssa. Kyberhyökkäyksiä vastaan tehokkain pelote koostuu kaikista käytettävissä olevista keinoista, kuten poliittinen painostus, taloudelliset sanktiot tai sotilaalliset suorituskyvyt.

Kybersuorituskykyjä voidaan viestiä käytettävän tai demonstroida lähes jokaiseen pelotteen keinovalikoiman keinoon liittyen. Kybertoimintaympäristön näkökulmasta taloudelliset keinot voivat kohdistua esimerkiksi informaatioteknologian vientiin ja tuontiin liittyviin sanktioihin, jolloin keinoilla voi olla vaikutusta kohdevaltion kyberturvallisuuteen pitkällä aikavälillä. Poliittiset keinot voivat olla esimerkiksi kyberturvallisuuteen liittyvän yhteistyön vahvistamista ja sen julki tuomista tai valtion strategia kyberuhkiin vastaamisesta.

Kybersuorituskyvyt ovat osa valtion asevoimien suorituskykyä, mutta ne luetaan ei-kineettisiin toimiin. Näin ollen konventionaalinen asevoima ja ydinase ovat sellaisia suorituskykyjä, jonka osana hyökkäykselliset kybersuorituskyvyt eivät ole varsinaisesti, mutta niitä voidaan käyttää edellä mainittujen kanssa pelotekeinoina. Puolustuksellisia kyberoperaatioita tarvitaan turvaamaan näiden suorituskykyjen käyttö ja takaamaan toiminnanvapaus jokaisessa sotilaallisessa ulottuvuudessa. Kybersuorituskykyjä voidaan käyttää myös peloteviestinnässä vakuuttamaan potentiaalinen uhkatoimija siitä, että konventionaalinen asevoima ja ydinase ovat kybersuojatut ja toimintavalmiit.

Kybersuorituskykyjen käyttö liittyy kiinteästi informaatiovaikuttamiseen ja elektroniseen sodankäyntiin, koska toimet kohdistuvat tai ne toteutetaan saman informaatioteknologisen ympäristön kautta. Tällöin ympäristö ja sitä käyttävät ihmiset ovat joko kohde tai väylä haluttujen vaikutusten luomiseen.

Kyberoperaatioiden piirteet määräävät sen, miten niitä on optimaalisinta käyttää pelotevaikutusten luomiseen. Puolustuksellisiin kyberoperaatioihin ja JOJÄ-operaatioihin kuuluu omien verkkojen suojaamiseen, hyökkäysten sietokyvyn kasvattamiseen ja nopeaan toipumiskykyyn tähtääviä toimia. Näillä toimilla varmistetaan, että kyberhyökkäyksien vaikutuksia kyetään vähentämään omissa järjestelmissä. Tällöin uhkatoimija ei pääse tarkoittamaansa vaikutukseen. Uhkatoimijan toimien tyhjäksi tekeminen on kieltopelotteen hengen mukaista

toimintaa, joten puolustuksellisten kyberoperaatioiden suojatoimien ja JOJÄ-operaatioiden voidaan katsoa soveltuvan nimenomaan kieltopelotteen yhdeksi osatekijäksi kybertoimintaympäristössä.

Hyökkäykselliset kyberoperaatiot ja puolustuksellisten kyberoperaatioiden vastatoimet sisältävät aktiivista ja uhkatoimijaan vaikuttavaa toimintaa. Hyökkäyksellisiä kyberoperaatioita voidaan toteuttaa osana muita sotilaallisia operaatioita täydentäen operaatioiden yhteisvaikutusta. Vastatoimet tähtäävät usein uhkatoimijan lyömiseen kybertoimintaympäristössä sen jälkeen, kun hyökkäysaikeet on havaittu tai hyökkäys jo alkanut. Hyökkäyksellisen luonteensa vuoksi näitä kahta operaatiotyyppiä voidaan käyttää osana rankaisupelotetta. Toisaalta vastatoimien luonteen vuoksi ne voivat olla myös osa kieltopelotetta silloin, kun uhkatoimijan toimet pyritään tekemään tyhjiksi, mutta tarvetta varsinaiseen uhkatoimijan vahingoittamiseen ei ole.

Pelotteen yksi tärkeä tekijä on viestintä, jossa omia suorituskykyjä uskottavasti esittelemällä saadaan uhkatoimija pidättäytymään hyökkäyksestä. Valtiot harvoin haluavat julkistaa yksityiskohtaisesti omia kybersuorituskykyjään. Tästä syntyykin todellinen haaste, mikäli kyberpelotetta aiotaan käyttää yksinään. Edullisempaa onkin, että muun peloteviestinnän keinoin vakuutetaan uhkatoimija siitä, että myöskään kybertoimintaympäristöön kohdistuvia hyökkäyksiä ei suvaita ja niistä seuraa vastatoimia. Toinen mahdollisuus on hienovaraisesti vihjailla omista suorituskyvyistä paljastamatta liikaa, mutta vaarana tässä on, ettei vastapuoli ymmärrä mitä viestitään.

TAULUKKO 11 Kyberoperaatioiden käyttö osana pelotetta

Tyyppi	**Alatyyppi**	**Selite**	**Kyberoperaatiot**
Pelotteen kulmakivet	Suorituskyvyt	Valtion voima	Vaikeaa osoittaa paljastamatta liikaa omista kyvyistä
	Uhka	Voiman käytön mahdollisuudesta muodostuva uhka	Voidaan kommunikoida, mutta tarvitsee myös todistuspohjan
	Viestintä	Uskottava viestintä voiman olemassa olosta ja tahdosta käyttää sitä	Rajallinen mahdollisuus viestiä uskottavasti
	Uhkatoimijat	Näitä vastaan pelote rakennetaan	Tunnistettava uhkatoimijat kybertoimintaympäristössä sekä ne kohteet, joihin uhkatoimija haluaa vaikuttaa

Jatkuu

Taulukko 11 (jatkuu)

Tyyppi	Alatyyppi	Selite	Kyberoperaatiot
Pelotteen tyyppi	Kielto	Minimoidaan hyökkääjän saama hyöty	Puolustukselliset kyberoperaatiot, JOJÄ-operaatiot
	Rankaisu	Rankaistaan hyökkääjää	Hyökkäykselliset kyberoperaatiot, puolustuksellisten kyberoperaatioiden vastatoimet
Pelotteen osatekijä	Viestintä	Miten oma pelote kommunikoidaan	Viestitään osana muuta pelotetta
	Suorituskyky	Poliittinen, sotilaallinen, yhteiskunnallinen suorituskyky	Vaikeaa osoittaa paljastamatta liikaa omista kyvyistä. Demonstroidaan muita suorituskykyjä.
	Uskottavuus	Miten uhkatoimija tulkitsee peloteviestinnän	Muilla suorituskyvyillä saavutettava riittävä uskottavuus
	Intressi	Omien intressien suojeleminen	Kybertoimintaympäristön suojaaminen
	Vakuus	Julkisesti kommunikoitu tae siitä, että mitä vastustaja ei menetä/ hyötyy, jos pidättäytyy hyökkäämästä	Osana kokonaispelotetta
	Pelko	Uhkatoimijassa herätetty pelko	Osana kokonaispelotetta
	Riskihyötysuhteen laskeminen / rationaalisuus	Uhkatoimijan harkinta	Osana kokonaispelotetta
	Resilienssi	Oma kyky toipua hyökkäyksestä	JOJÄ-operaatiot

4 POHDINTA

4.1 Johtopäätökset ja pohdinta

Tässä tutkimuksessa etsittiin vastausta kyberoperaatioiden käyttömahdollisuuksista pelotevaikutusten luomiseen teemoittelemalla ja tyypittelemällä teoreettista lähdeaineistoa. Aineiston keruuta varten muodostettiin tutkijan esiymmärryksen pohjalta kolme teemaa: pelote, kyberpelote ja kyberoperaatiot. Nämä teemat johtivat aineiston keruuta ja analyysiä. Aineistolähtöisen laadullisen analyysin avulla muodostettiin vastaus ensin alatutkimuskysymyksiin. Tehdyistä havainnoista luotiin synteesi päätutkimuskysymykseen vastaamiseksi.

Tutkimuksen ensimmäisten analyysikierrosten aikana tehtiin kaksi havaintoa, jotka ohjasivat analyysin jatkamista. Ensinnäkin, Toisen maailmansodan jälkeen syntynyt jako kielto- ja rankaisupelotteeseen on perustavanlaatuinen. Vaikka globaalin uhkaympäristön ja kybertoimintaympäristön kehitys ovat asettaneet uudenlaisia vaatimuksia pelotestrategioille, pohjautuvat ne kuitenkin mainitulle kahtiajaolle. Toisekseen, kyberpelote on haastavaa rakentaa pelkin kybersuorituskyvyin kybertoimintaympäristössä tapahtuvaksi toiminnaksi muun muassa attribuutiohaasteen ja valtioiden pyrkimyksen salata kybersuorituskykynsä takia.

Tutkimuksen johtopäätöksenä voidaan esittää, että kyberoperaatioita voidaan käyttää sekä kielto- että rankaisupelotevaikutusten luomiseen, mutta yksinään ne eivät ole tarpeeksi uskottavia kybertoimintaympäristön suvereniteetin suojaamiseksi. Michael Fischerkellerin (2017) ja Martin Libickin (2009) esittämien johtopäätösten mukaisesti, myös tässä tutkimuksessa todettiin, että kyberpelotetta onkin edullisempaa tarkastella osana valtion pelotestrategiaa, joka sisältää sotilaallisten suorituskykyjen lisäksi muita valtion voiman instrumentteja, kuten poliittiset ja taloudelliset sekä lain ja informaatioympäristön mahdollistamat keinot.

Kyberpelotetta on tutkittu 2000-luvulla peilaten klassisiin peloteteorioihin ja myös niistä irrallaan ja kyseenalaistaen kyberpelotteen rakentamisen mahdollisuudet. Akateemisessa keskustelussa ei olla päästy yksimielisyyteen siitä, millä tavoin kyberpelote tulisi rakentaa ja onko sillä mahdollisuuksia onnistua. Aineiston teemoittelun ja tyypittelyn avulla löydettiin kuitenkin suuntaviivoja siitä, millä tavoin kyberpelote voitaisiin rakentaa onnistuneimmin. Yksi oleellisimmista huomioista on, että koska kybertoimintaympäristö leikkaa läpikoko yhteiskunnan toiminnot ja myös sotilaallisen toimintaympäristön fyysiset ulottuvuudet, ei pelkkä kyberpelote vain kybertoimin toteutettuna ole kestävä ratkaisu.

Kyberpelote on edullisinta rakentaa osana muuta pelotetta, koska erilaisia keinoja yhdistelemällä valtiolla on suuremmat mahdollisuudet vakuuttaa uhkatoimija siitä, että aggressiota vastaa vähintään yhtä suuri vastatoimi tai aggressiolla ei saavuteta haluttuja vaikutuksia. Nykyaikainen uhkaympäristö ja kompleksiset kansainväliset suhteet edellyttävät onnistuneelta pelotteelta yhdistelmää poliittisia, taloudellisia ja sotilaallisia keinoja. Kyberpelote on osa tätä kokonaisuutta. Pelotevaikutus luodaan edelleen klassisen peloteteorian mukaan kieltoja rankaispelotteen yhdistelmänä, mutta keinovalikoimaan on syntynyt ydinaseen ja konventionaalisen asevoiman rinnalle pehmeitä keinoja, kuten kyberoperaatiot, poliittinen eristäminen ja taloudelliset sanktiot. Puolustautuminen tai rankaisu ei ole symmetristä, koska esimerkiksi kyberhyökkäyksiin voidaan vastata vaikkapa poliittisin keinoin ja kansainväliseen lakiin ja sopimuksiin nojaten. Toisaalta taas usein paras puolustus kybertoimintaympäristössä on tekoälyn tarjoama välitön ja tehokas vastareaktio.

Kyberoperaatioiden rooli nousee useimmiten esiin pelotteessa silloin, kun uhkatekijät kohdistuvat kybertoimintaympäristöön. Yleensä kyberhyökkäyksiin halutaan vastata symmetrisesti kyberoperaatioiden keinoin, koska tällöin on mahdollista saavuttaa nopea ja välitön vastareaktio. Toisaalta taas samalla on tavoite toipua kyberhyökkäyksestä mahdollisimman nopeasti ja palauttaa järjestelmien toiminta ilman suuria vahinkoja. Nämä toiminnot edellyttävät oman taistelutilan hallintaa kybertoimintaympäristössä. Omat verkot ja järjestelmät tulee tuntea, jotta kyetään rakentamaan ensinnäkin onnistunut puolustus ja toisekseen kyky kestää hyökkäykset ja toipua niistä. Näin ollen kaikkia kyberoperaatioiden tyyppejä tukitoimintoineen tarvitaan onnistuneen kyberpelotteen rakentamisessa.

Puolustuksellisilla kyberoperaatioilla ja johtamisjärjestelmäoperaatioilla luodaan kyberpelotteen perusta sekä kielto- että rankaisupelotteen näkökulmasta. Johtamisjärjestelmäoperaatio tulee käsittää jatkuvana ja pitkäaikaisena panostuksena kyberturvallisuuden rakentamiseen ja kehittämiseen. Resilienssin rakentaminen nojaa täysin JOJÄ-operaation varaan, koska tässä operaatiotyypissä painopiste on tietojärjestelmien ja tietoverkkojen ylläpidossa, hallinnassa, häiriönsiedossa ja palauttamisessa sekä kehittämisessä. JOJÄ-operaatio mahdollistaa resilienssin luomisen turvattaviin järjestelmiin ja luo täten edellytyksiä kieltopelotteen onnistumiseen, koska kyky toipua vie uhkatoimijan hyökkäyksiltä terävimmän kärjen.

Puolustukselliset kyberoperaatiot sisältävät suojatoimet ja vastatoimet. Suojatoimiin kuuluvat muun muassa verkonvalvonta, järjestelmien aktiiviset muutokset, uhkanmetsästyksen ja uhkatoimijoiden harhautukset. Näillä toimilla luodaan JOJÄ-operaatioiden ohella perusta kieltopelotteelle. Verkonvalvonnalla havaitaan anomaliat omissa verkoissa ja uhkametsästyksellä jäljitetään hyökkäyksen alkuperä sekä sen vaikutukset omissa verkoissa. Mikäli näitä toimintoja toteutetaan tekoälyn ja koneoppimisen avulla, voidaan saavuttaa reaaliaikainen kyky havaita ja tunnistaa uhkatoimija.

Vastatoimiin kuuluvat sellaiset keinot, joilla lyödään uhkatoimija pois omista verkoista ja estetään sen mahdollisuudet jatkaa toimintaansa. Vastatoimiin voi kuulua myös uhkatoimijan toimintakyvyttömäksi tekeminen ja tällaiset toimet voivat ulottua omien verkkojen ulkopuolelle, jotta päästään uhkatoimijan resursseihin kiinni. Vastatoimia voidaan toteuttaa myös tekoälyn ja koneoppimisen avulla, jolloin saavutetaan reaaliaikainen kyky vastata uhkatoimiin. Vastatoimet ovat rankaisupelotteen keino lievemmässä muodossa kuin varsinainen hyökkäyksellinen kyberoperaatio. Vastatoimilla viestitään uhkatoimijalle, että hyökkäys on havaittu ja siihen kyetään vastaamaan.

Hyökkäykselliset kyberoperaatiot ovat yksi rankaisupelotteen keino. Siinä missä JOJÄ-operaatiot ja puolustukselliset kyberoperaatiot tähtäävät kiistämään uhkatoimijan toimien vaikutuksen omissa verkoissa, on hyökkäyksellinen kyberoperaatio selvä keino toteuttaa rankaisupelotetta. Sven Herpigin (2015) tavoin tässä tutkimuksessa tehtiin havainto, että kyberhyökkäykset ovat kohteeseen räätälöityjä ja tällä tavoin ainutkertaisia. Usein kyberhyökkäyksen valmistelu vie aikaa, koska kohdejärjestelmä on tiedusteltava, kartoitettava ja siihen on luotava jalansija vaikutuksen toteuttamiseen haluttuna ajankohtana. Tällaiseen toimintaan ei täysin kyetä käyttämään tekoälyä ja koneoppimista, koska välttämättä tarvitaan myös ihmisen tilanteenarviointia ja päätöksentekoa. Hyökkäyksellisellä kyberoperaatiolla kyetään selkeään ja voimakkaaseen vastatoimeen, mutta riskinä on hyökkäysten vaikutusten hallitsematon leviäminen tai kriisin eskaloituminen. Näiden seikkojen takia ulkopuoliseen verkkoon tai järjestelmään vaikuttaminen on riskialtis toimenpide.

Johtopäätöksenä voidaan esittää, että kyberoperaatioilla, etenkin JOJÄ- ja puolustuksellisilla kyberoperaatioilla, on selkeä rooli pelotteen luomisessa kybertoimintaympäristössä tai sen välityksellä tapahtuvia uhkatoimia vastaan. Hyökkäykselliset kyberoperaatiot toimivat parhaiten osana kokonaispelotetta, johon liittyy asevoiman käytön lisäksi myös poliittiset ja taloudelliset keinot. Jotta hyökkäyksellistä kyberoperaatiota kannattaisi käyttää osana pelotevaikutusta, on oltava selkeäksi osoitettava syy, miksi näin tehdään. Luultavasti tällaisessa tilanteessa uhkatoimija tekee jo niin provosoivia ja vahingoittavia tekoja, että vain kyberoperaatio ei riitä riittävään vastatoimeen, vaan on tarpeen käyttää myös muita pelotekeinoja. Tässä vaiheessa saattaa mennä myös raja siinä, onko kyseessä enää puhtaasti pelotevaikutus vai jo alkavan kriisin torjuminen ja eskalaation estäminen. Näiltä osin tutkimuksen tulokset myötäilevät Martin Libickin (2009) tekemiä havaintoja puolustuksellisten ja hyökkäyksellisten kyberoperaatioiden roolista pelotevaikutusten luomisessa.

Tutkimusta ei oltu rajattu tiettyyn valtioon, joten tutkimustuloksia voidaan pitää yleisluontoisena kuvaksena tarkastellusta ilmiöstä. On kuitenkin huomattava, että valtioiden pelotestrategiat eroavat käytännössä toisistaan muun muassa valtion geopoliittisen aseman, koon ja käytettävissä olevien resurssien mukaan. Esimerkiksi valtio, jolla ei ole omaa ydinasetta, joutuu nojaamaan pelotteessa muihin suorituskykyihin tai sotilaallisen liittoutumisen myötä liittolaisvaltioiden ydinasepelotteeseen. Tutkimuksessa ei myöskään käsitelty muita uhkatoimijoita kuin toinen valtio. Nykyajan uhkaympäristössä muun muassa terrorismi ja rikollisuus luovat etenkin kybertoimintaympäristön mahdollistamana oma uhkatoimijakokonaisuutensa. Näitä tulee tarkastella pelotteen näkökulmasta eri tavoin kuin toista valtiota, lähtien motivaatiotekijöistä ja rationaalisuuden oletuksesta, joka liittyy kiinteästi pelotteen teoriaan. Tutkimuksen tuloksia voidaankin pitää yleiskuvauksena aiheesta ja tulosten soveltaminen määriteltyihin tapauksiin on tehtävä erillistarkasteluina.

Tässä tutkimuksessa syvennettiin olemassa olevia käsityksiä tutkittavasta aiheesta. Lisäksi huomattiin, että vaikka kyberpelotetutkimus painottuu hyökkäyksellisten kybersuorituskykyjen käyttöön, saattaa olla valtiolle edullisempaa keskittyä puolustuksellisiin kybersuorituskykyihin, joilla turvataan oma kybertoimintaympäristö ja luodaan siihen resilienssiä. Kieltovaikutus saattaa olla uskottavampi kuin rankaisulla uhkaaminen. Tutkimuksen tuloksia voidaan hyödyntää jatkotutkimuksessa alaluvussa 4.3 kuvatulla tavalla tai mikäli halutaan tutustua tutkittuun aiheeseen yleisellä tasolla vaikkapa Jyväskylän yliopiston opetuksessa.

Lopuksi voidaan todeta, että kyberpelote yksinään ei riitä tarvittavan pelotevaikutuksen luomiseen kyberhyökkäyksiä vastaan. Valtioiden tulee hyväksyä, että väistämättä kyberhyökkäyksiä tulee esiintymään toisten valtioiden ja muiden toimijoiden toteuttamina. Niistä ei pelotevaikutuksella päästä nykyajan tekniikalla eroon, mutta kokonaisvaltaisella pelotteella voidaan yrittää ennaltaehkäistä kyberhyökkäysten vakavimpia muotoja, jotka vaikuttavat kriittisiin yhteiskunnan toimintoihin. Tähän puolestaan ei riitä kyberoperaatioiden käyttö yksinään, vaan tarvitaan valmiutta käyttää muitakin keinoja kyberoperaatioiden tueksi tai niiden sijaan. Ennen kaikkea valtioiden tulee määritellä ja selkeästi viestiä ne rajat, joita ei sovi ylittää kybertoimintaympäristössä tai muilla suvereniteetin osa-alueilla. Samoin valtioiden tulee viestiä omasta kyberpuolustuksen kyvystä riittävästi, jotta kieltopelote muodostuu uskottavaksi. Koska kybersuorituskyvyt halutaan yleisesti pitää salassa, on todellinen haaste kertoa tarpeeksi ja uskottavasti, mutta ei liikaa paljastaen.

4.2 Tutkimuksen luotettavuuden tarkastelu

Tieteelliseen tutkimukseen kuuluu tutkijan kyky arvioida oman tutkimuksensa luotettavuutta. Määrällisessä tutkimuksessa luotettavuutta arvioidaan reabiliteetin ja validiteetin arvioinnilla. Näistä reabiliteetilla tarkoitetaan mittaustulosten

toistettavuutta ja validiteetilla mittarin tai tutkimusmenetelmän kykyä mitata tarkoitettua asiaa. (Hirsjärvi, Remes & Sajavaara, 2015)

Laadullisessa tutkimuksessa on usein luontevampaa mitata luotettavuutta arvioimalla tutkimuskokonaisuutta. (Metteri, 2008) Arvioinnissa huomioidaan tutkijan kyky raportoida tarkasti käyttämänsä tutkimusmenetelmät ja tutkimuksen vaiheet. Tarkkuus raportoinnissa parantaa tutkimuksen avoimuutta ja läpinäkyvyyttä. Esimerkiksi haastatteluista raportoidaan se, miten haastattelut ovat käytännössä toteutettu ja niiden tulokset tulkittu. Aineiston analyysissä tutkija raportoi käyttämänsä luokittelumenetelmät ja perustelee tekemänsä päätelmät aineistosta. (Hirsjärvi, Remes & Sajavaara, 2015)

Laadullisen tutkimuksen luotettavuuden arvioinnissa voidaan kiinnittää huomiota esimerkiksi tutkijan lähtökohtiin tutkimuksen toteuttamisessa, tutkijan omaan arvioon tutkimuksen luotettavuudesta sekä siihen, miten tutkija on raportoinut tutkimuksensa vaiheet ja tulokset. Tarkasteltavia seikkoja ovat myös tutkimuksen tavoite, tarkoitus ja kohteet sekä aineiston keruu- ja analyysimenetelmät. (Metteri, 2008)

Tässä tutkimuksessa tutkimuskysymyksiin vastaaminen tutkimusmenetelmineen on esitelty luvussa 1 ja raportoitu tarkemmin luvussa 3. Lukuun 3 on sisällytetty myös lopullisen mallin ulkopuolelle jätetty luokitteluaineisto ja perusteltu, miksi kyseisiä kohtia ei sisällytetty johtopäätöksiin. Tällä tavoin tutkija pyrkii osoittamaan oman loogisen päättelyketjunsa kulkua ja analyysin vaiheita, joista lopulta syntyy tutkimuksen lopputulos. Avoimuuteen on pyritty myös esittämällä luvussa 3 ne lähteet, joihin esitetyt päätelmät perustuvat.

Tutkijan oma esitietämys aiheesta on esitetty luvussa 1 ja myös sen vaikutus ennakko-oletuksiin, jotka ovat väistämättä vaikuttaneet muun muassa tutkimuskysymyksien ja tutkimuksen viitekehyksen muodostamiseen sekä niihin hakusanoihin, joilla lähdemateriaalia kerättiin tietokannoista. Hermeneuttisen tieteenfilosofian ja laadullisen tutkimuksen periaatteiden mukaan on hyväksyttävää, että tutkija sisällyttää oman esitietämyksensä tutkimukseen, koska lopunperin laadullinen analyysi on tutkijan tulkinta aiheesta.

Aineisto-, menetelmä-, teoria- tai tutkijatriangulaatiota käytetään erityisesti sellaisessa tutkimuksessa, jossa käsitellään epävarmaa tietoa tai yksilöiden käsityksillä on oleellinen merkitys tutkimusaineistossa. Esimerkiksi aineistotriangulaatiossa kerätään erilaisia aineistoja tutkimusongelmaan vastaamiseksi. Menetelmätriangulaatiossa sen sijaan käytetään erilaisia aineiston keruu- ja analyysimenetelmiä. (Metteri, 2008)

Tämän tutkimuksen aiheesta oli löydettävissä runsaasti materiaalia, joten yksittäisten ihmisten käsityksillä ei ollut suurta painoarvoa tutkimustulosten muodostamisessa. Koska tutkimuksen lähtökohtana oli muodostaa teoreettinen käsitys aiheesta, ei esimerkiksi haastatteluja katsottu tarpeellisiksi. Asia olisi toisin, jos tutkimus olisi esimerkiksi pyrkinyt vertaamaan muodostettuja johtopäätöksiä yksilöiden, esimerkiksi poliitikkojen ja kyberasiantuntijoiden, käsityksiin.

Tässä tutkimuksessa aineisto koostui kolmesta aihekategoriasta, jotka olivat pelote, kyberpelote ja kyberoperaatiot. Aineistoksi kerättiin tieteellisiä artikkeleita ja kirjoituksia, mutta kyberoperaatioiden osalta nojauduttiin osittain

sotilaallisiin doktriineihin ja ohjesääntöihin, jotta käsitys kyberoperaatioista olisi realistinen. Varsinaisen aineistotriangulaation muodostamiseen tämä jaottelu on kuitenkin liian heikko, koska sotilaallisen materiaalin osuus on vähäinen ja painottuu vain muutaman valtion kirjoituksiin, eikä tutkimuksessa tehty tarkastelua esimerkiksi sotilaallisten doktriinien ja tieteellisen tutkimuksen yhteyksistä ja eroista.

Esitettyjen perusteluiden perusteella, tämän tutkimuksen voidaan katsoa olevan avoimesti raportoitu ja niiltä osin luotettava. Tutkimuksen luotettavuutta olisi voitu nostaa triangulaation keinoin, mutta tutkija ei tässä tapauksessa katsonut sitä tarpeelliseksi tutkimusongelmaan vastaamiseksi.

4.3 Jatkotutkimusaiheet

Tutkimuksessa muodostettiin teoreettinen käsitys kyberoperaatioiden käytöstä pelotevaikutusten luomiseen. Tämä käsitys voi toimia pohjana tutkimusaiheen syventämiselle jatkotutkimuksessa, esimerkiksi rikastamalla luotua mallia haastatteluiden avulla tai käytännön esimerkein. Tällainen aiheen syventäminen voi luoda tietoa siitä, onko kyberoperaatioilla käytännön mahdollisuuksia toimia pelotevaikutusten luomiseen, vai tekevätkö esimerkiksi valtioiden halu salata kybersuorituskykynsä ja attribuutiohaaste tästä liian haastavaa.

Tutkimuksessa ei otettu kantaa valtion kokoon ja asemaan kansainvälisessä politiikassa. Yksi jatkotutkimusaihe voisi olla siinä, onko pelotteen muodostaminen mahdollista ylipäätään vain globaaleille suurvalloille ja onko pienemmillä valtioilla mahdollisuuksia olla tarpeeksi uskottavia toimijoita pelotteen luomisessa yksin tai jonkin liittouman tai yhteisön jäsenenä. Kybersuorituskykyjen käyttö tässä kontekstissa on myös mielenkiintoinen tutkimuskohde useastakin syystä.

Ensinnäkin, kybertoimintaympäristöllä on sellaisia ominaisuuksia, jotka tekevät siitä globaalin toimintaympäristön esimerkiksi Internetin myötä. Valtioiden on siis huomattavasti haastavampaa suojella omaa suvereniteettiaan kybertoimintaympäristössä kuin fyysisessä ulottuvuudessa. Voidaanko pelotteella ylipäätään suojella kybertoimintaympäristöä, vai onko teknologisesti edistyneiden valtioiden vain siedettävä kyberhyökkäyksiä?

Toisekseen, maailmassa on valtioita kuten Venäjä ja Kiina, jotka pyrkivät eristämään oman verkkonsa muusta maailmasta. Vähentääkö tällainen pyrkimys keinovalikoimaa pelotteelta yleensä?

Kolmanneksi, perinteisessä mielessä pieni valtio ei välttämättä ole pieni kybertoimintaympäristössä, mikäli valtiolla on sellaisia kybersuorituskykyjä ja tahtoa käyttää niitä, jotka vetävät vertoja suurvalloille. Kybertoimintaympäristö mahdollistaa myös epäsymmetristen keinojen käyttämisen, joten tämä saattaa toimia pienen valtion eduksi sissitaktiikan hengessä. Voisiko siis pieni valtio rakentaa uskottavan pelotteen kybersuorituskykyjensä avulla?

Pelotteen yksi kulmakivistä on onnistunut viestintä. Tämä tarkoittaa valtion kykyä kertoa aikeensa yksiselitteisesti potentiaaliselle uhkatoimijalle siitä,

että aggressiota seuraa vähintään yhtä voimakas vastatoimi tai aggressiolla ei tulla pääsemään haluttuun lopputulokseen suunnitelluin keinoin. Peloteviestintä kybersuorituskykyjen käytöstä on haastavaa jo sen vuoksi, että valtiot eivät halua paljastaa liikaa omista suorituskyvyistään. Miten siis demonstroida kybervoimaa, jos mitään ei haluta paljastaa? Tähän kysymykseen vastaaminen muodostaa yhden jatkotutkimusaiheen, joka voidaan yhdistää myös pelotetutkimukseen yleensä: miten erilaisia suorituskykyjä demonstroidaan, jotta luodaan uskottava mielikuva omasta voimasta?

LÄHTEET

Alperovitch, D. (2011). Towards Establishment of Cyberspace Deterrence Strategy. Teoksessa E. Tyugu, T. Wingfield & C. Czosseck. (toim.), *2011 3rd International Conference on Cyber Conflict* (s. 87–94). CCD COE Publication. http://195.222.11.251/uploads/2018/10/TowardsEstablishmentOfCyberstapeDeterrenceStrategy-Alperovitch.pdf

Arie, K. (2016). Complex Deterrence Theory and the Post-Cold War Security Environment. Teoksessa *NIDS Journal of Defense and Security* (s. 21–39). http://www.nids.mod.go.jp/english/publication/kiyo/pdf/2016/bulletin_e2016_3.pdf

Bendiek, A. & Metzger, T. (2015). *Deterrence theory in the cyber-century.* Working Paper, Research Division EU/Europe, Stiftung Wissenschaft und Politik German Institute for International and Security Affairs. https://www.swp-berlin.org/publications/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Brantly, A. (2018). The Cyber Deterrence Problem. Teoksessa T. Minárik, R. Jakschis, L. Lindström (toim.), *2018 10th International Conference on Cyber Conflict* (s. 31–53). CCD COE Publication. https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf

Burton, J. (2018). *Cyber Deterrence: A Comprehensive Approach?* Nato Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Chen, J. (2017a). Deterrence and its Implementation in Cyber Warfare. Teoksessa A. Bryant, J. Lopez & R. Mills (toim.), *ICCWS 2017 12th International Conference on Cyber Warfare and Security* (s. 83–89). ACPIL.

Chen, J. (2017b). Take the Rein of Cyber Deterrence. Teoksessa E. Sobiesk, D. Bennett, P. Maxwell (toim.), *2017 IEEE International Conference on Cyber Conflict* (s. 29–35). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8167510

Chen, J. (2018a). Does Conventional Deterrence Work in the Cyber Domain? Teoksessa A. Jesang (toim.), *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2* (s. 106–111). ACPIL.

Chen, J. (2018b). Effectively Exercising Deterrence in the Cyber Domain. Teoksessa J. Chen, J. Hurley (toim.). *13th International Conference on Cyber Warfare and Security (*s. 120–125). ACPIL. https://www.proquest.com/conference-papers-proceedings/effectively-exercising-deterrence-cyber-domain/docview/2018924244/se-2

Conti, G., T. Cross, M. Nowatkowski & D. Raymond (2014). Key Terrain in Cyberspace: Seeking the High Ground. Teoksessa B. Pascal, M. Maybaum & J. Stinissen (toim.), *2014 6th International Conference on Cyber Conflict*. CCD COE Publication. https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

Ducheine, P. & J. van Haaster (2014). Fighting Power, Targeting and Cyber Operations. Teoksessa P. Brangetto, M. Maybaum, J. Stinissen (toim.), *2014 6th International Conference on Cyber Conflict*, (s. 287–300). CCD COE Publication. https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. *Survival*. 59. (s. 103-134). https://doi.org/10.1080/00396338.2017.1282679

Freedman, L. (2021). Introduction—The Evolution of Deterrence Strategy and Research. Teoksessa F. Osinga, T. Sweijs (toim.), *NL ARMS Netherlands Annual Review of Military Studies 2020.* NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_1

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice, *Strategic Studies Quarterly* 4, no. 3 (s. 102–135). https://apps.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf

Hanska, J. (2019). Pelotetta vai pidäkettä? Deterrenssiteorian käytäntöä pienen valtion näkökulmasta. *Tiede Ja Ase* (s. 42–70). https://journal.fi/ta/article/view/88681

Herpig, S., (2015). Strategic operations in the cyber domain and their implications for national cyber security. Teoksessa D. Cunningham, P. Hofstedt, K. Meer & I. Schmitt (toim.), *INFORMATIK 2015* (s. 597–607). Bonn: Gesellschaft für Informatik e.V.

Harknett, R. & M. Smeets. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*. (s. 1–34). https://doi.org/10.1080/01402390.2020.1732354

Hirsjärvi, S., P. Remes & P. Sajavaara (2015). *Tutki ja kirjoita*. Bookwell Oy.

Hurley, J. & L.Watkins (2016). Cyberspace: The new Battlefield. Teoksessa D. Slateva (toim.), *ICCWS 2016 11th International Conference on Cyber Warfare and Security* (s. 180–188). APCIL. https://www.proquest.com/conference-papers-proceedings/cyberspace-new-battlefield/docview/1779928728/se-2

Jasper, S. (2015). Deterring Malicious Behavior in Cyberspace. *Strategic Studies Quarterly,* 9(1), (s. 60–85). https://www.jstor.org/stable/26270834

Klimburg, A. (toim.) (2012). *National Cyber Security Framework Manual*. Nato Cooperative Cyber Defence Centre of Excellence. ISBN 978-9949-9211-2-6 PDF.

Kuusisto, R. (2008). Tieteenfilosofia — ajattelun kehys. Teoksessa M. Huttunen & J. Metteri (toim.), *Ajatuksia operaatiotaidon ja Sotataidon laadullisesta tutkimuksesta* (s. 34–65). Maanpuolustuskorkeakoulun Taktiikan laitoksen julkaisusarja 2, Edita Prima Oy.

Laari, T., J. Flyktman, K. Härmä, J. Timonen & J. Tuovinen (2019). *#kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle.* Maanpuolustuskorkeakoulu. https://urn.fi/URN:ISBN:978-951-25-3120-2

Leuprecht, C., J. Szeman & D. Skillicorn (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, 40:3, (s. 382–407). https://doi.org/10.1080/13523260.2019.1590960

Lehto, M. (2018). *Kybermaailma ja tiedustelu*, asiantuntijalausunto Eduskunnan Puolustusvaliokunnalle 20.2.2018. Jyväskylän yliopisto. Asia: HE 198/2017 vp, HE 199/2017 vp, HE 202/2017 vp, HE 203/2017 vp.

Lehto, M. (2016). Theoretical Examination of the Cyber Warfare Environment. Teoksessa D. Zlateva, V. Greiman (toim.), *11th International Conference on Cyber Warfare and Security ICCWS-2016* (s. 223–231). APCIL.

Lehto, M. & J. Limnéll (2017). Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede Ja Ase*, 75 (s. 179–212). https://journal.fi/ta/article/view/67730

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Mazarr; M. (2018). *Understanding Deterrence*. Rand Corporation. https://www.rand.org/pubs/perspectives/PE295.html

Mazarr, M. & J. Goodby (2010). Redefining the role of deterrence. Teoksessa G. Shultz, S. Drell, J. Goodby (toim.), *Deterrence: Its past and future : papers presented at Hoover Institution*, Hoover Institution on War, Revolution, and Peace.

McKenzie, T. (2017). *Is Cyber Deterrence Possible?* Air Force Research Institute, Air University Press. https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

Metteri, J. (2008). Laadullinen tutkimus. Teoksessa M. Huttunen & J. Metteri (toim.), *Ajatuksia operaatiotaidon ja Sotataidon laadullisesta tutkimuksesta* (s. 34–65). Maanpuolustuskorkeakoulun Taktiikan laitoksen julkaisusarja 2, Edita Prima Oy.

Morgan, P. (2003). *Deterrence Now*. Cambridge University Press. https://doi.org/10.1017/CBO9780511491573

Multinational Capability Development Campaign (2014). *Handbook for Integrating Cyber Defense into the Operational Planning Process V1.0*. Kjeller, 2013–14.

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security 2017*; 41 (s. 44–71). https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf

Paul, T. (2009). Complex Deterrence: An Introduction. In T. Paul, P. Morgan & J. Wirtz (toim.), *Complex Deterrence: Strategy in the Global Age* (s. 1-28). University of Chicago Press. https://doi.org/10.7208/9780226650043-003

Puusa, A. & P. Juuti (2021). *Laadullisen tutkimuksen näkökulmat ja menetelmät.* (2. painos). Gaudeamus.

Raitasalo, J. & J. Sipilä (2008). *Sota – teoria ja todellisuus: näkökulmia sodan muutokseen*. Edita Prima oy.

Soesanto, S. & M. Smeets (2021). Cyber Deterrence: The Past, Present, and Future. Teoksessa F. Osinga, T. Sweijs (toim.), *NL ARMS Netherlands Annual Review of Military Studies 2020.* NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_20

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, 33:1, (s. 148–170). https://doi.org/10.1080/13523260.2012.659597

Sweijs, T. & S. Zilincik (2021). The Essence of Cross-Domain Deterrence. Teoksessa F. Osinga, T. Sweijs (toim.), *NL ARMS Netherlands Annual Review of Military Studies 2020.* NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_8

Sweijs, T., Zilincik, S. Bekkers, F. & Meessen, R. (2021). *A Framework for Cross-Domain Strategies Against Hybrid Threats*, The Hague Centre for Strategic

Studies. https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

Taddeo, M. (2018a). The Limits of Deterrence Theory in Cyberspace. *Philos. Technol.* 31, (s. 339–355). https://doi.org/10.1007/s13347-017-0290-2

Taddeo, M. (2018b). *How to Deter in Cyberspace.* Hybrid COE *Strategic Analysis 9.* The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-9-Taddeo.pdf

Tor, U. (2017). 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40:1-2, (s. 92–117). https://doi.org/10.1080/01402390.2015.1115975

UK Ministry of Defence (2016). *Cyber Primer Second Edition*. Development, Concepts and Doctrine Centre. http://www.fraw.org.uk/data/wbd/mod-cyber-2016.pdf

UK Ministry of Defence (2022). *Cyber Primer Third Edition*. Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115061/Cyber_Primer_Edition_3.pdf

US Department of the Army (2021). *FM 3-12 Cyberspace Operations and Electromagnetic Warfare*. https://irp.fas.org/doddir/army/fm3-12.pdf

US Joint Chiefs of Staff (2018). *Joint Publication 3-12 Cyberspace Operations.* https://irp.fas.org/doddir/dod/jp3_12.pdf

US Joint Chiefs of Staff (2017). *Joint Publication 3-0 Joint Operations.* https://irp.fas.org/doddir/dod/jp3_0.pdf

US Army War College (2022). *Strategic Cyberspace Operations Guide*. https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf

Valtioneuvosto (2018). *Turvallisuus ja puolustus – Suomalaisen hyvinvoinnin kivijalka*. Valtioneuvoston julkaisusarja 19/2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162613/19_18_TUKA_PLM_V2.pdf?sequence=1&isAllowed=y

Zagare, F. & D. Kilgour (2000). *Perfect Deterrence. Cambridge Studies in International Relations.* Cambridge University Press. https://doi.org/10.1017/CBO9780511491788